OmniMessage SMPP Gateway - Guia de Operações

Versão: 1.0.0
Para Equipes de Operações

O que é o Gateway SMPP?

O Gateway SMPP da OmniMessage é um dos vários protocolos de frontend para a plataforma de telecomunicações OmniMessage. Ele permite o envio de mensagens SMS conectando sua infraestrutura a redes móveis usando o protocolo SMPP (Short Message Peer-to-Peer), padrão da indústria.

Importante: Este gateway é um frontend de protocolo sem estado. Ele não possui lógica de negócios, processamento de mensagens ou capacidades de armazenamento. Toda a inteligência vem do OmniMessage, acessado via REST API. Assim como outros frontends do OmniMessage (Diameter, MAP, IMS), ele simplesmente traduz mensagens de protocolo para o formato interno do OmniMessage e vice-versa.

Principais Capacidades

- **Mensagens SMPP Bidirecionais**: Enviar e receber mensagens SMS via SMPP
- **Conexões Múltiplas**: Conectar-se a múltiplos operadores simultaneamente
- **Alto Desempenho**: Processar milhares de mensagens por segundo
- **Monitoramento**: Métricas Prometheus integradas e painel web
- **Confiabilidade**: Reconexão automática e reenvio de mensagens
- **Operação Sem Estado**: Todo o processamento delegado ao backend do OmniMessage

Quem Deve Usar Este Guia?

Este guia é para equipes de operações responsáveis por:

- Instalar e configurar o gateway
- Monitorar o tráfego de mensagens
- Gerenciar conexões SMPP
- Solucionar problemas

Início Rápido

Configuração Inicial

1. **Acessar o Painel Web**: `https://your-server:8087`
2. **Verificar o Status do Sistema**: Navegue até SMPP → Status Ao Vivo
3. **Revisar a Configuração**: Veja CONFIGURATION.md
4. **Configurar Monitoramento**: Veja MONITORING.md

Operações Diárias

Tarefas operacionais comuns:

Tarefa	Ação
Verificar status da conexão	Web UI → SMPP → Status Ao Vivo
Visualizar tráfego de mensagens	Web UI → Fila
Monitorar saúde do sistema	Web UI → Logs ou métricas Prometheus
Adicionar/modificar conexões	Web UI → SMPP → Pares Cliente/Servidor

Veja OPERATIONS.md para procedimentos detalhados.

Arquitetura do Sistema

O Gateway SMPP é um tradutor de protocolo sem estado que opera como parte da plataforma OmniMessage:

Conceitos Chave:

- **Gateway SMPP**: Apenas tradutor de protocolo - sem processamento de mensagens, armazenamento ou lógica de negócios
- **OmniMessage**: Plataforma central que lida com toda a lógica de mensagens, roteamento e armazenamento
- **Comunicação API**: O gateway recupera mensagens a serem enviadas do OmniMessage e relata o status de entrega

Integração com OmniMessage

O Gateway SMPP da OmniMessage é um **frontend de protocolo** para a plataforma de mensagens OmniMessage. É um dos vários tipos de frontend idênticos que se conectam a redes móveis usando diferentes protocolos:

Frontend	Protocolo	Propósito
Gateway SMPP	SMPP (SMS)	Envio de mensagens SMS via protocolo SMPP
Gateway Diameter	Diameter	Mensagens baseadas em IMS
Gateway MAP	MAP	Sinalização de rede móvel

Frontend	Protocolo	Propósito
Gateway IMS	IMS	Subsistema de Mídia IP

Todos os frontends compartilham a mesma arquitetura: **Eles são tradutores de protocolo sem estado que delegam toda a inteligência ao OmniMessage Core**.

Como Funciona

Fluxo de Mensagem de Entrada (Sistema Externo → Operadora):

Fluxo de Mensagem de Saída (Operadora → Gateway SMPP):

O que o Gateway Faz

- Recebe PDUs SMPP de operadoras e clientes externos
- Analisa e valida mensagens de protocolo SMPP
- Traduz o formato SMPP para o formato interno do OmniMessage
- Chama a REST API do OmniMessage com os dados da mensagem
- Recebe mensagens do OmniMessage via polling da API
- Converte o formato do OmniMessage de volta para PDUs SMPP
- Relata recibos de entrega de volta ao OmniMessage

O que o Gateway NÃO Faz

- 🚫 Sem armazenamento ou persistência de mensagens
- 🚫 Sem decisões de roteamento (OmniMessage decide)
- 🚫 Sem limitação de taxa (OmniMessage impõe)
- 🚫 Sem validação de número (OmniMessage valida)
- 🚫 Sem rastreamento de estado (OmniMessage mantém estado)
- 🚫 Sem lógica de negócios (OmniMessage lida com toda a lógica)

API REST do OmniMessage

O gateway se comunica com o OmniMessage Core via REST API:

Configuração:

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

Principais Operações da API:

- `GET /api/message_queue?destination_smsc=<bind_name>` - Recuperar mensagens pendentes
- `PUT /api/messages/<id>/delivery_status` - Relatar recibo de entrega
- `GET /api/system/health` - Verificação de saúde

Formato da Mensagem: Mensagens na fila contêm todas as informações necessárias para entrega:

- Número de destino
- Corpo da mensagem
- Número de origem
- Prioridade
- Período de validade
- SMSC alvo (nome de ligação da operadora)

O gateway simplesmente recupera esses dados, os formata como SMPP, os envia para a operadora e relata o status de volta.

Estrutura da Documentação

Esta documentação está organizada nos seguintes guias:

- **CONFIGURATION.md** - Referência completa de configuração com todos os parâmetros explicados
- **MONITORING.md** - Guia de métricas Prometheus e alertas
- **OPERATIONS.md** - Procedimentos operacionais do dia a dia
- **TROUBLESHOOTING.md** - Problemas comuns e soluções
- **GLOSSARY.md** - Termos e definições

Pontos de Acesso

Painel Web

- **URL**: `https://your-server:8087`
- **Recursos**:
  - Verificar status da conexão SMPP
  - Monitorar fila de mensagens
  - Visualizar logs do sistema
  - Configurar pares SMPP
  - Acessar documentação

Métricas Prometheus

- **URL**: `http://your-server:4000/metrics`
- **Formato**: Formato de texto Prometheus
- **Uso**: Integração com Grafana/Prometheus

Endpoint da API

- **URL**: Configurado em `API_BASE_URL`
- **Propósito**: Integração do backend da fila de mensagens

Referência Rápida

Tarefas Comuns

Tarefa	Comando/Localização
Iniciar gateway	`systemctl start omnimessage-smpp`
Parar gateway	`systemctl stop omnimessage-smpp`
Reiniciar gateway	`systemctl restart omnimessage-smpp`
Ver logs	`journalctl -u omnimessage-smpp -f`
Verificar status	Web UI → SMPP → Status Ao Vivo
Ver métricas	`curl http://localhost:4000/metrics`
Editar config	`/opt/omnimessage-smpp/config/runtime.exs`

Arquivos Importantes

Arquivo	Propósito
`/opt/omnimessage-smpp/config/runtime.exs`	Configuração principal
`/opt/omnimessage-smpp/priv/cert/`	Certificados SSL
`/var/log/omnimessage-smpp/`	Logs da aplicação
`/etc/systemd/system/omnimessage-smpp.service`	Definição do serviço

Notas de Seguran��a

- **Web UI**: Usa HTTPS com seus certificados SSL
- **Comunicação API**: Pode verificar SSL ou usar certificados autoassinados
- **SMPP**: Protocolo em texto simples - use segurança de rede
- **Credenciais**: Armazenadas no arquivo de configuração - proteja o acesso

Próximos Passos

1. Revise **CONFIGURATION.md** para todas as opções de configuração
2. Configure **MONITORING.md** com Prometheus
3. Familiarize-se com **OPERATIONS.md** para tarefas diárias
4. Adicione aos favoritos **TROUBLESHOOTING.md** para referência rápida
5. Revise **GLOSSARY.md** para terminologia

Referência de Configuração

Guia completo para todos os parâmetros de configuração

Visão Geral da Arquitetura

O Gateway SMPP OmniMessage é um **frontend de protocolo sem estado** que traduz mensagens SMPP para/de OmniMessage. Toda a lógica de negócios, decisões de roteamento e armazenamento de mensagens são gerenciados pelo OmniMessage Core - o gateway simplesmente:

1. **Recebe** PDUs SMPP de operadoras e clientes
2. **Traduz** para o formato OmniMessage via REST API
3. **Consulta** o OmniMessage em busca de mensagens para enviar
4. **Envia** PDUs SMPP para as operadoras
5. **Relata** o status de entrega de volta ao OmniMessage

Isso é idêntico ao funcionamento de outros frontends do OmniMessage (Diameter, MAP, IMS) - todos são tradutores de protocolo sem estado que delegam ao OmniMessage Core.

Localização do Arquivo de Configuração

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

Importante: Após alterar a configuração, reinicie o gateway:

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

Estrutura da Configuração

O arquivo de configuração usa a sintaxe Elixir. Estrutura básica:

```
import Config

# Configurações globais
config :omnimessage_smpp,
  setting_name: value

# Vínculos SMPP
config :omnimessage_smpp, :binds, [
  %{
    name: "bind_name",
```

```
    # ... configurações de vínculo
  }
]
```

Configurações Globais

API_BASE_URL

URL da plataforma OmniMessage Core

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

Parâmetro	Tipo	Obrigatório	Padrão
`api_base_url`	String (URL)	Sim	-

Propósito: URL da plataforma OmniMessage Core. O gateway se comunica com o OmniMessage via REST API para todo o processamento de mensagens:

- **Enviar Mensagens**: Enviar mensagens SMPP recebidas para o OmniMessage para processamento
- **Recuperar Mensagens**: Consultar mensagens destinadas às operadoras SMPP
- **Relatar Status de Entrega**: Atualizar o status de entrega da mensagem de volta ao OmniMessage
- **Saúde do Sistema**: Verificações de saúde periódicas

Crítico: É aqui que o gateway obtém todo o seu "cérebro". O OmniMessage gerencia:

- ✓ Validação de mensagens e verificação de formato
- ✓ Decisões de roteamento (qual operadora usar)
- ✓ Limitação de taxa e controle de fluxo
- ✓ Validação de número
- ✓ Armazenamento e persistência de mensagens
- ✓ Lógica de nova tentativa de entrega
- ✓ Rastreamento de status

O gateway simplesmente traduz o formato SMPP ↔ OmniMessage.

Exemplos:

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

# HTTPS com nome do host
```

```
api_base_url: "https://omnimessage-core.company.com:8443"

# HTTP (não recomendado para produção)
api_base_url: "http://192.168.1.100:8080"
```

Requisitos de Rede:

- O gateway deve ter acesso à rede do OmniMessage Core
- Use HTTPS em produção (configure `verify_ssl_peer`)
- O firewall deve permitir HTTPS de saída na porta especificada

SMPP_POLL_INTERVAL

Frequência de verificação da fila (milissegundos)

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

Parâmetro	Tipo	Obrigatório	Padrão
`smpp_poll_interval`	Inteiro	Não	100

Propósito: Com que frequência (em milissegundos) cada cliente verifica a fila de mensagens.

Diretrizes:

- **Alto volume (>100 TPS)**: 100-500ms
- **Volume médio (10-100 TPS)**: 500-1000ms
- **Baixo volume (<10 TPS)**: 1000-2000ms

Variável de ambiente: `SMPP_POLL_INTERVAL`

VERIFY_SSL_PEER

Verificação de certificado SSL

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

Parâmetro	Tipo	Obrigatório	Padrão
`verify_ssl_peer`	Booleano	Não	false

Propósito: Se deve verificar os certificados SSL ao conectar-se à API de backend.

Valores:

- `true`: Verificar certificados (produção com certificados válidos)
- `false`: Ignorar verificação (certificados autoassinados, teste)

Variável de ambiente: `VERIFY_SSL_PEER`

SMSC_NAME

Identificador do gateway para registro

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

Parâmetro	Tipo	Obrigatório	Padrão
`smsc_name`	String	Não	"smpp_gateway"

Propósito: Identifica esta instância do gateway no backend da fila de mensagens.

Variável de ambiente: `SMSC_NAME`

Configuração de Vínculo do Cliente SMPP

Os vínculos do cliente são **conexões de saída** para servidores SMPP de operadoras.

Exemplo Completo de Vínculo do Cliente

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

    # Modo de conexão
    mode: :client,

    # Tipo de vínculo SMPP
    bind_type: :transceiver,

    # Endereço do servidor SMPP da operadora
    host: "smpp.vodafone.co.uk",
    port: 2775,

    # Credenciais de autenticação
    system_id: "your_username",
    password: "your_password",

    # Limitação de taxa
    tps_limit: 100,

    # Frequência de verificação da fila
```

```
    queue_check_frequency: 1000
  }
]
```

Parâmetros do Vínculo do Cliente

name

Identificador único da conexão

Tipo	Obrigatório	Exemplo
String	Sim	`"vodafone_uk"`

Propósito: Identifica de forma única esta conexão SMPP.

- Usado em logs e métricas
- Deve ser único entre todos os vínculos
- Use nomes descritivos (operadora, região, propósito)

Convenções de nomenclatura:

- `operadora_região`: `"vodafone_uk"`, `"att_us"`
- `número_proposito`: `"marketing_1"`, `"alerts_primary"`

mode

Tipo de conexão

Tipo	Obrigatório	Valor
Átomo	Sim	`:client`

Propósito: Define isso como uma conexão de saída.

Valor fixo: Sempre `:client` para conexões de saída.

bind_type

Tipo de sessão SMPP

Tipo	Obrigatório	Valores Permitidos
Átomo	Sim	`:transmitter`, `:receiver`, `:transceiver`

Propósito: Define a capacidade de direção da mensagem.

Opções:

- `:transmitter` - Enviar mensagens apenas (submit_sm)

- `:receiver` - Receber mensagens apenas (deliver_sm)
- `:transceiver` - Enviar e receber (mais comum)

Recomendação: Use `:transceiver` a menos que a operadora exija um tipo específico.

host

Nome do host ou IP do servidor SMPP da operadora

Tipo	Obrigatório	Exemplo
String	Sim	`"smpp.carrier.com"` ou `"10.5.1.100"`

Propósito: Endereço do servidor SMPP da operadora.

Exemplos:

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

port

Porta do servidor SMPP

Tipo	Obrigatório	Padrão	Faixa
Inteiro	Sim	2775	1-65535

Propósito: Porta TCP para a conexão SMPP.

Porta padrão: 2775

Exemplos:

```
port: 2775  # Padrão
port: 3000  # Personalizada
```

system_id

Nome de usuário de autenticação

Tipo	Obrigatório	Exemplo
String	Sim	`"company_user"`

Propósito: Nome de usuário fornecido pela operadora para autenticação.

Segurança: Proteja esta credencial - armazenada no arquivo de configuração.

password

Senha de autenticação

Tipo	Obrigatório	Exemplo
String	Sim	`"secret_password"`

Propósito: Senha fornecida pela operadora para autenticação.

Segurança:

- Proteja esta credencial
- Use senhas fortes
- Rotacione periodicamente

tps_limit

Limite de transações por segundo

Tipo	Obrigatório	Padrão	Faixa
Inteiro	Sim	100	1-10000

Propósito: Máximo de mensagens por segundo a serem enviadas através desta conexão.

Diretrizes:

- Defina para 70-80% do máximo da operadora
- Previne controle de fluxo/desconexão
- Permite margem para recibos de entrega

Exemplos:

```
tps_limit: 10    # Baixo volume
tps_limit: 50    # Volume médio
tps_limit: 100   # Alto volume (mais comum)
tps_limit: 1000  # Volume muito alto
```

Cálculo:

```
Se o máximo da operadora = 100 TPS
Defina tps_limit = 70-80
Deixa 20-30 TPS de margem
```

queue_check_frequency

Intervalo de polling da fila de mensagens (milissegundos)

Tipo	Obrigatório	Padrão	Faixa
Inteiro	Sim	1000	100-10000

Propósito: Com que frequência verificar o backend em busca de novas mensagens para enviar.

Diretrizes:

- **Alto volume (>100 TPS)**: 500-1000ms
- **Volume médio (10-100 TPS)**: 1000-2000ms
- **Baixo volume (<10 TPS)**: 2000-5000ms

Compensações:

- Valor mais baixo = coleta de mensagens mais rápida, mais carga na API
- Valor mais alto = coleta mais lenta, menos carga na API

Exemplo de UI Web:

Configuração de Vínculo do Servidor SMPP

Os vínculos do servidor definem **conexões de entrada** de clientes SMPP externos.

Exemplo Completo de Vínculo do Servidor

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

    # Credenciais esperadas do cliente
    system_id: "acme_corp",
    password: "acme_secret",

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

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

    # Limitação de taxa
    tps_limit: 50,

    # Frequência de verificação da fila
    queue_check_frequency: 1000
```

```
  }
]
```

Parâmetros do Vínculo do Servidor

name

Identificador do cliente

Tipo	Obrigatório	Exemplo
String	Sim	`"partner_acme"`

Propósito: Identifica o cliente externo que está se conectando a você.

Convenções de nomenclatura: Use o nome do parceiro/cliente para fácil identificação.

system_id

Nome de usuário esperado do cliente

Tipo	Obrigatório	Exemplo
String	Sim	`"acme_corp"`

Propósito: Nome de usuário que o cliente externo deve fornecer para autenticação.

Fornecer ao cliente: Compartilhe esta credencial com seu parceiro.

password

Senha esperada do cliente

Tipo	Obrigatório	Exemplo
String	Sim	`"secure_password"`

Propósito: Senha que o cliente externo deve fornecer para autenticação.

Segurança:

- Use senhas fortes
- Única por cliente
- Compartilhe com segurança com o parceiro

allowed_bind_types

Tipos de sessão permitidos

Tipo	Obrigatório	Padrão
Lista de Átomos	Sim	-

Propósito: Restringe quais tipos de vínculo o cliente pode usar.

Opções:

```
allowed_bind_types: [:transceiver]  # Apenas transceiver
allowed_bind_types: [:transmitter, :receiver]  # TX ou RX
allowed_bind_types: [:transmitter, :receiver, :transceiver]  #
Qualquer
```

Recomendação: Permita os três a menos que precise de restrições.

ip_whitelist

Endereços IP permitidos do cliente

Tipo	Obrigatório	Padrão	Formato
Lista de Strings	Sim	`[]`	IPs ou notação CIDR

Propósito: Segurança - permitir apenas conexões de IPs conhecidos.

Formatos:

- IP único: `"192.168.1.100"` (automaticamente `/32`)
- Sub-rede CIDR: `"192.168.1.0/24"`, `"10.0.0.0/8"`
- Mistura de ambos: `["192.168.1.0/24", "10.50.1.100"]`

Exemplos:

```
# Permitir qualquer IP (não recomendado)
ip_whitelist: []

# IP único
ip_whitelist: ["203.0.113.50"]

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

# Sub-rede
ip_whitelist: ["192.168.1.0/24"]

# Misto
```

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

Sub-redes comuns:

- `/32` - IP único (automático para IPs sem máscara)
- `/24` - 256 endereços (ex: 192.168.1.0-255)
- `/16` - 65.536 endereços (ex: 10.50.0.0-255.255)
- `/8` - 16.777.216 endereços (ex: 10.0.0.0-255.255.255.255)

tps_limit

Limite de mensagens por segundo

Igual ao `tps_limit` do vínculo do cliente - controla a taxa de deliver_sm de saída.

queue_check_frequency

Intervalo de polling da fila

Igual ao `queue_check_frequency` do vínculo do cliente - com que frequência verificar mensagens para entregar a este cliente.

Exemplo de UI Web:

Configuração de Escuta do Servidor

Quando os vínculos do servidor são configurados, o gateway escuta conexões de entrada.

Exemplo Completo de Escuta

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

Parâmetros de Escuta

host

Endereço IP para vincular

Tipo	Obrigatório	Padrão	Valores Comuns
String	Não	`"0.0.0.0"`	`"0.0.0.0"`, `"127.0.0.1"`

Propósito: Em qual interface de rede escutar.

Valores:

- `"0.0.0.0"` - Escutar em todas as interfaces (recomendado)
- `"127.0.0.1"` - Escutar apenas no localhost (teste)
- `"192.168.1.10"` - Escutar em IP específico

port

Porta TCP para escutar

Tipo	Obrigatório	Padrão	Faixa
Inteiro	Não	2775	1-65535

Propósito: Porta para conexões SMPP de entrada.

Padrão: 2775

max_connections

Número máximo de conexões simultâneas

Tipo	Obrigatório	Padrão	Faixa
Inteiro	Não	100	1-10000

Propósito: Limita o número total de conexões simultâneas de clientes.

Diretrizes:

- Defina com base nos clientes esperados
- Valores mais altos usam mais memória
- Típico: 10-100 conexões

Exemplos Completos de Configuração

Exemplo 1: Conexão de Um Único Transportador

```
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
  }
]
```

Exemplo 2: Múltiplos Transportadores

```
import Config

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

config :omnimessage_smpp, :binds, [
  # América do 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
  }
]
```

Exemplo 3: Gateway com Vínculos de Servidor

```
import Config

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

# Conexões de saída
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
  }
]

# Definições de clientes de entrada
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
  }
]

# Escuta do servidor
config :omnimessage_smpp, :listen, %{
  host: "0.0.0.0",
  port: 2775,
```

```
  max_connections: 100
}
```

Validação da Configuração

Após editar a configuração, valide antes de reiniciar:

Verificação de Sintaxe

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

Se a sintaxe for inválida, você verá um erro. Corrija antes de reiniciar.

Testar Configuração

```
# Reiniciar em primeiro plano para ver erros
sudo -u omnimessage-smpp /opt/omnimessage-smpp/bin/omnimessage-smpp
console
```

Pressione `Ctrl+C` duas vezes para sair.

Melhores Práticas de Segurança

1. **Proteja o arquivo de configuração**:

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

2. **Use senhas fortes**:

   - Mínimo de 12 caracteres
   - Misture letras, números, símbolos
   - Única por conexão

3. **Use listas brancas de IP**:

   - Sempre configure `ip_whitelist` para vínculos de servidor
   - Nunca use lista vazia `[]` em produção

4. **Ative a verificação SSL**:

   - Defina `verify_ssl_peer: true` com certificados válidos

5. **Rotação regular de credenciais**:
    - Altere senhas trimestralmente
    - Coordene com operadoras/parceiros

Próximos Passos

- Revise MONITORING.md para configuração de métricas
- Leia OPERATIONS.md para gerenciar conexões
- Veja TROUBLESHOOTING.md para problemas comuns
- Retorne ao README.md para uma visão geral

Glossário

Termos e Definições

A

API (Application Programming Interface) Interface usada para se comunicar com o sistema de backend da fila de mensagens.

Auto-Scroll Recurso na aba de Logs da interface web que rola automaticamente para mostrar as entradas de log mais recentes.

B

Backend O sistema de fila de mensagens ao qual o Gateway SMPP se conecta para recuperar e armazenar mensagens.

Bind Uma conexão SMPP entre dois sistemas. Pode ser transmissor, receptor ou transceptor.

Bind Type O tipo de sessão SMPP:

- **Transmissor**: Enviar mensagens apenas
- **Receptor**: Receber mensagens apenas
- **Transceptor**: Enviar e receber mensagens

Bind Failure Quando uma tentativa de autenticação SMPP falha, geralmente devido a credenciais incorretas ou restrições de IP.

C

CIDR (Classless Inter-Domain Routing) Notação para especificar intervalos de endereços IP (por exemplo, `192.168.1.0/24` representa 256 endereços IP).

Client Bind Uma conexão SMPP de saída do gateway para o servidor SMPP de um operador.

Connection Status Estado atual de um bind SMPP:

- **Conectado**: Ativo e operacional
- **Desconectado**: Não conectado
- **Reconectando**: Tentando estabelecer conexão

Counter Uma métrica que só aumenta (reinicia na reinicialização do serviço), usada para totais como mensagens enviadas.

D

Data Coding Campo SMPP que especifica a codificação de caracteres da mensagem (GSM-7, UCS-2, etc.).

Delivery Failure Quando uma mensagem não pode ser entregue, indicado por uma resposta de erro do operador.

Delivery Receipt (DLR) Confirmação do operador sobre o status de entrega da mensagem.

dest_smsc Campo na fila de mensagens que indica qual conexão SMPP deve lidar com a mensagem.

Disconnection Quando uma conexão SMPP ativa é encerrada, seja intencionalmente ou devido a um erro.

E

Enquire Link Mensagem de keepalive SMPP enviada periodicamente para verificar se a conexão está ativa.

ESM Class Campo SMPP que indica o tipo e os recursos da mensagem.

Exponential Backoff Estratégia de nova tentativa onde o tempo de espera dobra após cada falha (1min, 2min, 4min, 8min...).

F

Firewall Sistema de segurança de rede que controla o tráfego de rede de entrada e saída.

G

Gateway O aplicativo Gateway SMPP que faz a ponte entre a fila de mensagens e as redes móveis.

Gauge Uma métrica que pode aumentar ou diminuir, representando o valor atual (por exemplo, status da conexão).

Grafana Ferramenta de visualização popular para exibir métricas do Prometheus em painéis.

GSM-7 Codificação de caracteres padrão de 7 bits para SMS, suportando até 160 caracteres por mensagem.

H

HTTP/HTTPS Protocolos usados para comunicação web. HTTPS é a versão criptografada.

I

IP Whitelist Lista de endereços IP permitidos que podem se conectar ao gateway (recurso de segurança).

ISDN (Integrated Services Digital Network) Plano de numeração comumente usado para números de telefone.

J

(Sem termos)

K

Keepalive Mensagens periódicas (enquire_link) enviadas para manter a conexão e detectar falhas.

KPI (Key Performance Indicator) Valor mensurável que indica o desempenho do sistema (por exemplo, taxa de sucesso de entrega).

L

Label No Prometheus, pares de chave-valor anexados a métricas para identificação (por exemplo, `bind_name="vodafone_uk"`).

LiveView Tecnologia do framework Phoenix usada para atualizações em tempo real da interface web.

M

Message Queue Sistema de backend que armazena mensagens aguardando para serem enviadas ou recebidas.

Metrics Medições quantitativas do desempenho do sistema, expostas no formato Prometheus.

MO (Mobile Originated) Mensagens enviadas de telefones móveis para o

gateway (entrada).

MT (Mobile Terminated) Mensagens enviadas do gateway para telefones móveis (saída).

MSISDN (Mobile Station International Subscriber Directory Number) Formato padrão para números de telefone móvel.

N

NPI (Numbering Plan Indicator) Campo SMPP que especifica o esquema de numeração (por exemplo, ISDN).

O

Outbound Mensagens fluindo do gateway para as redes móveis.

Inbound Mensagens fluindo das redes móveis para o gateway.

P

PDU (Protocol Data Unit) Pacote de mensagem SMPP individual (por exemplo, submit_sm, deliver_sm).

Prometheus Sistema de monitoramento de código aberto que coleta e armazena métricas de séries temporais.

Q

Queue Lista de mensagens aguardando para serem processadas ou enviadas.

Queue Check Frequency Com que frequência (em milissegundos) o gateway consulta o backend em busca de novas mensagens.

Queue Worker Componente que recupera mensagens da fila e as envia via SMPP.

R

Rate Limiting Controle do throughput de mensagens para cumprir as restrições do operador. Veja TPS.

Receiver Tipo de bind SMPP que apenas recebe mensagens (deliver_sm).

Reconnect Restabelecendo uma conexão SMPP desconectada.

Retry Tentando enviar uma mensagem falhada novamente, geralmente com backoff exponencial.

S

Server Bind Configuração que define um cliente externo permitido a se conectar ao gateway.

Session Conexão SMPP ativa entre dois sistemas.

SMPP (Short Message Peer-to-Peer) Protocolo padrão da indústria para troca de mensagens SMS entre sistemas.

SMSC (Short Message Service Center) Sistema que gerencia o roteamento e a entrega de mensagens SMS.

SSL/TLS Protocolos de criptografia para comunicação segura.

Submit_SM PDU SMPP para submeter uma mensagem para entrega.

Submit_SM_Resp Resposta SMPP ao submit_sm, indicando sucesso ou falha.

System ID Nome de usuário usado para autenticação SMPP.

T

Telemetry Coleta e transmissão automatizada de métricas do sistema.

TON (Type of Number) Campo SMPP que especifica o formato do número (por exemplo, internacional, nacional).

TPS (Transactions Per Second) Limite de taxa para o máximo de mensagens por segundo através de uma conexão.

Transceiver Tipo de bind SMPP que pode enviar e receber mensagens (mais comum).

Transmitter Tipo de bind SMPP que apenas envia mensagens (submit_sm).

Throughput Taxa de processamento de mensagens, tipicamente medida em mensagens por segundo.

U

UCS-2 Codificação de caracteres Unicode de 16 bits para SMS, suportando até 70 caracteres por mensagem.

Uptime Duração que uma conexão ou serviço esteve continuamente operacional.

V

Validity Period Limite de tempo para a tentativa de entrega da mensagem antes da expiração.

W

Web Dashboard Interface de usuário baseada em navegador para monitorar e gerenciar o gateway.

Whitelist Veja IP Whitelist.

X

(Sem termos)

Y

(Sem termos)

Z

(Sem termos)

Referência Rápida de Acrônimos

Acrônimo	Termo Completo
API	Application Programming Interface
CIDR	Classless Inter-Domain Routing
DLR	Delivery Receipt
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISDN	Integrated Services Digital Network
KPI	Key Performance Indicator
MO	Mobile Originated
MSISDN	Mobile Station International Subscriber Directory Number
MT	Mobile Terminated
NPI	Numbering Plan Indicator

Acrônimo	Termo Completo
PDU	Protocol Data Unit
SMPP	Short Message Peer-to-Peer
SMSC	Short Message Service Center
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TON	Type of Number
TPS	Transactions Per Second
UCS	Universal Coded Character Set
UI	User Interface
URL	Uniform Resource Locator

Documentação Relacionada

- **README.md** - Visão geral do sistema e como começar
- **CONFIGURATION.md** - Parâmetros de configuração explicados
- **OPERATIONS.md** - Operações do dia a dia
- **MONITORING.md** - Métricas e monitoramento
- **TROUBLESHOOTING.md** - Resolução de problemas

Guia de Monitoramento e Métricas

Referência completa para monitorar o SMPP Gateway

Visão Geral

O SMPP Gateway expõe métricas no formato Prometheus para monitorar a saúde da conexão, a taxa de mensagens e o desempenho do sistema.

Crítico: Como o gateway é sem estado e depende do OmniMessage Core, **a conectividade do OmniMessage é a métrica mais importante a ser monitorada**. Monitore ambos:

1. **Métricas do SMPP Gateway** - Saúde em nível de protocolo
2. **Métricas da API OmniMessage** - Conectividade e saúde do backend

Endpoint de Métricas

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

Formato: Formato de texto Prometheus

Acesso: Aberto para localhost por padrão (configure o firewall para acesso remoto)

Teste Rápido

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

Métricas Disponíveis

Todas as métricas são prefixadas com `smpp_` e incluem rótulos para identificação.

Métricas de Status da Conexão

smpp_connection_status

Tipo: Gauge
Descrição: Status atual da conexão do SMPP bind
Valores:

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

Rótulos:

- `bind_name` - Nome da conexão (ex: "vodafone_uk")
- `mode` - Tipo de conexão ("client" ou "server")
- `host` - Host remoto (apenas modo cliente)
- `port` - Porta remota (apenas modo cliente)
- `bind_type` - Tipo de bind SMPP (apenas modo cliente)
- `system_id` - ID do sistema utilizado

Exemplo:

```
smpp_connection_status{bind_name="vodafone_uk",mode="client",host="smpp.vodafone.co.uk",port="2775",bind_type="transceiver",system_id="user1"}
1
```

Uso:

- Alertar quando o valor for 0 (desconectado)
- Rastrear a porcentagem de tempo de atividade da conexão
- Monitorar a frequência de reconexões

Contadores de Mensagens

smpp_messages_sent_total

Tipo: Counter
Descrição: Número total de mensagens enviadas através do SMPP bind
Unidade: Mensagens

Rótulos: Mesmo que connection_status

Exemplo:

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

Uso:

- Calcular a taxa de mensagens (mensagens/segundo)
- Rastrear o volume diário/mensal
- Comparar a taxa real com a esperada

smpp_messages_received_total

Tipo: Counter
Descrição: Número total de mensagens recebidas através do SMPP bind
Unidade: Mensagens

Rótulos: Mesmo que connection_status

Exemplo:

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

Uso:

- Monitorar o volume de mensagens recebidas
- Rastrear o tráfego originado em dispositivos móveis (MO)
- Alertar sobre mudanças inesperadas no volume

Métricas de Entrega

smpp_delivery_failures_total

Tipo: Counter
Descrição: Número total de falhas na entrega de mensagens
Unidade: Falhas

Rótulos: Mesmo que connection_status

Exemplo:

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

Uso:

- Calcular a taxa de sucesso na entrega
- Alertar sobre altas taxas de falhas
- Identificar conexões problemáticas

Cálculo da Taxa de Sucesso:

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

Métricas de Operação de Bind

smpp_bind_success_total

Tipo: Counter
Descrição: Número total de operações de bind bem-sucedidas
Unidade: Tentativas de bind

Exemplo:

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

Uso:

- Rastrear a estabilidade do bind
- Monitorar o sucesso da autenticação

smpp_bind_failures_total

Tipo: Counter
Descrição: Número total de operações de bind falhadas
Unidade: Tentativas de bind

Exemplo:

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

Uso:

- Alertar sobre falhas de autenticação
- Identificar problemas de credenciais
- Rastrear problemas de conexão com a operadora

Métricas de Eventos de Conexão

smpp_connection_attempts_total

Tipo: Counter
Descrição: Número total de tentativas de conexão
Unidade: Tentativas

Exemplo:

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

Uso:

- Rastrear a rotatividade de conexões
- Monitorar a frequência de reconexões

smpp_disconnection_total

Tipo: Counter
Descrição: Número total de desconexões
Unidade: Desconexões

Exemplo:

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

Uso:

- Alertar sobre desconexões frequentes

- Identificar problemas de rede
- Rastrear a estabilidade da conexão

Métricas de Tempo de Atividade

smpp_uptime_seconds

Tipo: Gauge
Descrição: Tempo de atividade atual do SMPP bind em segundos
Unidade: Segundos

Exemplo:

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

Uso:

- Rastrear a estabilidade da conexão
- Calcular a porcentagem de tempo de atividade
- Alertar sobre reinicializações recentes

Métricas de Saúde da API OmniMessage

Enquanto o gateway em si expõe métricas relacionadas ao SMPP, **a saúde da API OmniMessage é crítica**. Você também deve monitorar:

Das Métricas do OmniMessage (se disponíveis)

- `omnimessage_api_requests_total` - Total de solicitações da API do gateway
- `omnimessage_api_request_duration_seconds` - Tempos de resposta da API
- `omnimessage_queue_depth` - Mensagens pendentes na fila do OmniMessage

Dos Logs do Gateway (se métricas não expostas)

Procure por esses padrões para detectar problemas na API:

- "api.*connection refused" - Não é possível alcançar o OmniMessage
- "api.*timeout" - OmniMessage não está respondendo
- "api.*http 503" - OmniMessage temporariamente fora do ar
- "api.*parse error" - Problema no formato da resposta

Configuração do Prometheus

Configuração Básica de Scrape

Adicione em `/etc/prometheus/prometheus.yml`:

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

Múltiplos Gateways

```yaml
scrape_configs:
  - job_name: 'omnimessage-smpp-instances'
    scrape_interval: 15s
    static_configs:
      - targets:
        - 'smpp-gw-1:4000'
        - 'smpp-gw-2:4000'
        - 'smpp-gw-3:4000'
        labels:
          environment: 'production'
```

Descoberta de Serviço

Usando descoberta baseada em arquivo:

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

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

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

Painéis de Dashboard do Grafana

Painéis de Dashboard de Exemplo

Painel de Status da Conexão

Consulta:

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

Visualização: Stat
Limites:

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

Painel de Taxa de Mensagens

Consulta:

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

Visualização: Gráfico
Unidade: mensagens/segundo
Legenda: {{bind_name}}

Painel de Taxa de Sucesso na Entrega

Consulta:

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

Visualização: Gauge
Unidade: Porcentagem (0-100)
Limites:

- Vermelho: < 95%
- Amarelo: 95-98%
- Verde: > 98%

Painel de Tempo de Atividade da Conexão

Consulta:

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

Visualização: Stat
Unidade: Horas

Regras de Alerta

Regras de Alerta do Prometheus

Salve em `/etc/prometheus/rules/smpp-alerts.yml`:

```yaml
groups:
  - name: smpp_gateway
    interval: 30s
    rules:
      # Conexão fora do ar
      - alert: SMPPConnectionDown
        expr: smpp_connection_status == 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "A conexão SMPP {{ $labels.bind_name }} está fora do ar"
          description: "A conexão {{ $labels.bind_name }} foi desconectada por mais de 2 minutos."

      # Alta taxa de falhas
      - 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 taxa de falhas de entrega em {{ $labels.bind_name }}"
          description: "A taxa de falhas de entrega é {{ $value | humanizePercentage }} em {{ $labels.bind_name }}."

      # Falhas de bind
      - alert: SMPPBindFailures
        expr: increase(smpp_bind_failures_total[10m]) > 3
        labels:
          severity: warning
        annotations:
          summary: "Múltiplas falhas de bind em {{ $labels.bind_name }}"
          description: "{{ $labels.bind_name }} falhou ao bindar {{ $value }} vezes nos últimos 10 minutos."
```

```
    # Nenhuma mensagem enviada (quando esperado)
    - alert: SMPPNoTraffic
      expr: rate(smpp_messages_sent_total[10m]) == 0
      for: 30m
      labels:
        severity: warning
      annotations:
        summary: "Nenhuma mensagem enviada em {{ $labels.bind_name }}"
        description: "{{ $labels.bind_name }} não enviou nenhuma mensagem por 30 minutos."

    # Desconexões frequentes
    - alert: SMPPFrequentDisconnections
      expr: increase(smpp_disconnection_total[1h]) > 5
      labels:
        severity: warning
      annotations:
        summary: "Desconexões frequentes em {{ $labels.bind_name }}"
        description: "{{ $labels.bind_name }} desconectou {{ $value }} vezes na última hora."

    # API OmniMessage inacessível
    - alert: OmniMessageAPIUnreachable
      expr: |
        count(count_over_time({job="omnimessage-smpp"} |= "api.*connection refused"[5m])) > 0
      for: 1m
      labels:
        severity: critical
      annotations:
        summary: "API OmniMessage está inacessível"
        description: "O SMPP Gateway não consegue alcançar a API OmniMessage. Verifique a configuração de API_BASE_URL e a conectividade de
rede."

    # Timeouts da API OmniMessage
    - alert: OmniMessageAPITimeout
      expr: |
        count(count_over_time({job="omnimessage-smpp"} |= "api.*timeout"[5m])) > 5
      for: 2m
      labels:
        severity: warning
      annotations:
        summary: "API OmniMessage está com timeout"
        description: "Múltiplos timeouts da API detectados. O OmniMessage pode estar lento ou sobrecarregado."

    # Nenhum fluxo de mensagem (problema na 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: "Nenhum fluxo de mensagem detectado - verifique a conectividade do OmniMessage"
        description: "Nenhuma mensagem enviada ou recebida por 30 minutos. Verifique a conectividade da API OmniMessage e o status da fila."
```

Carregue as regras em `prometheus.yml`:

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

Monitoramento do Dashboard Web

A interface web integrada fornece monitoramento em tempo real sem o Prometheus.

Acesso

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

Página de Status Ao Vivo

Navegação: SMPP → Status Ao Vivo

Recursos:

- Status de conexão em tempo real
- Contadores de mensagens
- Tempo de atividade da conexão
- Controles manuais de reconexão/desconexão
- Atualização automática a cada 5 segundos

Uso:

- Verificação rápida de status
- Intervenção manual
- Solução de problemas em tempo real

O dashboard exibe:

- **Total de Binds**: Contagem combinada de todas as conexões de cliente e servidor
- **Binds de Cliente**: Conexões de saída para operadoras (mostrando contagem de conectado/desconectado)
- **Binds de Servidor**: Conexões de entrada de parceiros (mostrando contagem de ativo/aguardando)
- **Servidor Escutando**: Configuração do socket de servidor de entrada (host, porta, conexões máximas)

Monitoramento de Logs

Logs do Sistema

Visualizar logs:

```
# Acompanhar logs em tempo real
sudo journalctl -u omnimessage-smpp -f

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

# Desde um horário específico
sudo journalctl -u omnimessage-smpp --since "1 hour ago"

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

Logs da Interface Web

Navegação: Aba de logs na interface web

Recursos:

- Streaming de logs em tempo real
- Filtrar por nível (debug, info, warning, error)
- Buscar logs
- Pausar/retomar
- Limpar logs

A visualização de logs permite que você:

- **Filtrar por Nível**: Selecionar nível de log (Todos, Debug, Info, Warning, Error)
- **Buscar**: Encontrar entradas de log específicas por conteúdo de texto
- **Auto-rolar**: Habilitar/desabilitar rolagem automática à medida que novos logs chegam
- **Pausar/Retomar**: Pausar atualizações de log para revisar entradas específicas
- **Limpar**: Limpar todos os logs exibidos

Indicadores-Chave de Desempenho (KPIs)

Saúde da Conexão

Métrica: Porcentagem de tempo de atividade da conexão

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

Meta: > 99.9%

Taxa de Entrega de Mensagens

Métrica: Mensagens entregues por segundo

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

Meta: Corresponde ao volume esperado

Taxa de Sucesso na Entrega

Métrica: Porcentagem de entregas bem-sucedidas

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

Meta: > 98%

Estabilidade do Bind

Métrica: Tentativas de bind por hora

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

Meta: < 10 por hora (indica conexão estável)

Melhores Práticas de Monitoramento

1. Configurar Alertas

- Configure alertas do Prometheus para métricas críticas
- Use PagerDuty/OpsGenie para alertas 24/7
- Teste alertas regularmente

2. Criar Dashboards

- Construa dashboards do Grafana para cada gateway
- Inclua todas as conexões em um dashboard
- Adicione painéis de planejamento de capacidade

3. Revisões Regulares

- Revise métricas semanalmente
- Identifique tendências e padrões
- Planeje ajustes de capacidade

4. Documentar Linhas de Base

- Registre volumes normais de mensagens
- Documente taxas de TPS esperadas
- Anote horários/dias de pico

5. Correlacionar com o Backend

- Monitore métricas da API do backend
- Rastreie o fluxo de mensagens de ponta a ponta
- Identifique gargalos

Solução de Problemas com Métricas

Problemas de Conexão

Verifique: `smpp_connection_status`

- Valor 0 = Revise logs, verifique a rede, verifique credenciais
- Mudanças frequentes = Instabilidade na rede

Baixas Taxas de Entrega

Verifique: `smpp_delivery_failures_total`

- Alta taxa = Verifique o status da operadora, revise o formato da mensagem
- Compare entre conexões = Identifique a operadora problemática

Baixa Taxa de Transferência

Verifique: taxa de `smpp_messages_sent_total`

- Abaixo do esperado = Verifique limites de TPS, disponibilidade da fila
- Verifique métricas da API do backend

Problemas de Bind

Verifique: `smpp_bind_failures_total`

- Aumentando = Problemas de autenticação, problemas de credenciais
- Verifique system_id e senha na configuração

Documentação Relacionada

- **CONFIGURATION.md** - Configurar configurações de monitoramento
- **OPERATIONS.md** - Procedimentos operacionais
- **TROUBLESHOOTING.md** - Resolver problemas
- **README.md** - Visão geral e início rápido

Guia de Operações

Procedimentos operacionais do dia-a-dia

Dependência Crítica: OmniMessage Core

IMPORTANTE: O Gateway SMPP do OmniMessage não pode funcionar sem acesso ao OmniMessage Core. Todo o processamento de mensagens acontece no OmniMessage - o gateway é apenas um tradutor de protocolo.

Se o OmniMessage ficar indisponível:

- 🔀 Novas mensagens não podem ser enviadas
- 🔀 Mensagens pendentes não podem ser recuperadas
- 🔀 O status de entrega não pode ser reportado
- 🔀 O sistema parece travar ou expirar

Verifique a Saúde do OmniMessage:

```
# Testar conectividade da API
curl -k https://omnimessage-core.example.com:8443/api/system/health

# Verificar URL da API configurada nos logs
grep api_base_url /opt/omnimessage-smpp/config/runtime.exs
```

Operações Diárias

Verificação de Saúde Matinal

Realize essas verificações no início de cada dia:

1. **Acessar o Painel da Web**
    - URL: `https://your-server:8087`
    - Verifique se o painel carrega corretamente
2. **Verificar Status da Conexão**
    - Navegue para: SMPP → Status Ao Vivo
    - Verifique se todas as conexões mostram "Conectado" (verde)
    - Anote quaisquer binds desconectados
3. **Revisar Métricas de Mensagens**

    - Navegue para: aba Fila
    - Verifique se as contagens de mensagens são razoáveis
    - Verifique se não há acúmulo inesperado na fila

4. **Verificar Logs do Sistema**

    - Navegue para: aba Logs
    - Procure por mensagens de erro (vermelho)
    - Anote quaisquer padrões de aviso

5. **Revisar Métricas do Prometheus**

    - `curl http://localhost:4000/metrics`
    - Ou verifique os painéis do Grafana
    - Verifique se as taxas de mensagens estão normais

Monitoramento Contínuo

Configure alertas para:

- Falhas de conexão (> 2 minutos fora)
- Altas taxas de falha de entrega (> 5%)
- Sem tráfego por períodos prolongados
- Desconexões frequentes

Veja MONITORING.md para configuração de alertas.

Gerenciando Conexões SMPP

Como os Pares SMPP São Configurados

As conexões SMPP (pares) podem ser configuradas usando **dois métodos**:

Método 1: Interface Web (Recomendado)

- **Vantagem**: As mudanças entram em vigor imediatamente, sem necessidade de reinício
- **Localização**: SMPP → Abas Clientes / Servidores
- **Operações**: Adicionar, editar, excluir pares
- **Persistência**: Armazenado no banco de dados Mnesia
- **Melhor para**: Operações do dia-a-dia, testes, mudanças rápidas

Método 2: Arquivo de Configuração

- **Vantagem**: Configuração como código, controle de versão
- **Localização**: `/opt/omnimessage-smpp/config/runtime.exs`

- **Operações**: Definir pares na configuração Elixir
- **Persistência**: Baseado em arquivo, sobrevive a reinicializações
- **Requer**: Reinício do serviço após mudanças
- **Melhor para**: Configuração inicial, infraestrutura como código

Nota: As mudanças na interface web são armazenadas separadamente e substituem as configurações do arquivo de configuração.

Veja CONFIGURATION.md para referência do arquivo de configuração.

Adicionando uma Nova Conexão de Cliente

Objetivo: Conectar a um novo servidor SMPP de operadora

Preparação: Reúna informações da operadora:

- Nome do host/IP do servidor SMPP
- Número da porta (geralmente 2775)
- ID do sistema (nome de usuário)
- Senha
- Tipo de bind (geralmente transceiver)
- Limite de TPS

Escolha um dos seguintes métodos:

Opção A: Via Interface Web (Recomendado)

Vantagens: Efeito imediato, sem necessidade de reinício

Passos:

1. **Navegar para Pares de Clientes**:
    - Abra a Interface Web: `https://your-server:8087`
    - Navegue para: SMPP → Pares de Clientes
2. **Adicionar Novo Par**:
    - Clique em "Adicionar Novo Par de Cliente"
    - Preencha o formulário:
        - **Nome**: `vodafone_uk` (identificador único)
        - **Host**: `smpp.vodafone.co.uk`
        - **Porta**: `2775`
        - **ID do Sistema**: `your_username`
        - **Senha**: `your_password`
        - **Tipo de Bind**: `Transceiver`
        - **Limite de TPS**: `100`
        - **Frequência de Verificação da Fila**: `1000`

- Clique em "Salvar"

3. **Conexão Estabelece Automaticamente**:
   - O gateway tenta imediatamente a conexão
   - Navegue para: SMPP → Status Ao Vivo
   - O status deve mudar para "Conectado" (verde) dentro de 10-30 segundos
   - Verifique a aba de Logs para mensagem de bind bem-sucedida

4. **Testar Fluxo de Mensagens**:
   - Navegue para: aba Fila
   - Envie uma mensagem de teste com dest_smsc correspondente ao nome do bind
   - Monitore no Status Ao Vivo para transmissão
   - Verifique a confirmação de entrega

Opção B: Via Arquivo de Configuração

Vantagens: Infraestrutura como código, controle de versão

Passos:

1. **Editar Arquivo de Configuração**:

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

2. **Adicionar Novo Bind à Configuração**:

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

  # Adicionar novo bind
  %{
    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. **Salvar e Reiniciar o Serviço**:

```
# Salvar arquivo (Ctrl+X, Y, Enter no nano)

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

4. **Verificar Conexão**:
    - Navegue para: SMPP → Status Ao Vivo
    - Encontre nova conexão
    - O status deve ser "Conectado" (verde)
    - Verifique os logs para bind bem-sucedido

5. **Testar Fluxo de Mensagens**:
    - Navegue para: aba Fila
    - Envie uma mensagem de teste com dest_smsc correspondente ao novo nome do bind
    - Monitore no Status Ao Vivo para transmissão
    - Verifique a confirmação de entrega

Adicionando um Bind de Servidor

Objetivo: Permitir que um parceiro externo se conecte ao seu gateway

Preparação:

1. **Gerar Credenciais**:
    - Crie um ID de sistema único: `partner_name`
    - Crie uma senha forte
    - Documente e compartilhe com segurança com o parceiro

2. **Obter Informações do Parceiro**:
    - Endereços IP de origem do parceiro
    - Volume esperado de mensagens (para limite de TPS)
    - Tipos de bind necessários

Escolha um dos seguintes métodos:

Opção A: Via Interface Web (Recomendado)

Vantagens: Efeito imediato, sem necessidade de reinício

Passos:

1. **Navegar para Pares de Servidor**:

- Abra a Interface Web: `https://your-server:8087`
- Navegue para: SMPP → Pares de Servidor

2. **Adicionar Novo Par de Servidor**:
   - Clique em "Adicionar Novo Par de Servidor"
   - Preencha o formulário:
     - **Nome**: `partner_acme` (identificador único)
     - **ID do Sistema**: `acme_corp`
     - **Senha**: `secure_password_123`
     - **Tipos de Bind Permitidos**: Selecione todos (Transmissor, Receptor, Transceiver)
     - **Lista de IP Permitidos**: `203.0.113.0/24` (separados por vírgula para múltiplos)
     - **Limite de TPS**: `50`
     - **Frequência de Verificação da Fila**: `1000`
   - Clique em "Salvar"

3. **Gateway Pronto para Conexão**:
   - O par de servidor agora está ativo e aguardando a conexão do parceiro
   - Nenhum reinício é necessário

4. **Compartilhar Informações com o Parceiro**:
   - Endereço IP do gateway
   - Porta: `2775`
   - ID do Sistema: `acme_corp`
   - Senha: `secure_password_123`
   - Tipo de Bind: Conforme configurado

5. **Aguardar Conexão do Parceiro**:
   - Navegue para: SMPP → Status Ao Vivo
   - Observe a conexão de entrada
   - Verifique o sucesso da autenticação
   - Verifique se o IP corresponde à lista permitida

Opção B: Via Arquivo de Configuração

Vantagens: Infraestrutura como código, controle de versão

Passos:

1. **Editar Arquivo de Configuração**:

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

2. **Adicionar Bind de Servidor e Configuração de Escuta**:

```
# Adicionar à lista de server_binds
config :omnimessage_smpp, :server_binds, [
  # Binds de servidor existentes...

  # Adicionar novo bind 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
  }
]

# Garantir que a configuração de escuta exista (apenas
necessário uma vez)
config :omnimessage_smpp, :listen, %{
  host: "0.0.0.0",
  port: 2775,
  max_connections: 100
}
```

3. **Salvar e Reiniciar o Serviço**:

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

4. **Compartilhar Informações com o Parceiro**:
    - Endereço IP do gateway
    - Porta: `2775`
    - ID do Sistema: `acme_corp`
    - Senha: `secure_password_123`
    - Tipo de Bind: Conforme configurado

5. **Aguardar Conexão do Parceiro**:
    - Navegue para: SMPP → Status Ao Vivo
    - Observe a conexão de entrada
    - Verifique o sucesso da autenticação
    - Verifique se o IP corresponde à lista permitida

Modificando Conexão Existente

Objetivo: Atualizar parâmetros de conexão (limites de TPS, senhas, lista de IP permitidos, etc.)

Escolha um dos seguintes métodos:

Opção A: Via Interface Web (Recomendado)

Vantagens: Efeito imediato, sem necessidade de reinício

Passos:

1. **Navegar para Pares**:
    - Abra a Interface Web: `https://your-server:8087`
    - Para conexões de cliente: SMPP → Pares de Clientes
    - Para conexões de servidor: SMPP → Pares de Servidor
2. **Editar Par**:
    - Encontre o par a ser modificado
    - Clique no botão "Editar"
    - Atualize os parâmetros desejados:
        - Mudanças comuns: limite de TPS, senha, lista de IP, host/porta
    - Clique em "Salvar"
3. **Mudanças Aplicam-se Imediatamente**:
    - A conexão reconecta automaticamente com as novas configurações
    - Nenhum reinício do serviço é necessário
    - Navegue para: SMPP → Status Ao Vivo para verificar
4. **Verificar Mudanças**:
    - Verifique se a conexão se estabelece com sucesso
    - Monitore a aba de Logs para erros
    - Teste o fluxo de mensagens, se aplicável

Opção B: Via Arquivo de Configuração

Vantagens: Infraestrutura como código, controle de versão

Passos:

1. **Editar Arquivo de Configuração**:

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

2. **Modificar Parâmetros do Bind**:
    - Encontre o bind na lista `:binds` ou `:server_binds`
    - Atualize os parâmetros desejados:

        - Mudanças comuns: limite de TPS, senhas, lista de IP, host/porta
    - Exemplo:

```
%{
  name: "vodafone_uk",
  # ... outros parâmetros
  tps_limit: 150,  # Mudado de 100
  password: "new_password"  # Senha atualizada
}
```

3. **Salvar e Reiniciar o Serviço**:

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

4. **Verificar Mudanças**:
    - Navegue para: SMPP → Status Ao Vivo
    - Verifique se a conexão se estabelece com sucesso
    - Monitore os logs para erros
    - Teste o fluxo de mensagens

Removendo uma Conexão

Objetivo: Descomissionar uma conexão SMPP

Passos:

1. **Notificar Stakeholders**:
    - Informar a operadora/parceiro
    - Coordenar janela de inatividade
2. **Desconectar via Interface Web**:
    - Navegue para: SMPP → Status Ao Vivo
    - Encontre a conexão
    - Clique em "Desconectar"
    - Confirme a ação
3. **Remover Configuração**:
    - Navegue para: SMPP → Pares de Clientes/Servidores
    - Encontre a conexão
    - Clique em "Excluir"
    - Confirme a remoção
4. **Verificar Remoção**:

- Verifique o Status Ao Vivo - a conexão deve ter sumido
- Revise os logs para um desligamento limpo

Gerenciando Fluxo de Mensagens

Verificando a Fila de Mensagens

Objetivo: Monitorar mensagens pendentes

Passos:

1. **Acessar Fila**:
   - Navegue para: aba Fila
   - Veja a lista de mensagens pendentes
2. **Verificar Detalhes da Mensagem**:
   - Clique na linha da mensagem
   - Revise:
     - Número de destino
     - Corpo da mensagem
     - SMSC alvo (dest_smsc)
     - Tentativas de entrega
     - Status
3. **Pesquisar Mensagem Específica**:
   - Use filtro de pesquisa
   - Filtrar por destino, conteúdo ou SMSC

Solucionando Mensagens Presas

Sintomas: Mensagens não sendo entregues

Passos:

1. **Verificar Status da Conexão**:
   - Navegue para: SMPP → Status Ao Vivo
   - Verifique se a conexão alvo está conectada
   - Se desconectada, veja Reconectando
2. **Verificar Detalhes da Mensagem**:
   - Navegue para: aba Fila
   - Encontre a mensagem presa

- Verifique se o campo `dest_smsc` corresponde ao nome da conexão
- Verifique o timestamp `deliver_after` (agendamento de reenvio)

3. **Verificar Tentativas de Entrega**:
   - Altas tentativas = falhas repetidas
   - Verifique logs para mensagens de erro
   - Pode indicar formato inválido ou rejeição da operadora
4. **Intervenção Manual** (se necessário):
   - Contate a operadora para verificar o problema
   - Pode ser necessário cancelar e reenviar a mensagem
   - Verifique com a equipe de backend por problemas na fila

Solução de Problemas de Conexão

Reconectando um Bind

Sintomas: A conexão mostra "Desconectado" (vermelho)

Passos:

1. **Verificar Conectividade de Rede**:

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

2. **Verificar Logs para Erros**:
   - Navegue para: aba Logs
   - Filtrar: Nível de erro
   - Procure por falhas de autenticação, timeouts de rede
3. **Verificar Credenciais**:
   - Navegue para: SMPP → Pares de Clientes/Servidores
   - Verifique se o system_id e a senha estão corretos
   - Contate a operadora se não tiver certeza
4. **Reconexão Manual**:
   - Navegue para: SMPP → Status Ao Vivo
   - Encontre o bind desconectado
   - Clique no botão "Reconectar"
   - Aguarde 10-30 segundos
   - Verifique se o status muda para "Conectado"

5. **Se a Reconexão Falhar**:
    - Verifique regras de firewall
    - Verifique se o servidor da operadora está operacional
    - Contate o suporte da operadora
    - Veja TROUBLESHOOTING.md

Lidando com Falhas de Autenticação

Sintomas: Falhas repetidas de bind nos logs

Causas:

- Nome de usuário/senha incorretos
- IP não autorizado na operadora
- Conta suspensa/expirada

Passos:

1. **Verificar Credenciais**:
    - Navegue para: SMPP → Pares de Clientes
    - Verifique novamente o system_id e a senha
    - Confirme com a operadora
2. **Verificar Lista de IP Permitidos**:
    - Confirme o IP do seu gateway com a operadora
    - Solicite à operadora que verifique a lista de IPs permitidos
3. **Verificar Status da Conta**:
    - Verifique se a conta está ativa
    - Verifique se há contratos expirados
    - Contate a cobrança da operadora
4. **Atualizar Configuração**:
    - Se as credenciais mudaram, atualize na Interface Web
    - Clique em "Reconectar" para tentar novamente com as novas credenciais

---

Monitoramento e Alerta

Verificando Métricas do Prometheus

Verificação rápida:

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

Saída esperada:

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

Todos os valores devem ser 1 (conectado).

Respondendo a Alertas

Alerta de Conexão Fora:

1. Verifique a Interface Web → SMPP → Status Ao Vivo
2. Tente reconexão manual
3. Verifique logs para erros
4. Contate a operadora se a interrupção for prolongada
5. Veja TROUBLESHOOTING.md

Alerta de Alta Taxa de Falha:

1. Verifique logs para padrões de erro
2. Revise mudanças recentes na configuração
3. Contate a operadora sobre rejeições
4. Verifique conformidade do formato da mensagem

Alerta de Sem Tráfego:

1. Verifique se a fila de backend tem mensagens
2. Verifique se o roteamento `dest_smsc` está correto
3. Verifique se os limites de TPS não são muito restritivos
4. Revise a configuração de `queue_check_frequency`

Procedimentos de Manutenção

Manutenção Rotineira

Realizar mensalmente:

1. **Revisar Métricas**:
    - Analisar tendências de volume de mensagens
    - Verificar taxas de sucesso de entrega
    - Identificar oportunidades de otimização
2. **Atualizar Documentação**:

    - Documentar quaisquer mudanças de configuração
    - Atualizar informações de contato
    - Anotar janelas de manutenção da operadora

3. **Auditoria de Credenciais**:

    - Revisar todas as senhas SMPP
    - Planejar rotação de credenciais
    - Verificar se as listas de IPs permitidos estão atualizadas

4. **Planejamento de Capacidade**:

    - Revisar taxas de mensagens de pico
    - Verificar contra limites de TPS
    - Planejar para crescimento

Reinício do Serviço

Quando necessário:

- Após mudanças no arquivo de configuração
- Após atualizações do sistema
- Durante solução de problemas

Passos:

```
# Verificar status atual
sudo systemctl status omnimessage-smpp

# Reiniciar serviço
sudo systemctl restart omnimessage-smpp

# Verificar reinício
sudo systemctl status omnimessage-smpp

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

Verifique via Interface Web:

1. Acesse o painel (pode levar 30-60 segundos para voltar online)
2. Navegue para: SMPP → Status Ao Vivo
3. Aguarde que todas as conexões sejam estabelecidas (1-2 minutos)
4. Verifique logs para erros

Backup de Configuração

Faça backup de arquivos críticos antes de mudanças:

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

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

Restaurar se necessário:

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

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

Procedimentos de Emergência

Interrupção Completa do Serviço

Passos:

1. **Verificar status do serviço**:

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

2. **Se o serviço estiver parado, inicie-o**:

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

3. **Verificar logs para razão do crash**:

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

4. **Se não iniciar**:

   - Verifique erros de sintaxe na configuração
   - Verifique se os certificados SSL existem
   - Verifique espaço em disco: `df -h`
   - Verifique memória: `free -h`

5. **Contate o suporte** se não resolver

Solicitações de Desconexão de Emergência da Operadora

Passos:

1. **Desconectar imediatamente**:
    - Navegue para: SMPP → Status Ao Vivo
    - Encontre a conexão afetada
    - Clique em "Desconectar"
2. **Documentar razão**:
    - Anote o nome da operadora
    - Registre hora e razão
    - Salve a correspondência
3. **Investigar o problema**:
    - Verifique padrões recentes de mensagens
    - Revise logs para erros
    - Identifique a causa raiz
4. **Coordenar resolução**:
    - Trabalhe com a operadora
    - Implemente correções
    - Teste antes de reconectar

Pico de Volume Alto

Sintomas: Tráfego de mensagens inesperadamente alto

Passos:

1. **Verificar limites de TPS**:
    - Navegue para: SMPP → Status Ao Vivo
    - Verifique se as conexões não estão sendo limitadas
    - Pode ser necessário aumentar temporariamente os limites de TPS
2. **Monitorar estabilidade da operadora**:
    - Observe desconexões
    - Verifique taxas de sucesso de entrega
3. **Coordenar com o backend**:
    - Verifique se a fonte da mensagem é legítima
    - Pode ser necessário implementar limitação de taxa a montante
4. **Escalar se necessário**:
    - Pode ser necessário instâncias adicionais do gateway

    - Contate o suporte para conselhos sobre escalonamento

Melhores Práticas

Lista de Verificação Diária

- [ ] Verificar se todas as conexões SMPP estão conectadas
- [ ] Revisar logs de erro para quaisquer problemas
- [ ] Monitorar fila de mensagens para acúmulo
- [ ] Verificar painéis do Prometheus/Grafana
- [ ] Verificar taxas de sucesso de entrega > 98%

Tarefas Semanais

- [ ] Revisar tendências de métricas
- [ ] Verificar por anomalias de padrão
- [ ] Testar procedimentos de recuperação de desastres
- [ ] Atualizar documentação conforme necessário
- [ ] Revisar e reconhecer alertas

Tarefas Mensais

- [ ] Auditoria de credenciais
- [ ] Revisão de planejamento de capacidade
- [ ] Atualizar contatos da operadora
- [ ] Revisar e otimizar configurações de TPS
- [ ] Fazer backup dos arquivos de configuração

Documentação Relacionada

- **CONFIGURATION.md** - Configurar conexões e configurações
- **MONITORING.md** - Configurar alertas do Prometheus
- **TROUBLESHOOTING.md** - Resolver problemas comuns
- **README.md** - Visão geral do sistema

Guia de Solução de Problemas

Problemas comuns e soluções

Problemas de Conectividade do OmniMessage

Como o SMPP Gateway é sem estado e depende inteiramente do OmniMessage Core, problemas de conectividade com o OmniMessage são os problemas mais críticos.

Sintomas de Desconexão do OmniMessage

- **Sem mensagens de saída**: A fila aumenta, mensagens não estão sendo enviadas
- **Sem mensagens de entrada**: Parceiros não conseguem enviar mensagens
- **Timeouts**: Chamadas de API com timeout ou travadas
- **Logs mostram**: "Conexão recusada", "Timeout", "HTTP 503", "Conexão redefinida"

Diagnóstico

1. Verifique a Disponibilidade do OmniMessage:

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

# Testar especificamente do host do gateway
ssh gateway-server 'curl -k https://omnimessage-
core.example.com:8443/api/system/health'
```

2. Verifique a URL da API Configurada:

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

# Verificar conectividade de rede
ping omnimessage-core.example.com
nc -zv omnimessage-core.example.com 8443
```

3. Verifique os Logs do Gateway para Erros de API:

```
# Procurar por erros relacionados à API
sudo journalctl -u omnimessage-smpp -f | grep -i
```

```
'api\|omnimessage\|connect'

# Pesquisar logs por erros recentes
sudo journalctl -u omnimessage-smpp -n 200 | grep -i error
```

Soluções

Se o OmniMessage estiver fora do ar:

1. Contate a equipe de operações do OmniMessage
2. Mensagens pendentes se acumularão na fila
3. O gateway continuará tentando (veja `SMPP_POLL_INTERVAL`)
4. Verifique a página de status do OmniMessage ou monitoramento

Se o OmniMessage estiver ativo, mas o gateway não conseguir alcançá-lo:

1. Verifique se as regras do firewall permitem HTTPS de saída
2. Verifique a resolução de DNS: `nslookup omnimessage-core.example.com`
3. Verifique o roteamento de rede: `traceroute omnimessage-core.example.com`
4. Verifique os certificados SSL se estiver usando HTTPS

Se a URL da API estiver mal configurada:

1. Edite `/opt/omnimessage-smpp/config/runtime.exs`
2. Verifique se `api_base_url` está correto (deve ser HTTPS para produção)
3. Reinicie o gateway: `sudo systemctl restart omnimessage-smpp`

Problemas de Conexão

A Conexão Não Estabelece

Sintomas:

- O status mostra "Desconectado" (vermelho)
- Nenhum bind bem-sucedido nos logs
- Tentativas de conexão repetidas

Causas Possíveis & Soluções:

1. Problemas de Conectividade de Rede

Verifique:

```
# Testar resolução de DNS
nslookup smpp.carrier.com
```

```
# Testar conectividade
ping -c 3 smpp.carrier.com

# Testar porta
telnet smpp.carrier.com 2775
# ou
nc -zv smpp.carrier.com 2775
```

Soluções:

- Se o DNS falhar: Use o endereço IP em vez do nome do host na configuração
- Se o ping falhar: Verifique as regras do firewall, contate o provedor
- Se a porta falhar: Verifique o número da porta correta, verifique o firewall

2. Credenciais Incorretas

Verifique:

- Logs mostram "bind failed" ou "authentication error"
- Web UI: SMPP → Client Peers → verifique system_id e password

Soluções:

- Confirme as credenciais com o provedor
- Verifique se há erros de digitação (sensível a maiúsculas)
- Atualize a configuração e reconecte

3. IP Não Está na Lista Branca

Verifique:

- Conexão rejeitada imediatamente
- Logs do provedor mostram IP não autorizado

Soluções:

- Confirme o IP público do seu gateway:

  ```
  curl ifconfig.me
  ```

- Solicite ao provedor que adicione o IP à lista branca
- Verifique se o IP não mudou (IP dinâmico)

4. Firewall Bloqueando

Verifique:

```
# Verifique se a porta está aberta
sudo iptables -L -n | grep 2775

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

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

Soluções:

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

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

A Conexão Continua Caindo

Sintomas:

- Conexão estabelecida, mas desconecta frequentemente
- Métrica `smpp_disconnection_total` aumentando
- Logs mostram reconexões repetidas

Causas Possíveis & Soluções:

1. Instabilidade de Rede

Verifique:

```
# Monitorar perda de pacotes
ping -c 100 smpp.carrier.com | grep loss

# Verifique erros de rede
netstat -s | grep -i error
```

Soluções:

- Contate o provedor sobre problemas de rede
- Verifique com o ISP se é do seu lado
- Considere conexão/rota de backup

2. Timeout de Enquiry Link

Verifique:

- Logs mostram "enquire_link timeout"
- Conexão cai após períodos de inatividade

Soluções:

- O timeout padrão é de 30 segundos
- Verifique se a rede permite pacotes keepalive
- Verifique se firewalls agressivos estão encerrando conexões ociosas

3. Limite de TPS Excedido

Verifique:

- Alta taxa de mensagens no momento da desconexão
- Provedor limitando mensagens

Soluções:

- Revise a configuração de `tps_limit`
- Reduza o TPS para 70-80% do máximo do provedor
- Espalhe o tráfego entre múltiplos binds

4. Problemas no Servidor do Provedor

Verifique:

- Verifique o status do serviço do provedor
- Contate o suporte do provedor

Soluções:

- Aguarde o provedor resolver
- Configure um provedor de backup, se disponível

Problemas de Entrega de Mensagens

Mensagens Não Sendo Enviadas

Sintomas:

- Mensagens presas na fila
- `smpp_messages_sent_total` não aumentando
- Conexão mostra conectada

Causas Possíveis & Soluções:

1. Roteamento `dest_smsc` Incorreto

Verifique:

- Web UI → Queue → Verifique o campo `dest_smsc` da mensagem
- Compare com o nome da conexão em SMPP → Live Status

Soluções:

- Mensagens são roteadas com base no campo `dest_smsc`
- Verifique se o backend está definindo o `dest_smsc` correto
- Se `dest_smsc` for NULL, verifique o roteamento padrão

2. Mensagens Agendadas para o Futuro

Verifique:

- Web UI → Queue → Verifique o campo `deliver_after`
- Mensagens com timestamp futuro não serão enviadas ainda

Explicação:

- O sistema de retry define `deliver_after` para mensagens falhadas
- Mensagens aguardam até esse horário antes de tentar novamente

Soluções:

- Aguarde o horário agendado
- Se urgente, contate a equipe de backend para redefinir o timestamp

3. Limite de TPS Muito Baixo

Verifique:

- Grande acúmulo na fila
- Mensagens sendo enviadas muito lentamente

Soluções:

- Aumente o `tps_limit` na configuração
- Verifique se o provedor pode lidar com uma taxa mais alta
- Veja CONFIGURATION.md

4. Worker da Fila Não Está Executando

Verifique:

- Status do serviço

- Logs para erros

Soluções:

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

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

Alta Taxa de Falhas de Entrega

Sintomas:

- `smpp_delivery_failures_total` aumentando
- Logs mostram "submit_sm_resp" com status de erro
- Mensagens não chegando aos destinatários

Causas Possíveis & Soluções:

1. Números de Destino Inválidos

Verifique:

- Logs para códigos de erro específicos
- Revise o formato do destino da mensagem

Códigos de Erro Comuns:

- `0x0000000B` - Destino inválido
- `0x00000001` - Comprimento da mensagem inválido
- `0x00000003` - Comando inválido

Soluções:

- Valide o formato do número (E.164 recomendado)
- Verifique se o número inclui o código do país
- Verifique os requisitos do provedor

2. Conteúdo da Mensagem Inválido

Verifique:

- Comprimento da mensagem
- Caracteres especiais
- Codificação

Soluções:

- GSM-7: Máx. 160 caracteres
- UCS-2: Máx. 70 caracteres
- Remova caracteres não suportados
- Verifique as configurações de codificação

3. Rejeição do Provedor

Verifique:

- Códigos de erro específicos do provedor
- Padrões em mensagens rejeitadas

Soluções:

- Contate o provedor para saber o motivo da rejeição
- Pode ser necessário filtragem de conteúdo
- Verifique padrões de spam/abuso

4. Mensagens Expiradas

Verifique:

- Timestamp de `expires` da mensagem
- Tempo de tentativa de entrega

Soluções:

- Aumente o período de validade da mensagem
- Reduza o atraso de retry para mensagens sensíveis ao tempo

Problemas na Web UI

Não Consigo Acessar o Painel da Web

Sintomas:

- O navegador não consegue se conectar a https://your-server:8087
- Timeout ou conexão recusada

Causas Possíveis & Soluções:

1. Serviço Não Está Executando

Verifique:

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

Soluções:

```
# Se parado, inicie-o
sudo systemctl start omnimessage-smpp

# Verifique logs para erros
sudo journalctl -u omnimessage-smpp -n 50
```

2. Firewall Bloqueando a Porta 8087

Verifique:

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

Soluções:

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

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

3. Problemas com Certificado SSL

Verifique:

- O navegador mostra aviso de segurança
- Certificado expirado ou inválido

Soluções:

- Aceitar exceção de segurança (se autoassinado)
- Instalar certificado SSL válido
- Verifique se os arquivos do certificado existem:

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

4. URL Errada

Verifique:

- Verifique se está usando HTTPS (não HTTP)
- Verifique o IP/hostname do servidor correto

- Verifique a porta 8087

A Web UI Mostra Erros

Sintomas:

- A página carrega, mas mostra erros
- Funções não funcionam
- Dados não exibidos

Soluções:

1. **Limpar Cache do Navegador**:
    - Ctrl+F5 (atualização forçada)
    - Limpar cache e cookies do navegador
2. **Verifique o Console do Navegador**:
    - Pressione F12
    - Verifique a aba Console para erros de JavaScript
    - Relate ao suporte se erros forem encontrados
3. **Tente um Navegador Diferente**:
    - Teste no Chrome, Firefox, Edge
    - Isolar problemas específicos do navegador
4. **Verifique os Logs do Serviço**:

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

Problemas de Métricas

Métricas do Prometheus Não Disponíveis

Sintomas:

- `curl http://localhost:4000/metrics` falha
- Prometheus não consegue coletar métricas
- Resposta vazia ou com erro

Causas Possíveis & Soluções:

1. Serviço Não Está Executando

Verifique:

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

Soluções:

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

2. Porta Não Acessível

Verifique:

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

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

Soluções:

- Se local funciona, mas remoto não: Verifique o firewall
- Abra a porta 4000 no firewall para o servidor Prometheus

3. Endpoint Errado

Verifique:

- O endpoint é `/metrics` (não `/prometheus` ou `/stats`)
- A porta é 4000 (não 8087)

Métricas Mostram Valores Inesperados

Sintomas:

- Contadores redefinidos para zero
- Medidores mostram valores errados
- Métricas ausentes para alguns binds

Soluções:

1. **Reinício do Serviço Redefine Contadores**:
    - Contadores são redefinidos no reinício do serviço
    - Isso é comportamento normal
    - Use `increase()` ou `rate()` nas consultas do Prometheus

2. **Novos Binds Não Aparecendo**:
    - Métricas só aparecem após o primeiro evento
    - Envie uma mensagem de teste para preencher as métricas
    - Verifique se o bind está habilitado e conectado
3. **Métricas Obsoletas**:
    - Binds antigos podem ainda aparecer nas métricas
    - Reinicie o serviço para limpar entradas obsoletas
    - Ou use relabeling do Prometheus para filtrar

Problemas de Desempenho

Alta Utilização de CPU

Verifique:

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

Causas Possíveis:

- Volume de mensagens muito alto
- Muitas conexões
- Problema de configuração

Soluções:

- Verifique se a taxa de mensagens está dentro da capacidade
- Revise os limites de TPS
- Contate o suporte se a CPU alta for sustentada

Alta Utilização de Memória

Verifique:

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

Causas Possíveis:

- Grande fila de mensagens na memória
- Vazamento de memória (raro)

Soluções:

- Reinicie o serviço para limpar a memória
- Verifique o tamanho da fila de mensagens

- Contate o suporte se a memória crescer continuamente

Processamento Lento de Mensagens

Sintomas:

- Mensagens demoram para enviar
- Fila se acumulando
- Baixa taxa de mensagens

Verifique:

1. Limites de TPS - podem ser muito restritivos
2. `queue_check_frequency` - pode estar muito alto
3. Tempo de resposta da API de backend - pode estar lento
4. Latência de rede para o provedor

Soluções:

- Aumente o TPS se o provedor permitir
- Diminua `queue_check_frequency` para polling mais rápido
- Otimize a API de backend
- Verifique a latência da rede

Problemas de Configuração

Erros de Sintaxe no Arquivo de Configuração

Sintomas:

- O serviço não inicia após alteração de configuração
- Logs mostram "erro de sintaxe" ou "erro de análise"

Verifique:

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

Erros Comuns:

- Vírgula faltando entre entradas de mapa
- Aspas não correspondentes (" vs ')
- Colchetes ou chaves não correspondentes
- Faltando `import Config` no topo

Soluções:

- Restaurar a partir do backup
- Revisar cuidadosamente a sintaxe
- Usar editor de texto com destaque de sintaxe Elixir

Mudanças Não Têm Efeito

Sintomas:

- Configuração modificada, mas sem mudança no comportamento
- Configurações antigas ainda ativas

Soluções:

```
# Mudanças de configuração requerem reinício
sudo systemctl restart omnimessage-smpp

# Verifique se o reinício foi bem-sucedido
sudo systemctl status omnimessage-smpp

# Verifique logs para erros
sudo journalctl -u omnimessage-smpp -n 50
```

Recuperação de Emergência

Falha Completa do Sistema

Passos:

1. **Verifique a saúde básica do sistema**:

   ```
   # Espaço em disco
   df -h

   # Memória
   free -h

   # Carga da CPU
   uptime
   ```

2. **Verifique o status do serviço**:

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

3. **Revise logs recentes**:

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

4. **Tente reiniciar o serviço**:

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

5. **Se a reinicialização falhar**:

   - Verifique a sintaxe da configuração
   - Verifique se os certificados SSL existem
   - Verifique permissões de arquivo
   - Revise logs para erro específico

6. **Restaure a partir do backup** (se necessário):

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

   # Reiniciar
   sudo systemctl restart omnimessage-smpp
   ```

7. **Contate o suporte** se não for resolvido

Obtendo Ajuda

Informações a Coletar

Antes de contatar o suporte, colete:

1. **Versão**: `cat /opt/omnimessage-smpp/VERSION`
2. **Logs Recentes**:

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

3. **Configuração** (sanitizar senhas):

   ```
   sudo cp /opt/omnimessage-smpp/config/runtime.exs /tmp/config.exs
   # Edite /tmp/config.exs para remover senhas antes de enviar
   ```

4. **Saída de Métricas**:

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

5. **Informações do Sistema**:

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

Contate o Suporte

- **Email**: support@omnitouch.com
- **Telefone**: +61 XXXX XXXX (24/7)
- **Inclua**: Todas as informações acima

Documentação Relacionada

- **OPERATIONS.md** - Procedimentos operacionais normais
- **CONFIGURATION.md** - Referência de configuração
- **MONITORING.md** - Monitoramento e métricas
- **README.md** - Visão geral do sistema
