

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 **تستقبل**
2. REST عبر واجهة برمجة التطبيقات OmniMessage **ترجمها** إلى تنسيق
3. للحصول على رسائل لإرسالها OmniMessage **تستعلم** عن
4. إلى شركات النقل SMPP PDUs **ترسل**
5. OmniMessage **تبلغ** حالة التسليم مرة أخرى إلى

- (Diameter, MAP, IMS) الأخرى OmniMessage هذا هو نفس الطريقة التي تعمل بها واجهات OmniMessage Core جميعها 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. يستخدم ملف التكوين بناء جملة

```
import Config

# الإعدادات العالمية
config :omnimessage_smpp,
  setting_name: value

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

الإعدادات العالمية

API_BASE_URL

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 لمعالجة جميع الرسائل REST واجهة برمجة التطبيقات:

- للمعالجة OmniMessage المستلمة إلى **إرسال الرسائل**: إرسال رسائل
- **استرجاع الرسائل**: الاستعلام عن الرسائل الموجهة لشركات النقل
- OmniMessage **تقرير حالة التسليم**: تحديث حالة تسليم الرسالة مرة أخرى إلى
- **صحة النظام**: فحوصات صحية دورية

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

- التحقق من صحة الرسالة وفحص التنسيق ✓
- قرارات التوجيه (أي شركة نقل يجب استخدامها) ✓
- تحديد المعدل والتقييد ✓
- التحقق من صحة 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 تكون البوابة لديها وصول إلى الشبكة إلى
- (قم بتكوين `verify_ssl_peer` في الإنتاج HTTPS استخدم
- على المنفذ المحدد HTTPS يجب أن يسمح جدار الح🔒🔒اية بالاتصالات الصادرة عبر

SMPP_POLL_INTERVAL

تكرار فحص قائمة الانتظار (بالملي ثانية)

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

المعلمة	النوع	مطلوب	الافتراضي
<code>smpp_poll_interval</code>	عدد صحيح	لا	100

الغرض: كم مرة (بالملي ثانية) يتحقق كل عميل من قائمة انتظار الرسائل.

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
<code>verify_ssl_peer</code>	بولياني	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`:   التحقق (شهادات موقعة ذاتيًا، اختبار)

متغير البيئة: `VERIFY_SSL_PEER`

SMSC_NAME

معرف البوابة للتسجيل

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

المعلمة	النوع	مطلوب	الافتراضي
smsc_name	سلسلة	لا	"smpp_gateway"

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

متغير البيئة: `SMSC_NAME`

SMPP تكوين ربط عميل

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

مثال كامل لربط العميل

```
config :omnimessage_smpp, :binds, [
  %{
    # معرف فريد لهذا 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 للمصادقة
    system_id: "your_username",
    password: "your_password",

    # تحديد المعدل
    tps_limit: 100,

    # تكرار فحص قائمة الانتظار
    queue_check_frequency: 1000
  }
]
```

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 عمليات الربط
- استخدم أسماء وصفية (شركة النقل، المنطقة، الغرض)

قواعد التسمية:

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

mode

نوع الاتصال

النوع	مطلوب	القيمة
ذرة	نعم	:client

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

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

bind_type

SMPP نوع جلسة

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

الغرض: يحدد قدرة اتجاه الرسالة

الخيارات:

- :transmitter (submit_sm) إرسال الرسائل فقط -
- :receiver (deliver_sm) استلام 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	"smpp.carrier.com" أو "10.5.1.100"

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

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	نعم	2775	1-65535

SMPP لاتصال TCP الغرض: منفذ

المنفذ القياسي: 2775

أمثلة:

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

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:

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

tps_limit

حد المعاملات في الثانية

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	نعم	100	1-10000

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

إرشادات:

- اضبط على 70-80% من الحد الأقصى لشركة النقل
- يمنع التقييد/الانفصال

- يتيح مساحة لتسليم الإيصال

أمثلة:

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

الحساب:

TPS إذا كان الحد الأقصى لشركة النقل = 100
اضبط $tps_limit = 70-80$
مساحة TPS يترك 30-20

queue_check_frequency

فترة استعلام قائمة الانتظار (بالملي ثانية)

النطاق	الافتراضي	مطلوب	النوع
100-10000	1000	نعم	عدد صحيح

الغرض: كم مرة يتم 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

المقايضات:

- قيمة أقل = أسرع التقاط الرسائل، مزيد من تحميل واجهة برمجة التطبيقات
- قيمة أعلى = أبطأ التقاط، أقل تحميل واجهة برمجة التطبيقات

مثال واجهة الويب:

SMPP تكوين ربط خادم

SMSC عمليات الربط الخاصة بالخادم تحدد الاتصالات الواردة حيث تعمل البوابة كـ الخارجيين. في هذا الوضع، تتصل الأنظمة الشريكة (العملاء) **ESMEs** تقبل الاتصالات من (الخادم) بالبوابة لإرسال واستقبال 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"],

    # تحديد المعدل
    tps_limit: 50,

    # تكرار فحص قائمة الانتظار
    queue_check_frequency: 1000
  }
]
```

معلومات ربط الخادم

name

معرف العميل

النوع	مطلوب	مثال
سلسلة	نعم	"partner_acme"

الغرض: يحدد   لعميل الخارجي الذي يتصل بك.

قواعد 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.

توفير للعميل: شارك هذه البيانات مع شريكك.

password

كلمة المرور المتوقعة من العميل

النوع	مطلوب	مثال
سلسلة	نعم	"secure_password"

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

الأمان:

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

allowed_bind_types

أنواع الجلسات المسموح بها

النوع	مطلوب	الافتراضي
قائمة من الذرات	نعم	-

الغرض: يحدد أنواع الربط التي يمكن للعميل استخدامها.

الخيارات:

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

التوصية: السماح بجميع الأنواع الثلاثة ما لم تكن بحاجة إلى قيود.

ip_whitelist

المسموح بها للعمليات IP عناوين

النوع	مطلوب	الافتراضي	التنسيق
قائمة من السلاسل	نعم	[]	CIDR أو تنسيق IPs

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 الفرعية الشائعة:

- بدون  نوع IPs تلقائي لـ فردي IP - /32
- عنوان (مثل 255-192.168.1.0) - /24
- عنوان (مثل 255.255-10.50.0.0) - /16
- عنوان (مثل 255.255.255.255-10.0.0.0) - /8

tps_limit

حد الرسائل في الثانية

الصادر deliver_sm لربط العميل - يتحكم في معدل tps_limit نفس

queue_check_frequency

فترة استعلام قائمة الانتظار

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

مثال واجهة الويب:

تكوين الاستماع للخادم

. عندما يتم تكوين عمليات الربط للخادم، 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

النطاق	الافتراضي	مطلوب	النوع
1-65535	2775	لا	عدد صحيح

SMPP. **الغرض:** 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 للعميل.

إرشادات:

- اضبط بناءً على العملاء المتوقعين
 - القيم الأعلى تستخدم المزيد من الذاكرة
 - المعتاد: 10-100 اتصال
-

أمثلة تكوين كاملة

المثال 1: اتصال شركة نقل واحدة

```
import Config

config :omnimessage_smpp,
  api_base_url: "https://smcsc.company.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 عمليات الربط للخادم

```
import Config

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

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

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

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

التحقق من التكوين

بعد تحرير التكوين، تحقق قبل إعادة التشغيل:

فحص التركيب

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

إذا كان التركيب غير صالح، 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.

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 والأرقام والرموز
- فريدة لكل اتصال

3. البيضاء IP استخدم قوائم:

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

4. SSL قم بتمكين التحقق من:

- مع شهادات صالحة `verify_ssl_peer: true` اضبط

5. تدوير بيانات الاعتماد بشكل منتظم:

- تغيير كلمات المرور كل ثلاثة أشهر
- التنسيق مع شركات النقل/الشركاء

الخطوات التالية

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

المعجم

المصطلحات والتعريفات

أ

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

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

ب

للاسترجاع وتخزين الرسائل SMPP نظام قائمة الرسائل الذي يتصل به بوابة **Backend**.

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

Bind Type نوع جلسة SMPP:

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

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

ج

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

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

Connection Status SMPP الحالة الحالية لارتباط

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

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

د

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

Delivery Failure عندما لا يمكن تسليم رسالة، مما يشير إلى ذلك استجابة خطأ من مزود الخدمة.

Delivery Receipt (DLR) تأكيد من مزود الخدمة حول حالة تسليم الرسالة.

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

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

هـ

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

ESM Class يشير إلى نوع الرسالة وميزاتها SMPP حقل

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

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

و

Firewall نظام أمان الشبكة الذي يتحكم في حركة المرور الواردة والصادرة

ز

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 7 بت للرسائل القصيرة، يدعم حتى 160 حرفًا لكل رسالة

ح

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

ط

IP Whitelist .المسموح لها بالاتصال بالبوابة (ميزة أمان) IP قائمة بعناوين

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

ي

(لا توجد مصطلحات)

ك

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

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

ل

، 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 تكنولوجيا إطار **LiveView** الحقيقي.

م

نظام خلفية يخزن الرسائل التي تنتظر أن تُرسل أو تُستقبل **Message Queue**.

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

رسائل تُرسل من الهواتف المحمولة إلى البوابة (داخلي) (**المصدر المحمول**) **MO**.

رسائل تُرسل من البوابة إلى الهواتف المحمولة (خارجي) (**المحمول المنتهي**) **MT**.

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

ن

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

هـ

رسائل تتدفق من البوابة إلى الشبكات المحمولة **Outbound**.

رسائل تتدفق من الشبكات المحمولة إلى البوابة **Inbound**.

ص

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

نظام مراقبة مفتوح المصدر يجمع ويخزن مقاييس السلاسل الزمنية **Prometheus**.

ق

قائمة الرسائل التي تنتظر المعالجة أو الإرسال **Queue**.

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

SMPP مكون يسترجع الرسائل من القائمة ويرسلها عبر **Queue Worker**.

ر

TPS التحكم في معدل مرور الرسائل للامثال لقيود مزود الخدمة. انظر **Rate Limiting**.

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

مفصول SMPP إعادة إنشاء اتصال **Reconnect**.

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

س

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

نشط بين نظامين SMPP اتصال **Session**.

بروتوكول قياسي في الصناعة لتبادل رسائل (**رسائل قصيرة من نظير إلى نظير**) **SMPP** بين الأنظمة SMS.

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

بروتوكولات التشفير للتواصل الآمن **SSL/TLS**.

Submit_SM PDU SMPP لتقديم رسالة للتسليم.

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

System ID اسم المستخدم المستخدم لمصادقة SMPP.

ط

Telemetry جمع ونقل تلقائي لمقاييس النظام.

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

TPS حد معدل لحد أقصى 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، يقاس عادةً بالرسائل في الثانية.

ع

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

Uptime مدة استمرار اتصال أو خدمة في العمل بشكل مستمر.

ص

Validity Period حد زمني لمحاولة تسليم الرسالة قبل انتهاء صلاحيتها.

و

Web Dashboard واجهة مستخدم قائمة على المتصفح لمراقبة وإدارة البوابة.

Whitelist IP Whitelist انظر.

س

(لا توجد مصطلحات)

ط

(لا توجد مصطلحات)

ظ

(لا توجد مصطلحات)

مرجع سريع للاختصارات

الاختصار	المصطلح الكامل
API	واجهة برمجة التطبيقات
CIDR	توجيه بين النطاقات 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	المصدر المحمول
MSISDN	رقم دليل المشترك الدولي لمحطة المحمول
MT	المحمول المنتهي
NPI	مؤشر خطة الترقيم
PDU	وحدة بيانات البروتوكول
SMPP	رسائل قصيرة 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
 - **OPERATIONS.md** - العمليات اليومية
 - **MONITORING.md** - المقاييس والمراقبة
 - **TROUBLESHOOTING.md** - حل المشكلات
-

دليل المراقبة والقياسات

SMPP مرجع كامل لمراقبة بوابة

نظرة عامة

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

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

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

نقطة نهاية القياسات

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

Prometheus التنسيق: تنسيق نص

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

اختبار سريع

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

القياسات المتاحة

وتتضمن تسميات 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 كون 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 مستلمة 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 - معالجة الرسائل الصادرة"
    محظورة"
```

قياسات حالة الاتصال

smpp_connection_status

النوع: Gauge

SMPP الوصف: حالة الاتصال الحالية لربط

القيم:

- 1 = متصل
- 0 = غير متصل

التسميات:

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

مثال:

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

الاستخدام:

- تنبيه عند كون القيمة 0 (غير متصل)
- تتبع نسبة وقت التشغيل للاتصال
- مراقبة ت♦♦رار إعادة الاتصال

عدادات الرسائل

smpp_messages_sent_total

النوع: Counter

SMPP الوصف: العدد الإجمالي للرسائل المرسله عبر ربط

الوحدة: رسائل

التسميات: نفس قياسات 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 قياسات 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 عند حدوث تغييرات غير متوقعة في الحجم

قياسات التسليم

smpp_delivery_failures_total

النوع: Counter

الوصف: العدد الإجمالي لفشل تسليم الرسائل

الوحدة: حالات الفشل

التسميات: نفس قياسات حالة الاتصال

مثال:

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

الاستخدام:

- حساب معدل نجاح التسليم
- تنبيه عند ارتفاع معدلات الفشل
- تحديد الاتصالات المشككة

حساب معدل النجاح:

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

قياسات عمليات الربط

smpp_bind_success_total

النوع: Counter

الوصف: العدد الإجمالي لعمليات الربط الناجحة

الوحدة: محاولات الربط

مثال:

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

الاستخدام:

- تتبع استقرار الربط
- مراقبة نجاح المصادقة

smpp_bind_failures_total

النوع: Counter

الوصف: العدد الإجمالي لعمليات الربط الفاشلة

الوحدة: محاولات الربط

مثال:

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

الاستخدام:

- تنبيه عند فشل المصادقة
- تحديد مشاكل الاعتماد
- تتبع مشاكل 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 تغيرات الاتصال
- مراقبة تكرار إعادة الاتصال

smpp_disconnection_total

النوع: Counter

الوصف: العدد الإجمالي لفقدان الاتصال
الوحدة: فقدان الاتصال

مثال:

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

الاستخدام:

- تنبيه عند فقدان الاتصال المتكرر
- تحديد مشاكل الشبكة
- تتبع استقرار الاتصال

قياسات وقت التشغيل

smpp_uptime_seconds

النوع: Gauge

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

مثال:

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

الاستخدام:

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

OmniMessage API قياسات صحة

OmniMessage API فإن صحة SMPP، بينما تقوم البوابة نفسها بعرض قياسات متعلقة بـ: **أمر حرج**. يجب عليك أيضًا مراقبة

(إذا كانت متاحة) **OmniMessage** من قياسات

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

من سجلات البوابة (إذا لم يتم عرض القياسات)

API: ابحث عن هذه الأنماط لاكتشاف مشاكل

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

تكوين Prometheus

تكوين سحب أساسي

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

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

بوابات متعددة

```
scrape_configs:
  - job_name: 'omnmessage-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: 'omnmessage-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

الحدود:

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

لوحة معدل الرسائل

الاستعلام:

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

التصور: Graph

الوحدة: رسائل/ثانية

الأسطورة: `{{bind_name}}`

لوحة معدل نجاح التسليم

الاستعلام:

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

التصور: Gauge

الوحدة: نسبة مئوية (100-0)

الحدود:

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

لوحة وقت تشغيل الاتصال

الاستعلام:

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

التصور: Stat

الوحدة: ساعات

قواعد التنبيه

Prometheus قواعد تنبيه

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

```

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

    # معدل فشل مرتفع
    - alert: SMPPHighFailureRate
      expr: |
        (
          rate(smpp_delivery_failures_total[5m])
          /
          rate(smpp_messages_sent_total[5m])
        ) > 0.05
      for: 5m
      labels:
        severity: warning
      annotations:
        summary: "{{ معدل فشل التسليم 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 في الربط على }} $labels.bind_name }}"
        description: "{{ فشل في الربط }} $labels.bind_name }} مرات في آخر 10 دقائق"

    # 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"

# فقدان الاتصال المتكرر
- alert: SMPPFrequentDisconnections
  expr: increase(smpp_disconnection_total[1h]) > 5
  labels:
    severity: warning
  annotations:
    summary: "{{ $labels.bind_name }} فقدان الاتصال المتكرر على"
    description: "{{ $labels.bind_name }} تم فصله {{ $value }} مرات في آخر ساعة"

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

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

```

```
summary: "OmniMessage API مهلات  
description: "قد تكون API. تم اكتشاف عدة مهلات  
OmniMessage بطيئة أو مثقلة."  
  
# API مشكلة لا توجد تدفقات رسائل  
- alert: NoMessageFlow  
  expr: rate(smpp_messages_sent_total[10m]) == 0 and  
rate(smpp_messages_received_total[10m]) == 0  
  for: 30m  
  labels:  
    severity: warning  
  annotations:  
    summary: "لا توجد تدفقات رسائل مكتشفة - تحقق من الاتصال بـ  
OmniMessage"  
    description: "لم يتم إرسال أو استلام أي رسائل لمدة 30  
".وحالة قائمة الانتظار OmniMessage API دقيقة. تحقق من الاتصال بـ"
```

قم بتحميل القواعد في prometheus.yml:

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

مراقبة لوحة المعلومات على الويب

Prometheus تقدم واجهة الويب المدمجة مراقبة في الوقت الحقيقي دون

الوصول

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

صفحة الحالة الحية

الحالة الحية → SMPP: التنقل

الميزات:

- حالة الاتصال في الوقت الحقيقي

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

الاستخدام:

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

تظهر لوحة المعلومات:

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

مراقبة السجلات

سجلات النظام

عرض السجلات:

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

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

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

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

سجلات واجهة الويب

التنقل: علامة السجلات في واجهة الويب

الميزات:

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

تتيح لك عرض السجلات

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

(KPIs) مؤشرات الأداء الرئيسية

صحة الاتصال

المقياس: نسبة وقت تشغيل الاتصال

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

%الهدف: < 99.9

معدل تسليم الرسائل

المقياس: الرسائل 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
- للتنبيهات على مدار الساعة PagerDuty/OpsGenie استخدام
- اختبار التنبيهات بانتظام

2. إنشاء لوحات المعلومات

- 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
- تخطيط تعديلات السعة

4. توثيق الأسس

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

5. الربط مع الخلفية

- الخلفية API مراقبة قياسات
- تتبع تدفق الرسائل من البداية إلى النهاية
- تحديد الاختناقات

استكشاف الأخطاء باستخدام القياسات

مشاكل 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
- مقارنة عبر الاتصالات = تحديد الناقل المشككة

الإنتاجية المنخفضة

معدل `smpp_messages_sent_total` تحقق: معدل

- توفر قائمة الانتظار، TPS أقل من المتوقع = تحقق من حدود
- الخلفية API تحقق من قياسات

مشاكل الربط

تحقق: `smpp_bind_failures_total`

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

الوثائق ذات الصلة

- **CONFIGURATION.md** - تكوين إعدادات المراقبة
 - **OPERATIONS.md** - إجراءات التشغيل
 - **TROUBLESHOOTING.md** - حل المشكلات
 - **README.md** - نظرة عامة وبداية سريعة
-

دليل العمليات

إجراءات التشغيل اليومية

OmniMessage Core: الاعتماد الحرج

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

:غير متاح OmniMessage إذا أصبح

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

OmniMessage: تحقق من صحة

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

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

العمليات اليومية

فحص الصحة الصباحية

:قم بإجراء هذه ال❖❖حوصات في بداية كل يوم

1. الوصول إلى لوحة التحكم على الويب

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

- تحقق مما إذا كانت لوحة التحكم تُحمّل بشكل صحيح

2. تحقق من حالة الاتصال

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

3. مراجعة مقاييس الرسائل

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

4. تحقق من سجلات النظام

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

5. Prometheus مراجعة مقاييس

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

المراقبة المستمرة

قم بإعداد تنبيهات لـ

- فشل الاتصال (< 2 دقيقة تعطل)
- معدلات فشل التسليم العالية ($< 5\%$)
- عدم وجود حركة مرور لفترات طويلة
- انقطاعات متكررة

لتكوين التنبيهات [MONITORING.md](#) انظر

SMPP إدارة اتصالات

SMPP كيفية تكوين نظائر

باستخدام **طريقتين** (النظائر) SMPP يمكن تكوين اتصالات

الطريقة 1: واجهة الويب (موصى بها)

- **الميزة:** التغييرات تدخل حيز التنفيذ على الفور، لا حاجة لإعادة التشغيل
- Client Peers / Server Peers علامات التويب → SMPP: **الموقع**
- **العمليات:** إضافة، تحرير، حذف النظائر
- Mnesia **الاستمرارية:** مخزنة في قاعدة بيانات
- **الأفضل لـ:** العمليات اليومية، الاختبار، التغييرات السريعة

الطريقة 2: ملف التكوين

- **الميزة:** التكوين ككود، التحكم في الإصدارات
- **الموقع:** `/opt/omnimessage-smpp/config/runtime.exs`
- Elixir **العمليات:** تعريف النظائر في تكوين
- **الاستمرارية:** ت  ت  تمتد 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.

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

إضافة اتصال عميل جديد

الناقل (خادم) **SMSC** يتصل 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 جهاز إرسال واستقبال)
- TPS حد

اختر واحدة من الطرق التالية

الخيار أ: عبر واجهة الويب (موصى بها)

المزايا: تأثير فوري، لا حاجة لإعادة التشغيل

الخطوات:

1. **انتقل إلى نظائر العملاء:**

- افتح واجهة الويب: `https://your-server:8087`
- انتقل إلى: SMPP → Client Peers

2. **أضف 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: 100 حد**
- **تكرار فحص الطابور: 1000**
- انقر على "حفظ"

3. يتم إنشاء الاتصال تلقائيًا:

- يحاول الجسر الاتصال على الفور
- الانتقال إلى SMPP → Live Status
- يجب أن تتغير الحالة إلى "متصل" (باللون الأخضر) خلال 10-30 ثانية
- للحصول على رسالة ربط ناجحة Logs تحقق من علامة التبويب

4. اختبار تدفق الرسائل:

- Queue انتقل إلى: علامة التبويب
- تطابق اسم الربط dest_smsc قدم رسالة اختبار مع
- للإرسال Live Status راقب في
- تحقق من تأكيد التسليم

الخيار ب: عبر ملف التكوين

المزايا: البنية التحتية ككود، التحكم في الإصدارات

الخطوات:

1. تحرير ملف التكوين:

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

2. إضافة ربط جديد إلى التكوين:

```
config :omnimessage_smpp, :binds, [  
  # الروابط الحالية...  
  
  # 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. احفظ وأعد تشغيل الخدمة:

```
# حفظ الملف (Ctrl+X, Y, Enter في nano)  
  
# إعادة تشغيل الخدمة  
sudo systemctl restart omnimessage-smpp
```

4. تحقق من الاتصال:

- SMPP → Live Status: انتقل إلى
- ابحث عن الاتصال الجديد
- يجب أن تكون الحالة "متصلة" (باللون الأخضر)
- تحقق من السجلات للحصول على ربط ناجح

5. اختبر تدفق الرسائل:

- Queue انتقل إلى: علامة التبويب   يجب

- تطابق اسم الربط الجديد `dest_smsc` قدم رسالة اختبار مع
- للإرسال Live Status راقب في
- تحقق من تأكيد التسليم

إضافة ربط خادم

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

التحضير:

1. إنشاء بيانات الاعتماد:

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

2. احصل على معلومات الشريك:

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

اختر واحدة من الطرق التالية:

الخيار أ: عبر واجهة الويب (موصى بها)

المزايا: تأثير فوري، لا حاجة لإعادة التشغيل

الخطوات:

1. انتقل إلى نظائر الخادم:

- افتح واجهة الويب: `https://your-server:8087`
- انتقل إلى: SMPP → Server Peers

2. أضف نظير خادم جديد:

- انقر على "إضافة نظير خادم جديد"
- املأ النموذج: ج

- (معرف فريد) partner_acme :الاسم
- معرف النظام: acme_corp
- كلمة المرور: secure_password_123
- أنواع الربط المسموح بها: اختر الكل (جهاز إرسال، جهاز استقبال، جهاز إرسال واستقبال)
- البيضاء: 203.0.113.0/24 (مفصلة بفواصل IP قائمة لعدة)
- TPS: 50 حد
- 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. شارك 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:

- الانتقال إلى SMPP → Live Status
- 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 الإصدارات

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 الخادمة الحالية...

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

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

3. احفظ وأعد تشغيل الخدمة:

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

4. شارك المعلومات مع الشريك:

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

5. انتظر اتصال الشريك:

- انتقل إلى: SMPP → Live Status

- 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 النطائر:

- افتح واجهة الويب: `https://your-server:8087`
- للاتصالات العميلة: SMPP → Client Peers
- للاتصالات الخادمة: SMPP → Server Peers

2. تحرير النطير:

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

3. تطبيق التغييرات على الفور:

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

4. تحقق من التغييرات:

- تحقق من أن الاتصال تم إنشاؤه بنجاح
- للأخطاء Logs راقب علامة التبويب
- اختبر تدفق الرسائل إذا لزم الأمر

الخيار ب: عبر ملف التكوين

المزايا: البنية التحتية ككود، التحكم في الإصدارات

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
- تحديث 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. احفظ وأعد تشغيل الخدمة:

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

4. تحقق من التغييرات:

- SMPP → Live Status: انتقل إلى
- تحقق من أن الاتصال تم إنشاؤه بنجاح

- راقب السجلات للأخطاء
- اختبر تدفق الرسائل

إزالة اتصال

SMPP الغرض: إيقاف تشغيل اتصال

الخطوات:

1. إخطار المعنيين:

- أبلغ الناقل/الشريك
- تنسيق نافذة التوقف

2. قطع الاتصال عبر واجهة الويب:

- انتقل إلى: SMPP → Live Status
- ابحث عن الاتصال
- انقر على "قطع الاتصال"
- أكد الإجراء

3. إزالة التكوين:

- انتقل إلى: SMPP → Client/Server Peers
- ابحث عن الاتصال
- انقر على "حذف"
- أكد الإزالة

4. تحقق من الإزالة:

- يجب أن يكون الاتصال قد اختفى - Live Status تحقق من
 - راجع السجلات لإيقاف التشغيل النظيف
-

إدارة تدفق الرسائل

فحص طابور الرسائل

الغرض: مراقبة الرسائل المعلقة

الخطوات:

1. الوصول إلى الطابور:

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

2. تحقق من تفاصيل الرسالة:

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

3. بحث عن رسالة معينة:

- استخدم فلتر البحث

- SMSC تصفية حسب الوجهة، المحتوى، أو

استكشاف رسائل عالقة

الأعراض: الرسائل لا يتم تسليمها

الخطوات:

1. تحقق من حالة الاتصال:

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

2. تحقق من تفاصيل الرسالة:

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

3. تحقق من محاولات التسليم:

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

4. التدخل اليدوي (إذا لزم الأمر):

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

استكشاف مشكلات الاتصال

إعادة الاتصال برابط

الأعراض: الاتصال يظهر "مفصول" (باللون الأحمر)

الخطوات:

1. تحقق من الاتصال الشبكي:

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

2. تحقق من السجلات للأخطاء:

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

3. تحقق من بيانات الاعتماد:

- الانتقال إلى: SMPP → Client/Server Peers
- وكلمة المرور صحيحة `system_id` تحقق من أن
- اتصل بالناقل إذا كنت غير متأكد

4. إعادة الاتصال اليدوي:

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

5. إذا فشل إعادة الاتصال:

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

التعامل مع فشل المصادقة

الأعراض: فشل الربط المتكرر في السجلات

الأسباب:

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

الخطوات:

1. تحقق من بيانات الاعتماد:

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

2. في القائمة البيضاء IP تحقق من إدراج:

- لجسر الخاص بك مع الناقل IP تأكد من عنوان
- في القائمة البيضاء IP اطلب من الناقل التحقق من إدراج

3. تحقق من حالة الحساب:

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

4. تحديث التكوين:

- إذا تغيرت 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
```

المخرجات المتوقعة:

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

يجب أن تكون جميع القيم ¹ (متصلة).

الاستجابة للتنبيهات

تنبيه الاتصال معطل:

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

تنبيه معدل الفشل العالي:

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

تنبيه عدم وجود حركة مرور:

1. تحقق من أن الطابور الخلفي يحتوي على رسائل.
 2. صحيح `dest_smsc` تحقق من أن توجيهه.
 3. ليست صارمة جدًا TPS تحقق من أن حدود.
 4. راجع إعداد `queue_check_frequency`.
-

إجراءات الصيانة

الصيانة الروتينية

قم بإجراء الصيانة الشهرية:

1. مراجعة المقاييس:

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

2. تحديث الوثائق:

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

3. تدقيق بيانات الاعتماد:

- SMPP مراجعة جميع كلمات مرور
- تخطيط لتدوير بيانات الاعتماد

- البيضاء محدثة IP التحقق من أن قوائم

4. تخطيط السعة:

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

إعادة تشغيل الخدمة

عند الحاجة:

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

الخطوات:

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

# إعادة تشغيل الخدمة
sudo systemctl restart omnimessage-smpp

# تحقق من إعادة التشغيل
sudo systemctl status omnimessage-smpp

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

تحقق عبر واجهة الويب:

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

❖❖ النسخ الاحتياطي للتكوي

قم بعمل نسخ احتياطي للملفات 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
- df -h: تحقق من مساحة القرص
- free -h: تحقق من الذاكرة

5. اتصل بالدعم إذا لم يتم حل المشكلة.

طلبات الناقل لقطع الاتصال الطارئ

الخطوات:

1. قطع الاتصال على الفور:

- SMPP → Live Status: انتقل إلى
- ابحث عن الاتصال المتأثر
- "انقر على "قطع الاتصال"

2. وثق السبب:

- لاحظ اسم الناقل
- سجل الوقت والسبب
- احفظ المراسلات

3. تحقق من المشكلة:

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

4. تنسيق الحل:

- العمل مع الناقل

- تنفيذ الإصلاحات
- اختبار قبل إعادة الاتصال

زيادة حجم الرسائل

الأعراض: حركة مرور رسائل عالية بشكل غير متوقع

الخطوات:

1. TPS تحقق من حدود:

- الانتقال إلى SMPP → Live Status
- تحقق من أن الاتصالات لا تعاني من اختناق
- مؤقتًا TPS قد تحتاج إلى زيادة حدود

2. راقب استقرار الناقل:

- راقب الانقطاعات
- تحقق من معدلات نجاح التسليم

3. تنسيق مع الفريق الخلفي:

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

4. قم بالتوسع 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 مشكلات

- ☐ مراقبة طابور الرسائل لتراكم
- ☐ Prometheus/Grafana تحقق من لوحات
- ☐ %تحقق من أن معدلات نجاح التسليم < 98

المهام الأسبوعية

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

المهام الشهرية

- ☐ تدقيق بيانات الاعتماد
- ☐ مراجعة تخطيط السعة
- ☐ تحديث جهات اتصال الناقل
- ☐ TPS مراجعة وتحسين إعدادات
- ☐ النسخ الاحتياطي لملفات التكوين

الوثائق ذات الصلة

- **CONFIGURATION.md** - تكوين الاتصالات والإعدادات
 - **MONITORING.md** - إعداد تنبيهات Prometheus
 - **TROUBLESHOOTING.md** - حل المشكلات الشائعة
 - **README.md** - نظرة عامة على النظام
-

دليل استكشاف الأخطاء وإصلاحها

المشاكل والحلول الشائعة

OmniMessage مشكلات الاتصال بـ

فإن مشكلات OmniMessage Core، غير متصلة وتعتمد بالكامل على SMPP نظرًا لأن بوابة هي أكثر المشكلات حرجية OmniMessage الاتصال بـ.

OmniMessage أعراض انقطاع الاتصال بـ

- لا توجد رسائل صادرة: تتراكم الرسائل في قائمة الانتظار، ولا يتم إرسال الرسائل
- لا توجد رسائل واردة: لا يمكن للشركاء إرسال الرسائل
- أو تعليقها API أوقات الانتظار: انتهاء مهلة استدعاءات
- إعادة تعيين، "HTTP 503"، "السجلات تظهر: "تم رفض الاتصال"، "انتهاء المهلة الاتصال"

التشخيص

1. OmniMessage تحقق من توفر:

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

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

2. المكون API الخاص بـ URL تحقق من عنوان:

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

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

3. API: تحقق من سجلات البوابة لأخطاء:

```
# API ابحث عن الأخطاء المتعلقة بـ
sudo journalctl -u omnmessage-smpp -f | grep -i
'api\|omnmessage\|connect'

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

الحلول

:معتلاً 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 قواعد جدار الحماية للسماح بـ
2. DNS: nslookup omnmessage-core.example.com تحقق من حل
3. traceroute omnmessage-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/omnmessage-smpp/config/runtime.exs
2. (للإنتاج HTTPS يجب أن يكون) صحيح api_base_url تحقق من أن
3. أعد تشغيل البوابة: sudo systemctl restart omnmessage-smpp

مشكلات الاتصال

الاتصال لا يتم إنشاؤه

الأعراض:

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

الأسباب المحتملة والحلول:

1. مشكلات الاتصال بالشبكة

تحقق:

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

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

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

الحلول:

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

2. بيانات اعتماد غير صحيحة

تحقق:

- "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 يمنع

تحقق:

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

# تحقق من UFW (Ubuntu/Debian)
sudo ufw status | grep 2775

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

الحلول:

```
# Ubuntu/Debian
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 إنشاؤه 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 مشكلات الشبكة
- تحقق مع مزود خدمة الإنترنت إذا كانت المشكلة من جانبك
- النظر في اتصال/مسار احتياطي

2. انتهاء مهلة استعلام الرابط

تحقق:

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

الحلول:

- المهلة الافتراضية هي 30 ثانية
- keepalive تحقق من أن ال  بكة تسمح بحزم
- تحقق من جدران الحماية العدوانية التي تنهي الاتصالات الخاملة

3. تجاوز حد TPS

تحقق:

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

الحلول:

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

4. مشكلات خادم الناقل

تحقق:

- تحقق من حالة خدمة الناقل
- اتصل بدعم الناقل

الحلول:

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

مشكلات تسليم الرسائل

الرسائل لا تُرسل

الأعراض:

- الرسائل عالقة في قائمة الانتظار
- لا يزيد `smpplib_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 المباشرة → SMPP قارن مع اسم الاتصال في

❖❖ حلول:

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

2. الرسائل المجدولة للمستقبل

تحقق:

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

التفسير:

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

الحلول:

- الانتظار 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
- إرسال الرسائل ببطء شديد

الحلول:

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

4. عامل قائمة الانتظار غير قيد التشغيل

تحقق:

- حالة الخدمة
- السجلات للأخطاء

الحلول:

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

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

معدل فشل التسليم مرتفع

الأعراض:

- في زيادة `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 الأخطاء المحددة
- مراجعة تنسيق وجهة الرسالة

أكواد الأخطاء الشائعة:

- 0x0000000B - وجهة غير صالحة
- 0x00000001 - طول رسالة غير صالح
- 0x00000003 - أمر غير صالح

الحلول:

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

2. محتوى الرسالة غير صالح

تحقق:

- طول الرسالة
- الأحرف الخاصة
- الترميز

الحلول:

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

3. رفض الناقل

تحقق:

- أكواد الأخطاء المحددة من الناقل
- أنماط في الرسائل المرفوضة

الحلول:

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

4. الرسائل منتهية الصلاحية

تحقق:

- للرسالة `expires` الطابع الزمني
- توقيت محاولة التسليم

الحلول:

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

مشكلات واجهة الويب

لا يمكن الوصول إلى لوحة التحكم على الويب

الأعراض:

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

الأسباب المحتملة والحلول:

1. الخدمة غير قيد التشغيل

تحقق:

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

الحلول:

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

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

2. جدار الحماية يمنع المنفذ 8087

تحقق:

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

الحلول:

```
# Ubuntu/Debian
sudo ufw allow 8087/tcp

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

3. SSL مشكلات شهادة

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 (وليس HTTPS) تحقق من استخدام
- اسم المضيف الصحيح/IP تحقق من عنوان
- تحقق من المنفذ 8087

واجهة الويب تظهر أخطاء

الأعراض:

- الصفحة يتم تحميلها 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 التحكم في المتصفح:

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

3. جرب متصفحًا مختلفًا:

- Chrome وFirefox وEdge اختبر في
- عزل المشكلات الخاصة بالمتصفح

4. تحقق من سجلات الخدمة:

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

مشكلات القياسات

غير متاحة Prometheus قياسات

الأعراض:

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

الأسباب المحتملة والحلول

1. الخدمة غير قيد التشغيل

تحقق:

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

الحلول:

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

2. المنفذ غير متاح

تحقق:

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

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

الحلول:

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

3. نقطة النهاية خاطئة

تحقق:

- `/stats` أو `/prometheus` وليس `/metrics` نقطة النهاية هي
- المنفذ هو 4000 (وليس 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 أول حدث

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

3. قياسات قديمة:

- قد تظهر الروابط القديمة في القياسات
- أعد تش❓❓يل الخدمة لمسح الإدخالات القديمة
- للتصفية Prometheus أو استخدم إعادة تسمية

مشكلات الأداء

مرتفع CPU استخدام

تحقق:

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

الأسباب المحتملة:

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

الحلول:

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

استخدام الذاكرة مرتفع

تحقق:

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

الأسباب المحتملة:

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

الحلول:

- أعد تشغيل الخدمة لمسح الذاكرة
- تحقق من حجم قائمة انتظار الرسائل
- اتصل بالدعم إذا كانت الذاكرة تنمو باستمرار

معالجة الرسائل ببطء

الأعراض:

- تستغرق الرسائل وقتًا طويلًا للإرسال
- تراكم قائمة الانتظار
- معدل رسائل منخفض

تحقق:

1. قد تكون صارمة جدًا - TPS حد ∞ د
2. `queue_check_frequency` مرتفعة جدًا
3. الخلفية - قد يكون بطيئًا API وقت استجابة
4. تأخير الشبكة إلى الناقل

الحلول:

- إذا سمح الناقل بذلك TPS زيادة
 - لزيادة سرعة الاستطلاع `queue_check_frequency` تقليل
 - الخلفية API تحسين
 - تحقق من تأخير الشبكة
-

مشكلات 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 بناء الجملة بعناية
- Elixir استخدام محرر نصوص مع تمييز بناء جمل

التغييرات لا تؤثر

الأعراض:

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

# تحميل CPU
uptime
```

2. تحقق من حالة الخدمة:

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

3. راجع السجلات الأخيرة:

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

4. حاول إعادة تشغيل الخدمة:

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

5. إذا فشلت إعادة التشغيل:

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

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

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

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

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 بتطهير 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 المعلومات من أعلاه

الوثائق ذات الصلة

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

