Referencia de Configuración

Guía completa de todos los parámetros de configuración

Visión 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** estos a formato OmniMessage a través de la API REST
3. **Consulta** a OmniMessage para mensajes a enviar
4. **Envía** PDUs SMPP a los transportistas
5. **Reporta** 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 en 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

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

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	Por Defecto
`api_base_url`	Cadena (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
- **Reportar Estado de Entrega**: Actualizar el estado de entrega de mensajes de vuelta a OmniMessage
- **Salud del Sistema**: Comprobaciones de salud periódicas

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	Por Defecto
`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 de certificados SSL

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

Parámetro	Tipo	Requerido	Por Defecto
`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	Por Defecto
`smsc_name`	Cadena	No	"smpp_gateway"

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

Variable de entorno: `SMSC_NAME`

Configuración de Vinculación del Cliente SMPP

Las vinculaciones 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 Vinculación del Cliente

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

    # Modo de conexión
    mode: :client,

    # Tipo de vinculación 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",

    # Campos del protocolo SMPP (opcional, establecer si el
transportista lo requiere)
    system_type: "",
    addr_ton: 0,
    addr_npi: 0,
    address_range: "",

    # Limitación de tasa
    tps_limit: 100,

    # Frecuencia de verificación de la cola
    queue_check_frequency: 1000,

    # Intervalo de keepalive (segundos, 0 para deshabilitar)
    enquire_link_interval: 60,

    # Caché de mensajes (opcional)
    cache_enabled: false,
    cache_max_size: 10000,
    cache_retry_interval: 60
```

```
  }
]
```

Parámetros de Vinculación del Cliente

name

Identificador único de conexión

Tipo	Requerido	Ejemplo
Cadena	Sí	`"vodafone_uk"`

Propósito: Identifica de manera única esta conexión SMPP.

- Usado en registros y m��tricas
- Debe ser único entre todas las vinculaciones
- Usar nombres descriptivos (transportista, región, propósito)

Convenciones de nombrado:

- `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
Cadena	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	Por Defecto	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
Cadena	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
Cadena	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	Por Defecto	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 el estrangulamiento/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	Por Defecto	Rango
Entero	Sí	1000	100-10000

Propósito: Con qué frecuencia verificar al backend para 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, más carga en la API
- Valor más alto = recogida más lenta, menos carga en la API

enquire_link_interval

Intervalo de keepalive SMPP (segundos)

Tipo	Requerido	Por Defecto	Rango
Entero	No	60	0-3600

Propósito: Con qué frecuencia (en segundos) enviar PDUs enquire_link SMPP para verificar que la conexión está viva. El servidor remoto responde con enquire_link_resp.

Directrices:

- **Por defecto (60)**: Adecuado para la mayoría de los transportistas
- **Valores más bajos (15-30)**: Detección de fallos más rápida, más tráfico
- **Valores más altos (120-300)**: Menos sobrecarga, detección de fallos más lenta

- **0**: Desactiva enquire_link por completo (no recomendado)

Ejemplos:

```
enquire_link_interval: 60   # Estándar (1 minuto)
enquire_link_interval: 30   # Keepalive agresivo
enquire_link_interval: 0    # Deshabilitado
```

system_type

Identificador de tipo de sistema SMPP

Tipo	Requerido	Por Defecto	Ejemplo
Cadena	No	`""`	`"OTP"`

Propósito: Campo del protocolo SMPP enviado durante la vinculación. Algunos transportistas requieren un valor específico. Dejar en blanco a menos que el transportista especifique uno.

addr_ton

Tipo de Número de Dirección

Tipo	Requerido	Por Defecto	Rango
Entero	No	0	0-6

Propósito: Campo del protocolo SMPP que especifica el tipo de número utilizado en la solicitud de vinculación.

Valores comunes:

- `0` - Desconocido
- `1` - Internacional
- `2` - Nacional
- `5` - Alfanumérico

Establecer según lo requerido por el transportista.

addr_npi

Indicador del Plan de Numeración de Dirección

Tipo	Requerido	Por Defecto	Rango
Entero	No	0	0-18

Propósito: Campo del protocolo SMPP que especifica el plan de numeración en la solicitud de vinculación.

Valores comunes:

- `0` - Desconocido
- `1` - ISDN/E.164
- `3` - Datos/X.121
- `9` - Privado

Establecer según lo requerido por el transportista.

address_range

Rango de direcciones para vinculación

Tipo	Requerido	Por Defecto	Ejemplo
Cadena	No	`""`	`"614*"`

Propósito: Campo del protocolo SMPP que especifica el rango de direcciones que esta vinculación maneja. Usado por algunos transportistas para filtrar qué mensajes se entregan a esta conexión. Dejar en blanco a menos que el transportista especifique un valor.

enabled

Estado habilitado del par

Tipo	Requerido	Por Defecto
Booleano	No	`true`

Propósito: Controla si este par está activo. Los pares deshabilitados se conservan en la configuración pero no establecen conexiones. Útil para tomar temporalmente una conexión fuera de línea sin eliminar su configuración.

cache_enabled

Habilitar caché local de mensajes

Tipo	Requerido	Por Defecto
Booleano	No	`false`

Propósito: Cuando está habilitado, los mensajes entrantes se almacenan en caché localmente si la API de backend no está disponible, y luego se entregan automáticamente cuando se restaura la conectividad. Consulte MESSAGE_CACHE.md para obtener todos los detalles.

cache_max_size

Número máximo de mensajes en caché

Tipo	Requerido	Por Defecto	Rango
Entero	No	10000	1-1000000

Propósito: Número máximo de mensajes para almacenar en caché por vinculación. Cuando se alcanza el límite, los mensajes más antiguos son expulsados (FIFO). Solo se aplica cuando `cache_enabled` es `true`.

cache_retry_interval

Intervalo base de reintento (segundos)

Tipo	Requerido	Por Defecto
Entero	No	60

Propósito: Intervalo base en segundos antes de reintentar la entrega de un mensaje en caché. Combinado con retroceso exponencial (reintento 0: 60s, reintento 1: 120s, reintento 2: 240s, etc.). Solo se aplica cuando `cache_enabled` es `true`.

Ejemplo de Interfaz Web:

Configuración de Vinculación del Servidor SMPP

Las vinculaciones 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 Vinculación 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 vinculación permitidos
    allowed_bind_types: [:transmitter, :receiver, :transceiver],

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

    # Restricciones de dirección de origen (vacío = permitir
todos)
    source_address_whitelist: [],

    # Limitación de tasa
    tps_limit: 50,

    # Frecuencia de verificación de la cola
    queue_check_frequency: 1000,

    # Intervalo de keepalive (segundos, 0 para deshabilitar)
    enquire_link_interval: 60,

    # Caché de mensajes (opcional)
    cache_enabled: false,
    cache_max_size: 10000,
    cache_retry_interval: 60
  }
]
```

Parámetros de Vinculación del Servidor

name

Identificador del cliente

Tipo	Requerido	Ejemplo
Cadena	Sí	`"partner_acme"`

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

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

system_id

Nombre de usuario esperado del cliente

Tipo	Requerido	Ejemplo
Cadena	Sí	`"acme_corp"`

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

Proporcionar al cliente: Compartir esta credencial con su socio.

password

Contraseña esperada del cliente

Tipo	Requerido	Ejemplo
Cadena	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	Por Defecto
Lista de Átomos	Sí	-

Propósito: Restringe qué tipos de vinculación 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	Por Defecto	Formato
Lista de Cadenas	Sí	`[]`	IPs o notación CIDR

Propósito: Seguridad - permitir solo 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"`
- Mezcla 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)

source_address_whitelist

Direcciones de origen permitidas

Tipo	Requerido	Por Defecto	Formato
Lista de Cadenas	No	`[]`	Patrones exactos o comodín

Propósito: Restringe qué direcciones de origen (IDs de remitente) pueden usar los clientes conectados al enviar mensajes. Una lista vacía permite todas las direcciones.

Tipos de patrones:

- Coincidencia exacta: `"MyBrand"` coincide solo con "MyBrand"
- Coincidencia de sufijo comodín: `"614*"` coincide con cualquier dirección que comience con "614"

Ejemplos:

```
# Permitir cualquier dirección de origen
source_address_whitelist: []

# Solo direcciones específicas
source_address_whitelist: ["MyBrand", "AlertService"]

# Coincidencia de prefijo comodín
source_address_whitelist: ["614*", "+61*"]

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

Los mensajes con direcciones de origen no permitidas son rechazados con `ESME_RINVSRCADR`. Consulte SOURCE_ADDRESS_WHITELIST.md para obtener todos los detalles.

tps_limit

Límite de mensajes por segundo

Igual que el `tps_limit` de vinculación del cliente - controla la tasa de entrega de deliver_sm a los clientes conectados.

queue_check_frequency

Intervalo de sondeo de la cola

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

enquire_link_interval

Intervalo de keepalive SMPP (segundos)

Igual que el `enquire_link_interval` de vinculación del cliente. Controla con qué frecuencia el servidor envía PDUs enquire_link a los clientes conectados para verificar que aún están vivos.

enabled

Estado habilitado del par

Igual que el `enabled` de vinculación del cliente. Los pares de servidor deshabilitados no aceptan conexiones entrantes.

cache_enabled

Habilitar caché local de mensajes

Igual que el `cache_enabled` de vinculación del cliente. Consulte MESSAGE_CACHE.md.

cache_max_size

Número máximo de mensajes en caché

Igual que el `cache_max_size` de vinculación del cliente.

cache_retry_interval

Intervalo base de reintento (segundos)

Igual que el `cache_retry_interval` de vinculación del cliente.

Ejemplo de Interfaz Web:

Configuración de Escucha del Servidor

Cuando las vinculaciones del servidor están configuradas, 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	Por Defecto	Valores Comunes
Cadena	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	Por Defecto	Rango
Entero	No	2775	1-65535

Propósito: Puerto para conexiones SMPP entrantes.

Estándar: 2775

max_connections

Número máximo de conexiones concurrentes

Tipo	Requerido	Por Defecto	Rango
Entero	No	100	1-10000

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

Directrices:

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

- Típico: 10-100 conexiones

Ejemplos Completos de Configuración

Ejemplo 1: Conexión a un Solo Transportista

```
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 Vinculaciones 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.

Variables de Entorno

Todas las configuraciones globales pueden ser sobrescritas con variables de entorno. Establezca estas en su archivo de unidad systemd o entorno de shell antes de iniciar el gateway.

Variable de Entorno	Clave de Configuración	Por De
`API_BASE_URL`	`api_base_url`	`"https://10.17`
`SMSC_NAME`	`smsc_name`	`"smpp_gateway"`
`SMPP_POLL_INTERVAL`	`smpp_poll_interval`	`100`
`VERIFY_SSL_PEER`	`verify_ssl_peer`	`false`
`CACHE_FLUSH_INTERVAL`	`cache_flush_interval`	`10000`
`CACHE_MAX_RETRY_ATTEMPTS`	`cache_max_retry_attempts`	`10`
`CACHE_BACKOFF_MULTIPLIER`	`cache_backoff_multiplier`	`2`

Variable de Entorno	Clave de Configuración	Por De
`MNESIA_STORAGE_TYPE`	`mnesia_storage_type`	`disc_copies`

Ejemplo de anulación systemd:

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

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

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
   - Única por conexión

3. **Usar listas blancas de IP**:
    - Siempre configurar `ip_whitelist` para vinculaciones de 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 USAGE.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 el Gateway 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 el gateway actúa como un **ESME** conectándose a un **SMSC** externo (típicamente un servidor SMPP de un operador). En este modo, el gateway 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.).

Deliver_SM PDU SMPP enviado por un SMSC (servidor) para entregar un mensaje a un ESME (cliente) conectado. Utilizado por los binds del servidor para enviar mensajes a socios conectados.

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 intencionadamente 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 el gateway 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.

Frontend Registration Proceso mediante el cual el gateway SMPP se registra con OmniMessage Core. Se envía un latido cada 60 segundos para mantener viva la registración. Si el gateway se detiene, la registración expira después de 90 segundos y OmniMessage deja de enrutar mensajes hacia él.

G

Gateway La aplicación Gateway SMPP que actúa como puente entre la cola de mensajes y 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 al gateway (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 framework 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 (Móvil Originado) Mensajes enviados desde teléfonos móviles al gateway (entrantes).

MT (Móvil Terminado) Mensajes enviados desde el gateway 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 el gateway hacia las redes móviles.

Inbound Mensajes que fluyen desde las redes móviles hacia el gateway.

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) el gateway 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

Sequence Number Identificador numérico único asignado a cada PDU SMPP dentro de una sesión. Se utiliza para hacer coincidir solicitudes con sus respuestas (por ejemplo, emparejar un submit_sm con su submit_sm_resp).

Server Bind Configuración que permite a **ESMEs** externos (clientes) conectarse al gateway. En este modo, el gateway actúa como un **SMSC** (servidor) aceptando conexiones entrantes de sistemas socios.

Session Conexión SMPP activa entre dos sistemas.

source_smsc Campo en la cola de mensajes que indica qué bind de servidor debe entregar el mensaje a sus clientes conectados a través de deliver_sm.

SMPP (Protocolo de Mensaje Corto de Par a Par) Protocolo estándar de la industria para intercambiar mensajes SMS entre sistemas.

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

V

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

W

Web Dashboard Interfaz de usuario basada en navegador para monitorear y gestionar el gateway.

Whitelist Ver IP Whitelist y Source Address 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	Móvil Originado
MSISDN	Número de Directorio Internacional de Suscriptor de Estación Móvil
MT	Móvil Terminado
NPI	Indicador de Plan de Numeración
PDU	Unidad de Datos de Protocolo
SMPP	Protocolo de Mensaje Corto de Par a Par

Acrónimo	Término Completo
SMSC	Centro de Servicio de Mensajes Cortos
SMS	Servicio de Mensajes Cortos
SSL	Capa de Conexiones Seguras
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** - Descripción general del sistema y cómo empezar
- **CONFIGURATION.md** - Parámetros de configuración explicados
- **USAGE.md** - Operaciones diarias
- **MONITORING.md** - Métricas y monitoreo
- **TROUBLESHOOTING.md** - Resolución de problemas

Caché de Mensajes SMPP

Descripción General

La Caché de Mensajes SMPP es una capa de persistencia local que permite que la puerta de enlace SMPP continúe aceptando mensajes entrantes incluso cuando la API de backend no está disponible. Los mensajes se almacenan localmente en Mnesia y se entregan automáticamente a la API cuando se restaura la conectividad, utilizando una lógica de reintento inteligente con retroceso exponencial.

Características

- **Aceptación Resiliente de Mensajes** - Continuar aceptando mensajes SMPP durante interrupciones de la API
- **Almacenamiento Persistente** - Utiliza Mnesia con `:disc_copies` para durabilidad a través de reinicios
- **Reintento Automático** - Trabajadores en segundo plano intentan automáticamente la entrega con retroceso exponencial
- **Configuración por Bind** - Habilitar/deshabilitar el almacenamiento en caché de forma independiente para cada bind SMPP
- **Protección contra Desbordamiento** - Desalojo FIFO cuando la caché alcanza el límite de tamaño configurado
- **Retención de Mensajes Fallidos** - Mensajes que fallan permanentemente se mantienen para revisión manual
- **Monitoreo en Tiempo Real** - Panel de LiveView con estadísticas y métricas de caché
- **Métricas de Prometheus** - Exportación completa de métricas para monitoreo y alertas

Arquitectura

Flujo de Mensajes

Con Caché Habilitada

```
SMPP Client → submit_sm → Gateway Server
                                ↓
                        Cache in Mnesia (respuesta inmediata)
                                ↓
                        CacheFlushWorker (en segundo plano)
                                ↓
                          Backend API
```

Con Caché Deshabilitada

```
SMPP Client → submit_sm → Gateway Server
                                ↓
                          Backend API (directo)
```

Componentes

1. **Módulo MessageCache** (`lib/sms_c/smpp/message_cache.ex`)
   - Lógica central de almacenamiento en caché
   - Manejo de desbordamiento
   - Funciones de consulta para LiveView y trabajadores
2. **CacheFlushWorker** (`lib/sms_c/smpp/cache_flush_worker.ex`)
   - GenServer por bind con almacenamiento en caché habilitado
   - Sondea mensajes listos para reintentar
   - Implementa retroceso exponencial
   - Marca mensajes que fallan permanentemente
3. **Tabla Mnesia** (`:smpp_message_cache`)

- Almacenamiento persistente con `:disc_copies`
- Indexada por bind_name, next_retry_at y status
- Sobrevive a reinicios de la aplicación

Configuración

Configuraciones Globales

Edita `config/runtime.exs`:

```
config :omnimessage_smpp,
  # Cada cuánto los trabajadores de vaciado sondean mensajes
(milisegundos)
  cache_flush_interval: 10_000,

  # Máximo de intentos de reintento antes de marcar como
failed_permanent
  cache_max_retry_attempts: 10,

  # Multiplicador de retroceso exponencial
  cache_backoff_multiplier: 2,

  # Tipo de almacenamiento de Mnesia (:disc_copies o :ram_copies)
  mnesia_storage_type: :disc_copies
```

Configuración por Bind

Cada bind SMPP (cliente o servidor) puede configurarse de forma independiente:

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

    # Configuración de caché
    cache_enabled: true,         # Habilitar almacenamiento en
caché (predeterminado: false)
    cache_max_size: 10_000,      # Máx. mensajes a almacenar en
caché (predeterminado: 10,000)
    cache_retry_interval: 60     # Intervalo base de reintento en
segundos (predeterminado: 60)
  }
]
```

Variables de Entorno

```
# Configuraciones globales de caché
CACHE_FLUSH_INTERVAL=10000              # Intervalo de sondeo de
vaciado (ms)
CACHE_MAX_RETRY_ATTEMPTS=10             # Máx. reintentos antes de
fallo permanente
CACHE_BACKOFF_MULTIPLIER=2              # Multiplicador de
retroceso exponencial
MNESIA_STORAGE_TYPE=disc_copies         # Tipo de almacenamiento
de Mnesia
```

Comportamiento de Reintento

Retroceso Exponencial

Cuando la entrega de mensajes falla, el intervalo de reintento se duplica con cada intento:

```
Intervalo base: 60 segundos
Multiplicador de retroceso: 2

Reintento 0: 60s   (1 minuto)
Reintento 1: 120s  (2 minutos)
Reintento 2: 240s  (4 minutos)
Reintento 3: 480s  (8 minutos)
Reintento 4: 960s  (16 minutos)
Reintento 5: 1920s (32 minutos)
...
Reintento 9: 30,720s (8.5 horas)
```

Fallo Permanente

Después de 10 intentos fallidos (por defecto), los mensajes se marcan como `failed_permanent` y:

- Permanecen en la caché para revisión manual
- Dejan de ser reintentados automáticamente
- Aparecen en la sección "Fallo Permanente" del panel de caché
- Pueden ser reintentados o eliminados manualmente

Transiciones de Estado

```
:pending → :delivering → SUCCESS (eliminado de la caché)
                      → FAILURE → :pending (reintento con
retroceso)
                                → :failed_permanent (después de los
reintentos máximos)
```

Monitoreo

Panel de LiveView

Accede al panel de caché en `http://your-server:4000/smpp` → pestaña "Caché de Mensajes"

Tarjetas de Resumen:

- Total en Caché - Todos los mensajes actualmente en caché
- Entrega Pendiente - Mensajes esperando reintento
- Fallo Permanente - Mensajes que superaron los reintentos máximos

Tabla por Bind:

- Nombre del bind
- Conteo de mensajes en caché
- Desglose Pendiente / Fallido
- Tamaño máximo de caché
- Porcentaje de utilización (con barra de progreso visual)

Métricas de Prometheus

```
# Tamaño actual de la caché por bind
smpp_cache_size{bind_name="my_bind",mode="server"} 42

# Total de mensajes entregados con éxito
smpp_cache_delivered_total{bind_name="my_bind"} 1234

# Total de intentos de reintento
smpp_cache_retry_total{bind_name="my_bind"} 56

# Total de fallos permanentes
smpp_cache_permanent_failures_total{bind_name="my_bind"} 2

# Total de eventos de desbordamiento (mensajes eliminados)
smpp_cache_overflow_total{bind_name="my_bind"} 0
```

Mensajes de Registro

```
INFO  Mensaje -123456789 almacenado en caché para my_smpp_bind
INFO  Mensaje en caché -123456789 entregado con éxito, ID de API:
99999
WARN  Falló al entregar el mensaje -123456789 (reintento 3/10),
próximo reintento en 2026-02-01 12:34:56Z
ERROR Mensaje -123456789 superó los reintentos máximos (10),
marcando como failed_permanent
WARN  Desbordamiento de caché para my_smpp_bind: mensaje más
antiguo eliminado
```

Operaciones

Habilitar/Deshabilitar Almacenamiento en Caché

A través de la Interfaz de Usuario de LiveView

1. Navega a `http://your-server:4000/smpp`
2. Ve a la pestaña "Client Peers" o "Server Peers"
3. Edita el bind
4. Activa/desactiva la casilla "Cache Enabled"
5. Guarda los cambios

A través de la Consola IEx

```
# Habilitar almacenamiento en caché para un bind
SmsC.SMPPConfig.update_server_peer("my_bind", "username",
"password",
  cache_enabled: true,
  cache_max_size: 10_000,
  cache_retry_interval: 60
)

# Deshabilitar almacenamiento en caché
SmsC.SMPPConfig.update_server_peer("my_bind", "username",
"password",
  cache_enabled: false
)
```

Monitorear el Estado de la Caché

```
# Obtener resumen global
SmsC.SMPP.MessageCache.get_cache_summary()
# => %{total_cached: 42, pending: 40, failed: 2}

# Obtener desglose por bind
SmsC.SMPP.MessageCache.get_cache_by_bind()
# => [
#   %{bind_name: "bind1", total: 30, pending: 28, failed: 2,
max_size: 10_000},
#   %{bind_name: "bind2", total: 12, pending: 12, failed: 0,
max_size: 10_000}
# ]

# Contar mensajes para un bind específico
SmsC.SMPP.MessageCache.count_cached_messages("my_bind")
# => 42
```

Intervenciones Manuales

Limpiar Mensajes Fallidos

```
# Obtener todos los mensajes fallidos para un bind
{:atomic, failed_messages} = :mnesia.transaction(fn ->
  :mnesia.match_object({:smpp_message_cache, :_, "my_bind", :_,
:_, :_, :_, :_, :_, :failed_permanent})
end)

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

Forzar Reintento de Mensaje Fallido

```
# Restablecer un mensaje failed_permanent a pending
SmsC.SMPP.MessageCache.update_cache_record("my_bind", -123456, %{
  status: :pending,
  retry_count: 0,
  next_retry_at: DateTime.utc_now(),
  last_error: nil
})
```

Solución de Problemas

Caché Llena / Eventos de Desbordamiento

Síntoma: métrica `cache_overflow_total` en aumento, mensajes más antiguos siendo eliminados

Causa: Límite de tamaño de caché alcanzado

Soluciones:

1. Aumentar `cache_max_size` para el bind
2. Investigar por qué la entrega de la API está fallando (revisar registros de la API, red)
3. Limpiar manualmente mensajes fallidos antiguos

4. Verificar si el intervalo de vaciado es demasiado lento

Mensajes No Entregados

Síntoma: Mensajes atascados en estado `:pending`

Posibles Causas:

1. **API está caída**
   - Verificar disponibilidad de la API
   - Verificar registros de la API de backend
   - Comprobar conectividad de red
2. **next_retry_at está en el futuro**
   - Los mensajes serán reintentados cuando se alcance `next_retry_at`
   - Verificar el cronograma de retroceso exponencial
3. **Trabajador de vaciado no está en ejecución**

```
# Verificar si los trabajadores están en ejecución
Supervisor.which_children(SmsC.SMPP.Supervisor)
```

4. **Caché deshabilitada**
   - Verificar `cache_enabled: true` en la configuración del bind

Altas Cantidades de Reintentos

Síntoma: Muchos mensajes con altos valores de `retry_count`

Investigación:

```
# Encontrar mensajes con altos conteos de reintentos
{:atomic, messages} = :mnesia.transaction(fn ->
  :mnesia.match_object({:smpp_message_cache, :_, "my_bind", :_,
:_, :_, :_, :_, :_, :_})
end)

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

# Verificar last_error para cada uno
Enum.each(high_retry, fn {_, _, _, msg_id, _, _, retry_count, _,
last_error, _} ->
  IO.puts("Mensaje #{msg_id}: #{retry_count} reintentos, error: #
{inspect(last_error)}")
end)
```

Espacio en Disco de Mnesia

Síntoma: Espacio en disco llenándose

Verificar el directorio de Mnesia:

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

Limpiar:

1. Limpiar mensajes fallidos antiguos (ver Intervenciones Manuales arriba)
2. Reducir `cache_max_size` por bind
3. Habilitar desbordamiento de caché (asegurar desalojo FIFO adecuado)

Consideraciones de Rendimiento

Uso de Memoria

- Cada mensaje almacenado en caché utiliza aproximadamente 500-1000 bytes (dependiendo del tamaño del mensaje)
- 10,000 mensajes ≈ 5-10 MB de memoria
- Con `:disc_copies`, los datos también se escriben en disco

Uso de CPU

- Los trabajadores de vaciado sondean cada 10 segundos por defecto (configurable)
- El procesamiento por lotes (100 mensajes por ciclo) reduce la sobrecarga
- Entrega concurrente (máx. 10 llamadas API concurrentes por trabajador)

I/O de Disco

- `:disc_copies` escribe en disco en cada transacción
- Para un rendimiento muy alto (>1000 msg/sec), considerar:
  - Usar `:ram_copies` (pierde persistencia)
  - Aumentar intervalos de vaciado
  - Escalar horizontalmente

Límites Recomendados

Escenario	cache_max_size	cache_flush_interval
Bajo volumen (<100 msg/sec)	10,000	10,000ms
Volumen medio (100-500 msg/sec)	50,000	5,000ms
Alto volumen (>500 msg/sec)	100,000	3,000ms

Escenarios de Recuperación

Reinicio de la Aplicación

1. Mnesia carga automáticamente las tablas `:disc_copies` desde el disco
2. Los mensajes almacenados en caché permanecen intactos
3. Los trabajadores de vaciado se reinician y continúan procesando

Migración de Base de Datos

Al actualizar desde una versión sin soporte de caché:

1. La migración agrega automáticamente campos de caché a los binds existentes
2. Valores predeterminados: `cache_enabled: false`, `cache_max_size: 10_000`, `cache_retry_interval: 60`
3. Sin pérdida de datos
4. Tabla de caché creada en la primera ejecución

Recuperación de Interrupción de API

1. Los mensajes se acumulan en caché durante la interrupción
2. Cuando la API se recupera, los trabajadores de vaciado entregan automáticamente
3. Los mensajes más antiguos se entregan primero (FIFO)
4. El retroceso exponencial previene la sobrecarga de la API durante la recuperación

Mejores Prácticas

1. **Habilitar Almacenamiento en Caché por Defecto** - Previene la pérdida de mensajes durante interrupciones
2. **Monitorear Métricas** - Configurar alertas en `cache_permanent_failures_total` y `cache_overflow_total`

3. **Dimensionar Apropiadamente** - Establecer `cache_max_size` basado en la duración esperada de la interrupción
4. **Revisar Mensajes Fallidos** - Revisar regularmente mensajes failed_permanent en busca de patrones
5. **Probar Failover** - Simular interrupciones de API para verificar el comportamiento de la caché
6. **Ajustar Intervalos de Reintento** - Afinar según los patrones de tiempo de recuperación de la API
7. **Usar Almacenamiento Persistente** - Mantener `mnesia_storage_type: disc_copies` en producción

Ver También

- Referencia de Configuración
- Monitoreo y Métricas
- Solución 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 de Prometheus

Acceso: Abierto a localhost por defecto (configurar 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 sea 0 (licencia inválida)
- Cuando la licencia es inválida, el procesamiento de la cola de salida se detiene, pero las conexiones SMPP permanecen conectadas
- La interfaz web permanece accesible para solucionar problemas

Nombre del Producto: `omnimessage_smpp`

Notas:

- Cuando la licencia es inválida (`license_status == 0`), el gateway deja de procesar colas de salida
- Las conexiones SMPP (tanto cliente como servidor) permanecen conectadas y aceptan solicitudes de conexión

- 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 de salida está bloqueado"
```

Métricas de Estado de Conexión

smpp_connection_status

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

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

Etiquetas:

- `bind_name` - Nombre de la conexión (por ejemplo, "vodafone_uk")
- `mode` - Tipo de conexión ("client" o "server")
- `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 sea 0 (desconectado)
- Rastrear el porcentaje de tiempo de actividad de la conexión
- Monitorear la frecuencia de reconexión

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 con 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 fallos en la entrega de mensajes
Unidad: Fallos

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 fallos
- 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 fallos 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 reconexión

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 Enlace de Consulta

smpp_enquire_link_sent_total

Tipo: Counter
Descripción: Número total de PDUs enquire_link enviados para verificar la vitalidad de la conexión
Unidad: PDUs

Etiquetas: Igual que connection_status

Ejemplo:

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

Uso:

- Rastrear la actividad de keepalive
- Comparar con los recibidos para detectar fallos unidireccionales

smpp_enquire_link_received_total

Tipo: Counter
Descripción: Número total de PDUs enquire_link_resp recibidos del par remoto
Unidad: PDUs

Etiquetas: Igual que connection_status

Ejemplo:

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

Uso:

- Detectar pares no responsivos (enviados >> recibidos)
- Monitorear la salud de la conexión más allá del estado simple

---

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 Caché de Mensajes

Estas métricas están disponibles cuando la caché de mensajes está habilitada en uno o más enlaces. Consulta MESSAGE_CACHE.md para obtener detalles sobre la configuración de la caché.

smpp_cache_size

Tipo: Gauge
Descripción: Número actual de mensajes en la caché local por enlace
Unidad: Mensajes

Etiquetas:

- `bind_name` - Nombre de la conexión
- `mode` - Tipo de conexión ("client" o "server")

Ejemplo:

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

Uso:

- Monitorear la utilización de la caché
- Alertar cuando se acerque a `cache_max_size`

smpp_cache_delivered_total

Tipo: Counter
Descripción: Número total de mensajes en caché entregados con éxito a la API del backend
Unidad: Mensajes

Ejemplo:

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

smpp_cache_retry_total

Tipo: Counter
Descripción: Número total de intentos de reintento para mensajes en caché
Unidad: Intentos

Ejemplo:

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

smpp_cache_permanent_failures_total

Tipo: Counter
Descripción: Número total de mensajes que superaron los intentos máximos de reintento y se marcaron como fallidos permanentemente
Unidad: Mensajes

Ejemplo:

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

Uso:

- Alertar cuando > 0 (requiere revisión manual)

smpp_cache_overflow_total

Tipo: Counter
Descripción: Número total de eventos de desbordamiento de caché donde el mensaje más antiguo fue expulsado para hacer espacio
Unidad: Eventos

Ejemplo:

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

Uso:

- Alertar cuando aumente (caché demasiado pequeña o interrupción de API demasiado larga)

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 de 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 no se exponen métricas)

Busca estos patrones para detectar problemas de 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 con el formato de respuesta

Configuración de Prometheus

Configuración Básica de Scrape

Agrega a `/etc/prometheus/prometheus.yml`:

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

Múltiples Gateways

```
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: Graph
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 fallos
      - 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 fallos de entrega en {{
$labels.bind_name }}"
          description: "La tasa de fallos de entrega es {{ $value
| humanizePercentage }} en {{ $labels.bind_name }}."

      # Fallos de enlace
      - alert: SMPPBindFailures
        expr: increase(smpp_bind_failures_total[10m]) > 3
        labels:
          severity: warning
        annotations:
          summary: "Múltiples fallos de enlace en {{
$labels.bind_name }}"
          description: "{{ $labels.bind_name }} ha fallado al
enlazar {{ $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: "La 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 expirando"
          description: "Se detectaron múltiples timeouts de 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 incorporada 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 de salida a operadores (mostrando conteo de conectados/desconectados)

- **Enlaces de Servidor**: Conexiones de entrada de socios (mostrando conteo activo/en espera)
- **Servidor Escuchando**: Configuración del socket de servidor de entrada (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 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

- Configurar alertas de Prometheus para métricas críticas
- Utilizar PagerDuty/OpsGenie para alertas 24/7
- Probar alertas regularmente

2. Crear Dashboards

- Construir dashboards de Grafana para cada gateway
- Incluir todas las conexiones en un solo dashboard
- Agregar paneles de planificación de capacidad

3. Revisiones Regulares

- Revisar métricas semanalmente
- Identificar tendencias y patrones
- Planificar ajustes de capacidad

4. Documentar Líneas Base

- Registrar volúmenes de mensajes normales
- Documentar tasas de TPS esperadas
- Anotar tiempos/días pico

5. Correlacionar con el Backend

- Monitorear 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

Verificar: `smpp_connection_status`

- Valor 0 = Revisar registros, verificar red, verificar credenciales
- Cambios frecuentes = Inestabilidad de red

Bajas Tasas de Entrega

Verificar: `smpp_delivery_failures_total`

- Alta tasa = Verificar estado del operador, revisar formato de mensaje
- Comparar entre conexiones = Identificar operador problemático

Bajo Rendimiento

Verificar: tasa de `smpp_messages_sent_total`

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

Problemas de Enlace

Verificar: `smpp_bind_failures_total`

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

Documentación Relacionada

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

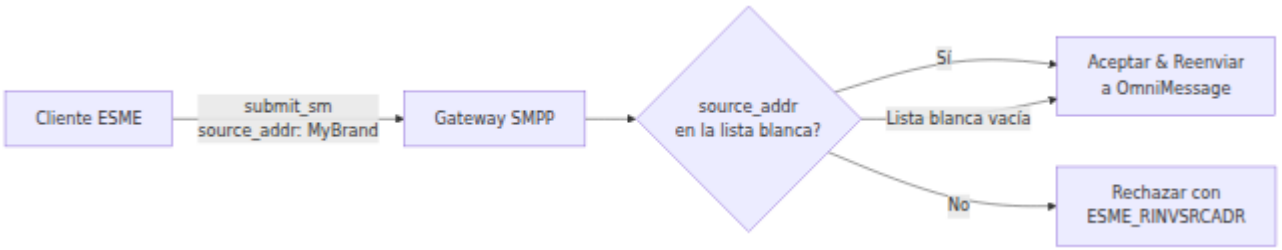
Lista Blanca de Direcciones de Origen

Control por par sobre qué direcciones de origen (source_addr) puede usar un cliente SMPP al enviar mensajes.

Descripción General

Cuando un ESME externo (cliente) envía un PDU `submit_sm` a través del Gateway SMPP, el PDU incluye un campo `source_addr` que representa la dirección de origen (CLI / ID del remitente). Por defecto, los clientes autenticados pueden usar cualquier dirección de origen. La función de Lista Blanca de Direcciones de Origen permite a los operadores restringir qué direcciones de origen cada par de servidor puede usar.

Esto sigue el mismo patrón que la Lista Blanca de IP existente: cuando la lista blanca está vacía, se permiten todos los valores. Cuando está poblada, solo se aceptan las direcciones de origen que coincidan.



Reglas de Coincidencia

La coincidencia de direcciones de origen admite dos modos:

Coincidencia Exacta

La dirección de origen debe coincidir exactamente con la entrada de la lista blanca. La coincidencia es **sensible a mayúsculas y minúsculas**.

Entrada de la Lista Blanca	Dirección de Origen	Resultado
`MyBrand`	`MyBrand`	Permitido
`MyBrand`	`mybrand`	Rechazado
`MyBrand`	`MyBrands`	Rechazado
`+61400000001`	`+61400000001`	Permitido

Coincidencia de Comodín (Prefijo)

Agregue `*` a una entrada de la lista blanca para coincidir con cualquier dirección de origen que comience con el prefijo antes del `*`.

Entrada de la Lista Blanca	Dirección de Origen	Resultado
`614*`	`61400000001`	Permitido
`614*`	`61412345678`	Permitido
`614*`	`61500000001`	Rechazado
`+614*`	`+61400000001`	Permitido
`My*`	`MyBrand`	Permitido
`My*`	`MyCompany`	Permitido

Múltiples Entradas

Cuando se configuran múltiples entradas, la dirección de origen se permite si coincide con **cualquiera** de las entradas en la lista blanca.

Ejemplo de lista blanca: `MyBrand, 614*, +61400000001`

Dirección de Origen	Coincide	Resultado
`MyBrand`	`MyBrand` (exacto)	Permitido
`61412345678`	`614*` (comodín)	Permitido
`+61400000001`	`+61400000001` (exacto)	Permitido
`OtherBrand`	Ninguna	Rechazado
`61500000001`	Ninguna	Rechazado

Manejo de Errores

Cuando un `submit_sm` es rechazado debido a una violación de la lista blanca de direcciones de origen, el gateway responde con:

Campo	Valor
PDU	`submit_sm_resp`
Estado del Comando	`0x0000000A`
Nombre del Error	`ESME_RINVSRCADR` (Dirección de Origen Inválida)
ID del Mensaje	Vacío

Se registra una advertencia con la dirección de origen rechazada y el nombre del par:

```
Servidor SMPP: Rechazado submit_sm de partner_acme - source_addr
'UnauthorisedBrand' no en la lista blanca
```

Configuración

A través de la Interfaz Web

1. Navegue a **SMPP > Servidores Peers**
2. Haga clic en **Editar** en el par objetivo (o **Agregar Nuevo Servidor Peer**)
3. Localice el campo **Lista Blanca de Direcciones de Origen** (debajo de la Lista Blanca de IP)
4. Ingrese patrones separados por comas:

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

5. Haga clic en **Guardar**

Los cambios entran en vigor de inmediato para nuevos PDUs `submit_sm` en conexiones existentes.

A través del Archivo de Configuración

Agregue `source_address_whitelist` a la configuración de enlace del servidor en `runtime.exs`:

```
config :omnimessage_smpp, :server_binds, [
  %{
    name: "partner_acme",
    system_id: "acme_corp",
    password: "secure_password",
    allowed_bind_types: [:transmitter, :receiver, :transceiver],
    ip_whitelist: ["203.0.113.0/24"],
    source_address_whitelist: ["MyBrand", "614*", "+61400000001"],
    tps_limit: 50,
    queue_check_frequency: 1000
  }
]
```

Parámetros

Parámetro	Tipo	Requerido	Predeterminado
`source_address_whitelist`	Lista de cadenas	No	`[]` (permitir todos)

Migración

Los pares de servidor existentes se migran automáticamente cuando se inicia el gateway. Los pares creados antes de que se añadiera esta función reciben una lista blanca vacía (todas las direcciones de origen permitidas), preservando el comportamiento existente.

Flujo de Validación

Ejemplos

Restringir a una Sola Marca

Solo permitir mensajes del ID del remitente `AcmeCorp`:

```
AcmeCorp
```

Permitir un Rango de Números Australianos

Permitir cualquier número de móvil australiano (que comience con `614`):

```
614*
```

Alfanumérico y Numérico Mixto

Permitir un nombre de marca y un rango de números:

```
AcmeCorp,614*,+61290000001
```

Permitir Todos (Predeterminado)

Deje el campo vacío para permitir cualquier dirección de origen. Este es el comportamiento predeterminado.

Solución de Problemas

Mensajes Rechazados con ESME_RINVSRCADR

Síntomas: El socio informa `submit_sm_resp` con estado de comando `0x0A`.

Causas posibles:

- La dirección de origen no coincide con ninguna entrada en la lista blanca
- La entrada de la lista blanca tiene un error tipográfico o patrón incorrecto
- Desajuste de mayúsculas y minúsculas (la coincidencia es sensible a mayúsculas y minúsculas)
- El patrón de comodín es demasiado restrictivo

Resolución:

1. Verifique la Lista Blanca de Direcciones de Origen del par del servidor en la Interfaz Web
2. Compare la dirección de origen rechazada con cada entrada de la lista blanca
3. Agregue la dirección de origen faltante o ajuste el patrón de comodín

4. Verifique que la coincidencia de mayúsculas y minúsculas sea exacta para las entradas no comodín

La Lista Blanca No Toma Efecto

Síntomas: Mensajes aceptados a pesar de que la dirección de origen no coincide con la lista blanca.

Causas posibles:

- La lista blanca está vacía (permite todo por defecto)
- El ESME está conectado a un par de servidor diferente
- El cambio en el archivo de configuración aún no se ha aplicado (requiere reinicio)

Resolución:

1. Verifique que la lista blanca esté poblada (no vacía) en la Interfaz Web
2. Verifique a qué par de servidor está vinculado el ESME en el Estado en Vivo
3. Si utiliza un archivo de configuración, reinicie el servicio

---

Documentación Relacionada

- **Referencia de Configuración** - Documentación completa de parámetros de pares de servidor
- **Guía de Uso** - Gestión de conexiones SMPP
- **Solución de Problemas** - Procedimientos generales de solución de problemas

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
- **Tiempos de espera**: Llamadas a la API que se agotan o se cuelgan
- **Los registros muestran**: "Conexión rechazada", "Tiempo de espera", "HTTP 503", "Conexión restablecida"

Diagnóstico

1. Verificar 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. Verificar 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. Verificar 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 caído:

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

2. Credenciales Incorrectas

Verificar:

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

Soluciones:

- Confirmar credenciales con el operador
- Verificar errores tipográficos (sensible a mayúsculas)
- Actualizar 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 keepalive
- Verificar firewalls agresivos que cierran 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 `tps_limit`
- Reducir TPS al 70-80% del máximo del operador
- Distribuir el tráfico entre múltiples enlaces

4. Problemas en el 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

Los Mensajes No Se Envían

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 marca de tiempo futura no se enviarán aún

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 Fallo en la 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 la razón del rechazo
- Puede ser necesario filtrar contenido
- Verificar patrones de spam/abuso

4. Mensajes Expirados

Verificar:

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

Soluciones:

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

---

Problemas de la 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 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 funciona localmente pero no remotamente: Verificar firewall
- Abrir el 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
- 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 el etiquetado 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 la CPU se mantiene alta

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 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 de backend - puede ser lento
4. Latencia de red hacia el operador

Soluciones:

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

Problemas de Configuración

Errores de Sintaxis en el Archivo de Configuración

Síntomas:

- El servicio no se inicia después del cambio de 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 del mapa
- Comillas desiguales (" vs ')
- Corchetes o llaves no emparejados
- 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
- Antiguas configuraciones aún activas

Soluciones:

```
# Los cambios en la 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 a 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

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

Documentación Relacionada

- **USAGE.md** - Procedimientos operativos normales
- **CONFIGURATION.md** - Referencia de configuración
- **MONITORING.md** - Monitoreo y métricas
- **README.md** - Visión general del sistema

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 la conectividad de la API
curl -k https://omnimessage-
core.example.com:8443/api/system/health

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

Operaciones Diarias

Verificación de Salud de la Mañana

Realizar estas verificaciones al inicio de cada día:

1. **Acceder al Panel Web**

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

2. **Verificar el Estado de Conexión**

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

3. **Revisar Métricas de Mensajes**

- Navegar a: pestaña de Cola
- Verificar que los conteos de mensajes sean razonables
- Asegurarse de que no haya acumulación inesperada en la cola

4. **Verificar Registros del Sistema**

- Navegar a: pestaña de Registros
- Buscar mensajes de error (rojo)
- Anotar cualquier patrón de advertencia

5. **Revisar Métricas de Prometheus**

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

Monitoreo Continuo

Configurar alertas para:

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

Ver MONITORING.md para la configuración de alertas.

Comprendiendo el Enrutamiento de Mensajes

La puerta de enlace enruta mensajes entre OmniMessage Core y conexiones SMPP utilizando dos campos clave:

- `dest_smsc` — Rutea mensajes salientes a **vínculos de cliente**. Cuando OmniMessage coloca un mensaje en la cola con `dest_smsc: "vodafone_uk"`, el vínculo de cliente de la puerta de enlace llamado `vodafone_uk` lo recoge y lo envía a través de SMPP `submit_sm`.
- `source_smsc` — Rutea mensajes entrantes a **vínculos de servidor**. Cuando OmniMessage coloca un mensaje en la cola con `source_smsc: "partner_acme"`, la puerta de enlace lo entrega a los clientes conectados al vínculo de servidor llamado `partner_acme` a través de SMPP `deliver_sm`.

Distinción clave: Los vínculos de cliente envían PDUs `submit_sm` (la puerta de enlace es el ESME que se presenta a un operador). Los vínculos de servidor envían PDUs `deliver_sm` (la puerta de enlace es el SMSC que entrega a un ESME conectado).

Registro del Frontend

La puerta de enlace se registra automáticamente con OmniMessage Core para que el backend sepa qué conexiones SMPP están disponibles para el enrutamiento de mensajes.

- **Nombre de registro**: Controlado por la configuración `smsc_name` (predeterminado: `"smpp_gateway"`, env: `SMSC_NAME`)
- **Heartbeat**: Enviado cada 60 segundos para mantener el registro activo
- **Expiración**: El registro expira en el backend después de 90 segundos sin un heartbeat
- **Registro por vínculo**: Cada par habilitado se registra individualmente utilizando el formato `{hostname}_{peer_name}`

Si la puerta de enlace se detiene o pierde conectividad con OmniMessage Core, sus registros expiran y el backend deja de enrutar mensajes hacia ella.

Solución de problemas: Si los mensajes no se están enrutando a la puerta de enlace, verifique:

1. Registros en busca de entradas "frontend_register"
2. Que el `smsc_name` coincida con lo que OmniMessage espera
3. Conectividad de red a OmniMessage Core (`api_base_url`)

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**: SMPP → Pestañas de Pares de Cliente / Pares de Servidor
- **Operaciones**: Agregar, editar, eliminar pares

- **Persistencia**: Almacenado 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 cambios
- **Mejor para**: Configuración inicial, infraestructura como código

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

Ver CONFIGURATION.md para 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: Reunir 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 (Recomendada)

Ventajas: Efecto inmediato, no se requiere reinicio

Pasos:

1. **Navegar a Pares de Clientes**:
    - Abrir la 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 la conexión de inmediato
    - Navegar a: SMPP → Estado en Vivo
    - El estado debería cambiar a "Conectado" (verde) dentro de 10-30 segundos

- Verificar la pestaña de Registros para el 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 el Archivo de Configuración**:

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

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

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

  # Agregar nuevo vínculo
  %{
    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 vínculo
    - Monitorear en Estado en Vivo para la transmisión
    - Verificar la confirmación de entrega

Agregar un Vínculo de Servidor

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

Preparación:

1. **Generar Credenciales**:
    - Crear un ID de sistema único: `partner_name`
    - Crear una contraseña fuerte
    - Documentar y compartir de forma 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 (Recomendada)

Ventajas: Efecto inmediato, no se requiere reinicio

Pasos:

1. **Navegar a Pares de Servidor**:
   - Abrir la Interfaz Web: `https://your-server:8087`
   - Navegar a: SMPP → Pares de Servidor
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: Según lo configurado
5. **Esperar la Conexión del Socio**:
    - Navegar a: SMPP → Estado en Vivo
    - Observar la conexión entrante
    - Verificar el éxito de la autenticación
    - Comprobar 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 el Archivo de Configuración**:

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

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

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

  # Agregar nuevo vínculo 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
  }
]

# Asegurarse 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 el 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: Según lo configurado

5. **Esperar la Conexión del Socio**:

   - Navegar a: SMPP → Estado en Vivo
   - Observar la conexión entrante
   - Verificar el éxito de la autenticación
   - Comprobar 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 (Recomendada)

Ventajas: Efecto inmediato, no se requiere reinicio

Pasos:

1. **Navegar a Pares**:

   - Abrir la Interfaz Web: `https://your-server:8087`
   - Para conexiones de cliente: SMPP → Pares de Clientes
   - Para conexiones de servidor: SMPP → Pares de Servidor

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**:
    - Comprobar 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 el Archivo de Configuración**:

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

2. **Modificar Parámetros de Vínculo**:
    - Encontrar el vínculo 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 el Servicio**:

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

4. **Verificar Cambios**:
    - Navegar a: SMPP → Estado en Vivo
    - Comprobar 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**:
    - Comprobar Estado en Vivo - la conexión debería haber desaparecido
    - Revisar registros para un apagado limpio

Habilitar y Deshabilitar Conexiones

Propósito: Llevar temporalmente una conexión fuera de línea sin eliminar su configuración

Los pares tienen un campo `enabled` que controla si están activos. Los pares deshabilitados conservan toda su configuración pero no establecen ni aceptan conexiones.

A través de la Interfaz Web:

1. Navegar a: SMPP → Pares de Clientes o Pares de Servidor
2. Encontrar el par a deshabilitar
3. Hacer clic en "Editar"
4. Desmarcar la casilla "Habilitado"
5. Hacer clic en "Guardar"

La conexión se eliminará de inmediato. Para volver a habilitar, repetir los pasos y marcar la casilla nuevamente.

Casos de uso:

- Ventanas de mantenimiento planificadas del operador
- Pausar temporalmente una conexión de socio durante una investigación
- Deshabilitar una conexión mientras se esperan nuevas credenciales

---

Comportamiento de Conexión

Lógica de Reconexión

Cuando un vínculo de cliente se desconecta inesperadamente, la puerta de enlace intenta reconectarse automáticamente:

- **Intervalo de reintento**: Cada 30 segundos
- **Inicio escalonado**: Cuando múltiples vínculos se inician simultáneamente (por ejemplo, después de un reinicio del servicio), las conexiones se

escalonan con retrasos de 500 ms entre cada vínculo para evitar abrumar la red
- **Inicio resiliente**: Si un operador no es accesible al inicio de la puerta de enlace, esta se inicia correctamente y reintenta la conexión en segundo plano

Enquire Link (Keepalive)

La puerta de enlace envía periódicamente PDUs SMPP `enquire_link` para verificar que las conexiones estén vivas:

- **Intervalo predeterminado**: 60 segundos (configurable por vínculo a través de `enquire_link_interval`)
- **Deshabilitar**: Establecer `enquire_link_interval: 0` (no recomendado)
- **Detección de fallos**: Si el par remoto deja de responder a enquire_link, la conexión se considera muerta y comienza la reconexión

Monitorear la salud de enquire link a través de las métricas de Prometheus `smpp_enquire_link_sent_total` y `smpp_enquire_link_received_total`. Una creciente brecha entre enviados y recibidos indica problemas de conexión.

Limitación de Tasa de TPS

Cada vínculo aplica su `tps_limit` utilizando una ventana deslizante por segundo:

- Los mensajes se cuentan dentro de cada ventana de 1 segundo
- Cuando se alcanza el límite, el trabajador de la cola se pausa hasta el siguiente segundo
- Un máximo de 100 mensajes puede estar en vuelo (esperando respuesta) por vínculo en cualquier momento
- La ventana se restablece automáticamente al inicio de cada nuevo segundo

Si observa un rendimiento lento, verifique que:

1. `tps_limit` esté configurado lo suficientemente alto para su tráfico

2. `queue_check_frequency` sea lo suficientemente bajo para mantener el flujo de la tubería
3. El operador esté respondiendo a los mensajes de manera oportuna (respuestas lentas reducen el rendimiento efectivo)

Gestión del Flujo de Mensajes

Verificación de la 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 de destino (dest_smsc)
        - Intentos de entrega
        - Estado

3. **Buscar Mensaje Específico**:
    - Usar filtro de búsqueda
    - Filtrar por destino, contenido o SMSC

Solución de Problemas de 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, ver 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 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 Vínculo

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 vínculo 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 de firewall
   - Verificar que el servidor del operador esté operativo
   - Contactar al soporte del operador
   - Ver TROUBLESHOOTING.md

Manejo de Fallos de Autenticación

Síntomas: Fallos de enlace repetidos en los registros

Causas:

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

Pasos:

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

- Confirmar la IP de su puerta de enlace con el operador
- Solicitar al operador verificar la lista blanca de IP

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

---

Monitoreo y Alertas

Verificación de 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. Ver 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. Comprobar 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. Comprobar 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 en la configuración
    - Actualizar información de contacto
    - Anotar ventanas de mantenimiento del operador

3. **Auditoría de Credenciales**:
    - Revisar todas las contraseñas de SMPP
    - Planificar rotación de credenciales
    - Verificar que las listas blancas de IP estén actualizadas
4. **Planificación de Capacidad**:
    - Revisar tasas de mensajes pico
    - Comprobar 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

Respaldo de Configuración

Respaldar archivos críticos antes de realizar cambios:

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

# Respaldar 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

Corte Completo del Servicio

Pasos:

1. **Verificar estado del servicio**:

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

2. **Si el servicio se detuvo, iniciarlo**:

```
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
   - Comprobar espacio en disco: `df -h`
   - Comprobar memoria: `free -h`

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

Solicitudes de Emergencia de Desconexión del Operador

Pasos:

1. **Eliminar conexión de inmediato**:

   - 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 limitadas
    - Puede ser necesario aumentar temporalmente los límites de TPS
2. **Monitorear la 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 tasa en la parte superior
4. **Escalar si es necesario**:
    - Puede ser necesario instancias adicionales de la puerta de enlace
    - Contactar soporte para consejos 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 en busca de acumulación
- [ ] Verificar paneles de Prometheus/Grafana
- [ ] Verificar tasas de éxito de entrega > 98%

Tareas Semanales

- [ ] Revisar tendencias de métricas
- [ ] Comprobar patrones anómalos
- [ ] 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
- [ ] Respaldar archivos de configuración

Documentación Relacionada

- **CONFIGURATION.md** - Configurar conexiones y ajustes
- **SOURCE_ADDRESS_WHITELIST.md** - Restringir direcciones de origen por par de servidor
- **MONITORING.md** - Configurar alertas de Prometheus

- **TROUBLESHOOTING.md** - Resolver problemas comunes
- **README.md** - Visión general del sistema
