Passerelle SMPP OmniMessage - Guide d'Opérations

Version : 1.0.0
Pour les Équipes d'Opérations

Qu'est-ce que la Passerelle SMPP ?

La Passerelle SMPP OmniMessage est l'un des plusieurs protocoles frontend pour la plateforme de télécommunications OmniMessage. Elle permet l'envoi de SMS en connectant votre infrastructure aux réseaux mobiles en utilisant le protocole SMPP (Short Message Peer-to-Peer) standard de l'industrie.

Important : Cette passerelle est un frontend de protocole sans état. Elle n'a pas de logique métier, de traitement de message ou de capacités de stockage. Toute l'intelligence provient d'OmniMessage, accessible via l'API REST. Comme d'autres frontends OmniMessage (Diameter, MAP, IMS), elle traduit simplement les messages de protocole vers/depuis le format interne d'OmniMessage.

Capacités Clés

- **Messagerie SMPP Bidirectionnelle** : Envoyer et recevoir des messages SMS via SMPP
- **Connexions Multiples** : Se connecter à plusieurs opérateurs simultanément
- **Haute Performance** : Gérer des milliers de messages par seconde
- **Surveillance** : Métriques Prometheus intégrées et tableau de bord web
- **Fiabilité** : Reconnexion automatique et nouvelle tentative d'envoi de message
- **Fonctionnement Sans État** : Tout le traitement est délégué au backend OmniMessage

Qui Devrait Utiliser Ce Guide ?

Ce guide est destiné aux équipes d'opérations responsables de :

- L'installation et la configuration de la passerelle
- La surveillance du trafic de messages
- La gestion des connexions SMPP
- La résolution de problèmes

Démarrage Rapide

Configuration Initiale

1. **Accéder au Tableau de Bord Web** : `https://your-server:8087`
2. **Vérifier l'État du Système** : Naviguer vers SMPP → État en Direct
3. **Revoir la Configuration** : Voir CONFIGURATION.md
4. **Configurer la Surveillance** : Voir MONITORING.md

Opérations Quotidiennes

Tâches opérationnelles courantes :

Tâche	Action
Vérifier l'état de la connexion	Interface Web → SMPP → État en Direct
Voir le trafic de messages	Interface Web → File d'attente
Surveiller la santé du système	Interface Web → Journaux ou métriques Prometheus
Ajouter/modifier des connexions	Interface Web → SMPP → Pairs Client/Serveur

Voir OPERATIONS.md pour des procédures détaillées.

Architecture du Système

La Passerelle SMPP est un traducteur de protocole sans état qui fonctionne comme partie de la plateforme OmniMessage :

Concepts Clés :

- **Passerelle SMPP** : Traducteur de protocole uniquement - pas de traitement de message, de stockage ou de logique métier
- **OmniMessage** : Plateforme centrale gérant toute la logique de messagerie, le routage et le stockage
- **Communication API** : La passerelle récupère les messages à envoyer d'OmniMessage et rapporte l'état de livraison

Intégration OmniMessage

La Passerelle SMPP OmniMessage est un **frontend de protocole** pour la plateforme de messagerie OmniMessage. C'est l'un des plusieurs types de frontends identiques qui interagissent avec les réseaux mobiles en utilisant différents protocoles :

Frontend	Protocole	Objectif
Passerelle SMPP	SMPP (SMS)	Messagerie SMS via le protocole SMPP
Passerelle Diameter	Diameter	Messagerie basée sur IMS
Passerelle MAP	MAP	Signalisation de réseau mobile
Passerelle IMS	IMS	Système Multimédia IP

Tous les frontends partagent la même architecture : **Ce sont des traducteurs de protocole sans état qui délèguent toute l'intelligence au cœur d'OmniMessage**.

Comment Ça Fonctionne

Flux de Message Inbound (Système Externe → Opérateur) :

Flux de Message Outbound (Opérateur → Passerelle SMPP) :

Ce Que Fait la Passerelle

- Reçoit des PDUs SMPP des opérateurs et des clients externes
- Analyse et valide les messages de protocole SMPP
- Traduit le format SMPP en format interne d'OmniMessage
- Appelle l'API REST d'OmniMessage avec les données du message
- Reçoit des messages d'OmniMessage via le polling API
- Convertit le format OmniMessage en PDUs SMPP
- Rapporte les accusés de réception à OmniMessage

Ce Que la Passerelle NE Fait PAS

- 🚫 Pas de stockage ou de persistance de message
- 🚫 Pas de décisions de routage (OmniMessage décide)
- 🚫 Pas de limitation de taux (OmniMessage applique)
- 🚫 Pas de validation de numéro (OmniMessage valide)
- 🚫 Pas de suivi d'état (OmniMessage maintient l'état)
- 🚫 Pas de logique métier (OmniMessage gère toute la logique)

API REST d'OmniMessage

La passerelle communique avec le Cœur d'OmniMessage via l'API REST :

Configuration :

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

Opérations Clés de l'API :

- `GET /api/message_queue?destination_smsc=<bind_name>` - Récupérer

les messages en attente
- `PUT /api/messages/<id>/delivery_status` - Rapporter un accusé de réception
- `GET /api/system/health` - Vérification de santé

Format de Message : Les messages dans la file d'attente contiennent toutes les informations nécessaires à la livraison :

- Numéro de destination
- Corps du message
- Numéro d'origine
- Priorité
- Période de validité
- SMSC cible (nom de liaison de l'opérateur)

La passerelle récupère simplement ces informations, les formate en SMPP, les envoie à l'opérateur et rapporte l'état.

Structure de la Documentation

Cette documentation est organisée en plusieurs guides :

- **CONFIGURATION.md** - Référence complète de configuration avec tous les paramètres expliqués
- **MONITORING.md** - Guide des métriques Prometheus et d'alerte
- **OPERATIONS.md** - Procédures opérationnelles quotidiennes
- **TROUBLESHOOTING.md** - Problèmes courants et solutions
- **GLOSSARY.md** - Termes et définitions

Points d'Accès

Tableau de Bord Web

- **URL** : `https://your-server:8087`
- **Fonctionnalités** :
  - Voir l'état de la connexion SMPP
  - Surveiller la file d'attente de messages
  - Voir les journaux système
  - Configurer les pairs SMPP
  - Accéder à la documentation

Métriques Prometheus

- **URL** : `http://your-server:4000/metrics`
- **Format** : Format texte Prometheus
- **Utilisation** : Intégration avec Grafana/Prometheus

Point de Terminaison API

- **URL** : Configuré dans `API_BASE_URL`
- **Objectif** : Intégration du backend de la file d'attente de messages

Référence Rapide

Tâches Courantes

Tâche	Commande/Emplacement
Démarrer la passerelle	`systemctl start omnimessage-smpp`
Arrêter la passerelle	`systemctl stop omnimessage-smpp`
Redémarrer la passerelle	`systemctl restart omnimessage-smpp`
Voir les journaux	`journalctl -u omnimessage-smpp -f`
Vérifier l'état	Interface Web → SMPP → État en Direct
Voir les métriques	`curl http://localhost:4000/metrics`
Éditer la config	`/opt/omnimessage-smpp/config/runtime.exs`

Fichiers Importants

Fichier	Objectif
`/opt/omnimessage-smpp/config/runtime.exs`	Configuration principale
`/opt/omnimessage-smpp/priv/cert/`	Certificats SSL
`/var/log/omnimessage-smpp/`	Journaux de l'application
`/etc/systemd/system/omnimessage-smpp.service`	Définition du service

Notes de Sécurité

- **Interface Web** : Utilise HTTPS avec vos certificats SSL
- **Communication API** : Peut vérifier SSL ou utiliser des certificats auto-signés
- **SMPP** : Protocole en texte clair - utiliser la sécurité réseau
- **Identifiants** : Stockés dans le fichier de configuration - protéger l'accès

Prochaines Étapes

1. Revoir **CONFIGURATION.md** pour toutes les options de configuration
2. Configurer **MONITORING.md** avec Prometheus
3. Se familiariser avec **OPERATIONS.md** pour les tâches quotidiennes
4. Ajouter en favori **TROUBLESHOOTING.md** pour référence rapide
5. Revoir **GLOSSARY.md** pour la terminologie

Licencié à : Omnitouch

Référence de Configuration

Guide complet de tous les paramètres de configuration

Vue d'ensemble de l'architecture

La passerelle OmniMessage SMPP est un **frontend de protocole sans état** qui traduit les messages SMPP vers/depuis OmniMessage. Toute la logique métier, les décisions de routage et le stockage des messages sont gérés par OmniMessage Core - la passerelle se contente de :

1. **Recevoir** les PDU SMPP des opérateurs et des clients
2. **Les traduire** au format OmniMessage via l'API REST
3. **Interroger** OmniMessage pour les messages à envoyer
4. **Envoyer** les PDU SMPP aux opérateurs
5. **Rapporter** le statut de livraison à OmniMessage

C'est identique à la façon dont d'autres frontends OmniMessage (Diameter, MAP, IMS) fonctionnent - ce sont tous des traducteurs de protocole sans état qui délèguent à OmniMessage Core.

Emplacement du fichier de configuration

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

Important : Après avoir modifié la configuration, redémarrez la passerelle :

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

Structure de Configuration

Le fichier de configuration utilise la syntaxe Elixir. Structure de base :

```
import Config

# Paramètres globaux
config :omnimessage_smpp,
  setting_name: value

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

```
    # ... paramètres de liaison
  }
]
```

Paramètres Globaux

API_BASE_URL

URL de la plateforme OmniMessage Core

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

Paramètre	Type	Requis	Par défaut
`api_base_url`	Chaîne (URL)	Oui	-

But : URL de la plateforme OmniMessage Core. La passerelle communique avec OmniMessage via l'API REST pour tout le traitement des messages :

- **Soumettre des messages** : Envoyer les messages SMPP reçus à OmniMessage pour traitement
- **Récupérer des messages** : Interroger pour les messages destinés aux opérateurs SMPP
- **Rapporter le statut de livraison** : Mettre à jour le statut de livraison des messages vers OmniMessage
- **Santé du système** : Vérifications de santé périodiques

Critique : C'est ici que la passerelle obtient tout son "cerveau". OmniMessage gère :

- ✓ Validation des messages et vérification de format
- ✓ Décisions de routage (quel opérateur utiliser)
- ✓ Limitation de débit et régulation
- ✓ Validation de numéro
- ✓ Stockage et persistance des messages
- ✓ Logique de réessai de livraison
- ✓ Suivi de statut

La passerelle se contente de traduire le format SMPP ↔ OmniMessage.

Exemples :

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

# HTTPS avec nom d'hôte
```

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

# HTTP (non recommandé pour la production)
api_base_url: "http://192.168.1.100:8080"
```

Exigences Réseau :

- La passerelle doit avoir un accès réseau à OmniMessage Core
- Utilisez HTTPS en production (configurez `verify_ssl_peer`)
- Le pare-feu doit autoriser le HTTPS sortant sur le port spécifié

SMPP_POLL_INTERVAL

Fréquence de vérification de la file d'attente (millisecondes)

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

Paramètre	Type	Requis	Par défaut
`smpp_poll_interval`	Entier	Non	100

But : À quelle fréquence (en millisecondes) chaque client vérifie la file d'attente des messages.

Directives :

- **Volume élevé (>100 TPS)** : 100-500ms
- **Volume moyen (10-100 TPS)** : 500-1000ms
- **Faible volume (<10 TPS)** : 1000-2000ms

Variable d'environnement : `SMPP_POLL_INTERVAL`

VERIFY_SSL_PEER

Vérification du certificat SSL

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

Paramètre	Type	Requis	Par défaut
`verify_ssl_peer`	Booléen	Non	false

But : Vérifier les certificats SSL lors de la connexion à l'API backend.

Valeurs :

- `true` : Vérifier les certificats (production avec certificats valides)
- `false` : Ignorer la vérification (certificats auto-signés, test)

Variable d'environnement : `VERIFY_SSL_PEER`

SMSC_NAME

Identifiant de la passerelle pour l'enregistrement

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

Paramètre	Type	Requis	Par défaut
`smsc_name`	Chaîne	Non	"smpp_gateway"

But : Identifie cette instance de passerelle dans le backend de la file d'attente des messages.

Variable d'environnement : `SMSC_NAME`

Configuration de Liaison Client SMPP

Les liaisons clients sont des **connexions sortantes** aux serveurs SMPP des opérateurs.

Exemple Complet de Liaison Client

```
config :omnimessage_smpp, :binds, [
  %{
    # Identifiant unique pour cette connexion
    name: "vodafone_uk",

    # Mode de connexion
    mode: :client,

    # Type de liaison SMPP
    bind_type: :transceiver,

    # Adresse du serveur SMPP de l'opérateur
    host: "smpp.vodafone.co.uk",
    port: 2775,

    # Informations d'authentification
    system_id: "your_username",
    password: "your_password",

    # Limitation de débit
    tps_limit: 100,
```

```
    # Fréquence de vérification de la file d'attente
    queue_check_frequency: 1000
  }
]
```

Paramètres de Liaison Client

name

Identifiant de connexion unique

Type	Requis	Exemple
Chaîne	Oui	`"vodafone_uk"`

But : Identifie de manière unique cette connexion SMPP.

- Utilisé dans les journaux et les métriques
- Doit être unique parmi toutes les liaisons
- Utilisez des noms descriptifs (opérateur, région, but)

Conventions de nommage :

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

mode

Type de connexion

Type	Requis	Valeur
Atome	Oui	`:client`

But : Définit ceci comme une connexion sortante.

Valeur fixe : Toujours `:client` pour les connexions sortantes.

bind_type

Type de session SMPP

Type	Requis	Valeurs autorisées
Atome	Oui	`:transmitter`, `:receiver`, `:transceiver`

But : Définit la capacité de direction des messages.

Options :

- `:transmitter` - Envoyer des messages uniquement (submit_sm)
- `:receiver` - Recevoir des messages uniquement (deliver_sm)
- `:transceiver` - Envoyer et recevoir (le plus courant)

Recommandation : Utilisez `:transceiver` sauf si l'opérateur exige un type spécifique.

host

Nom d'hôte ou IP du serveur SMPP de l'opérateur

Type	Requis	Exemple
Chaîne	Oui	`"smpp.carrier.com"` ou `"10.5.1.100"`

But : Adresse du serveur SMPP de l'opérateur.

Exemples :

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

port

Port du serveur SMPP

Type	Requis	Par défaut	Plage
Entier	Oui	2775	1-65535

But : Port TCP pour la connexion SMPP.

Port standard : 2775

Exemples :

```
port: 2775  # Standard
port: 3000  # Personnalisé
```

system_id

Nom d'utilisateur d'authentification

Type	Requis	Exemple
Chaîne	Oui	`"company_user"`

But : Nom d'utilisateur fourni par l'opérateur pour l'authentification.

Sécurité : Protégez cette information d'identification - stockée dans le fichier de configuration.

password

Mot de passe d'authentification

Type	Requis	Exemple
Chaîne	Oui	`"secret_password"`

But : Mot de passe fourni par l'opérateur pour l'authentification.

Sécurité :

- Protégez cette information d'identification
- Utilisez des mots de passe forts
- Changez périodiquement

tps_limit

Limite de transactions par seconde

Type	Requis	Par défaut	Plage
Entier	Oui	100	1-10000

But : Nombre maximum de messages par seconde à envoyer via cette connexion.

Directives :

- Réglez à 70-80% du maximum de l'opérateur
- Empêche le throttling/déconnexion
- Permet une marge pour les accusés de réception de livraison

Exemples :

```
tps_limit: 10    # Faible volume
tps_limit: 50    # Volume moyen
tps_limit: 100   # Volume élevé (le plus courant)
tps_limit: 1000  # Volume très élevé
```

Calcul :

```
Si le maximum de l'opérateur = 100 TPS
Réglez tps_limit = 70-80
Laisse 20-30 TPS de marge
```

queue_check_frequency

Intervalle de sondage de la file d'attente des messages (millisecondes)

Type	Requis	Par défaut	Plage
Entier	Oui	1000	100-10000

But : À quelle fréquence vérifier le backend pour de nouveaux messages à envoyer.

Directives :

- **Volume élevé (>100 TPS)** : 500-1000ms
- **Volume moyen (10-100 TPS)** : 1000-2000ms
- **Faible volume (<10 TPS)** : 2000-5000ms

Compromis :

- Valeur plus basse = prise en charge plus rapide des messages, plus de charge API
- Valeur plus élevée = prise en charge plus lente, moins de charge API

Exemple d'interface Web :

Configuration de Liaison Serveur SMPP

Les liaisons serveur définissent des **connexions entrantes** des clients SMPP externes.

Exemple Complet de Liaison Serveur

```
config :omnimessage_smpp, :server_binds, [
  %{
    # Identifiant unique pour ce client
    name: "partner_acme",

    # Informations d'identification attendues du client
    system_id: "acme_corp",
    password: "acme_secret",

    # Types de liaison autorisés
    allowed_bind_types: [:transmitter, :receiver, :transceiver],

    # Restrictions IP
    ip_whitelist: ["192.168.1.0/24", "10.50.1.100"],
```

```
    # Limitation de débit
    tps_limit: 50,

    # Fréquence de vérification de la file d'attente
    queue_check_frequency: 1000
  }
]
```

Paramètres de Liaison Serveur

name

Identifiant du client

Type	Requis	Exemple
Chaîne	Oui	`"partner_acme"`

But : Identifie le client externe se connectant à vous.

Conventions de nommage : Utilisez le nom du partenaire/client pour une identification facile.

system_id

Nom d'utilisateur attendu du client

Type	Requis	Exemple
Chaîne	Oui	`"acme_corp"`

But : Nom d'utilisateur que le client externe doit fournir pour s'authentifier.

À fournir au client : Partagez cette information d'identification avec votre partenaire.

password

Mot de passe attendu du client

Type	Requis	Exemple
Chaîne	Oui	`"secure_password"`

But : Mot de passe que le client externe doit fournir pour s'authentifier.

Sécurité :

- Utilisez des mots de passe forts
- Unique par client

- Partagez en toute sécurité avec le partenaire

allowed_bind_types

Types de session autorisés

Type	Requis	Par défaut
Liste d'Atomes	Oui	-

But : Restreint les types de liaison que le client peut utiliser.

Options :

```
allowed_bind_types: [:transceiver]  # Seulement transceiver
allowed_bind_types: [:transmitter, :receiver]  # TX ou RX
allowed_bind_types: [:transmitter, :receiver, :transceiver]  # Tout
```

Recommandation : Autorisez les trois à moins que vous n'ayez besoin de restrictions.

ip_whitelist

Adresses IP des clients autorisées

Type	Requis	Par défaut	Format
Liste de Chaînes	Oui	[]	IPs ou notation CIDR

But : Sécurité - n'autoriser que les connexions provenant d'IPs connues.

Formats :

- IP unique : `"192.168.1.100"` (automatiquement `/32`)
- Sous-réseau CIDR : `"192.168.1.0/24"`, `"10.0.0.0/8"`
- Mélanger les deux : `["192.168.1.0/24", "10.50.1.100"]`

Exemples :

```
# Autoriser n'importe quelle IP (non recommandé)
ip_whitelist: []

# IP unique
ip_whitelist: ["203.0.113.50"]

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

# Sous-réseau
ip_whitelist: ["192.168.1.0/24"]
```

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

Sous-réseaux courants :

- `/32` - IP unique (automatique pour les IP sans masque)
- `/24` - 256 adresses (par exemple, 192.168.1.0-255)
- `/16` - 65,536 adresses (par exemple, 10.50.0.0-255.255)
- `/8` - 16,777,216 adresses (par exemple, 10.0.0.0-255.255.255.255)

tps_limit

Limite de messages par seconde

Identique au `tps_limit` de la liaison client - contrôle le taux de delivery_sm sortant.

queue_check_frequency

Intervalle de sondage de la file d'attente

Identique à `queue_check_frequency` de la liaison client - à quelle fréquence vérifier les messages à livrer à ce client.

Exemple d'interface Web :

Configuration d'Écoute du Serveur

Lorsque les liaisons serveur sont configurées, la passerelle écoute les connexions entrantes.

Exemple Complet d'Écoute

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

Paramètres d'Écoute

host

Adresse IP à laquelle se lier

Type	Requis	Par défaut	Valeurs courantes
Chaîne	Non	`"0.0.0.0"`	`"0.0.0.0"`, `"127.0.0.1"`

But : Sur quelle interface réseau écouter.

Valeurs :

- `"0.0.0.0"` - Écouter sur toutes les interfaces (recommandé)
- `"127.0.0.1"` - Écouter uniquement sur localhost (test)
- `"192.168.1.10"` - Écouter sur une IP spécifique

port

Port TCP à écouter

Type	Requis	Par défaut	Plage
Entier	Non	2775	1-65535

But : Port pour les connexions SMPP entrantes.

Standard : 2775

max_connections

Nombre maximum de connexions simultanées

Type	Requis	Par défaut	Plage
Entier	Non	100	1-10000

But : Limite le nombre total de connexions clients simultanées.

Directives :

- Réglez en fonction des clients attendus
- Des valeurs plus élevées utilisent plus de mémoire
- Typique : 10-100 connexions

Exemples Complets de Configuration

Exemple 1 : Connexion à un Opérateur Unique

```
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
  }
]
```

Exemple 2 : Plusieurs Opérateurs

```
import Config

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

config :omnimessage_smpp, :binds, [
  # Amérique du Nord
  %{
    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
  },

  # Europe
  %{
    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
  }
]
```

Exemple 3 : Passerelle avec Liaisons Serveur

```
import Config

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

# Connexions sortantes
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
  }
]

# Définitions des clients entrants
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
  }
]
```

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

Validation de Configuration

Après avoir modifié la configuration, validez avant de redémarrer :

Vérification de Syntaxe

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

Si la syntaxe est invalide, vous verrez une erreur. Corrigez avant de redémarrer.

Tester la Configuration

```
# Redémarrez au premier plan pour voir les erreurs
sudo -u omnimessage-smpp /opt/omnimessage-smpp/bin/omnimessage-smpp
console
```

Appuyez sur `Ctrl+C` deux fois pour quitter.

Meilleures Pratiques de Sécurité

1. **Protégez le fichier de configuration** :

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

2. **Utilisez des mots de passe forts** :

   - Minimum 12 caractères
   - Mélangez lettres, chiffres, symboles
   - Unique par connexion

3. **Utilisez des listes blanches IP** :

   - Configurez toujours `ip_whitelist` pour les liaisons serveur
   - N'utilisez jamais une liste vide `[]` en production

4. **Activez la vérification SSL** :
    - Réglez `verify_ssl_peer: true` avec des certificats valides
5. **Rotation régulière des informations d'identification** :
    - Changez les mots de passe tous les trimestres
    - Coordonnez avec les opérateurs/partenaires

Prochaines Étapes

- Consultez MONITORING.md pour la configuration des métriques
- Lisez OPERATIONS.md pour gérer les connexions
- Consultez TROUBLESHOOTING.md pour les problèmes courants
- Retournez à README.md pour un aperçu

Glossaire

Termes et Définitions

A

API (Interface de Programmation d'Applications) Interface utilisée pour communiquer avec le système backend de la file de messages.

Défilement Automatique Fonctionnalité dans l'onglet Logs de l'interface web qui fait défiler automatiquement pour afficher les nouvelles entrées de journal.

B

Backend Le système de file de messages auquel la passerelle SMPP se connecte pour récupérer et stocker des messages.

Bind Une connexion SMPP entre deux systèmes. Peut être émetteur, récepteur ou transcepteur.

Type de Bind Le type de session SMPP :

- **Émetteur** : Envoie uniquement des messages
- **Récepteur** : Reçoit uniquement des messages
- **Transcepteur** : Envoie et reçoit des messages

Échec de Bind Lorsque la tentative d'authentification SMPP échoue, généralement en raison de mauvaises informations d'identification ou de restrictions IP.

C

CIDR (Routage Inter-Domaines Sans Classe) Notation pour spécifier des plages d'adresses IP (par exemple, `192.168.1.0/24` représente 256 adresses IP).

Bind Client Une connexion SMPP sortante de la passerelle vers le serveur SMPP d'un opérateur.

Statut de Connexion État actuel d'un bind SMPP :

- **Connecté** : Actif et opérationnel
- **Déconnecté** : Non connecté
- **Reconnaissance** : Tentative d'établissement de la connexion

Compteur Une métrique qui n'augmente que (se réinitialise au redémarrage du service), utilisée pour des totaux comme les messages envoyés.

D

Codage des Données Champ SMPP spécifiant l'encodage des caractères du message (GSM-7, UCS-2, etc.).

Échec de Livraison Lorsque qu'un message ne peut pas être livré, indiqué par une réponse d'erreur de l'opérateur.

Accusé de Réception de Livraison (DLR) Confirmation de l'opérateur concernant le statut de livraison du message.

dest_smsc Champ dans la file de messages indiquant quelle connexion SMPP doit gérer le message.

Déconnexion Lorsque une connexion SMPP active est terminée, soit intentionnellement, soit en raison d'une erreur.

E

Lien de Vérification Message keepalive SMPP envoyé périodiquement pour vérifier que la connexion est active.

Classe ESM Champ SMPP indiquant le type et les caractéristiques du message.

Retard Exponentiel Stratégie de réessai où le temps d'attente double après chaque échec (1min, 2min, 4min, 8min...).

F

Pare-feu Système de sécurité réseau qui contrôle le trafic réseau entrant et sortant.

G

Passerelle L'application de passerelle SMPP qui fait le lien entre la file de messages et les réseaux mobiles.

Jauge Une métrique qui peut augmenter ou diminuer, représentant la valeur actuelle (par exemple, statut de connexion).

Grafana Outil de visualisation populaire pour afficher les métriques Prometheus dans des tableaux de bord.

GSM-7 Encodage de caractères standard à 7 bits pour les SMS, prenant en charge jusqu'à 160 caractères par message.

H

HTTP/HTTPS Protocoles utilisés pour la communication web. HTTPS est la version cryptée.

I

Liste Blanche IP Liste d'adresses IP autorisées à se connecter à la passerelle (fonction de sécurité).

ISDN (Réseau Numérique à Intégration de Services) Plan de numérotation couramment utilisé pour les numéros de téléphone.

J

(Aucun terme)

K

Keepalive Messages périodiques (enquire_link) envoyés pour maintenir la connexion et détecter les échecs.

KPI (Indicateur Clé de Performance) Valeur mesurable indiquant la performance du système (par exemple, taux de succès de livraison).

L

Étiquette Dans Prometheus, paires clé-valeur attachées aux métriques pour identification (par exemple, `bind_name="vodafone_uk"`).

LiveView Technologie du framework Phoenix utilisée pour les mises à jour en temps réel de l'interface web.

M

File de Messages Système backend qui stocke les messages en attente d'être envoyés ou reçus.

Métriques Mesures quantitatives de la performance du système, exposées au format Prometheus.

MO (Mobile Originate) Messages envoyés depuis des téléphones mobiles vers

la passerelle (entrant).

MT (Mobile Terminate) Messages envoyés de la passerelle vers des téléphones mobiles (sortant).

MSISDN (Numéro de Répertoire International de Station Mobile) Format standard pour les numéros de téléphone mobile.

N

NPI (Indicateur de Plan de Numérotation) Champ SMPP spécifiant le schéma de numérotation (par exemple, ISDN).

O

Sortant Messages circulant de la passerelle vers les réseaux mobiles.

Entrant Messages circulant des réseaux mobiles vers la passerelle.

P

PDU (Unité de Données de Protocole) Paquet de message SMPP individuel (par exemple, submit_sm, deliver_sm).

Prometheus Système de surveillance open-source qui collecte et stocke des métriques de séries temporelles.

Q

File Liste de messages en attente d'être traités ou envoyés.

Fréquence de Vérification de la File À quelle fréquence (en millisecondes) la passerelle interroge le backend pour de nouveaux messages.

Travailleur de File Composant qui récupère des messages de la file et les envoie via SMPP.

R

Limitation de Taux Contrôle du débit de messages pour se conformer aux restrictions de l'opérateur. Voir TPS.

Récepteur Type de bind SMPP qui ne reçoit que des messages (deliver_sm).

Reconnecter Rétablir une connexion SMPP déconnectée.

Réessayer Tenter d'envoyer à nouveau un message échoué, généralement avec un retard exponentiel.

S

Bind Serveur Configuration définissant un client externe autorisé à se connecter à la passerelle.

Session Connexion SMPP active entre deux systèmes.

SMPP (Short Message Peer-to-Peer) Protocole standard de l'industrie pour l'échange de messages SMS entre systèmes.

SMSC (Centre de Service de Messages Courts) Système qui gère le routage et la livraison des messages SMS.

SSL/TLS Protocoles de cryptage pour une communication sécurisée.

Submit_SM PDU SMPP pour soumettre un message pour livraison.

Submit_SM_Resp Réponse SMPP à submit_sm, indiquant le succès ou l'échec.

ID Système Nom d'utilisateur utilisé pour l'authentification SMPP.

T

Télémétrie Collecte et transmission automatisées de métriques système.

TON (Type de Numéro) Champ SMPP spécifiant le format du numéro (par exemple, international, national).

TPS (Transactions Par Seconde) Limite de taux pour le nombre maximum de messages par seconde à travers une connexion.

Transcepteur Type de bind SMPP qui peut à la fois envoyer et recevoir des messages (le plus courant).

Émetteur Type de bind SMPP qui envoie uniquement des messages (submit_sm).

Débit Taux de traitement des messages, généralement mesuré en messages par seconde.

U

UCS-2 Encodage de caractères Unicode à 16 bits pour les SMS, prenant en charge jusqu'à 70 caractères par message.

Temps de Fonctionnement Durée pendant laquelle une connexion ou un service a été opérationnel en continu.

V

Période de Validité Limite de temps pour la tentative de livraison d'un message avant expiration.

W

Tableau de Bord Web Interface utilisateur basée sur un navigateur pour surveiller et gérer la passerelle.

Liste Blanche Voir Liste Blanche IP.

X

(Aucun terme)

Y

(Aucun terme)

Z

(Aucun terme)

Référence Rapide des Acronymes

Acronyme	Terme Complet
API	Interface de Programmation d'Applications
CIDR	Routage Inter-Domaines Sans Classe
DLR	Accusé de Réception de Livraison
GSM	Système Mondial de Communications Mobiles
HTTP	Protocole de Transfert Hypertexte
HTTPS	Protocole de Transfert Hypertexte Sécurisé
IP	Protocole Internet
ISDN	Réseau Numérique à Intégration de Services
KPI	Indicateur Clé de Performance
MO	Mobile Originate
MSISDN	Numéro de Répertoire International de Station Mobile
MT	Mobile Terminate

Acronyme	Terme Complet
NPI	Indicateur de Plan de Numérotation
PDU	Unité de Données de Protocole
SMPP	Short Message Peer-to-Peer
SMSC	Centre de Service de Messages Courts
SMS	Service de Messages Courts
SSL	Couche de Sockets Sécurisée
TLS	Sécurité de la Couche de Transport
TON	Type de Numéro
TPS	Transactions Par Seconde
UCS	Jeu de Caractères Codé Universel
UI	Interface Utilisateur
URL	Localisateur Uniforme de Ressources

Documentation Connexe

- **README.md** - Vue d'ensemble du système et guide de démarrage
- **CONFIGURATION.md** - Paramètres de configuration expliqués
- **OPERATIONS.md** - Opérations quotidiennes
- **MONITORING.md** - Métriques et surveillance
- **TROUBLESHOOTING.md** - Résolution de problèmes

Guide de Surveillance et de Métriques

Référence complète pour la surveillance de la passerelle SMPP

Vue d'ensemble

La passerelle SMPP expose des métriques au format Prometheus pour surveiller la santé des connexions, le débit des messages et la performance du système.

Critique : Étant donné que la passerelle est sans état et dépend d'OmniMessage Core, **la connectivité OmniMessage est la métrique la plus importante à surveiller**. Surveillez à la fois :

1. **Métriques de la passerelle SMPP** - Santé au niveau du protocole
2. **Métriques de l'API OmniMessage** - Connectivité et santé du backend

Point de terminaison des métriques

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

Format : Format texte Prometheus

Accès : Ouvert à localhost par défaut (configurer le pare-feu pour l'accès à distance)

Test rapide

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

Métriques Disponibles

Toutes les métriques sont préfixées par `smpp_` et incluent des étiquettes pour l'identification.

Métriques de Statut de Connexion

smpp_connection_status

Type : Gauge
Description : Statut de connexion actuel du lien SMPP
Valeurs :

- `1` = Connecté
- `0` = Déconnecté

Étiquettes :

- `bind_name` - Nom de la connexion (par exemple, "vodafone_uk")
- `mode` - Type de connexion ("client" ou "serveur")
- `host` - Hôte distant (mode client uniquement)
- `port` - Port distant (mode client uniquement)
- `bind_type` - Type de liaison SMPP (mode client uniquement)
- `system_id` - ID système utilisé

Exemple :

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

Utilisation :

- Alerter lorsque la valeur est 0 (déconnecté)
- Suivre le pourcentage de disponibilité de la connexion
- Surveiller la fréquence de reconnexion

Compteurs de Messages

smpp_messages_sent_total

Type : Counter
Description : Nombre total de messages envoyés via le lien SMPP
Unité : Messages

Étiquettes : Identiques à connection_status

Exemple :

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

Utilisation :

- Calculer le taux de messages (messages/seconde)
- Suivre le volume quotidien/mensuel
- Comparer le débit réel au débit attendu

smpp_messages_received_total

Type : Counter
Description : Nombre total de messages reçus via le lien SMPP
Unité : Messages

Étiquettes : Identiques à connection_status

Exemple :

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

Utilisation :

- Surveiller le volume de messages entrants
- Suivre le trafic d'origine mobile (MO)
- Alerter sur des changements de volume inattendus

Métriques de Livraison

smpp_delivery_failures_total

Type : Counter
Description : Nombre total d'échecs de livraison de messages
Unité : Échecs

Étiquettes : Identiques à connection_status

Exemple :

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

Utilisation :

- Calculer le taux de réussite de livraison
- Alerter sur des taux d'échec élevés
- Identifier les connexions problématiques

Calcul du Taux de Réussite :

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

Métriques d'Opération de Liaison

smpp_bind_success_total

Type : Counter
Description : Nombre total d'opérations de liaison réussies
Unité : Tentatives de liaison

Exemple :

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

Utilisation :

- Suivre la stabilité de la liaison
- Surveiller le succès de l'authentification

smpp_bind_failures_total

Type : Counter
Description : Nombre total d'opérations de liaison échouées
Unité : Tentatives de liaison

Exemple :

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

Utilisation :

- Alerter sur des échecs d'authentification
- Identifier des problèmes de crédentiels
- Suivre les problèmes de connexion avec le transporteur

Métriques d'Événements de Connexion

smpp_connection_attempts_total

Type : Counter
Description : Nombre total de tentatives de connexion
Unité : Tentatives

Exemple :

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

Utilisation :

- Suivre le taux de rotation des connexions
- Surveiller la fréquence de reconnexion

smpp_disconnection_total

Type : Counter
Description : Nombre total de déconnexions
Unité : Déconnexions

Exemple :

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

Utilisation :

- Alerter sur des déconnexions fréquentes

- Identifier des problèmes de réseau
- Suivre la stabilité de la connexion

Métriques de Disponibilité

smpp_uptime_seconds

Type : Gauge
Description : Disponibilité actuelle du lien SMPP en secondes
Unité : Secondes

Exemple :

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

Utilisation :

- Suivre la stabilité de la connexion
- Calculer le pourcentage de disponibilité
- Alerter sur des redémarrages récents

Métriques de Santé de l'API OmniMessage

Bien que la passerelle elle-même expose des métriques liées à SMPP, **la santé de l'API OmniMessage est critique**. Vous devez également surveiller :

Depuis les Métriques OmniMessage (si disponibles)

- `omnimessage_api_requests_total` - Total des requêtes API de la passerelle
- `omnimessage_api_request_duration_seconds` - Temps de réponse de l'API
- `omnimessage_queue_depth` - Messages en attente dans la file d'attente OmniMessage

Depuis les Journaux de la Passerelle (si les métriques ne sont pas exposées)

Recherchez ces motifs pour détecter des problèmes d'API :

- "api.*connection refused" - Impossible d'atteindre OmniMessage
- "api.*timeout" - OmniMessage ne répond pas
- "api.*http 503" - OmniMessage temporairement hors service
- "api.*parse error" - Problème de format de réponse

Configuration de Prometheus

Configuration de Scrape de Base

Ajoutez à `/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'
```

Plusieurs Passerelles

```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'
```

Découverte de Service

Utilisation de la découverte basée sur des fichiers :

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

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

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

Tableaux de Bord Grafana

Panneaux de Tableau de Bord Exemples

Panneau de Statut de Connexion

Requête :

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

Visualisation : Stat
Seuils :

- Rouge : valeur < 1 (déconnecté)
- Vert : valeur == 1 (connecté)

Panneau de Taux de Messages

Requête :

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

Visualisation : Graph
Unité : messages/seconde
Légende : {{bind_name}}

Panneau de Taux de Réussite de Livraison

Requête :

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

Visualisation : Gauge
Unité : Pourcentage (0-100)
Seuils :

- Rouge : < 95%
- Jaune : 95-98%
- Vert : > 98%

Panneau de Disponibilité de Connexion

Requête :

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

Visualisation : Stat
Unité : Heures

Règles d'Alerte

Règles d'Alerte Prometheus

Enregistrez dans `/etc/prometheus/rules/smpp-alerts.yml` :

```yaml
groups:
  - name: smpp_gateway
    interval: 30s
    rules:
      # Connexion hors service
      - alert: SMPPConnectionDown
        expr: smpp_connection_status == 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "La connexion SMPP {{ $labels.bind_name }} est hors service"
          description: "La connexion {{ $labels.bind_name }} a été déconnectée pendant plus de 2 minutes."

      # Taux d'échec élevé
      - alert: SMPPHighFailureRate
        expr: |
          (
            rate(smpp_delivery_failures_total[5m])
            /
            rate(smpp_messages_sent_total[5m])
          ) > 0.05
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Taux d'échec de livraison élevé sur {{ $labels.bind_name }}"
          description: "Le taux d'échec de livraison est {{ $value | humanizePercentage }} sur {{ $labels.bind_name }}."

      # Échecs de liaison
      - alert: SMPPBindFailures
        expr: increase(smpp_bind_failures_total[10m]) > 3
        labels:
          severity: warning
        annotations:
          summary: "Multiples échecs de liaison sur {{ $labels.bind_name }}"
          description: "{{ $labels.bind_name }} a échoué à se lier {{ $value }} fois au cours des 10 dernières minutes."
```

```
      # Aucun message envoyé (lorsqu'attendu)
      - alert: SMPPNoTraffic
        expr: rate(smpp_messages_sent_total[10m]) == 0
        for: 30m
        labels:
          severity: warning
        annotations:
          summary: "Aucun message envoyé sur {{ $labels.bind_name }}"
          description: "{{ $labels.bind_name }} n'a pas envoyé de messages pendant 30 minutes."

      # Déconnexions fréquentes
      - alert: SMPPFrequentDisconnections
        expr: increase(smpp_disconnection_total[1h]) > 5
        labels:
          severity: warning
        annotations:
          summary: "Déconnexions fréquentes sur {{ $labels.bind_name }}"
          description: "{{ $labels.bind_name }} s'est déconnecté {{ $value }} fois au cours de la dernière heure."

      # API OmniMessage injoignable
      - alert: OmniMessageAPIUnreachable
        expr: |
          count(count_over_time({job="omnimessage-smpp"} |= "api.*connection refused"[5m])) > 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "L'API OmniMessage est injoignable"
          description: "La passerelle SMPP ne peut pas atteindre l'API OmniMessage. Vérifiez la configuration API_BASE_URL et la connectivité
réseau."

      # Délai d'attente de l'API OmniMessage
      - alert: OmniMessageAPITimeout
        expr: |
          count(count_over_time({job="omnimessage-smpp"} |= "api.*timeout"[5m])) > 5
        for: 2m
        labels:
          severity: warning
        annotations:
          summary: "L'API OmniMessage prend du temps"
          description: "Plusieurs délais d'attente de l'API détectés. OmniMessage peut être lent ou surchargé."

      # Aucun flux de message (problème 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: "Aucun flux de message détecté - vérifiez la connectivité OmniMessage"
          description: "Aucun message envoyé ou reçu pendant 30 minutes. Vérifiez la connectivité de l'API OmniMessage et l'état de la file
d'attente."
```

Chargez les règles dans `prometheus.yml` :

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

Surveillance du Tableau de Bord Web

L'interface web intégrée fournit une surveillance en temps réel sans Prometheus.

Accès

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

Page de Statut en Direct

Navigation : SMPP → Statut en Direct

Fonctionnalités :

- Statut de connexion en temps réel
- Compteurs de messages
- Disponibilité de la connexion
- Contrôles de reconnexion/déconnexion manuels
- Actualisation automatique toutes les 5 secondes

Utilisation :

- Vérification rapide de l'état
- Intervention manuelle
- Dépannage en temps réel

Le tableau de bord affiche :

- **Total des Liens** : Compte combiné de toutes les connexions client et serveur
- **Liens Clients** : Connexions sortantes vers les transporteurs (affichant le compte connecté/déconnecté)
- **Liens Serveurs** : Connexions entrantes des partenaires (affichant le compte actif/en attente)
- **Serveur Écoute** : Configuration de la socket serveur entrante (hôte, port, connexions maximales)

Surveillance des Journaux

Journaux Système

Voir les journaux :

```
# Suivre les journaux en temps réel
sudo journalctl -u omnimessage-smpp -f

# Dernières 100 lignes
sudo journalctl -u omnimessage-smpp -n 100

# Depuis un temps spécifique
sudo journalctl -u omnimessage-smpp --since "1 hour ago"

# Filtrer par niveau
sudo journalctl -u omnimessage-smpp -p err
```

Journaux de l'Interface Web

Navigation : Onglet Journaux dans l'interface web

Fonctionnalités :

- Diffusion en temps réel des journaux
- Filtrer par niveau (debug, info, warning, error)
- Rechercher dans les journaux
- Mettre en pause/reprendre
- Effacer les journaux

La vue des journaux vous permet de :

- **Filtrer par Niveau** : Sélectionner le niveau de journal (Tous, Debug, Info, Avertissement, Erreur)
- **Rechercher** : Trouver des entrées de journal spécifiques par contenu texte
- **Défilement Automatique** : Activer/désactiver le défilement automatique à l'arrivée de nouveaux journaux
- **Mettre en Pause/Reprendre** : Mettre à jour les journaux pour examiner des entrées spécifiques
- **Effacer** : Effacer tous les journaux affichés

Indicateurs Clés de Performance (KPI)

Santé de la Connexion

Métrique : Pourcentage de disponibilité de la connexion

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

Cible : > 99.9%

Taux de Livraison des Messages

Métrique : Messages livrés par seconde

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

Cible : Correspond au volume attendu

Taux de Réussite de Livraison

Métrique : Pourcentage de livraisons réussies

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

Cible : > 98%

Stabilité de la Liaison

Métrique : Tentatives de liaison par heure

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

Cible : < 10 par heure (indique une connexion stable)

Meilleures Pratiques de Surveillance

1. Configurer des Alertes

- Configurer des alertes Prometheus pour les métriques critiques
- Utiliser PagerDuty/OpsGenie pour des alertes 24/7
- Tester régulièrement les alertes

2. Créer des Tableaux de Bord

- Construire des tableaux de bord Grafana pour chaque passerelle
- Inclure toutes les connexions sur un tableau de bord
- Ajouter des panneaux de planification de capacité

3. Revue Régulière

- Revoir les métriques chaque semaine
- Identifier les tendances et les motifs
- Planifier des ajustements de capacité

4. Documenter les Lignes de Base

- Enregistrer les volumes de messages normaux
- Documenter les taux TPS attendus
- Noter les heures/jours de pointe

5. Corréler avec le Backend

- Surveiller les métriques de l'API backend
- Suivre le flux de messages de bout en bout
- Identifier les goulets d'étranglement

Dépannage avec les M��triques

Problèmes de Connexion

Vérifiez : `smpp_connection_status`

- Valeur 0 = Vérifiez les journaux, vérifiez le réseau, vérifiez les crédentiels
- Changements fréquents = Instabilité du réseau

Mauvais Taux de Livraison

Vérifiez : `smpp_delivery_failures_total`

- Taux élevé = Vérifiez l'état du transporteur, examinez le format des messages
- Comparez entre les connexions = Identifiez le transporteur problématique

Faible Débit

Vérifiez : taux de `smpp_messages_sent_total`

- En dessous de l'attendu = Vérifiez les limites TPS, disponibilité de la file d'attente
- Vérifiez les métriques de l'API backend

Problèmes de Liaison

Vérifiez : `smpp_bind_failures_total`

- En augmentation = Problèmes d'authentification, problèmes de crédentiels
- Vérifiez system_id et mot de passe dans la configuration

Documentation Connexe

- **CONFIGURATION.md** - Configurer les paramètres de surveillance
- **OPERATIONS.md** - Procédures opérationnelles
- **TROUBLESHOOTING.md** - Résoudre les problèmes
- **README.md** - Vue d'ensemble et démarrage rapide

Guide des opérations

Procédures opérationnelles quotidiennes

Dépendance critique : OmniMessage Core

IMPORTANT : La passerelle SMPP OmniMessage ne peut pas fonctionner sans accès à OmniMessage Core. Tout le traitement des messages se fait dans OmniMessage - la passerelle n'est qu'un traducteur de protocole.

Si OmniMessage devient indisponible :

- 🔀 De nouveaux messages ne peuvent pas être soumis
- 🔀 Les messages en attente ne peuvent pas être récupérés
- 🔀 L'état de livraison ne peut pas être signalé
- 🔀 Le système semble se bloquer ou expirer

Vérifiez la santé d'OmniMessage :

```
# Tester la connectivité API
curl -k https://omnimessage-core.example.com:8443/api/system/health

# Vérifiez l'URL API configurée dans les journaux
grep api_base_url /opt/omnimessage-smpp/config/runtime.exs
```

Opérations quotidiennes

Vérification de santé du matin

Effectuez ces vérifications au début de chaque journée :

1. **Accéder au tableau de bord Web**
    - URL : `https://your-server:8087`
    - Vérifiez si le tableau de bord se charge correctement
2. **Vérifier l'état de la connexion**
    - Naviguez vers : SMPP → État en direct
    - Vérifiez que toutes les connexions affichent "Connecté" (vert)
    - Notez les liaisons déconnectées
3. **Examiner les métriques de message**

    - Naviguez vers : Onglet Queue
    - Vérifiez que les comptes de messages sont raisonnables
    - Vérifiez qu'il n'y a pas d'accumulation inattendue dans la file d'attente

4. **Vérifier les journaux système**

    - Naviguez vers : Onglet Logs
    - Recherchez des messages d'erreur (rouge)
    - Notez les motifs d'avertissement

5. **Examiner les métriques Prometheus**

    - `curl http://localhost:4000/metrics`
    - Ou vérifiez les tableaux de bord Grafana
    - Vérifiez que les taux de message sont normaux

Surveillance continue

Configurez des alertes pour :

- Échecs de connexion (> 2 minutes hors ligne)
- Taux d'échec de livraison élevé (> 5 %)
- Pas de trafic pendant de longues périodes
- Déconnexions fréquentes

Voir MONITORING.md pour la configuration des alertes.

Gestion des connexions SMPP

Comment les pairs SMPP sont configurés

Les connexions SMPP (pairs) peuvent être configurées en utilisant **deux méthodes** :

Méthode 1 : Interface Web (Recommandée)

- **Avantage** : Les modifications prennent effet immédiatement, aucun redémarrage requis
- **Emplacement** : Onglets SMPP → Pairs clients / Pairs serveurs
- **Opérations** : Ajouter, modifier, supprimer des pairs
- **Persistance** : Stocké dans la base de données Mnesia
- **Meilleur pour** : Opérations quotidiennes, tests, modifications rapides

Méthode 2 : Fichier de configuration

- **Avantage** : Configuration en tant que code, contrôle de version
- **Emplacement** : `/opt/omnimessage-smpp/config/runtime.exs`
- **Opérations** : Définir des pairs dans la configuration Elixir
- **Persistance** : Basé sur des fichiers, survit aux redémarrages
- **Nécessite** : Redémarrage du service après modifications
- **Meilleur pour** : Configuration initiale, infrastructure en tant que code

Remarque : Les modifications de l'interface Web sont stockées séparément et remplacent les paramètres du fichier de configuration.

Voir CONFIGURATION.md pour référence au fichier de configuration.

Ajouter une nouvelle connexion client

But : Se connecter à un nouveau serveur SMPP de transporteur

Préparation : Rassembler des informations du transporteur :

- Nom d'hôte/IP du serveur SMPP
- Numéro de port (généralement 2775)
- ID système (nom d'utilisateur)
- Mot de passe
- Type de liaison (généralement transceiver)
- Limite TPS

Choisissez l'une des méthodes suivantes :

Option A : Via l'interface Web (Recommandée)

Avantages : Effet immédiat, aucun redémarrage requis

Étapes :

1. **Naviguer vers les pairs clients** :
    - Ouvrir l'interface Web : `https://your-server:8087`
    - Naviguer vers : SMPP → Pairs clients
2. **Ajouter un nouveau pair** :
    - Cliquez sur "Ajouter un nouveau pair client"
    - Remplissez le formulaire :
        - **Nom** : `vodafone_uk` (identifiant unique)
        - **Hôte** : `smpp.vodafone.co.uk`
        - **Port** : 2775
        - **ID système** : `your_username`

        - **Mot de passe** : `your_password`
        - **Type de liaison** : `Transceiver`
        - **Limite TPS** : `100`
        - **Fréquence de vérification de la file d'attente** : `1000`
    - Cliquez sur "Enregistrer"

3. **La connexion s'établit automatiquement** :
    - La passerelle tente immédiatement de se connecter
    - Naviguez vers : SMPP → État en direct
    - L'état devrait changer en "Connecté" (vert) dans les 10 à 30 secondes
    - Vérifiez l'onglet Logs pour un message de liaison réussi

4. **Tester le flux de messages** :
    - Naviguez vers : Onglet Queue
    - Soumettez un message de test avec `dest_smsc` correspondant au nom de la liaison
    - Surveillez dans l'état en direct pour la transmission
    - Vérifiez la confirmation de livraison

Option B : Via le fichier de configuration

Avantages : Infrastructure en tant que code, contrôle de version

Étapes :

1. **Modifier le fichier de configuration** :

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

2. **Ajouter une nouvelle liaison à la configuration** :

```
config :omnimessage_smpp, :binds, [
  # Liaisons existantes...

  # Ajouter une nouvelle liaison
  %{
    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. **Enregistrer et redémarrer le service** :

```
# Enregistrer le fichier (Ctrl+X, Y, Entrée dans nano)

# Redémarrer le service
sudo systemctl restart omnimessage-smpp
```

4. **Vérifier la connexion** :
    - Naviguez vers : SMPP → État en direct
    - Trouvez la nouvelle connexion
    - L'état devrait être "Connecté" (vert)
    - Vérifiez les journaux pour une liaison réussie

5. **Tester le flux de messages** :
    - Naviguez vers : Onglet Queue
    - Soumettez un message de test avec `dest_smsc` correspondant au nouveau nom de liaison
    - Surveillez dans l'état en direct pour la transmission
    - Vérifiez la confirmation de livraison

Ajouter une liaison serveur

But : Permettre à un partenaire externe de se connecter à votre passerelle

Préparation :

1. **Générer des identifiants** :
    - Créer un ID système unique : `partner_name`
    - Créer un mot de passe fort
    - Documenter et partager en toute sécurité avec le partenaire

2. **Obtenir des informations sur le partenaire** :
    - Adresses IP sources du partenaire
    - Volume de messages attendu (pour la limite TPS)
    - Types de liaison requis

Choisissez l'une des méthodes suivantes :

Option A : Via l'interface Web (Recommandée)

Avantages : Effet immédiat, aucun redémarrage requis

Étapes :

1. **Naviguer vers les pairs serveurs** :
    - Ouvrir l'interface Web : `https://your-server:8087`
    - Naviguer vers : SMPP → Pairs serveurs
2. **Ajouter un nouveau pair serveur** :
    - Cliquez sur "Ajouter un nouveau pair serveur"
    - Remplissez le formulaire :
        - **Nom** : `partner_acme` (identifiant unique)
        - **ID système** : `acme_corp`
        - **Mot de passe** : `secure_password_123`
        - **Types de liaison autorisés** : Sélectionner tous (Transmetteur, Récepteur, Transceiver)
        - **Liste blanche IP** : `203.0.113.0/24` (séparé par des virgules pour plusieurs)
        - **Limite TPS** : `50`
        - **Fréquence de vérification de la file d'attente** : `1000`
    - Cliquez sur "Enregistrer"
3. **Passerelle prête pour la connexion** :
    - Le pair serveur est maintenant actif et attend la connexion du partenaire
    - Aucun redémarrage requis
4. **Partager les informations avec le partenaire** :
    - Adresse IP de la passerelle
    - Port : `2775`
    - ID système : `acme_corp`
    - Mot de passe : `secure_password_123`
    - Type de liaison : Comme configuré
5. **Attendre la connexion du partenaire** :
    - Naviguez vers : SMPP → État en direct
    - Surveillez la connexion entrante
    - Vérifiez le succès de l'authentification
    - Vérifiez que l'IP correspond à la liste blanche

Option B : Via le fichier de configuration

Avantages : Infrastructure en tant que code, contrôle de version

Étapes :

1. **Modifier le fichier de configuration** :

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

2. **Ajouter la liaison serveur et la configuration d'écoute** :

   ```
   # Ajouter à la liste des server_binds
   config :omnimessage_smpp, :server_binds, [
     # Liaisons serveur existantes...

     # Ajouter une nouvelle liaison serveur
     %{
       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
     }
   ]

   # Assurez-vous que la configuration d'écoute existe (nécessaire
   une seule fois)
   config :omnimessage_smpp, :listen, %{
     host: "0.0.0.0",
     port: 2775,
     max_connections: 100
   }
   ```

3. **Enregistrer et redémarrer le service** :

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

4. **Partager les informations avec le partenaire** :

   - Adresse IP de la passerelle
   - Port : `2775`
   - ID système : `acme_corp`
   - Mot de passe : `secure_password_123`
   - Type de liaison : Comme configuré

5. **Attendre la connexion du partenaire** :

   - Naviguez vers : SMPP → État en direct
   - Surveillez la connexion entrante
   - Vérifiez le succès de l'authentification
   - Vérifiez que l'IP correspond à la liste blanche

Modifier une connexion existante

But : Mettre à jour les paramètres de connexion (limites TPS, mots de passe, liste blanche IP, etc.)

Choisissez l'une des méthodes suivantes :

Option A : Via l'interface Web (Recommandée)

Avantages : Effet immédiat, aucun redémarrage requis

Étapes :

1. **Naviguer vers les pairs** :
    - Ouvrir l'interface Web : `https://your-server:8087`
    - Pour les connexions clients : SMPP → Pairs clients
    - Pour les connexions serveurs : SMPP → Pairs serveurs
2. **Modifier le pair** :
    - Trouvez le pair à modifier
    - Cliquez sur le bouton "Modifier"
    - Mettez à jour les paramètres souhaités :
        - Modifications courantes : Limite TPS, mot de passe, liste blanche IP, hôte/port
    - Cliquez sur "Enregistrer"
3. **Les modifications s'appliquent immédiatement** :
    - La connexion se reconnecte automatiquement avec les nouveaux paramètres
    - Aucun redémarrage de service requis
    - Naviguez vers : SMPP → État en direct pour vérifier
4. **Vérifier les modifications** :
    - Vérifiez que la connexion s'établit avec succès
    - Surveillez l'onglet Logs pour les erreurs
    - Testez le flux de messages si applicable

Option B : Via le fichier de configuration

Avantages : Infrastructure en tant que code, contrôle de version

Étapes :

1. **Modifier le fichier de configuration** :

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

2. **Modifier les paramètres de liaison** :
    - Trouvez la liaison dans la liste `:binds` ou `:server_binds`
    - Mettez à jour les paramètres souhaités :
        - Modifications courantes : Limite TPS, mots de passe, liste blanche IP, hôte/port
    - Exemple :

```
%{
  name: "vodafone_uk",
  # ... autres paramètres
  tps_limit: 150,  # Changé de 100
  password: "new_password"  # Mot de passe mis à jour
}
```

3. **Enregistrer et redémarrer le service** :

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

4. **Vérifier les modifications** :
    - Naviguez vers : SMPP → État en direct
    - Vérifiez que la connexion s'établit avec succès
    - Surveillez les journaux pour les erreurs
    - Testez le flux de messages

Supprimer une connexion

But : Décommissionner une connexion SMPP

Étapes :

1. **Notifier les parties prenantes** :
    - Informer le transporteur/partenaire
    - Coordonner la fenêtre d'arrêt
2. **Déconnecter via l'interface Web** :
    - Naviguez vers : SMPP → État en direct
    - Trouvez la connexion
    - Cliquez sur "Supprimer la connexion"
    - Confirmez l'action
3. **Supprimer la configuration** :
    - Naviguez vers : SMPP → Pairs clients/serveurs

- Trouvez la connexion
- Cliquez sur "Supprimer"
- Confirmez la suppression

4. **Vérifier la suppression** :

   - Vérifiez l'état en direct - la connexion devrait avoir disparu
   - Consultez les journaux pour un arrêt propre

Gestion du flux de messages

Vérification de la file d'attente des messages

But : Surveiller les messages en attente

Étapes :

1. **Accéder à la file d'attente** :

   - Naviguez vers : Onglet Queue
   - Voir la liste des messages en attente

2. **Vérifier les détails du message** :

   - Cliquez sur la ligne du message
   - Examiner :
     - Numéro de destination
     - Corps du message
     - SMSC cible (`dest_smsc`)
     - Tentatives de livraison
     - État

3. **Rechercher un message spécifique** :

   - Utilisez le filtre de recherche
   - Filtrer par destination, contenu ou SMSC

Dépannage des messages bloqués

Symptômes : Les messages ne sont pas livrés

Étapes :

1. **Vérifier l'état de la connexion** :

   - Naviguez vers : SMPP → État en direct
   - Vérifiez que la connexion cible est connectée

- Si déconnectée, voir Reconnecter

2. **Vérifier les détails du message** :
   - Naviguez vers : Onglet Queue
   - Trouvez le message bloqué
   - Vérifiez que le champ `dest_smsc` correspond au nom de la connexion
   - Vérifiez le timestamp `deliver_after` (planification de la nouvelle tentative)
3. **Vérifier les tentatives de livraison** :
   - Tentatives élevées = échecs répétés
   - Vérifiez les journaux pour des messages d'erreur
   - Peut indiquer un format invalide ou un rejet du transporteur
4. **Intervention manuelle** (si nécessaire) :
   - Contacter le transporteur pour vérifier le problème
   - Peut nécessiter d'annuler et de soumettre à nouveau le message
   - Vérifiez avec l'équipe backend pour des problèmes de file d'attente

---

Dépannage de connexion

Reconnecter une liaison

Symptômes : La connexion affiche "Déconnecté" (rouge)

Étapes :

1. **Vérifier la connectivité réseau** :

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

2. **Vérifier les journaux pour des erreurs** :
   - Naviguez vers : Onglet Logs
   - Filtrer : Niveau d'erreur
   - Rechercher des échecs d'authentification, des délais d'attente réseau
3. **Vérifier les identifiants** :
   - Naviguez vers : SMPP → Pairs clients/serveurs
   - Vérifiez que `system_id` et le mot de passe sont corrects
   - Contacter le transporteur si incertain

4. **Reconnecter manuellement** :
    - Naviguez vers : SMPP → État en direct
    - Trouvez la liaison déconnectée
    - Cliquez sur le bouton "Reconnecter"
    - Attendez 10 à 30 secondes
    - Vérifiez si l'état change en "Connecté"
5. **Si la reconnexion échoue** :
    - Vérifiez les règles de pare-feu
    - Vérifiez que le serveur du transporteur est opérationnel
    - Contacter le support du transporteur
    - Voir TROUBLESHOOTING.md

Gestion des échecs d'authentification

Symptômes : Échecs de liaison répétés dans les journaux

Causes :

- Nom d'utilisateur/mot de passe incorrect
- IP non autorisée par le transporteur
- Compte suspendu/expiré

Étapes :

1. **Vérifier les identifiants** :
    - Naviguez vers : SMPP → Pairs clients
    - Vérifiez à nouveau `system_id` et le mot de passe
    - Confirmez avec le transporteur
2. **Vérifier la liste blanche IP** :
    - Confirmez l'IP de votre passerelle avec le transporteur
    - Demandez au transporteur de vérifier la liste blanche IP
3. **Vérifier l'état du compte** :
    - Vérifiez que le compte est actif
    - Vérifiez les contrats expirés
    - Contacter la facturation du transporteur
4. **Mettre à jour la configuration** :
    - Si les identifiants ont changé, mettez à jour dans l'interface Web
    - Cliquez sur "Reconnecter" pour réessayer avec les nouveaux identifiants

Surveillance et alertes

Vérification des métriques Prometheus

Vérification rapide :

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

Sortie attendue :

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

Tous les valeurs devraient être 1 (connecté).

Répondre aux alertes

Alerte de connexion hors ligne :

1. Vérifiez l'interface Web → SMPP → État en direct
2. Tentez une reconnexion manuelle
3. Vérifiez les journaux pour des erreurs
4. Contacter le transporteur en cas de panne prolongée
5. Voir TROUBLESHOOTING.md

Alerte de taux d'échec ��levé :

1. Vérifiez les journaux pour des motifs d'erreur
2. Examinez les modifications récentes de configuration
3. Contacter le transporteur au sujet des rejets
4. Vérifiez la conformité du format des messages

Alerte de trafic nul :

1. Vérifiez que la file d'attente backend a des messages
2. Vérifiez que le routage `dest_smsc` est correct
3. Vérifiez que les limites TPS ne sont pas trop restrictives
4. Examinez le paramètre `queue_check_frequency`

Procédures de maintenance

Maintenance de routine

Effectuer mensuellement :

1. **Examiner les métriques** :
    - Analyser les tendances du volume de messages
    - Vérifier les taux de succès de livraison
    - Identifier les opportunités d'optimisation
2. **Mettre à jour la documentation** :
    - Documenter toute modification de configuration
    - Mettre à jour les informations de contact
    - Noter les fenêtres de maintenance du transporteur
3. **Audit des identifiants** :
    - Vérifier tous les mots de passe SMPP
    - Planifier la rotation des identifiants
    - Vérifier que les listes blanches IP sont à jour
4. **Planification de la capacité** :
    - Examiner les taux de messages de pointe
    - Vérifier par rapport aux limites TPS
    - Planifier la croissance

Redémarrage du service

Quand nécessaire :

- Après des modifications du fichier de configuration
- Après des mises à jour système
- Lors du dépannage

Étapes :

```
# Vérifier l'état actuel
sudo systemctl status omnimessage-smpp

# Redémarrer le service
sudo systemctl restart omnimessage-smpp

# Vérifier le redémarrage
sudo systemctl status omnimessage-smpp

# Vérifier les journaux
sudo journalctl -u omnimessage-smpp -n 50
```

Vérifier via l'interface Web :

1. Accédez au tableau de bord (peut prendre 30 à 60 secondes pour se mettre

en ligne)
2. Naviguez vers : SMPP → État en direct
3. Attendez que toutes les connexions s'établissent (1 à 2 minutes)
4. Vérifiez les journaux pour des erreurs

Sauvegarde de configuration

Sauvegarder les fichiers critiques avant les modifications :

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

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

Restaurer si nécessaire :

```
# Restaurer la configuration
sudo cp /opt/omnimessage-smpp/config/runtime.exs.backup.YYYYMMDD \
  /opt/omnimessage-smpp/config/runtime.exs

# Redémarrer le service
sudo systemctl restart omnimessage-smpp
```

Procédures d'urgence

Panne de service complète

Étapes :

1. **Vérifiez l'état du service** :

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

2. **Si le service est arrêté, démarrez-le** :

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

3. **Vérifiez les journaux pour la raison du plantage** :

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

4. **Si ne démarre pas** :

   - Vérifiez les erreurs de syntaxe de configuration

- Vérifiez que les certificats SSL existent
- Vérifiez l'espace disque : `df -h`
- Vérifiez la mémoire : `free -h`

5. **Contacter le support** si non résolu

Demandes d'urgence de déconnexion du transporteur

Étapes :

1. **Supprimer la connexion immédiatement** :
   - Naviguez vers : SMPP → État en direct
   - Trouvez la connexion concernée
   - Cliquez sur "Supprimer la connexion"
2. **Documenter la raison** :
   - Notez le nom du transporteur
   - Enregistrez l'heure et la raison
   - Sauvegardez la correspondance
3. **Enquêter sur le problème** :
   - Vérifiez les motifs de message récents
   - Examinez les journaux pour des erreurs
   - Identifiez la cause profonde
4. **Coordonner la résolution** :
   - Travailler avec le transporteur
   - Mettre en œuvre des corrections
   - Tester avant de reconnecter

Pic de volume élevé

Symptômes : Trafic de message anormalement élevé

Étapes :

1. **Vérifiez les limites TPS** :
   - Naviguez vers : SMPP → État en direct
   - Vérifiez que les connexions ne sont pas throttling
   - Peut nécessiter d'augmenter temporairement les limites TPS
2. **Surveillez la stabilité du transporteur** :
   - Surveillez les déconnexions

    - Vérifiez les taux de succès de livraison

3. **Coordonner avec le backend** :
    - Vérifiez que la source des messages est légitime
    - Peut nécessiter d'implémenter une limitation de taux en amont

4. **Évoluer si nécessaire** :
    - Peut nécessiter des instances supplémentaires de passerelle
    - Contacter le support pour des conseils sur l'évolutivité

Meilleures pratiques

Liste de contrôle quotidienne

- [ ] Vérifiez que toutes les connexions SMPP sont connectées
- [ ] Examinez les journaux d'erreurs pour tout problème
- [ ] Surveillez la file d'attente de messages pour l'accumulation
- [ ] Vérifiez les tableaux de bord Prometheus/Grafana
- [ ] Vérifiez que les taux de succès de livraison > 98 %

Tâches hebdomadaires

- [ ] Examiner les tendances des métriques
- [ ] Vérifiez les anomalies de motifs
- [ ] Tester les procédures de récupération après sinistre
- [ ] Mettre à jour la documentation si nécessaire
- [ ] Examiner et reconnaître les alertes

Tâches mensuelles

- [ ] Audit des identifiants
- [ ] Révision de la planification de la capacité
- [ ] Mettre à jour les contacts du transporteur
- [ ] Examiner et optimiser les paramètres TPS
- [ ] Sauvegarder les fichiers de configuration

Documentation connexe

- **CONFIGURATION.md** - Configurer les connexions et les paramètres
- **MONITORING.md** - Configurer les alertes Prometheus

- **TROUBLESHOOTING.md** - Résoudre les problèmes courants
- **README.md** - Vue d'ensemble du système

Guide de Dépannage

Problèmes courants et solutions

Problèmes de Connectivité OmniMessage

Puisque la passerelle SMPP est sans état et dépend entièrement d'OmniMessage Core, les problèmes de connectivité avec OmniMessage sont les problèmes les plus critiques.

Symptômes de Déconnexion d'OmniMessage

- **Aucun message sortant** : La file d'attente s'accumule, les messages ne sont pas envoyés
- **Aucun message entrant** : Les partenaires ne peuvent pas soumettre de messages
- **Délai d'attente** : Les appels API expirent ou se bloquent
- **Les journaux montrent** : "Connection refused", "Timeout", "HTTP 503", "Connection reset"

Diagnostic

1. Vérifiez la Disponibilité d'OmniMessage :

```
# Tester la connectivité
curl -k -v https://omnimessage-core.example.com:8443/api/system/
health

# Tester depuis l'hôte de la passerelle spécifiquement
ssh gateway-server 'curl -k https://omnimessage-
core.example.com:8443/api/system/health'
```

2. Vérifiez l'URL API Configurée :

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

# Vérifier la connectivité réseau
ping omnimessage-core.example.com
nc -zv omnimessage-core.example.com 8443
```

3. Vérifiez les Journaux de la Passerelle pour les Erreurs API :

```
# Rechercher des erreurs liées à l'API
```

```
sudo journalctl -u omnimessage-smpp -f | grep -i
'api\|omnimessage\|connect'

# Rechercher des erreurs récentes dans les journaux
sudo journalctl -u omnimessage-smpp -n 200 | grep -i error
```

Solutions

Si OmniMessage est hors service :

1. Contacter l'équipe des opérations d'OmniMessage
2. Les messages en attente s'accumuleront dans la file d'attente
3. La passerelle continuera d'essayer (voir `SMPP_POLL_INTERVAL`)
4. Vérifier la page d'état d'OmniMessage ou la surveillance

Si OmniMessage est opérationnel mais que la passerelle ne peut pas y accéder :

1. Vérifiez que les règles de pare-feu permettent HTTPS sortant
2. Vérifiez la résolution DNS : `nslookup omnimessage-core.example.com`
3. Vérifiez le routage réseau : `traceroute omnimessage-core.example.com`
4. Vérifiez les certificats SSL si vous utilisez HTTPS

Si l'URL de l'API est mal configurée :

1. Éditez `/opt/omnimessage-smpp/config/runtime.exs`
2. Vérifiez que `api_base_url` est correct (doit être HTTPS pour la production)
3. Redémarrez la passerelle : `sudo systemctl restart omnimessage-smpp`

Problèmes de Connexion

La Connexion ne S'établit Pas

Symptômes :

- Le statut indique "Déconnecté" (rouge)
- Aucun lien réussi dans les journaux
- Tentatives de connexion répétées

Causes Possibles & Solutions :

1. Problèmes de Connectivité Réseau

Vérifiez :

```
# Tester la résolution DNS
```

```
nslookup smpp.carrier.com

# Tester la connectivité
ping -c 3 smpp.carrier.com

# Tester le port
telnet smpp.carrier.com 2775
# ou
nc -zv smpp.carrier.com 2775
```

Solutions :

- Si DNS échoue : Utilisez l'adresse IP au lieu du nom d'hôte dans la configuration
- Si le ping échoue : Vérifiez les règles de pare-feu, contactez le transporteur
- Si le port échoue : Vérifiez le numéro de port correct, vérifiez le pare-feu

2. Identifiants Incorrects

Vérifiez :

- Les journaux montrent "bind failed" ou "authentication error"
- Interface Web : SMPP → Client Peers → vérifiez system_id et mot de passe

Solutions :

- Confirmez les identifiants avec le transporteur
- Vérifiez les fautes de frappe (sensible à la casse)
- Mettez à jour la configuration et reconnectez

3. IP Non Autorisée

Vérifiez :

- Connexion rejetée immédiatement
- Les journaux du transporteur montrent une IP non autorisée

Solutions :

- Confirmez l'IP publique de votre passerelle :

  ```
  curl ifconfig.me
  ```

- Demandez au transporteur d'ajouter l'IP à la liste blanche
- Vérifiez que l'IP n'a pas changé (IP dynamique)

4. Pare-feu Bloquant

Vérifiez :

```
# Vérifiez si le port est ouvert
sudo iptables -L -n | grep 2775

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

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

Solutions :

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

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

La Connexion Continue de Se Couper

Symptômes :

- Connexion établie mais se déconnecte fréquemment
- La métrique `smpp_disconnection_total` augmente
- Les journaux montrent des reconnexions répétées

Causes Possibles & Solutions :

1. Instabilité Réseau

Vérifiez :

```
# Surveillez la perte de paquets
ping -c 100 smpp.carrier.com | grep loss

# Vérifiez les erreurs réseau
netstat -s | grep -i error
```

Solutions :

- Contactez le transporteur au sujet des problèmes de réseau
- Vérifiez avec votre FAI si c'est de votre côté
- Envisagez une connexion/routage de secours

2. Délai d'Attente de Lien de Demande

Vérifiez :

- Les journaux montrent "enquire_link timeout"
- La connexion se coupe après des périodes d'inactivité

Solutions :

- Le délai d'attente par défaut est de 30 secondes
- Vérifiez que le réseau permet les paquets keepalive
- Vérifiez les pare-feu agressifs qui expirent les connexions inactives

3. Limite TPS Dépassée

Vérifiez :

- Taux de message élevé au moment de la déconnexion
- Le transporteur limite les messages

Solutions :

- Examinez le paramètre `tps_limit`
- Réduisez le TPS à 70-80 % du maximum du transporteur
- Répartissez le trafic sur plusieurs liaisons

4. Problèmes de Serveur du Transporteur

Vérifiez :

- Vérifiez l'état du service du transporteur
- Contactez le support du transporteur

Solutions :

- Attendez que le transporteur résolve le problème
- Configurez un transporteur de secours si disponible

Problèmes de Livraison de Messages

Messages Non Envoyés

Symptômes :

- Messages bloqués dans la file d'attente
- `smpp_messages_sent_total` n'augmente pas

- La connexion montre qu'elle est connectée

Causes Possibles & Solutions :

1. Mauvais Routage dest_smsc

Vérifiez :

- Interface Web → Queue → Vérifiez le champ `dest_smsc` du message
- Comparez avec le nom de connexion dans SMPP → État en Direct

Solutions :

- Les messages sont routés en fonction du champ `dest_smsc`
- Vérifiez que le backend définit le bon `dest_smsc`
- Si `dest_smsc` est NULL, vérifiez le routage par défaut

2. Messages Planifiés pour le Futur

Vérifiez :

- Interface Web → Queue → Vérifiez le champ `deliver_after`
- Les messages avec un horodatage futur ne seront pas envoyés

Explication :

- Le système de réessai définit `deliver_after` pour les messages échoués
- Les messages attendent jusqu'à ce moment avant de réessayer

Solutions :

- Attendez l'heure prévue
- Si urgent, contactez l'équipe backend pour réinitialiser l'horodatage

3. Limite TPS Trop Basse

Vérifiez :

- Grande accumulation dans la file d'attente
- Messages envoyés très lentement

Solutions :

- Augmentez `tps_limit` dans la configuration
- Vérifiez que le transporteur peut gérer un taux plus élevé
- Voir CONFIGURATION.md

4. Le Worker de File d'Attente ne Fonctionne Pas

Vérifiez :

- État du service
- Journaux pour les erreurs

Solutions :

```
# Redémarrer le service
sudo systemctl restart omnimessage-smpp

# Vérifiez les journaux
sudo journalctl -u omnimessage-smpp -f
```

Taux d'Échec de Livraison Élevé

Symptômes :

- `smpp_delivery_failures_total` augmente
- Les journaux montrent "submit_sm_resp" avec un statut d'erreur
- Les messages n'atteignent pas les destinataires

Causes Possibles & Solutions :

1. Numéros de Destination Invalides

Vérifiez :

- Les journaux pour des codes d'erreur spécifiques
- Examinez le format de destination du message

Codes d'Erreur Courants :

- `0x0000000B` - Destination invalide
- `0x00000001` - Longueur de message invalide
- `0x00000003` - Commande invalide

Solutions :

- Validez le format du numéro (E.164 recommandé)
- Vérifiez que le numéro inclut le code pays
- Vérifiez les exigences du transporteur

2. Contenu du Message Invalide

Vérifiez :

- Longueur du message
- Caractères spéciaux
- Encodage

Solutions :

- GSM-7 : Max 160 caractères
- UCS-2 : Max 70 caractères
- Supprimez les caractères non pris en charge
- Vérifiez les paramètres d'encodage

3. Rejet du Transporteur

Vérifiez :

- Codes d'erreur spécifiques du transporteur
- Modèles dans les messages rejetés

Solutions :

- Contactez le transporteur pour connaître la raison du rejet
- Peut nécessiter un filtrage de contenu
- Vérifiez les modèles de spam/abus

4. Messages Expirés

Vérifiez :

- Horodatage `expires` du message
- Timing des tentatives de livraison

Solutions :

- Augmentez la période de validité des messages
- Réduisez le délai de réessai pour les messages sensibles au temps

---

Problèmes d'Interface Web

Impossible d'Accéder au Tableau de Bord Web

Symptômes :

- Le navigateur ne peut pas se connecter à https://your-server:8087
- Délai d'attente ou connexion refusée

Causes Possibles & Solutions :

1. Service Non Fonctionnel

Vérifiez :

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

Solutions :

```
# Si arrêté, démarrez-le
sudo systemctl start omnimessage-smpp

# Vérifiez les journaux pour les erreurs
sudo journalctl -u omnimessage-smpp -n 50
```

2. Pare-feu Bloquant le Port 8087

Vérifiez :

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

Solutions :

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

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

3. Problèmes de Certificat SSL

Vérifiez :

- Le navigateur montre un avertissement de sécurité
- Certificat expiré ou invalide

Solutions :

- Accepter l'exception de sécurité (si auto-signé)
- Installer un certificat SSL valide
- Vérifiez que les fichiers de certificat existent :

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

4. Mauvaise URL

Vérifiez :

- Vérifiez en utilisant HTTPS (pas HTTP)
- Vérifiez l'IP/nom d'hôte du serveur correct
- Vérifiez le port 8087

L'Interface Web Montre des Erreurs

Symptômes :

- La page se charge mais montre des erreurs
- Les fonctions ne fonctionnent pas
- Les données ne s'affichent pas

Solutions :

1. **Vider le Cache du Navigateur** :
    - Ctrl+F5 (rafraîchissement forcé)
    - Vider le cache et les cookies du navigateur
2. **Vérifiez la Console du Navigateur** :
    - Appuyez sur F12
    - Vérifiez l'onglet Console pour les erreurs JavaScript
    - Signalez au support si des erreurs sont trouvées
3. **Essayez un Navigateur Différent** :
    - Testez dans Chrome, Firefox, Edge
    - Isolez les problèmes spécifiques au navigateur
4. **Vérifiez les Journaux du Service** :

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

Problèmes de Métriques

Métriques Prometheus Non Disponibles

Symptômes :

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

- Prometheus ne peut pas récupérer les métriques
- Réponse vide ou erreur

Causes Possibles & Solutions :

1. Service Non Fonctionnel

Vérifiez :

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

Solutions :

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

2. Port Non Accessible

Vérifiez :

```
# Tester localement
curl http://localhost:4000/metrics

# Tester à distance
curl http://your-server-ip:4000/metrics
```

Solutions :

- Si local fonctionne mais distant ne fonctionne pas : Vérifiez le pare-feu
- Ouvrez le port 4000 dans le pare-feu pour le serveur Prometheus

3. Mauvais Point de Terminaison

Vérifiez :

- Le point de terminaison est `/metrics` (pas `/prometheus` ou `/stats`)
- Le port est 4000 (pas 8087)

Métriques Montrent des Valeurs Inattendues

Symptômes :

- Les compteurs se réinitialisent à zéro
- Les jauges montrent de mauvaises valeurs
- Métriques manquantes pour certaines liaisons

Solutions :

1. **Le Redémarrage du Service Réinitialise les Compteurs** :
    - Les compteurs se réinitialisent lors du redémarrage du service
    - C'est un comportement normal
    - Utilisez `increase()` ou `rate()` dans les requêtes Prometheus
2. **Nouvelles Liaisons Non Affichées** :
    - Les métriques n'apparaissent qu'après le premier événement
    - Envoyez un message de test pour peupler les métriques
    - Vérifiez que la liaison est activée et connectée
3. **Métriques Obsolètes** :
    - Les anciennes liaisons peuvent encore apparaître dans les métriques
    - Redémarrez le service pour effacer les entrées obsolètes
    - Ou utilisez le relabeling de Prometheus pour filtrer

Problèmes de Performance

Utilisation Élevée du CPU

Vérifiez :

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

Causes Possibles :

- Volume de messages très élevé
- Trop de connexions
- Problème de configuration

Solutions :

- Vérifiez que le taux de messages est dans la capacité
- Examinez les limites TPS
- Contactez le support si l'utilisation élevée du CPU persiste

Utilisation Élevée de la Mémoire

Vérifiez :

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

Causes Possibles :

- Grande file d'attente de messages en mémoire

- Fuite de mémoire (rare)

Solutions :

- Redémarrez le service pour libérer de la mémoire
- Vérifiez la taille de la file d'attente de messages
- Contactez le support si la mémoire augmente continuellement

Traitement des Messages Lent

Symptômes :

- Les messages prennent du temps à être envoyés
- Accumulation dans la file d'attente
- Faible taux de messages

Vérifiez :

1. Les limites TPS - peuvent être trop restrictives
2. `queue_check_frequency` - peut être trop élevé
3. Temps de réponse de l'API backend - peut être lent
4. Latence réseau vers le transporteur

Solutions :

- Augmentez le TPS si le transporteur le permet
- Diminuez `queue_check_frequency` pour un polling plus rapide
- Optimisez l'API backend
- Vérifiez la latence réseau

Problèmes de Configuration

Erreurs de Syntaxe dans le Fichier de Configuration

Symptômes :

- Le service ne démarre pas après un changement de configuration
- Les journaux montrent "syntax error" ou "parse error"

Vérifiez :

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

Erreurs Courantes :

- Virgule manquante entre les entrées de la carte
- Guillemets non appariés (" vs ')
- Crochets ou accolades non appariés
- Manque `import Config` en haut

Solutions :

- Restaurer à partir d'une sauvegarde
- Examiner soigneusement la syntaxe
- Utiliser un éditeur de texte avec la coloration syntaxique Elixir

Changements Non Prendre Effet

Symptômes :

- Configuration modifiée mais aucun changement de comportement
- Anciens paramètres toujours actifs

Solutions :

```
# Les changements de configuration nécessitent un redémarrage
sudo systemctl restart omnimessage-smpp

# Vérifiez que le redémarrage a réussi
sudo systemctl status omnimessage-smpp

# Vérifiez les journaux pour les erreurs
sudo journalctl -u omnimessage-smpp -n 50
```

Récupération d'Urgence

Échec Complet du Système

Étapes :

1. **Vérifiez la santé de base du système** :

   ```
   # Espace disque
   df -h

   # Mémoire
   free -h

   # Charge CPU
   uptime
   ```

2. **Vérifiez l'état du service** :

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

3. **Examinez les journaux récents** :

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

4. **Essayez de redémarrer le service** :

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

5. **Si le redémarrage échoue** :
    - Vérifiez la syntaxe de la configuration
    - Vérifiez que les certificats SSL existent
    - Vérifiez les permissions des fichiers
    - Examinez les journaux pour des erreurs spécifiques

6. **Restaurer à partir d'une sauvegarde** (si nécessaire) :

```
# Restaurer la configuration
sudo cp /opt/omnimessage-smpp/config/runtime.exs.backup \
  /opt/omnimessage-smpp/config/runtime.exs

# Redémarrer
sudo systemctl restart omnimessage-smpp
```

7. **Contactez le support** si non résolu

Obtenir de l'Aide

Informations à Collecter

Avant de contacter le support, collectez :

1. **Version** : `cat /opt/omnimessage-smpp/VERSION`
2. **Journaux Récents** :

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

3. **Configuration** (sanitize passwords) :

```
sudo cp /opt/omnimessage-smpp/config/runtime.exs /tmp/config.exs
# Éditez /tmp/config.exs pour supprimer les mots de passe avant
d'envoyer
```

4. **Sortie des Métriques** :

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

5. **Informations Système** :

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

Contacter le Support

- **Email** : support@omnitouch.com
- **Téléphone** : +61 XXXX XXXX (24/7)
- **Inclure** : Toutes les informations ci-dessus

Documentation Connexe

- **OPERATIONS.md** - Procédures opérationnelles normales
- **CONFIGURATION.md** - Référence de configuration
- **MONITORING.md** - Surveillance et métriques
- **README.md** - Vue d'ensemble du système
