

مرجع التكوين

دليل كامل لجميع معلمات التكوين

نظرة عامة على المعمارية

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

1. من شركات النقل والعملاء SMPP PDUs **استقبال**
2. REST API عبر OmniMessage **ترجمتها** إلى تنسيق
3. للرسائل لإرسالها OmniMessage **التحقق** من
4. إلى شركات النقل SMPP PDUs **إرسال**
5. OmniMessage **الإبلاغ** عن حالة التسليم مرة أخرى إلى

جميعها - (Diameter, MAP, IMS) OmniMessage هذا هو نفسه كيف تعمل الواجهات الأخرى لـ OmniMessage Core مترجمات بروتوكول بدون 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. يستخ **م** ملف التكوين بناء جملة

```
import Config

# الإعدادات العالمية
config :omnimessage_smpp,
  setting_name: value

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

الإعدادات العالمية

API_BASE_URL

عنوان URL لمنصة OmniMessage Core

```
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 API

- للمعالجة OmniMessage المستلمة إلى SMPP **إرسال الرسائل**: إرسال رسائل
- SMPP **استرجاع الرسائل**: التحقق من الرسائل الموجهة لشركات النقل
- **الإبلاغ 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 الرسائل والتحقق من التنسيق ✓
- قرارات التوجيه (أي شركة نقل يجب استخدامها) ✓
- تحديد المعدل والحد من السرعة ✓
- التحقق من الأرقام ✓
- تخزين الرسائل واستمراريتها ✓
- منطق إعادة التسليم ✓
- 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 تتمتع البوابة بالوصول الشبكي إلى
- (قم بتكوين `verify_ssl_peer` في الإنتاج HTTPS استخدم
- على المنفذ المحدد HTTPS يجب أن يسمح جدار الحماية بالاتصالات الخارجية عبر

SMPP_POLL_INTERVAL

تكرار التحقق من قائمة الانتظار (بالميلي ثانية)

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

المعلمة	النوع	مطلوب	الافتراضي
smpp_poll_interval	عدد صحيح	لا	100

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

إرشادات:

- **حجم عالي (>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

عند الاتصال بواجهة برمجة التطبيقات الخلفية 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	ال نوع	مطلوب	الافتراضي
smsc_name	سلسلة	لا	"smpp_gateway"

الغرض: يحدد هذه الحالة من البوابة في واجهة قائمة الانتظار للرسائل.

متغير البيئة: `SMSC_NAME`

SMPP تكوين ربط عميل

تتصل بخوادم (عميل) **ESME** **ربطات العميل** هي اتصالات خارجية حيث تعمل البوابة كـ لشركات النقل. في هذا الوضع، تقوم البوابة ببدء الاتصال لإرسال واستقبال الرسائل عبر **SMSC** شركات النقل الخارجية.

مثال كامل لربط العميل

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

  # وضع الاتصال
  mode: :client,

  # نوع ربط SMPP
  bind_type: :transceiver,

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

  # بيانات الاعتماد الخاصة بالمصادقة
  system_id: "your_username",
  password: "your_password",

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

  # تحديد المعدل
  tps_limit: 100,

  # تكرار التحقق من قائمة الانتظار
  queue_check_frequency: 1000,

  # فترة إبقاء الاتصال (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 الربطات
- استخدم أسماء وصفية (شركة النقل، 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 خارجي حيث تعمل البوابة كـ

.للاتصالات الخارجية :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 النقل نوعًا محددًا :transceiver **التوصية:** استخدم

host

لشركة النقل SMPP لخادم IP اسم المضيف أو

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

لشركة النقل SMPP **الغرض:** عنوان خادم

أمثلة:

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

port

SMPP منفذ خادم

النطاق	الافتراضي	مطلوب	النوع
1-65535	2775	نعم	عدد  حيز

SMPP لاتصال TCP **الغرض**: منفذ

المنفذ القياسي: 2775

أمثلة:

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

system_id

اسم المستخدم للمصادقة

النوع	مطلوب	مثال
سلسلة	نعم	"company_user"

الغرض: اسم المستخدم المقدم من شركة النقل للمصادقة

الأمان: احمِ هذه البيانات - مخزنة في ملف التكوين

password

كلمة مرور المصادقة

النوع	مطلوب	مثال
سلسلة	نعم	"secret_password"

الغرض: كلمة المرور المقدمة من شركة النقل للمصادقة

الأمان:

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

tps_limit

حدود 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

إرشادات:

- تعيين إلى 70-80% من الحد الأقصى لشركة النقل
- يمنع تحديد السرعة/قطع الاتصال
- يسمح بمساحة للتسليم

أمثلة:

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

الحساب:

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

queue_check_frequency

فترة التحقق من قائمة الرسائل (بالميلي ثانية)

النطاق	الافتراضي	مطلوب	النوع
100-10000	1000	نعم	عدد صحيح

الغرض: كم مرة يجب التحقق من الخلفية للحصول على رسائل جديدة لإرسالها

إرشادات:

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

التوازنات:

- 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

(بالتواني) SMPP فترة إبقاء

النطاق	الافتراضي	مطلوب	النوع
0-3600	60	لا	عدد صحيح

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

إرشادات:

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

أمثلة:

enquire_link_interval: 60 # قياسي (1 دقيقة)
enquire_link_interval: 30 # إبقاء نشط بشكل عدواني
enquire_link_interval: 0 # معطل

system_type

SMPP معرف نوع نظام

النوع	مطلوب	الافتراضي	مثال
سلسلة	لا	" "	"OTP"

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

addr_ton

نوع عنوان الرقم

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	لا	0	0-6

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

القيم الشائعة:

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

تعيين حسب متطلبات شركة النقل.

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

.تعيين حسب متطلبات شركة النقل

address_range

نطاق العنوان للربط

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

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

enabled

حالة تمكين النظيف

الافتراضي	مطلوب	النوع
true	لا	منطقي

الغرض: يتحكم في ما إذا كان هذا النظيف نشطًا. يتم الاحتفاظ بالنظائر المعطلة في التكوين ولكن لا تقيم اتصالات. مفيد لإيقاف الاتصال مؤقتًا دون حذف تكوينه.

cache_enabled

تمكين تخزين الرسائل محليًا

النوع	مطلوب	الافتراضي
منطقي	لا	false

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

cache_max_size

الحد الأقصى للرسائل المخزنة

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	لا	10000	1-1000000

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

cache_retry_interval

فترة إعادة المحاولة الأساسية (بالثواني)

النوع	مطلوب	الافتراضي
عدد صحيح	لا	60

الغرض: الفترة الأساسية بالثواني قبل إعادة محاولة تسليم رسالة مخزنة. يتم دمجها مع التراجع الأسّي (إعادة المحاولة 0: 60 ثانية، إعادة المحاولة 1: 120 ثانية، إعادة المحاولة 2: 240 ثانية، true. هي cache_enabled إلخ). ينطبق فقط عندما تكون.

مثال واجهة الويب:

SMPP تكوين ربط خادم

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

مثال كامل لربط 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 التحقق من قائمة الانتظار
    queue_check_frequency: 1000,

    # فترة إبقاء الاتصال (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 العم $\diamond\diamond$ ل 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 بأمان مع الشريك

allowed_bind_types

أنواع الجلسات المسموح بها

الافتراضي	مطلوب	النوع
-	نعم	قائمة من الذرات

العرض: يقيد 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 صيغة IPs	[]	نعم	قائمة من السلاسل

المعروفة IPs **العرض:** الأمان - السماح فقط بالاتصالات من

التنسيقات:

- فردية: "192.168.1.100" (بشكل تلقائي 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: []

# IP فردي
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 IPs تلقائي لـ IP فردي - /32
- عنوان (مثلاً 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

النوع	مطلوب	الافتراضي	التنسيق
قائمة من السلاسل	لا	[]	wildcard أنماط دقيقة أو نمط

الغرض: يقيد أي عناوين مصدر (معرفات المرسل) يمكن للعملاء المتصلين استخدامها عند تقديم الرسائل. يسمح القائمة الفارغة بجميع العناوين.

أنواع الأنماط:

- "MyBrand" يتطابق فقط مع "MyBrand": تطابق دقيق
- "614*" wildcard: يتطابق مع أي عنوان يبدأ بـ "614"

أمثلة:

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

# عناوين محددة فقط
source_address_whitelist: ["MyBrand", "AlertService"]

# wildcard تطابق نمط
source_address_whitelist: ["614*", "+61*"]

# مختلط
source_address_whitelist: ["MyBrand", "614*", "+61400000001"]
```

راجع `ESME_RINVSRCADR` تُرفض الرسائل التي تحتوي على عناوين مصدر غير مسموح بها مع [SOURCE_ADDRESS_WHITELIST.md](#) للحصول على التفاصيل الكاملة.

tps_limit

حدود الرسائل في الثانية

الخارجي للعملاء المتصلين deliver_sm لربط العميل - يتحكم في معدل `tps_limit` نفس

queue_check_frequency

فترة التحقق من قائمة الانتظار

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

enquire_link_interval

(بالثواني) SMPP فترة إبقاء

PDUs لربط العميل. يتحكم في مدى تكرار إرسال الخادم لـ `enquire_link_interval` نفس للعملاء المتصلين للتحقق من أنهم لا يزالون نشطين `enquire_link`.

enabled

حالة تمكين النظير

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

cache_enabled

تمكين تخزين الرسائل محليًا

`cache_enabled` نفس [MESSAGE_CACHE.md](#) لربط العميل. راجع

cache_max_size

الحد الأقصى للرسائل المخزنة

`cache_max_size` نفس لربط العميل.

cache_retry_interval

فترة إعادة المحاولة الأساسية (بالثواني)

`cache_retry_interval` نفس لربط العميل.

مثال واجهة الويب:

تكوين الاستماع للخادم

.عند تكوين ربطات الخادم، تستمع البوابة للاتصالات الواردة

مثال كامل للاستماع

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

معلومات الاستماع

host

للربط به 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 عبر

القياسي: 2775

max_connections

الحد الأقصى للاتصالات المتزامنة

النطاق	الافتراضي	مطلوب	النوع
1-10000	100	لا	عدد صحيح

الغرض: يحدد العدد الإجمالي للاتصالات المتزامنة للعملاء.

إرشادات:

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

أمثلة تكوين كاملة

المثال 1: اتصال شركة نقل واحدة

```
import Config

config :omnimessage_smpp,
  api_base_url: "https://smcsc.companv.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: شركات نقل متعددة

```
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 ربطات خادم

```
import Config

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

# اتصالات خارجية
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
}
```

التحقق من التكوين

بعد تحرير التكوين، تحقق قبل إعادة التشغيل:

تحقق من الصياغة

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

إذا كانت الصياغة غير صحيحة، ستري خطأ. قم بإصلاحه قبل إعادة التشغيل.

اختبار التكوين

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

مرتين للخروج **Ctrl+C** اضغط على

متغيرات البيئية

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

متغير البيئة	مفتاح التكوين	راسمي
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 ممارسات الأمان

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، الأرقام، الرموز
- فريدة لكل اتصال

3. البضاء IP استخدم قوائم:

- لربط الخادم `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 بانتظام:

- قم بتغيير كلمات المرور كل ثلاثة أشهر
- تنسيق مع شركات النقل/الشركاء

الخطوات التالية

- لتكوين القياسات [MONITORING.md](#) راجع
 - لإدارة الاتصالات [USAGE.md](#) اقرأ
 - للمشاكل الشائعة [TROUBLESHOOTING.md](#) انظر
 - للحصول على نظرة عامة [README.md](#) عد إلى
-

المعجم

المصطلحات والتعريفات

A

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

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

B

Backend لاسترجاع وتخزين الرسائل SMPP نظام قائمة الرسائل الذي يتصل به بوابة.

Bind بين نظامين. يمكن أن يكون مرسلاً أو مستقبلاً أو جهاز إرسال واستقبال SMPP اتصال.

Bind Type نوع جلسة SMPP:

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

Bind Failure عادةً بسبب بيانات اعتماد غير صحيحة أو SMPP، عندما تفشل محاولة مصادقة IP. قيود على عنوان.

C

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

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

Connection Status SMPP الحالة الحالية لارتباط:

- **Connected:** نشط وقابل للتشغيل
- **Disconnected:** غير متصل
- **Reconnecting:** محاولة إعادة الاتصال

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

D

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

لتسليم رسالة (الخادم) SMSC يتم إرسالها بواسطة SMPP وحدة بيانات بروتوكول **Deliver_SM** متصل (العميل). تستخدمها الاتصالات الخادمة لدفع الرسائل إلى الشركاء المتصلين ESME إلى

عندما لا يمكن تسليم رسالة، مما يد  عليه استجابة خطأ من مشغل الاتصالات.

Delivery Receipt (DLR) تأكيد من مشغل الاتصالات حول حالة تسليم الرسالة

يجب أن يتعامل مع الرسالة SMPP حقل في قائمة الرسائل يشير إلى أي اتصال **dest_smsc**

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**

التطبيق العميل الذي، SMPP في مصطلحات **(كيان الرسائل القصيرة الخارجي) ESME** ESME لإرسال أو استلام الرسائل. عندما تعمل البوابة في **وضع العميل**، تعمل كـ SMSC يتصل بـ ESMEs لمشغل الاتصالات. عندما تعمل في **وضع الخادم**، تقبل الاتصالات من SMSCs تتصل بـ الخارجية.

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

F

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

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، فإن التسجيل Core. عن توجيه الرسائل إليها OmniMessage ينتهي بعد 90 ثانية ويتوقف.

G

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

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

Grafana في لوحات المعلومات Prometheus أداة تصور شائعة لعرض مقاييس.

GSM-7 ترميز أحرف قياسي مكون من 7 بتات للرسائل القصيرة، يدعم حتى 160 حرفًا لكل رسالة.

H

HTTP/HTTPS هو النسخة المشفرة HTTPS. بروتوكولات تستخدم للتواصل عبر الويب.

I

IP Whitelist المسموح بها التي يمكن أن تتصل بالبوابة (ميزة أمان) IP قائمة بعناوين.

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

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 مفتاح-قيمة مرتبطة بالمقاييس للتعريف، Prometheus في **Label** (`bind_name="vodafone_uk"`).

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

M

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

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

رسائل تُرسل من الهواتف المحمولة إلى **(الرسائل المرسلة من الهاتف المحمول) MO** البوابة (واردة).

رسائل تُرسل من البوابة إلى الهواتف **(الرسائل المرسلة إلى الهاتف المحمول) MT** المحمولة (صادرة).

تنسيق قياسي لأرقام الهواتف **(رقم دليل المشترك الدولي لمحطة المحمول) MSISDN** المحمولة.

N

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

O

Outbound رسائل تتدفق من البوابة إلى الشبكات المحمولة.

Inbound رسائل تتدفق من الشبكات المحمولة إلى البوابة.

P

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

Prometheus نظام مراقبة مفتوح المصدر يجمع ويخزن مقاييس السلاسل الزمنية.

Q

Queue قائمة الرسائل التي تنتظر المعالجة أو الإرسال.

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

Queue Worker SMPP مكون يسترجع الرسائل من القائمة ويرسلها عبر.

R

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

Receiver (deliver_sm) الذي يستقبل الرسائل فقط SMPP نوع ارت❖❖ اط.

Reconnect مفصول SMPP إعادة إنشاء اتصال.

Retry محاولة إرسال رسالة فاشلة مرة أخرى، عادةً مع استخدام التراجع الأسّي.

S

Sequence Number ضمن جلسة. يُستخدم PDU SMPP معرف رقمي فريد يُخصص لكل **submit_sm** مع استجاباتها **submit_sm_resp** لمطابقة الطلبات مع استجاباتها.

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

Session نشط بين نظامين SMPP اتصال.

حقل في قائمة الرسائل يشير إلى أي ارتباط خادِم يجب أن يسلم الرسالة إلى **source_smsc** **deliver_sm** عملائه المتصلين عبر.

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

المكون الخادِم 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 الخادِم**، تعمل كـ.

SSL/TLS بروتوكولات التشفير للتواصل الآمن.

Submit_SM لتقديم رسالة للتسليم PDU SMPP.

Submit_SM_Resp تشير إلى النجاح أو الفشل، **submit_sm** لـ 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 للحد الأقصى من الرسائل 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، عادةً ما يُقاس بالرسائل في الثانية

U

ترميز أحرف يونيكود مكون من 16 بت للرسائل القصيرة، يدعم حتى 70 حرفًا لكل UCS-2 رسالة.

Uptime المدة التي كان فيها اتصال أو خدمة تعمل بشكل مستمر

V

Validity Period حد زمني لمحاولة تسليم الرسالة قبل انتهاء صلاحيتها

W

Web Dashboard واجهة مستخدم قائمة على المتصفح لمراقبة وإدارة البوابة

Whitelist المسموح بها وقائمة عناوين المصدر المسموح بها IP انظر قائمة عناوين

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 تصنيف
DLR	إيصال التسليم
ESME	كيان الرسائل القصيرة الخارجي
GSM	النظام العالمي للاتصالات المحمولة
HTTP	بروتوكول نقل النص الفائق
HTTPS	بروتوكول نقل النص الفائق الآمن
IP	بروتوكول الإنترنت
ISDN	شبكة الخدمات الرقمية المتكاملة
KPI	مؤشر الأداء الرئيسي
MO	الرسائل المرسلة من الهاتف المحمول
MSISDN	رقم دليل المشترك الدولي لمحطة المحمول
MT	الرسائل المرسلة 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

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

الميزات

- أثناء انقطاع واجهة SMPP **قبول الرسائل بشكل مرن** - الاستمرار في قبول رسائل برمجة التطبيقات
- لضمان المتانة عبر إعادة `disc_copies` مع Mnesia **تخزين دائم** - يستخدم التشغيل
- **إعادة المحاولة التلقائية** - يقوم العمال في الخلفية بمحاولة 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 الفيض** - **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
- **مقاييس بروميثيوس** - تصدير كامل للقياسات للمراقبة والتنبيه

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 (lib/sms_c/smpp/message_cache.ex)

- منطق التخزين الأساسي
- معالجة الفيضانات
- و❖❖ لعمال LiveView وظائف الاستعلام لـ

2. CacheFlushWorker (lib/sms_c/smpp/cache_flush_worker.ex)

- 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 حسب
- يبقى بعد إعادة تشغيل التطبيق

التكوين

الإعدادات العالمية

قم بتحرير `config/runtime.exs`:

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

  # الحد الأقصى لمحاولات إعادة المحاولة قبل وضع علامة كفشل 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 :omnimessage_smpp, :binds, [
  %{
    name: "my_smpp_bind",
    mode: :server,
    system_id: "username",
    password: "password",

    # إعدادات 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 # الحد الأدنى لفترة إعادة المحاولة
    بالثواني (افتراضي: 60)
  }
]
```

متغيرات البيئة

# إعدادات التخزين المؤقت العالمية	
CACHE_FLUSH_INTERVAL=10000	# فترة استعلام التخزين
المؤقت (بالملي 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 المخزن - جميع الرسائل الموجودة حاليًا في الذاكرة المؤقتة
- انتظار التسليم - ال❖❖ رسائل التي تنتظر إعادة المحاولة
- الفشل الدائم - الرسائل التي تجاوزت الحد الأقصى لإعادة المحاولات

جدول لكل ارتباط:

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

مقاييس بروميثيوس

```
# الحجم الحالي للذاكرة المؤقتة 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 المحذوفة)
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 "الأقران العملاء" أو "الأقران الخوادم"
3. تحرير الارتباط

"تديل خاة "تمكين التخزين المؤقت 4.

حفظ التغيرات 5.

Ex عبر وحدة التحكم

```
# 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 إعادة 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` العرض: زيادة مقياس

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 الفاشلة القديمة يدويًا
- تحقق مما إذا كانت فترة الاستعلام بطيئة جدًا

الرسائل لا يتم تسليمها

`pending`: العرض: 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 الاتصال الشبكي

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 غير قيد التشغيل

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

4. تم تعطيل التخزين المؤقت

- في تكوين الارتباط `cache_enabled: true` تحقق من

عدد محاولات إعادة المحاولة العالية

عالية `retry_count`: العرض: العديد من الرسائل مع قيم

التحقيق:


```

# العثور على الرسائل ذات عدد محاولات إعادة المحاولة 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

العرض: امتلاء مساحة القرص

Mnesia: تحقق من دليل

```

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

```

تنظيف:

1. مسح الرسائل الفاشلة القديمة (انظر التدخلات اليدوية أعلاه).
2. تقليل `cache_max_size` لكل ارتباط
3. بشكل صحيح FIFO ضمان إخلاء) تمكين الفيضانات في الذاكرة المؤقتة.

اعتبارات الأداء

استخدام الذاكرة

- كل رسالة مخزنة تستخدم 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

- يقوم عمال الإخلاء بالاستعلام كل 10 ثوانٍ بشكل افتراضي (يمكن تكوينه)
- معالجة دفعات (100 رسالة لكل دورة) تقلل من الحمل
- التسليم المتزامن (حد أقصى 10 مكالمات واجهة برمجة التطبيقات المتزامنة لكل عامل)

إدخال/إخراج القرص

- يكتب إلى القرص في كل معاملة `disc_copies`
- ضع في اعتبارك ، (>1000 msg/sec) لسرعة نقل عالية 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 سليمة
3. يتم إعادة تشغيل عمال الإخلاء ويستمررون في المعالجة

ترحيل قاعدة البيانات

:عند الترقية من إصدار بدون دعم التخزين المؤقت

1. يضيف الترحيل تلقائيًا حقول التخزين المؤقت إلى الارتباطات 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 انقطاع واجهة برمجة التطبيقات

1. تتراكم الرسائل في الذاكرة المؤقتة أثناء الانقطاع
2. عند استعادة واجهة برمجة التطبيقات، يقوم عمال الإخلاء بتسليم الرسائل تلقائيًا
3. (FIFO) يتم تسليم الرسائل الأقدم أولاً
4. تمنع زيادة زمن الانتظار بشكل أسي من تحميل واجهة برمجة التطبيقات أثناء الاسترداد

أفضل الممارسات

1. تمكين التخزين المؤقت بشكل افتراضي - يمنع فقدان الرسائل أثناء الانقطاعات
2. `cache_permanent_failures_total` مراقبة المقاييس - إعداد تنبيهات على `cache_overflow_total`
3. بناءً على مدة الانقطاع `cache_max_size` تحديد الحجم بشكل مناسب - تعيين المتوقعة
4. مراجعة الرسائل الفاشلة - تحقق 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 استرداد واجهة برمجة التطبيقات
7. **استخدام تخزين دائم** - الاحتفاظ بـ `mnesia_storage_type: disc_copies` في الإنتاج

انظر أيضًا

- مرجع التكوين
- المراقبة والمقاييس
- استكشاف الأخطاء وإصلاحها

دليل المراقبة والقياسات

SMPP مرجع كامل لمراقبة بوابة

نظرة عامة

لمراقبة صحة الاتصال، ومعدل الرسائل، Prometheus يعرض القياسات بتنسيق SMPP تقوم بوابة وأداء النظام.

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

- صحة على مستوى البروتوكول - **SMPP قياسات بوابة**
- 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

وتحتوي على تسميات للتعريف `smpp_` تبدأ جميع القياسات بـ

قياسات الترخيص

omnmessage_smpp_license_status

النوع: Gauge

الوصف: حالة الترخيص الحالية

القيم:

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

التسميات: لا شيء

مثال:

```
omnmessage_smpp_license_status 1
```

الاستخدام:

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

اسم المنتج: omnmessage_smpp

ملاحظات:

- تتوقف البوابة عن (`license_status == 0`) عندما يكون الترخيص غير صالح معالجة قوائم الانتظار الصادرة
- متصلة وتقبل طلبات الربط (كل 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 ("عميل" أو "خادم")
- `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 تكون القيمة 0 (غير متصل)
- تتبع نسبة وقت تشغيل الاتصال
- مراقبة تكرار إعادة الاتصال

عدادات الرسائل

smpp_messages_sent_total

النوع: Counter

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

التسميات: نفس تسميات حالة الاتصال

مثال:

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

الاستخدام:

- حساب معدل الرسائل (رسائل/ثانية)
- تتبع الحجم اليومي/الشهري
- مقارنة الإنتاج الفعلي مقابل المتوقع

smpp_messages_received_total

النوع: Counter

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

التسميات: نفس تسميات 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 الهواتف المحمولة
- تنبيه على تغييرات غير متوقعة في الحجم

قياسات التسليم

smpp_delivery_failures_total

النوع: Counter

الوصف: العدد الإجمالي لفشل تسليم الرسائل

الوحدة: حالات الفشل

التسميات: نفس تسميات 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 الإشكالية

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 مشكلات الاعتماد
- تتبع مشكلات الاتصال مع الناقل

قياسات أحداث الاتصال

smpp_connection_attempts_total

النوع: Counter

الوصف: العدد الإجمالي لمحاولات الاتصال

الوحدة: محاولات

مثال:

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

الاستخدام:

- تتبع تقلبات الاتصال
- مراقبة تكرار إعادة الاتصال

smpp_disconnection_total

النوع: Counter

الوصف: العدد الإجمالي للفصل

الوحدة: حالات الفصل

مثال:

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

الاستخدام:

- تنبيه على الفصول المتكررة
- تحديد مشكلات الشبكة
- تتبع استقرار الاتصال

قياسات استعلام الرابط

smpp_enquire_link_sent_total

النوع: Counter

الخاصة باستعلام الرابط المرسل للتحقق من حيوية PDUs **الوصف:** العدد الإجمالي لوحدات

الاتصال

الوحدة: PDUs

التسميات: نفس تسميات   آلة الاتصال

مثال:

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

الاستخدام:

- تتبع نشاط الحفاظ على الاتصال
- المقارنة مع المستلم للكشف عن الفشل في اتجاه واحد

smpp_enquire_link_received_total

النوع: Counter

الخاصة باستجابة استعلام الرابط المستلمة من النظير PDUs **الوصف:** العدد الإجمالي لوحدات البعيد

الوحدة: PDUs

التسميات: نفس تسميات حالة الاتصال

مثال:

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

الاستخدام:

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

قياسات وقت التشغيل

smpp_uptime_seconds

النوع: Gauge

الوصف: SMPP بالثواني 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 تكون ذاكرة التخزين المؤقت للرسائل مفعلة على واحد أو أكثر للحصول على تفاصيل تكوين الذاكرة المؤقتة **MESSAGE_CACHE.md** من الرابط. انظر

smpp_cache_size

النوع: Gauge

الوصف: العدد الحالي للرسائل في الذاكرة المؤقتة المحلية لكل ربط

الوحدة: رسائل

التسميات:

- `bind_name` - اسم الاتصال
- `mode` - نوع الاتصال ("عميل" أو "خادم")

مثال:

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

الاستخدام:

- مراقبة استخدام الذاكرة المؤقتة
- تنبيه عند الاقتراب من `cache_max_size`

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: محاولات

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 لحدوث تجاوز الذاكرة المؤقتة حيث تمت إزالة أقدم رسالة لإفساح المجال
الوحدة: أحداث

مثال:

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

الاستخدام:

- تنبيه عند الزيادة (الذاكرة المؤقتة صغيرة جدًا أو انقطاع واجهة برمجة التطبيقات طويل جدًا)

OmniMessage API قياسات صحة

حرجة. OmniMessage API فإن صحة، SMPP، بينما تعرض البوابة نفسها قياسات متعلقة بـ: يجب عليك أيضًا مراقبة

(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)

ابحث عن هذه الأنماط لاكتشاف مشكلات واجهة برمجة التطبيقات

- "api.*connection refused" - لا يمكن الوصول إلى OmniMessage
- "api.*timeout" - لا تستجيب OmniMessage

- "api.*http 503" - OmniMessage مؤقتًا معطلة
 - "api.*parse error" - مشكلة في تنسيق الاستجابة
-

Prometheus تكوين

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 معلومات

لوحات معلومات نموذجية

لوحة حالة الاتصال

الاستعلام:

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

التصور: Stat

العتبات:

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

التصور: Gauge

الوحدة: النسبة المئوية (100-0)

العتبات:

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

لوحة وقت تشغيل الاتصال

الاستعلام:

```
smpp_uptime_seconds{job="omnimessage-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 2 دقائق {{ $labels.bind_name }}."

    # 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: "{{ $labels.bind_name }} لم ترسل أي رسائل لمدة 30 دقيقة"

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

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

# OmniMessage مهلات واجهة برمجة التطبيقات
- alert: OmniMessageAPITimeout
  expr: |
    count(count_over_time({job="omnimessage-smpp"} |=
"api.*timeout"[5m])) > 5
  for: 2m
  labels:
    severity: warning
  annotations:

```

```
summary: "تعاني من مهلات OmniMessage واجهة برمجة تطبيقات"  
description: "تم اكتشاف عدة مهلات في واجهة برمجة  
".بطيئة أو مثقلة OmniMessage التطبيقات. قد تكون
```

```
# لا توجد تدفقات رسائل (مشكلة في 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 اتصال  
OmniMessage"  
    description: "لا توجد رسائل مرسله أو مستلمة لمدة 30  
وحالة OmniMessage دقيقة. تحقق من اتصال واجهة برمجة التطبيقات  
القائمة."
```

قم بتحميل القواعد في `prometheus.yml`:

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

مراقبة لوحة المعلومات على الويب

Prometheus توفر واجهة المستخدم المدمجة مراقبة في الوقت الفعلي دون

الوصول

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

صفحة الحالة الحية

الحالة الحية → SMPP:                                          

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

الاستخدام:

- تحقق سريع من الحالة
- تدخل يدوي
- استكشاف الأخطاء وإصلاحها في الوقت الفعلي

تظهر لوحة المعلومات:

- **إجمالي الربط:** العدد الإجمالي لجميع اتصالات العميل والخادم
 - **ربط العميل:** اتصالات صادرة إلى الناقلين (تظهر العدد المتصل/غير المتصل)
 - **ربط الخادم:** اتصالات واردة من الشركاء (تظهر العدد النشط/المنتظر)
 - **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 المستخدم على الويب

التنقل: علامة التبويب السجلات في واجهة المستخدم على الويب

الميزات:

- بث السجلات في الوقت الفعلي
- تصفية حسب المستوى (تصحيح، معلومات، تحذير، خطأ)
- البحث في السجلات
- إيقاف مؤقت/استئناف
- مسح السجلات

تسمح لك عرض السجلات بـ:

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

- لكل بوابة Grafana بناء لوحات معلومات

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

3. المراجعات المنتظمة

- مراجعة القياسات أسبوعيًا
- تحديد الاتجاهات والأنماط
- التخطيط لتعديلات 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 النهاية إلى النهاية
- تحديد الاختناقات

استكشاف الأخطاء باستخدام القياسات

مشكلات الاتصال

تحقق: `smpp_connection_status`

- القيمة 0 = مراجعة السجلات، التحقق من الشبكة، التحقق 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 الناقل الإشكالي

الإنتاج المنخفض

معدل `smpp_messages_sent_total` تحقق: معدل

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

مشكلات الربط

تحقق: `smpp_bind_failures_total`

- زيادة = مشكلات في المصادقة، مشكلات 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
-

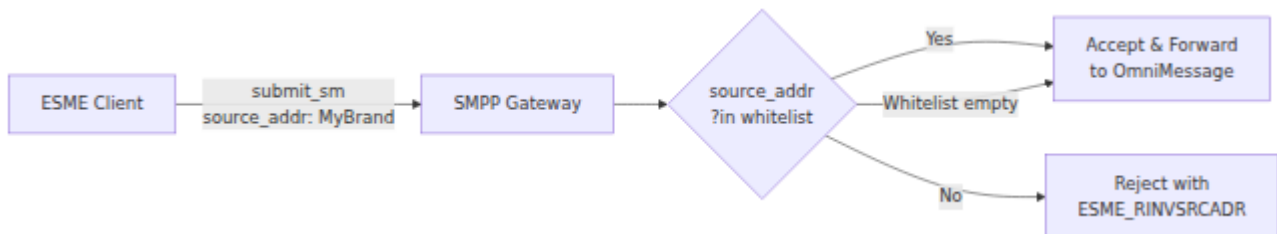
قائمة العناوين المسموح بها

SMPP التي يمكن لعميل (source_addr) تحكم فردي على العناوين الأصلية استخدامها عند إرسال الرسائل.

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.

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



قواعد المطابقة

:تدعم مطابقة عنوان المصدر وضعين

المطابقة الدقيقة

يجب أن يتطابق عنوان المصدر تمامًا مع إدخال القائمة المسموح بها. المطابقة حساسة لحالة الأحرف.

النتيجة	عنوان المصدر	إدخال القائمة المسموح بها
مسموح	MyBrand	MyBrand
مرفوض	mybrand	MyBrand
مرفوض	MyBrands	MyBrand
مسموح	+61400000001	+61400000001

المطابقة باستخدام البدل (البادئة)

. * أضيف * إلى إدخال القائمة المسموح بها لمطابقة أي عنوان مصدر يبدأ بالبادة قبل

النتيجة	عنوان المصدر	إدخال القائمة المسموح بها
مسموح	61400000001	614*
مسموح	61412345678	614*
مرفوض	61500000001	614*
مسموح	+61400000001	+614*
مسموح	MyBrand	My*
مسموح	MyCompany	My*

إدخالات متعددة

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

مثال على القائمة المسموح بها: MyBrand, 614*, +61400000001

النتيجة	المطابقات	عنوان المصدر
مسموح	MyBrand (دقيق)	MyBrand
مسموح	614* (بدل)	61412345678
مسموح	+61400000001 (دقيق)	+61400000001
مرفوض	لا شيء	OtherBrand
مرفوض	لا شيء	61500000001

معالجة الأخطاء

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

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

:يتم تسجيل تحذير مع عنوان المصدر المرفوض واسم النظيف

```
SMPP Server: Rejected submit_sm from partner_acme - source_addr  
'UnauthorisedBrand' not in whitelist
```

التكوين

عبر واجهة الويب

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

```
MyBrand,614*,+61400000001
```

5. انقر على **حفظ**

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*", "+61400000001"],  
    tps_limit: 50,  
    queue_check_frequency: 1000  
  }  
]
```

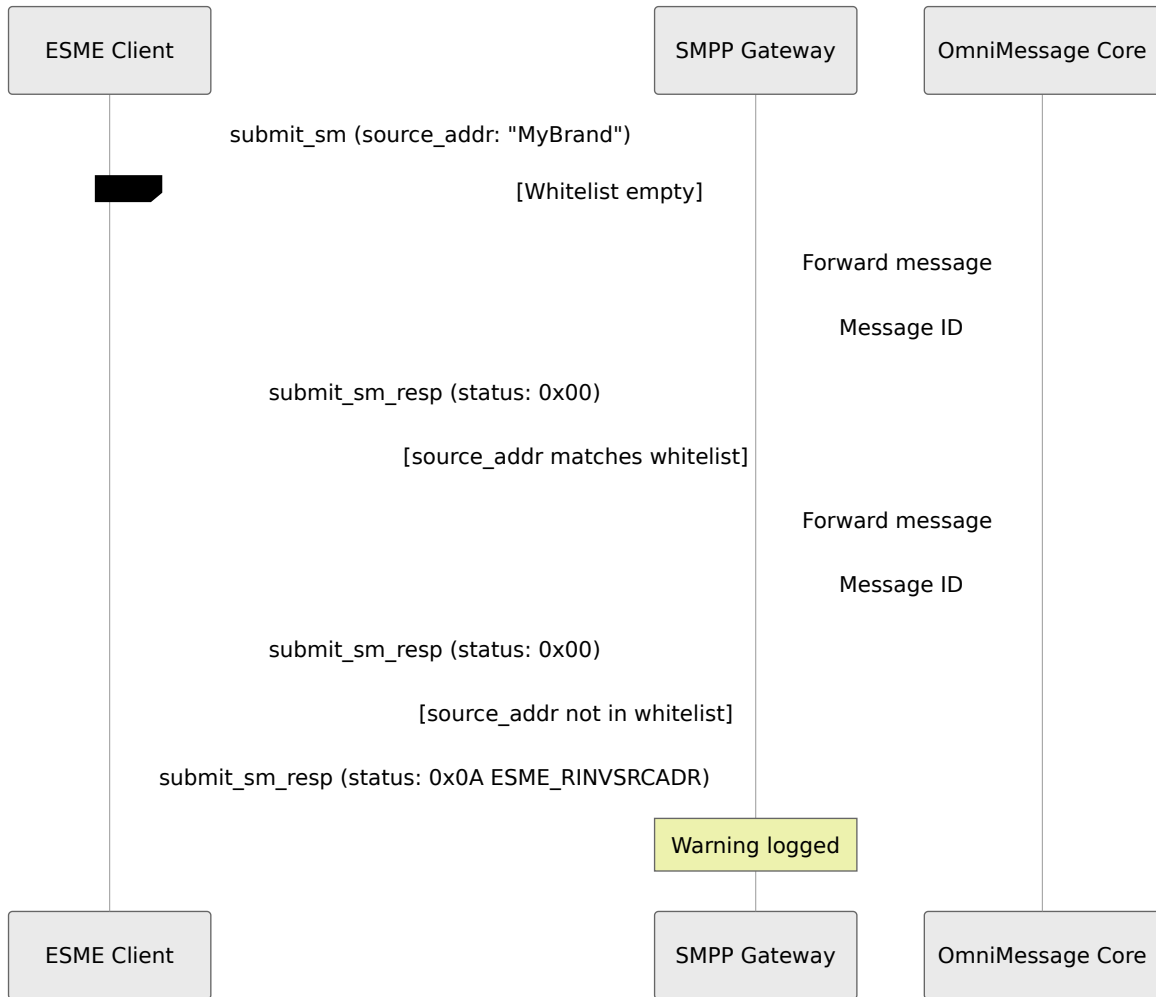

المعلومات

الوصف	الافتراضي	مطلوب	النوع	المعلمة
قائمة بأنماط عناوين المصدر المسموح بها. تدعم المطابقة الدقيقة والبدل (*). النهائي (suffix). قائمة فارغة تسمح بجميع عناوين المصدر.	يسمح ([]) (بالجميع)	لا	قائمة من السلاسل	source_address_whitelist

الترحيل

يتم ترحيل خوادم النظير الموجودة تلقائيًا عند بدء البوابة. تتلقى النظائر التي تم إنشاؤها قبل إضافة هذه الميزة قائمة فارغة (يسمح بجميع عناوين المصدر)، مما يحافظ على السلوك الحالي.

تدفق التحقق



أمثلة

تقييد إلى علامة تجارية واحدة

السماح فقط بالرسائل من معرف المرسل **AcmeCorp**:

AcmeCorp

ا??؟ سماح بنطاق أرقام أسترالية

السماح بأي رقم هاتف محمول أسترالي (يبدأ بـ 614)

614*

مختلط أبجدي رقمي

:السماح باسم علامة تجارية ونطاق من الأرقام

AcmeCorp,614*,+61290000001

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

- عنوان المصدر لا يتطابق مع أي إدخال في القائمة المسموح بها
- إدخال القائمة المسموح بها يحتوي على خطأ مطبعي أو نمط غير صحيح
- عدم تطابق الحالة (المطابقة حساسة لحالة الأحرف)
- نمط البديل صارم جدًا

:الحل

1. تحقق من قائمة العناوين المسموح بها للنظير الخادم في واجهة الويب
2. قارن عنوان المصدر المرفوض مع كل إدخال في القائمة المسموح بها
3. أضف عنوان المصدر المفقود أو قم بتعديل نمط البديل
4. تحقق من تطابق الحالة تمامًا للإدخالات غير البديل

عدم تأثير القائمة المسموح بها

الأعراض: قبول الرسائل على الرغم من عدم تطابق عنوان المصدر مع القائمة المسموح بها

الأسباب المحتملة:

- القائمة المسموح بها فارغة (تسمح بالجميع بشكل افتراضي)
- متصل بنظير خادم مختلف ESME
- تغيير ملف التكوين لم يتم تطبيقه بعد (يتطلب إعادة تشغيل)

الحل:

- تحقق من أن القائمة المسموح بها ممتلئة (ليست فارغة) في واجهة الويب.
- في الحالة الحية ESME تحقق من أي نظير خادم يتصل به.
- إذا كنت تستخدم ملف التكوين، أعد تشغيل الخدمة.

الوثائق ذات الصلة

- مرجع التكوين** - وثائق كاملة عن مع   مات خادم النظير
- SMPP **دليل الاستخدام** - إدارة اتصالات
- استكشاف الأخطاء وإصلاحها** - إجراءات استكشاف الأخطاء وإصلاحها العامة

دليل استكشاف الأخطاء وإصلاحها

المشكلات والحلول الشائعة

OmniMessage مشاكل الاتصال بـ

فإن مشاكل الاتصال، OmniMessage Core، غير حالة وتعتمد بالكامل على SMPP نظرًا لأن بوابة هي من أكثر المشكلات حرجة OmniMessage بـ.

OmniMessage أعراض انقطاع الاتصال بـ

- لا توجد رسائل صادرة: تتزايد قائمة الانتظار، الرسائل لا تُرسل
- لا توجد رسائل واردة: الشركاء لا يمكنهم إرسال الرسائل
- تتوقف أو تتعطل API مهلات: مكالمات
- "إعادة تعيين الاتصال"، "HTTP 503"، "السجلات تظهر: "تم رفض الاتصال"، "مهلة"

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. المكون API الخاص بـ 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. API: تحقق من سجلات البوابة لأخطاء:

```
# API ابحث عن الأخطاء المتعلقة بـ
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

:معطلاً OmniMessage إذا كان

1. OmniMessage اتصل بفريق عمليات
2. ستتراكم الرسائل المعلقة في قائمة الانتظار
3. (SMPP_POLL_INTERVAL انظر) ستستمر البوابة في المحاولة
4. أو المراقبة OmniMessage تحقق من صفحة حالة

:يعمل ولكن البوابة لا تستطيع الوصول إليه OmniMessage إذا كان

1. الصادر HTTPS تحقق من أن قواعد جدار الحماية تسمح 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

:غير مكون بشكل صحيح API الخاص بـ 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

الاتصال لا يتم تأسيسه

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 الاعتماد غير صحيحة

تحقق:

- "السجلات تظهر" 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 مصرح به IP سجلات الناقل تظهر

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
```

الاتصال يستمر في الانقطاع

الأعراض:

- الاتصال تم تأسيسه ولكن ينقطع بشكل متكرر
- زيادة مقياس `smpp_disconnection_total`
- السجلات تظهر 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 بشأن مشاكل الشبكة
- تحقق مع مزود خدمة الإنترنت إذا كانت المشكلة من جانبك
- النظر في اتصال/مسار احتياطي

2. مهلة استعلام الرابط

تحقق:

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

الحلول:

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

3. تجاوز حد TPS

تحقق:

- معدل الرسائل مرتفع عند وقت الانقطاع
- الناقل يحد من الرسائل

الحلول:

- مراجعة إعداد `tps_limit`
- إلى 70-80% من الحد الأقصى للناقل TPS تقليل
- توزيع الحركة عبر عدة روابط

4. مشاكل خادم الناقل

تحقق:

- تحقق من حالة خدمة الناقل
- اتصل بدعم الناقل

الحلول:

- انتظر حتى يقوم الناقل بحل المشكلة
 - تكوين ناقل احتياطي إذا كان متاحًا
-

مشاكل تسليم الرسائل

الرسائل لا تُرسل

الأعراض:

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

الأسباب المحتملة والحلول:

1. خاطئ `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 مجدولة للمستقبل

تحقق:

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

الشرح:

- للمرسائل الفاشلة `deliver_after` نظام إعادة المحاولة يحدد
- تنتظر الرسائل حتى ذلك الوقت قبل المحاولة مرة أخرى

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 نشط

تحقق:

- حالة الخدمة
- السجلات للأخطاء

الحلول:

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

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

معدل فشل التسليم مرتفع

الأعراض:

- تزداد `smpp_delivery_failures_total`
- مع حالة خطأ "submit_sm_resp" السجلات تظهر

- 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
- 0x00000003 - أمر غير صالح

الحلول:

- (E.164 موصى به) 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 في الرسائل المرفوضة

الحلول:

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

رسائل منتهية الصلاحية. 4.

تحقق:

- للرسالة `expires` طابع
- 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:

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

الأسباب المحتملة والحلول:

1. الخدمة غير نشطة

تحقق:

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

الحلول:

```
# إذا كانت متوقفة، قم بتشغيلها
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:

- المتصفح يظهر 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. خاطئ 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:

- الصفحة تُحمّل ولكن تظهر أخطاء
- الوظائف لا تعمل
- البيانات لا تعرض

الحلول:

1. مسح ذاكرة التخزين المؤقت للمتصفح:

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

2. تحقق من وحدة تحكم المتصفح:

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

3. جرب متصفحًا مختلفًا:

- Edge وFirefox وChrome اختبار في
- عزل المشكلات الخاصة بالمتصفح

4. تحقق من سجلات الخدمة:

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

مشاكل القياسات

غير متاحة Prometheus قياسات

الأعراض:

- يفشل `curl http://localhost:4000/metrics`
- لا يمكنه سحب القياسات Prometheus
- استجابة فارغة أو خطأ

الأسباب المحتملة والحلول:

1. الخدمة غير نشطة

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 كان المحلي يعمل ولكن البعيد لا: تحقق من جدار الحماية 🔒🔒 الحماية
- Prometheus افتح المنفذ 4000 في جدار الحماية ل خادم

3. نقطة النهاية خاطئة

تحقق:

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

القياسات تظهر قيم غير متوقعة

الأعراض:

- العدادات تعود إلى الصفر
- المقاييس تظهر قيم خاطئة
- القياسات مفقودة لبعض الروابط

الحلول:

1. إعادة تشغيل الخدمة تعيد تعيين العدادات:

- العدادات تعود إلى الصفر عند إعادة تشغيل الخدمة
- هذا سلوك طبيعي
- Prometheus في استعلامات `rate()` أو `increase()` استخدم

2. الروابط الجديدة لا تظهر:

- تظهر القياسات فقط بعد الحدث الأول

- أرسل رسالة اختبار لتعبئة القياسات
- تحقق من أن الربط مفعّل وملتصّل

3. قياسات قديمة:

- قد تظهر الروابط القديمة في القياسات
- 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 رسائل مرتفع جدًا
- عدد كبير جدًا من الاتصالات
- مشكلة في التكوين

الحلول:

- تحقق من أن معدل الرسائل ضمن القدرة
- TPS مراجعة حدود
- المرتفع CPU اتصل بالدعم إذا استمر استخدام

استخدام الذاكرة مرتفع

تحقق:

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

الأسباب المحتملة:

- قائمة انتظار رسائل كبيرة في الذاكرة
- تسرب في الذاكرة (نادر)

الحلول:

- إعادة تشغيل الخدمة لمسح الذاكرة
- تحقق من حجم قائمة الانتظار للرسائل
- اتصل بالدعم إذا استمرت الذاكرة في النمو

معالجة الرسائل ببطء

الأعراض:

- الرسائل تستغرق وقتًا طويلاً للإرسال
- تزايد قائمة الانتظار
- معدل الرسائل منخفض

تحقق:

1. قد تكون صارمة جدًا - TPS حدود
2. `queue_check_frequency` - قد تكون مرتفعة جدًا
3. الخلفية - قد ي❖❖ون بطيئًا API وقت استجابة
4. زمن الانتقال الشبكي إلى الناقل

الحلول:

- إذا سمح الناقل بذلك TPS زيادة
 - لتسريع الاستطلاع `queue_check_frequency` تقليل
 - الخلفية API تحسين
 - تحقق من زمن الانتقال الشبكي
-

مشاكل التكوين

أخطاء في بناء جملة ملف التكوين

الأعراض:

- الخدمة لن تبدأ بعد تغيير التكوين
- السجلات تظهر "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 البناء بعناية
- Elixir استخدام محرر نصوص مع تمييز بناء جملة

التغييرات لا تؤثر

الأعراض:

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

الحلول:

```
# تتطلب تغييرات التكوين إعادة تشغيل
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
```

الاسترداد الطارئ

فشل النظام بالكامل

الخطوات:

1. تحقق من صحة النظام الأساسية:

```
# مساحة القرص
df -h

# الذاكرة
free -h

# حمل 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
```

7. اتصل بالدعم إذا لم يتم حل المشكلة.

الحصول على المساعدة

المعلومات التي يجب جمعها

قبل الاتصال بالدعم، اجمع:

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

2. السجلات الأخيرة:

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

3. التكوين (قم بتنظيف كلمات المرور):

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

4. مخرجات القياسات:

```
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 الم❖❖لومات من أعلاه

الوثائق ذات الصلة

- **USAGE.md** - إجراءات التشغيل العادية
- **CONFIGURATION.md** - مرجع التكوين
- **MONITORING.md** - المراقبة والقياسات
- **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 استرداد الرسائل المعلقة
- لا يمكن الإبلاغ عن حالة التسليم
- يبدو أن النظام يتجمد أو ينتهي وقته

OmniMessage: تحقق من صحة

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

```
# المكون في السجلات API الخاص بـ 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 لوحة التحكم تحميل بشكل صحيح

2. تحقق من حالة الاتصال

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

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 تحذير

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 متصل)
- معدلات فشل التسليم العالية (< 5%)
- عدم وجود حركة مرور لفترات طويلة
- الانقطاعات المتكررة

لتكوين التنبيهات [MONITORING.md](#) راجع.

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"` بصف رسالة مع `submit_sm` OmniMessage SMPP الرسالة وترسلها عبر `vodafone_uk` العميل الخاص بالجسر المسمى `submit_sm`.
- **source_smsc** — يوجه الرسائل الواردة إلى **روابط الخادم**. عندما يقوم `source_smsc: "partner_acme"` بصف رسالة مع `deliver_sm` OmniMessage SMPP عبر `partner_acme` بتسليمها إلى العملاء المتصلين برابط الخادم المسمى `deliver_sm`.

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

تسجيل الواجهة الأمامية

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

- الافتراضي) `smssc_name` اسم التسجيل: يتم التحكم فيه بواسطة تكوين `"smpp_gateway"`, env: `SMSSC_NAME`)
- نبض القلب: يتم إرساله كل 60 ثانية للحفاظ على التسجيل نشطاً
- انتهاء الصلاحية: ينتهي التسجيل في الجزء الخلفي بعد 90 ثانية بدون نبض قلب
- تسجيل لكل رابط: يتم تسجيل كل نظير مفعّل بشكل فردي باستخدام التنسيق `{hostname}_{peer_name}`

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 مع ما يتوقعه `smssc_name` تطابق
3. OmniMessage Core (`api_base_url`) الاتصال الشبكي به.

SMPP إدارة اتصالات

SMPP كيفية تكوين أقران

بإستخدام **طريقتين** (الأقران) SMPP يمكن تكوين اتصالات

الطريقة 1: واجهة ويب (موصى بها)

- **الميزة:** التغييرات تدخل حيز التنفيذ على الفور، لا حاجة لإعادة التشغيل
- Client Peers / Server Peers علامات التوبيخ → 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 الخدمة بعد التغييرات
- **الأفضل لـ:** الإعداد الأولي، البنية التحتية ككود

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

كمرجع لملف التكوين [CONFIGURATION.md](#) راجع

إضافة اتصال عميل جديد

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

التحضير: جمع المعلومات من الناقل:

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

اختر واحدة من الطرق التالية:

الخيار أ: عبر واجهة الويب (موصى بها)

المزايا: تأثير فوري، لا حاجة لإعادة التشغيل

الخطوات:

1. **انتقل إلى أقران العملاء:**

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

2. **إضافة نظير جديد:**

- انقر على "إضافة نظير عميل جديد"
- املأ النموذج:
 - (معرف فريد) `vodafone_uk`: **الاسم**

- **المضيف:** `smpp.vodafone.co.uk`
- **المنفذ:** `2775`
- **معرف النظام:** `your_username`
- **كلمة المرور:** `your_password`
- **نوع الربط:** `Transceiver`
- **TPS حد:** `100`
- **تكرار فحص الطابور:** `1000`
- انقر على "حفظ"

3. تأسيس الاتصال تلقائيًا:

- يحاول الجسر الاتصال على الفور
- الحالة الحية → SMPP: انتقل إلى
- يجب أن تتغير 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  
  }  
]
```

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 الغرض**: تكوين الجسر للعمل كـ الخارجيين

التحضير:

1. إنشاء بيانات الاعتماد:

- إنشاء معرف نظام ف `partner_name`: `partner_name`
- إنشاء كلمة مرور قوية
- توثيق ومشاركة بأمان مع الشريك

2. الحصول على معلومات ال `SMPP` ريك:

- 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 أقران الخادم:

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

2. إضافة نظير خادم جديد:

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

3. الجسر جاهز للاتصال:

- أصبح نظير الخادم نشطاً الآن و ينتظر اتصال 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:

```
# أضيف إلى قائمة server_binds
config :omnimessage_smpp, :server_binds, [
  # الروابط 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 (يحتاج 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 اتصال موجود

(.البيضاء، إلخ IP كلمات المرور، قائمة، 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`
- أقران العملاء → SMPP للاتصالات العميلة
- أقران الخادم → SMPP للاتصالات الخادمة

2. تحرير النظيف:

- ابحث عن النظيف الذي تريد تعديله
- انقر على زر "تحرير"
- قم بتحديث المعلومات المطلوبة
 - البيضاء، IP كلمة المرور، قائمة، TPS التغييرات الشائعة: حد المضيف/المنفذ
- انقر على "حفظ"

3. تدخل التغييرات على الفور:

- يعيد الاتصال الاتصال تلقائيًا بالإعدادات الجديدة
- لا حاجة لإعادة تشغيل الخدمة
- الحالة الحية للتحقق → SMPP: انتقل إلى

4. تحقق من التغييرات:

- تحقق من أن الاتصال تم تأسيسه بنجاح
- للبحث عن الأخطاء Logs راقب علامة التبويب
- اختبر تدفق الرسائل إذا كان ذلك ممكناً

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 معلومات الربط:

- `:server_binds` أو `:binds` ابحث عن الربط في قائمة
- قم بتحديث المعلومات المطلوبة
 - البيضاء، IP كلمات المرور، قائمة TPS، التغييرات الشائعة: حد المضيف/المنفذ
- مثال:

```
%{  
  name: "vodafone_uk",  
  # معلومات 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. تحقق من التغييرات:

- الحالة الحية → SMPP: انتقل إلى
- تحقق من أن الاتصال تم تأسيسه بنجاح

- راقب السجلات للبحث عن الأخطاء
- اختبر تدفق الرسائل

إزالة اتصال

SMPP الغرض: إلغاء تشغيل اتصال

الخطوات:

1. إخطار المعنيين:

- أبلغ الناقل/الشريك
- تن   يق 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:

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

4. تحقق من الإزالة:

- تحقق من الحالة الحية - يجب أن يكون الاتصال قد اختفى
- راجع السجلات للتأكد من الإيقاف النظيف

تمكين وتعطيل الاتصالات

الغرض: أخذ اتصال خارج الخدمة مؤقتًا دون حذف تكوينه

الذي يتحكم في ما إذا كانت نشطة. تحتفظ الأقران المعطلة بجميع `enabled` تمتلك الأقران حقل تكويناتها ولكن لا تقيم أو تقبل الاتصالات.

:عبر واجهة الويب

1. أقران العملاء أو أقران الخادم → SMPP :انتقل إلى
2. ابحث عن النطير لتعطيله
3. "انقر على "تحرير"
4. "قم بإلغاء تحديد خانة "مفعّل"
5. "انقر على "حفظ"

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

:حالات الاستخدام

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

سلوك الاتصال

منطق إعادة الاتصال

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

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

(Keepalive) استعلام الرابط

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

- قابلة للتكوين لكل ربط عبر **الفترة الافتراضية:** 60 ثانية
(`enquire_link_interval`)

- (غير موصى به) `enquire_link_interval: 0` **تعطيل**: تعيين
- `enquire_link`، تعتبر الاتصال، **كشف الفشل**: إذا توقف النظير البعيد عن الاستجابة لـ ميّناً وتبدأ إعادة الاتصال

و `smpp_enquire_link_sent_total` Prometheus راقب صحة استعلام الرابط عبر مقاييس تشير الفجوة المتزايدة بين المرسل والمستلمة إلى `smpp_enquire_link_received_total`. مشاكل في الاتصال.

TPS تحديد معدل

الخاص به باستخدام نافذة منزلقة لكل ثانية `tps_limit` يفرض كل ربط حد

- يتم عد الرسائل داخل كل نافذة زمنية مدتها 1 ثانية
- عند الوصول إلى الحد، يتوقف عامل الطابور حتى الثانية التالية
- يمكن أن تكون هناك 100 رسالة كحد أقصى في الهواء (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

1. محدد بشكل كافٍ لحركتك `tps_limit` أن
2. منخفض بما يكفي للحفاظ على تغذية خط الأنابيب `queue_check_frequency` أن
3. أن الناقل يستجيب للرسائل بسرعة (تؤدي الاستجابات البطيئة إلى تقليل الإنتاجية الفعالة)

إدارة تدفق الرسائل

التحقق من 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
- مراجعة:
 - 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 تـ❖❖ليمها

الخطوات:

1. تحقق من حالة الاتصال:

- الحالة الحية → SMPP: انتقل إلى
- تحقق من أن الاتصال المستهدف متصل

- إذا كان غير متصل، راجع **إعادة الاتصال**

2. تحقق من تفاصيل الرسالة:

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

3. تحقق من محاولات التسليم:

- محاولات عالية = فشل متكرر
- تحقق من السجلات للرسائل 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 فريق الجزء 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
- فلترة: مستوى الخطأ
- ابحث عن فشل المصادقة، انتهاء مهلة الشبكة

3. تحقق من بيانات الاعتماد:

- أقران العملاء/الخادم → SMPP: انتقل إلى
- وكلمة المرور صحيحة `system_id` تحقق من أن
- اتصل بالناقل إذا كنت غير متأكد

4. إعادة الاتصال يدويًا:

- الحالة الحية → SMPP: انتقل إلى
- ابحث عن الربط المنفصل
- "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
- راجع [TROUBLESHOOTING.md](#)

التعامل مع فشل المصادقة

الأعراض: فشل الربط المتكرر في السجلات

الأسباب:

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

الخطوات:

1. تحقق من بيانات الاعتماد:

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

2. البيضاء IP تحقق من قائمة:

- للجسر مع الناقل IP تأكد من عنوان
- البيضاء IP اطلب من الناقل التحقق من قائمة

3. تحقق من حالة الحساب:

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

4. تحديث التكوين:

- إذا تم تغيير بيانات الاعتماد، قم بتحديثها في واجهة الويب
 - انقر على "إعادة الاتصال" لإعادة المحاولة باستخدام بيانات الاعتماد الجديدة
-

المراقبة والتنبيه

Prometheus التحقق من مقاييس

تحقق سريع:

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

الإخراج المتوقع:

```
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. راجع [TROUBLESHOOTING.md](#)

تنبيه معدل الفشل العالي:

1. تحقق من السجلات للأنماط الخطأ
2. راجع التغييرات الأخيرة في التكوين
3. اتصل بالناقل بشأن 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 توجيه

- 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:

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

3. تدقيق بيانات الاعتماد:

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

4. تخطيط السعة:

- مراجعة معدلات الرسائل القصوى
- TPS التحقق 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 للعودة على الإنترنت).
2. الحالة الحية: SMPP → انتقل إلى
3. انتظر حتى يتم تأسيس جميع الاتصالات (1-2 دقيقة).
4. تحقق من السجلات للأخطاء.

النسخ الاحتياطي للتكوين

قم بعمل نسخة احتياطية من الملفات الحرجة قبل التغييرات:

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

# النسخ الاحتياطي 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 الكاملة

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. توثيق السبب:

- ملاحظة اسم الناقل
- تسجيل الوقت والسبب
- حفظ المراسلات

3. تحقيق في المشكلة:

- تحقق من أنماط الرسائل الأخيرة
- مراجعة السجلات للأخطاء
- تحديد السبب الجذري

4. تنسيق الحل:

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

ارتفاع حجم الرسائل

الأعراض: حركة مرور رسائل مرتفعة بشكل غير متوقع

الخطوات:

1. TPS تحقق من حدود:

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

2. مراقبة استقرار الناقل:

- راقب الانقطاعات
- تحقق من معدلات النجاح في التسليم

3. تنسيق مع الجزء الخلفى:

- تحقق من أن مصدر الرسالة 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 أن معدلات النجاح في 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 مع الناقل
 - ☐ TPS مراجعة وتحسين إعدادات
 - ☐ النسخ الاحتياطي 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
-

