

مرجع التكوين

دليل كامل لجميع معلمات التكوين

نظرة عامة على المعمارية

من / SMPP هي واجهة بروتوكول بلا حالة تقوم بترجمة رسائل SMPP OmniMessage بوابة يتم التعامل مع جميع منطق الأعمال، وقرارات التوجيه، وتخزين الرسائل. OmniMessage إلى : حيث تقوم البوابة ببساطة - OmniMessage Core بواسطة

1. من شركات الاتصالات والعملاء SMPP PDUs **تستقبل**
2. REST عبر واجهة برمجة التطبيقات OmniMessage **ترجمها** إلى تنسيق
3. للرسائل المراد إرسالها OmniMessage **تستعلم** عن
4. إلى شركات الاتصالات SMPP PDUs **ترسل**
5. OmniMessage **تبلغ** حالة التسليم مرة أخرى إلى

جميعها - (Diameter, MAP, IMS) الأخرى OmniMessage هذا هو نفسه كيفية عمل واجهات OmniMessage Core مترجمات بروتوكول بلا حالة تفوض إلى

موقع ملف التكوين

```
/opt/omnimessage-smpp/config/runtime.exs
```

مهم: بعد تغيير التكوين، أعد تشغيل البوابة

```
sudo systemctl restart omnimessage-smpp
```

هيكل التكوين

:الهيكل الأساسي Elixir. يستخدم ملف التكوين بناء جملة

```
import Config

# الإعدادات العالمية
config :omnimessage_smpp,
  setting_name: value

# عمليات الربط SMPP
config :omnimessage_smpp, :binds, [
  %{
    name: "bind_name",
    # ... إعدادات الربط
  }
]
```

الإعدادات العالمية

API_BASE_URL

OmniMessage Core لمنصة URL عنوان

```
config :omnimessage_smpp,
  api_base_url: "https://omnimessage-core.example.com:8443"
```

المعلمة	النوع	مطلوب	الافتراضي
api_base_url	(URL) سلسلة	نعم	-

عبر OmniMessage تتواصل البوابة مع. OmniMessage Core لمنصة URL الغرض: عنوان
للمعالجة جميع الرسائل REST واجهة برمجة التطبيقات

- للمعالجة OmniMessage المستلمة إلى SMPP إرسال الرسائل: إرسال رسائل
- SMPP استرجاع الرسائل: الاستعلام عن الرسائل الموجهة إلى شركات الاتصالات
- لإبلاغ عن حالة التسليم: تحديث حالة تسليم الرسالة مرة أخرى إلى  OmniMessage

- **صحة النظام:** فحوصات صحة دورية

مع OmniMessage **حرج:** هنا تحصل البوابة على كل "عقلها". يتعامل

- التحقق من صحة الرسائل وفحص التنسيق ✓
- قرارات التوجيه (أي شركة اتصالات يجب استخدامها) ✓
- تحديد المعدل والتقليل ✓
- التحقق من صحة الأرقام ✓
- تخزين الرسائل واستمراريتها ✓
- منطق إعادة المحاولة للتسليم ✓
- تتبع الحالة ✓

OmniMessage ↔ SMPP تقوم البوابة ببساطة بترجمة تنسيق

أمثلة:

```
# HTTPS مع IP
api_base_url: "https://192.168.1.100:8443"

# HTTPS مع اسم المضيف
api_base_url: "https://omnimessage-core.company.com:8443"

# HTTP (غير موصى به للإنتاج)
api_base_url: "http://192.168.1.100:8080"
```

متطلبات الشبكة:

- OmniMessage Core يجب أن تكون البوابة لديها وصول إلى الشبكة إلى
- (`verify_ssl_peer` قم بتكوين) في الإنتاج HTTPS استخدم
- على المنفذ المحدد HTTPS يجب أن يسمح جدار الحماية بخروج

OAM/ إدارة API (`api_ex`) منفذ

الخاصة بالبوابة API إدارة/OAM المنفذ لواجهة

واجهة (`/status`, `/smpp/client_peers`, `/smpp/server_peers`, `/smpp/binds`, `/smpp/summary`) الخاصة بها API إدارة/OAM تقدم البوابة واجهة مع الافتراضي، `api_ex` عبر

`api_base_url` هذه **خادم** تستضيفه البوابة — متميز عن `(config/config.exs)` 8443 ، OmniMessage Core الذي هو نقطة النهاية **العميل** التي تستدعيها البوابة على

لا تخطئ بين الاثنين:

المعنى	الافتراضي	الاتجاه	الإعداد
حيث ترسل البوابة/تستعلم عن الرسائل	8443:...	Core → بوابة (عميل)	<code>api_base_url</code>
الخاصة OAM حيث تستمع واجهة بالبوابة	8443	بوابة (خادم)	<code>api_ex</code> <code>port</code>

API أيضًا واجهة OmniMessage Core يستضيف **OmniMessage Core التواجد مع** على **نفس** SMPP عندما تعمل بوابة `api_ex` 8443 الخاصة بالتخزين/الرسائل على منفذ كلاهما الافتراضي 8443 ولا يمكن أن يرتبط سوى واحد منهما — الآخر، Core **المضيف** مثل تضرب الخدمة `/api/messages` وطلبات `:eaddrinuse` يتسبب في حدوث حلقة تحطم مع 404 (الخاطئة، مما يعيد).

المعتمد في `config/runtime.exs` لإصلاح ذلك، قم بتحرير مع تعيين منفذ `api_ex` وقم بإلغاء تعليق تجاوز `(/etc/omnimessage_smpp/runtime.exs)` لا يزال Core الخاصة بالبوابة بعيدًا عن منفذ OAM مجاني بحيث تتحرك واجهة Core: يستهدف 8443 الخاص بـ

```
# OAM الخاصة بالتخزين؛ انقل واجهة API لواجهة 8443: Core يمتلك
8444: الخاصة بالبوابة إلى
config :api_ex,
  api:
    Application.get_env(:api_ex, :api, %{})
    |> Map.put(:port, 8444)
    |> Map.put(:listen_ip, "0.0.0.0")
```

إذا تم ترك التجاوز غير معلق، فإن المنفذ الافتراضي سيكون 8443. لا تحتاج البوابات المستقلة إلى أي تغيير (على مضيف مختلف Core).

SMPP_POLL_INTERVAL

تكرار فحص قائمة الانتظار (بالملي ثانية)

```
config :omnimessage_smpp,  
  smpp_poll_interval: 100
```

المعلمة	النوع	مطلوب	الافتراضي
smpp_poll_interval	عدد صحيح	لا	100

الغرض: كم مرة (بالملي ثانية) يتحقق كل عميل من قائمة الانتظار للرسائل.

الإرشادات:

- **حجم مرتفع (>100 TPS):** 100-500ms
- **حجم متوسط (100-10 TPS):** 500-1000ms
- **حجم منخفض (<10 TPS):** 1000-2000ms

متغير البيئة: SMPP_POLL_INTERVAL

VERIFY_SSL_PEER

SSL التحقق من شهادة

```
config :omnimessage_smpp,  
  verify_ssl_peer: false
```

المعلمة	النوع	مطلوب	الافتراضي
verify_ssl_peer	منطقي	لا	false

الخلفية API عند الاتصال بواجهة SSL **الغرض:** ما إذا كان يجب التحقق من شهادات.

القيم:

- **true:** تحقق من الشهادات (الإنتاج مع شهادات صالحة)
- **false:** تخطي التحقق (شهادات موقعة ذاتيًا، اختبار)

متغير البيئة: VERIFY_SSL_PEER

SMSC_NAME

معرف البوابة للتسجيل

```
config :omnimessage_smpp,  
  smsc_name: "smpp_gateway"
```

المعلمة	النوع	مطلوب	الافتراضي
smsc_name	سلسلة	لا	"smpp_gateway"

الغرض: يحدد هذه النسخة من البوابة في واجهة قائمة انتظار الرسائل الخلفية.

متغير البيئة: `SMSC_NAME`

SMPP تكوين رب ؟؟ عميل

(عميل) **ESME** عمليات الربط الخاصة بالعميل هي اتصالات صادرة حيث تعمل البوابة كـ لشركات الاتصالات. في هذا الوضع، تقوم البوابة ببدء الاتصال لإرسال **SMSC** تتصل بخوادم واستقبال الرسائل عبر شركات الاتصالات الخارجية.

مثال كامل على ربط العميل

```
config :omnimessage_smpp, :binds, [
  %{
    # معرف فريد لهذه الاتصال
    name: "vodafone_uk",

    # وضع الاتصال
    mode: :client,

    # نوع ربط SMPP
    bind_type: :transceiver,

    # لشركة الاتصالات SMPP عنوان خادم
    host: "smpp.vodafone.co.uk",
    port: 2775,

    # تثبيت عنوان/منفذ المصدر المحلي للاتصال الصادر (اختياري
    # (المنفذ المصدر/ IP تعيين إذا كانت شركة الاتصالات تبيض حسب
    bind_source_ip: "10.20.30.40",
    bind_source_port: 5000,

    # بيانات اعتماد المصادقة
    system_id: "your_username",
    password: "your_password",

    # اختياري، تعيين إذا كانت شركة الاتصالات SMPP حقول بروتوكول
    # تتطلب
    system_type: "",
    addr_ton: 0,
    addr_npi: 0,
    address_range: "",

    # تحديد المعدل
    tps_limit: 100,

    # اسم قائمة الانتظار المشتركة (اختياري، الافتراضي هو اسم الربط).
    # تعيين نفس
    # القيمة على عدة روابط لجعلها تستنزف قائمة انتظار واحدة
    # مشتركة.
    queue: "vodafone_uk",

    # تكرار فحص قائمة الانتظار
```

```
queue_check_frequency: 1000,  
  
# فترة التحقق (بالثواني، 0 لتعطيل)  
enquire_link_interval: 60,  
  
# تخزين الرسائل (اختياري)  
cache_enabled: false,  
cache_max_size: 10000,  
cache_retry_interval: 60  
}  
]
```

معلومات ربط العميل

name

معرف الاتصال الفريد

النوع	مطلوب	مثال
سلسلة	نعم	"vodafone_uk"

بشكل فريد SMPP **الغرض**: يحدد هذا الاتصال

- يستخدم في السجلات والقياسات
- يجب أن يكون فريدًا عبر جميع الروابط
- استخدم أسماء وصفية (شركة الاتصالات، المنطقة، الغرض)

اتفاقيات التسمية:

- `carrier_region`: "vodafone_uk", "att_us"
- `purpose_number`: "marketing_1", "alerts_primary"

mode

نوع الاتصال

النوع	مطلوب	القيمة
ذرة	نعم	:client

.خارجي **SMSC** تتصل بـ **ESME الغرض**: يحدد هذا كاتصال صادر حيث تعمل البوابة كـ

.للاتصالات الصادرة :client **القيمة الثابتة**: دائمًا

bind_type

SMPP نوع جلسة

النوع	مطلوب	القيم المسموح بها
ذرة	نعم	:transmitter, :receiver, :transceiver

.**الغرض**: يحدد قدرة اتجاه الرسالة

الخيارات:

- :transmitter (submit_sm) إرسال الرسائل فقط -
- :receiver (deliver_sm) استقبال الرسائل فقط -
- :transceiver إرسال واستقبال (الأكثر شيوعًا) -

.ما لم تتطلب شركة الاتصالات نوعًا محددًا :transceiver **التوصية**: استخدم

host

لشركة الاتصالات SMPP لخدم IP اسم المضيف أو

النوع	مطلوب	مثال
سلسلة	نعم	"أو" 10.5.1.100 "smp carrier.com"

.لشركة الاتصالات SMPP **الغرض**: عنوان خادم

أمثلة:

```
host: "smpp.vodafone.co.uk"
host: "10.20.30.40"
host: "smpp-primary.carrier.net"
```

port

SMPP منفذ خادم

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	نعم	2775	1-65535

SMPP لاتصال TCP الغرض: منفذ

المنفذ القياسي: 2775

أمثلة:

```
port: 2775 # قياسي
port: 3000 # مخصص
```

bind_source_ip

المصدر المحلي للاتصال الصادر IP

النوع	مطلوب	الافتراضي	مثال
سلسلة	لا	(الافتراضي للنظام)	"10.20.30.40"

الصادر إلى شركة الاتصالات. قم TCP المصدر المحلي المستخدم للاتصال IP الغرض: يثبت عنوان المصدر ولدى مضيف البوابة IP بتعيين هذا عندما تقوم شركة الاتصالات بتبويض الاتصالات حسب (المصدر IP يختار النظام عنوان) عدة عناوين. يتم تسجيل عنوان غير صالح وتجاهله.

لا يمكن تحريره (`binds`: يتم قراءته من تكوين تطبيق) **ملاحظة**: هذا حقل خاص بالتكوين فقط Mnesia من واجهة الويب / تخزين.

bind_source_port

المنفذ المصدر المحلي للاتصال الصادر

النطاق	الافتراضي	مطلوب	النوع
1-65535	(عابر)	لا	عدد صحيح

الصادر. قم بتعيين هذا عندما تقوم TCP **الغرض**: يثبت المنفذ المصدر المحلي المستخدم للاتصال بحيث `SO_REUSEADDR` المصدر **و** المنفذ. يتم فتح المقبس مع IP شركة الاتصالات بتبييض حسب `eadrriuse`: بدلاً من الفشل مع) يمكن إعادة ربط المنفذ المثبت على الفور عند إعادة الاتصال (`TIME_WAIT`). بينما يكون المقبس السابق في

هذا حقل خاص بالتكوين فقط ولا يمكن تحريره من واجهة `bind_source_ip`، **ملاحظة**: مثل الويب.

system_id

اسم المستخدم للمصادقة

مثال	مطلوب	النوع
<code>"company_user"</code>	نعم	سلسلة

الغرض: اسم المستخدم المقدم من شركة الاتصالات للمصادقة.

الأمان: احم هذه البيانات - مخزنة في ملف التكوين.

password

كلمة مرور المصادقة

مثال	مطلوب	النوع
<code>"secret_password"</code>	نعم	سلسلة

الغرض: كلمة المرور المقدمة من شركة الاتصالات للمصادقة.

الأمان:

- احم هذه البيانات
- استخدم كلمات مرور قوية
- قم بتدويرها بشكل دوري

tps_limit

حد المعاملات في الثانية

النطاق	الافتراضي	مطلوب	النوع
1-10000	100	نعم	عدد صحيح

الغرض: الحد الأقصى للرسائل في الثانية التي يمكن إرسالها عبر هذا الاتصال

الإرشادات:

- تعيين إلى 70-80% من الحد الأقصى لشركة الاتصالات
- يمنع التقييد/قطع الاتصال
- يسمح بمساحة للتسليم للإصالات

أمثلة:

```
tps_limit: 10    # حجم منخفض
tps_limit: 50    # حجم متوسط
tps_limit: 100   # (الأكثر شيوعًا)
tps_limit: 1000  # حجم مرتفع جدًا
```

الحساب:

TPS إذا كان الحد الأقصى لشركة الاتصالات = 100
 tps_limit = 70-80 تعيين
 مساحة TPS يترك 20-30

queue

اسم قائمة الانتظار المشتركة

النوع	مطلوب	الافتراضي	مثال
سلسلة	لا	اسم الربط	"sinch.smpp"

الخاص **name** الغرض: قائمة الانتظار التي تستنزف منها هذه الربط من الخلفية. الافتراضي هو على عدة **queue** بالربط، لذا تستنزف كل ربط قائمة انتظارها الخاصة. قم بتعيين نفس قيمة روابط لجعلها جميعًا تستنزف قائمة انتظار مشتركة واحدة - على سبيل المثال، اثنان من اتصالات لمشاركة الحمل/الاحتياطي "sinch.smpp" كلاهما يستنزف Sinch.

أمثلة:

```
# رابطان يشتركان في قائمة انتظار واحدة
%{name: "sinch_1", queue: "sinch.smpp", ...}
%{name: "sinch_2", queue: "sinch.smpp", ...}
```

queue_check_frequency

فترة استعلام قائمة الانتظار للرسائل (بالمللي ثانية)

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	نعم	1000	100-10000

الغرض: كم مرة يجب التحقق من الخلفية عن رسائل ❖❖ديدة للإرسال.

الإرشادات:

- **حجم مرتفع (>100 TPS):** 500-1000ms
- **حجم متوسط (100-10 TPS):** 1000-2000ms
- **حجم منخفض (<10 TPS):** 2000-5000ms

التجارة:

- قيمة أقل = أسرع التقاط الرسائل، مزيد من الحمل على واجهة برمجة التطبيقات
- قيمة أعلى = أبطأ التقاط، أقل حمل على واجهة برمجة التطبيقات

enquire_link_interval

SMPP (بالتواني) فترة التحقق من

النطاق	الافتراضي	مطلوب	النوع
0-3600	60	لا	عدد صحيح

للتحقق من أن الاتصال لا SMPP enquire_link PDUs **الغرض**: كم مرة (بالتواني) يجب إرسال enquire_link_resp. يزال نشطًا. يستجيب الخادم البعيد بـ

الإرشادات:

- الافتراضي (60)**: مناسب لمعظم شركات الاتصالات
- قيم أقل (15-30)**: أسرع اكتشاف الفشل، مزيد من الحركة
- قيم أعلى (120-300)**: أقل حمل، أبطأ اكتشاف الفشل
- تمامًا (غير موصى به) enquire_link يعطل: **0**

أمثلة:

```
enquire_link_interval: 60  # قياسي (1 دقيقة)
enquire_link_interval: 30  # تحقق نشط
enquire_link_interval: 0   # معطل
```

system_type

SMPP معرف نوع نظام

مثال	الافتراضي	مطلوب	النوع
"OTP"	" "	لا	سلسلة

المرسل أثناء الربط. تتطلب بعض شركات الاتصالات قيمة محددة. SMPP **الغرض**: حقل بروتوكول. اتركه فارغًا ما لم تحدد شركة الاتصالات واحدة.

addr_ton

نوع عنوان الرقم

النطاق	الافتراضي	مطلوب	النوع
0-6	0	لا	عدد صحيح

.يحدد نوع الرقم المستخدم في طلب الربط SMPP **الغرض**: حقل بروتوكول

:القيم الشائعة

- 0 - غير معروف
- 1 - دولي
- 2 - وطني
- 5 - أبجدي رقمي

.قم بتعيينه حسب متطلبات شركة الاتصالات

addr_npi

مؤشر خطة ترقيم العنوان

النطاق	الافتراضي	مطلوب	النوع
0-18	0	لا	عدد صحيح

.يحدد خطة الترقيم في طلب الربط SMPP **الغرض**: حقل بروتوكول

:القيم الشائعة

- 0 - غير معروف
- 1 - ISDN/E.164
- 3 - بيانات/X.121
- 9 - خاص

.قم بتعيينه حسب متطلبات شركة الاتصالات

address_range

نطاق العنوان للربط

النوع	مطلوب	الافتراضي	مثال
سلسلة	لا	" "	"614*"

يحدد نطاق العنوان الذي تتعامل معه هذه الربط. تستخدمه بعض SMPP **الغرض**: حقل بروتوكول شركات الاتصالات لتصفية الرسائل التي يتم تسليمها إلى هذا الاتصال. اتركه فارغًا ما لم تحدد شركة الاتصالات قيمة.

enabled

حالة تمكين النظير

النوع	مطلوب	الافتراضي
منطقي	لا	true

الغرض: يتحكم فيما إذا كان هذا النظير نشطًا. يتم الاحتفاظ بالنظائر المعطلة في التكوين ولكن لا تقيم اتصالات. مفيد لأخذ اتصال مؤقتًا خارج الخدمة دون حذف تكوينه.

cache_enabled

تمكين التخزين المؤقت للرسائل المحلية

النوع	مطلوب	الافتراضي
منطقي	لا	false

الخلفية غير API **الغرض**: عند التمكين، يتم تخزين الرسائل الواردة مؤقتًا محليًا إذا كانت واجهة للحصول على MESSAGE_CACHE.md متاحة، ثم يتم تسليمها تلقائيًا عند استعادة الاتصال. انظر التفاصيل الكاملة.

cache_max_size

أقصى عدد من الرسائل المخزنة مؤقتًا

النطاق	الافتراضي	مطلوب	النوع
1-1000000	10000	لا	عدد صحيح

الغرض: الحد الأقصى لعدد الرسائل التي يمكن تخزينها مؤقتًا لكل ربط. عند الوصول إلى الحد، يتم `true` هو `cache_enabled` ينطبق فقط عندما يكون (FIFO) طرد أقدم الرسائل.

cache_retry_interval

فترة إعادة المحاولة الأساسية (بالثواني)

الافتراضي	مطلوب	النوع
60	لا	عدد صحيح

الغرض: فترة أساسية بالثواني قبل إعادة محاولة تسليم رسالة مخزنة مؤقتًا. يتم دمجها مع التراجع الأسّي (إعادة المحاولة 0: 60 ثانية، إعادة المحاولة 1: 120 ثانية، إعادة المحاولة 2: 240 ثانية، `true` هو `cache_enabled` إلخ). ينطبق فقط عندما يكون.

مثال واجهة الويب:

SMPP تكوين ربط خادم

(خادم) **SMSC** عمليات الربط الخاصة بالخادم تحدد الاتصالات الواردة حيث تعمل البوابة كـ خارجيين. في هذا الوضع، تتصل الأنظمة الشريكة بالبوابة (عملاء) **ESMEs** تقبل الاتصالات من لإرسال واستقبال الرسائل.

مثال كامل على ربط الخادم

```
config :omnimessage_smpp, :server_binds, [
  %{
    # معرف فريد لهذا العميل
    name: "partner_acme",

    # بيانات الاعتماد المتوقعة من العميل
    system_id: "acme_corp",
    password: "acme_secret",

    # أنواع الربط المسموح بها
    allowed_bind_types: [:transmitter, :receiver, :transceiver],

    # قيود IP
    ip_whitelist: ["192.168.1.0/24", "10.50.1.100"],

    # قيود عنوان المصدر (فارغ = السماح للجميع)
    source_address_whitelist: [],

    # تحديد المعدل
    tps_limit: 50,

    # تكرار فحص قائمة الانتظار
    queue_check_frequency: 1000,

    # فترة التحقق (بالثواني، 0 لتعطيل)
    enquire_link_interval: 60,

    # تخزين الرسائل (اختياري)
    cache_enabled: false,
    cache_max_size: 10000,
    cache_retry_interval: 60
  }
]
```

معلومات ربط الخادم

name

معرف العميل

النوع	مطلوب	مثال
سلسلة	نعم	"partner_acme"

الغرض: يحدد العميل الخارجي الذي يتصل بك.

اتفاقيات التسمية: استخدم اسم الشريك/العميل لتسهيل التعرف.

system_id

اسم المستخدم المتوقع من العميل

النوع	مطلوب	مثال
سلسلة	نعم	"acme_corp"

الغرض: اسم المستخدم الذي يجب أن يقدمه العميل الخارجي للمصادقة.

تقديم للعميل: شارك هذه البيانات مع شريكك.

password

كلمة المرور المتوقعة من العميل

النوع	مطلوب	مثال
سلسلة	نعم	"secure_password"

الغرض: كلمة المرور التي يجب أن يقدمها العميل الخارجي للمصادقة.

الأمان:

- استخدم كلمات مرور قوية
- فريدة لكل عميل
- شاركها بشكل آمن مع الشريك

allowed_bind_types

أنواع الجلسات المسموح بها

الافتراضي	مطلوب	النوع
-	نعم	قائمة من الذرات

الغرض: يحدد أنواع الربط التي يمكن للعميل استخدامها.

الخيارات:

```
allowed_bind_types: [:transceiver] # فقط transceiver
allowed_bind_types: [:transmitter, :receiver] # TX أو RX
allowed_bind_types: [:transmitter, :receiver, :transceiver] # أي
```

التوصية: السماح بالثلاثة ما لم تكن بحاجة إلى قيود.

ip_whitelist

المسموح بها للعميل IP عناوين

التنسيق	الافتراضي	مطلوب	النوع
CIDR أو تدوين IP عناوين	[]	نعم	قائمة من السلاسل

المعروفة IPS **الغرض:** الأمان - السماح فقط بالاتصالات من

التنسيقات:

- واحد: "192.168.1.100" (تلقائيًا 32) IP
- CIDR شبكة: "192.168.1.0/24", "10.0.0.0/8"
- مزيج من الاثنين: ["10.50.1.100", "192.168.1.0/24"]

أمثلة:

```
# (غير موصى به) IP السماح بأي
ip_whitelist: []

# واحد IP
ip_whitelist: ["203.0.113.50"]

# عدة IPs
ip_whitelist: ["203.0.113.50", "203.0.113.51"]

# شبكة
ip_whitelist: ["192.168.1.0/24"]

# مختلط
ip_whitelist: ["192.168.1.0/24", "10.50.1.100", "10.60.0.0/16"]
```

الشبكات الشائعة:

- (بدون قناع IP تلقائي لعناوين) واحد IP - /32
- عنوان (مثل 255-192.168.1.0) - /24
- عنوان (مثل 255.255-10.50.0.0) - /16
- عنوان (مثل 255.255.255.255-10.0.0.0) - /8

source_address_whitelist

العناوين المسموح بها

التنسيق	الافتراضي	مطلوب	النوع
أنماط التعبير العادي	[]	لا	قائمة من السلاسل

الغرض: يحدد أي عناوين مصدر (معرفات المرسل) يمكن للعملاء المتصلين استخدامها عند تقديم الرسائل. القائمة الفارغة تسمح بجميع العناوين. كل إدخال هو نمط تعبير عادي.

أمثلة:

```
# السماح بأي عنوان مصدر
source_address_whitelist: []

# تطابق دقيق (مربوط)
source_address_whitelist: ["^MyBrand$", "^AlertService$"]

# تطابق بادية
source_address_whitelist: ["^614", "^\\+61"]

# نطاق الأرقام مع فئة الأحرف
source_address_whitelist: ["^61[45]\\d{8}$"]

# مختلط
source_address_whitelist: ["^MyBrand$", "^614", "^\\+61400000001$"]
```

انظر `ESME_RINVSRCADR` تُرفض الرسائل ذات العناوين المصدر غير المسموح بها مع [SOURCE_ADDRESS_WHITELIST.md](#) للحصول على التفاصيل الكاملة.

tps_limit

حد الرسائل في الثانية

الصادر للعم  المتصلين deliver_sm لربط العميل - يتحكم في معدل `tps_limit` مثل

queue_check_frequency

فترة استعلام قائمة الانتظار

لربط العميل - كم مرة يجب التحقق من الرسائل لتسليمها إلى `queue_check_frequency` مثل هذا العميل.

enquire_link_interval

(بالثواني) SMPP فترة التحقق من

PDUs لربط العميل. يتحكم في مدى تكرار الخادم لإرسال `enquire_link_interval` مثل العملاء المتصلين للتحقق مما إذا كانوا لا يزالون نشطين `enquire_link`.

enabled

حالة تمكين النظيف

لربط العميل. لا تقبل النظائر الخادمة المعطلة الاتصالات الواردة `enabled` مثل

cache_enabled

تمكين التخزين المؤقت للرسائل المحلية

لربط العميل. انظر `cache_enabled` مثل `MESSAGE_CACHE.md`.

cache_max_size

أقصى عدد من الرسائل المخزنة مؤقتًا

لربط العميل `cache_max_size` مثل

cache_retry_interval

فترة إعادة المحاولة الأساسية (بالثواني)

لربط العميل `cache_retry_interval` مثل

مثال واجهة الويب:

تكوين الاستماع للخادم

عند تكوين عمليات الربط للخادم، تستمع البوابة للاتصالات الواردة

مثال كامل على الاستماع

```
config :omnimessage_smpp, :listen, %{
  host: "0.0.0.0",
  port: 2775,
  max_connections: 100
}
```

معلومات الاستماع

host

لربط عليه IP عنوان

النوع	مطلوب	الافتراضي	القيم الشائعة
سلسلة	لا	"0.0.0.0"	"0.0.0.0", "127.0.0.1"

الغرض: أي واجهة شبكة للاستماع عليها

القيم:

- "0.0.0.0" - الاستماع على جميع الواجهات (موصى به)
- "127.0.0.1" - فقط (اختبار) localhost الاستماع على
- "192.168.1.10" - محدد IP الاستماع على

port

للاستماع عليه TCP منفذ

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	لا	2775	1-65535

الغرض: SMPP. المنفذ للاتصالات الواردة

القياسي: 2775

max_connections

أقصى عدد من الاتصالات المتزامنة

النطاق	الافتراضي	مطلوب	النوع
1-10000	100	لا	عدد صحيح

الغرض: يحدد العدد الإجمالي للاتصالات المتزامنة للعملاء.

الإرشادات:

- تعيين بناءً على العملاء المتوقعين
 - القيم الأعلى تستخدم المزيد من الذاكرة
 - النموذجي: 10-100 اتصال
-

أمثلة تكوين كاملة

واحد Carrier المثال 1: اتصال ب

```
import Config

config :omnimessage_smpp,
  api_base_url: "https://smcsc.comany.com:8443",
  verify_ssl_peer: true,
  smsc_name: "smpp_prod"

config :omnimessage_smpp, :binds, [
  %{
    name: "att_primary",
    mode: :client,
    bind_type: :transceiver,
    host: "smpp.att.com",
    port: 2775,
    system_id: "company_user",
    password: "secure_pass_123",
    tps_limit: 100,
    queue_check_frequency: 1000
  }
]
```

المثال 2: عدة شركات اتصالات

```
import Config

config :omnimessage_smpp,
  api_base_url: "https://smcsc.companay.com:8443"

config :omnimessage_smpp, :binds, [
  # أمريكا الشمالية
  %{
    name: "att_us",
    mode: :client,
    bind_type: :transceiver,
    host: "smpp.att.com",
    port: 2775,
    system_id: "att_username",
    password: "att_password",
    tps_limit: 100,
    queue_check_frequency: 1000
  },

  # أوروبا
  %{
    name: "vodafone_uk",
    mode: :client,
    bind_type: :transceiver,
    host: "smpp.vodafone.co.uk",
    port: 2775,
    system_id: "voda_username",
    password: "voda_password",
    tps_limit: 50,
    queue_check_frequency: 1000
  }
]
```

المثال 3: بوابة مع عمليات الربط للخادم

```
import Config

config :omnimessage_smpp,
  api_base_url: "https://smcsc.company.com:8443"

# اتصالات صادرة
config :omnimessage_smpp, :binds, [
  %{
    name: "upstream_carrier",
    mode: :client,
    bind_type: :transceiver,
    host: "smpp.carrier.com",
    port: 2775,
    system_id: "my_username",
    password: "my_password",
    tps_limit: 100,
    queue_check_frequency: 1000
  }
]

# تعريفات العملاء الواردة
config :omnimessage_smpp, :server_binds, [
  %{
    name: "partner_alpha",
    system_id: "alpha_corp",
    password: "alpha_secret",
    allowed_bind_types: [:transmitter, :receiver, :transceiver],
    ip_whitelist: ["203.0.113.0/24"],
    tps_limit: 50,
    queue_check_frequency: 1000
  },
  %{
    name: "partner_beta",
    system_id: "beta_inc",
    password: "beta_password",
    allowed_bind_types: [:transceiver],
    ip_whitelist: ["198.51.100.50"],
    tps_limit: 25,
    queue_check_frequency: 2000
  }
]
```

```
# الاستماع للخادم
config :omnimessage_smpp, :listen, %{
  host: "0.0.0.0",
  port: 2775,
  max_connections: 100
}
```

المثال 4: قائمة انتظار مشتركة مع ربط المصدر

(sinch.smpp) اتصال بنفس شركة الاتصالات، كلاهما يستنزف قائمة انتظار واحدة مشتركة المصدر و المنفذ، لذا يثبت IP لمشاركة الحمل والاحتياطي. تقوم شركة الاتصالات بتبويض حسب المصدر IP كل ربط منفذ مصدر محلي متميز على نفس

```

import Config

config :omnimessage_smpp,
  api_base_url: "https://smcsc.com:8443"

config :omnimessage_smpp, :binds, [
  %{
    name: "sinch_1",
    mode: :client,
    bind_type: :transceiver,
    host: "smpp.sinch.com",
    port: 2775,
    system_id: "sinch_user",
    password: "sinch_pass",
    tps_limit: 100,
    queue_check_frequency: 1000,

    # كلا الربطين يستنزفان نفس قائمة الانتظار الخلفية
    queue: "sinch.smpp",

    # تثبيت عنوان/منفذ المصدر (تبيض شركة الاتصالات حسب كليهما)
    bind_source_ip: "10.20.30.40",
    bind_source_port: 5001
  },
  %{
    name: "sinch_2",
    mode: :client,
    bind_type: :transceiver,
    host: "smpp.sinch.com",
    port: 2775,
    system_id: "sinch_user",
    password: "sinch_pass",
    tps_limit: 100,
    queue_check_frequency: 1000,

    # sinch_1 نفس قائمة الانتظار المشتركة مثل
    queue: "sinch.smpp",

    # المصدر، منفذ مصدر متميز IP نفس
    bind_source_ip: "10.20.30.40",
    bind_source_port: 5002
  }
]

```

```
}  
]
```

مفتاح التوجيه) `sinch.smpp` **كيف يعمل**: يقوم كلا الربطين بتسجيل واجهة أمامية واحدة تُدعى من قبل أي `dest_smsc: "sinch.smpp"` يتم استنزاف الرسائل ذات. (المشترك الخاص بهما ربط يلتقطها أولاً، مما ينشر الحمل عبر الاتصاليين. إذا انقطع أحد الاتصالات، يستمر الآخر في ثابتًا ومنفذًا لشركة الاتصالات للتبويض؛ يسمح IP استنزاف قائمة الانتظار. يقدم كل اتصال عنوان `SO_REUSEADDR` بإعادة ربط منفذ مثبت على الفور عند إعادة الاتصال.

للحصول على تفاصيل المعلومات `bind_source_port`، و `bind_source_ip`، `queue` انظر

التحقق من التكوين

:بعد تحرير التكوين، تحقق قبل إعادة التشغيل

التحقق من بناء الجملة

```
# Elixir تحقق من بناء جملة  
/opt/omnimessage-smpp/bin/omnimessage-smpp eval "File.read!  
( 'config/runtime.exs' )"
```

.إذا كان البناء غير صالح، ستري خطأ. قم بإصلاحه قبل إعادة التشغيل

اختبار التكوين

```
# إعادة التشغيل في الواجهة الأمامية لرؤية الأخطاء  
sudo -u omnimessage-smpp /opt/omnimessage-smpp/bin/omnimessage-  
smpp console
```

.مرتين للخروج `Ctrl+C` اضغط على

متغيرات البيئة

يمكن تجاوز جميع الإعدادات العالمية باستخدام متغيرات البيئة. قم بتعيين هذه في ملف وحدة shell الخاص بك أو بيئة systemd قبل بدء البوابة.

متغير البيئة	مفتاح التكوين	راضي
API_BASE_URL	api_base_url	"https://10.17
SMSC_NAME	smsc_name	"smpp_gateway"
SMPP_POLL_INTERVAL	smpp_poll_interval	100
VERIFY_SSL_PEER	verify_ssl_peer	false
CACHE_FLUSH_INTERVAL	cache_flush_interval	10000
CACHE_MAX_RETRY_ATTEMPTS	cache_max_retry_attempts	10
CACHE_BACKOFF_MULTIPLIER	cache_backoff_multiplier	2

متغير البيئة	مفتاح التكوين	راضي
MNESIA_STORAGE_TYPE	mnesia_storage_type	disc_copies

systemd مثال على تجاوز:

```
sudo systemctl edit omnimessage-smpp
```

```
[Service]
Environment="API_BASE_URL=https://omnimessage-
core.company.com:8443"
Environment="SMSC_NAME=smpp_prod_01"
Environment="VERIFY_SSL_PEER=true"
```

أفضل الممارسات الأمنية

1. احم ملف التكوين:

```
sudo chmod 600 /opt/omnimessage-smpp/config/runtime.exs
sudo chown omnimessage-smpp:omnimessage-smpp
/opt/omnimessage-smpp/config/runtime.exs
```

2. استخدم كلمات مرور قوية:

- الحد الأدنى 12 حرفًا
- مزيج من الحروف والأرقام والرموز
- فريدة لكل اتصال

3. IP استخدم قوائم بيضاء:

- لعمليات الربط بالخادم `ip_whitelist` قم دائمًا بتكوين
- لا تستخدم قائمة فارغة `[]` في الإنتاج

4. SSL: قم بتمكين التحقق من

- مع شهادات صالحة `verify_ssl_peer: true` قم بتعيين

5. تدوير بيانات الاعتماد بشكل منتظم:

- قم بتغيير كلمات المرور كل ثلاثة أشهر
- التنسيق مع شركات الاتصالات/الشركاء

الخطوات التالية

- لتكوين القياسات `MONITORING.md` مراجعة
 - لإدارة الات❖❖الات `USAGE.md` قراءة
 - للمشاكل الشائعة `TROUBLESHOOTING.md` الاطلاع على
 - للحصول على نظرة عامة `README.md` العودة إلى
-

مصدر

المصطلحات والتعريفات

A

واجهة تُستخدم للتواصل مع نظام خلفية قائمة الرسائل (**واجهة برمجة التطبيقات API**).

ميزة في واجهة المستخدم على الويب في علامة التبويب السجلات التي تقوم **Auto-Scroll** بالتمرير تلقائيًا لعرض أحدث إدخالات السجل.

B

لاسترجاع الرسائل وتخزينها SMPP نظام قائمة الرسائل الذي يتصل به بوابة **Backend**.

بين نظامين. يمكن أن يكون مرسلاً، مستلمًا، أو جهاز إرسال واستقبال SMPP اتصال **Bind**.

Bind Type نوع جلسة SMPP:

- **Transmitter**: إرسال الرسائل فقط
- **Receiver**: استلام الرسائل فقط
- **Transceiver**: إرسال واستقبال الرسائل

عادةً بسبب بي❓❓ نات اعتماد غير SMPP، عندما تفشل محاولة المصادقة على **Bind Failure** IP صحيحة أو قيود على عنوان.

C

على سبيل المثال،) IP ترميز لتحديد نطاقات عناوين (**توجيه بين المجالات بدون فئات CIDR** (192.168.1.0/24 IP). يمثل 256 عنوان

عادةً) خارجي **SMSC** تتصل بـ **ESME** صادر حيث تعمل البوابة كـ SMPP اتصال **Client Bind** (لمشغل الاتصالات SMPP خادم. في هذا الوضع، تكون البوابة هي العميل).

Connection Status SMPP الحالة الحالية لارتباط:

- **Connected:** نشط وعامل
- **Disconnected:** غير متصل
- **Reconnecting:** محاولة لإعادة إنشاء الاتصال

مقياس يزيد فقط (يتم إعادة تعيينه عند إعادة تشغيل الخدمة)، يُستخدم للإجماليات مثل **Counter** الرسائل المرسله.

D

Data Coding (إلخ، UCS-2، GSM-7) يحدد ترميز أحرف الرسالة SMPP حقل

متصل ESME لتسليم رسالة إلى (الخادم) SMSC يُرسل بواسطة SMPP PDU **Deliver_SM** (العميل). يُستخدم بواسطة ارتباطات الخادم لدفع الرسائل إلى الشركاء المتصلين

عندما لا يمكن تسلل ❖❖ م رسالة، مما يشير إليه رد خطأ من المشغل **Delivery Failure**

تأكيد من المشغل حول حالة تسليم الرسالة **Delivery Receipt (DLR)**

حقل في قائمة الرسائل يحمل الطابع الزمني الذي تم فيه تسليم الرسالة. يتم **deliver_time** عندما تبلغ البوابة عن تسليم ناجح. هذا هو اسم الحقل الذي OmniMessage Core تعيينه بواسطة يتوقعه النظام الخلفي عند وضع علامة على الرسالة كتم تسليمها

يجب أن يتعامل مع الرسالة. SMPP حقل في قائمة الرسائل يشير إلى أي اتصال **dest_smsc** **Frontend** انظر) الذي تم تسجيل النظير المستهدف تحته **Routing Key** يجب أن تساوي قيمته **Registration**).

نشط، سواء عن عمد أو بسبب خطأ SMPP عندما يتم إنهاء اتصال **Disconnection**

E

للحفاظ على الاتصال تُرسل بشكل دوري للتحقق من أن الاتصال SMPP رسالة **Enquire Link** نشط.

يشير إلى نوع الرسالة وميزاتها SMPP حقل **ESM Class**

التطبي ❖❖ العميل الذي، SMPP، في مصطلحات (كيان الرسائل القصيرة الخارجي) **ESME** ESME لإرسال أو استلام الرسائل. عندما تعمل البوابة في **وضع العميل**، تعمل ك SMSC يتصل بـ

الخارجية ESMES للمشغلين. عندما تعمل في **وضع الخادم**، تقبل الاتصالات من SMSCs تتصل بـ

استراتيجية إعادة المحاولة حيث يتضاعف وقت الانتظار بعد كل فشل **Exponential Backoff** (1 دقيقة، 2 دقيقة، 4 دقائق، 8 دقائق...).

F

نظام أمان الشبكة الذي يتحكم في حركة المرور الواردة والصادرة **Firewall**.

Frontend Registration OmniMessage نفسها مع SMPP العملية التي تسجل بها بوابة Core. يتم إرسال نبضة كل 60 ثانية للحفاظ على التسجيل نشطًا. إذا توقفت البوابة، تنتهي صلاحية Core. عن توجيه الرسائل إليها. يتم تسجيل كل نظير OmniMessage التسجيل بعد 90 ثانية ويتوقف الذي يتجه إليه `dest_smsc` الخاصة به بحيث يساوي الاسم المسجل **Routing Key** تحت الخاصة بهم (أو اسم النظير العاري)، وارتباطات الخادم `queue` النظام الخلفي: نظائر العملاء تحت تحت اسم الربط الخاص بهم.

G

الذي يربط بين قائمة الرسائل والشبكات المحمولة SMPP تطبيق بوابة **Gateway**.

مقياس يمكن أن يزيد أو ينقص، يمثل القيمة الحالية (على سبيل المثال، حالة الاتصال) **Gauge**.

في لوحات المعلومات Prometheus أداة تصور شائعة لعرض مقياس **Grafana**.

ترميز أحرف قياسي 7 بت للرسائل القصيرة، يدعم حتى 160 حرفًا لكل رسالة **GSM-7**.

H

هو النسخة المشفرة HTTPS. البروتوكولات المستخدمة للتواصل عبر الويب **HTTP/HTTPS**.

I

المسموح بها التي يمكنها الاتصال بالبوابة (ميزة أمان) IP قائمة بعنوانين **IP Whitelist**.

خطة ترقيم تُستخدم عادةً لأرقام الهواتف (**شبكة الخدمات الرقمية المتكاملة**) **ISDN**.

J

(لا توجد مصطلحات)

K

Keepalive تُرسل للحفاظ على الاتصال واكتشاف الأخطاء (enquire_link) رسائل دورية.

قيمة قابلة للقياس تشير إلى أداء النظام (على سبيل المثال، **مؤشر الأداء الرئيسي KPI**، معدل نجاح التسليم).

L

، (على سبيل المثال) أزواج المفتاح والقيمة المرفقة بالمقاييس للتعريف، Prometheus في **Label** (`bind_name="vodafone_uk"`).

المستخدمة لتحديث واجهة المستخدم على الويب في الوقت Phoenix تكنولوجيا إطار **LiveView** الحقيقي.

M

Message Queue نظام خلفية يخزن الرسائل التي تنتظر الإرسال أو الاستلام.

Prometheus قياسات كمية لأداء النظام، تُعرض بتنسيق **Metrics**.

الرسائل المرسل من الهواتف المحمولة إلى **(الرسائل المنشأة من الهاتف المحمول) MO** البوابة (واردة).

الرسائل المرسل من البوابة إلى الهواتف **(الرسائل الموجهة إلى الهاتف المحمول) MT** المحمولة (صادرة).

تنسيق قياسي لأرقام **(رقم الدليل الدولي للمشارك في المحطة المحمولة) MSISDN** الهواتف المحمولة.

N

(ISDN ، على سبيل المثال) يحدد نظام الترميز SMPP حقل (مؤشر خطة الترميز) NPI.

O

الرسائل المتدفقة   ن البوابة إلى الشبكات المحمولة Outbound.

الرسائل المتدفقة من الشبكات المحمولة إلى البوابة Inbound.

P

(على سبيل المثال) فردية SMPP حزمة رسالة (وحدة بيانات البروتوكول) PDU (submit_sm, deliver_sm).

نظام مراقبة مفتوح المصدر يجمع ويخزن مقاييس السلاسل الزمنية Prometheus.

Q

قائمة الرسائل التي تنتظر المعالجة أو الإرسال Queue.

مدى تكرار (بالملي ثانية) استعلام البوابة للنظام الخلفي عن Queue Check Frequency رسائل جديدة.

SMPP مكون يسترجع الرسائل من القائمة ويرسلها عبر Queue Worker.

R

TPS التحكم في معدل مرور الرسائل للامتثال لقيود المشغل. انظر Rate Limiting.

(deliver_sm) الذي يستقبل الرسائل فقط SMPP نوع ارتباط Receiver.

مفصول SMPP إعادة إنشاء اتصال Reconnect.

محاولة إرسال رسالة فاشلة مرة أخرى، عادةً مع زيادة زمن الانتظار بشكل أسّي Retry.

OmniMessage Core الاسم الذي يسجله النظير كواجهة أمامي مع **Routing Key** ، **queue** التي توجه الرسائل إليه. بالنسبة لنظير العميل، يكون هذا هو `dest_smsc` وبالتالي قيمة بالنسبة لارتباط الخادم، يكون هو `(queue)` أو اسم النظير العاري عندما لا يتم تعيين) المكونة له اسم الربط.

S

ضمن جلسة. يُستخدم PDU SMPP معرف رقمي فريد يُخصص لكل **Sequence Number** `submit_sm` مع `submit_sm_resp` على سبيل المثال، مطابقة) لمطابقة الطلبات مع ردودها.

الخارجية (العملاء) بالاتصال بالبوابة. في هذا الوضع، **ESMEs** تكوين يسمح لـ **Server Bind** . تقبل الاتصالات الواردة من الأنظمة الشريكة (خادم) **SMSC** تعمل البوابة كـ

نشط بين نظامين SMPP اتصال **Session** .

قائمة خلفية واحدة يتم تفريغها بواسطة أكثر من ارتباط عميل واحد. تختار **Shared Queue** على سبيل المثال، اتصالان) في تكوينها `queue` الارتباطات الانضمام عن طريق تعيين نفس قيمة مما يسمح بمشاركة الحمل والازدواج **ة** عبر `"sinch.smpp"` لمشغلين كلاهما يقوم بتفريغ الاتصالات. يتم تعيين القيمة الافتراضية إلى اسم الربط الخاص بها، وفي هذه الحالة، يكون لكل ربط قائمته الخاصة.

مختصر (عادةً 5-6 أرقام) يُستخدم للرسائل من التطبيق إلى الشخص. SMS عنوان **Short Code** **غير معروف** حتى لا يسيء TON المكونة من خمسة أرقام مع `deliver_sm` يتم إرسال وجهات المشغلون تفسيرها كأرقام دولية.

لاتصال صادر (عميل) عبر معلمات TCP المحلي وميناء IP تثبيت عنوان **Source Binding** يُستخدم عندما يقوم المشغل بإدراج الاتصالات `bind_source_ip` و `bind_source_port` . **CONFIGURATION.md** والميناء المصدر. انظر IP حسب عنوان

حقل في قائمة الرسائل يشير إلى أي ارتباط خادم يجب أن يسلم الرسالة إلى `source_smsc` `deliver_sm` عملائه المتصلين عبر

بروتوكول قياسي في الصناعة لتبادل **(الرسائل القصيرة من نظير إلى نظير) SMPP** . الرسائل القصيرة بين الأنظمة

المكون الخادم الذي يقبل ، SMPP في مصطلحات **(مركز خدمة الرسائل القصيرة) SMSC** ويتعامل مع توجيه الرسائل القصيرة وتسليمها. عندما تعمل البوابة (العملاء) **ESMEs** الاتصالات من الخارجية **ESMEs** تقبل الاتصالات من **SMSC** في **وضع الخادم** ، تعمل كـ

SSL/TLS بروتوكولات التشفير للاتصالات الآمنة.

Submit_SM PDU SMPP لتقديم رسالة للتسليم.

Submit_SM_Resp تشير إلى النجاح أو الفشل، submit_sm، SMPP استجابة.

System ID اسم المستخدم المستخدم لمصادقة SMPP.

T

Telemetry جمع ونقل تلقائي لمقاييس النظام.

TON يحدد تنسيق الرقم (على سبيل المثال، دولي، وطني) SMPP حقل (نوع الرقم).

TPS حد معدل أقصى للرسائل في الثانية عبر اتصال (المعاملات في الثانية).

Transceiver يمكنه إرسال واستقبال الرسائل (الأكثر شيوعًا) SMPP نوع ارتباط.

Transmitter (submit_sm) يرسل الرسائل فقط SMPP نوع ارتباط.

Throughput معدل معالجة الرسائل، يُقاس عادةً بالرسائل في الثانية.

U

UCS-2 بت للرسائل القصيرة، يدعم حتى 70 حرفًا لكل رسالة Unicode 16 ترمي ٢٠٢٠ أحرف.

Uptime مدة تشغيل الاتصال أو الخدمة بشكل مستمر.

V

Validity Period الحد الزمني لمحاولة تسليم الرسالة قبل انتهاء الصلاحية.

W

Web Dashboard واجهة مستخدم قائمة على المتصفح لمراقبة وإدارة البوابة.

البيضاء وقائمة عناوين المصدر البيضاء IP انظر قائمة **Whitelist**.

X

(لا توجد مصطلحات)

Y

(لا توجد مصطلحات)

Z

(لا توجد مصطلحات)

مرجع سريع للاختصارات

الاختصار	المصطلح الكامل
API	واجهة برمجة التطبيقات
CIDR	توجيه بين المجالات بدون فئات
DLR	إيصال التسليم
ESME	كيان الرسائل القصيرة الخارجي
GSM	النظام العالمي للاتصالات المحمولة
HTTP	بروتوكول نقل النصوص التشعبية
HTTPS	بروتوكول نقل النصوص التشعبية الآمن
IP	بروتوكول الإنترنت
ISDN	شبكة الخدمات الرقمية المتكاملة
KPI	مؤشر الأداء الرئيسي
MO	الرسائل المنشأة من الهاتف المحمول
MSISDN	رقم الدليل الدولي للمشارك في المحطة المحمولة
MT	الرسائل الموجهة إلى الهاتف المحمول
NPI	مؤشر خطة الترقيم
PDU	وحدة بيانات البروتوكول
SMPP	الرسائل القصيرة من نظير إلى نظير
SMSC	مركز خدمة الرسائل القصيرة

الاختصار	المصطلح الكامل
SMS	خدمة الرسائل القصيرة
SSL	طبقة المقابس الآمنة
TLS	أمان طبقة النقل
TON	نوع الرقم
TPS	المعاملات في الثانية
UCS	مجموعة الأحرف المشفرة العالمية
UI	واجهة المستخدم
URL	محدد موقع الموارد الموحد

الوثائق ذات الصلة

- **README.md** - نظرة عامة على النظام وكيفية البدء
 - **CONFIGURATION.md** - شرح معلمات التكوين
 - **USAGE.md** - العمليات اليومية
 - **MONITORING.md** - المقاييس والمراقبة
 - **TROUBLESHOOTING.md** - حل المشكلات
-

SMPP ذاكرة تخزين رسائل

نظرة عامة

بالاستمرار في قبول SMPP هي طبقة تخزين محلية تسمح لبوابة SMPP ذاكرة تخزين رسائل الرسائل الواردة حتى عندما تكون واجهة برمجة التطبيقات الخلفية غير متاحة. يتم تخزين الرسائل ويتم تسليمها تلقائيًا إلى واجهة برمجة التطبيقات عند استعادة الاتصال، Mnesia محليًا في. باستخدام منطق إعادة المحاولة الذكي مع زيادة زمن الانتظار بشكل أسي

الميزات

- خلال انقطاع واجهة SMPP **قبول الرسائل المرن** - الاستمرار في قبول رسائل برمجة التطبيقات
- لضمان الاستمرارية عبر إعادة `disc_copies` مع Mnesia **تخزين دائم** - يستخدم التشغيل
- **إعادة المحاولة التلقائية** - تحاول العمال في الخلفية التسليم تلقائيًا مع زيادة زمن الانتظار بشكل أسي
- **تكوين لكل ارتباط** - تمكين/تعطيل التخزين المؤقت بشكل مستقل لكل ارتباط SMPP
- عند وصول الذاكرة المؤقتة إلى حد الحجم FIFO **حماية من الفيضانات** - إخلاء المحدد
- **احتفاظ بالرسائل الفاشلة** - الاحتفاظ بالرسائل التي فشلت بشكل دائم للمراجعة اليدوية
- مع إحصائيات الذاكرة LiveView **المراقبة في الوقت الحقيقي** - لوحة معلومات المؤقتة والقياسات
- تصدير كامل للقياسات للمراقبة والتنبيه - **Prometheus قياسات**

الهيكلية

تدفق الرسائل

مع تمكين التخزين المؤقت

SMPP Client → submit_sm → Gateway Server



Cache in Mnesia (immediate response)



CacheFlushWorker (background)



Backend API

مع تعطيل التخزين المؤقت

SMPP Client → submit_sm → Gateway Server



Backend API (direct)

المكونات

1. MessageCache وحدة

- منطق التخزين الأساسي
- معالجة الفيضانات
- والعمال LiveView وظائف الاستعلام لـ

2. CacheFlushWorker

- لكل ارتباط مع تمكين التخزين المؤقت GenServer
- يستعلم عن الرسائل الجاهزة لإعادة المحاولة
- ينفذ زيادة زمن الانتظار بشكل أسي
- يحدد الرسائل التي فشلت بشكل دائم

3. Mnesia جدول (:smpp_message_cache)

- تخزين دائم مع :disc_copies
- status و next_retry_at و bind_name مفهرس بواسطة
- يبقى بعد إعادة تشغيل التطبيق

التكوين

الإعدادات العالمية

قم بتحرير `config/runtime.exs`:

```
config :omnmessage_smpp,
  # مدى تكرار استعلام العمال عن الرسائل (بالملي ثانية)
  cache_flush_interval: 10_000,

  # الحد الأقصى لعدد محاولات إعادة المحاولة قبل وضع علامة ك فشل دائم
  cache_max_retry_attempts: 10,

  # مضاعف زيادة زمن الانتظار
  cache_backoff_multiplier: 2,

  # نوع تخزين Mnesia (:disc_copies أو :ram_copies)
  mnesia_storage_type: :disc_copies
```

تكوين لكل ارتباط

بشكل مستقل (عميل أو خادم) SMPP يمكن تكوين كل ارتباط

```
config :omnmessage_smpp, :binds, [
  %{
    name: "my_smpp_bind",
    mode: :server,
    system_id: "username",
    password: "password",

    # تكوين التخزين المؤقت
    cache_enabled: true, # افتراضي) تمكين التخزين المؤقت
    false)
    cache_max_size: 10_000, # الحد الأقصى للرسائل للتخزين
    (المؤقت (افتراضي: 10,000)
    cache_retry_interval: 60 # فترة إعادة المحاولة الأساسية
    بالثواني (افتراضي: 60)
  }
]
```

المتغيرات البيئية

# إعدادات التخزين المؤقت العالمية	
CACHE_FLUSH_INTERVAL=10000	فترة استعلام الإخلاء (مللي #
(ثانية	
CACHE_MAX_RETRY_ATTEMPTS=10	الحد الأقصى لإعادة #
المحاولات قبل الفشل الدائم	
CACHE_BACKOFF_MULTIPLIER=2	مضاعف زيادة زمن الانتظار #
MNESIA_STORAGE_TYPE=disc_copies	# نوع تخزين Mnesia

سلوك إعادة المحاولة

زيادة زمن الانتظار بشكل أسي

: عند فشل تسليم الرسالة، يتضاعف زمن إعادة المحاولة مع كل محاولة

```
Base interval: 60 seconds
Backoff multiplier: 2

Retry 0: 60s    (1 minute)
Retry 1: 120s   (2 minutes)
Retry 2: 240s   (4 minutes)
Retry 3: 480s   (8 minutes)
Retry 4: 960s   (16 minutes)
Retry 5: 1920s  (32 minutes)
...
Retry 9: 30,720s (8.5 hours)
```

الفشل الدائم

بعد 10 محاولات فاشلة (بشكل افتراضي)، يتم وضع علامة على الرسائل كـ `failed_permanent` و:

- تبقى الذاكرة المؤقتة للمراجعة اليدوية
- تتوقف عن إعادة المحاولة تلقائيًا
- تظهر في قسم "الفشل الدائم" في لوحة معلومات الذاكرة المؤقتة
- يمكن إعادة المحاولة يدويًا أو مسحها

انتقالات الحالة

```
:pending → :delivering → SUCCESS (deleted from cache)
      → FAILURE → :pending (retry with backoff)
      → :failed_permanent (after max
retries)
```

المراقبة

LiveView لوحة معلومات

يمكن الوصول إلى لوحة معلومات الذاكرة المؤقتة على <http://your-server:4000/smpp> → علامة "ذاكرة الرسائل"

بطاقات الملخص:

- إجمالي التخزين المؤقت - جميع الرسائل الموجودة حاليًا في الذاكرة المؤقتة
- التسليم المعلق - الرسائل التي تنتظر إعادة المحاولة
- الفشل الدائم - الرسائل التي تجاوزت الحد الأقصى لإعادة المحاولات

جدول لكل ارتباط:

- اسم الارتباط
- عدد الرسائل المخزنة مؤقتًا
- تقسيم المعلق / الفاشل
- الحد الأقصى لحجم الذاكرة المؤقتة
- نسبة الاستخدام (مع شريط تقدم مرئي)

قياسات Prometheus

```
# حجم الذاكرة المؤقتة الحالية لكل ارتباط
smpp_cache_size{bind_name="my_bind",mode="server"} 42

# إجمالي الرسائل التي تم تسليمها بنجاح
smpp_cache_delivered_total{bind_name="my_bind"} 1234

# إجمالي محاولات إعادة المحاولة
smpp_cache_retry_total{bind_name="my_bind"} 56

# إجمالي الفشل الدائم
smpp_cache_permanent_failures_total{bind_name="my_bind"} 2

# إجمالي أحداث الفيضانات (الرسائل المفقودة)
smpp_cache_overflow_total{bind_name="my_bind"} 0
```

رسائل السجل

```
INFO Message -123456789 cached for my_smpp_bind
INFO Successfully delivered cached message -123456789, API ID:
99999
WARN Failed to deliver message -123456789 (retry 3/10), next
retry at 2026-02-01 12:34:56Z
ERROR Message -123456789 exceeded max retries (10), marking as
failed_permanent
WARN Cache overflow for my_smpp_bind: deleted oldest message
```

العمليات

تمكين/تعطيل التخزين المؤقت

LiveView عبر واجهة

1. انتقل إلى `http://your-server:4000/smpp`
2. "انتقل إلى علامة "أقران العملاء" أو "أقران الخادم"
3. حرر الارتباط

"قم بتعديل مربع "تمكين التخزين المؤقت 4.

احفظ التغييرات 5.

IEx عبر وحدة تحكم

```
# تمكين التخزين المؤقت لارتباط
SmsC.SMPPConfig.update_server_peer("my_bind", "username",
    "password",
    cache_enabled: true,
    cache_max_size: 10_000,
    cache_retry_interval: 60
)

# تعطيل التخزين المؤقت
SmsC.SMPPConfig.update_server_peer("my_bind", "username",
    "password",
    cache_enabled: false
)
```

مراقبة حالة الذاكرة المؤقتة

```
# الحصول على ملخص عالمي
SmsC.SMPP.MessageCache.get_cache_summary()
# => %{total_cached: 42, pending: 40, failed: 2}

# الحصول على تقسيم لكل ارتباط
SmsC.SMPP.MessageCache.get_cache_by_bind()
# => [
#   %{bind_name: "bind1", total: 30, pending: 28, failed: 2,
#     max_size: 10_000},
#   %{bind_name: "bind2", total: 12, pending: 12, failed: 0,
#     max_size: 10_000}
# ]

# عد الرسائل لارتباط محدد
SmsC.SMPP.MessageCache.count_cached_messages("my_bind")
# => 42
```

التدخلات اليدوية

مسح الرسائل الفاشلة

```
# الحصول على جميع الرسائل الفاشلة لارتباط
{:atomic, failed_messages} = :mnesia.transaction(fn ->
  :mnesia.match_object({:smpp_message_cache, :_, "my_bind", :_,
    :_, :_, :_, :_, :_, :failed_permanent})
end)

# حذفها
Enum.each(failed_messages, fn {_, {bind_name, msg_id}, _, _, _, _,
  _, _, _, _} ->
  SmsC.SMPP.MessageCache.delete_cache_record(bind_name, msg_id)
end)
```

فرض إعادة المحاولة لرسالة فاشلة

```
# failed_permanent إلى pending وإعادة تعيين رسالة
SmsC.SMPP.MessageCache.update_cache_record("my_bind", -123456, %{
  status: :pending,
  retry_count: 0,
  next_retry_at: DateTime.utc_now(),
  last_error: nil
})
```

استكشاف الأخطاء وإصلاحها

الذاكرة المؤقتة ممتلئة / أحداث الفيضانات

حذف الرسائل الأقدم، `cache_overflow_total` الأعراض: زيادة قياس

السبب: تم الوصول إلى حد حجم الذاكرة المؤقتة

الحلول:

للاارتباط `cache_max_size` زيادة 1.

- التحقيق في سبب فشل تسليم واجهة برمجة التطبيقات (تحقق من سجلات واجهة برمجة التطبيقات، الشبكة)
- مسح الرسائل القديمة الفاشلة يدويًا
- تحقق مما إذا كانت فترة الإخلاء بطيئة جدًا

الرسائل لا يتم تسليمها

pending: الأعراض: الرسائل عالقة في حالة

الأسباب المحتملة:

1. واجهة برمجة التطبيقات معطلة

- تحقق من توفر واجهة برمجة التطبيقات
- تحقق من سجلات واجهة برمجة التطبيقات الخلفية
- تحقق من اتصال الشبكة

2. next_retry_at في المستقبل

- next_retry_at سيتم إعادة محاولة الرسائل عند الوصول إلى
- تحقق من جدول زيادة زمن الانتظار بشكل أسي

3. عامل الإخلاء لا يعمل

```
# تحقق مما إذا كانت العمال تعمل  
Supervisor.which_children(SmsC.SMPP.Supervisor)
```

4. التخزين المؤقت معطل

- في تكوين الارتباط cache_enabled: true تحقق من

عدد المحاولات العالية

عالية retry_count الأعراض: العديد من الرسائل مع قيم

التحقيق:

```

# العثور على الرسائل ذات عدد المحاولات العالية
{:atomic, messages} = :mnesia.transaction(fn ->
  :mnesia.match_object({:smpp_message_cache, :_, "my_bind", :_,
    :_, :_, :_, :_, :_, :_})
end)

high_retry = Enum.filter(messages, fn {_ , _ , _ , _ , _ , _ ,
  retry_count, _ , _ , _} ->
  retry_count >= 5
end)

# لكل منها last_error تحقق من
Enum.each(high_retry, fn {_ , _ , _ , msg_id, _ , _ , retry_count, _ ,
  last_error, _} ->
  IO.puts("Message #{msg_id}: #{retry_count} retries, error: #
    {inspect(last_error)}")
end)

```

Mnesia مساحة قرص

الأعراض: امتلاء مساحة القرص

Mnesia: تحقق من دليل

```

ls -lh Mnesia.*
du -sh Mnesia.*

```

تنظيف:

1. مسح الرسائل القديمة الفاشلة (انظر التدخلات اليدوية أعلاه).
2. لكل ارتباط `cache_max_size` تقليل
3. (المناسب FIFO ضمان الإخلاء) تمكين الفيضانات

اعتبارات الأداء

استخدام الذاكرة

- تستخدم كل رسالة مخزنة مؤقتًا حوالي 500-1000 بايت (اعتمادًا على حجم الرسالة)
- رسالة $\approx 5-10$ ميغابايت من الذاكرة 10,000
- يتم أيضًا كتابة البيانات إلى القرص ، `disc_copies` مع

استخدام وحدة المعالجة المركزية

- يستعلم عمال الإخلاء كل 10 ثوانٍ بشكل افتراضي (يمكن تكوينه)
- المعالجة الدفعية (100 رسالة لكل دورة) تقلل من الحمل الزائد
- التسليم المتزامن (حد أقصى 10 مكالمات واجهة برمجة التطبيقات المتزامنة لكل عامل)

إدخال/إخراج القرص

- تكتب إلى القرص في كل معاملة `disc_copies`
- ضع في اعتبارك ، (>1000 msg/sec) من أجل معدل نقل بيانات مرتفع جدًا
 - (يفقد الاستمرارية) `ram_copies` استخدام
 - زيادة فترات الإخلاء
 - التوسع أفقيًا

الحدود الموصى بها

السيناريو	cache_max_size	cache_flush_interval
حجم منخفض (<100 msg/sec)	10,000	10,000ms
حجم متوسط (100-500 msg/sec)	50,000	5,000ms
حجم مرتفع (>500 msg/sec)	100,000	3,000ms

سيناريوهات الاسترداد

إعادة تشغيل التطبيق

1. من القرص تلقائيًا `disc_copies`: بتحميل جداول Mnesia يقوم
2. تبقى الرسائل المخزنة مؤقتًا سليمة
3. يتم إعادة تشغيل عمال الإخلاء ويستمرون في المعالجة

ترحيل قاعدة البيانات

عند الترقية من إصدار بدون دعم التخزين المؤقت:

1. يضيف الترحيل تلقائيًا حقول التخزين المؤقت إلى الروابط الموجودة
2. القيم الافتراضية: `cache_enabled: false`, `cache_max_size: 10_000`, `cache_retry_interval: 60`
3. لا فقدان للبيانات
4. يتم إنشاء جدول التخزين المؤقت عند التشغيل الأول

استرداد من انقطاع واجهة برمجة التطبيقات

1. تتجمع الرسائل في الذاكرة المؤقتة أثناء الانقطاع
2. عند استعادة واجهة برمجة التطبيقات، يقوم عمال الإخلاء بالتسليم تلقائيًا
3. (FIFO) يتم تسليم الرسائل الأقدم أولاً
4. تمنع زيادة زمن الانتظار ب `⚡⚡` كل أسّي من تحميل واجهة برمجة التطبيقات أثناء الاسترداد

أفضل الممارسات

1. **تمكين التخزين المؤقت بشكل افتراضي** - يمنع فقدان الرسائل أثناء الانقطاعات
2. **مراقبة القياسات** - `cache_permanent_failures_total` و `cache_overflow_total` إعداد تنبيهات على
3. **بناءً على مدة الانقطاع** `cache_max_size` **تحديد الحجم بشكل مناسب** - تعيين المتوقعة
4. **مراجعة الرسائل الفاشلة** - التحقق بانتظام من الرسائل الفاشلة الدائمة للأنماط

5. **اختبار الفشل** - محاكاة انقطاعات واجهة برمجة التطبيقات للتحقق من سلوك التخزين المؤقت
6. **تعديل فترات إعادة المحاولة** - ضبطها بناءً على أنماط وقت استعادة واجهة برمجة التطبيقات
7. **استخدام التخزين الدائم** - الاحتفاظ بـ `mnesia_storage_type: disc_copies` في الإنتاج

انظر أيضًا

- مرجع التكوين
- المراقبة والقياسات
- استكشاف الأخطاء وإصلاحها

دليل المراقبة والقياسات

SMPP مرجع كامل لمراقبة بوابة

نظرة عامة

لمراقبة صحة الاتصال، وسرعة Prometheus بعرض القياسات بتنسيق SMPP تقوم بوابة الرسائل، وأداء النظام.

فإن الاتصال بـ OmniMessage Core، حرج: نظرًا لأن البوابة بلا حالة وتعتمد على: هو أهم مقياس يجب مراقبته. راقب كلا من OmniMessage

1. صحة على مستوى البروتوكول - SMPP قياسات بوابة
2. الاتصال والصحة في الخلفية - OmniMessage API قياسات

نقطة نهاية القياسات

URL: `http://your-server:4000/metrics`

Prometheus التنسيق: تنسيق نص

بشكل افتراضي (قم بتكوين جدار الحماية للوصول عن بُعد) localhost الوصول: مفتوح لـ

اختبار سريع

```
curl http://localhost:4000/metrics
```

القياسات المتاحة

وتتضمن تسميات للتعرف `smpp_` جميع القياسات مسبوقة بـ.

قياسات الترخيص

omnimessage_smpp_license_status

النوع: Gauge

الوصف: حالة الترخيص الحالية

القيم:

- 1 = ترخيص صالح
- 0 = ترخيص غير صالح/منتهي

التسميات: لا شيء

مثال:

```
omnimessage_smpp_license_status 1
```

الاستخدام:

- تنبيه عند أن القيمة 0 (ترخيص غير صالح)
- عندما يكون الترخيص غير صالح، تتوقف معالجة قائمة الانتظار الصادرة ولكن تظل متصلة SMPP اتصالات
- تظل واجهة الويب متاحة لاستكشاف الأخطاء وإصلاحها

اسم المنتج: omnimessage_smpp

ملاحظات:

- تتوقف البوابة عن (`license_status == 0`) عندما يكون الترخيص غير صالح معالجة قوائم الانتظار الصادرة
- متصلة وتقبل طلبات الربط (كلا من العميل والخادم) SMPP تظل اتصالات
- لا تزال الرسائل الواردة تُستقبل ولكن لا تتم معالجتها
- تظل واجهة المستخدم والمراقبة متاحة بغض النظر عن حالة الترخيص

مثال على التنبيه:

```
- alert: SMPP_License_Invalid
  expr: omnimessage_smpp_license_status == 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "غير صالح أو منتهي SMPP ترخيص بوابة"
    description: "حالة الترخيص غير صالحة - تم حظر معالجة الرسائل الصادرة"
```

قياسات حالة الاتصال

smpp_connection_status

النوع: Gauge

SMPP الوصف: حالة الاتصال الحالية لربط

القيم:

- 1 = متصل
- 0 = غير متصل

التسميات:

- `bind_name` - اسم الاتصال (مثل "vodafone_uk")
- `mode` - نوع الاتصال ("client" أو "server")
- `host` - المضيف البعيد (وضع العميل فقط)
- `port` - المنفذ البعيد (وضع العميل فقط)
- `bind_type` - نوع ربط SMPP (وضع العميل فقط)
- `system_id` - معرف النظام المستخدم

مثال:

```
smpp_connection_status{bind_name="vodafone_uk",mode="client",host="sn1
```

الاستخدام:

- تنبيه عند أن القيمة 0 (غير متصل)
- تتبع نسبة وقت التشغيل للاتصال
- مراقبة تكرار إعادة الاتصال

عدادات الرسائل

smpp_messages_sent_total

النوع: Counter

SMPP الوصف: العدد الإجمالي للرسائل المرسله عبر ربط
الوحدة: رسائل

التسميات: نفس ح  لة الاتصال

مثال:

```
smpp_messages_sent_total{bind_name="vodafone_uk",mode="client",...}  
150234
```

الاستخدام:

- حساب معدل الرسائل (رسائل/ثانية)
- تتبع الحجم اليومي/الشهري
- مقارنة السرعة الفعلية مقابل المتوقعة

smpp_messages_received_total

النوع: Counter

SMPP الوصف: العدد الإجمالي للرسائل المستلمة عبر ربط
الوحدة: رسائل

التسميات: نفس حالة الاتصال

مثال:

```
smpp_messages_received_total{bind_name="partner_acme",mode="server",...
45123
```

الاستخدام:

- مراقبة حجم الرسائل الواردة
- (MO) تتبع حركة المرور المنبعثة من الهاتف المحمول
- تنبيه على تغييرات غير متوقعة في الحجم

قياسات التسليم

smpp_delivery_failures_total

النوع: Counter

الوصف: العدد الإجمالي الذي فشل تسليم الرسائل

الوحدة: الفشل

التسميات: نفس حالة الاتصال

مثال:

```
smpp_delivery_failures_total{bind_name="vodafone_uk",mode="client",...
234
```

الاستخدام:

- حساب معدل نجاح التسليم
- تنبيه على معدلات الفشل العالية
- تحديد الاتصالات المشككة

حساب معدل النجاح:

```
success_rate = (messages_sent - delivery_failures) / messages_sent
* 100
```

قياسات عمليات الربط

smpp_bind_success_total

النوع: Counter

الوصف: العدد الإجمالي لعمليات الربط الناجحة

الوحدة: محاولات الربط

مثال:

```
smpp_bind_success_total{bind_name="vodafone_uk",...} 45
```

الاستخدام:

- تتبع استقرار الربط
- مراقبة نجاح المصادقة

smpp_bind_failures_total

النوع: Counter

الوصف: العدد الإجمالي لعمليات الربط الفاشلة

الوحدة: محاولات الربط

مثال:

```
smpp_bind_failures_total{bind_name="vodafone_uk",...} 3
```

الاستخدام:

- تنبيه على فشل المصادقة
- تحديد مشاكل ال◆◆ اعتماد
- تتبع مشاكل اتصال الناقل

قياسات أحداث الاتصال

smpp_connection_attempts_total

النوع: Counter

الوصف: العدد الإجمالي لمحاولات الاتصال
الوحدة: المحاولات

مثال:

```
smpp_connection_attempts_total{bind_name="vodafone_uk",...} 48
```

الاستخدام:

- تتبع معدل تغير الاتصال
- مراقبة تكرار إعادة الاتصال

smpp_disconnection_total

النوع: Counter

الوصف: العدد الإجمالي لفصل الاتصالات
الوحدة: فصل

مثال:

```
smpp_disconnection_total{bind_name="vodafone_uk",...} 3
```

الاستخدام:

- تنبيه على فصل الاتصالات المتكرر
- تحديد مشاكل الشبكة
- تتبع استقرار الاتصال

قياسات استفسار الرابط

smpp_enquire_link_sent_total

النوع: Counter

الخاصة بالاستفسار المرسل للتحقق من حيوية الاتصال PDUs **الوصف:** العدد الإجمالي لوحدات
الوحدة: PDUs

التسميات: نفس حالة الاتصال

مثال:

```
smpp_enquire_link_sent_total{bind_name="vodafone_uk",mode="client",...  
1440
```

الاستخدام:

- تتبع نشاط الحفاظ على الاتصال
- المقارنة مع المستلم لاكتشاف الفشل من جانب واحد

smpp_enquire_link_received_total

النوع: Counter

الخاصة بالاستجابة للاستفسار المستلمة من النظير البعيد PDUs **الوصف:** العدد الإجمالي لوحدة

الوحدة: PDUs

التسميات: نفس حالة الاتصال

مثال:

```
smpp_enquire_link_received_total{bind_name="vodafone_uk",mode="client"  
1438
```

الاستخدام:

- اكتشاف النظائر غير المستجيبة (المُرسل < المستلم)
- مراقبة صحة الاتصال بما يتجاوز الحالة البسيطة

قياسات وقت التشغيل

smpp_uptime_seconds

النوع: Gauge

بالثواني SMPP **الوصف:** وقت التشغيل الحالي لربط

الوحدة: ثواني

مثال:

```
smpp_uptime_seconds{bind_name="vodafone_uk",...} 86400
```

الاستخدام:

- تتبع استقرار الاتصال
- حساب نسبة وقت التشغيل
- تنبيه على إعادة التشغيل الأخيرة

قياسات ذاكرة التخزين المؤقت للرسائل

تكون هذه القياسات متاحة عندما يكون تخزين الرسائل مؤهلاً على واحد أو أكثر من الروابط. راجع [MESSAGE_CACHE.md](#) للحصول على تفاصيل تكوين التخزين المؤقت.

smpp_cache_size

النوع: Gauge

الوصف: العدد الحالي للرسائل في التخزين المؤقت المحلي لكل رابط

الوحدة: رسائل

التسميات:

- `bind_name` - اسم الاتصال
- `mode` - نوع الاتصال ("client" أو "server")

مثال:

```
smpp_cache_size{bind_name="partner_acme",mode="server"} 42
```

الاستخدام:

- مراقبة استخدام التخزين المؤقت
- `cache_max_size` تنبيه عند الاقتراب من

smpp_cache_delivered_total

النوع: Counter

الوصف: العدد الإجمالي للرسائل المخزنة مؤقتًا التي تم تسليمها بنجاح إلى واجهة برمجة التطبيقات الخلفية

الوحدة: رسائل

مثال:

```
smpp_cache_delivered_total{bind_name="partner_acme"} 1234
```

smpp_cache_retry_total

النوع: Counter

الوصف: العدد الإجمالي لمحاولات إعادة المحاولة للرسائل المخزنة مؤقتًا

الوحدة: المحاولات

مثال:

```
smpp_cache_retry_total{bind_name="partner_acme"} 56
```

smpp_cache_permanent_failures_total

النوع: Counter

الوصف: العدد الإجمالي للرسائل التي تجاوزت الحد الأقصى لمحاولات إعادة المحاولة وتم وضع علامة عليها على أنها فشلت بشكل دائم

الوحدة: رسائل

مثال:

```
smpp_cache_permanent_failures_total{bind_name="partner_acme"} 2
```

الاستخدام:

- تنبيه عند $0 <$ (يتطلب مراجعة يدوية)

smpp_cache_overflow_total

النوع: Counter

الوصف: العدد الإجمالي لأحداث تجاوز التخزين المؤقت حيث تم طرد أقدم رسالة لتوفير مساحة
الوحدة: أحداث

مثال:

```
smpp_cache_overflow_total{bind_name="partner_acme"} 0
```

الاستخدام:

- تنبيه عند الزيادة (التخزين المؤقت صغير جدًا أو انقطاع واجهة برمجة التطبيقات طويل جدًا)

OmniMessage قياسات صحة واجهة برمجة التطبيقات

فإن صحة واجهة برمجة SMPP، بينما تقوم البوابة بنفسه   بعرض القياسات المتعلقة بـ **حاسمة**. يجب عليك أيضًا مراقبة **OmniMessage التطبيقات**:

(إذا كانت متاحة) OmniMessage من قياسات

- `omnimessage_api_requests_total` - إجمالي طلبات واجهة برمجة التطبيقات من البوابة
- `omnimessage_api_request_duration_seconds` - أوقات استجابة واجهة برمجة التطبيقات
- `omnimessage_queue_depth` - OmniMessage الرسائل المعلقة في قائمة انتظار

من سجلات البوابة (إذا لم يتم عرض القياسات)

إبحث عن هذه الأنماط لاكتشاف مشاكل واجهة برمجة التطبيقات

- "api.*connection refused" - OmniMessage لا يمكن الوصول إلى
- "api.*timeout" - OmniMessage لا تستجيب
- "api.*http 503" - OmniMessage معطلة مؤقتًا
- "api.*parse error" - مشكلة في تنسيق الاستجابة

تكوين Prometheus

تكوين سحب أساسي

أضف إلى `/etc/prometheus/prometheus.yml`:

```
scrape_configs:
  - job_name: 'omnimessage-smpp'
    scrape_interval: 15s
    static_configs:
      - targets: ['your-server:4000']
        labels:
          environment: 'production'
          service: 'omnimessage-smpp'
```

بوابات متعددة

```
scrape_configs:
  - job_name: 'omnimessage-smpp-instances'
    scrape_interval: 15s
    static_configs:
      - targets:
          - 'smpp-gw-1:4000'
          - 'smpp-gw-2:4000'
          - 'smpp-gw-3:4000'
        labels:
          environment: 'production'
```

اكتشاف الخدمة

باستخدام اكتشاف قائم على الملفات:

```
scrape_configs:
  - job_name: 'omnimessage-smpp-instances'
    file_sd_configs:
      - files:
          - '/etc/prometheus/targets/smpp-*.json'
```

ملف /etc/prometheus/targets/smpp-production.json:

```
[
  {
    "targets": ["smpp-gw-1:4000", "smpp-gw-2:4000"],
    "labels": {
      "environment": "production",
      "datacenter": "us-east"
    }
  }
]
```

Grafana لوحات تحكم

لوحات التحكم النموذجية

لوحة حالة الاتصال

الاستعلام:

```
smpp_connection_status{job="omnimessage-smpp"}
```

التصور: Stat

الحدود:

- أحمر: القيمة $1 >$ (غير متصل)
- أخضر: القيمة $1 ==$ (متصل)

لوحة معدل الرسائل

الاستعلام:

```
rate(smpp_messages_sent_total{job="omnimessage-smpp"}[5m])
```

التصور: Graph

الوحدة: رسائل/ثانية

التسمية: `{{bind_name}}`

لوحة معدل نجاح التسليم

الاستعلام:

```
100 * (1 - (
  rate(smpp_delivery_failures_total{job="omnmessage-smpp"}[5m])
  /
  rate(smpp_messages_sent_total{job="omnmessage-smpp"}[5m])
))
```

التصور: Gauge

الوحدة: النسبة المئوية (100-0)

الحدود:

- %أحمر: > 95
- %أصفر: 98-95
- %أخضر: < 98

لوحة وقت تشغيل الاتصال

الاستعلام:

```
smpp_uptime_seconds{job="omnmessage-smpp"} / 3600
```

التصور: Stat

الوحدة: ساعات

قواعد التنبيه

Prometheus قواعد تنبيه

احفظ إلى `/etc/prometheus/rules/smpp-alerts.yml`:

```

groups:
- name: smpp_gateway
  interval: 30s
  rules:
    # الاتصال معطل
    - alert: SMPPConnectionDown
      expr: smpp_connection_status == 0
      for: 2m
      labels:
        severity: critical
      annotations:
        summary: "معطل SMPP {{ $labels.bind_name }}"
        description: "مفصول لأكثر من 00 دقائق الاتصال {{ $labels.bind_name }}."
        من دقيقتين

    # معدل فشل مرتفع
    - alert: SMPPHighFailureRate
      expr: |
        (
          rate(smpp_delivery_failures_total[5m])
          /
          rate(smpp_messages_sent_total[5m])
        ) > 0.05
      for: 5m
      labels:
        severity: warning
      annotations:
        summary: "معدل فشل تسليم مرتفع على {{ $labels.bind_name }}"
        description: "معدل فشل التسليم هو {{ $value | humanizePercentage }} على {{ $labels.bind_name }}."

    # فشل الربط
    - alert: SMPPBindFailures
      expr: increase(smpp_bind_failures_total[10m]) > 3
      labels:
        severity: warning
      annotations:
        summary: "عدة فشل ربط على {{ $labels.bind_name }}"
        description: "فشل في الربط {{ $labels.bind_name }} مرات في آخر 10 دقائق {{ $value }}"

    # لا توجد رسائل مرسله (عند المتوقع)

```

```
- alert: SMPPNoTraffic
  expr: rate(smpp_messages_sent_total[10m]) == 0
  for: 30m
  labels:
    severity: warning
  annotations:
    summary: "{{ $labels.bind_name }} لا توجد رسائل مرسله على"
    description: "لم ترسل أي رس00ئ00ل {{ $labels.bind_name }} لمدة 30 دقيقة"
```

فصل متكرر

```
- alert: SMPPFrequentDisconnections
  expr: increase(smpp_disconnection_total[1h]) > 5
  labels:
    severity: warning
  annotations:
    summary: "فصل متكرر على {{ $labels.bind_name }}"
    description: "فصلت {{ $value }} مرات في الساعة الماضية"
```

غير قابلة للوصول لOmniMessage واجهة برمجة التطبيقات

```
- alert: OmniMessageAPIUnreachable
  expr: |
    count(count_over_time({job="omnmessage-smpp"} |=
"api.*connection refused"[5m])) > 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "OmniMessage واجهة برمجة التطبيقات غير قابلة للوصول"
    description: "الوصول إلى واجهة برمجة SMPP لا يمكن لبوابة OmniMessage والاتصال API_BASE_URL تحقق من تكوين التطبيقات بالشبكة."
```

OmniMessage مهلات واجهة برمجة التطبيقات

```
- alert: OmniMessageAPITimeout
  expr: |
    count(count_over_time({job="omnmessage-smpp"} |=
"api.*timeout"[5m])) > 5
  for: 2m
  labels:
    severity: warning
```

```

annotations:
  summary: "تعا ني من OmniMessage اجهة برمجة التطبيقات00"
  "مهلات"
  description: "تم اكتشاف عدة مهلات واجهة برمجة التطبيقات."
  ".بطيئة أو محملة بشكل زائد OmniMessage قد تكون

# لا توجد تدفقات رسائل (مشكلة واجهة برمجة التطبيقات)
- alert: NoMessageFlow
  expr: rate(smpp_messages_sent_total[10m]) == 0 and
rate(smpp_messages_received_total[10m]) == 0
  for: 30m
  labels:
    severity: warning
  annotations:
    summary: "لا توجد تدفقات رسائل مكتشفة - تحقق من الاتصال بـ
OmniMessage"
    description: "لم يتم إرسال أو استلام أي رسائل لمدة 30
وحالة قائمة OmniMessage دقيقة. تحقق من اتصال واجهة برمجة التطبيقات
الانتظار."

```

قم بتحميل القواعد في prometheus.yml:

```

rule_files:
  - '/etc/prometheus/rules/smpp-alerts.yml'

```

مراقبة لوحة الويب

Prometheus توفر واجهة الويب المدمجة مراقبة في الوقت الفعلي دون

الوصول

URL: `https://your-server:8087`

صفحة الحالة الحية

الحالة الحية → SMPP: التنقل

الميزات:

- حالة الاتصال في الوقت الفعلي
- عدادات الرسائل
- وقت تشغيل الاتصال
- عناصر التحكم في إعادة الاتصال/الفصل اليدوي
- تحديث تلقائي كل 5 ثوانٍ

الاستخدام:

- فحص الحالة بسرعة
- تدخل يدوي
- استكشاف الأخطاء وإصلاحها في الوقت الفعلي

تظهر لوحة المعلومات

- **إجمالي الربط:** العدد المجمع لجميع اتصالات العميل والخادم
 - **ربط العميل:** الاتصالات الصادرة إلى الناقلين (تظهر العدد المتصل/غير المتصل)
 - **ربط الخادم:** الاتصالات الواردة من الشركاء (تظهر العدد النشط/الانتظار)
 - **استماع الخادم:** تكوين مقبس الخادم الوارد (المضيف، المنفذ، الحد الأقصى من الاتصالات)
-

مراقبة السجلات

سجلات النظام

عرض السجلات:

```
# متابعة السجلات في الوقت الفعلي
sudo journalctl -u omnimessage-smpp -f

# آخر 100 سطر
sudo journalctl -u omnimessage-smpp -n 100

# منذ وقت محدد
sudo journalctl -u omnimessage-smpp --since "1 hour ago"

# تصفية حسب المستوى
sudo journalctl -u omnimessage-smpp -p err
```

سجلات واجهة الويب

التنقل: علامة السجلات في واجهة الويب

الميزات:

- تدفق السجلات في الوقت الفعلي
- تصفية حسب المستوى (debug, info, warning, error)
- البحث في السجلات
- إيقاف مؤقت/استئناف
- مسح السجلات

تسمح لك واجهة السجلات بـ

- **تصفية المستوى:** اختيار مستوى السجل (الكل، تصحيح، معلومات، تحذير، خطأ)
- **البحث:** العثور على إدخالات سجل محددة حسب محتوى النص
- **التمرير التلقائي:** تمكين/تعطيل التمرير التلقائي عند وصول سجلات جديدة
- **إيقاف مؤقت/استئناف:** إيقاف تحديث السجلات لمراجعة إدخالات محددة
- **مسح:** مسح جميع  السجلات المعروضة

(KPIs) مؤشرات الأداء الرئيسية

صحة الاتصال

المقياس: نسبة وقت تشغيل الاتصال

```
avg_over_time(smpp_connection_status[24h]) * 100
```

%الهدف: < 99.9

معدل تسليم الرسائل

المقياس: الرسائل التي تم تسليمها في الثانية

```
rate(smpp_messages_sent_total[5m])
```

الهدف: يتطابق مع الحجم المتوقع

معدل نجاح التسليم

المقياس: نسبة التسليم الناجح

```
100 * (1 - rate(smpp_delivery_failures_total[5m]) /  
rate(smpp_messages_sent_total[5m]))
```

%الهدف: < 98

استقرار الربط

المقياس: محاولات الربط في الساعة

```
rate(smpp_bind_success_total[1h]) * 3600
```

الهدف: > 10 في الساعة (يشير إلى اتصال مستقر)

أفضل ممارسات المراقبة

1. إعداد التنبيهات

- للقياسات الحرجة Prometheus تكوين تنبيهات
- للتنبيه على مدار الساعة PagerDuty/OpsGenie استخدام
- اختبار التنبيهات بانتظام

2. إنشاء لوحات التحكم

- لكل بوابة Grafana بناء لوحات تحكم

- تضمين جميع الاتصالات في لوحة تحكم واحدة
- إضافة لوحات تخطيط السعة

3. المراجعات المنتظمة

- مراجعة القياسات أسبوعيًا
- تحديد الاتجاهات والأنماط
- تخطيط تعديلات السعة

4. توثيق الأسس

- تسجيل أحجام الرسائل العادية
- المتوقعة TPS توثيق معدلات
- ملاحظة أوقات/أيام الذروة

5. الربط مع الخلفية

- مراقبة قياسات واجهة برمجة التطبيقات الخلفية
- تتبع تدفق الرسائل من البداية إلى النهاية
- تحديد الاختناقات

استكشاف الأخطاء باستخدام القياسات

مشاكل الاتصال

تحقق: `smpp_connection_status`

- القيمة 0 = مراجعة السجلات، تحقق من الشبكة، تحقق من الاعتماد
- التغييرات المتكررة = عدم استقرار الشبكة

معدلات التسليم الضعيفة

تحقق: `smpp_delivery_failures_total`

- معدل مرتفع = تحقق من حالة الناقل، مراجعة تنسيق الرسالة
- المقارنة عبر الاتصالات = تحديد  ناقل المشكلة

الإنتاجية المنخفضة

معدل `smpp_messages_sent_total` تحقق: معدل

- توفر قائمة الانتظار، TPS أقل من المتوقع = تحقق من حدود
- تحقق من قياسات واجهة برمجة التطبيقات الخلفية

مشاكل الربط

تحقق: `smpp_bind_failures_total`

- زيادة = مشاكل في المصادقة، مشاكل في الاعتماد
- وكلمة المرور في التكوين `system_id` تحقق من

الوثائق ذات الصلة

- **CONFIGURATION.md** - تكوين إعدادات المراقبة
 - **USAGE.md** - الإجراءات التشغيلية
 - **TROUBLESHOOTING.md** - حل المشكلات
 - **README.md** - نظرة عامة وبدء سريع
-

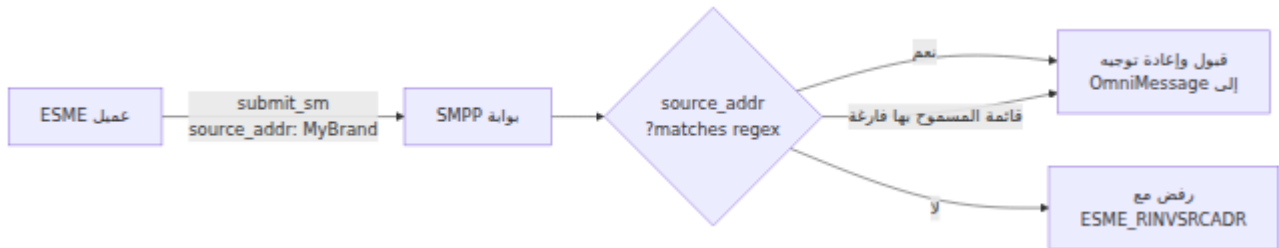
قائمة العناوين المسموح بها

التي يمكن أن يستخدمها (source_addr) تحكم لكل نظير في العناوين الأصلية . عند إرسال الرسائل SMPP عميل

نظرة عامة

حقل PDU يتضمن SMPP، عبر بوابة submit_sm PDU خارجي (عميل) ESME عندما يرسل بشكل افتراضي، يمكن . (معرف المرسل / CLI) الذي يمثل العنوان الأصلي source_addr للعملاء المعتمدين استخدام أي عنوان مصدر. تتيح ميزة قائمة العناوين المسموح بها للمشغلين تقييد العناوين المصدرة التي يُسمح لكل نظير خادم باستخدامها.

المسموح بها الحالية: عندما تكون القائمة فارغة، يُسمح IP يتبع هذا نفس النمط كما في قائمة . بجميع القيم. عند تعبئتها، يتم قبول العناوين المصدرة المطابقة فقط.



قواعد المطابقة

كل إدخال في قائمة المسموح بها هو نمط **تعبير منتظم**. يتم اختبار العنوان المصدر ضد كل نمط. إذا تطابق أي نمط، يُسمح بالعنوان.

المطابقة الدقيقة

قم بتثبيت النمط باستخدام `^` و `$` لطلب مطابقة دقيقة. المطابقة هي **حساسة لحالة الأحرف** بشكل افتراضي.

النتيجة	عنوان المصدر	إدخال قائمة المسموح بها
مسموح	MyBrand	<code>^MyBrand\$</code>
مرفوض	mybrand	<code>^MyBrand\$</code>
مرفوض	MyBrands	<code>^MyBrand\$</code>
مسموح	+61400000001	<code>^\+61400000001\$</code>

مطابقة البادئة

استخدم `^` بدون `$` في النهاية لمطابقة العناوين التي تبدأ ببادئة.

النتيجة	عنوان المصدر	إدخال قائمة المسموح بها
مسموح	61400000001	<code>^614</code>
مسموح	61412345678	<code>^614</code>
مرفوض	61500000001	<code>^614</code>
مسموح	+61400000001	<code>^\+614</code>

الأنماط المتقدمة

يدعم بناء جملة التعبير المنتظم الكامل، مما يمكّن من قواعد مطابقة قوية.

الأمثلة	الوصف	إدخال قائمة المسموح بها
61400000001, 61512345678	أرقام الهواتف المحمولة الأسترالية 614/615 (رقمًا)	<code>^61[45]\d{8}\$</code>
MyBrand, AlertSvc	مطابقة دقيقة على أي من الاسمين	<code>^(MyBrand AlertSvc)\$</code>
MyBrand, mybrand, MYBRAND	مطابقة دقيقة غير حساسة لحالة الأحرف	<code>(?i)^mybrand\$</code>
MyBrand (مسموح), TestBrand (مرفوض)	أي عنوان غير فارغ لا يبدأ بـ "Test"	<code>^(?!Test).+\$</code>

إدخالات متعددة

عندما يتم تكوين إدخالات متعددة، يُسمح بالعنوان المصدر إذا تطابق مع أي إدخال في قائمة المسموح بها.

مثال على قائمة المسموح بها: `^MyBrand$, ^614, ^\+614000000001$`

النتيجة	المطابقات	عنوان المصدر
مسموح	<code>^MyBrand\$</code>	MyBrand
مسموح	<code>^614</code>	61412345678
مسموح	<code>^\+614000000001\$</code>	+614000000001
مرفوض	لا شيء	OtherBrand
مرفوض	لا شيء	615000000001

معالجة الأخطاء

:بسبب انتهاك قائمة العناوين المسموح بها، تستجيب البوابة بـ `submit_sm` عندما يتم رفض

الحقل	القيمة
PDU	<code>submit_sm_resp</code>
حالة الأمر	<code>0x0000000A</code>
اسم الخطأ	<code>ESME_RINVSRCADR</code> (عنوان مصدر غير صالح)
معرف الرسالة	فارغ

:يتم تسجيل تحذير مع عنوان المصدر المرفوض واسم النظير

partner_acme - source_addr من submit_sm تم رفض SMPP خادم
غير موجود في قائمة المسموح بها 'UnauthorisedBrand'

.غير الصالحة غير مطابقة (يتم رفض العنوان) ويتم تسجيل تحذير regex تُعتبر أنماط

التكوين

عبر واجهة الويب

- نظائر الخادم > SMPP انتقل إلى 1.
- انقر على تحرير على النظير المستهدف (أو إضافة نظير خادم جديد) 2.
- (المسموح بها IP أسفل قائمة) ابحث عن حقل قائمة العناوين المسموح بها 3.
- :مفصولة بفواصل regex أدخل أنماط 4.

```
^MyBrand$,^614,^\+61400000001$
```

- انقر على حفظ 5.

.الجديدة على الاتصالات الحالية PDUs `submit_sm` تدخل التغييرات حيز التنفيذ على الفور للـ

عبر ملف التكوين

runtime.exs إلى تكوين ربط الخادم في source_address_whitelist أضف

```
config :omnimessage_smpp, :server_binds, [
  %{
    name: "partner_acme",
    system_id: "acme_corp",
    password: "secure_password",
    allowed_bind_types: [:transmitter, :receiver, :transceiver],
    ip_whitelist: ["203.0.113.0/24"],
    source_address_whitelist: ["^MyBrand$", "^614",
    "^\\+614000000001$"],
    tps_limit: 50,
    queue_check_frequency: 1000
  }
]
```

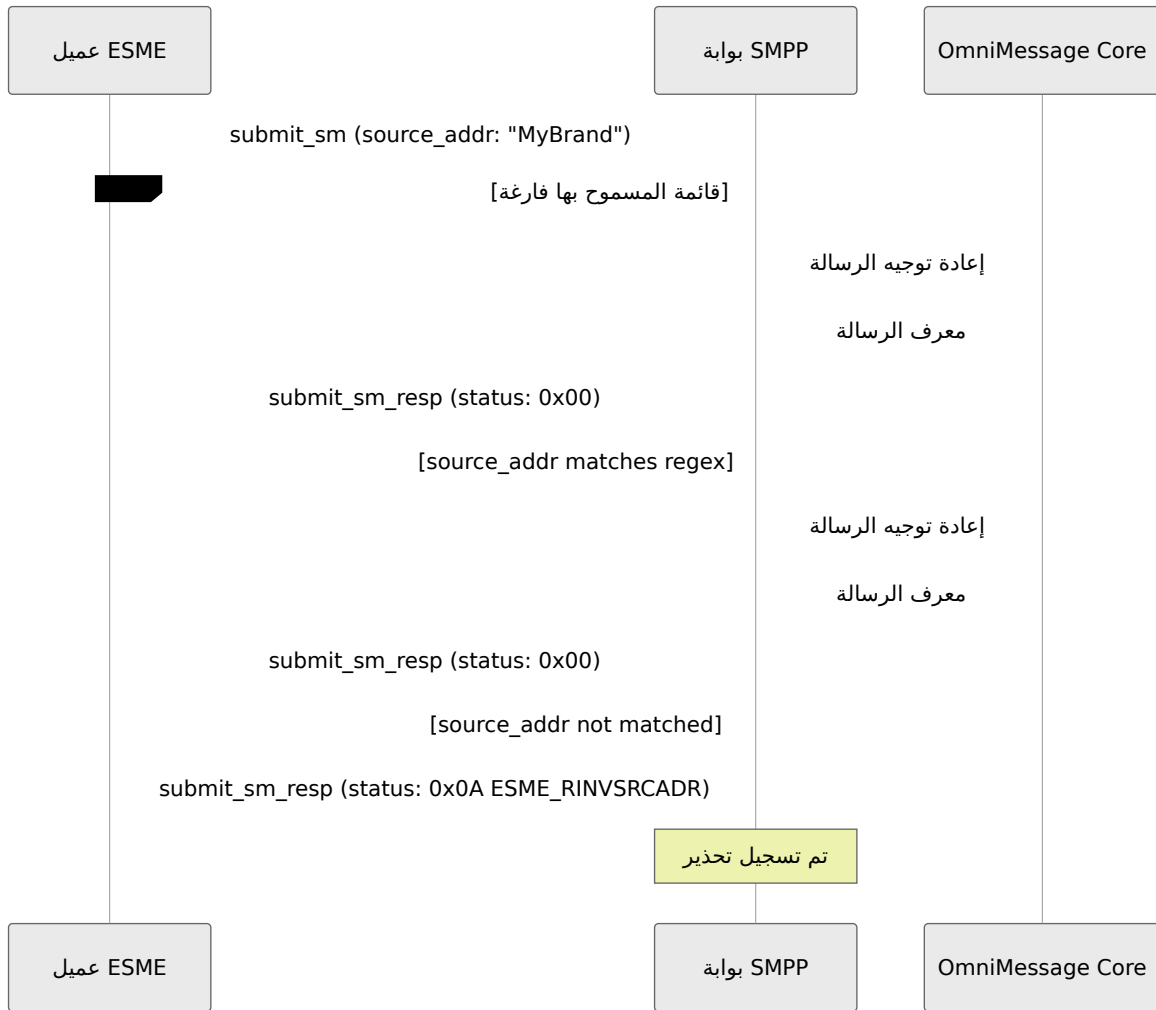
المعلومات

الوصف	الافتراضي	مطلوب	النوع	المعلمة
قائمة أنماط regex المسموح بها للعناوين المصدرة. القائمة الفارغة تسمح بجميع العناوين المصدرة.	يسمح ([]) للجميع	لا	قائمة من السلاسل	source_address_whitelist

الترحيل

يتم ترحيل نظائر الخادم الموجودة تلقائيًا عند بدء البوابة. النظائر التي تم إنشاؤها قبل إضافة هذه الميزة تتلقى قائمة فارغة (جميع العناوين المصدرة مسموح بها)، مما يحافظ على السلوك الحالي.

تدفق التحقق



أمثلة

تقييد إلى علامة تجارية واحدة

السماح فقط بالرسائل AcmeCorp: من معرف المرسل

```
^AcmeCorp$
```

السماح بنطاق أرقام أسترالية

السماح بأي رقم هاتف محمول أسترالي (يبدأ بـ 614)

^614

السماح بنطاقات أرقام محددة

السماح بأرقام الهواتف المحمولة الأسترالية 614 و 615 (بالضبط 11 رقمًا)

^61[45]\d{8}\$

مزيج من الأحرف الأبجدية الرقمية والأرقام

السماح باسم علامة تجارية ونطاق من الأرقام

^AcmeCorp\$,^614,^\+61290000001\$

مطابقة علامة تجارية غير حساسة لحالة الأحرف

السماح باسم علامة تجارية بغض النظر عن الحالة

(?i)^acmecorp\$

السماح بالجميع (افتراضي)

اترك الحقل فارغًا للسماح بأي عنوان مصدر. هذا هو السلوك الافتراضي

استكشاف الأخطاء وإصلاحها

ESME_RINVSRCADR الرسائل المرفوضة مع

.x0A مع حالة الأمر 0 submit_sm_resp الأعراض: الشريك يبلغ عن

الأسباب المحتملة:

- في قائمة المسموح بها regex عنوان المصدر لا يتطابق مع أي نمط
- يحتوي على خطأ في بناء الجملة (يُعتبر غير مطابق) regex نمط
- عدم وجود مثبتات (\$) (^) مما يتسبب في مطابقة جزئية غير متوقعة أو رفض
- المطابقة حساسة لحالة الأحرف بشكل افتراضي؛ استخدم) عدم تطابق الحالة (?i) (لمطابقة غير حساسة لحالة الأحرف

الحل:

1. تحقق من قائمة العناوين المسموح بها للنظير الخادم في واجهة الويب
2. regex قارن عنوان المصدر المرفوض مع كل نمط
3. Elixir: Regex.match? regex اختبر الأنماط باستخدام مختبر
4. أضف النمط المفقود أو اضبط الأنماط الموجودة
5. regex تذكر الهروب من الأحرف الخاصة في (مثل \+ \- \+ الحرفي)

قائمة المسموح بها لا تأخذ التأثير

الأعراض: الرسائل مقبولة على الرغم من عدم تطابق عنوان المصدر مع قائمة المسموح بها

الأسباب المحتملة:

- قائمة المسموح بها فارغة (تسمح بالجميع بشكل افتراضي)
- (X614Y مثل 614 يتطابق مع) النمط غير مثبت ويتطابق كجزء فرعي
- متصل بنظير خادم مختلف ESME
- تغيير ملف التكوين لم يتم تطبيقه بعد (يتطلب إعادة تشغيل)

الحل:

1. تحقق من أن قائمة المسموح بها ممتلئة (ليست فارغة) في واجهة الويب
2. تأكد من أن الأنماط تستخدم مثبتات ^ و \$ حيثما كانت المطابقة الدقيقة مقصودة
3. في الحالة الحية ESME تحقق من أي نظير خادم يرتبط به
4. إذا كنت تستخدم ملف التكوين، أعد تشغيل الخدمة

الوثائق ذات الصلة

- **مرجع التكوين** - الوثائق الكاملة لبارامترات نظير الخادم
- SMPP **دليل الاستخدام** - إدارة اتصالات
- **استكشاف الأخطاء وإصلاحها** - إجراءات استكشاف الأخطاء وإصلاحها العامة

دليل استكشاف الأخطاء وإصلاحها

المشاكل والحلول الشائعة

الخدمة لا تبدأ / تعارضات المنافذ

مع OmniMessage Core أو SMPP تعطل بوابة
على المنفذ 8443 :eaddrinuse

الأعراض:

- يتم إعادة تشغيل إحدى الخدمات باستمرار (systemctl show <unit> -p NRestarts يرتفع بسرعة).
- تظهر السجلات:

```
Running ApiEx.Endpoint with Bandit ... at https failed,  
port 8443 already in use  
... failed to start child: ApiEx.Supervisor ... ** (EXIT)  
:eaddrinuse
```

- curl -sk https://<host>:8443/api/messages على الرغم من أن 404 يعيد المتجر يجب أن يجيب.

موجودتان على نفس المضيف وكلاهما يربطان OmniMessage Core و SMPP **السبب:** بوابة على المنفذ الافتراضي 8443. الذي يبدأ أولاً يفوز بالمنفذ؛ الآخر api_ex واجهة برمجة التطبيقات من قبل البوابة (التي ليس /api/messages يدخل في حلقة تعطل. إذا فازت البوابة، يتم تقديم 404 لديها متجر) ويعيد 404.

Core الخاصة بالبوابة من منفذ OAM/Management **الحل:** نقل واجهة برمجة التطبيقات وإلغاء تعليق /etc/omnimessage_smpp/runtime.exs قم بتحرير. (بـ 8443 Core يحتفظ) مع تعيين منفذ مجاني. تظل البوابة عميلاً لواجهة برمجة تطبيقات المتجر الخاصة بـ api_ex تجاوز api_base_url عبر Core.

```
# /etc/omnimessage_smpp/runtime.exs
config :api_ex,
  api:
    Application.get_env(:api_ex, :api, %{})
    |> Map.put(:port, 8444)
    |> Map.put(:listen_ip, "0.0.0.0")
```

ثم أعد تشغيل كلا الخدمتين

```
sudo systemctl restart omnimessage-smpp
sudo systemctl restart omnimessage # let Core reclaim :8443
```

يملك 8443 وأن البوابة تملك منفذها الجديد Core بعد إعادة التشغيل، تحقق من أن

```
ss -lntp | grep -E ':8443|:8444'
curl -sk -o /dev/null -w '%{http_code}\n'
https://127.0.0.1:8443/api/messages # store answers (not 404)
```

للحصول على التفاصيل [CONFIGURATION.md](#) → [OAM/Management API port](#) انظر.

OmniMessage مشاكل الاتصال بـ

فإن مشاكل الاتصال بـ OmniMessage Core، بلا حالة وتعتمد بالكامل على SMPP نظرًا لأن بوابة OmniMessage حرجة المشاكل حرجة.

OmniMessage أعراض قطع الاتصال بـ

- لا توجد رسائل صادرة: تتراكم الرسائل، ولا يتم إرسال الرسائل
- لا توجد رسائل واردة: لا يمكن للشركاء تقديم الرسائل
- وقتًا طويلاً أو تتعطل API أوقات الانتظار: تستغرق مكالمات
- إعادة تعيين "، "HTTP 503"، "تظهر السجلات: "تم رفض الاتصال"، "انتهت المهلة الاتصال"

التشخيص

1. OmniMessage تحقق من توفر:

```
# اختبار الاتصال
curl -k -v https://omnimessage-
core.example.com:8443/api/system/health

# اختبار من مضيف البوابة بشكل محدد
ssh gateway-server 'curl -k https://omnimessage-
core.example.com:8443/api/system/health'
```

2. لواجهة برمجة التطبيقات المكونة URL تحقق من عنوان:

```
# مراجعة التكوين
grep -A1 'api_base_url' /opt/omnimessage-smpp/config/runtime.exs

# تحقق من الاتصال بالشبكة
ping omnimessage-core.example.com
nc -zv omnimessage-core.example.com 8443
```

3. تحقق من سجلات البوابة لأخطاء واجهة برمجة التطبيقات:

```
# ابحث عن الأخطاء المتعلقة بواجهة برمجة التطبيقات
sudo journalctl -u omnimessage-smpp -f | grep -i
'api\|omnimessage\|connect'

# ابحث في السجلات عن الأخطاء الأخيرة
sudo journalctl -u omnimessage-smpp -n 200 | grep -i error
```

الحلول

معطلة OmniMessage إذا كانت:

1. OmniMessage اتصل بفريق عمليات
2. ستتراكم الرسائل المعلقة في قائمة الانتظار
3. ستستمر البوابة في إعادة المحاولة (انظر `SMPP_POLL_INTERVAL`)

أو المراقبة OmniMessage تحقق من صفحة حالة 4.

تعمل ولكن البوابة لا تستطيع الوصول إليها OmniMessage إذا كانت

1. الصادرة HTTPS تحقق من قواعد جدار الحماية للسماح بـ.
2. DNS: nslookup omnimessage-core.example.com تحقق من حل.
3. traceroute omnimessage-core.example.com: تحقق من توجيه الشبكة.
4. HTTPS إذا كنت تستخدم SSL تحقق من شهادات.

لواجهة برمجة التطبيقات غير مكون بشكل صحيح URL إذا كان عنوان

1. قم بتحرير /opt/omnimessage-smpp/config/runtime.exs
2. (للإنتاج HTTPS يجب أن يكون) صحيح api_base_url تحقق من أن
3. أعد تشغيل البوابة: sudo systemctl restart omnimessage-smpp

مشاكل الاتصال

لا يمكن إنشاء الاتصال

الأعراض:

- الحالة تظهر "غير متصل" (أحمر)
- لا يوجد ربط ناجح في السجلات
- محاولات اتصال متكررة

الأسباب المحتملة والحلول:

1. مشاكل الاتصال بالشبكة.

تحقق:

```
# اختبار حل DNS
nslookup smpp.carrier.com

# اختبار الاتصال
ping -c 3 smpp.carrier.com

# اختبار المنفذ
telnet smpp.carrier.com 2775
أو
nc -zv smpp.carrier.com 2775
```

الحلول:

- بدلاً من اسم المضيف في التكوين IP استخدم عنوان DNS: إذا فشل
- تحقق من قواعد جدار الحماية، اتصل بالناقل: ping إذا فشل
- إذا فشل المنفذ: تحقق من رقم المنفذ الصحيح، تحقق من جدار الحماية

2. بيانات اعتماد غير صحيحة

تحقق:

- "تظهر السجلات" فشل الربط "أو" خطأ في المصادقة
- وكلمة المرور system_id أقران العملاء → تحقق من → SMPP: واجهة الويب

الحلول:

- تأكيد بيانات الاعتماد مع الناقل
- تحقق من الأخطاء المطبعية (حساسية لحالة الأحرف)
- تحديث التكوين وإعادة الاتصال

3. غير مدرج في القائمة البيضاء IP عنوان

تحقق:

- تم رفض الاتصال على الفور
- غير المصرح به IP تظهر سجلات الناقل عنوان

الحلول:

- العام للبوابة الخاصة بك IP تأكيد عنوان:

```
curl ifconfig.me
```

- إلى القائمة البيضاء IP طلب من الناقل إضافة
- (ديناميكي IP) لم يتغير IP تحقق من أن

4. جدار الحماية يحظر.

تحقق:

```
# تحقق مما إذا كان المنفذ مفتوحًا
sudo iptables -L -n | grep 2775

# (أوبونتو/ديبيان) UFW تحقق من
sudo ufw status | grep 2775

# firewalld (RHEL/CentOS) تحقق من
sudo firewall-cmd --list-ports | grep 2775
```

الحلول:

```
# أوبونتو/ديبيان
sudo ufw allow out 2775/tcp

# RHEL/CentOS
sudo firewall-cmd --permanent --add-port=2775/tcp
sudo firewall-cmd --reload
```

5. عنوان/منفذ المصدر المثبت غير متاح

انظر) `bind_source_port` و/أو `bind_source_ip` ينطبق فقط عندما يحدد عميل الربط [CONFIGURATION.md](#)).

تحقق:

- تظهر السجلات فشل الاتصال في فتح المقبس المحلي
- ليس عنوانًا تحتفظ به هذه المضيف `bind_source_ip`
- المكون `bind_source_port` يحتفظ عملية أخرى بالفعل بـ

الحلول:

- `ip addr show`: هو عنوان محلي `bind_source_ip` تأكيد أن
- غير صالح ويتم تجاهله - ثم يختار نظام التشغيل عنوان `bind_source_ip` يتم تسجيل المصدر، والذي قد لا يتطابق مع القائمة البيضاء للناقل. صحح العنوان إذا كانت التسليم تفشل.
- لذا يعيد الاتصال الربط على الفور، `SO_REUSEADDR` يتم فتح المنفذ المثبت باستخدام إذا كان المنفذ لا يزال غير متاح، `TIME_WAIT` حتى أثناء وجود المقبس القديم في `sudo ss -ltnp | grep <port>` تحقق مما إذا كانت خدمة أخرى تستخدمه

الاتصال يستمر في الانقطاع

الأعراض:

- تم إنشاء الاتصال ولكن يتم قطع الاتصال بشكل متكرر
- زيادة مقياس `smpp_disconnection_total`
- تظهر السجلات إعادة اتصالات متكررة

الأسباب المحتملة والحلول:

1. عدم استقرار الشبكة

تحقق:

```
# مراقبة فقدان الحزم
ping -c 100 smpp.carrier.com | grep loss

# تحقق من أخطاء الشبكة
netstat -s | grep -i error
```

الحلول:

- اتصل بالناقل حول مشاكل الشبكة
- تحقق مع مزود خدمة الإنترنت إذا كان من جانبك
- النظر في اتصال/مسار احتياطي

2. انتهاء مهلة استفسار الرابط

تحقق:

- "تظهر السجلات" انتهاء مهلة استفسار الرابط
- ينقطع الاتصال بعد فترات من عدم النشاط

الحلول:

- مدة انتهاء المهلة الافتراضية هي 30 ثانية
- keepalive تحقق من أن الشبكة تسمح بحزم
- تحقق من جدران الحماية العدوانية التي تنتهي مهلة الاتصالات الخاملة

3. تجاوز حد TPS

تحقق:

- معدل الرسائل مرتفع عند وقت قطع الاتصال
- يقوم الناقل بتقليل الرسائل

الحلول:

- `tps_limit` مراجعة إعداد
- إلى 70-80% من الحد الأقصى للناقل TPS تقليل
- توزيع حركة المرور عبر عمليات ربط متعددة

4. مشاكل خادم الناقل

تحقق:

- تحقق من حالة خدمة الناقل
- اتصل بدعم الناقل

الحلول:

- انتظر حتى يحل الناقل المشكلة
 - تكوين ناقل احتياطي إذا كان متاحًا
-

مشاكل تسليم الرسائل

الرسائل لا تُرسل

الأعراض:

- الرسائل عالقة في قائمة الانتظار
- `smpp_messages_sent_total` لا يرتفع
- الاتصال يظهر متصل

الأسباب المحتملة والحلول:

1. غير صحيح `dest_smsc` توجيه

تحقق:

- للمرسلة `dest_smsc` واجهة الويب → قائمة الانتظار → تحقق من حقل
- الحالة الحية → SMPP قارن مع اسم الاتصال في

الحلول:

- `dest_smsc` يتم توجيه الرسائل بناءً على حقل
- الصحيح `dest_smsc` تحقق من أن الخلفية تعين
- تحقق من التوجيه الافتراضي، `dest_smsc` NULL، إذا كان

2. الرسائل المجدولة للمستقبل

تحقق:

- `deliver_after` واجهة الويب → قائمة الانتظار → تحقق من حقل
- الرسائل ذات الطابع الزمني المستقبلي لن تُرسل بعد

الشرح:

- للمرسلة الفاشلة `deliver_after` يقوم نظام إعادة المحاولة بتعيين
- تنتظر الرسائل حتى ذلك الوقت قبل إعادة المحاولة

الحلول:

- انتظر حتى الوقت المجدول
- إذا كان الأمر عاجلاً، اتصل بفريق الخلفية لإعادة تعيين الطابع الزمني

3. منخفض جدًا TPS حد

تحقق:

- تراكم كبير في قائمة الانتظار
- الرسائل تُرسل ببطء شديد

الحلول:

- في التكوين `tps_limit` زيادة
- تحقق من أن الناقل يمكنه التعامل مع معدل أعلى
- انظر [CONFIGURATION.md](#)

4. عامل قائمة الانتظار غير قيد التشغيل

تحقق:

- حالة الخدمة
- السجلات للأخطاء

الحلول:

```
# إعادة تشغيل الخدمة
sudo systemctl restart omnimessage-smpp

# تحقق من السجلات
sudo journalctl -u omnimessage-smpp -f
```

5. الواجهة الأمامية غير مسجلة تحت الاسم المتوقع

بتوجيه الرسالة إلى هذه البوابة فقط إذا تم تسجيل نظير تحت اسم OmniMessage Core يقوم للرسالة. يسجل كل نظير تحت **مفتاح التوجيه** الخاص به `dest_smsc` الواجهة الأمامية يساوي (انظر [تسجيل الواجهة الأمامية](#)):

- **أقران العملاء:** قائمة الانتظار المكونة، أو اسم النظير العاري إذا لم يتم تعيين أي `queue`.

- **عمليات الربط:** اسم الربط .

تحقق:

- Successfully registered SMPP peer frontend السجلات للمدخلات على الرسائل العالقة dest_smsc يتطابق مع <name> تأكد من أن — '<name>'
- توقع تسجيلًا واحدًا تحت اسم قائمة الانتظار ، queue بالنسبة للربط التي تشارك المشتركة، وليس واحدًا لكل نظير

الحلول:

- إلى مفتاح التوجيه (قائمة انتظار النظير، وإلا dest_smsc تأكد من أن الخلفية تعين (نظام التسمية السابق الذي لم يعد ينطبق) {hostname}_{peer} اسمه)، وليس إلى مشتركة، قم بتوجيه الرسائل إلى اسم قائمة الانتظار بدلاً من queue إذا كنت تستخدم اسم نظير فردي
- تأكد من أن النظير مفعل — النظائر المعطلة غير مسجلة

معدل فشل التسليم مرتفع

الأعراض:

- smpp_delivery_failures_total يرتفع
- مع حالة خطأ "submit_sm_resp" تظهر السجلات
- الرسائل لا تصل إلى المستلمين

الأسباب المحتملة والحلول:

1. أرقام وجهة غير صالحة

تحقق:

- السجلات لأكواد الخطأ المحددة
- مراجعة تنسيق وجهة الرسالة

أكواد الخطأ الشائعة:

- 0x0000000B - وجهة غير صالحة
- 0x00000001 - طول رسالة غير صالح

- أمر غير صالح - 0x00000003

الحلول:

- (E.164 يوصى بـ) تحقق من تنسيق الرقم
- تحقق من أن الرقم يتضمن رمز الدولة
- تحقق من متطلبات الناقل

2. محتوى الرسالة غير صالح

تحقق:

- طول الرسالة
- الأحرف الخاصة
- الترميز

الحلول:

- الحد الأقصى 160 حرفًا: GSM-7
- الحد الأقصى 70 حرفًا: UCS-2
- إزالة الأحرف غير المدعومة
- تحقق من إعدادات الترميز

3. رفض الناقل

تحقق:

- أكواد الخطأ المحددة من الناقل
- أنماط الرسائل المرفوضة

الحلول:

- اتصل بالناقل لمعرفة سبب الرفض
- قد تحتاج إلى تصفية المحتوى
- تحقق من أنماط البريد العشوائي/الإساءة

4. الرسائل منتهية الصلاحية

تحقق:

- للرسالة `expires` الطابع الزمني
- توقيت محاولة التسليم

الحلول:

- زيادة فترة صلاحية الرسالة
- تقليل تأخير إعادة المحاولة للرسائل الحساسة للوقت

مشاكل واجهة الويب

لا يمكن الوصول إلى لوحة التحكم على الويب

الأعراض:

- <https://your-server:8087> المتصفح لا يمكنه الاتصال بـ
- انتهاء المهلة أو تم رفض الاتصال

الأسباب المحتملة والحلول

1. الخدمة غير قيد التشغيل

تحقق:

```
sudo systemctl status omnimessage-smpp
```

الحلول:

```
# إذا كانت متوقفة، ابدأها
sudo systemctl start omnimessage-smpp

# تحقق من السجلات للأخطاء
sudo journalctl -u omnimessage-smpp -n 50
```

2. جدار الحماية يحظر المنفذ 8087

تحقق:

```
sudo ufw status | grep 8087
# أو
sudo firewall-cmd --list-ports | grep 8087
```

الحلول:

```
# أوبونتو/ديبيان
sudo ufw allow 8087/tcp

# RHEL/CentOS
sudo firewall-cmd --permanent --add-port=8087/tcp
sudo firewall-cmd --reload
```

3. مشاكل شهادة SSL

تحقق:

- يظهر المتصفح تحذير أمان
- الشهادة منتهية الصلاحية أو غير صالحة

الحلول:

- قبول استثناء الأمان (إذا كانت موقعة ذاتيًا)
- صالحة SSL تثبيت شهادة
- تحقق من وجود ملفات الشهادة:

```
ls -l /opt/omnimessage-smpp/priv/cert/
```

4. غير صحيح URL عنوان

تحقق:

- HTTP ليس HTTPS تحقق من استخدام
 - اسم المضيف الصحيح/IP تحقق من عنوان
 - تحقق من المنفذ 8087
-

واجهة الويب تظهر أخطاء

الأعراض:

- يتم تحميل الصفحة ولكن تظهر أخطاء
- لا تعمل الوظائف
- البيانات لا تعرض

الحلول:

1. مسح ذاكرة التخزين المؤقت للمتصفح:

- Ctrl+F5 (تحديث صعب)
- مسح ذاكرة التخزين المؤقت للمتصفح وملفات تعريف الارتباط

2. تحقق من وحدة تحكم المتصفح:

- F12 اضغط على
- JavaScript تحقق من علامة التبويب "وحدة التحكم" لأخطاء
- أبلغ الدعم إذا تم العثور على أخطاء

3. جرب متصفحًا مختلفًا:

- Edge وFirefox وChrome اختبر في
- عزل المشكلات الخاصة بالمتصفح

4. تحقق من سجلات الخدمة:

```
sudo journalctl -u omnimessage-smpp -f
```

مشاكل المقاييس

غير متاحة Prometheus مقاييس

الأعراض:

- `curl http://localhost:4000/metrics` يفشل
- جمع المقاييس Prometheus لا يمكن لـ
- استجابة فارغة أو خطأ

الأسباب المحتملة والحلول:

1. الخدمة غير قيد التشغيل

تحقق:

```
sudo systemctl status omnimessage-smpp
```

الحلول:

```
sudo systemctl start omnimessage-smpp
```

2. المنفذ غير متاح

تحقق:

```
# اختبار محليًا
curl http://localhost:4000/metrics

# اختبار عن بُعد
curl http://your-server-ip:4000/metrics
```

الحلول:

- إذا كانت المحلية تعمل ولكن البعيدة لا تعمل: تحقق من جدار الحماية
- Prometheus افتح المنفذ 4000 في جدار الحماية لخادم

3. نقطة النهاية غير صحيحة

تحقق:

- `/stats` أو `/prometheus` (ليس `/metrics`) نقطة النهاية هي
- المنفذ هو 4000 (ليس 8087)

المقاييس تظهر قيم غير متوقعة

الأعراض:

- تعود العدادات إلى الصفر
- تظهر المقاييس قيم خاطئة
- المقاييس مفقودة لبعض الربط

الحلول:

1. إعادة تشغيل الخدمة تعيد تعيين العدادات:

- يتم إعادة تعيين العدادات عند إعادة تشغيل الخدمة
- هذا سلوك طبيعي
- Prometheus في استعلامات `rate()` أو `increase()` استخدم

2. الربط الجديدة لا تظهر:

- تظهر المقاييس فقط بعد الحدث الأول
- أرسل رسالة اختبار لتعبئة المقاييس
- تحقق من أن الربط مفعّل ومتصل

3. مقاييس قديمة:

- قد تظهر الربط القديمة في المقاييس
- أعد تشغيل الخدمة لمسح الإدخالات القديمة
- للتصفية Prometheus أو استخدم إعادة تسمية

مشاكل الأداء

مرتفع CPU استخدام

تحقق:

```
top -p $(pgrep -f omnimessage-smpp)
```

الأسباب المحتملة:

- حجم رسالة مرتفع جدًا
- عدد كبير من الاتصالات
- مشكلة في التكوين

الحلول:

- تحقق من أن معدل الرسائل ضمن السعة
- TPS مراجعة حدود
- مرتفعًا بشكل مستمر CPU اتصل بالدعم إذا كان استخدام

استخدام الذاكرة مرتفع

تحقق:

```
ps aux | grep omnimessage-smpp
```

الأسباب المحتملة:

- قائمة انتظار الرسائل الكبيرة في الذاكرة
- تسرب الذاكرة (نادرًا)

الحلول:

- أعد تشغيل الخدمة لمسح الذاكرة
- تحقق من حجم قائمة انتظار الرسائل
- اتصل بالدعم إذا استمرت الذاكرة في النمو

معالجة الرسائل ببطء

الأعراض:

- تستغرق الرسائل وقتًا طويلًا للإرسال

- تتراكم قائمة الانتظار
- معدل الرسائل منخفض

تحقق:

1. قد تكون صارمة جدًا - TPS دود
2. `queue_check_frequency` - قد تكون مرتفعة جدًا
3. وقت استجابة واجهة برمجة التطبيقات الخلفية - قد تكون بطيئة
4. زمن الانتقال الشبكي إلى الناقل

الحلول:

- إذا كان الناقل يسمح بذلك TPS زيادة
- لزيادة سرعة الاستطلاع `queue_check_frequency` تقليل
- تحسين واجهة برمجة التطبيقات الخلفية
- تحقق من زمن الانتقال الشبكي

مشاكل التكوين

أخطاء في بناء جملة ملف التكوين

الأعراض:

- الخدمة لا تبدأ بعد تغيير التكوين
- "تظهر السجلات خطأ في بناء الجملة" أو "خطأ في التحليل"

تحقق:

```
# Elixir تحقق من بناء جملة
/opt/omnimessage-smpp/bin/omnimessage-smpp eval "File.read!
('config/runtime.exs')"
```

الأخطاء الشائعة:

- فاصلة مفقودة بين إدخالات الخريطة

- اقتباسات غير متطابقة (" مقابل ')
- أقواس أو أقواس غير متطابقة
- في الأعلى `import Config` مفقود

الحلول:

- استعادة من النسخة الاحتياطية
- مراجعة بناء الجملة بعناية
- Elixir استخدم محرر نصوص مع تمييز بناء جملة

التغييرات لا تؤثر

الأعراض:

- تم تعديل التكوين ولكن لا يوجد تغيير في السلوك
- لا تزال الإعدادات القديمة نشطة

الحلول:

```
# تتطلب تغييرات التكوين إعادة التشغيل
sudo systemctl restart omnimessage-smpp

# تحقق من نجاح إعادة التشغيل
sudo systemctl status omnimessage-smpp

# تحقق من السجلات للأخطاء
sudo journalctl -u omnimessage-smpp -n 50
```

استعادة الطوارئ

فشل النظام بالكامل

الخطوات:

1. تحقق من صحة النظام الأساسية.

```
# مساحة القرص  
df -h
```

```
# الذاكرة  
free -h
```

```
# تحميل CPU  
uptime
```

2. تحقق من حالة الخدمة:

```
sudo systemctl status omnimessage-smpp
```

3. راجع السجلات الأخيرة:

```
sudo journalctl -u omnimessage-smpp -n 200
```

4. حاول إعادة تشغيل الخدمة:

```
sudo systemctl restart omnimessage-smpp
```

5. إذا فشلت إعادة التشغيل:

- تحقق من بناء جملة التكوين
- SSL تحقق من وجود شهادات
- تحقق من أذونات الملفات
- راجع السجلات للخطأ المحدد

6. استعادة من النسخة الاحتياطية (إذا لزم الأمر):

```
# استعادة التكوين  
sudo cp /opt/omnimessage-smpp/config/runtime.exs.backup \  
/opt/omnimessage-smpp/config/runtime.exs
```

```
# إعادة التشغيل  
sudo systemctl restart omnimessage-smpp
```

اتصل بالدعم إذا لم يتم حل المشكلة 7.

الحصول على المساعدة

المعلومات التي يجب جمعها

قبل الاتصال بالدعم، اجمع

1. الإصدار: `cat /opt/omnmessage-smpp/VERSION`

2. السجلات الأخيرة:

```
sudo journalctl -u omnmessage-smpp -n 200 > /tmp/smpp-logs.txt
```

3. التكوين (قم بتطهير كلمات المرور):

```
sudo cp /opt/omnmessage-smpp/config/runtime.exs  
/tmp/config.exs  
# لإزالة كلمات المرور قبل الإرسال /tmp/config.exs تحرير
```

4. مخرجات المقاييس:

```
curl http://localhost:4000/metrics > /tmp/metrics.txt
```

5. معلومات النظام:

```
uname -a > /tmp/system-info.txt  
free -h >> /tmp/system-info.txt  
df -h >> /tmp/system-info.txt
```

الاتصال بالدعم

- البريد الإلكتروني: support@omnitouch.com
 - 61+ XXXX XXXX (24/7) الهاتف
 - تضمين: جميع المعلومات من أعلاه
-

الوثائق ذات الصلة

- **USAGE.md** - إجراءات التشغيل العادية
 - **CONFIGURATION.md** - مرجع التكوين
 - **MONITORING.md** - المراقبة والمقاييس
 - **README.md** - نظرة عامة على النظام
-

دليل العمليات

إجراءات التشغيل اليومية

OmniMessage Core: الاعتماد الحرج

OmniMessage Core العمل بدون الوصول إلى OmniMessage SMPP **مهم**: لا يمكن لجسر الجسر هو مجرد مترجم بروتوكول - OmniMessage تتم معالجة جميع الرسائل في

:غير متاح OmniMessage إذا أصبح

- لا يمكن تقديم رسائل جديدة □
- لا يمكن استرجاع الرسائل المعلقة □
- لا يمكن الإبلاغ عن حالة التسليم □
- يبدو أن النظام يتوقف أو ينتهي وقته □

OmniMessage: تحقق من صحة

```
# اختبار اتصال API
curl -k https://omnimessage-
core.example.com:8443/api/system/health
```

```
# المكون في السجلات URL تحقق من عنوان
grep api_base_url /opt/omnimessage-smpp/config/runtime.exs
```

العمليات اليومية

فحص الصحة الصباحية

:قم بإجراء هذه الفحوصات في بداية كل يوم

1. الوصول إلى لوحة التحكم على الويب

- URL: `https://your-server:8087`

- تحقق مما إذا كانت اللوحة تُحمّل بشكل صحيح

2. تحقق من حالة الاتصال

- الحالة الحية → SMPP: انتقل إلى
- تحقق من أن جميع الاتصالات تظهر "متصلة" (باللون الأخضر)
- لاحظ أي روابط مفصولة

3. مراجعة مقاييس الرسائل

- Queue انتقل إلى: علامة التبويب
- تحقق من أن عدد الرسائل معقول
- تحقق من عدم وجود تراكم غير متوقع في الطابور

4. تحقق من سجلات النظام

- Logs انتقل إلى: علامة التبويب
- ابحث عن رسائل الخطأ (باللون الأحمر)
- لاحظ أي أنماط تحذيرية

5. Prometheus مراجعة مقاييس

- `curl http://localhost:4000/metrics`
- Grafana أو تحقق من لوحات
- تحقق من أن معدلات الرسائل طبيعية

المراقبة المستمرة

قم بإعداد تنبيهات لـ

- فشل الاتصال (< 2 دقيقة غير متصلة)
- ارتفاع معدلات فشل التـليم (< 5%)
- عدم وجود حركة مرور لفترات طويلة
- انقطاعات متكررة

لتكوين التنبيهات **MONITORING.md** انظر.

فهم توجيه الرسائل

باستخدام حقلين SMPP واتصالات OmniMessage Core يقوم الجسر بتوجيه الرسائل بين رئيسيين:

- **dest_smsc** — يوجه الرسائل الصادرة إلى **روابط العملاء**. عندما يقوم `dest_smsc: "vodafone_uk"` بتجميع رسالة مع `submit_sm` SMPP وترسلها عبر `vodafone_uk` العميل للجسر المسمى `submit_sm`.
- **source_smsc** — يوجه الرسائل الواردة إلى **روابط الخادم**. عندما يقوم `source_smsc: "partner_acme"` بتجميع رسالة مع `partner_acme` الجسر بتسليمها إلى العملاء المتصلين برابط الخادم المسمى `deliver_sm` SMPP.

الذي يقدم إلى ESME الجسر هو `submit_sm` PDUs **التميز الرئيسي**: روابط العملاء ترسل ESME الذي يسلم إلى SMSC الجسر هو `deliver_sm` PDUs روابط الخادم ترسل. (الناقل المتصل).

تسجيل الواجهة الأمامية

حتى يعرف الجزء الخلفي أي OmniMessage Core يقوم الجسر بتسجيل نفسه تلقائيًا مع متاحة لتوجيه الرسائل SMPP اتصالات.

- افتراضي (smc_name اسم التسجيل: تم التحكم فيه بواسطة إعداد "smpp_gateway", env: SMSC_NAME)
- نبض القلب: يُرسل كل 60 ثانية للحفاظ على التسجيل نشطاً
- انتهاء الصلاحية: تنتهي صلاحية التسجيل في الجزء الخلفي بعد 90 ثانية بدون نبض قلب
- تسجيل لكل رابط: يتم تسجيل كل نظير مفعّل بشكل فردي تحت مفتاح التوجيه الذي يتوجّه dest_smc الخاص به، لذا فإن اسم الواجهة الأمامية المسجل يساوي عليه الجزء الخلفي:
 - المكونة (إذا تم تعيينها)، وإلا queue الأقران العملاء: يتم تسجيلها تحت تحت اسم النظير الأساسي. لذلك، يتم تسجيل العديد من الأقران العملاء تحت اسم مشترك واحد.
 - روابط الخادم: يتم تسجيلها تحت اسم الرابط الخاص بها.

فإن تسجيلاته تنتهي ويتوقف الجزء، OmniMessage Core إذا توقف الجسر أو فقد الاتصال به الخلفي عن توجيه الرسائل إليه.

استكشاف الأخطاء: إذا لم يتم توجيه الرسائل إلى الجسر، تحقق من

1. "frontend_register" السجلات لمداخلات
2. OmniMessage يتطابق مع ما يتوقعه smc_name أن
3. OmniMessage Core (api_base_url) الاتصال الشبكي بـ

SMPP إدارة اتصالات

SMPP كيفية تكوين أقران

بإستخدام طريقتين (الأقران) SMPP يمكن تكوين اتصالات

الطريقة 1: واجهة الويب (موصى بها)

- الميزة: التغييرات تأخذ مفعولها على الفور، لا حاجة لإعادة التشغيل
- علامات التبويب الأقران العملاء / الأقران الخادم → SMPP: الموقع
- العمليات: إضافة، تعديل، حذف الأقران
- Mnesia الاستمرارية: مخزنة في قاعدة بيانات
- الأفضل لـ: العمليات اليومية، الاختبار، التغييرات السريعة

الطريقة 2: ملف التكوين

- **الميزة:** التكوين ككود، التحكم في النسخ
- **الموقع:** `/opt/omnimessage-smpp/config/runtime.exs`
- **Elixir العمليات:** تعريف الأقران في تكوين
- **الاستمرارية:** تعتمد على الملفات، تبقى بعد إعادة التشغيل
- **يتطلب:** إعادة تشغيل **❖❖** خدمة بعد التغييرات
- **الأفضل لـ:** الإعداد الأولي، البنية التحتية ككود

ملاحظة: يتم تخزين تغييرات واجهة الويب بشكل منفصل وتجاوز إعدادات ملف التكوين.

للرجوع إلى ملف التكوين **CONFIGURATION.md** انظر

إضافة اتصال عميل جديد

لِلناقل (خادم) **SMSC** متصل بـ (عميل) **ESME** **الغرض:** تكوين الجسر ليعمل كـ

التحضير: جمع المعلومات من الناقل

- SMPP خادم IP اسم مضيف/عنوان
- رقم المنفذ (عادة 2775)
- معرف النظام (اسم المستخدم)
- كلمة المرور
- نوع الربط (عادة ما يكون ثنائي الاتجاه)
- حد TPS

اختر واحدة من الطرق التالية

الخيار أ: عبر واجهة الويب (موصى بها)

ال❖❖زايا: تأثير فوري، لا حاجة لإعادة التشغيل

الخطوات:

1. انتقل إلى الأقران العملاء

- افتح واجهة الويب `https://your-server:8087`
- الأقران العملاء → SMPP: انتقل إلى

2. إضافة نظير جديد:

- انقر على "إضافة نظير عميل جديد"
- املأ النموذج:
 - (معرف فريد) `vodafone_uk`: الاسم
 - `smpp.vodafone.co.uk`: المضيف
 - `2775`: المنفذ
 - `your_username`: معرف النظام
 - `your_password`: كلمة المرور
 - `Transceiver`: نوع الربط
 - `100` TPS: حد
 - `1000`: تكرار فحص الطابور
- انقر على "حفظ"

3. الاتصال يتم إنشاؤه تلقائيًا:

- يحاول الجسر الاتصال على الفور
- الحالة الحية → SMPP: انتقل إلى
- يجب أن يتغير الحالة إلى "متصل" (باللون الأخضر) خلال 10-30 ثانية
- لرسالة الربط الناجحة Logs تحقق من علامة التبويب

4. اختبار تدفق الرسائل:

- Queue انتقل إلى: علامة التبويب
- تتطابق مع اسم الربط `dest_smsc` قدم رسالة اختبار مع

- راقب في الحالة الحية للإرسال
- تحقق من تأكيد التسليم

الخيار ب: عبر ملف التكوين

المزايا: البنية التحتية ككود، التحكم في النسخ

الخطوات:

1. تحرير ملف التكوين:

```
sudo nano /opt/omnimessage-smpp/config/runtime.exs
```

2. إضافة ربط جديد إلى التكوين:

```
config :omnimessage_smpp, :binds, [  
  # الروابط الموجودة...  
  
  # إضافة ربط جديد  
  %{  
    name: "vodafone_uk",  
    mode: :client,  
    bind_type: :transceiver,  
    host: "smpp.vodafone.co.uk",  
    port: 2775,  
    system_id: "your_username",  
    password: "your_password",  
    tps_limit: 100,  
    queue_check_frequency: 1000,  
  
    # المنفذ المحلي إذا كان الناقل/IP اختياري: تثبيت عنوان  
    # يبيضهما  
    bind_source_ip: "10.20.30.40",  
    bind_source_port: 5000,  
  
    # اختياري: مشاركة طابور خلفي واحد عبر عدة روابط (يكون  
    # افتراضيًا على الاسم)  
    queue: "vodafone_uk"  
  }  
]
```

للحصول على القائمة الكاملة لمعلومات ربط العميل، بما `CONFIGURATION.md` انظر `bind_source_ip`، `bind_source_port`، و `queue` في ذلك.

3. حفظ وإعادة تشغيل الخدمة:

```
# حفظ الملف (Ctrl+X, Y, Enter في nano)

# إعادة تشغيل الخدمة
sudo systemctl restart omnimessage-smpp
```

4. التحقق من الاتصال:

- الحالة الحية → SMPP: انتقل إلى
- ابحث عن الاتصال الجديد
- يجب أن تكون الحالة "متصلة" (باللون الأخضر)
- تحقق من السجلات لرسالة الربط الناجحة

5. اختبار تدفق الرسائل:

- Queue انتقل إلى: علامة التبويب
- تتطابق مع اسم الربط الجديد `dest_smsc` قدم رسالة اختبار مع
- راقب في الحالة الحية للإرسال
- تحقق من تأكيد التسليم

إضافة ربط خادم

(عملاء الشركاء) **ESMEs** يقبل الاتصالات من (خادم) **SMSC العرض**: تكوين الجسر ليعمل كـ الخارجيين

التحضير:

1. إنشاء بيانات الاعتماد:

- `partner_name`: أنشئ معرف نظام فريد
- أنشئ كلمة مرور قوية
- وثق وشارك بشكل آمن مع الشريك

2. الحصول على معلومات الشريك:

- المصدر للشريك IP عناوين
- (TPS لحد) حجم الرسائل المتوقع
- أنواع الربط المطلوبة

اختر واحدة من الطرق التالية

الخيار أ: عبر واجهة الويب (موصى بها)

المزايا: تأثير فوري، لا حاجة لإعادة التشغيل

الخطوات:

1. انتقل إلى الأقران الخادم:

- افتح واجهة الويب: `https://your-server:8087`
- الأقران الخادم → SMPP: انتقل إلى

2. إضافة نظير خادم جديد:

- انقر على "إضافة نظير خادم جديد"
- املأ النموذج:
 - (معرف فريد) `partner_acme`: الاسم
 - `acme_corp`: معرف النظام
 - `secure_password_123`: كلمة المرور
 - أنواع الربط المسموح بها: اختر الكل (مرسل، مستلم، ثنائي الاتجاه)
 - IP قائمة البيضاء لـ: `203.0.113.0/24` (مفصولة بفواصل لعدة)
 - TPS: `50`
 - تكرار فحص الطابور: `1000`
- انقر على "حفظ"

3. الجسر جاهز للاتصال:

- أصبح نظير الخادم الآن نشطاً وينتظر الاتصال من الشريك
- لا حاجة لإعادة التشغيل

4. مشاركة المعلومات مع الشريك:

- للجسر IP عنوان
- المنفذ: 2775
- معرف النظام: acme_corp
- كلمة المرور: secure_password_123
- نوع الربط: كما هو مكون

5. انتظر اتصال الشريك:

- الحالة الحية → SMPP: انتقل إلى
- راقب الاتصال الوارد
- تحقق من نجاح المصادقة
- مع القائمة البيضاء IP تحقق من تطابق

الخيار ب: عبر ملف التكوين

المزايا: البنية التحتية ككود، التحكم في النسخ

الخطوات:

1. تحرير ملف التكوين:

```
sudo nano /opt/omnimessage-smpp/config/runtime.exs
```

2. إضافة ربط خادم وتكوين الاستماع:

```
# server_binds أضف إلى قائمة
config :omnimessage_smpp, :server_binds, [
  # الروابط الخادمة الموجودة...

  # إضافة ربط خادم جديد
  %{
    name: "partner_acme",
    system_id: "acme_corp",
    password: "secure_password_123",
    allowed_bind_types: [:transmitter, :receiver,
:transceiver],
    ip_whitelist: ["203.0.113.0/24"],
    tps_limit: 50,
    queue_check_frequency: 1000
  }
]

# تأكد من وجود تكوين الاستماع (مطلوب مرة واحدة فقط)
config :omnimessage_smpp, :listen, %{
  host: "0.0.0.0",
  port: 2775,
  max_connections: 100
}
```

3. حفظ وإعادة تشغيل الخدمة:

```
sudo systemctl restart omnimessage-smpp
```

4. مشاركة المعلومات مع الشريك:

- للجسر IP عنوان
- المنفذ: 2775
- معرف النظام: acme_corp
- كلمة المرور: secure_password_123

- نوع الربط: كما هو مكون

5. انتظر اتصال الشريك:

- الحالة الحية → SMPP: انتقل إلى
- راقب الاتصال الوارد
- تحقق من نجاح المصادقة
- مع القائمة البيضاء IP تحقق من تطابق

تعديل الاتصال الحالي

(إلخ، IP كلمات المرور، قائمة البيضاء ل، TPS حدود) **الغرض:** تحديث معلومات الاتصال

اختر واحدة من الطرق التالية:

الخيار أ: عبر واجهة الويب (موصى بها)

المزايا: تأثير فوري، لا حاجة لإعادة التشغيل

الخطوات:

1. انتقل إلى الأقران:

- افتح واجهة الويب: `https://your-server:8087`
- الأقران العملاء → SMPP: للاتصالات العميلة
- الأقران الخادم → SMPP: للاتصالات الخادمة

2. تعديل النظير:

- ابحث عن النظير الذي ترغب في تعديله
- انقر على زر "تعديل"
- تحديث المعلومات المطلوبة
 - IP، كلمة المرور، قائمة البيضاء ل، TPS التغييرات الشائعة: حد المضيف/المنفذ
- انقر على "حفظ"

3. تطبيق التغييرات على الفور:

- يعيد الاتصال الاتصال تلقائيًا بالإعدادات الجديدة

- لا حاجة لإعادة تشغيل الخدمة
- الحالة الحية للتحقق → SMPP: انتقل إلى

4. التحقق من التغييرات:

- تحقق من أن الاتصال يتم إنشاؤه بنجاح
- للأخطاء Logs راقب علامة التبويب
- اختبر تدفق الرسائل إذا كان ذلك مناسبًا

الخيار ب: عبر ملف التكوين

المزايا: البنية التحتية ككود، التحكم في النسخ

الخطوات:

1. تحرير ملف التكوين:

```
sudo nano /opt/omnimessage-smpp/config/runtime.exs
```

2. تعديل معلمات الربط:

- `:server_binds` أو `:binds` ابحث عن الربط في قائمة
- تحديث المعلمات المطلوبة:
 - كلمات المرور، قائمة البيضاء لـ TPS، التغييرات الشائعة: حدود المضيف/المنفذ، IP
- مثال:

```
%{  
  name: "vodafone_uk",  
  # ... معلمات أخرى  
  tps_limit: 150, # تم تغييره من 100  
  password: "new_password" # كلمة المرور المحدثة  
}
```

3. حفظ وإعادة تشغيل الخدمة:

```
sudo systemctl restart omnimessage-smpp
```

4. التحقق من التغييرات:

- الحالة الحية → SMPP :انتقل إلى
- تحقق من أن الاتصال يتم إنشاؤه بنجاح
- راقب السجلات للأخطاء
- اختبر تدفق الرسائل

إزالة اتصال

SMPP الغرض: إيقاف تشغيل اتصال

الخطوات:

1. إخطار المعنيين:

- إبلاغ الناقل/الشريك
- تنسيق نافذة التوقف

2. قطع الاتصال عبر واجهة الويب:

- الحالة الحية → SMPP :انتقل إلى
- ابحث عن الاتصال
- "انقر على "قطع الاتصال"
- أكد الإجراء

3. إزالة التكوين:

- الأقران العملاء/الأقران الخادم → SMPP :انتقل إلى
- ابحث عن الاتصال
- "انقر على "حذف"
- أكد الإزالة

4. التحقق من الإزالة:

- تحقق من الحالة الحية - يجب أن يكون الاتصال قد اختفى
- راجع السجلات لإيقاف تشغيل نظيف

تمكين وتعطيل الاتصالات

الغرض: أخذ اتصال مؤقتًا خارج الخدمة دون حذف تكوينه

الذي يتحكم فيما إذا كانت نشطة. تحتفظ الأقران المعطلة بجميع **enabled** تمتلك الأقران حقل تكويناتها ولكنه ❖❖ لا تقيم أو تقبل الاتصالات.

عبر واجهة الويب:

1. الأقران العملاء أو الأقران الخادم → SMPP :انتقل إلى
2. ابحث عن النظير الذي ترغب في تعطيله
3. "انقر على "تعديل"
4. "قم بإلغاء تحديد خانة "مفعّل"
5. "انقر على "حفظ"

.سيتم قطع الاتصال على الفور. لإعادة التمكين، كرر الخطوات وحدد المربع مرة أخرى

حالات الاستخدام:

- نوافذ صيانة الناقل المخطط لها
- إيقاف مؤقت لاتصال الشريك أثناء التحقيق
- تعطيل اتصال أثناء انتظار بيانات اعتماد جديدة

سلوك الاتصال

منطق إعادة الاتصال

:عندما ينقطع ربط العميل بشكل غير متوقع، يحاول الجسر إعادة الاتصال تلقائيًا

- **فترة إعادة المحاولة:** كل 30 ثانية
- **بدء متدرج:** عندما تبدأ عدة روابط في نفس الوقت (على سبيل المثال، بعد إعادة تشغيل الخدمة)، يتم توزيع الاتصالات مع تأخيرات 500 مللي ثانية بين كل ربط لتجنب إغراق الشبكة
- **بدء مرن:** إذا كان الناقل غير متاح عند بدء الجسر، يبدأ الجسر بنجاح ويحاول إعادة الاتصال في الخلفية

استفسار الرابط (Keepalive)

بشكل دوري للتحقق من أن الاتصالات نشطة `enquire_link` SMPP PDUs يرسل الجسر:

- يمكن تكوينها لكل ربط عبر **الفترة الافتراضية**: 60 ثانية (`enquire_link_interval`)
- (غير موصى به) `enquire_link_interval: 0` **تعطيل**: تعيين
- يعتبر الاتصال `enquire_link` **كشف الفشل**: إذا توقف النظير البعيد عن الاستجابة لـ `enquire_link`، يبدأ إعادة الاتصال

Prometheus `smpp_enquire_link_sent_total` راقب صحة استفسار الرابط عبر مقاييس `smpp_enquire_link_received_total` وتشير الفجوة المتزايدة بين المرسل والمستلمة. إلى مشاكل في الاتصال.

TPS تحديد معدل

باستخدام نافذة منزلقة لكل ثانية `tps_limit` يفرض كل ربط حد:

- يتم حساب الرسائل ضمن كل نافذة مدتها 1 ثانية
- عند الوصول إلى الحد، يتوقف عامل الطابور حتى الثانية التالية
- يمكن أن يكون الحد الأقصى 100 رسالة قيد الانتظار (في انتظار الاستجابة) لكل ربط في أي وقت
- يتم إعادة تعيين النافذة تلقائيًا في بداية كل ثانية جديدة

إذا كنت ترى انخفاضًا في الإنتاجية، تحقق من أن:

- مرتفعًا بما يكفي لحركتك `tps_limit` تم تعيين
- منخفضة بما يكفي للحفاظ على تغذية الأنابيب `queue_check_frequency`
- يستجيب الناقل للرسائل بسرعة (الاستجابات البطيئة تقلل من الإنتاجية الفعالة).

إدارة تدفق الرسائل

فحص طابور الرسائل

الغرض: مراقبة الرسائل المعلقة

الخطوات:

1. الوصول إلى الطابور:

- Queue انتقل إلى: علامة التبويب
- عرض قائمة الرسائل المعلقة

2. تحقق من تفاصيل الرسالة:

- انقر على صف الرسالة
- راجع:
 - رقم الوجهة
 - نص الرسالة
 - المستهدف SMSC (dest_smsc)
 - محاولات التسليم
 - الحالة

3. البحث عن رسالة معينة:

- استخدم فلتر البحث
- SMSC تصفية حسب الوجهة، المحتوى، أو

استكشاف الأخطاء في الرسائل العالقة

الأعراض: الرسائل لا يتم تسليمها

الخطوات:

1. تحقق من حالة الاتصال:

- الحالة الحية → SMPP: انتقل إلى
- تحقق من أن الاتصال المستهدف متصل
- إذا كان مفصولاً، انظر إعادة الاتصال

2. تحقق من تفاصيل الرسالة:

- Queue انتقل إلى: علامة التبويب
- ابحث عن الرسالة العالقة
- يتطابق مع اسم الاتصال `dest_smsc` تحقق من أن حقل
- (جدولة إعادة المحاولة) `deliver_after` تحقق من طابع

3. تحقق من محاولات التسليم:

- محاولات عالية = فشل متكرر
- تحقق من السجلات لرسائل الخطأ
- قد تشير إلى تنسيق غير صالح أو رفض من الناقل

4. التدخل اليدوي (إذا لزم الأمر):

- اتصل بالناقل للتحقق من المشكلة
- قد تحتاج إلى إلغاء الرسالة وإعادة تقديمها
- تحقق مع الفريق الخلفي لمشاكل الطابور

استكشاف أخطاء الاتصال

إعادة الاتصال برابط

الأعراض: الاتصال يظهر "غير متصل" (باللون الأحمر)

الخطوات:

1. تحقق من الاتصال الشبكي:

```
ping -c 3 carrier-smpp-server.com  
telnet carrier-smpp-server.com 2775
```

2. تحقق من السجلات للأخطاء:

- Logs انتقل إلى: علامة التبويب
- فلتر: مستوى الخطأ
- ابحث عن فشل المصادقة، انتهاء مهلة الشبكة

3. تحقق من بيانات الاعتماد:

- الأقران العملاء/الأقران الخادم → SMPP: انتقل إلى
- وكلمة المرور صحيحة `system_id` تحقق من أن
- اتصل بالناقل إذا لم تكن متأكدًا

4. إعادة الاتصال يدويًا:

- الحالة الحية → SMPP: انتقل إلى
- ابحث عن الربط المفصول
- انقر على زر "إعادة الاتصال"
- انتظر 10-30 ثانية
- "تحقق مما إذا كانت الحالة تتغير إلى "متصل"

5. إذا فشلت إعادة الاتصال:

- تحقق من قواعد جدار الحماية

- تحقق من أن خادم الناقل يعمل
- اتصل بدعم الناقل
- انظر [TROUBLESHOOTING.md](#)

التعامل مع فشل المصادقة

الأعراض: فشل الربط المتكرر في السجلات

الأسباب:

- اسم المستخدم/كلمة المرور غير صحيحة
- غير موجود في القائمة البيضاء لدى الناقل IP
- الحساب معلق/منتهي

الخطوات:

1. تحقق من بيانات الاعتماد:

- الأقران العملاء → SMPP: انتقل إلى
- وكلمة المرور `system_id` تحقق مرة أخرى من
- تأكد مع الناقل

2. IP تحقق من قائمة البيضاء لـ:

- للجسر مع الناقل IP تأكد من عنوان
- IP اطلب من الناقل التحقق من القائمة البيضاء لـ

3. تحقق من حالة الحساب:

- تحقق من أن الحساب نشط
- تحقق من العقود المنتهية
- اتصل بفوترة الناقل

4. تحديث التكوين:

-   تغييرت بيانات الاعتماد، قم بتحديثها في واجهة الويب
- انقر على "إعادة الاتصال" لإعادة المحاولة مع بيانات الاعتماد الجديدة

المراقبة والتنبيه

Prometheus التحقق من مقاييس

تحقق سريع:

```
curl http://localhost:4000/metrics | grep smpp_connection_status
```

النتائج المتوقعة:

```
smpp_connection_status{bind_name="vodafone_uk",...} 1  
smpp_connection_status{bind_name="att_us",...} 1
```

يجب أن تكون جميع القيم 1 (متصلة).

الاستجابة للتنبيهات

تنبيه الاتصال غير متصل:

1. الحالة الحية → SMPP → تحقق من واجهة الويب
2. حاول إعادة الاتصال يدويًا
3. تحقق من السجلات للأخطاء
4. اتصل بالناقل إذا كانت الانقطاع لفترة طويلة
5. انظر [TROUBLESHOOTING.md](#)

تنبيه معدل الفشل العالي:

1. تحقق من السجلات لأنماط الأخطاء
2. راجع التغييرات الأخيرة في التكوين
3. اتصل بالناقل حول الرفض
4. تحقق من الامتثال لتنسيق الرسالة

تنبيه عدم وجود حركة مرور:

1. تحقق من أن الطابور الخلفي يحتوي على رسائل
2. صحيح `dest_smsc` تحقق من أن توجيهه

- ليست صارمة جدًا TPS تحقق من أن حدود 3.
 - راجع إعداد `queue_check_frequency` 4.
-

إجراءات الصيانة

الصيانة الروتينية

قم بإجراء الصيانة الشهرية

1. مراجعة المقاييس:

- تحليل اتجاهات حجم الرسائل
- تحقق من معدلات النجاح في التسليم
- تحديد فرص التحسين

2. تحديث الوثائق:

- وثق أي تغييرات في التكوين
- تحديث معلومات الاتصال
- ملاحظة نوافذ صيانة الناقل

3. تدقيق بيانات الاعتماد:

- SMPP مراجعة جميع كلمات مرور
- تخطيط لتدوير بيانات الاعتماد
- محدثة IP التحقق من أن قوائم البيضاء لـ

4. تخطيط السعة:

- مراجعة معدلات الرسائل القصوى
- TPS تحقق من حدود
- التخطيط للنمو

إعادة تشغيل الخدمة

عند الحاجة:

- بعد تغييرات ملف التكوين
- بعد تحديثات النظام
- أثناء استكشاف الأخطاء

الخطوات:

```
# تحقق من الحالة الحالية
sudo systemctl status omnimessage-smpp

# إعادة تشغيل الخدمة
sudo systemctl restart omnimessage-smpp

# تحقق من إعادة التشغيل
sudo systemctl status omnimessage-smpp

# تحقق من السجلات
sudo journalctl -u omnimessage-smpp -n 50
```

تحقق عبر واجهة الويب:

1. الوصول إلى لوحة التحكم (قد يستغرق 30-60 ثانية للظهور على الإنترنت).
2. الحالة الحية: SMPP → انتقل إلى
3. انتظر حتى يتم إنشاء جميع الاتصالات (1-2 دقيقة).
4. تحقق من السجلات للأخطاء.

النسخ الاحتياطي للتكوين

قم بعمل نسخ احتياطي للملفات الحرجة قبل التغييرات:

```
# نسخ احتياطي للتكوين
sudo cp /opt/omnimessage-smpp/config/runtime.exs \
/opt/omnimessage-smpp/config/runtime.exs.backup.$(date +%Y%m%d)

# نسخ احتياطي للشهادات
sudo tar -czf /tmp/smpp-certs-$(date +%Y%m%d).tar.gz \
/opt/omnimessage-smpp/priv/cert/
```

استعادة إذا لزم الأمر:

```
# استعادة التكوين
sudo cp /opt/omnimessage-smpp/config/runtime.exs.backup.YYYYMMDD \
/opt/omnimessage-smpp/config/runtime.exs

# إعادة تشغيل الخدمة
sudo systemctl restart omnimessage-smpp
```

إجراءات الطوارئ

انقطاع الخدمة الكامل

الخطوات:

1. تحقق من حالة الخدمة:

```
sudo systemctl status omnimessage-smpp
```

2. إذا توقفت الخدمة، ابدأها:

```
sudo systemctl start omnimessage-smpp
```

3. تحقق من السجلات لمعرفة سبب التعطل:

```
sudo journalctl -u omnimessage-smpp -n 100
```

4. إذا لم تبدأ:

- تحقق من أخطاء بناء الجملة في التكوين
- SSL تحقق من وجود شهادات
- تحقق من مساحة القرص: `df -h`
- تحقق من الذاكرة: `free -h`

5. اتصل بالدعم إذا لم يتم حل المشكلة.

طلبات الناقل لإيقاف الطوارئ

الخطوات:

1. قطع الاتصال على الفور:

- الحالة الحية → SMPP: انتقل إلى
- ابحث عن الاتصال المتأثر
- "انقر على "قطع الاتصال"

2. وثق السبب:

- لاحظ اسم الناقل
- سجل الوقت والسبب
- احفظ المراسلات

3. تحقق من المشكلة:

- تحقق من أنماط الرسائل الأخيرة
- راجع السجلات للأخطاء
- حدد السبب الجذري

4. تنسيق الحل:

- العمل مع الناقل
- تنفيذ الإصلاحات
- اختبار قبل إعادة الاتصال

ارتفاع حجم الرسائل

الأعراض: حركة مرور رسائل عالية بشكل غير متوقع

الخطوات:

1. TPS تحقق من حدود:

- الحالة الحية → SMPP: انتقل إلى
- تحقق من أن الاتصالات لا تعاني من التقييد
- مؤقتًا TPS قد تحتاج إلى زيادة حدود

2. راقب استقرار الناقل:

- راقب الانقطاعات
- تحقق من معدلات النجاح في التسليم

3. تنسيق مع الجزء الخلفي:

- تحقق من أن مصدر الرسائل شرعي
- قد تحتاج إلى تنفيذ تحديد المعدل في الأعلى

4. التوسع إذا لزم الأمر:

- قد تحتاج إلى حالات جسر إضافية
- اتصل بالدعم للحصول على نصائح حول التوسع

أفضل الممارسات

قائمة التحقق اليومية

- ☐ متصلة SMPP تحقق من أن جميع اتصالات
- ☐ مراجعة سجلات الأخطاء لأي مشاكل
- ☐ مراقبة طابور الرسائل للتراكم
- ☐ Prometheus/Grafana تحقق من لوحات
- ☐ %تحقق من معدلات نجاح التسليم < 98

المهام الأسبوعية

- ☐ مراجعة اتجاهات المقاييس
- ☐ تحقق من الأنماط الشاذة
- ☐ اختبار إجراءات استعادة الكوارث
- ☐ تحديث الوثائق حسب الحاجة
- ☐ مراجعة والاعتراف بالتنبيهات

المهام الشهرية

- ☐ تدقيق بيانات الاعتماد
 - ☐ مراجعة تخطيط السعة
 - ☐ تحديث جهات الاتصال للناقل
 - ☐ TPS مراجعة وتحسين إعدادات
 - ☐ نسخ احتياطي لملفات التكوين
-

الوثائق ذات الصلة

- **CONFIGURATION.md** - تكوين الاتصالات والإعدادات
 - **SOURCE_ADDRESS_WHITELIST.md** - تقييد العناوين الأصلية لكل نظير خادم
 - **MONITORING.md** - إعداد تنبيهات Prometheus
 - **TROUBLESHOOTING.md** - حل المشكلات الشائعة
 - **README.md** - نظرة عامة على النظام
-

