Referencia de Configuración

Guía completa de todos los parámetros de configuración

Descripción General de la Arquitectura

El Gateway SMPP de OmniMessage es un **frontend de protocolo sin estado** que traduce mensajes SMPP hacia/desde OmniMessage. Toda la lógica de negocio, decisiones de enrutamiento y almacenamiento de mensajes son manejados por OmniMessage Core - el gateway simplemente:

1. **Recibe** PDUs SMPP de transportistas y clientes
2. **Traduce** a formato OmniMessage a través de la API REST
3. **Consulta** a OmniMessage por mensajes para enviar
4. **Envía** PDUs SMPP a transportistas
5. **Informa** el estado de entrega de vuelta a OmniMessage

Esto es idéntico a cómo funcionan otros frontends de OmniMessage (Diameter, MAP, IMS) - todos son traductores de protocolo sin estado que delegan a OmniMessage Core.

Ubicación del Archivo de Configuración

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

Importante: Después de cambiar la configuración, reinicie el gateway:

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

Estructura de Configuración

El archivo de configuración utiliza la sintaxis de Elixir. Estructura básica:

```
import Config

# Configuraciones globales
config :omnimessage_smpp,
  setting_name: value

# Vínculos SMPP
config :omnimessage_smpp, :binds, [
  %{
    name: "bind_name",
    # ... configuraciones de vínculo
  }
]
```

Configuraciones Globales

API_BASE_URL

URL de la plataforma OmniMessage Core

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

Parámetro	Tipo	Requerido	Predeterminado
`api_base_url`	String (URL)	Sí	-

Propósito: URL de la plataforma OmniMessage Core. El gateway se comunica con OmniMessage a través de la API REST para todo el procesamiento de mensajes:

- **Enviar Mensajes**: Enviar mensajes SMPP recibidos a OmniMessage para su procesamiento
- **Recuperar Mensajes**: Consultar mensajes destinados a transportistas SMPP
- **Informar Estado de Entrega**: Actualizar el estado de entrega de mensajes de vuelta a OmniMessage
- **Salud del Sistema**: Chequeos de salud periódicos

Crítico: Aquí es donde el gateway obtiene toda su "inteligencia". OmniMessage maneja:

- ✓ Validación de mensajes y verificación de formato
- ✓ Decisiones de enrutamiento (qué transportista usar)
- ✓ Limitación de tasa y control de flujo
- ✓ Validación de números
- ✓ Almacenamiento y persistencia de mensajes
- ✓ Lógica de reintento de entrega
- ✓ Seguimiento de estado

El gateway simplemente traduce el formato SMPP ↔ OmniMessage.

Ejemplos:

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

# HTTPS con nombre de host
api_base_url: "https://omnimessage-core.company.com:8443"

# HTTP (no recomendado para producción)
api_base_url: "http://192.168.1.100:8080"
```

Requisitos de Red:

- El gateway debe tener acceso a la red de OmniMessage Core
- Usar HTTPS en producción (configurar `verify_ssl_peer`)
- El firewall debe permitir HTTPS saliente en el puerto especificado

SMPP_POLL_INTERVAL

Frecuencia de verificación de la cola (milisegundos)

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

Parámetro	Tipo	Requerido	Predeterminado
`smpp_poll_interval`	Entero	No	100

Propósito: Con qué frecuencia (en milisegundos) cada cliente verifica la cola de mensajes.

Directrices:

- **Alto volumen (>100 TPS)**: 100-500ms
- **Volumen medio (10-100 TPS)**: 500-1000ms
- **Bajo volumen (<10 TPS)**: 1000-2000ms

Variable de entorno: `SMPP_POLL_INTERVAL`

VERIFY_SSL_PEER

Verificación del certificado SSL

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

Parámetro	Tipo	Requerido	Predeterminado
`verify_ssl_peer`	Booleano	No	false

Propósito: Si se debe verificar los certificados SSL al conectarse a la API de backend.

Valores:

- `true`: Verificar certificados (producción con certificados válidos)
- `false`: Omitir verificación (certificados autofirmados, pruebas)

Variable de entorno: `VERIFY_SSL_PEER`

SMSC_NAME

Identificador del gateway para registro

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

Parámetro	Tipo	Requerido	Predeterminado
`smsc_name`	String	No	"smpp_gateway"

Propósito: Identifica esta instancia de gateway en el backend de la cola de mensajes.

Variable de entorno: `SMSC_NAME`

Configuración de Vínculo del Cliente SMPP

Los vínculos del cliente son **conexiones salientes** donde el gateway actúa como un **ESME** (cliente) conectándose a servidores **SMSC** de transportistas. En este modo, el gateway inicia la conexión para enviar y recibir mensajes a través de transportistas externos.

Ejemplo Completo de Vínculo del Cliente

```
config :omnimessage_smpp, :binds, [
  %{
    # Identificador único para esta conexión
    name: "vodafone_uk",

    # Modo de conexión
    mode: :client,

    # Tipo de vínculo SMPP
    bind_type: :transceiver,

    # Dirección del servidor SMPP del transportista
    host: "smpp.vodafone.co.uk",
    port: 2775,

    # Credenciales de autenticación
    system_id: "your_username",
    password: "your_password",

    # Limitación de tasa
    tps_limit: 100,

    # Frecuencia de verificación de la cola
    queue_check_frequency: 1000
  }
]
```

Parámetros del Vínculo del Cliente

name

Identificador único de conexión

Tipo	Requerido	Ejemplo
String	Sí	`"vodafone_uk"`

Propósito: Identifica de manera única esta conexión SMPP.

- Usado en registros y métricas
- Debe ser único entre todos los vínculos
- Usar nombres descriptivos (transportista, región, propósito)

Convenciones de nomenclatura:

- `transportista_región`: `"vodafone_uk"`, `"att_us"`
- `propósito_número`: `"marketing_1"`, `"alerts_primary"`

mode

Tipo de conexión

Tipo	Requerido	Valor
Átomo	Sí	`:client`

Propósito: Define esto como una conexión saliente donde el gateway actúa como un **ESME** conectándose a un **SMSC** externo.

Valor fijo: Siempre `:client` para conexiones salientes.

bind_type

Tipo de sesión SMPP

Tipo	Requerido	Valores Permitidos
Átomo	Sí	`:transmitter`, `:receiver`, `:transceiver`

Propósito: Define la capacidad de dirección del mensaje.

Opciones:

- `:transmitter` - Solo enviar mensajes (submit_sm)
- `:receiver` - Solo recibir mensajes (deliver_sm)
- `:transceiver` - Enviar y recibir (más común)

Recomendación: Usar `:transceiver` a menos que el transportista requiera un tipo específico.

host

Nombre de host o IP del servidor SMPP del transportista

Tipo	Requerido	Ejemplo
String	Sí	`"smpp.carrier.com"` o `"10.5.1.100"`

Propósito: Dirección del servidor SMPP del transportista.

Ejemplos:

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

port

Puerto del servidor SMPP

Tipo	Requerido	Predeterminado	Rango
Entero	Sí	2775	1-65535

Propósito: Puerto TCP para la conexión SMPP.

Puerto estándar: 2775

Ejemplos:

```
port: 2775  # Estándar
port: 3000  # Personalizado
```

system_id

Nombre de usuario de autenticación

Tipo	Requerido	Ejemplo
String	Sí	`"company_user"`

Propósito: Nombre de usuario proporcionado por el transportista para la autenticación.

Seguridad: Proteger esta credencial - almacenada en el archivo de configuración.

password

Contraseña de autenticación

Tipo	Requerido	Ejemplo
String	Sí	`"secret_password"`

Propósito: Contraseña proporcionada por el transportista para la autenticación.

Seguridad:

- Proteger esta credencial
- Usar contraseñas fuertes
- Rotar periódicamente

tps_limit

Límite de transacciones por segundo

Tipo	Requerido	Predeterminado	Rango
Entero	Sí	100	1-10000

Propósito: Máximo de mensajes por segundo a enviar a través de esta conexión.

Directrices:

- Establecer entre 70-80% del máximo del transportista
- Previene la limitación/desconexión
- Permite margen para recibos de entrega

Ejemplos:

```
tps_limit: 10    # Bajo volumen
tps_limit: 50    # Volumen medio
tps_limit: 100   # Alto volumen (más común)
tps_limit: 1000  # Muy alto volumen
```

Cálculo:

```
Si el máximo del transportista = 100 TPS
Establecer tps_limit = 70-80
Deja 20-30 TPS de margen
```

queue_check_frequency

Intervalo de sondeo de la cola de mensajes (milisegundos)

Tipo	Requerido	Predeterminado	Rango
Entero	Sí	1000	100-10000

Propósito: Con qué frecuencia verificar al backend por nuevos mensajes a enviar.

Directrices:

- **Alto volumen (>100 TPS)**: 500-1000ms
- **Volumen medio (10-100 TPS)**: 1000-2000ms
- **Bajo volumen (<10 TPS)**: 2000-5000ms

Compensaciones:

- Valor más bajo = recogida de mensajes más rápida, mayor carga de API
- Valor más alto = recogida más lenta, menor carga de API

Ejemplo de UI Web:

Configuración de Vínculo del Servidor SMPP

Los vínculos del servidor definen **conexiones entrantes** donde el gateway actúa como un **SMSC** (servidor) aceptando conexiones de **ESMEs** (clientes) externos. En este modo, los sistemas asociados se conectan al gateway para enviar y recibir mensajes.

Ejemplo Completo de Vínculo del Servidor

```
config :omnimessage_smpp, :server_binds, [
  %{
    # Identificador único para este cliente
    name: "partner_acme",

    # Credenciales esperadas del cliente
    system_id: "acme_corp",
    password: "acme_secret",

    # Tipos de vínculo permitidos
    allowed_bind_types: [:transmitter, :receiver, :transceiver],

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

    # Limitación de tasa
    tps_limit: 50,

    # Frecuencia de verificación de la cola
    queue_check_frequency: 1000
  }
]
```

Parámetros del Vínculo del Servidor

name

Identificador del cliente

Tipo	Requerido	Ejemplo
String	Sí	`"partner_acme"`

Propósito: Identifica al cliente externo que se conecta a usted.

Convenciones de nomenclatura: Usar el nombre del socio/cliente para fácil identificación.

system_id

Nombre de usuario esperado del cliente

Tipo	Requerido	Ejemplo
String	Sí	`"acme_corp"`

Propósito: Nombre de usuario que el cliente externo debe proporcionar para autenticarse.

Proveer al cliente: Compartir esta credencial con su socio.

password

Contraseña esperada del cliente

Tipo	Requerido	Ejemplo
String	Sí	`"secure_password"`

Propósito: Contraseña que el cliente externo debe proporcionar para autenticarse.

Seguridad:

- Usar contraseñas fuertes
- Única por cliente

- Compartir de manera segura con el socio

allowed_bind_types

Tipos de sesión permitidos

Tipo	Requerido	Predeterminado
Lista de Átomos	Sí	-

Propósito: Restringe qué tipos de vínculo puede usar el cliente.

Opciones:

```
allowed_bind_types: [:transceiver]  # Solo transceptor
allowed_bind_types: [:transmitter, :receiver]  # TX o RX
allowed_bind_types: [:transmitter, :receiver, :transceiver]  #
Cualquiera
```

Recomendación: Permitir los tres a menos que necesite restricciones.

ip_whitelist

Direcciones IP de cliente permitidas

Tipo	Requerido	Predeterminado	Formato
Lista de Strings	Sí	`[]`	IPs o notación CIDR

Propósito: Seguridad - solo permitir conexiones desde IPs conocidas.

Formatos:

- IP única: `"192.168.1.100"` (automáticamente `/32`)
- Subred CIDR: `"192.168.1.0/24"`, `"10.0.0.0/8"`
- Mezclar ambos: `["192.168.1.0/24", "10.50.1.100"]`

Ejemplos:

```
# Permitir cualquier IP (no recomendado)
ip_whitelist: []

# IP única
ip_whitelist: ["203.0.113.50"]

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

# Subred
ip_whitelist: ["192.168.1.0/24"]

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

Subredes comunes:

- `/32` - IP única (automático para IPs sin máscara)
- `/24` - 256 direcciones (por ejemplo, 192.168.1.0-255)
- `/16` - 65,536 direcciones (por ejemplo, 10.50.0.0-255.255)
- `/8` - 16,777,216 direcciones (por ejemplo, 10.0.0.0-255.255.255.255)

tps_limit

Límite de mensajes por segundo

Igual que el `tps_limit` del vínculo del cliente - controla la tasa de deliver_sm saliente.

queue_check_frequency

Intervalo de sondeo de la cola

Igual que el `queue_check_frequency` del vínculo del cliente - con qué frecuencia verificar mensajes para entregar a este cliente.

Ejemplo de UI Web:

Configuración de Escucha del Servidor

Cuando los vínculos del servidor están configurados, el gateway escucha conexiones entrantes.

Ejemplo Completo de Escucha

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

Parámetros de Escucha

host

Dirección IP a la que vincularse

Tipo	Requerido	Predeterminado	Valores Comunes
String	No	`"0.0.0.0"`	`"0.0.0.0"`, `"127.0.0.1"`

Propósito: Qué interfaz de red escuchar.

Valores:

- `"0.0.0.0"` - Escuchar en todas las interfaces (recomendado)
- `"127.0.0.1"` - Escuchar solo en localhost (pruebas)
- `"192.168.1.10"` - Escuchar en IP específica

port

Puerto TCP para escuchar

Tipo	Requerido	Predeterminado	Rango
Entero	No	2775	1-65535

Propósito: Puerto para conexiones SMPP entrantes.

Estándar: 2775

max_connections

Número máximo de conexiones concurrentes

Tipo	Requerido	Predeterminado	Rango
Entero	No	100	1-10000

Propósito: Limita el número total de conexiones simultáneas de clientes.

Directrices:

- Establecer según los clientes esperados
- Valores más altos usan más memoria

- Típico: 10-100 conexiones

Ejemplos Completos de Configuración

Ejemplo 1: Conexión de Transportista Único

```
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
  }
]
```

Ejemplo 2: Múltiples Transportistas

```
import Config

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

config :omnimessage_smpp, :binds, [
  # América del Norte
  %{
    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
  },

  # Europa
  %{
    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
  }
]
```

Ejemplo 3: Gateway con Vínculos del Servidor

```
import Config

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

# Conexiones salientes
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
  }
]

# Definiciones de clientes entrantes
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
  }
]
```

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

Validación de Configuración

Después de editar la configuración, valide antes de reiniciar:

Verificación de Sintaxis

```
# Verificar sintaxis de Elixir
/opt/omnimessage-smpp/bin/omnimessage-smpp eval "File.read!
('config/runtime.exs')"
```

Si la sintaxis es inválida, verá un error. Corrija antes de reiniciar.

Probar Configuración

```
# Reiniciar en primer plano para ver errores
sudo -u omnimessage-smpp /opt/omnimessage-smpp/bin/omnimessage-
smpp console
```

Presione `Ctrl+C` dos veces para salir.

Mejores Prácticas de Seguridad

1. **Proteger el archivo de configuración**:

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

2. **Usar contraseñas fuertes**:
   - Mínimo 12 caracteres
   - Mezclar letras, números, símbolos
   - Único por conexión
3. **Usar listas blancas de IP**:
   - Siempre configurar `ip_whitelist` para vínculos del servidor
   - Nunca usar lista vacía `[]` en producción
4. **Habilitar verificación SSL**:
   - Establecer `verify_ssl_peer: true` con certificados válidos
5. **Rotación regular de credenciales**:
   - Cambiar contraseñas trimestralmente
   - Coordinar con transportistas/socios

Próximos Pasos

- Revisar MONITORING.md para la configuración de métricas
- Leer OPERATIONS.md para gestionar conexiones
- Ver TROUBLESHOOTING.md para problemas comunes
- Volver a README.md para una visión general

Glosario

Términos y Definiciones

A

API (Interfaz de Programación de Aplicaciones) Interfaz utilizada para comunicarse con el sistema backend de la cola de mensajes.

Auto-Scroll Función en la pestaña de Registros de la interfaz web que se desplaza automáticamente para mostrar las entradas de registro más recientes.

B

Backend El sistema de cola de mensajes al que se conecta la puerta de enlace SMPP para recuperar y almacenar mensajes.

Bind Una conexión SMPP entre dos sistemas. Puede ser transmisor, receptor o transceptor.

Bind Type El tipo de sesión SMPP:

- **Transmisor**: Solo envía mensajes
- **Receptor**: Solo recibe mensajes
- **Transceptor**: Envía y recibe mensajes

Bind Failure Cuando un intento de autenticación SMPP falla, generalmente debido a credenciales incorrectas o restricciones de IP.

C

CIDR (Enrutamiento Inter-Dominio Sin Clase) Notación para especificar rangos de direcciones IP (por ejemplo, `192.168.1.0/24` representa 256

direcciones IP).

Client Bind Una conexión SMPP saliente donde la puerta de enlace actúa como un **ESME** conectándose a un **SMSC** externo (típicamente un servidor SMPP de un operador). En este modo, la puerta de enlace es el cliente.

Connection Status Estado actual de un bind SMPP:

- **Conectado**: Activo y operativo
- **Desconectado**: No conectado
- **Reconectando**: Intentando establecer conexión

Counter Una métrica que solo aumenta (se restablece al reiniciar el servicio), utilizada para totales como mensajes enviados.

D

Data Coding Campo SMPP que especifica la codificación de caracteres del mensaje (GSM-7, UCS-2, etc.).

Delivery Failure Cuando un mensaje no puede ser entregado, indicado por una respuesta de error del operador.

Delivery Receipt (DLR) Confirmación del operador sobre el estado de entrega del mensaje.

dest_smsc Campo en la cola de mensajes que indica qué conexión SMPP debe manejar el mensaje.

Disconnection Cuando una conexión SMPP activa es terminada, ya sea intencionalmente o debido a un error.

E

Enquire Link Mensaje de mantenimiento de conexión SMPP enviado periódicamente para verificar que la conexión está activa.

ESM Class Campo SMPP que indica el tipo de mensaje y características.

ESME (Entidad de Mensaje Corto Externa) En la terminología SMPP, la aplicación cliente que se conecta a un SMSC para enviar o recibir mensajes. Cuando la puerta de enlace opera en **modo Cliente**, actúa como un ESME conectándose a SMSCs de operadores. Cuando opera en **modo Servidor**, acepta conexiones de ESMEs externos.

Exponential Backoff Estrategia de reintento donde el tiempo de espera se duplica después de cada fallo (1min, 2min, 4min, 8min...).

F

Firewall Sistema de seguridad de red que controla el tráfico de red entrante y saliente.

G

Gateway La aplicación de la puerta de enlace SMPP que conecta la cola de mensajes con las redes móviles.

Gauge Una métrica que puede aumentar o disminuir, representando el valor actual (por ejemplo, estado de conexión).

Grafana Herramienta de visualización popular para mostrar métricas de Prometheus en paneles.

GSM-7 Codificación de caracteres estándar de 7 bits para SMS, que admite hasta 160 caracteres por mensaje.

H

HTTP/HTTPS Protocolos utilizados para la comunicación web. HTTPS es la versión encriptada.

I

IP Whitelist Lista de direcciones IP permitidas que pueden conectarse a la puerta de enlace (característica de seguridad).

ISDN (Red Digital de Servicios Integrados) Plan de numeración comúnmente utilizado para números de teléfono.

J

(Sin términos)

K

Keepalive Mensajes periódicos (enquire_link) enviados para mantener la conexión y detectar fallos.

KPI (Indicador Clave de Rendimiento) Valor medible que indica el rendimiento del sistema (por ejemplo, tasa de éxito de entrega).

L

Label En Prometheus, pares clave-valor adjuntos a métricas para identificación (por ejemplo, `bind_name="vodafone_uk"`).

LiveView Tecnología del marco Phoenix utilizada para actualizaciones en tiempo real de la interfaz web.

M

Message Queue Sistema backend que almacena mensajes esperando ser enviados o recibidos.

Metrics Mediciones cuantitativas del rendimiento del sistema, expuestas en formato Prometheus.

MO (Origen Móvil) Mensajes enviados desde teléfonos móviles a la puerta de enlace (entrantes).

MT (Terminado Móvil) Mensajes enviados desde la puerta de enlace a teléfonos móviles (salientes).

MSISDN (Número de Directorio Internacional de Suscriptor de Estación Móvil) Formato estándar para números de teléfono móvil.

N

NPI (Indicador de Plan de Numeración) Campo SMPP que especifica el esquema de numeración (por ejemplo, ISDN).

O

Outbound Mensajes que fluyen desde la puerta de enlace hacia las redes móviles.

Inbound Mensajes que fluyen desde las redes móviles hacia la puerta de enlace.

P

PDU (Unidad de Datos de Protocolo) Paquete de mensaje SMPP individual (por ejemplo, submit_sm, deliver_sm).

Prometheus Sistema de monitoreo de código abierto que recopila y almacena métricas de series temporales.

Q

Queue Lista de mensajes esperando ser procesados o enviados.

Queue Check Frequency Con qué frecuencia (en milisegundos) la puerta de enlace consulta el backend en busca de nuevos mensajes.

Queue Worker Componente que recupera mensajes de la cola y los envía a través de SMPP.

R

Rate Limiting Control del rendimiento de mensajes para cumplir con las restricciones del operador. Ver TPS.

Receiver Tipo de bind SMPP que solo recibe mensajes (deliver_sm).

Reconnect Restablecer una conexión SMPP desconectada.

Retry Intentar enviar nuevamente un mensaje fallido, generalmente con retroceso exponencial.

S

Server Bind Configuración que permite a los **ESMEs** externos (clientes) conectarse a la puerta de enlace. En este modo, la puerta de enlace actúa como un **SMSC** (servidor) aceptando conexiones entrantes de sistemas asociados.

Session Conexión SMPP activa entre dos sistemas.

SMPP (Protocolo de Mensaje Corto Peer-to-Peer) Protocolo estándar de la industria para intercambiar mensajes SMS entre sistemas.

SMSC (Centro de Servicio de Mensajes Cortos) En la terminología SMPP, el componente servidor que acepta conexiones de ESMEs (clientes) y maneja el enrutamiento y la entrega de mensajes SMS. Cuando la puerta de enlace opera

en **modo Servidor**, actúa como un SMSC aceptando conexiones de ESMEs externos.

SSL/TLS Protocolos de encriptación para comunicación segura.

Submit_SM PDU SMPP para enviar un mensaje para entrega.

Submit_SM_Resp Respuesta SMPP a submit_sm, indicando éxito o fallo.

System ID Nombre de usuario utilizado para la autenticación SMPP.

T

Telemetry Recopilación y transmisión automatizada de métricas del sistema.

TON (Tipo de Número) Campo SMPP que especifica el formato del número (por ejemplo, internacional, nacional).

TPS (Transacciones Por Segundo) Límite de tasa para el máximo de mensajes por segundo a través de una conexión.

Transceiver Tipo de bind SMPP que puede enviar y recibir mensajes (el más común).

Transmitter Tipo de bind SMPP que solo envía mensajes (submit_sm).

Throughput Tasa de procesamiento de mensajes, típicamente medida en mensajes por segundo.

U

UCS-2 Codificación de caracteres Unicode de 16 bits para SMS, que admite hasta 70 caracteres por mensaje.

Uptime Duración durante la cual una conexión o servicio ha estado operativo de manera continua.

V

Validity Period Límite de tiempo para el intento de entrega de un mensaje antes de la expiración.

W

Web Dashboard Interfaz de usuario basada en navegador para monitorear y gestionar la puerta de enlace.

Whitelist Ver IP Whitelist.

X

(Sin términos)

Y

(Sin términos)

Z

(Sin términos)

Referencia Rápida de Acrónimos

Acrónimo	Término Completo
API	Interfaz de Programación de Aplicaciones
CIDR	Enrutamiento Inter-Dominio Sin Clase
DLR	Recibo de Entrega
ESME	Entidad de Mensaje Corto Externa
GSM	Sistema Global para Comunicaciones Móviles
HTTP	Protocolo de Transferencia de Hipertexto
HTTPS	Protocolo de Transferencia de Hipertexto Seguro
IP	Protocolo de Internet
ISDN	Red Digital de Servicios Integrados
KPI	Indicador Clave de Rendimiento
MO	Origen Móvil
MSISDN	Número de Directorio Internacional de Suscriptor de Estación Móvil
MT	Terminado Móvil
NPI	Indicador de Plan de Numeración
PDU	Unidad de Datos de Protocolo
SMPP	Protocolo de Mensaje Corto Peer-to-Peer

Acrónimo	Término Completo
SMSC	Centro de Servicio de Mensajes Cortos
SMS	Servicio de Mensajes Cortos
SSL	Capa de Conexión Segura
TLS	Seguridad de la Capa de Transporte
TON	Tipo de Número
TPS	Transacciones Por Segundo
UCS	Conjunto de Caracteres Codificados Universalmente
UI	Interfaz de Usuario
URL	Localizador Uniforme de Recursos

Documentación Relacionada

- **README.md** - Visión general del sistema y cómo empezar
- **CONFIGURATION.md** - Parámetros de configuración explicados
- **OPERATIONS.md** - Operaciones diarias
- **MONITORING.md** - Métricas y monitoreo
- **TROUBLESHOOTING.md** - Resolución de problemas

Guía de Monitoreo y Métricas

Referencia completa para monitorear el Gateway SMPP

Descripción general

El Gateway SMPP expone métricas en formato Prometheus para monitorear la salud de la conexión, el rendimiento de mensajes y el rendimiento del sistema.

Crítico: Dado que el gateway es sin estado y depende de OmniMessage Core, **la conectividad de OmniMessage es la métrica más importante a monitorear**. Monitorea ambos:

1. **Métricas del Gateway SMPP** - Salud a nivel de protocolo
2. **Métricas de la API de OmniMessage** - Conectividad y salud del backend

Endpoint de Métricas

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

Formato: Formato de texto Prometheus

Acceso: Abierto a localhost por defecto (configura el firewall para acceso remoto)

Prueba Rápida

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

Métricas Disponibles

Todas las métricas están prefijadas con `smpp_` e incluyen etiquetas para identificación.

Métricas de Licencia

omnimessage_smpp_license_status

Tipo: Gauge
Descripción: Estado actual de la licencia
Valores:

- `1` = Licencia válida
- `0` = Licencia inválida/expirada

Etiquetas: Ninguna

Ejemplo:

```
omnimessage_smpp_license_status 1
```

Uso:

- Alertar cuando el valor es 0 (licencia inválida)
- Cuando la licencia es inválida, el procesamiento de la cola de salida se detiene, pero los enlaces SMPP permanecen conectados
- La interfaz web permanece accesible para la solución de problemas

Nombre del Producto: `omnimessage_smpp`

Notas:

- Cuando la licencia es inválida (`license_status == 0`), el gateway deja de procesar colas de salida
- Los enlaces SMPP (tanto cliente como servidor) permanecen conectados y aceptan solicitudes de enlace

- Los mensajes entrantes aún se reciben pero no se procesan
- La interfaz de usuario y el monitoreo permanecen accesibles independientemente del estado de la licencia

Ejemplo de Alerta:

```
- alert: SMPP_License_Invalid
  expr: omnimessage_smpp_license_status == 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "Licencia del Gateway SMPP inválida o expirada"
    description: "El estado de la licencia es inválido - el
procesamiento de mensajes salientes está bloqueado"
```

Métricas de Estado de Conexión

smpp_connection_status

Tipo: Gauge
Descripción: Estado actual de la conexión del enlace SMPP
Valores:

- `1` = Conectado
- `0` = Desconectado

Etiquetas:

- `bind_name` - Nombre de la conexión (por ejemplo, "vodafone_uk")
- `mode` - Tipo de conexión ("cliente" o "servidor")
- `host` - Host remoto (solo en modo cliente)
- `port` - Puerto remoto (solo en modo cliente)
- `bind_type` - Tipo de enlace SMPP (solo en modo cliente)
- `system_id` - ID del sistema utilizado

Ejemplo:

```
smpp_connection_status{bind_name="vodafone_uk",mode="client",host="sm
1
```

Uso:

- Alertar cuando el valor es 0 (desconectado)
- Rastrear el porcentaje de tiempo de actividad de la conexión
- Monitorear la frecuencia de reconexiones

Contadores de Mensajes

smpp_messages_sent_total

Tipo: Counter
Descripción: Número total de mensajes enviados a través del enlace SMPP
Unidad: Mensajes

Etiquetas: Igual que connection_status

Ejemplo:

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

Uso:

- Calcular la tasa de mensajes (mensajes/segundo)
- Rastrear el volumen diario/mensual
- Comparar el rendimiento real vs el esperado

smpp_messages_received_total

Tipo: Counter
Descripción: Número total de mensajes recibidos a través del enlace SMPP
Unidad: Mensajes

Etiquetas: Igual que connection_status

Ejemplo:

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

Uso:

- Monitorear el volumen de mensajes entrantes
- Rastrear el tráfico originado en móviles (MO)
- Alertar sobre cambios inesperados en el volumen

Métricas de Entrega

smpp_delivery_failures_total

Tipo: Counter
Descripción: Número total de fallas en la entrega de mensajes
Unidad: Fallas

Etiquetas: Igual que connection_status

Ejemplo:

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

Uso:

- Calcular la tasa de éxito de entrega
- Alertar sobre altas tasas de fallas
- Identificar conexiones problemáticas

Cálculo de Tasa de Éxito:

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

Métricas de Operación de Enlace

smpp_bind_success_total

Tipo: Counter
Descripción: Número total de operaciones de enlace exitosas
Unidad: Intentos de enlace

Ejemplo:

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

Uso:

- Rastrear la estabilidad del enlace
- Monitorear el éxito de la autenticación

smpp_bind_failures_total

Tipo: Counter
Descripción: Número total de operaciones de enlace fallidas
Unidad: Intentos de enlace

Ejemplo:

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

Uso:

- Alertar sobre fallas de autenticación
- Identificar problemas de credenciales
- Rastrear problemas de conexión con el operador

Métricas de Eventos de Conexión

smpp_connection_attempts_total

Tipo: Counter
Descripción: Número total de intentos de conexión
Unidad: Intentos

Ejemplo:

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

Uso:

- Rastrear la rotación de conexiones
- Monitorear la frecuencia de reconexiones

smpp_disconnection_total

Tipo: Counter
Descripción: Número total de desconexiones
Unidad: Desconexiones

Ejemplo:

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

Uso:

- Alertar sobre desconexiones frecuentes
- Identificar problemas de red
- Rastrear la estabilidad de la conexión

Métricas de Tiempo de Actividad

smpp_uptime_seconds

Tipo: Gauge
Descripción: Tiempo de actividad actual del enlace SMPP en segundos
Unidad: Segundos

Ejemplo:

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

Uso:

- Rastrear la estabilidad de la conexión
- Calcular el porcentaje de tiempo de actividad
- Alertar sobre reinicios recientes

Métricas de Salud de la API de OmniMessage

Mientras que el gateway en sí expone métricas relacionadas con SMPP, **la salud de la API de OmniMessage es crítica**. También deberías monitorear:

Desde las Métricas de OmniMessage (si están disponibles)

- `omnimessage_api_requests_total` - Total de solicitudes API desde el gateway
- `omnimessage_api_request_duration_seconds` - Tiempos de respuesta de la API
- `omnimessage_queue_depth` - Mensajes pendientes en la cola de OmniMessage

Desde los Registros del Gateway (si las métricas no están expuestas)

Busca estos patrones para detectar problemas de la API:

- "api.*connection refused" - No se puede alcanzar OmniMessage

- "api.*timeout" - OmniMessage no responde
- "api.*http 503" - OmniMessage temporalmente fuera de servicio
- "api.*parse error" - Problema de formato de respuesta

Configuración de Prometheus

Configuración Básica de Scrape

Agrega a `/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'
```

Múltiples Gateways

```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'
```

Descubrimiento de Servicios

Usando descubrimiento basado en archivos:

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

Archivo `/etc/prometheus/targets/smpp-production.json`:

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

Dashboards de Grafana

Paneles de Dashboard de Ejemplo

Panel de Estado de Conexión

Consulta:

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

Visualización: Stat
Umbrales:

- Rojo: valor < 1 (desconectado)
- Verde: valor == 1 (conectado)

Panel de Tasa de Mensajes

Consulta:

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

Visualización: Gráfico
Unidad: mensajes/segundo
Leyenda: `{{bind_name}}`

Panel de Tasa de Éxito de Entrega

Consulta:

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

Visualización: Gauge
Unidad: Porcentaje (0-100)
Umbrales:

- Rojo: < 95%
- Amarillo: 95-98%
- Verde: > 98%

Panel de Tiempo de Actividad de Conexión

Consulta:

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

Visualización: Stat
Unidad: Horas

Reglas de Alerta

Reglas de Alerta de Prometheus

Guarda en `/etc/prometheus/rules/smpp-alerts.yml`:

```yaml
groups:
  - name: smpp_gateway
    interval: 30s
    rules:
      # Conexión caída
      - alert: SMPPConnectionDown
        expr: smpp_connection_status == 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "La conexión SMPP {{ $labels.bind_name }} está
caída"
          description: "La conexión {{ $labels.bind_name }} ha
estado desconectada por más de 2 minutos."

      # Alta tasa de fallas
      - alert: SMPPHighFailureRate
        expr: |
          (
            rate(smpp_delivery_failures_total[5m])
            /
            rate(smpp_messages_sent_total[5m])
          ) > 0.05
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Alta tasa de fallas de entrega en {{
$labels.bind_name }}"
          description: "La tasa de fallas de entrega es {{ $value
| humanizePercentage }} en {{ $labels.bind_name }}."

      # Fallas de enlace
      - alert: SMPPBindFailures
        expr: increase(smpp_bind_failures_total[10m]) > 3
        labels:
          severity: warning
        annotations:
          summary: "Múltiples fallas de enlace en {{
$labels.bind_name }}"
          description: "{{ $labels.bind_name }} ha fallado en
enlazarse {{ $value }} veces en los últimos 10 minutos."
```

```
      # No se enviaron mensajes (cuando se esperaba)
      - alert: SMPPNoTraffic
        expr: rate(smpp_messages_sent_total[10m]) == 0
        for: 30m
        labels:
          severity: warning
        annotations:
          summary: "No se enviaron mensajes en {{
$labels.bind_name }}"
          description: "{{ $labels.bind_name }} no ha enviado
ningún mensaje durante 30 minutos."

      # Desconexiones frecuentes
      - alert: SMPPFrequentDisconnections
        expr: increase(smpp_disconnection_total[1h]) > 5
        labels:
          severity: warning
        annotations:
          summary: "Desconexiones frecuentes en {{
$labels.bind_name }}"
          description: "{{ $labels.bind_name }} se ha desconectado
{{ $value }} veces en la última hora."

      # API de OmniMessage inalcanzable
      - alert: OmniMessageAPIUnreachable
        expr: |
          count(count_over_time({job="omnimessage-smpp"} |=
"api.*connection refused"[5m])) > 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "API de OmniMessage es inalcanzable"
          description: "El Gateway SMPP no puede alcanzar la API
de OmniMessage. Verifica la configuración de API_BASE_URL y la
conectividad de red."

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

```
        labels:
          severity: warning
        annotations:
          summary: "La API de OmniMessage está tardando demasiado"
          description: "Se detectaron múltiples timeouts de la
API. OmniMessage puede estar lento o sobrecargado."

      # Sin flujo de mensajes (problema de 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: "No se detectó flujo de mensajes - verifica la
conectividad de OmniMessage"
          description: "No se enviaron ni recibieron mensajes
durante 30 minutos. Verifica la conectividad de la API de
OmniMessage y el estado de la cola."
```

Carga las reglas en `prometheus.yml`:

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

Monitoreo del Dashboard Web

La interfaz web integrada proporciona monitoreo en tiempo real sin Prometheus.

Acceso

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

Página de Estado en Vivo

Navegación: SMPP → Estado en Vivo

Características:

- Estado de conexión en tiempo real
- Contadores de mensajes
- Tiempo de actividad de la conexión
- Controles manuales de reconexión/desconexión
- Actualización automática cada 5 segundos

Uso:

- Verificación rápida del estado
- Intervención manual
- Solución de problemas en tiempo real

El dashboard muestra:

- **Total de Enlaces**: Conteo combinado de todas las conexiones de cliente y servidor
- **Enlaces de Cliente**: Conexiones salientes a operadores (mostrando conteo de conectados/desconectados)

- **Enlaces de Servidor**: Conexiones entrantes de socios (mostrando conteo de activos/en espera)
- **Servidor Escuchando**: Configuración del socket del servidor entrante (host, puerto, conexiones máximas)

Monitoreo de Registros

Registros del Sistema

Ver registros:

```
# Seguir registros en tiempo real
sudo journalctl -u omnimessage-smpp -f

# Últimas 100 líneas
sudo journalctl -u omnimessage-smpp -n 100

# Desde un tiempo específico
sudo journalctl -u omnimessage-smpp --since "1 hour ago"

# Filtrar por nivel
sudo journalctl -u omnimessage-smpp -p err
```

Registros de la Interfaz Web

Navegación: Pestaña de registros en la interfaz web

Características:

- Transmisión de registros en tiempo real
- Filtrar por nivel (debug, info, warning, error)
- Buscar registros
- Pausar/reanudar
- Borrar registros

La vista de registros te permite:

- **Filtrar por Nivel**: Seleccionar nivel de registro (Todos, Debug, Info, Advertencia, Error)
- **Buscar**: Encontrar entradas de registro específicas por contenido de texto
- **Desplazamiento Automático**: Habilitar/deshabilitar el desplazamiento automático a medida que llegan nuevos registros
- **Pausar/Reanudar**: Pausar actualizaciones de registros para revisar entradas específicas
- **Borrar**: Borrar todos los registros mostrados

Indicadores Clave de Rendimiento (KPI)

Salud de la Conexión

Métrica: Porcentaje de tiempo de actividad de la conexión

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

Objetivo: > 99.9%

Tasa de Entrega de Mensajes

Métrica: Mensajes entregados por segundo

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

Objetivo: Coincide con el volumen esperado

Tasa de Éxito de Entrega

Métrica: Porcentaje de entregas exitosas

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

Objetivo: > 98%

Estabilidad del Enlace

Métrica: Intentos de enlace por hora

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

Objetivo: < 10 por hora (indica conexión estable)

Mejores Prácticas de Monitoreo

1. Configurar Alertas

- Configura alertas de Prometheus para métricas críticas
- Usa PagerDuty/OpsGenie para alertas 24/7
- Prueba las alertas regularmente

2. Crear Dashboards

- Construye dashboards de Grafana para cada gateway
- Incluye todas las conexiones en un dashboard
- Agrega paneles de planificación de capacidad

3. Revisiones Regulares

- Revisa métricas semanalmente
- Identifica tendencias y patrones
- Planifica ajustes de capacidad

4. Documentar Líneas Base

- Registra volúmenes de mensajes normales
- Documenta tasas de TPS esperadas
- Anota tiempos/días pico

5. Correlacionar con el Backend

- Monitorea métricas de la API del backend
- Rastrear el flujo de mensajes de extremo a extremo
- Identificar cuellos de botella

Solución de Problemas con Métricas

Problemas de Conexión

Verifica: `smpp_connection_status`

- Valor 0 = Revisa registros, verifica red, verifica credenciales
- Cambios frecuentes = Inestabilidad de red

Bajas Tasas de Entrega

Verifica: `smpp_delivery_failures_total`

- Alta tasa = Verifica estado del operador, revisa formato del mensaje
- Compara entre conexiones = Identifica operador problemático

Bajo Rendimiento

Verifica: tasa de `smpp_messages_sent_total`

- Por debajo de lo esperado = Verifica límites de TPS, disponibilidad de colas
- Verifica métricas de la API del backend

Problemas de Enlace

Verifica: `smpp_bind_failures_total`

- Aumentando = Problemas de autenticación, problemas de credenciales
- Verifica system_id y contraseña en la configuración

Documentación Relacionada

- **CONFIGURATION.md** - Configurar ajustes de monitoreo
- **OPERATIONS.md** - Procedimientos operativos
- **TROUBLESHOOTING.md** - Resolver problemas
- **README.md** - Descripción general y guía rápida

Guía de Operaciones

Procedimientos operativos diarios

Dependencia Crítica: OmniMessage Core

IMPORTANTE: La puerta de enlace SMPP de OmniMessage no puede funcionar sin acceso a OmniMessage Core. Todo el procesamiento de mensajes ocurre en OmniMessage - la puerta de enlace es solo un traductor de protocolo.

Si OmniMessage se vuelve inaccesible:

- □ No se pueden enviar nuevos mensajes
- □ No se pueden recuperar mensajes pendientes
- □ No se puede informar el estado de entrega
- □ El sistema parece colgarse o agotar el tiempo

Verificar la Salud de OmniMessage:

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

# Verificar la URL de API configurada en los registros
grep api_base_url /opt/omnimessage-smpp/config/runtime.exs
```

Operaciones Diarias

Verificación de Salud Matutina

Realice estas verificaciones al inicio de cada día:

1. **Acceder al Panel Web**

- URL: `https://your-server:8087`
- Verifique si el panel se carga correctamente

2. **Verificar el Estado de Conexión**

- Navegar a: SMPP → Estado en Vivo
- Verifique que todas las conexiones muestren "Conectado" (verde)
- Anote cualquier enlace desconectado

3. **Revisar Métricas de Mensajes**

- Navegar a: pestaña de Cola
- Verifique que los recuentos de mensajes sean razonables
- Verifique que no haya acumulación inesperada en la cola

4. **Verificar Registros del Sistema**

- Navegar a: pestaña de Registros
- Busque mensajes de error (rojo)
- Anote cualquier patrón de advertencia

5. **Revisar Métricas de Prometheus**

- `curl http://localhost:4000/metrics`
- O verifique los paneles de Grafana
- Verifique que las tasas de mensajes sean normales

Monitoreo Continuo

Configure alertas para:

- Fallos de conexión (> 2 minutos fuera de línea)
- Altas tasas de fallos de entrega (> 5%)
- Sin tráfico durante períodos prolongados
- Desconexiones frecuentes

Consulte MONITORING.md para la configuración de alertas.

Gestión de Conexiones SMPP

Cómo se Configuran los Pares SMPP

Las conexiones SMPP (pares) se pueden configurar utilizando **dos métodos**:

Método 1: Interfaz Web (Recomendado)

- **Ventaja**: Los cambios tienen efecto inmediato, no se requiere reinicio
- **Ubicación**: Pestañas SMPP → Pares de Clientes / Pares de Servidores
- **Operaciones**: Agregar, editar, eliminar pares
- **Persistencia**: Almacenados en la base de datos Mnesia
- **Mejor para**: Operaciones diarias, pruebas, cambios rápidos

Método 2: Archivo de Configuración

- **Ventaja**: Configuración como código, control de versiones
- **Ubicación**: `/opt/omnimessage-smpp/config/runtime.exs`
- **Operaciones**: Definir pares en la configuración de Elixir
- **Persistencia**: Basada en archivos, sobrevive a los reinicios
- **Requiere**: Reinicio del servicio después de los cambios
- **Mejor para**: Configuración inicial, infraestructura como código

Nota: Los cambios en la interfaz web se almacenan por separado y sobrescriben la configuración del archivo.

Consulte CONFIGURATION.md para la referencia del archivo de configuración.

Agregar una Nueva Conexión de Cliente

Propósito: Configurar la puerta de enlace para actuar como un **ESME** (cliente) conectándose al **SMSC** (servidor) de un operador

Preparación: Reúna información del operador:

- Nombre de host/IP del servidor SMPP
- Número de puerto (generalmente 2775)
- ID del sistema (nombre de usuario)
- Contraseña
- Tipo de enlace (generalmente transceptor)
- Límite de TPS

Elija uno de los siguientes métodos:

Opción A: A través de la Interfaz Web (Recomendado)

Ventajas: Efecto inmediato, no se requiere reinicio

Pasos:

1. **Navegar a Pares de Clientes**:
    - Abrir Interfaz Web: `https://your-server:8087`
    - Navegar a: SMPP → Pares de Clientes
2. **Agregar Nuevo Par**:
    - Hacer clic en "Agregar Nuevo Par de Cliente"
    - Completar el formulario:
        - **Nombre**: `vodafone_uk` (identificador único)
        - **Host**: `smpp.vodafone.co.uk`
        - **Puerto**: `2775`

        - **ID del Sistema**: `your_username`
        - **Contraseña**: `your_password`
        - **Tipo de Enlace**: `Transceptor`
        - **Límite de TPS**: `100`
        - **Frecuencia de Verificación de Cola**: `1000`
    - Hacer clic en "Guardar"

3. **La Conexión se Establece Automáticamente**:
    - La puerta de enlace intenta inmediatamente la conexión
    - Navegar a: SMPP → Estado en Vivo
    - El estado debería cambiar a "Conectado" (verde) dentro de 10-30 segundos
    - Verifique la pestaña de Registros para un mensaje de enlace exitoso
4. **Probar el Flujo de Mensajes**:
    - Navegar a: pestaña de Cola
    - Enviar un mensaje de prueba con dest_smsc que coincida con el nombre del enlace
    - Monitorear en Estado en Vivo para la transmisión
    - Verificar la confirmación de entrega

Opción B: A través del Archivo de Configuración

Ventajas: Infraestructura como código, control de versiones

Pasos:

1. **Editar Archivo de Configuración**:

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

2. **Agregar Nuevo Enlace a la Configuración**:

```
config :omnimessage_smpp, :binds, [
  # Enlaces existentes...

  # Agregar nuevo enlace
  %{
    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. **Guardar y Reiniciar el Servicio**:

```
# Guardar archivo (Ctrl+X, Y, Enter en nano)

# Reiniciar servicio
sudo systemctl restart omnimessage-smpp
```

4. **Verificar Conexión**:
   - Navegar a: SMPP → Estado en Vivo
   - Encontrar nueva conexión

- El estado debería ser "Conectado" (verde)
- Verificar registros para enlace exitoso

5. **Probar el Flujo de Mensajes**:

   - Navegar a: pestaña de Cola
   - Enviar un mensaje de prueba con dest_smsc que coincida con el nuevo nombre de enlace
   - Monitorear en Estado en Vivo para la transmisión
   - Verificar la confirmación de entrega

Agregar un Enlace de Servidor

Propósito: Configurar la puerta de enlace para actuar como un **SMSC** (servidor) aceptando conexiones de **ESMEs** externas (clientes asociados)

Preparación:

1. **Generar Credenciales**:

   - Crear un ID de sistema único: `partner_name`
   - Crear una contraseña fuerte
   - Documentar y compartir de manera segura con el socio

2. **Obtener Información del Socio**:

   - Direcciones IP de origen del socio
   - Volumen de mensajes esperado (para límite de TPS)
   - Tipos de enlace requeridos

Elija uno de los siguientes métodos:

Opción A: A través de la Interfaz Web (Recomendado)

Ventajas: Efecto inmediato, no se requiere reinicio

Pasos:

1. **Navegar a Pares de Servidores**:

- Abrir Interfaz Web: `https://your-server:8087`
- Navegar a: SMPP → Pares de Servidores

2. **Agregar Nuevo Par de Servidor**:

   - Hacer clic en "Agregar Nuevo Par de Servidor"
   - Completar el formulario:
     - **Nombre**: `partner_acme` (identificador único)
     - **ID del Sistema**: `acme_corp`
     - **Contraseña**: `secure_password_123`
     - **Tipos de Enlace Permitidos**: Seleccionar todos (Transmisor, Receptor, Transceptor)
     - **Lista Blanca de IP**: `203.0.113.0/24` (separado por comas para múltiples)
     - **Límite de TPS**: `50`
     - **Frecuencia de Verificación de Cola**: `1000`
   - Hacer clic en "Guardar"

3. **Puerta de Enlace Lista para Conexión**:

   - El par de servidor ahora está activo y esperando la conexión del socio
   - No se requiere reinicio

4. **Compartir Información con el Socio**:

- Dirección IP de la puerta de enlace
- Puerto: `2775`
- ID del Sistema: `acme_corp`
- Contraseña: `secure_password_123`
- Tipo de Enlace: Como se configuró

5. **Esperar la Conexión del Socio**:

   - Navegar a: SMPP → Estado en Vivo
   - Observar la conexión entrante
   - Verificar el éxito de la autenticación
   - Verificar que la IP coincida con la lista blanca

Opción B: A través del Archivo de Configuración

Ventajas: Infraestructura como código, control de versiones

Pasos:

1. **Editar Archivo de Configuración**:

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

2. **Agregar Enlace de Servidor y Configuración de Escucha**:

```
# Agregar a la lista de server_binds
config :omnimessage_smpp, :server_binds, [
  # Enlaces de servidor existentes...

  # Agregar nuevo enlace de servidor
  %{
    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
  }
]

# Asegúrese de que la configuración de escucha exista (solo se
necesita una vez)
config :omnimessage_smpp, :listen, %{
  host: "0.0.0.0",
  port: 2775,
  max_connections: 100
}
```

3. **Guardar y Reiniciar Servicio**:

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

4. **Compartir Información con el Socio**:
   - Dirección IP de la puerta de enlace
   - Puerto: `2775`
   - ID del Sistema: `acme_corp`
   - Contraseña: `secure_password_123`
   - Tipo de Enlace: Como se configuró
5. **Esperar la Conexión del Socio**:
   - Navegar a: SMPP → Estado en Vivo

- Observar la conexión entrante
- Verificar el éxito de la autenticación
- Verificar que la IP coincida con la lista blanca

Modificar Conexión Existente

Propósito: Actualizar parámetros de conexión (límites de TPS, contraseñas, lista blanca de IP, etc.)

Elija uno de los siguientes métodos:

Opción A: A través de la Interfaz Web (Recomendado)

Ventajas: Efecto inmediato, no se requiere reinicio

Pasos:

1. **Navegar a Pares**:
   - Abrir Interfaz Web: `https://your-server:8087`
   - Para conexiones de cliente: SMPP → Pares de Clientes
   - Para conexiones de servidor: SMPP → Pares de Servidores
2. **Editar Par**:
   - Encontrar el par a modificar
   - Hacer clic en el botón "Editar"
   - Actualizar los parámetros deseados:
     - Cambios comunes: límite de TPS, contraseña, lista blanca de IP, host/puerto
   - Hacer clic en "Guardar"
3. **Los Cambios se Aplican Inmediatamente**:
   - La conexión se reconecta automáticamente con la nueva configuración
   - No se requiere reinicio del servicio
   - Navegar a: SMPP → Estado en Vivo para verificar
4. **Verificar Cambios**:

- Verificar que la conexión se establezca correctamente
- Monitorear la pestaña de Registros en busca de errores
- Probar el flujo de mensajes si es aplicable

Opción B: A través del Archivo de Configuración

Ventajas: Infraestructura como código, control de versiones

Pasos:

1. **Editar Archivo de Configuración**:

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

2. **Modificar Parámetros de Enlace**:
   - Encontrar el enlace en la lista de `:binds` o `:server_binds`
   - Actualizar los parámetros deseados:
     - Cambios comunes: límite de TPS, contraseñas, lista blanca de IP, host/puerto
   - Ejemplo:

```
%{
  name: "vodafone_uk",
  # ... otros parámetros
  tps_limit: 150,  # Cambiado de 100
  password: "new_password"  # Contraseña actualizada
}
```

3. **Guardar y Reiniciar Servicio**:

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

4. **Verificar Cambios**:
   - Navegar a: SMPP → Estado en Vivo
   - Verificar que la conexión se establezca correctamente

- Monitorear registros en busca de errores
- Probar el flujo de mensajes

Eliminar una Conexión

Propósito: Descontinuar una conexión SMPP

Pasos:

1. **Notificar a las Partes Interesadas**:
   - Informar al operador/socio
   - Coordinar ventana de inactividad
2. **Desconectar a través de la Interfaz Web**:
   - Navegar a: SMPP → Estado en Vivo
   - Encontrar la conexión
   - Hacer clic en "Eliminar Conexión"
   - Confirmar acción
3. **Eliminar Configuración**:
   - Navegar a: SMPP → Pares de Clientes/Servidores
   - Encontrar la conexión
   - Hacer clic en "Eliminar"
   - Confirmar eliminación
4. **Verificar Eliminación**:
   - Verificar Estado en Vivo - la conexión debería haber desaparecido
   - Revisar registros para un apagado limpio

Gestión del Flujo de Mensajes

Verificar Cola de Mensajes

Propósito: Monitorear mensajes pendientes

Pasos:

1. **Acceder a la Cola**:
    - Navegar a: pestaña de Cola
    - Ver lista de mensajes pendientes

2. **Verificar Detalles del Mensaje**:
    - Hacer clic en la fila del mensaje
    - Revisar:
        - Número de destino
        - Cuerpo del mensaje
        - SMSC objetivo (dest_smsc)
        - Intentos de entrega
        - Estado

3. **Buscar Mensaje Específico**:

- Usar filtro de búsqueda
- Filtrar por destino, contenido o SMSC

Solucionar Mensajes Atascados

Síntomas: Mensajes no entregados

Pasos:

1. **Verificar Estado de Conexión**:
   - Navegar a: SMPP → Estado en Vivo
   - Verificar que la conexión objetivo esté conectada
   - Si está desconectada, consulte Reconectando
2. **Verificar Detalles del Mensaje**:
   - Navegar a: pestaña de Cola
   - Encontrar mensaje atascado
   - Verificar que el campo `dest_smsc` coincida con el nombre de la conexión
   - Verificar la marca de tiempo `deliver_after` (programación de reintentos)
3. **Verificar Intentos de Entrega**:
   - Altos intentos = fallos repetidos
   - Verificar registros en busca de mensajes de error
   - Puede indicar formato inválido o rechazo del operador
4. **Intervención Manual** (si es necesario):
   - Contactar al operador para verificar el problema
   - Puede ser necesario cancelar y reenviar el mensaje
   - Consultar con el equipo de backend sobre problemas en la cola

---

Solución de Problemas de Conexión

Reconectando un Enlace

Síntomas: La conexión muestra "Desconectado" (rojo)

Pasos:

1. **Verificar Conectividad de Red**:

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

2. **Verificar Registros en Busca de Errores**:

   - Navegar a: pestaña de Registros
   - Filtrar: Nivel de error
   - Buscar fallos de autenticación, tiempos de espera de red

3. **Verificar Credenciales**:

   - Navegar a: SMPP → Pares de Clientes/Servidores
   - Verificar que el system_id y la contraseña sean correctos

- Contactar al operador si no está seguro

4. **Reconexión Manual**:
   - Navegar a: SMPP → Estado en Vivo
   - Encontrar el enlace desconectado
   - Hacer clic en el botón "Reconectar"
   - Esperar 10-30 segundos
   - Verificar si el estado cambia a "Conectado"
5. **Si la Reconexión Falla**:
   - Verificar reglas del firewall
   - Verificar que el servidor del operador esté operativo
   - Contactar al soporte del operador
   - Consulte TROUBLESHOOTING.md

Manejo de Fallos de Autenticación

Síntomas: Fallos de enlace repetidos en los registros

Causas:

- Nombre de usuario/contraseña incorrectos
- IP no en la lista blanca del operador
- Cuenta suspendida/expirada

Pasos:

1. **Verificar Credenciales**:
   - Navegar a: SMPP → Pares de Clientes
   - Verificar el system_id y la contraseña
   - Confirmar con el operador
2. **Verificar la Lista Blanca de IP**:
   - Confirmar la IP de su puerta de enlace con el operador

- Solicitar al operador que verifique la lista blanca de IP

3. **Verificar el Estado de la Cuenta**:
   - Verificar que la cuenta esté activa
   - Comprobar si hay contratos expirados
   - Contactar al departamento de facturación del operador
4. **Actualizar Configuración**:
   - Si las credenciales cambiaron, actualice en la Interfaz Web
   - Hacer clic en "Reconectar" para intentar nuevamente con las nuevas credenciales

---

Monitoreo y Alertas

Verificando Métricas de Prometheus

Verificación rápida:

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

Salida esperada:

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

Todos los valores deberían ser `1` (conectado).

Respondiendo a Alertas

Alerta de Conexión Caída:

1. Verificar Interfaz Web → SMPP → Estado en Vivo
2. Intentar reconexión manual

3. Verificar registros en busca de errores
4. Contactar al operador si la interrupción es prolongada
5. Consulte TROUBLESHOOTING.md

Alerta de Alta Tasa de Fallos:

1. Verificar registros en busca de patrones de error
2. Revisar cambios recientes en la configuración
3. Contactar al operador sobre rechazos
4. Verificar cumplimiento del formato del mensaje

Alerta de Sin Tráfico:

1. Verificar que la cola del backend tenga mensajes
2. Verificar que el enrutamiento `dest_smsc` sea correcto
3. Verificar que los límites de TPS no sean demasiado restrictivos
4. Revisar la configuración de `queue_check_frequency`

Procedimientos de Mantenimiento

Mantenimiento de Rutina

Realizar mensualmente:

1. **Revisar Métricas**:
    - Analizar tendencias de volumen de mensajes
    - Verificar tasas de éxito de entrega
    - Identificar oportunidades de optimización
2. **Actualizar Documentación**:
    - Documentar cualquier cambio de configuración
    - Actualizar información de contacto
    - Anotar ventanas de mantenimiento del operador

3. **Auditoría de Credenciales**:
    - Revisar todas las contraseñas SMPP
    - Planificar rotación de credenciales
    - Verificar que las listas blancas de IP estén actualizadas
4. **Planificación de Capacidad**:
    - Revisar tasas de mensajes máximas
    - Verificar contra límites de TPS
    - Planificar para el crecimiento

Reinicio del Servicio

Cuando sea necesario:

- Después de cambios en el archivo de configuración
- Después de actualizaciones del sistema
- Durante la solución de problemas

Pasos:

```
# Verificar estado actual
sudo systemctl status omnimessage-smpp

# Reiniciar servicio
sudo systemctl restart omnimessage-smpp

# Verificar reinicio
sudo systemctl status omnimessage-smpp

# Verificar registros
sudo journalctl -u omnimessage-smpp -n 50
```

Verificar a través de la Interfaz Web:

1. Acceder al panel (puede tardar de 30 a 60 segundos en estar en línea)
2. Navegar a: SMPP → Estado en Vivo

3. Esperar a que todas las conexiones se establezcan (1-2 minutos)
4. Verificar registros en busca de errores

Copia de Seguridad de Configuración

Hacer copia de seguridad de archivos críticos antes de realizar cambios:

```
# Copia de seguridad de configuración
sudo cp /opt/omnimessage-smpp/config/runtime.exs \
  /opt/omnimessage-smpp/config/runtime.exs.backup.$(date +%Y%m%d)

# Copia de seguridad de certificados
sudo tar -czf /tmp/smpp-certs-$(date +%Y%m%d).tar.gz \
  /opt/omnimessage-smpp/priv/cert/
```

Restaurar si es necesario:

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

# Reiniciar servicio
sudo systemctl restart omnimessage-smpp
```

Procedimientos de Emergencia

Interrupción Completa del Servicio

Pasos:

1. **Verificar estado del servicio**:

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

2. **Si el servicio está detenido, inícielo**:

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

3. **Verificar registros para la razón del fallo**:

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

4. **Si no se inicia**:

   - Verificar errores de sintaxis en la configuración
   - Verificar que existan certificados SSL
   - Verificar espacio en disco: `df -h`
   - Verificar memoria: `free -h`

5. **Contactar soporte** si no se resuelve

Solicitudes de Desconexión de Emergencia del Operador

Pasos:

1. **Eliminar conexión inmediatamente**:

   - Navegar a: SMPP → Estado en Vivo
   - Encontrar la conexión afectada
   - Hacer clic en "Eliminar Conexión"

2. **Documentar razón**:

   - Anotar nombre del operador
   - Registrar hora y razón
   - Guardar correspondencia

3. **Investigar el problema**:

   - Verificar patrones recientes de mensajes
   - Revisar registros en busca de errores
   - Identificar la causa raíz

4. **Coordinar resolución**:
    - Trabajar con el operador
    - Implementar soluciones
    - Probar antes de reconectar

Pico de Volumen Alto

Síntomas: Tráfico de mensajes inesperadamente alto

Pasos:

1. **Verificar límites de TPS**:
    - Navegar a: SMPP → Estado en Vivo
    - Verificar que las conexiones no estén limitando
    - Puede ser necesario aumentar temporalmente los límites de TPS
2. **Monitorear estabilidad del operador**:
    - Observar desconexiones
    - Verificar tasas de éxito de entrega
3. **Coordinar con el backend**:
    - Verificar que la fuente de mensajes sea legítima
    - Puede ser necesario implementar limitación de tasas en el upstream
4. **Escalar si es necesario**:
    - Puede ser necesario instancias adicionales de la puerta de enlace
    - Contactar soporte para asesoramiento sobre escalado

Mejores Prácticas

Lista de Verificación Diaria

- [ ] Verificar que todas las conexiones SMPP estén conectadas
- [ ] Revisar registros de errores en busca de problemas
- [ ] Monitorear la cola de mensajes para acumulación
- [ ] Verificar paneles de Prometheus/Grafana
- [ ] Verificar tasas de éxito de entrega > 98%

Tareas Semanales

- [ ] Revisar tendencias de métricas
- [ ] Verificar anomalías en patrones
- [ ] Probar procedimientos de recuperación ante desastres
- [ ] Actualizar documentación según sea necesario
- [ ] Revisar y reconocer alertas

Tareas Mensuales

- [ ] Auditoría de credenciales
- [ ] Revisión de planificación de capacidad
- [ ] Actualizar contactos del operador
- [ ] Revisar y optimizar configuraciones de TPS
- [ ] Copia de seguridad de archivos de configuración

Documentación Relacionada

- **CONFIGURATION.md** - Configurar conexiones y ajustes
- **MONITORING.md** - Configurar alertas de Prometheus
- **TROUBLESHOOTING.md** - Resolver problemas comunes
- **README.md** - Visión general del sistema

Guía de Solución de Problemas

Problemas comunes y soluciones

Problemas de Conectividad de OmniMessage

Dado que el Gateway SMPP es sin estado y depende completamente de OmniMessage Core, los problemas de conectividad con OmniMessage son los problemas más críticos.

Síntomas de Desconexión de OmniMessage

- **No hay mensajes salientes**: La cola se acumula, los mensajes no se envían
- **No hay mensajes entrantes**: Los socios no pueden enviar mensajes
- **Time-outs**: Llamadas a la API que se agotan o se cuelgan
- **Los registros muestran**: "Conexión rechazada", "Tiempo de espera", "HTTP 503", "Conexión restablecida"

Diagnóstico

1. Verifique la Disponibilidad de OmniMessage:

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

# Probar desde el host del gateway específicamente
ssh gateway-server 'curl -k https://omnimessage-
core.example.com:8443/api/system/health'
```

2. Verifique la URL de la API Configurada:

```
# Revisar la configuración
grep -A1 'api_base_url' /opt/omnimessage-smpp/config/runtime.exs

# Verificar conectividad de red
ping omnimessage-core.example.com
nc -zv omnimessage-core.example.com 8443
```

3. Verifique los Registros del Gateway para Errores de API:

```
# Buscar errores relacionados con la API
sudo journalctl -u omnimessage-smpp -f | grep -i
'api\|omnimessage\|connect'

# Buscar registros de errores recientes
sudo journalctl -u omnimessage-smpp -n 200 | grep -i error
```

Soluciones

Si OmniMessage está inactivo:

1. Contactar al equipo de operaciones de OmniMessage
2. Los mensajes pendientes se acumularán en la cola
3. El gateway seguirá reintentando (ver `SMPP_POLL_INTERVAL`)
4. Verificar la página de estado de OmniMessage o el monitoreo

Si OmniMessage está activo pero el gateway no puede alcanzarlo:

1. Verificar que las reglas del firewall permitan HTTPS saliente
2. Verificar la resolución DNS: `nslookup omnimessage-core.example.com`
3. Verificar el enrutamiento de red: `traceroute omnimessage-core.example.com`
4. Verificar los certificados SSL si se utiliza HTTPS

Si la URL de la API está mal configurada:

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

2. Verificar que `api_base_url` sea correcto (debe ser HTTPS para producción)
3. Reiniciar el gateway: `sudo systemctl restart omnimessage-smpp`

Problemas de Conexión

La Conexión No Se Establece

Síntomas:

- El estado muestra "Desconectado" (rojo)
- No hay enlace exitoso en los registros
- Intentos de conexión repetidos

Causas Posibles y Soluciones:

1. Problemas de Conectividad de Red

Verificar:

```
# Probar resolución DNS
nslookup smpp.carrier.com

# Probar conectividad
ping -c 3 smpp.carrier.com

# Probar puerto
telnet smpp.carrier.com 2775
# o
nc -zv smpp.carrier.com 2775
```

Soluciones:

- Si DNS falla: Usar la dirección IP en lugar del nombre de host en la configuración
- Si el ping falla: Verificar las reglas del firewall, contactar al operador
- Si el puerto falla: Verificar el número de puerto correcto, revisar el firewall

2. Credenciales Incorrectas

Verificar:

- Los registros muestran "fallo de enlace" o "error de autenticación"
- Interfaz web: SMPP → Clientes Pares → verificar system_id y contraseña

Soluciones:

- Confirmar credenciales con el operador
- Verificar errores tipográficos (sensible a mayúsculas)
- Actualizar la configuración y reconectar

3. IP No Autorizada

Verificar:

- Conexión rechazada de inmediato
- Los registros del operador muestran IP no autorizada

Soluciones:

- Confirmar la IP pública de su gateway:

  ```
  curl ifconfig.me
  ```

- Solicitar al operador que agregue la IP a la lista blanca
- Verificar que la IP no haya cambiado (IP dinámica)

4. Firewall Bloqueando

Verificar:

```
# Verificar si el puerto está abierto
sudo iptables -L -n | grep 2775

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

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

Soluciones:

```
# Ubuntu/Debian
sudo ufw allow out 2775/tcp

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

La Conexión Sigue Caída

Síntomas:

- Conexión establecida pero se desconecta frecuentemente
- Métrica `smpp_disconnection_total` en aumento
- Los registros muestran reconexiones repetidas

Causas Posibles y Soluciones:

1. Inestabilidad de la Red

Verificar:

```
# Monitorear pérdida de paquetes
ping -c 100 smpp.carrier.com | grep loss

# Verificar errores de red
netstat -s | grep -i error
```

Soluciones:

- Contactar al operador sobre problemas de red
- Verificar con el ISP si es de su lado
- Considerar conexión/ruta de respaldo

2. Tiempo de Espera de Enlace de Consulta

Verificar:

- Los registros muestran "tiempo de espera de enlace de consulta"
- La conexión se cae después de períodos de inactividad

Soluciones:

- El tiempo de espera predeterminado es de 30 segundos
- Verificar que la red permita paquetes de keepalive
- Verificar si hay firewalls agresivos que agoten conexiones inactivas

3. Límite de TPS Excedido

Verificar:

- Alta tasa de mensajes en el momento de la desconexión
- El operador está limitando los mensajes

Soluciones:

- Revisar la configuración de `tps_limit`
- Reducir TPS al 70-80% del máximo del operador
- Distribuir el tráfico entre múltiples enlaces

4. Problemas del Servidor del Operador

Verificar:

- Verificar el estado del servicio del operador
- Contactar al soporte del operador

Soluciones:

- Esperar a que el operador resuelva
- Configurar un operador de respaldo si está disponible

Problemas de Entrega de Mensajes

Mensajes No Enviados

Síntomas:

- Mensajes atascados en la cola
- `smpp_messages_sent_total` no aumenta
- La conexión muestra conectada

Causas Posibles y Soluciones:

1. Enrutamiento Incorrecto de dest_smsc

Verificar:

- Interfaz web → Cola → Verificar el campo `dest_smsc` del mensaje
- Comparar con el nombre de conexión en SMPP → Estado en Vivo

Soluciones:

- Los mensajes se enrutan según el campo `dest_smsc`
- Verificar que el backend esté configurando el `dest_smsc` correcto
- Si `dest_smsc` es NULL, verificar el enrutamiento predeterminado

2. Mensajes Programados para el Futuro

Verificar:

- Interfaz web → Cola → Verificar el campo `deliver_after`
- Los mensajes con una marca de tiempo futura aún no se enviarán

Explicación:

- El sistema de reintentos establece `deliver_after` para mensajes fallidos
- Los mensajes esperan hasta ese momento antes de reintentar

Soluciones:

- Esperar el tiempo programado
- Si es urgente, contactar al equipo de backend para restablecer la marca de tiempo

3. Límite de TPS Demasiado Bajo

Verificar:

- Gran acumulación en la cola
- Mensajes enviándose muy lentamente

Soluciones:

- Aumentar `tps_limit` en la configuración
- Verificar que el operador pueda manejar una tasa más alta
- Ver CONFIGURATION.md

4. Trabajador de Cola No Ejecutándose

Verificar:

- Estado del servicio
- Registros de errores

Soluciones:

```
# Reiniciar servicio
sudo systemctl restart omnimessage-smpp

# Verificar registros
sudo journalctl -u omnimessage-smpp -f
```

Alta Tasa de Fallos de Entrega

Síntomas:

- `smpp_delivery_failures_total` en aumento
- Los registros muestran "submit_sm_resp" con estado de error
- Los mensajes no llegan a los destinatarios

Causas Posibles y Soluciones:

1. Números de Destino Inválidos

Verificar:

- Registros para códigos de error específicos
- Revisar el formato del destino del mensaje

Códigos de Error Comunes:

- `0x0000000B` - Destino inválido
- `0x00000001` - Longitud de mensaje inválida
- `0x00000003` - Comando inválido

Soluciones:

- Validar el formato del número (se recomienda E.164)
- Verificar que el número incluya el código de país
- Verificar con los requisitos del operador

2. Contenido del Mensaje Inválido

Verificar:

- Longitud del mensaje
- Caracteres especiales
- Codificación

Soluciones:

- GSM-7: Máx. 160 caracteres
- UCS-2: Máx. 70 caracteres
- Eliminar caracteres no soportados
- Verificar configuraciones de codificación

3. Rechazo del Operador

Verificar:

- Códigos de error específicos del operador
- Patrones en mensajes rechazados

Soluciones:

- Contactar al operador para conocer el motivo del rechazo
- Puede ser necesario filtrado de contenido
- Verificar patrones de spam/abuso

4. Mensajes Expirados

Verificar:

- Marca de tiempo `expires` del mensaje
- Tiempos de intento de entrega

Soluciones:

- Aumentar el período de validez del mensaje
- Reducir el retraso de reintento para mensajes sensibles al tiempo

---

Problemas de Interfaz Web

No se Puede Acceder al Panel Web

Síntomas:

- El navegador no puede conectarse a https://your-server:8087

- Tiempo de espera o conexión rechazada

Causas Posibles y Soluciones:

1. Servicio No Ejecutándose

Verificar:

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

Soluciones:

```
# Si está detenido, inícielo
sudo systemctl start omnimessage-smpp

# Verificar registros de errores
sudo journalctl -u omnimessage-smpp -n 50
```

2. Firewall Bloqueando el Puerto 8087

Verificar:

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

Soluciones:

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

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

3. Problemas con el Certificado SSL

Verificar:

- El navegador muestra advertencia de seguridad
- Certificado expirado o inválido

Soluciones:

- Aceptar excepción de seguridad (si es autofirmado)
- Instalar un certificado SSL válido
- Verificar que los archivos del certificado existan:

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

4. URL Incorrecta

Verificar:

- Verificar usando HTTPS (no HTTP)
- Verificar IP/hostname del servidor correcto
- Verificar puerto 8087

La Interfaz Web Muestra Errores

Síntomas:

- La página se carga pero muestra errores
- Las funciones no funcionan
- Los datos no se muestran

Soluciones:

1. **Limpiar Caché del Navegador**:
    - Ctrl+F5 (actualización forzada)
    - Limpiar caché y cookies del navegador
2. **Verificar Consola del Navegador**:
    - Presionar F12
    - Verificar la pestaña de Consola para errores de JavaScript

- Informar al soporte si se encuentran errores

3. **Probar Diferente Navegador**:
   - Probar en Chrome, Firefox, Edge
   - Aislar problemas específicos del navegador
4. **Verificar Registros del Servicio**:

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

Problemas de Métricas

Métricas de Prometheus No Disponibles

Síntomas:

- `curl http://localhost:4000/metrics` falla
- Prometheus no puede raspar métricas
- Respuesta vacía o de error

Causas Posibles y Soluciones:

1. Servicio No Ejecutándose

Verificar:

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

Soluciones:

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

2. Puerto No Accesible

Verificar:

```
# Probar localmente
curl http://localhost:4000/metrics

# Probar remotamente
curl http://your-server-ip:4000/metrics
```

Soluciones:

- Si local funciona pero remoto no: Verificar firewall
- Abrir puerto 4000 en el firewall para el servidor de Prometheus

3. Endpoint Incorrecto

Verificar:

- El endpoint es `/metrics` (no `/prometheus` o `/stats`)
- El puerto es 4000 (no 8087)

Métricas Muestran Valores Inesperados

Síntomas:

- Contadores se restablecen a cero
- Los medidores muestran valores incorrectos
- Faltan métricas para algunos enlaces

Soluciones:

1. **Reinicio del Servicio Restablece Contadores**:
    - Los contadores se restablecen al reiniciar el servicio
    - Este es un comportamiento normal
    - Usar `increase()` o `rate()` en las consultas de Prometheus
2. **Nuevos Enlaces No Aparecen**:

- Las métricas solo aparecen después del primer evento
- Enviar un mensaje de prueba para poblar métricas
- Verificar que el enlace esté habilitado y conectado

3. **Métricas Obsoletas**:
   - Los enlaces antiguos pueden seguir apareciendo en las métricas
   - Reiniciar el servicio para limpiar entradas obsoletas
   - O usar reetiquetado de Prometheus para filtrar

Problemas de Rendimiento

Alto Uso de CPU

Verificar:

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

Causas Posibles:

- Volumen de mensajes muy alto
- Demasiadas conexiones
- Problema de configuración

Soluciones:

- Verificar que la tasa de mensajes esté dentro de la capacidad
- Revisar límites de TPS
- Contactar soporte si el uso de CPU es sostenido

Alto Uso de Memoria

Verificar:

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

Causas Posibles:

- Gran cola de mensajes en memoria
- Fuga de memoria (rara)

Soluciones:

- Reiniciar el servicio para liberar memoria
- Verificar el tamaño de la cola de mensajes
- Contactar soporte si la memoria crece continuamente

Procesamiento Lento de Mensajes

Síntomas:

- Los mensajes tardan mucho en enviarse
- La cola se acumula
- Baja tasa de mensajes

Verificar:

1. Límites de TPS - pueden ser demasiado restrictivos
2. `queue_check_frequency` - puede ser demasiado alto
3. Tiempo de respuesta de la API del backend - puede ser lento
4. Latencia de red hacia el operador

Soluciones:

- Aumentar TPS si el operador lo permite
- Disminuir `queue_check_frequency` para un sondeo más rápido
- Optimizar la API del backend
- Verificar la latencia de la red

Problemas de Configuración

Errores de Sintaxis en el Archivo de Configuración

Síntomas:

- El servicio no se inicia después de un cambio en la configuración
- Los registros muestran "error de sintaxis" o "error de análisis"

Verificar:

```
# Validar sintaxis de Elixir
/opt/omnimessage-smpp/bin/omnimessage-smpp eval "File.read!
('config/runtime.exs')"
```

Errores Comunes:

- Falta una coma entre entradas de mapa
- Comillas desiguales (" vs ')
- Corchetes o llaves no coincidentes
- Falta `import Config` en la parte superior

Soluciones:

- Restaurar desde una copia de seguridad
- Revisar cuidadosamente la sintaxis
- Usar un editor de texto con resaltado de sintaxis de Elixir

Cambios No Efectuados

Síntomas:

- Configuración modificada pero sin cambio en el comportamiento
- Configuraciones antiguas aún activas

Soluciones:

```
# Los cambios de configuración requieren reinicio
sudo systemctl restart omnimessage-smpp

# Verificar que el reinicio haya tenido éxito
sudo systemctl status omnimessage-smpp

# Verificar registros de errores
sudo journalctl -u omnimessage-smpp -n 50
```

Recuperación de Emergencia

Fallo Completo del Sistema

Pasos:

1. **Verificar la salud básica del sistema**:

   ```
   # Espacio en disco
   df -h

   # Memoria
   free -h

   # Carga de CPU
   uptime
   ```

2. **Verificar el estado del servicio**:

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

3. **Revisar registros recientes**:

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

4. **Intentar reiniciar el servicio**:

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

5. **Si el reinicio falla**:
   - Verificar la sintaxis de la configuración
   - Verificar que existan certificados SSL
   - Verificar permisos de archivos
   - Revisar registros para errores específicos
6. **Restaurar desde una copia de seguridad** (si es necesario):

```
# Restaurar configuración
sudo cp /opt/omnimessage-smpp/config/runtime.exs.backup \
  /opt/omnimessage-smpp/config/runtime.exs

# Reiniciar
sudo systemctl restart omnimessage-smpp
```

7. **Contactar soporte** si no se resuelve

Obtener Ayuda

Información para Reunir

Antes de contactar al soporte, recopile:

1. **Versión**: `cat /opt/omnimessage-smpp/VERSION`
2. **Registros Recientes**:

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

3. **Configuración** (sanitizar contraseñas):

```
sudo cp /opt/omnimessage-smpp/config/runtime.exs
/tmp/config.exs
# Editar /tmp/config.exs para eliminar contraseñas antes de
enviar
```

4. **Salida de Métricas**:

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

5. **Información del Sistema**:

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

Contactar Soporte

- **Email**: support@omnitouch.com
- **Teléfono**: +61 XXXX XXXX (24/7)
- **Incluir**: Toda la información de arriba

Documentación Relacionada

- **OPERATIONS.md** - Procedimientos operativos normales
- **CONFIGURATION.md** - Referencia de configuración
- **MONITORING.md** - Monitoreo y métricas
- **README.md** - Resumen del sistema
