مرجع التكوين

دليل كامل لجميع معلمات التكوين

نظرة عامة على المعمارية

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

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

هذا هو نفس الطريقة التي تعمل بها واجهات OmniMessage الأخرى (Diameter، MAP، IMS) - جميعها مترجمات بروتوكول بدون حالة تفوض إلى OmniMessage Core.

موقع ملف التكوين

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

مهم: بعد تغيير التكوين، أعد تشغيل البوابة:

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

هيكل التكوين

يستخدم ملف التكوين بناء جملة Elixir. الهيكل الأساسي:

```
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`	سلسلة (URL)	نعم	-

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

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

تقوم البوابة ببساطة بترجمة تنسيق SMPP ↔ OmniMessage.

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:

- يجب أن تكون البوابة لديها وصول إلى الشبكة إلى OmniMessage Core
- استخدم HTTPS في الإنتاج (قم بتكوين `verify_ssl_peer`)
- يجب أن يسمح جدار الح��اية بالاتصالات الصادرة عبر HTTPS على المنفذ المحدد

SMPP_POLL_INTERVAL

تكرار فحص قائمة الانتظار (بالملي ثانية)

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

المعلمة	النوع	مطلوب	الافتراضي
`smpp_poll_interval`	عدد صحيح	لا	100

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

التحقق من شهادة SSL

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

المعلمة	النوع	مطلوب	الافتراضي
`verify_ssl_peer`	بولياني	لا	false

الغرض: ما إذا كان يجب التحقق من شهادات SSL عند الاتصال بواجهة برمجة التطبيقات الخلفية.

القيم:

- `true`: (الإنتاج مع شهادات صالحة) تحقق من الشهادات
- `false`: (شهادات موقعة ذاتيًا، اختبار) تخط�ّ التحقق

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`

تكوين ربط عميل SMPP

(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,

    # عنوان خادم SMPP لشركة النقل
    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
  }
]
```

معلمات ربط العميل

name

معرف الاتصال الفريد

النوع	مطلوب	مثال
سلسلة	نعم	`"vodafone_uk"`

الغرض: يحدد هذا الاتصال SMPP بشكل فريد.

- 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`

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

القيمة الثابتة: دائمًا `:client` للاتصالات الصادرة.

bind_type

نوع جلسة SMPP

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

الغرض: يحدد قدرة اتجاه الرسالة.

الخيارات:

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

التوصية: استخدم `:transceiver` ما لم تتطلب شركة النقل نوعًا محددًا.

host

اسم المضيف أو IP لخادم SMPP لشركة النقل

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

الغرض: عنوان خادم SMPP لشركة النقل.

أمثلة:

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

port

منفذ خادم SMPP

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	نعم	2775	1-65535

الغرض: منفذ TCP لاتصال SMPP.

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��ت

أمثلة:

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

الحساب:

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

queue_check_frequency

فترة استعلام قائمة الانتظار (بالملي ثانية)

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	نعم	1000	100-10000

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

إرشادات:

- **حجم عالي (>100 TPS)**: 500-1000ms
- **حجم متوسط (10-100 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:

تكوين ربط خادم SMPP

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

معلمات 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

عناوين IP المسموح بها للعميل

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

الغرض: الأمان - السماح فقط بالاتصالات من IPs المعروفة.

التنسيقات:

- فردي: `"192.168.1.100"` (بشكل تلقائي `/32`) IP
- CIDR: شبكة `"10.0.0.0/8"`، `"192.168.1.0/24"`
- مزيج من الاثنين: `["10.50.1.100" ,"192.168.1.0/24"]`

أمثلة:

```
# السماح بأي IP (غير موصى به)
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:

- `/32` - IP فردي (بدون IPs تلقائي لـ ناع��)
- `/24` - 256 عنوان (مثل 192.168.1.0-255)
- `/16` - 65,536 عنوان (مثل 10.50.0.0-255.255)
- `/8` - 16,777,216 عنوان (مثل 10.0.0.0-255.255.255.255)

tps_limit

حد الرسائل في الثانية

يتحكم في معدل `tps_limit` لربط العميل - نفس deliver_sm الصادر.

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
}
```

معلمات الاستماع

host

عنوان IP للربط به

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"` - الاستماع على localhost فقط (اختبار)
- `"192.168.1.10"` - الاستماع على IP محدد

port

منفذ TCP للاستماع عليه

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	لا	2775	1-65535

الغرض: المنفذ للاتصالات الواردة عبر SMPP.

القياسي: 2775

max_connections

الحد الأقصى للاتصالات المتزامنة

النوع	مطلوب	الافتراضي	النطاق
عدد صحيح	لا	100	1-10000

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://smsc.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://smsc.company.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://smsc.company.com:8443"

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

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

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

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، سترى 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
```

اضغط `Ctrl+C` مرتين للخروج.

أفضل ممارسات الأمان

1. **احمِ 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. **استخدم قوائم IP البيضاء**:
   - قم دائمًا بتكوين `ip_whitelist` لعمليات الربط بالخادم
   - لا تستخدم قائمة فارغة `[]` في الإنتاج
4. **قم بتمكين التحقق من SSL**:
   - اضبط `verify_ssl_peer: true` مع شهادات صالحة
5. **تدوير بيانات الاعتماد بشكل منتظم**:
   - تغيير كلمات المرور كل ثلاثة أشهر
   - التنسيق مع شركات النقل/الشركاء

الخطوات التالية

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

المعجم

المصطلحات والتعريفات

أ

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

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

ب

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

Bind اتصال SMPP بين نظامين. يمكن أن يكون مرسلًا أو مستقبلًا أو جهاز إرسال واستقبال.

Bind Type نوع جلسة SMPP:

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

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

ج

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

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

Connection Status الحالة الحالية لارتباط SMPP:

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

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

د

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

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.

dest_smsc حقل في قائمة الرسائل SMPP يجب أن يتعامل مع يشير إلى أي اتصال الرسا��ة.

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

هـ

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

ESM Class حقل SMPP يشير إلى نوع الرسالة وميزاتها.

ESME (كيان الرسائل القصيرة الخارجي) في مصطلحات SMPP، التطبيق العميل الذي 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 ESMEs.

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 تطبيق بوابة SMPP الذي يربط بين قائمة الرسائل والشبكات المحمولة.

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

Grafana أداة تصور شائعة لعرض مقاييس Prometheus في لوحات المعلومات.

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

ح

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

ط

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

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

ي

(لا توجد مصطلحات)

ك

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

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

ل

Label في Prometheus، أزواج مفتاح-قيمة مرتبطة بالمقاييس للتعريف (على سبيل المثال، `bind_name="vodafone_uk"`).

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

م

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

Metrics قياسات كمية لأداء النظام، تُعرض بتنسيق Prometheus.

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

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

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

ن

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

هـ

Outbound رسائل تتدفق من البوابة إلى الشبكات المحمولة.

Inbound رسائل تتدفق من الشبكات المحمولة إلى البوابة.

ص

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

Prometheus نظام مراقبة مفتوح المصدر يجمع ويخزن مقاييس السلاسل الزمنية.

ق

Queue قائمة الرسائل التي تنتظر المعالجة أو الإرسال.

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

Queue Worker مكون يسترجع الرسائل من القائمة ويرسلها عبر SMPP.

ر

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

Receiver نوع ارتباط SMPP يستقبل الرسائل فقط (deliver_sm).

Reconnect إعادة إنشاء اتصال SMPP مفصول.

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

س

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

Session اتصال SMPP نشط بين نظامين.

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

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

SSL/TLS بروتوكولات التشفير للتواصل الآمن.

Submit_SM PDU SMPP لتقديم رسالة للتسليم.

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

System ID اسم المستخدم المستخدم لمصادقة SMPP.

ط

Telemetry جمع ونقل تلقائي لمقاييس النظام.

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

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

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

Transmitter نوع ارتباط SMPP يرسل الرسائل فقط (submit_sm).

Throughput معدل معالجة الرسائل، يقاس عادةً بالرسائل في الثانية.

ع

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

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 انظر IP Whitelist.

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

مرجع كامل لمراقبة بوابة SMPP

نظرة عامة

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

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

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

نقطة نهاية القياسات

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

التنسيق: تنسيق نص Prometheus

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

اختبار سريع

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

القياسات المتاحة

تبدأ جميع القياسات بـ `smpp_` وتتضمن تسميات للتعريف.

قياسات الترخيص

omnimessage_smpp_license_status

النوع: Gauge
الوصف: حالة الترخيص الحالية
القيم:

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

التسميات: لا شيء

مثال:

```
omnimessage_smpp_license_status 1
```

الاستخدام:

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

اسم المنتج: `omnimessage_smpp`

ملاحظات:

- تتوقف البوابة عن معالجة قوائم الانتظار الصادرة، عندما يكون الترخيص غير صالح (`license_status == 0`)
- تظل اتصالات SMPP (كل من العميل والخادم) متصلة وتقبل طلبات الربط
- 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: "ترخيص بوابة SMPP غير صالح أو منتهي"
    description: "حالة الترخيص غير صالحة - معالجة الرسائل الصادرة
محظورة"
```

قياسات حالة الاتصال

smpp_connection_status

النوع: Gauge
الوصف: حالة الاتصال الحالية لربط SMPP
القيم:

- `1` = متصل
- `0` = غير متصل

التسميات:

- `bind_name` - اسم الاتصال (مثل "vodafone_uk")
- `mode` - نوع الاتصال ("server" أو "client")
- `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="sm
1
```

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

التسميات: نفس قياسات حالة الاتصال

مثال:

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

الاستخدام:

- مراقبة حجم الرسائل الواردة
- تتبع حركة المرور المنبعثة من الهواتف المحمولة (MO)
- 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 المشكلة

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
الوصف: وقت التشغيل الحالي لربط SMPP بالثواني
الوحدة: ثواني

مثال:

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

الاستخدام:

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

قياسات صحة OmniMessage API

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

من قياسات OmniMessage (إذا كانت متاحة)

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

من سجلات البوابة (إذا لم يتم عرض القياسات)

ابحث عن هذه الأنماط لاكتشاف مشاكل API:

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

تكوين Prometheus

تكوين سحب أساسي

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

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

بوابات متعددة

```yaml
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:

```yaml
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"
    }
  }
]
```

لوحات معلومات Grafana

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

التصور: Gauge
الوحدة: نسبة مئوية (0-100)
الحدود:

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

لوحة وقت تشغيل الاتصال

الاستعلام:

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

التصور: Stat
الوحدة: ساعات

قواعد التنبيه

قواعد تنبيه Prometheus

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

```yaml
groups:
  - name: smpp_gateway
    interval: 30s
    rules:
      # الاتصال معطل
      - alert: SMPPConnectionDown
        expr: smpp_connection_status == 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "الاتصال SMPP {{ $labels.bind_name }} معطل"
          description: "الاتصال {{ $labels.bind_name }} تم فصله لأك��ر 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: "{{ $labels.bind_name }} فشل في الربط {{ $value }} دقائق في آخر 10 مرات."

      # لا توجد رسائل مرسلة (عند المتوقع)
```

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

      # فقدان الاتصال المتكرر
      - alert: SMPPFrequentDisconnections
        expr: increase(smpp_disconnection_total[1h]) > 5
        labels:
          severity: warning
        annotations:
          summary: "فقدان الاتصال المتكرر على {{ $labels.bind_name
}}"
          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: "لا تستطيع الوصول إلى بوابة SMPP بـ OmniMessage
API. تحقق من تكوين API_BASE_URL والاتصال بالشبكة."

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

```
          summary: "OmniMessage API تعاني من مهلات"
          description: "قد تكون API. تم اكتشاف عدة مهلات
OmniMessage بطيئة أو مثقلة."

      # لا توجد تدفقات رسائل (مشكلة API)
      - 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
دقيقة. تحقق من الاتصال بـ OmniMessage API وحالة قائمة الانتظار."
```

قم بتحميل القواعد في `prometheus.yml`:

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

مراقبة لوحة المعلومات على الويب

تقدم واجهة الويب المدمجة مراقبة في الوقت الحقيقي دون Prometheus.

الوصول

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

صفحة الحالة الحية

التنقل: SMPP → الحالة الحية

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

مؤشرات الأداء الرئيسية (KPIs)

صحة الاتصال

المقياس: نسبة وقت تشغيل الاتصال

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

الهدف: > 99.9%

معدل تسليم الرسائل

المقياس: الرسائل المرسلة 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

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

2. إنشاء لوحات المعلومات

- بناء لوحات معلومات Grafana لكل بوابة

- 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
- توثيق معدلات TPS المتوقعة
- ملاحظة أوقات/أيام الذروة

5. الربط مع الخلفية

- مراقبة قياسات API الخلفية
- 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 المشكلة

الإنتاجية المنخفضة

تحقق: معدل `smpp_messages_sent_total`

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

مشاكل الربط

تحقق: `smpp_bind_failures_total`

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

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

الاعتماد الحرج: OmniMessage Core

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

إذا أصبح OmniMessage غير متاح:

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

تحقق من صحة OmniMessage:

```
# 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**

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

3. **مراجعة مقاييس الرسائل**

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

4. **تحقق من سجلات النظام**

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

5. **مراجعة مقاييس Prometheus**

   - `curl http://localhost:4000/metrics`
   - أو تحقق من لوحات Grafana
   - 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

انظر MONITORING.md لتكوين التنبيهات.

إدارة اتصالات SMPP

كيفية تكوين نظائر SMPP

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

الطريقة 1: واجهة الويب (موصى بها)

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

الطريقة 2: ملف التكوين

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

انظر CONFIGURATION.md للرجوع إلى ملف التكوين.

إضافة اتصال عميل جديد

الناقل (خادم) **SMSC** يتصل بـ (عميل) **ESME** **الغرض**: تكوين الجسر للعمل كـ

التحضير: جمع المعلومات من الناقل:

- اسم مضيف/عنوان IP خادم SMPP
- رقم المنفذ (عادةً 2775)
- معرف النظام (اسم المستخدم)
- كلمة المرور
- نوع الربط (عادةً جهاز إرسال واستقبال)
- 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 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:
        - **الاسم**: `vodafone_uk` (معرف فريد)
        - **المضيف**: `smpp.vodafone.co.uk`
        - **المنفذ**: `2775`
        - **معرف النظام**: `your_username`
        - **كلمة المرور**: `your_password`
        - **نوع الربط**: `Transceiver`

        - **حد TPS**: `100`
        - **تكرار فحص الطابور**: `1000`
    - انقر على "حفظ"

3. **يتم إنشاء الاتصال تلقائيًا**:
    - يحاول الجسر الاتصال على الفور
    - انتقل إلى: SMPP → Live Status
    - يجب أن تتغير الحالة إلى "متصل" (باللون الأخضر) خلال 10-30 ثانية
    - تحقق من علامة التبويب Logs للحصول على رسالة ربط ناجحة

4. **اختبر تدفق الرسائل**:
    - انتقل إلى علامة التبويب Queue
    - قدم رسالة اختبار مع `dest_smsc` تطابق اسم الربط
    - راقب في Live Status للإرسال
    - 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**:

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

5. **اختبر تدفق الرسائل**:

   - انتقل إلى: علامة التب�يب Queue

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

إضافة ربط خادم

الغرض SMSC يقبل الاتصالات من (خادم) **ESMEs** (عملاء الشركاء): 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
   - حجم الرسائل المتوقع (لحد TPS)
   - 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 النمو��ج:

- **الاسم**: `partner_acme` (معرف فريد)
- **معرف النظام**: `acme_corp`
- **كلمة المرور**: `secure_password_123`
- **أنواع الربط المسموح بها**: اختر الكل (جهاز إرسال، جهاز استقبال، جهاز إرسال واستقبال)
- **قائمة IP البيضاء**: `203.0.113.0/24` (مفصولة بفواصل لعدة)
- **حد TPS**: `50`
- **تكرار فحص الطابور**: `1000`

- انقر على "حفظ"

3. **الجسر جاهز للاتصال**:

   - أصبح نظير الخادم نشطًا الآن وينتظر اتصال الشريك
   - لا حاجة لإعادة التشغيل

4. **شارك المعلومات مع الشريك**:

   - عنوان IP للجسر
   - المنفذ: `2775`
   - معرف النظام: `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
- تحقق من تطابق IP مع القائمة البيضاء

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**:

```
# أضف 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**:

   - عنوان IP للجسر
   - 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
- تحقق من تطابق IP مع القائمة البيضاء

تعديل اتصال موجود

الغرض: تحديث معلمات الاتصال (حدود TPS، قائمة IP البيضاء، كلمات المرور، إلخ.)

اختر واحدة من الطرق التالية:

الخيار أ: عبر واجهة الويب (موصى بها)

المزايا: تأثير فوري، لا حاجة لإعادة التشغيل

الخطوات:

1. **انتقل إلى النظائر**:
   - افتح واجهة الويب: `https://your-server:8087`
   - للاتصالات العميلة: SMPP → Client Peers
   - للاتصالات الخادمة: SMPP → Server Peers
2. **تحرير النظير**:
   - ابحث عن النظير الذي تريد تعديله
   - انقر على زر "تحرير"
   - تحديث المعلمات المطلوبة:
     - التغييرات الشائعة: حد TPS، قائمة IP البيضاء، كلمة المرور، المضيف/المنفذ
   - انقر على "حفظ"
3. **تطبق التغييرات على الفور**:
   - يعيد الاتصال الاتصال تلقائيًا بالإعدادات الجديدة
   - لا حاجة لإعادة تشغيل الخدمة
   - للتحقق انتقل إلى: SMPP → Live Status
4. **تحقق من التغييرات**:

- تحقق من أن الاتصال تم إنشاؤه بنجاح
- راقب علامة التبويب Logs للأخطاء
- 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 معلمات الربط**:

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

```
%{
  name: "vodafone_uk",
  # ... معلمات 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**:

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

- راقب السجلات للأخطاء
- اختبر تدفق الرسائل

إزالة اتصال

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

إدارة تدفق الرسائل

فحص طابور الرسائل

الغرض: مراقبة الرسائل المعلقة

ال��طوات:

1. **الوصول إلى الطابور**:
    - انتقل إلى: علامة التبويب Queue
    - 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. **بحث عن رسالة معينة**:
    - استخدم فلتر البحث

- تصفية حسب الوجهة، المحتوى، أو SMSC

استكشاف رسائل عالقة

الأعراض: الرسائل لا يتم تسليمها

الخطوات:

1. **تحقق من حالة الاتصال**:
   - انتقل إلى: SMPP → Live Status
   - تحقق من أن الاتصال المستهدف متصل
   - إذا كان مفصولًا، انظر إعادة الاتصال
2. **تحقق من تفاصيل الرسالة**:
   - انتقل إلى: علامة التبويب Queue
   - ابحث عن الرسالة العالقة
   - تحقق من أن حقل `dest_smsc` يتطابق مع اسم الاتصال
   - تحقق من طابع `deliver_after` (جدولة إعادة المحاولة)
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**:

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

3. **تحقق من بيانات الاعتماد**:

   - انتقل إلى: SMPP → Client/Server Peers
   - تحقق من أن `system_id` وكلمة المرور صحيحة
   - 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
- IP غير مدرج في القائمة البيضاء لدى الناقل
- الحساب معلق/منتهي

الخطوات:

1. **تحقق من بيانات الاعتماد**:
   - انتقل إلى: SMPP → Client Peers
   - تحقق مرة أخرى من `system_id` وكلمة المرور
   - تأكد مع الناقل
2. **تحقق من إدراج IP في القائمة البيضاء**:
   - تأكد من عنوان IP الخاص بك مع الناقل لجسر
   - اطلب من الناقل التحقق من إدراج IP في القائمة البيضاء
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

التحقق من مقاييس Prometheus

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. تحقق من واجهة الويب → SMPP → Live Status
2. حاول إعادة الاتصال يدويًا
3. تحقق من السجلات للأخطاء
4. اتصل بالناقل إذا كانت الانقطاع لفترة طويلة
5. انظر TROUBLESHOOTING.md

تنبيه معدل الفشل العالي:

1. تحقق من السجلات 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. تحقق من أن توجيه `dest_smsc` صحيح
3. تحقق من أن حدود TPS ليست صارمة جدًا
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**:
    - مراجعة جميع كلمات مرور SMPP
    - تخطيط لتدوير بيانات الاعتماد

- التحقق من أن قوائم IP البيضاء محدثة

4. **تخطيط السعة**:
   - مراجعة معدلات الرسائل القصوى
   - تحقق من حدود TPS
   - 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. انتقل 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
   - تحقق من وجود شهادات SSL
   - تحقق من مساحة القرص: `df -h`
   - تحقق من الذاكرة: `free -h`

5. إذا لم يتم حل المشكلة **اتصل بالدعم**

طلبات الناقل لقطع الاتصال الطارئ

الخطوات:

1. **قطع الاتصال على الفور**:

   - انتقل إلى: SMPP → Live Status
   - 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. **تحقق من حدود TPS**:
   - انتقل إلى: SMPP → Live Status
   - تحقق من أن الاتصالات لا تعاني من اختناق
   - قد تحتاج إلى زيادة حدود TPS مؤقتًا
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

- [ ] تحقق من أن جميع اتصالات SMPP متصلة
- [ ] مراجعة سجلات الأخطاء لأي مشكلات

- [ ] مراقبة طابور الرسائل لتراكم
- [ ] تحقق من لوحات Prometheus/Grafana
- [ ] 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
- [ ] مراجعة وتحسين إعدادات TPS
- [ ] 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

مشكلات الاتصال بـ OmniMessage

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

أعراض انقطاع الاتصال بـ OmniMessage

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

التشخيص

1. تحقق من توفر OmniMessage:

```
# 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. تحقق من عنوان URL الخاص بـ API المكون:

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

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

3. تحقق من سجلات البوابة لأخطاء API:

```
# ابحث عن الأخطاء المتعلقة بـ API
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

إذا كان OmniMessage معطلاً:

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

إذا كان OmniMessage يعمل ولكن البوابة لا تستطيع الوصول إليه:

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

إذا كان عنوان URL الخاص بـ API غير مكون بشكل صحيح:

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

- إذا فشل DNS: استخدم عنوان IP بدلاً من اسم المضيف في التكوين
- إذا فشل ping: تحقق من قواعد جدار الحماية، اتصل بالناقل
- 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"
- واجهة الويب: SMPP → تحقق من أقران العملاء system_id وكلمة المرور

الحلول:

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

3. عنوان IP غير مدرج في القائمة البيضاء

تحقق:

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

الحلول:

- تأكيد عنوان IP العام للبوابة الخاصة بك:
  ```
  curl ifconfig.me
  ```
- طلب من الناقل إضافة IP إلى القائمة البيضاء
- تحقق من أن IP لم يتغير (IP ديناميكي)

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
- تحقق من أن ال keepalive بكة تسمح بحزم ال
- 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:

- مراجعة إعداد `tps_limit`
- تقليل TPS إلى 70-80% من الحد الأقصى للناقل
- 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
- `smpp_messages_sent_total` لا يزيد
- الاتصال يظهر متصل

الأسباب المحتملة والحلول:

1. توجيه dest_smsc خاطئ

تحقق:

- للرسالة `dest_smsc` واجهة الويب ← قائمة الانتظار ← تحقق من حقل
- الحالة المباشرة ← SMPP قارن مع اسم الاتصال في

��لحلول:

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

2. الرسائل المجدولة للمستقبل

تحقق:

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

التفسير:

- للرسائل 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. حد TPS منخفض جدًا

تحقق:

- تراكم كبير في قائمة الانتظار
- إرسال الرسائل ببطء شديد

الحلول:

- زيادة `tps_limit` في التكوين
- تحقق من أن الناقل يمكنه التعامل مع معدل أعلى
- انظر CONFIGURATION.md

4. عامل قائمة الانتظار غير قيد التشغيل

تح��ق:

- 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:

- `smpp_delivery_failures_total` في زيادة
- السجلات تظهر "submit_sm_resp" مع حالة خطأ

- 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:

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

2. محتوى الرسالة غير صالح

تحقق:

- طول الرسالة
- الأحرف الخاصة
- الترميز

الحلول:

- GSM-7: الحد الأقصى 160 حرفًا
- UCS-2: الحد الأقصى 70 حرفًا
- 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:

- الطابع الزمني `expires` للرسالة
- 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. مشكلات 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. عنوان URL خاطئ

تحقق:

- تحقق من استخدام HTTPS (وليس HTTP)
- تحقق من عنوان IP/اسم المضيف الصحيح
- 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**:
    - اضغط على F12
    - تحقق من علامة تبويب وحدة التحكم لأخطاء JavaScript
    - أبلغ الدعم إذا تم العثور على أخطاء
3. **جرب متصفحًا مختلفًا**:
    - اختبر في Chrome وFirefox وEdge
    - عزل المشكلات الخاصة بالمتصفح

4. **تحقق من سجلات الخدمة**:

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

مشكلات القياسات

قياسات Prometheus غير متاحة

الأعراض:

- `curl http://localhost:4000/metrics` يفشل
- Prometheus لا يمكنه جمع القياسات
- 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
- افتح المنفذ 4000 في جدار الحماية لخادم Prometheus

3. نقطة النهاية خاطئة

تحقق:

- نقطة النهاية هي `/metrics` (وليس `/prometheus` أو `/stats`)
- 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
    - استخدم `increase()` أو `rate()` في استعلامات Prometheus
2. **الروابط الجديدة لا تظهر**:
    - تظهر القياسات فقط بعد أول حدث

- أرسل رسالة اختبار لتعبئة القياسات
- تحقق من أن الربط مفعل ومتصل

3. **قياسات قديمة**:

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

مشكلات الأداء

استخدام CPU مرتفع

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
- مراجعة حدود TPS
- اتصل بالدعم إذا كان استخدام CPU مرتفعًا بشكل مستمر

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

الحلول:

- إذا سمح الناقل بذلك TPS زيادة
- تقليل `queue_check_frequency` لزيادة سرعة الاستطلاع
- تحسين API الخلفية
- 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:

```
# تحقق من بناء جملة Elixir
/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
- مفقود `import Config` في الأعلى

الحلول:

- استعادة من النسخة الاحتياطية
- مراجعة بناء الجملة بعناية
- استخدام محرر نصوص مع تمييز بناء جمل Elixir

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
   - تحقق من وجود شهادات SSL
   - 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
# تحرير /tmp/config.exs لإزالة كلمات المرور قبل الإرسال
```

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
- **الهاتف**: +61 XXXX XXXX (24/7)
- **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