Guide des Opérations du RAN Monitor

Plateforme de Surveillance et de Gestion du Réseau d'Accès Radio (RAN)

par Omnitouch Network Services

Table des Matières

1. Aperçu
2. Ce que fait RAN Monitor
3. Architecture du Système
4. Aperçu de l'Interface Web
5. Surveillance avec Grafana
6. Opérations Courantes
7. Index de Documentation
8. Référence Rapide
9. Support

Aperçu

RAN Monitor est une plateforme de gestion et de surveillance pour les stations de base Nokia AirScale dans les réseaux 3GPP LTE et 5G. Elle fournit une visibilité en temps réel sur la santé, la performance et la configuration de votre équipement RAN.

Caractéristiques Clés

- **Surveillance en Temps Réel** - Collecte continue des métriques de performance et des alarmes
- **Gestion Automatisée** - Maintient des connexions persistantes avec les stations de base
- **Analytique Historique** - Stocke des données pour l'analyse des tendances et la planification de capacité
- **Tableau de Bord Web** - Visibilité opérationnelle en temps réel via l'interface Web intégrée
- **Intégration Grafana** - Analytique avancée et tableaux de bord personnalisés

Composants du Système

Composant	But	Accès
Gestionnaire RAN Monitor	Application principale gérant les connexions des stations de base	Service en arrière-plan
Point de Terminaison NE3S Nokia	Récepteur de webhook PM/config/alarm de Nokia AirScale	http://<server>:9076
Point de Terminaison PM Casa	Récepteur de push PM de femtocell Casa (voir Collecte PM Casa)	http://<server>:9077
Point de Terminaison Push Flexi Zone	Récepteur de push PM/alarm de Classic Nokia Flexi Zone et API d'intégration (voir Collecte Flexi Zone)	http://<server>:9081
Poller Baicells	Interroge l'API `/fsmoam/` de Baicells eNB (voir Collecte Baicells)	sortant → cell :443
Collecteur OCUDU	Diffuse les métriques JSON OCUDU gNB depuis le WebSocket de contrôle à distance (voir Collecte OCUDU)	sortant → gNB :8001
Panneau de Contrôle de l'Interface Web	Tableau de bord opérationnel en temps réel	https://<server>:9443

Composant	But	Accès
Base de Données MySQL	État de session et configuration des dispositifs	Interne
InfluxDB	Stockage des métriques de séries temporelles	http://<server>:8086
Grafana	Tableaux de bord d'analytique et alertes	http://<server>:3000
Serveur TCE NSNTI	Collecte de traces des stations de base	Port TCP 49151
Transmetteur TCE TZSP	Exportation de traces en temps réel vers Wireshark	Port UDP 37008

Exemple : Tableau de Bord de Surveillance Détaillé

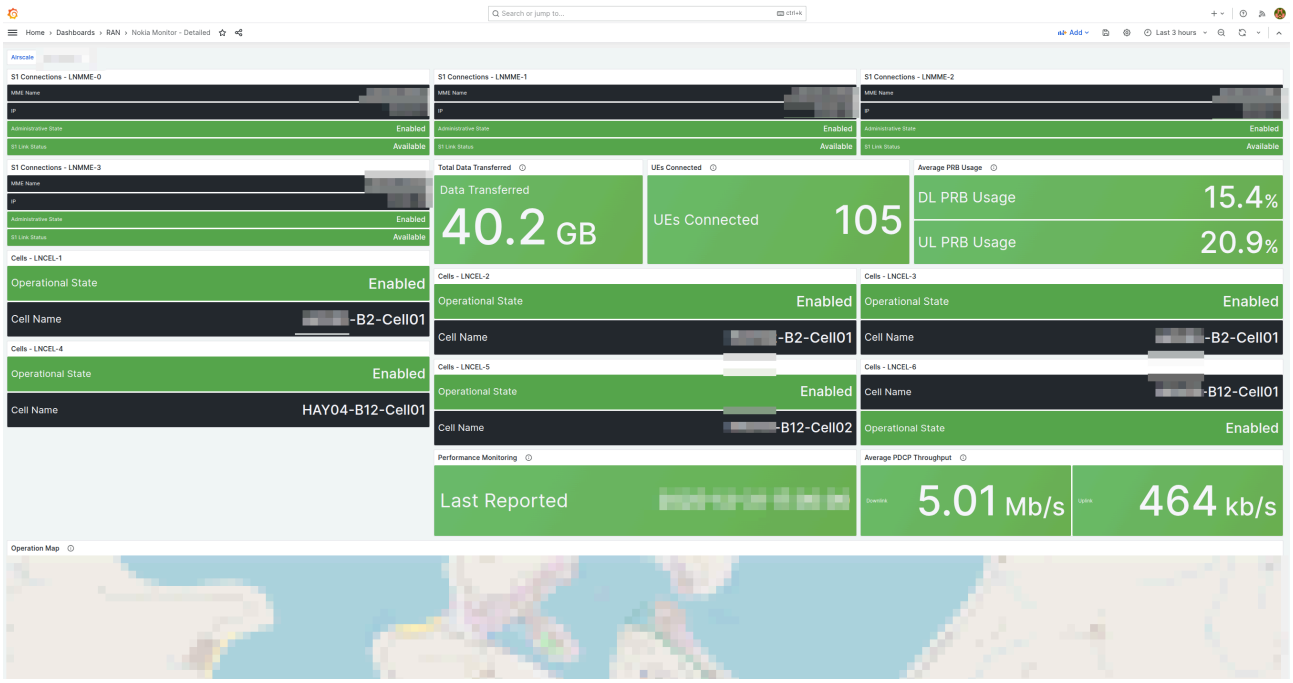


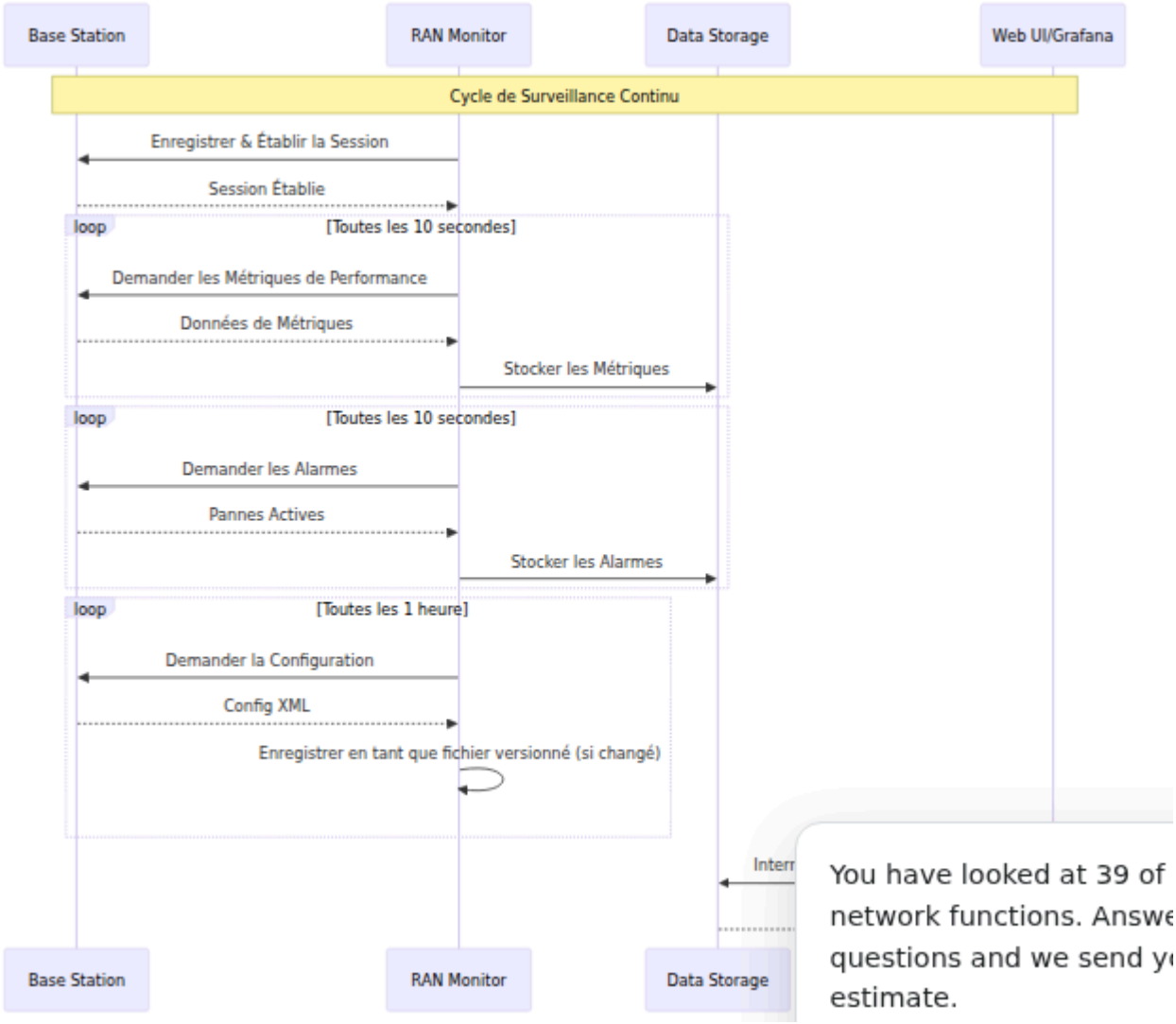
Tableau de bord de surveillance complet montrant l'état des connexions S1 par LNMME, l'état opérationnel, les données transférées, les UEs connectés, l'utilisation moyenne des PRB, les métriques de surveillance de performance, et la carte de couverture géographique. Ce tableau de bord fournit aux opérateurs de réseau une visibilité instantanée sur la santé des dispositifs, l'état de connectivité, et les indicateurs clés de performance.

Ce que fait RAN Monitor

RAN Monitor fonctionne en continu en arrière-plan pour :

1. **Enregistrer et Connecter** - Établit des connexions sécurisées avec vos stations de base Nokia
2. **Collecter des Données de Performance** - Rassemble les KPI toutes les 10 secondes (configurable)
3. **Surveiller les Alarmes** - Suit les pannes et leurs niveaux de gravité
4. **Suivre la Configuration** - Enregistre l'état du système et les changements de paramètres
5. **Stocker des Données Historiques** - Préserve les métriques dans une base de données de séries temporelles
6. **Fournir de la Visibilité** - Affiche l'état en temps réel via l'interface Web et Grafana

Flux de Données



Ce qui est Collecté

Métriques de Performance :

- Disponibilité et temps de fonctionnement de la cellule
- Débit de trafic (uplink/downlink)
- Utilisation des ressources (utilisation des PRB)
- Taux de réussite de mise en place d'appels
- Performance de transfert
- Mesures de qualité radio

Alarmes :

- Gravité des pannes (Critique, Majeur, Mineur, Avertissement)
- Systèmes et composants affectés
- Cause probable et descriptions
- Horodatages et durées

Configuration :

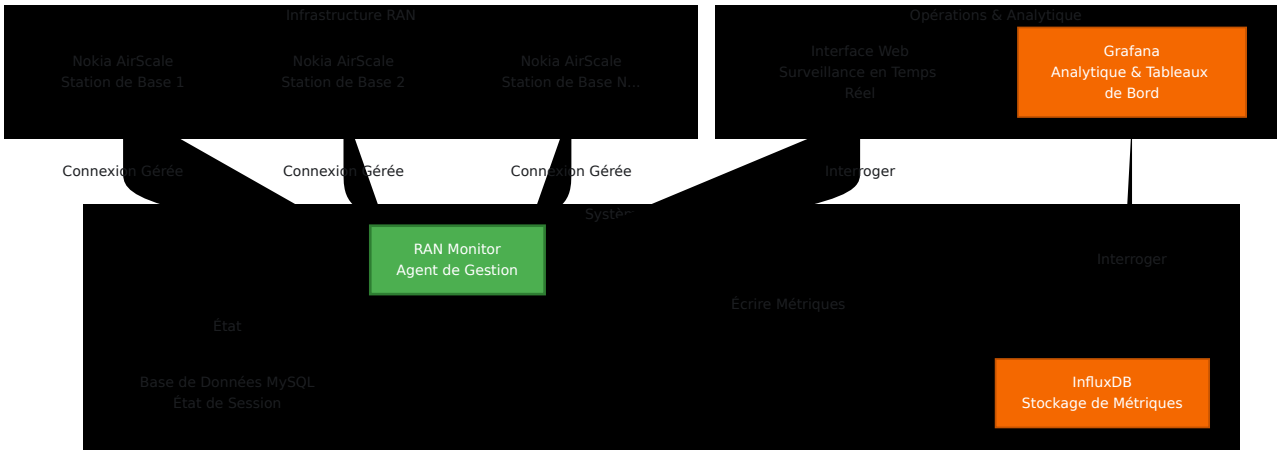
- Instantanés complets de la configuration XML (stockés en tant que fichiers versionnés)
- Détection automatique des changements et versionnage
- Historique de configuration et piste d'audit
- Dernières 10 versions conservées par dispositif

Pour des détails sur la gestion de la configuration, voir le Guide d'Archivage de Configuration.

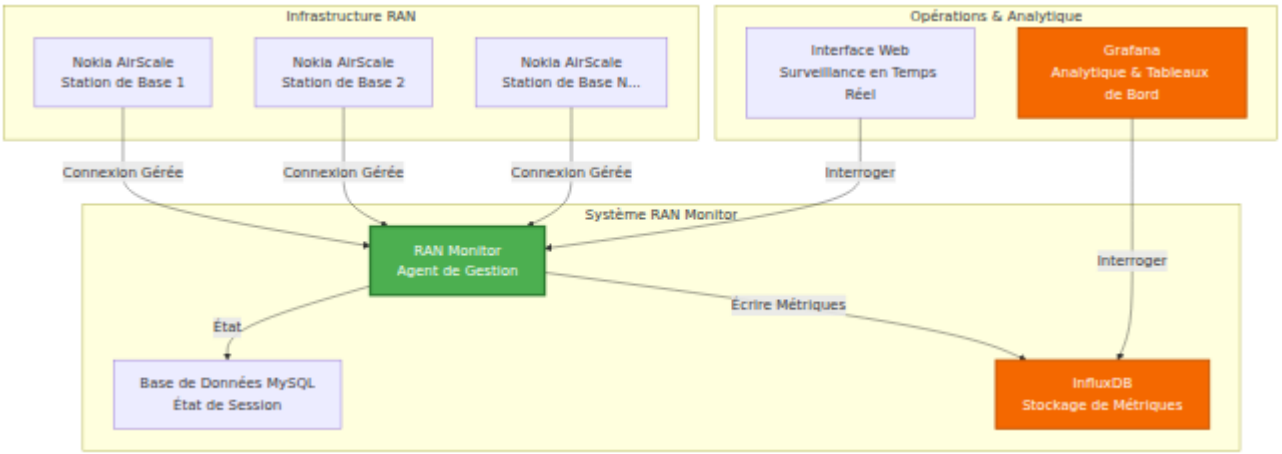
Pour des définitions détaillées des compteurs, voir le Référence des Compteurs Nokia.

Architecture du Système

Aperçu de l'Infrastructure



Aperçu de la Configuration



Pour des détails complets sur la configuration, voir le Guide de Configuration d'Exécution.

Entité de Collecte de Traces (TCE)

RAN Monitor inclut une Entité de Collecte de Traces intégrée pour capturer et analyser les messages de protocole LTE/5G. Cela permet un dépannage détaillé, des tests de conduite et une optimisation RF.

Qu'est-ce que TCE ?

L'Entité de Collecte de Traces reçoit des données de trace des stations de base Nokia AirScale contenant :

- **Messages S1-AP** - Signalisation du plan de contrôle entre eNodeB et EPC
- **Messages RRC** - Signalisation de Contrôle des Ressources Radio
- **Messages NAS** - Signalisation du Stratum Non-Accès
- **Données du Plan Utilisateur** - Informations sur le débit de la couche PDCP

Cas d'Utilisation

Tests de Conduite :

- Capturer l'expérience RF de l'utilisateur final
- Analyser la performance des transferts
- Mesurer la qualité du signal (RSRP, RSRQ, SINR)
- Identifier les trous de couverture

Dépannage :

- Déboguer les échecs de mise en place d'appels
- Analyser les problèmes de transfert
- Enquêter sur les appels abandonnés
- Examiner les événements de mobilité

Optimisation RF :

- Validation de la planification PCI
- Optimisation des relations voisines
- Réglage des paramètres de transfert
- Analyse de la couverture et de la capacité

Pour des procédures complètes de collecte de traces et d'analyse Wireshark, voir le **Guide de Collecte de Données TCE MDT**.

Aperçu de l'Interface Web

RAN Monitor inclut une interface Web intégrée pour la surveillance et la gestion opérationnelles en temps réel.

Accès : `https://<ran-monitor-ip>:9443`

Le tableau de bord principal fournit une visibilité instantanée sur la santé du système, l'état des dispositifs et les alarmes actives.

Pages Clés

Tableau de Bord Principal

Aperçu en temps réel du système avec :

- Indicateurs de santé du système
- Résumé de l'état des dispositifs (comptes associés/échoués)
- Comptes d'alarmes actives par gravité
- Activités et événements récents

Se rafraîchit automatiquement toutes les 5 secondes pour une visibilité en temps réel.

Page des Stations de Base

Voir tous les dispositifs gérés avec leur état actuel :

- État de connexion (vert = associé, rouge = échoué)
- État d'enregistrement et informations de session
- Horodatage du dernier contact
- Capacités de filtrage, de recherche et de tri

Cliquez sur n'importe quel dispositif pour voir des informations détaillées, y compris les détails d'enregistrement, le cycle de vie de la session, les métriques récentes et les alarmes actives.

Page des Alarmes

Surveillez toutes les pannes à travers votre réseau :

- Codé par couleur selon la gravité (Rouge = Critique, Orange = Majeur, Jaune = Mineur, Bleu = Avertissement, Vert = Résolu)
- Détails des alarmes, cause probable, système affecté
- Suivi des horodatages et des durées
- Tri par gravité et capacités de filtrage

Pour les procédures de gestion des alarmes, voir le Guide de Gestion des Alarmes.

Gestion de la Configuration

Gérez en toute sécurité les configurations des stations de base :

1. **Télécharger** la configuration actuelle (sauvegarde)
2. **Télécharger** une nouvelle configuration → recevoir l'ID de Plan
3. **Valider** la configuration en utilisant l'ID de Plan
4. **Activer** la configuration validée
5. **Vérifier** que les changements ont pris effet

Toujours valider avant d'activer pour éviter les interruptions de service.

Archivage de Configuration : Tous les changements de configuration sont automatiquement suivis et versionnés. Voir les configurations historiques, télécharger des versions précédentes, ou comparer les changements via la page d'Archivage de Configuration.

Pour des procédures détaillées, voir le Guide de l'Interface Web - Gestion de la Configuration et le Guide d'Archivage de Configuration.

- **Guide de Poussée de Configuration** - Pousser des changements de configuration complets ou partiels aux stations de base (impact de redémarrage, mises à jour partielles, format SCF)

---

eNodeBs Non Configurés

Découvrez les stations de base tentant de se connecter qui ne sont pas encore configurées :

- ID d'Agent (utilisé lors de l'ajout à la configuration)
- Horodatage du dernier aperçu
- Nombre de tentatives de connexion
- Actions : Actualiser, Supprimer, Effacer Tout

Cas d'Utilisation : Lorsque de nouvelles stations de base sont déployées, elles apparaissent ici. Copiez l'ID d'Agent et ajoutez-les à `config/runtime.exs`.

Journaux d'Application

Tableau de bord de journalisation en temps réel pour le dépannage :

- Filtrer par niveau de journal (Urgent à Débogage)
- Rechercher à travers tous les messages
- Mettre en pause/Reprendre le streaming en direct
- Changer dynamiquement le niveau de journal système
- Codé par couleur selon la gravité

Pour des procédures de dépannage, voir le Guide de Dépannage.

Politique de Conservation des Données

Gérez combien de temps les données sont stockées dans InfluxDB :

- Voir la politique de conservation globale et le nombre total d'enregistrements
- Définir des périodes de conservation par dispositif
- Voir le nombre d'enregistrements par type de mesure (Métriques de Performance, Configuration, Alarmes)
- Déclencher manuellement le nettoyage ou effacer toutes les données pour un dispositif

Pour des informations complètes sur la conservation des données, voir le Guide de Politique de Conservation des Données.

Statut InfluxDB

Surveillez la santé de la base de données de séries temporelles :

- Indicateur d'état de connexion
- Comptes de mesures par type
- Informations de stockage
- Version et configuration de la base de données
- Se rafraîchit automatiquement toutes les 5 minutes

Interprétation du Statut :

- Connecté + Comptes en Croissance = Fonctionnement Normal
- Connecté + Pas de Données = Vérifiez l'enregistrement du dispositif
- Déconnecté = Vérifiez la connectivité InfluxDB

Guide Complet de l'Interface Web

Pour une documentation complète de l'interface Web incluant toutes les fonctionnalités, flux de travail et meilleures pratiques, voir :

Guide de l'Interface Web - Référence complète du panneau de contrôle

---

Surveillance avec Grafana

Bien que l'interface Web fournisse une visibilité en temps réel, Grafana permet une analyse historique approfondie et des tableaux de bord personnalisés.

Pourquoi Utiliser Grafana ?

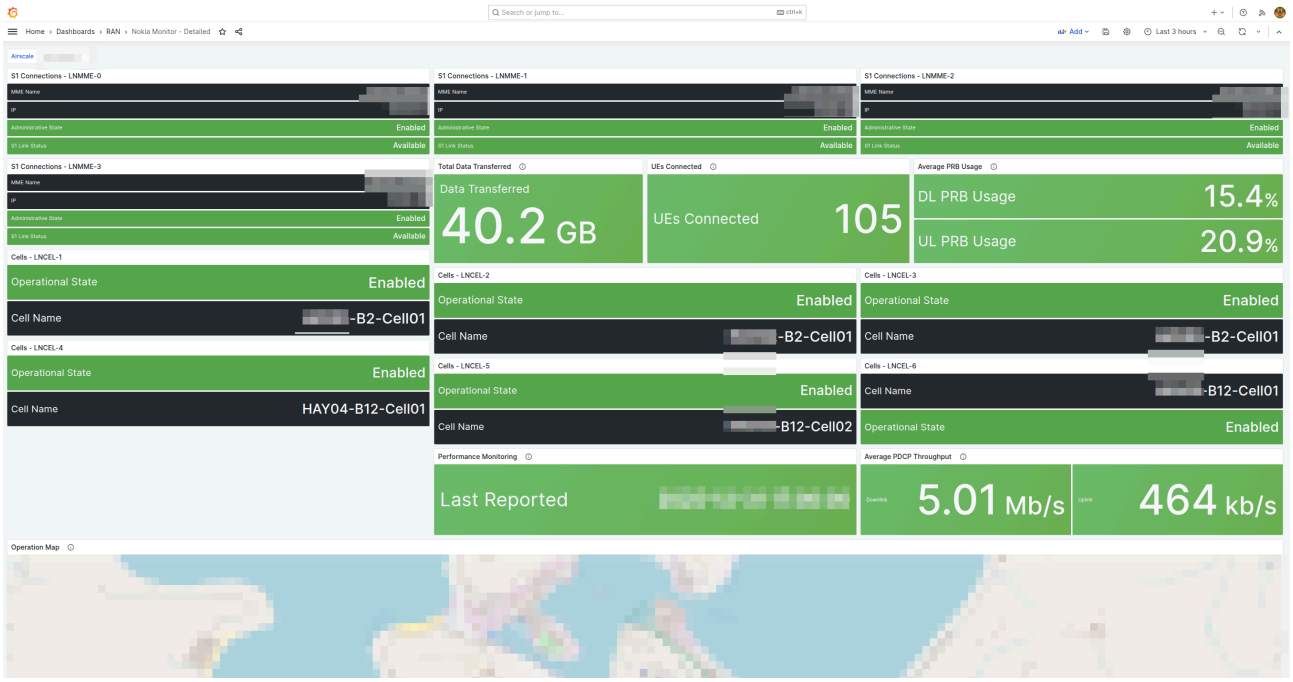
Grafana est Idéal Pour :

- Analyse des tendances historiques sur des jours/semaine/mois
- Tableaux de bord KPI personnalisés adaptés à vos besoins

- Planification de capacité à long terme
- Identification de motifs et détection d'anomalies
- Reporting exécutif et suivi des SLA
- Alertes avancées avec canaux de notification

L'Interface Web est Idéale Pour :

- Vérifications immédiates de l'état des dispositifs
- Surveillance des alarmes en temps réel
- Gestion de la configuration
- Dépannage de session
- Tâches d'administration système



Exemple de tableau de bord Grafana montrant la disponibilité des cellules, les tendances de débit et l'utilisation des ressources

Types de Tableaux de Bord

Tableau de Bord Résumé Exécutif :

- Vue d'ensemble de la santé du réseau
- Nombre total d'alarmes par gravité
- Disponibilité moyenne des cellules à travers tous les sites

- Métriques agrégées de débit et de capacité
- Grille d'état des dispositifs

Tableau de Bord des Opérations NOC :

- Tableau des problèmes actifs en temps réel
- Jauges d'utilisation des ressources
- Vue d'ensemble du trafic (dernières 24 heures)
- Graphiques de tendance des alarmes
- Vue rapide de l'état des dispositifs

Tableau de Bord d'Ingénierie Approfondie :

- Analyse des motifs de trafic
- Métriques de qualité de cellule (distributions SINR, RSRP)
- Performance radio (retransmission RLC, succès de mise en place RRC)
- Piste d'audit de configuration
- Analyse de corrélation

Tableau de Bord de Performance Nokia AirScale :

- Utilisation des PRB (DL/UL)
- Tendances de débit (couche PDCP)
- Comptes d'UE actifs
- Calculs de disponibilité des cellules
- Répartition des ressources par cellule
- Mesures RSSI
- Succès de mise en place de connexion RRC
- VSWR par antenne
- Consommation d'énergie

Pour des exemples complets de tableaux de bord, des modèles de requêtes et des définitions de compteurs, voir :

Guide d'Intégration Grafana - Guide complet d'analytique et de tableaux de bord

Référence des Compteurs Nokia - Définitions des compteurs de performance

---

Opérations Courantes

Opérations Quotidiennes

Vérification de Santé Quotidienne (5-10 minutes) :

1. Ouvrir le tableau de bord de l'interface Web
2. Vérifier que tous les dispositifs affichent un statut vert
3. Vérifier le nombre et la gravité des alarmes
4. Examiner les dispositifs échoués
5. Enquêter sur les problèmes si nécessaire

Pour des procédures détaillées, voir le Guide de l'Interface Web - Flux de Travail.

Enquête sur les Alarmes :

1. Ouvrir la page des Alarmes, trier par gravité
2. Cliquer sur l'alarme pour des détails complets
3. Naviguer vers le dispositif affecté
4. Croiser avec les métriques
5. Déterminer l'action requise et résoudre

Pour les procédures de gestion des alarmes, voir le Guide de Gestion des Alarmes.

Gestion des Dispositifs

Ajout d'une Nouvelle Station de Base :

1. Vérifier la connectivité réseau au dispositif

2. Vérifier la page des eNodeBs Non Configurés pour le dispositif
3. Ajouter le dispositif à `config/runtime.exs`
4. Redémarrer RAN Monitor
5. Vérifier que l'enregistrement réussit (statut vert)
6. Confirmer que les métriques affluent vers InfluxDB

Suppression d'une Station de Base :

1. Décider de conserver ou de supprimer les données historiques
2. Commenter ou supprimer le dispositif de `config/runtime.exs`
3. Optionnellement effacer les données via la page de Conservation des Données
4. Redémarrer RAN Monitor
5. Mettre à jour les tableaux de bord Grafana

Mise à Jour des Identifiants de Dispositif :

1. Noter l'état actuel du dispositif
2. Mettre à jour les identifiants dans `config/runtime.exs`
3. Redémarrer RAN Monitor
4. Vérifier que la reconnexion réussit

Pour des procédures opérationnelles complètes, voir :

Guide des Opérations Courantes - Tâches de gestion quotidiennes

Gestion de la Configuration

Flux de Travail de Mise à Jour de Configuration Sûre :

1. **Télécharger** la configuration actuelle (sauvegarde) - ou récupérer depuis l'Archivage de Configuration
2. **Modifier** la configuration hors ligne
3. **Télécharger** sur le dispositif → obtenir l'ID de Plan
4. **Valider** en utilisant l'ID de Plan → vérifier qu'il n'y a pas d'erreurs
5. **Activer** si la validation réussit
6. **Vérifier** que les changements ont pris effet
7. **Surveiller** la stabilité du dispositif pendant 15-30 minutes
8. **Confirmer** que la nouvelle version apparaît dans l'Archivage de Configuration (dans l'heure)

Important : Toujours valider avant d'activer. Planifiez les changements pendant les fenêtres de maintenance lorsque cela est possible.

Rétrogradation de Configuration : Si des problèmes surviennent, téléchargez une version précédente depuis l'Archivage de Configuration et

téléchargez-la en utilisant le même flux de travail.

Pour des détails sur la configuration des stations de base, voir le Guide de Configuration AirScale.

Pour l'historique de configuration et le versionnage, voir le Guide d'Archivage de Configuration.

Index de Documentation

La documentation de RAN Monitor est organisée par public et cas d'utilisation :

Pour les Équipes d'Opérations (NOC, Administrateurs)

Document	But	Quand l'utiliser
Guide de l'Interface Web	Référence complète du panneau de contrôle	Opérations quotidiennes, surveillance des dispositifs
Guide des Opérations Courantes	Tâches de gestion quotidiennes	Ajout de dispositifs, gestion des configs, sauvegardes
Guide d'Archivage de Configuration	Versionnage et historique de configuration	Suivi des changements de configuration, rétrogradation, audit
Guide de Gestion de Firmware	Répertoire de paquets logiciels	Téléchargement de firmware, mises à jour logicielles des stations de base
Guide de Gestion des Alarmes	Gestion et escalade des alarmes	Enquête sur les pannes, réponse aux alertes
Guide de Dépannage	Procédures de résolution de problèmes	Lorsque des problèmes surviennent, diagnostic des erreurs
Guide de Politique de Conservation des Données	Gestion du cycle de vie des données	Gestion du stockage, définition des périodes de conservation

Pour l'Ingénierie et l'Analytique

Document	But	Quand l'utiliser
Guide d'Intégration Grafana	Tableaux de bord, requêtes et alertes	Création de tableaux de bord, configuration des alertes
Référence des Métriques	Métriques Prometheus exposées par RAN Monitor (noms, types, étiquettes)	Alertes, tableaux de bord, surveillance de la santé de l'application
Référence des Compteurs Nokia	Définitions des compteurs de performance	Compréhension des métriques, création de requêtes
Guide de Configuration AirScale	Configuration et mise en place des stations de base	Configuration des dispositifs, compréhension des paramètres
Guide de Commissionnement DHCP	Intégration des stations de base via DHCP	Commissionnement de nouvelles stations de base via l'Option DHCP 43
Collecte Flexi Zone	Collecte PM/alarm classique de Nokia Flexi Zone et intégration API	Intégration et surveillance des stations de base Flexi Zone classiques
Collecte OCUDU	Métriques en direct des gNB 5G OCUDU via le WebSocket de contrôle à distance	Surveillance des gNB OCUDU, cellules et UEs

Document	But	Quand l'utiliser
Guide de Collecte de Données TCE MDT	Collecte de traces MDT et analyse Wireshark	Collecte de données de test de conduite, optimisation de la couverture
Référence des Points de Terminaison API	Documentation de l'API REST	Intégrations, automatisation, scripting

Pour la Configuration et le Déploiement

Document	Objectif	Quand l'utiliser
Guide de Configuration Runtime	Référence complète de configuration	Configuration initiale, modification des paramètres

Démarrage Rapide

Nouveau sur RAN Monitor ?

1. Commencez par le Guide de l'Interface Web pour apprendre l'interface
2. Consultez le Guide des Opérations Courantes pour les tâches routinières
3. Étudiez le Guide de Gestion des Alarmes pour la gestion des alarmes
4. Gardez le Guide de Dépannage en favori pour les problèmes

Configurer la Surveillance ?

1. Consultez le Guide d'Intégration Grafana pour les tableaux de bord
2. Référez-vous au Référentiel de Compteurs Nokia pour les métriques
3. Consultez le Guide de Politique de Conservation des Données pour la gestion du stockage

---

Référence Rapide

Points d'Accès

Service	URL	Objectif
Tableau de Bord de l'Interface Web	`https://<server>:9443`	Surveillance et gestion en temps réel
Grafana	`http://<server>:3000`	Tableaux de bord d'analytique et alertes
InfluxDB	`http://<server>:8086`	Base de données des métriques (généralement accès interne uniquement)

Chemins Importants

Chemin	Objectif
`config/runtime.exs`	Fichier de configuration principal (appareils, bases de données, paramètres)
`priv/cert/`	Certificats SSL pour l'Interface Web HTTPS
`priv/external/nokia/`	Clés d'authentification du gestionnaire
`priv/airscale_configs/`	Archive de configuration (fichiers XML versionnés)

Concepts Clés

Gestion des Sessions :

- RAN Monitor établit des sessions avec les stations de base
- Les sessions ont des temps d'expiration et nécessitent un keep-alive
- La réinscription se fait automatiquement (par défaut : toutes les 30 secondes)
- L'état de la session est stocké dans la base de données MySQL

Flux de Données :

- Les métriques sont collectées toutes les 10 secondes (configurable)
- Les alarmes sont collectées toutes les 10 secondes via polling + webhooks en temps réel
- Des instantanés de configuration sont pris toutes les 1 heure (sauvegardés en tant que fichiers versionnés lorsqu'ils sont modifiés)
- Les métriques de performance et les alarmes sont écrites dans InfluxDB pour un stockage historique

Conservation des Données :

- Par défaut global : 720 heures (30 jours)
- Remplacements par appareil disponibles
- Nettoyage automatique exécuté toutes les heures
- Nettoyage manuel disponible via l'Interface Web

Pour des détails de configuration, consultez le Guide de Configuration Runtime.

Flux de Travail Courants

Vérification de Santé Quotidienne :

1. Ouvrir l'Interface Web → Tableau de Bord
2. Vérifier l'état des appareils (tout est vert ?)
3. Examiner le nombre d'alarmes
4. Enquêter sur les problèmes éventuels

Répondre à une Alarme Critique :

1. Interface Web → Alarmes → Trier par gravité

2. Cliquez sur l'alarme pour plus de détails
3. Naviguer vers l'appareil
4. Examiner les métriques récentes et les modifications de configuration
5. Mettre en œuvre la résolution
6. Vérifier que l'alarme est effacée

Ajouter un Nouvel Appareil :

1. Vérifier la connectivité réseau
2. Modifier `config/runtime.exs`
3. Ajouter l'appareil à la liste des airscales
4. Redémarrer RAN Monitor
5. Vérifier l'enregistrement (état vert)

Support

Ressources de Dépannage

Ressource	Utiliser Pour
Guide de Dépannage	Problèmes courants et solutions
Page des Journaux d'Application	Journaux système en temps réel et erreurs
Vue Détails de l'Appareil	État de la session, problèmes d'enregistrement
Page d'État InfluxDB	Vérification de la collecte de données

Étapes de Diagnostic Rapides

Appareil Ne Se Connecte Pas :

1. Vérifier la page des Stations de Base → état de l'appareil
2. Vérifier la connectivité réseau : `ping <device-ip>`
3. Vérifier les identifiants dans `config/runtime.exs`
4. Examiner les Journaux d'Application pour les erreurs

Pas de Métriques dans Grafana :

1. Vérifier que l'appareil est associé (état vert)
2. Vérifier que la page d'État InfluxDB montre des comptes croissants
3. Tester la connectivité InfluxDB
4. Vérifier la configuration de la source de données Grafana

L'Interface Web Ne Charge Pas :

1. Vérifier que le port 9443 est accessible
2. Vérifier que le pare-feu autorise le trafic HTTPS
3. Vérifier que les certificats SSL existent
4. Examiner les journaux d'application pour les erreurs de démarrage de l'Interface Web

Pour des procédures de dépannage complètes, consultez le Guide de Dépannage.

Obtenir de l'Aide

Avant de Contacter le Support :

Rassemblez ces informations :

- Description du problème et quand il a commencé
- Messages d'erreur des Journaux d'Application
- Appareils affectés (noms/IPs)
- Modifications récentes de la configuration
- Version de RAN Monitor et OS

Contact :

Pour obtenir de l'aide avec RAN Monitor :

- Support Omnitouch Network Services
- Inclure les informations de diagnostic rassemblées
- Fournir les fichiers de configuration (sanitiser les mots de passe)
- Inclure des extraits de journaux pertinents

Service Autonome :

1. Rechercher dans le Guide de Dépannage
2. Vérifier les Journaux d'Application pour des erreurs spécifiques
3. Examiner les modifications récentes de la configuration
4. Tester la connectivité et la fonctionnalité de base
5. Consulter les guides de documentation pertinents

Carte de Documentation



Guide de Configuration Nokia AirScale

Configuration des Stations de Base pour l'Intégration du Moniteur RAN

Table des Matières

1. Aperçu
2. Prérequis
3. Accéder à l'Interface WebLM
4. Configurer la Surveillance de Performance
5. Référence des Paramètres de Configuration
6. Vérification
7. Dépannage

Aperçu

Pour permettre au Moniteur RAN de collecter des métriques de performance, des alarmes et des données de configuration des stations de base Nokia AirScale, vous devez configurer la station de base pour qu'elle rapporte des données au système Moniteur RAN. Cela se fait via l'interface Nokia Web Element Manager (WebLM).

Ce guide décrit le processus de configuration de l'objet géré Performance Measurement Common Administration (PMCADM), qui contrôle la manière dont la station de base envoie des données de performance aux systèmes externes.

Qui Devrait Utiliser Ce Guide

Important : Toute configuration de station de base Nokia AirScale est **effectuée par Omnitouch** dans le cadre du déploiement initial et du support continu. Ce guide est fourni pour :

- **Utilisateurs avancés** qui souhaitent comprendre la configuration de la station de base
- **Déploiements autogérés** où les clients configurent leurs propres stations de base
- **Dépannage** et compréhension de la configuration actuelle
- **Intégration de stations de base supplémentaires** dans des environnements autogérés

Si vous êtes un client géré par Omnitouch, contactez le support Omnitouch pour la configuration et l'intégration de la station de base.

Pour comprendre les métriques collectées, voir Référence des Compteurs Nokia. Pour la configuration du système, voir Guide de Configuration Runtime.

Prérequis

Avant de configurer la station de base, assurez-vous d'avoir :

- **Accès Réseau** - Connectivité à l'interface de gestion de la station de base
- **Identifiants Administrateur** - Nom d'utilisateur et mot de passe avec privilèges de configuration
- **Détails du Moniteur RAN** - Adresse IP et port où le Moniteur RAN écoute
- **Logiciel Supporté** - Version de logiciel de station de base Nokia AirScale compatible

Informations Requises :

Paramètre	Valeur	Exemple
Adresse IP du Moniteur RAN	IP où le Moniteur RAN fonctionne	10.179.2.139
Port du Moniteur RAN	Port de collecte (par défaut : 9076)	9076
Intervalle de Collecte	Fréquence d'envoi des métriques	60 secondes

---

Accéder à l'Interface WebLM

Étape 1 : Ouvrir le Gestionnaire d'Éléments Web

1. Ouvrez un navigateur web
2. Accédez à l'interface de gestion de la station de base :

   ```
   http://<adresse-ip-station-de-base>/
   ```

   ou

   ```
   https://<adresse-ip-station-de-base>/
   ```

3. Connectez-vous avec vos identifiants administrateur

Étape 2 : Naviguer vers la Gestion de Configuration

Une fois connecté :

1. Cliquez sur **Configuration** dans la barre de menu supérieure
2. Sélectionnez **Gestion de Configuration** dans le menu déroulant
3. Cliquez sur l'onglet **Éditeur de Paramètres**

Vous devriez maintenant voir l'arbre de configuration dans le panneau de gauche et l'éditeur de paramètres dans la fenêtre principale.

Configurer la Surveillance de Performance

Étape 1 : Désactiver OAM TLS

Important : Avant de configurer la surveillance de performance, vous devez désactiver l'application OAM TLS sur la station de base. Par défaut, l'objet géré `oamTls` est défini sur `forced`, ce qui empêche la communication non chiffrée avec les systèmes de gestion externes.

Dans le panneau de navigation gauche (Arbre des objets) :

1. Développez **Configuration BTS Actuelle**
2. Développez **CURRENT_BTS_CONF-1**
3. Développez **MRBTS-X** (où X est l'ID de votre station de base)
4. Localisez l'objet géré **oamTls**
5. Changez la valeur de `forced` à `off`

Paramètre	Valeur par Défaut	Valeur Requise
oamTls	forced	off

Remarque : Ce paramètre doit être modifié avant que le Moniteur RAN puisse établir une communication avec la station de base. S'il reste à la valeur par défaut `forced`, la station de base rejettera les connexions non TLS.

Étape 2 : Localiser l'Objet Géré PMCADM

Dans le panneau de navigation gauche (Arbre des objets) :

1. Développez **Configuration BTS Actuelle**
2. Développez **CURRENT_BTS_CONF-1**
3. Développez **MRBTS-X** (où X est l'ID de votre station de base)
4. Développez **MNL-1** (Lien de Gestion)
5. Développez **MNLENT-1** (Entité de Lien de Gestion)
6. Cliquez sur **PMCADM-1** (Administration Commune de Mesure de Performance)

L'éditeur de paramètres affichera les paramètres de configuration de PMCADM-1.

Étape 3 : Configurer la Surveillance de Performance en Temps Réel

Faites défiler vers le bas jusqu'à la section **Structure 1**, qui contient les paramètres de l'entité de collecte de surveillance de performance en temps réel. Configurez les paramètres suivants :

Paramètres Requis :

Paramètre	Description	Valeur Recommandée
Type de certificat pour l'authentification TLS	Type de certificat de sécurité	RSA (si TLS activé)
Hôte de l'entité de collecte de surveillance de performance en temps réel	Adresse IP du Moniteur RAN	Votre IP Moniteur RAN (ex : 10.179.2.139)
Numéro de Port de l'Entité de Collecte de Surveillance de Performance en Temps Réel	Port où le Moniteur RAN écoute	9076 (par défaut)
Intervalle de Collecte de Surveillance de Performance en Temps Réel	Fréquence d'envoi des métriques	60s (ajuster selon les besoins)
Activer TLS	Utiliser une connexion chiffrée	false (pour la configuration initiale)

Paramètres Optionnels :

Paramètre	Description	Valeur par Défaut
Nombre maximum de fichiers à télécharger SDL	Max téléchargements simultanés	1
Nonce SDL	Identifiant unique pour la sécurité	12345678
Activer la suppression des compteurs de valeur zéro	Supprimer les compteurs avec valeur 0	false (recommandé de garder toutes les données)

Étape 4 : Enregistrer et Activer la Configuration

Après avoir configuré tous les paramètres :

1. **Vérifiez vos modifications** - Vérifiez que toutes les adresses IP et ports sont corrects
2. **Créez un plan de configuration :**
    - Cliquez sur le bouton **Créer un Plan** en haut
    - Le système validera vos modifications
    - Notez l'ID du Plan fourni
3. **Validez le plan :**
    - Cliquez sur le bouton **Valider le Plan**
    - Entrez l'ID du Plan
    - Attendez que la validation soit terminée
    - Résolvez les erreurs de validation
4. **Activez la configuration :**
    - Cliquez sur le bouton **Activer le Plan**

- Entrez l'ID du Plan
- Confirmez l'activation
- La station de base appliquera la nouvelle configuration

Alternative : Configuration XML

Pour les utilisateurs avancés ou les déploiements automatisés, la configuration PMCADM peut être appliquée à l'aide de XML. Voici le fragment de configuration qui correspond à la configuration manuelle ci-dessus :

```
<managedObject class="com.nokia.srbts.mnl:PMCADM" distName="MRBTS-132/MNL-1/MNLENT-1/PMCADM-1" version="MNL25R1_2420_110" operation="create">
  <p name="act3gppXmlEnrichment">false</p>
  <p name="reportingIntervalPm">5min</p>
  <p name="sdlMaxUploadFileNumber">1</p>
  <p name="sdlPrimaryDestIp">10.179.2.139</p>
  <list name="rTPmCollEntity">
    <item>
      <p name="certTypeForTlsAuth">RSA</p>
      <p name="rTPmCollEntityHost">10.179.2.139</p>
      <p name="rTPmCollEntityPortNum">9076</p>
      <p name="rTPmCollInterval">60s</p>
      <p name="tlsEnabled">false</p>
    </item>
  </list>
</managedObject>
```

Paramètres Clés dans XML :

- `rTPmCollEntityHost` - Défini sur l'adresse IP de votre Moniteur RAN
- `rTPmCollEntityPortNum` - Défini sur 9076 (port webhook par défaut)
- `rTPmCollInterval` - Intervalle de collecte (60s recommandé)
- `tlsEnabled` - Défini sur false pour la configuration initiale
- `sdlPrimaryDestIp` - Défini sur l'adresse IP de votre Moniteur RAN

Remarque : Remplacez `10.179.2.139` par votre adresse IP Moniteur RAN réelle et ajustez `MRBTS-132` pour correspondre à l'ID de votre station de base.

Référence des Paramètres de Configuration

Paramètres de Mesure de Performance LNBTS

L'objet géré LNBTS (LTE NodeB) contient des paramètres qui contrôlent quels groupes de mesure de performance sont collectés. Ces paramètres doivent être activés pour collecter certaines catégories de compteurs PM.

actL1PM - Activer les Mesures de Performance de Couche 1

Réglage	Valeur
Paramètre	actL1PM
Emplacement	Objet géré NOKLTE:LNBTS
Type	Booléen (true/false)
Par Défaut	false
Requis pour	Compteurs RTWP (M8005C306-339)

Description : Active les mesures de performance de la couche 1 (couche physique) y compris RTWP (Received Total Wideband Power) par antenne. Lorsqu'il est désactivé, la station de base ne rapportera pas RTWP, l'interférence et d'autres mesures radio de bas niveau.

Compteurs Affectés :

- M8005C306-309 : AVG_RTWP_RX_ANT_1 à AVG_RTWP_RX_ANT_4
- M8005C310-313 : AVG_RTWP_RX_ANT_5 à AVG_RTWP_RX_ANT_8
- M8005C314 : MAX_RTWP
- M8005C317-325 : UL_IOT_PUSCH bins de distribution

- M8005C326-335 : AVG_SIR bins de distribution

Configuration via XML :

```
<managedObject class="NOKLTE:LNBTS" distName="MRBTS-XXXX/LNBTS-
XXXX" operation="update">
  <p name="actL1PM">true</p>
</managedObject>
```

Configuration via WebLM :

1. Naviguez vers Configuration > Gestion de Configuration > Éditeur de Paramètres
2. Développez MRBTS-X > LNBTS-X
3. Localisez le paramètre `actL1PM`
4. Définissez la valeur sur `true`
5. Créez, validez et activez le plan de configuration

actPCMDReport - Activer le Reporting des Données de Mesure par Appel

Réglage	Valeur
Paramètre	actPCMDReport
Emplacement	Objet géré NOKLTE:LNBTS
Type	Booléen (true/false)
Par Défaut	false
Requis pour	Données de mesure par appel

Description : Active le reporting des Données de Mesure par Appel (PCMD), qui fournit des mesures détaillées pour des sessions d'appel individuelles.

Configuration via XML :

```
<managedObject class="NOKLTE:LNBTS" distName="MRBTS-XXXX/LNBTS-
XXXX" operation="update">
  <p name="actPCMDReport">true</p>
</managedObject>
```

Vue d'Ensemble de l'Objet PMCADM-1

L'objet géré PMCADM (Administration Commune de Mesure de Performance) contrôle comment les données de performance sont collectées et rapportées depuis la station de base.

Responsabilités Clés :

- Configurer les destinations de surveillance de performance en temps réel
- Définir les intervalles de collecte pour le reporting des métriques
- Contrôler le format des données et les paramètres de transmission
- Gérer les paramètres de sécurité pour la transmission des données

Paramètres Clés de PMCADM

reportingIntervalPm - Intervalle de Reporting PM

Réglage	Valeur
Paramètre	reportingIntervalPm
Emplacement	Objet géré com.nokia.srbts.mnl:PMCADM
Type	Énumération
Options	5min, 15min, 30min, 60min
Recommandé	5min ou 15min pour la surveillance en temps réel

Description : Contrôle la fréquence à laquelle la station de base télécharge les données de mesure de performance. Des valeurs plus basses fournissent des données plus granulaires mais augmentent le trafic réseau et les exigences de stockage.

Impact sur la Collecte de Données :

- **5min** - Meilleur pour la surveillance en temps réel et le dépannage
- **15min** - Bon équilibre entre granularité et utilisation des ressources
- **60min** - Convient uniquement pour le suivi à long terme

Configuration via XML :

```
<managedObject class="com.nokia.srbts.mnl:PMCADM" distName="MRBTS-XXXX/MNL-1/MNLENT-1/PMCADM-1" operation="update">
  <p name="reportingIntervalPm">5min</p>
</managedObject>
```

Configuration via WebLM :

1. Naviguez vers Configuration > Gestion de Configuration > Éditeur de Paramètres
2. Développez MRBTS-X > MNL-1 > MNLENT-1 > PMCADM-1
3. Localisez le paramètre `reportingIntervalPm`
4. Définissez la valeur sur l'intervalle désiré (ex : `5min`)
5. Créez, validez et activez le plan de configuration

Entité de Collecte de Surveillance de Performance en Temps Réel

Cette sous-structure définit où et comment la station de base envoie des métriques de performance en temps réel.

certTypeForTlsAuth - Type de Certificat pour l'Authentification TLS

- **Type :** Énumération (RSA, DSA, ECDSA)

- **But :** Spécifie le type de certificat lorsque TLS est activé
- **Par Défaut :** RSA
- **Utilisation :** Seulement pertinent lorsque tlsEnabled = true

rTpmCollEntityHost - Hôte de l'Entité de Collecte

- **Type :** Adresse IP (IPv4 ou IPv6)
- **But :** Adresse IP de destination pour les métriques de performance
- **Requis :** Oui
- **Exemple :** 10.179.2.139
- **Remarques :** Doit être accessible depuis le réseau de gestion de la station de base

rTpmCollEntityPortNum - Numéro de Port de l'Entité de Collecte

- **Type :** Entier (1-65535)
- **But :** Port TCP où le système de collecte écoute
- **Par Défaut :** 9076
- **Remarques :** Doit correspondre à la configuration du Moniteur RAN

rTpmCollInterval - Intervalle de Collecte

- **Type :** Temps (secondes)
- **But :** Fréquence de transmission des données de performance
- **Options :** 15s, 30s, 60s, 300s, 900s, 1800s
- **Par Défaut :** 60s
- **Recommandation :** 60s pour la surveillance standard, 15s pour un dépannage détaillé

tlsEnabled - Activer TLS

- **Type :** Booléen (true/false)
- **But :** Chiffrer les données de performance en transit
- **Par Défaut :** false
- **Remarques :** Nécessite des certificats valides des deux côtés si activé

sdlMaxUploadFileNumber - Nombre Maximum de Fichiers à Télécharger SDL

- **Type :** Entier
- **But :** Nombre maximum de téléchargements de fichiers simultanés
- **Par Défaut :** 1
- **Remarques :** Augmenter pour des environnements à fort volume

sdlNonce - Nonce SDL

- **Type :** Chaîne (8 chiffres)
- **But :** Identifiant unique pour la sécurité du protocole SDL
- **Par Défaut :** 12345678
- **Remarques :** Peut être changé pour des raisons de sécurité

suppressZeroValueCount - Supprimer les Compteurs de Valeur Zéro

- **Type :** Booléen (true/false)
- **But :** Omettre les compteurs avec des valeurs zéro des rapports
- **Par Défaut :** false
- **Recommandation :** Garder false pour maintenir des données complètes pour le suivi

---

Vérification

Après avoir activé la configuration, vérifiez que la station de base envoie correctement des données au Moniteur RAN.

Vérifier l'Interface Web du Moniteur RAN

1. Ouvrez l'interface Web du Moniteur RAN : `http://<adresse-ip-moniteur-ran>:4000/`
2. Naviguez vers la page **État BTS**
3. Localisez votre station de base dans la liste des appareils

4. Vérifiez que le statut indique **Connecté** (indicateur vert) — cela signifie que le site a une session active ET a envoyé à la fois la configuration et les données PM
5. Si le statut indique **En Attente de Données PM**, la session est active mais le site n'a pas encore envoyé de métriques de performance (attendez le prochain cycle PM de 15 minutes)

Statut Attendu :

- **Statut :** Connecté (vert)
- **Session :** Active
- **Adresse :** Correspond à l'adresse IP de la station de base
- **Actions :** Tous les boutons activés

Si le Statut Indique En Attente :

L'appareil tente de s'enregistrer mais n'a pas terminé l'authentification.

Causes possibles :

- Mismatch entre l'ID du gestionnaire et la clé d'enregistrement
- Moniteur RAN non configuré pour accepter cet appareil
- Problèmes de connectivité réseau

Si le Statut Indique Erreur de Connexion :

L'appareil ne peut pas atteindre le Moniteur RAN.

Causes possibles :

- Adresse IP incorrecte dans la configuration PMCADM
- Problèmes de routage réseau
- Pare-feu bloquant le port 8080
- Service Moniteur RAN non en cours d'exécution

Vérifier la Collecte de Données

Voir l'État InfluxDB :

1. Dans l'interface Web du Moniteur RAN, naviguez vers **État InfluxDB**
2. Vérifiez que le nombre de points de données augmente
3. Vérifiez que le compte des **Métriques de Performance** augmente
4. Confirmez que l'horodatage de la **Dernière Mise à Jour** est récent

Métriques Attenues :

- **Métriques de Performance :** Compte augmentant régulièrement
- **Configuration :** Points de données présents
- **Alarmes :** Peut être 0 si aucune faute active

Vérifier la Rétention des Données :

1. Naviguez vers la page **Politique de Rétention des Données**
2. Localisez votre station de base
3. Vérifiez les comptes de **Métriques de Performance**, **Configuration**, et **Alarmes**

Dépannage

Station de Base Non Apparente dans le Moniteur RAN

Symptôme : L'appareil n'apparaît pas dans la page ��tat BTS

Solutions :

1. **Vérifiez la connectivité réseau :**

```
ping <adresse-ip-station-de-base>
```

2. **Vérifiez la configuration du Moniteur RAN :**
   - Assurez-vous que l'appareil est ajouté à `config/runtime.exs`
   - Vérifiez que l'adresse IP correspond à celle de la station de base
   - Confirmez que les identifiants sont corrects
3. **Consultez les journaux du Moniteur RAN :**
   - Naviguez vers la page **Journaux en Direct**
   - Filtrez pour les messages d'erreur
   - Recherchez des tentatives de connexion de la station de base
4. **Vérifiez la configuration de la station de base :**
   - Vérifiez à nouveau les paramètres PMCADM-1 dans WebLM
   - Confirmez que l'adresse IP du Moniteur RAN est correcte
   - Assurez-vous que le port 9076 est spécifié

L'Appareil Montre un Statut "En Attente"

Symptôme : L'appareil apparaît mais le statut est jaune "En Attente"

Solutions :

1. **Vérifiez l'enregistrement du gestionnaire :**
   - Vérifiez que l'ID du gestionnaire dans le Moniteur RAN correspond à l'attente de la station de base
   - Confirmez que les clés d'enregistrement sont correctement configurées
2. **Vérifiez l'authentification :**
   - Vérifiez les identifiants dans runtime.exs
   - Assurez-vous que le nom d'utilisateur/mot de passe correspondent aux paramètres de la station de base

3. **Attendez le cycle d'enregistrement :**
    - L'enregistrement peut prendre 30-60 secondes
    - Rafraîchissez la page après avoir attendu

Erreurs de Connexion

Symptôme : "Erreur réseau : enetunreach" ou similaire

Solutions :

1. **Vérifiez le chemin réseau :**
    - Testez la connectivité de la station de base au Moniteur RAN
    - Vérifiez les tables de routage
    - Assurez-vous que les VLANs/sous-réseaux sont correctement configurés
2. **Vérifiez les règles de pare-feu :**
    - Assurez-vous que le port 9076 est ouvert (pour les données de performance en temps réel)
    - Assurez-vous que le port 8080 est ouvert (pour la communication API SOAP)
    - Vérifiez qu'aucun ACL ne bloque le trafic
    - Vérifiez les règles iptables sur le serveur Moniteur RAN
3. **Vérifiez que le Moniteur RAN écoute :**

```
# Vérifiez les deux points de terminaison API SOAP et webhook
netstat -tlnp | grep -E '8080|9076'
```

Compteurs RTWP ou de Couche 1 Manquants

Symptôme : La station de base rapporte des données mais les compteurs RTWP (M8005C306-339) sont manquants dans InfluxDB

Cause : Le paramètre `actL1PM` est défini sur `false` dans la configuration LNBTS, ce qui désactive les mesures de performance de la couche 1.

Solution :

1. **Vérifiez le paramètre actuel :**
    - Exportez la configuration de la station de base
    - Recherchez `actL1PM` dans la section LNBTS
    - Si la valeur est `false`, c'est la cause
2. **Activez la PM de Couche 1 :**
    - Accédez à WebLM sur la station de base
    - Naviguez vers MRBTS-X > LNBTS-X
    - Définissez `actL1PM` sur `true`
    - Créez, validez et activez le plan de configuration
3. **Vérifiez après activation :**
    - Attendez le prochain intervalle de collecte (généralement 60 secondes)
    - Vérifiez InfluxDB pour les compteurs M8005C306-309
    - Les données RTWP devraient maintenant apparaître

Paramètres Connexes :

- `actPCMDReport` - Données de Mesure par Appel (peut également devoir être activé)

Aucune Métrique dans InfluxDB

Symptôme : L'appareil est connecté mais aucune donnée dans la base de données

Solutions :

1. **Vérifiez l'intervalle de collecte :**
    - Vérifiez le paramètre rTpmCollInterval de PMCADM-1
    - Attendez au moins une période d'intervalle complète
    - Rafraîchissez la page d'État InfluxDB

2. **Vérifiez la connexion InfluxDB :**
    - Naviguez vers la page d'État InfluxDB
    - Vérifiez que l'indicateur "Connecté" est vert
    - Confirmez que le nom du bucket est correct
3. **Consultez les journaux du Moniteur RAN :**
    - Recherchez des erreurs d'écriture InfluxDB
    - Vérifiez les problèmes de parsing des données
    - Vérifiez que le token API a les permissions d'écriture

Problèmes TLS/Certificat

Symptôme : La connexion échoue lorsque TLS est activé

Solutions :

1. **Vérifiez que les certificats sont installés :**
    - Vérifiez que la station de base a un certificat valide
    - Assurez-vous que le Moniteur RAN a le certificat CA correspondant
2. **Essayez d'abord sans TLS :**
    - Définissez tlsEnabled = false
    - Vérifiez que la connectivité de base fonctionne
    - Réactivez TLS après avoir confirmé la fonctionnalité
3. **Vérifiez la validité des certificats :**
    - Vérifiez que les certificats ne sont pas expirés
    - Confirmez que les noms de sujet des certificats correspondent
    - Vérifiez que la chaîne de certificats est complète

Ressources Supplémentaires

Documentation Connexe

- Guide d'Opérations - Documentation complète des opérations du Moniteur RAN
- Guide de Configuration Runtime - Référence de configuration du Moniteur RAN
- Référence des Compteurs Nokia - Définitions des compteurs de performance
- Intégration Grafana - Création de tableaux de bord avec les métriques collectées
- Points de Terminaison API - Référence API REST pour la gestion des appareils
- Politique de Rétention des Données - Gestion des données de performance stockées

Fichiers de Configuration

- **config/runtime.exs** - Configuration des appareils du Moniteur RAN

Support

Pour les problèmes non couverts dans ce guide :

1. Consultez les journaux d'application du Moniteur RAN
2. Vérifiez la documentation de la station de base Nokia pour votre version de logiciel
3. Vérifiez la configuration de l'infrastructure réseau
4. Consultez l'équipe des opérations réseau

Gestion des Alarmes & Escalade

Gestion des Pannes, Niveaux de Sévérité et Réponse Opérationnelle

Guide pour gérer les alarmes, enquêter sur les pannes et escalader les problèmes

---

Table des Matières

1. Aperçu
2. Cycle de Vie des Alarmes
3. Niveaux de Sévérité
4. Catégories d'Alarme
5. Enquête & Dépannage
6. Procédures d'Escalade
7. Suivi des Résolutions
8. Meilleures Pratiques

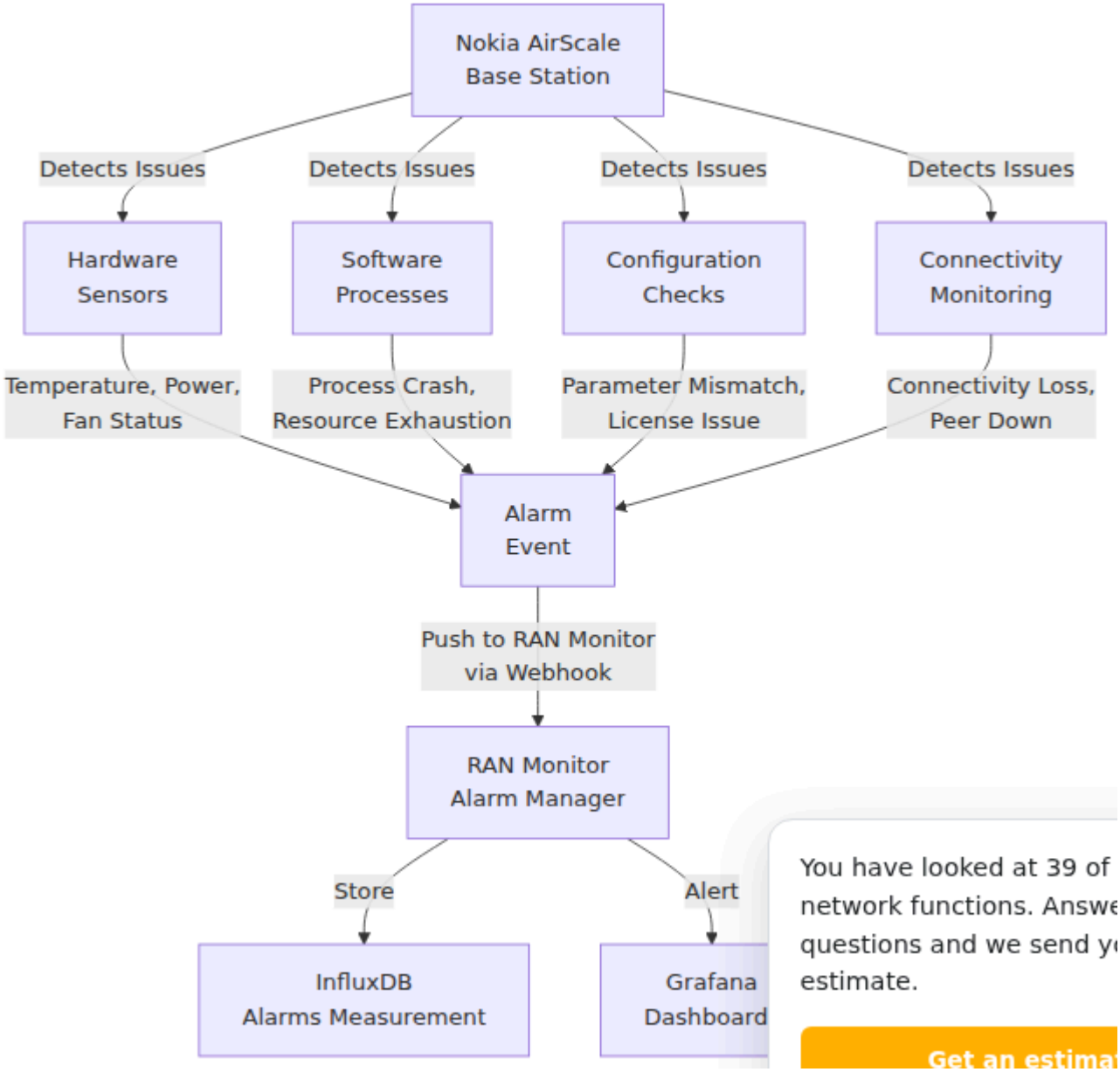
Aperçu

Les alarmes (également appelées "pannes") représentent des problèmes ou des anomalies détectés sur les stations de base Nokia AirScale. RAN Monitor surveille en continu les alarmes actives et suit leur cycle de vie depuis leur génération jusqu'à leur résolution.

Exemple de Tableau de Bord des Alarmes :

Exemple montrant l'état 4G avec un tableau d'aperçu des alarmes affichant l'état des alarmes (actif/effacé), les niveaux de sévérité (critique/avertissement), les horodatages et les descriptions des alarmes pour les pannes d'interface optique.

Sources d'Alarme



You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima

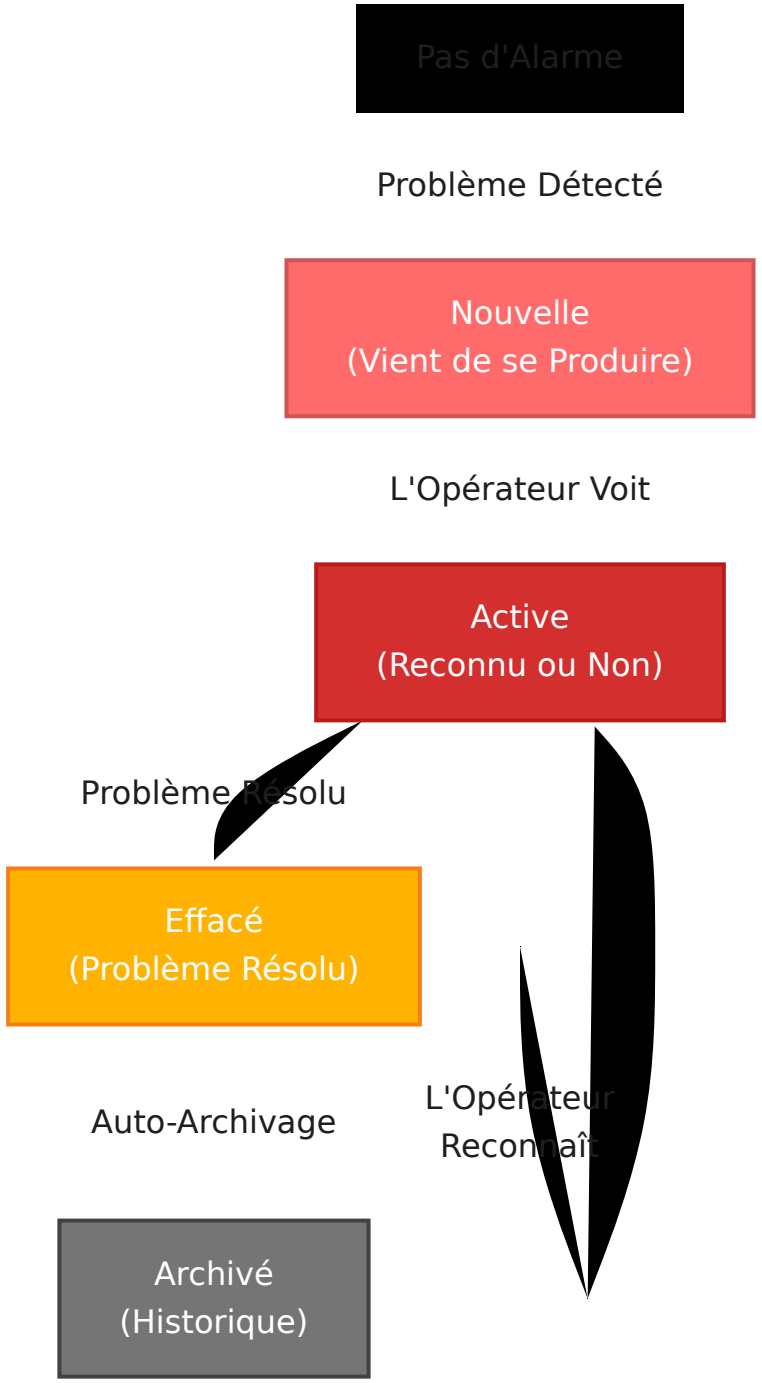
Attributs Clés des Alarmes

Chaque alarme contient :

Attribut	Exemple	Objectif
ID d'Alarme	a1b2c3d4-e5f6-...	Identifiant unique
Sévérité	Critique, Majeur, Mineur	Niveau de priorité
Cause Probable	"Cellule Indisponible"	Catégorie de cause racine
Problème Spécifique	"Connexion S1 Perdue"	Problème détaillé
Système Affecté	/BSC-1/BTS-23/Cell-A	Ce qui est impacté (DN)
Heure de l'Événement	2025-12-10 14:23:45	Quand détecté
Statut	Actif / Effacé	État actuel

Cycle de Vie des Alarmes

Transitions d'État



Exemple de Chronologie des Alarmes

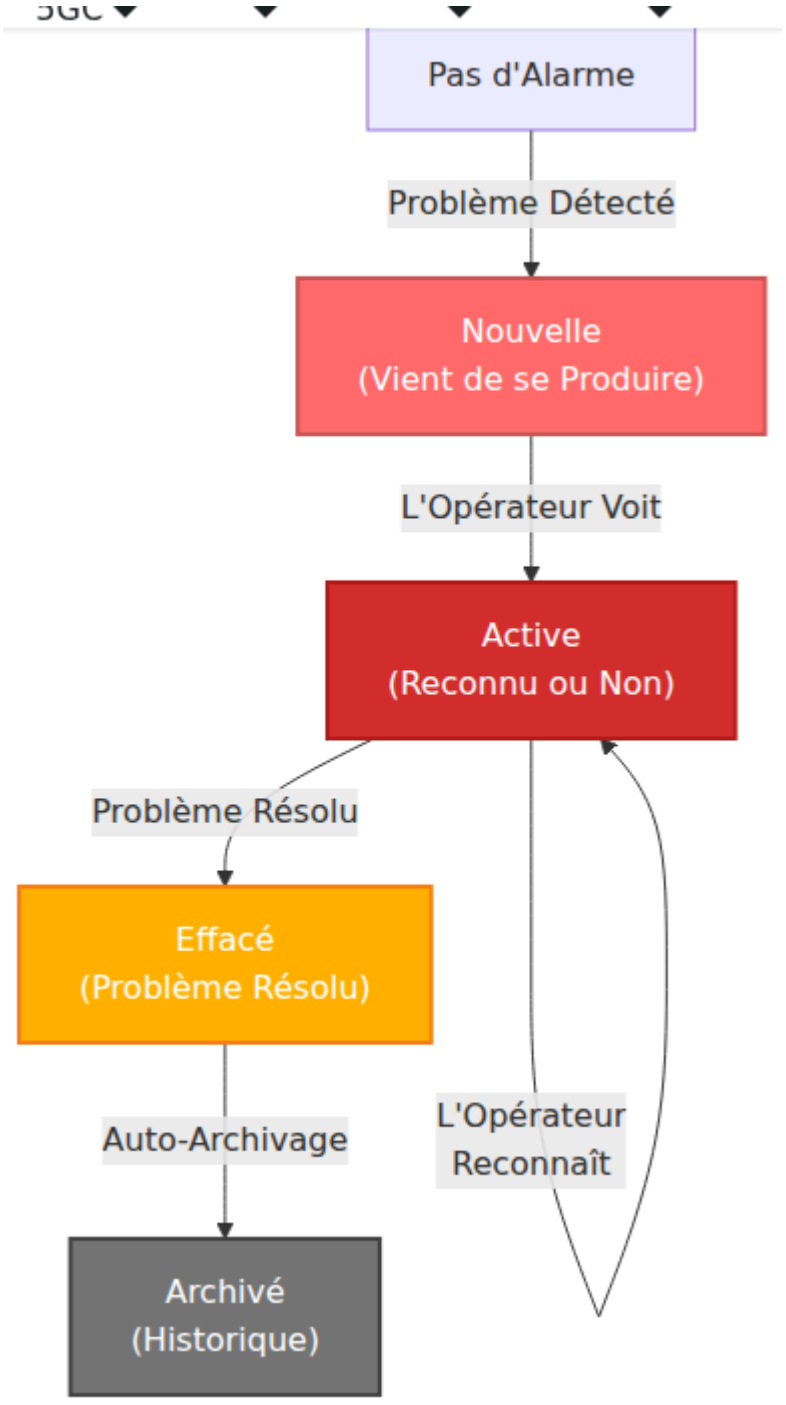
```
14:23:45 UTC - Problème Se Produit
            └─> La station de base détecte une perte de
connectivité
            └─> Génère une alarme : "Connexion S1 Perdue"
(Critique)

14:23:47 UTC - Alarme Transmise au RAN Monitor
            └─> Notification webhook NE3S reçue
            └─> Stockée dans InfluxDB
            └─> Règle d'alerte déclenchée

14:23:50 UTC - Notification Envoyée
            └─> Alerte Grafana déclenchée
            └─> Message Slack à l'équipe NOC
            └─> Incident PagerDuty créé

14:24:15 UTC - L'Opérateur Reconnaît
            └─> L'équipe NOC marque comme reconnu
            └─> Suivi de la durée commence

14:28:35 UTC - Problème Se Résout Automatiquement
            └─> Connectivité restaurée
            └─> La station de base efface l'alarme
            └─> RAN Monitor enregistre "Effacé"

14:28:36 UTC - Alarme Fermée
            └─> Durée enregistrée : 5 minutes 51 secondes
            └─> Suivi pour le reporting SLA
            └─> Archivée après 30 jours
```

Niveaux de Sévérité

RAN Monitor suit cinq niveaux de sévérité, chacun ayant un impact opérationnel différent et des exigences d'escalade :

Sévérité Critique

Définition : Impact sur le service, nécessite une action immédiate



Exemples :

- Appareil complètement injoignable (perte de connectivité)
- Toutes les cellules hors service (panne de bande de base)
- Interface de plan de contrôle hors service (S1 perdu)
- Échec complet du transfert de données

- Station de base ne répondant pas à la gestion

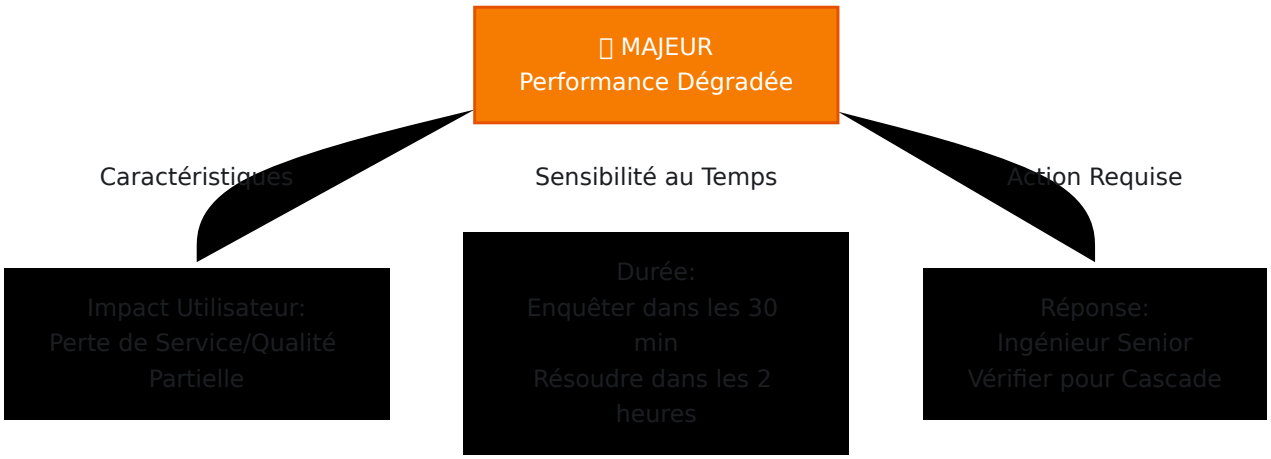
Escalade :

- Notifier immédiatement l'ingénieur de garde (appel téléphonique)
- Créer un incident dans le système de gestion des incidents
- Mettre à jour la page de statut
- Informer la direction si SLA affecté

SLA de Réponse : < 15 minutes

Sévérité Majeure

Définition : Performance dégradée, nécessite une enquête urgente



Exemples :

- Disponibilité de la cellule < 95 % pendant > 15 minutes
- Taux de réussite de transfert < 95 %
- Ressources DL/UL bloquées (> 95 % d'utilisation soutenue)
- Taux de retransmission RLC > 5 %
- Plusieurs cellules montrant une mauvaise qualité
- Dégradation de lien (erreurs E1/T1 en augmentation)

Escalade :

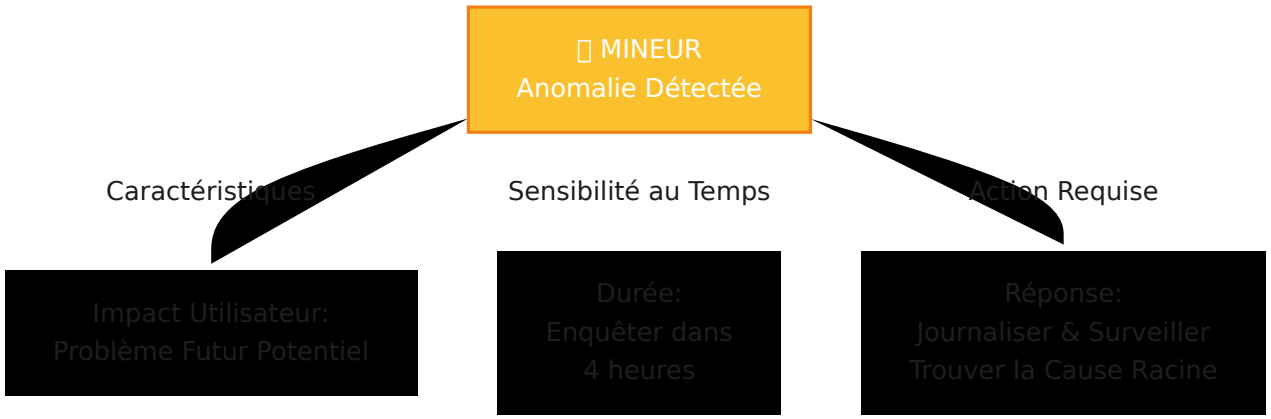
- Notifier l'équipe NOC + ingénieur senior
- Créer un incident dans la gestion des incidents

- Pager l'équipe d'ingénierie si toujours ouvert après 30 minutes
- Vérifier les problèmes en cascade vers d'autres cellules/sites

SLA de Réponse : < 30 minutes d'enquête

Sévérité Mineure

Définition : Dégradation, suivre et enquêter



Exemples :

- Disponibilité de la cellule 95-98 % (tendance à la baisse)
- Avertissement de température élevée sur l'amplificateur
- Capacité de licence approchant la limite
- Problèmes de cohérence de configuration
- Performance lente sur l'interface de gestion
- Alarmes intermittentes (< 5 occurrences/heure)

Escalade :

- Journaliser dans le tableau de bord pour sensibilisation
- Assigner à l'ingénierie pour enquête
- Planifier pour la prochaine fenêtre de maintenance si nécessaire
- Créer un ticket pour analyse de tendance

SLA de Réponse : Revue le même jour

Sévérité Avertissement

Définition : Informatif, surveiller les tendances

Exemples :

- Disponibilité de la cellule > 98 % mais tendance à la baisse
- Température/power dans la plage normale mais élevée
- Ressources à 60-70 % d'utilisation
- Mismatch de configuration (paramètres non critiques)
- Première occurrence d'un nouveau type de panne

Escalade :

- Visibilité dans le tableau de bord uniquement
- Pas de notifications automatiques
- Revue manuelle sur cadence

Effacé

Définition : Alarme précédemment active maintenant résolue

Objectif :

- Documente que le problème a été résolu
- Suit le temps moyen de réparation (MTTR)
- Permet le reporting de conformité SLA
- Identifie les problèmes récurrents

Catégories d'Alarme

Alarmes de Connectivité

```
Catégorie : Connectivité Externe
Causes Probables :
  - Connexion S1 Perdue       → MME/SGW injoignable
  - Lien de Retour Hors Service → Échec du transport IP
  - Erreur d'Interface USIM     → Problème de connectivité HSS
  - Synchronisation NTP Perdue → Problème de réseau de
synchronisation horaire

Impact : Interruption de service, échecs de configuration d'appel
Enquête :
  1. Vérifier la connectivité réseau entre les appareils
  2. Vérifier que les règles de pare-feu permettent les protocoles
requis
  3. Vérifier l'état et les erreurs de l'appareil pair
  4. Réviser les statistiques de l'interface réseau
```

Alarmes Matérielles & Environnementales

```
Catégorie : Infrastructure Physique
Causes Probables :
  - Avertissement de Haute Température  → Système de
refroidissement dégradé
  - Alimentation Électrique Dégradée     → Problème d'UPS/PSU
  - Panne de Ventilateur                → Dysfonctionnement du
ventilateur de refroidissement
  - Espace Disque Faible                 → Stockage approchant la
limite
  - Épuisement de Mémoire                → Fuite de mémoire de
processus

Impact : Pannes en cascade potentielles, perte de données
Enquête :
  1. Vérifier l'état matériel via l'interface de gestion
  2. Réviser les tendances de température
  3. Vérifier le fonctionnement du système de refroidissement
  4. Surveiller l'utilisation de la mémoire et du CPU
```

Alarmes Logicielles & de Processus

```
Catégorie : Couche d'Application
Causes Probables :
  - Panne de Processus            → Erreur logicielle ou OOM
  - Haute Utilisation du CPU     → Goulot d'étranglement de
performance
  - Surcharge de File d'Attente   → Arriéré de traitement des
messages
  - Violation de Licence          → Capacité dépassée

Impact : Dégradation ou interruption du service
Enquête :
  1. Vérifier l'état du processus
  2. Réviser les journaux pour les messages d'erreur
  3. Surveiller l'utilisation du CPU/mémoire/profondeur de file
d'attente
  4. Vérifier l'état de la licence
```

Alarmes de Ressources Radio

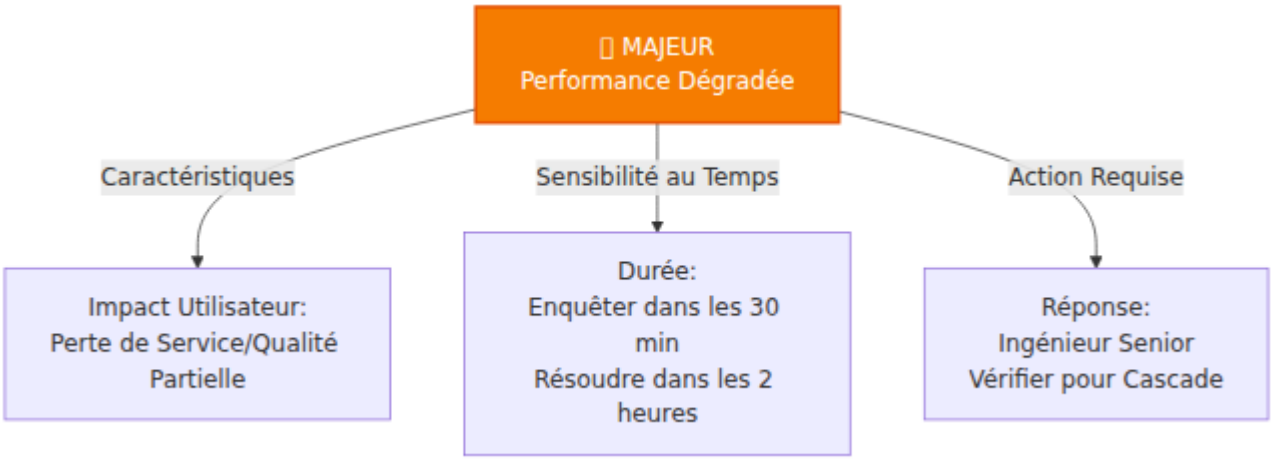
```
Catégorie : Interface Radio
Causes Probables :
  - Cellule Indisponible         → Pas de couverture/power radio
  - Ressource DL Bloquée      → Épuisement de capacité
  - Taux d'Échec de Transfert Élevé → Problème de configuration de
voisin
  - Mauvaise Qualité de Cellule        → Interférence RF ou perte
de chemin

Impact : Dégradation de l'expérience utilisateur
Enquête :
  1. Vérifier les paramètres physiques de la cellule
  2. Réviser la configuration de la cellule voisine
  3. Analyser les métriques de qualité RF
  4. Vérifier l'alignement de l'antenne
```

Alarmes de Configuration

```
Catégorie : État du Système
Causes Probables :
  - Mismatch de Paramètre       → Incohérence de configuration
  - Licence Expirée              → Problème de licence
  - Erreur de Somme de Contrôle de Configuration    → Corruption
ou conflit
  - Fonction Non Licenciée     → Utilisation de fonction dépassant
la licence

Impact : Indisponibilité ou dégradation de fonction
Enquête :
  1. Réviser les changements de configuration
  2. Comparer la configuration actuelle à celle prévue
  3. Vérifier le fichier de licence et son expiration
  4. Vérifier la compatibilité des versions logicielles
```

Enquête & Dépannage

Flux de Travail d'Enquête



Étape 1 : Réviser les Détails de l'Alarme

Lorsqu'une alarme se déclenche, commencez par rassembler des informations :

Ce qu'il faut collecter :

- ID d'Alarme et identifiant unique
- Sévérité et cause probable
- Système DN affecté (appareil/cellule/composant)
- Heure de l'événement (quand cela s'est produit)
- Durée (combien de temps cela a été actif)
- Description complète de l'alarme et texte

Outils :

- Interface Web RAN Monitor → Page des Alarmes
- Grafana → Tableau des Alarmes Actives
- InfluxDB → Interroger l'enregistrement brut de l'alarme

Étape 2 : Rechercher la Cause Probable

Chaque type d'alarme a des causes connues et des enquêtes :

Connaissances Documentées :

- Guides de dépannage Nokia AirScale
- Historique des tickets précédents (problèmes similaires)
- Livres de course documentés RAN Monitor
- Expertise de l'équipe (experts en la matière)

Étape 3 : Vérifier les Métriques Associées

Corréler les alarmes avec les métriques de performance pour comprendre l'impact :

```
Exemple : Alarme "Ressource DL Bloquée"
├─ Vérifier l'Utilisation des Ressources DL (devrait être > 95 %)
├─ Vérifier le Débit de Trafic (tendance à la hausse ?)
├─ Vérifier le Taux de Réussite de Configuration d'Appel
(abandonné ?)
├─ Vérifier le Taux de Réussite de Transfert (affecté ?)
└─ Vérifier la Disponibilité de la Cellule (hors service ?)
```

Outils :

- Grafana → Tableau de bord spécifique à l'appareil
- Interface Web → Page de détail de l'appareil → Section Métriques
- Requêtes directes InfluxDB pour corrélation

Étape 4 : Corréler avec les Changements Récents

De nombreux problèmes sont causés par des modifications récentes :

```
Chronologie :
├─ Changements de configuration (dernières 4 heures)
├─ Mises à jour logicielles (dernières 24 heures)
├─ Réglage des paramètres de fonction (derniers 7 jours)
├─ Activités de maintenance (derniers 7 jours)
├─ Changements de réseau (derniers 7 jours)
└─ Changements de tiers (réseau externe)
```

Outils :

- RAN Monitor → Historique de configuration
- Système de gestion des changements
- Historique des incidents (problèmes similaires auparavant)
- Journaux de notification inter-équipes

Étape 5 : Diagnostiquer la Cause Racine

Sur la base de l'enquête, identifier la cause racine :

Exemple d'Arbre de Décision : Alarme "Cellule Indisponible"

```
Alarme Cellule Indisponible
│
├─ L'appareil répond-il à la gestion ?
│  ├─ NON → Vérifier la connectivité de l'appareil, redémarrer si
nécessaire
│  └─ OUI → Continuer
��
├─ Toutes les cellules sont-elles hors service ou une cellule
spécifique ?
│  ├─ Toutes les cellules → Vérifier le matériel de bande de
base/alimentation
│  └─ Cellule spécifique → Continuer
│
├─ La cellule transmet-elle de l'énergie ?
│  ├─ NON → Vérifier l'Amplificateur de Puissance, connexion de
l'antenne
│  └─ OUI → Continuer
│
├─ Les cellules voisines signalent-elles cette cellule ?
│  ├─ OUI → D'autres appareils voient cette cellule comme
indisponible
│  │       → Vérifier l'alignement de l'antenne, connexion de
câble
│  └─ NON → La cellule est hors service pour une raison interne
│          → Vérifier le module de bande de base, état DSP
│
└─ Vérifier les journaux pour les messages d'erreur
   → Panne logicielle
   → Violation de licence
   → Erreur de paramètre
```

Étape 6 : Mettre en Œuvre la Résolution

Une fois la cause racine identifiée, mettre en œuvre la solution :

Types de Résolutions :

Type	Méthode	Exemple
Immédiate	Redémarrer/redémarrer	Redémarrage de l'appareil pour effacer le processus bloqué
Configuration	Ajuster les paramètres	Changer le seuil de transfert
Matériel	Remplacer/réparer	Échanger l'alimentation défaillante
Logiciel	Mettre à jour/patcher	Installer le correctif logiciel
Réseau	Réparer la connectivité	Restaurer la route BGP, corriger le pare-feu

Étape 7 : Vérifier la Résolution

Après avoir mis en œuvre la solution, vérifier :

```
Liste de Vérification de Vérification :
□ Alarme effacée dans RAN Monitor
□ Métriques associées normalisées
□ Pas d'alarmes secondaires/cascadées
□ Métriques de performance revenues à la normale
□ Rapports clients (si applicable) résolus
□ Système stable (> 30 minutes d'observation)
```

Étape 8 : Documenter l'Apprentissage

Enregistrer les conclusions pour référence future :

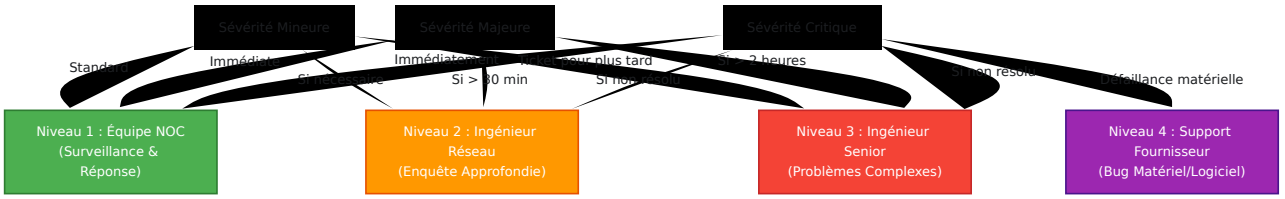
Documenter :

- Cause racine et facteurs contributifs
- Étapes prises pour résoudre

- Temps passé (pour le suivi SLA)
- Mesures préventives prises
- Connaissances partagées avec l'équipe

Procédures d'Escalade

Échelle d'Escalade



Déclencheurs d'Escalade

Escalader au Niveau 2 si :

- Alarme critique non effacée après 15 minutes
- Alarme majeure non effacée après 30 minutes
- Problème en dehors de l'expertise de l'équipe NOC
- Nécessite un redémarrage de l'appareil/changement majeur
- Affecte > 1 site simultanément

Escalader au Niveau 3 si :

- Niveau 2 incapable de diagnostiquer après 1 heure
- Problème critique persiste > 30 minutes
- Défaillance matérielle suspectée
- Problèmes en cascade détectés
- Nécessite l'implication du fournisseur

Contacter le Fournisseur (Niveau 4) si :

- Défaillance matérielle confirmée (PSU, CMON, etc.)

- Bug logiciel suspecté (plantage irrécupérable)
- Problème de licence/activation
- Problème documenté dans les problèmes connus du fournisseur
- Plusieurs niveaux d'escalade incapables de résoudre

Communication d'Escalade

Modèle pour Escalader au Niveau 2 :

```
Objet : Escalade - [Sévérité] - [Appareil] - [Problème]

Heure d'Alerte : [2025-12-10 14:30 UTC]
Durée : [15 minutes]
Appareil : [SITE_A_BS1]
Problème : [Cellule Indisponible]

Symptômes :
- Cellule A1 ne répond pas à la gestion
- Toutes les cellules signalant cellule indisponible
- Ping de l'appareil réussi

Enquête Réalisée :
- Connectivité de l'appareil vérifiée
- État du module de bande de base vérifié
- État de l'alimentation : OK
- Température : Normale

Métriques :
- Disponibilité de la cellule : 0 %
- Pas de trafic sur la cellule
- Plan de contrôle : Connecté

Analyse Initiale :
- Possible défaillance du module de bande de base
- Ou problème matériel de l'amplificateur de puissance

Prochaines Étapes Recommandées :
- Diagnostics matériels
- Échange de module si disponible
- Redémarrage de l'appareil en dernier recours

Lien d'Escalade : [Lien du Tableau de Bord]
```

Suivi des Résolutions

Suivi SLA

Suivre le temps de résolution pour la conformité SLA :

```
Chronologie de l'Alarme :
├─ Heure de l'Événement : 14:23:45 ← Quand le problème s'est
produit
├─ Heure de Détection : 14:23:47 (2 sec) ← Détecté par la gestion
├─ Heure d'Alerte : 14:23:50 (5 sec) ← Opérations notifiées
├─ Heure de Reconnaissance : 14:24:15 (30 sec) ← Opérateur reconnu
├─ Enquête : 14:24:15 → 14:28:00 (3.75 min)
├─ Résolution : 14:28:00 → 14:28:35 (35 sec de correction +
vérification)
└─ Heure d'Effacement : 14:28:36 ← Alarme effacée
    └─ Durée Totale : 5 min 51 sec

Métriques SLA :
├─ Latence de Détection : 2 secondes
├─ Alerte à ACK : 30 secondes
├─ Temps de Résolution : 5 min 51 sec
└─ Statut SLA : PASS (< 15 min cible)
```

Analyse de Tendance

Suivre les modèles dans les données d'alarme :

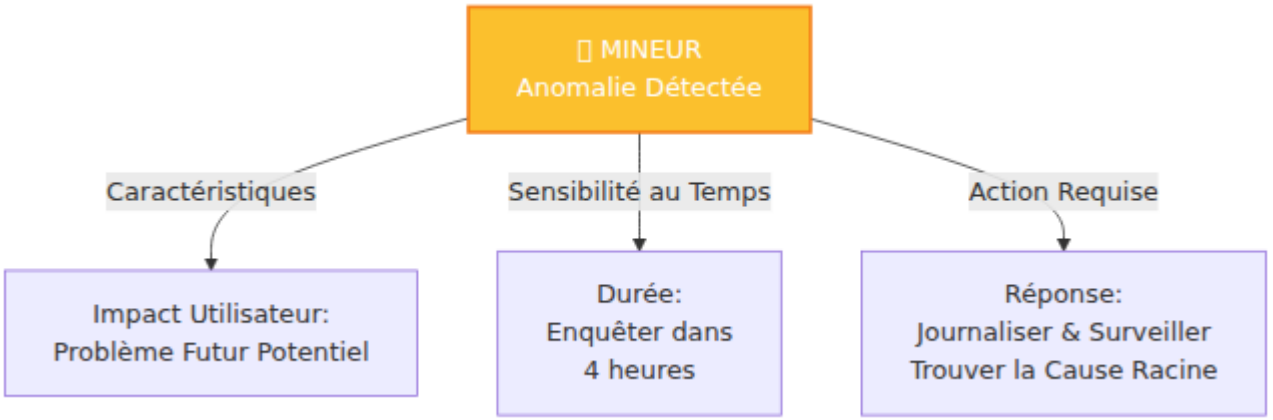
Questions à poser :

- Voyons-nous la même alarme se répéter ?
- Le taux d'alarme augmente-t-il/diminue-t-il ?
- Les alarmes se regroupent-elles à des moments spécifiques ?
- Plusieurs sites sont-ils affectés simultanément ?
- Le MTTR s'améliore-t-il au fil du temps ?

Outils :

- Grafana → Tableau de bord des tendances d'alarme
- Rapport des principales alarmes (hebdomadaire)
- Suivi du MTTR par appareil/type

Prévenir les Problèmes Répétitifs



Meilleures Pratiques

Excellence Opérationnelle

1. Prévention de la Fatigue des Alarmes

- Définir des seuils significatifs (pas trop sensibles)
- Utiliser des fenêtres de durée (pas un seul pic)
- Agréger les alarmes connexes
- Supprimer les faux positifs connus

2. Réponse Rapide

- Garder les livres de course à jour
- Former l'équipe sur les problèmes courants
- Utiliser l'automatisation pour les réinitialisations de routine
- Avoir les contacts d'escalade facilement disponibles

3. Documentation de Qualité

- Documenter chaque incident
- Partager les apprentissages avec l'équipe
- Mettre à jour les livres de course en fonction des incidents

- Former croisée des membres de l'équipe

4. Surveillance Proactive

- Surveiller les avertissements avant les critiques
- Analyse de tendance pour la planification de capacité
- Vérifications de santé régulières
- Établissement d'une ligne de base de performance

Développement de Livres de Course

Chaque alarme fréquente devrait avoir un livre de course :

Modèle :

```
Alarme : [Cellule Indisponible]
Probabilité : [Élevée]
MTTR : [5-15 minutes]
Cible SLA : [Résolu dans les 30 minutes]

Symptômes :
- Alarme : "Cellule Indisponible"
- Utilisateurs : Impossible de se connecter
- Métriques : Disponibilité de la cellule 0 %

Diagnostic Rapide (< 5 minutes) :
1. L'appareil répond-il au ping ?
2. D'autres cellules fonctionnent-elles ?
3. La bande de base fonctionne-t-elle (vérifier les journaux) ?

Étapes de Résolution :
Étape 1 : Vérification de la Connectivité de l'Appareil
  - Ping de l'appareil : ping 192.168.1.100
  - Si pas de réponse → Vérifier la connectivité réseau

Étape 2 : État Matériel
  - Vérifier l'état de l'Amplificateur de Puissance
  - Vérifier les LED du module de bande de base
  - Vérifier la connexion de l'antenne

Étape 3 : Redémarrer la Cellule
  - Redémarrer la cellule via l'interface de gestion
  - Attendre 60 secondes pour le démarrage
  - Vérifier que les métriques se normalisent

Étape 4 : Si Toujours Hors Service
  - Escalader au Niveau 2
  - Préparer le redémarrage de l'appareil
  - Notifier le client

Escalade :
- Si > 15 minutes → Escalader à [Nom de l'Ingénieur]
- Si > 30 minutes → Escalader à [Ingénieur Senior]
- Si défaillance matérielle → Contacter le Support Nokia

Prévention :
- Mises à jour régulières du firmware de bande de base
```

```
- Remplacement préventif de l'alimentation
- Inspection de la connexion de l'antenne trimestriellement
```

Points de terminaison API & Gestion de la configuration

API REST pour la gestion de la configuration et des opérations des dispositifs RAN

Guide pour gérer la configuration des stations de base, interroger l'état des dispositifs et automatiser les opérations RAN en utilisant l'API indépendante du fournisseur

---

Table des matières

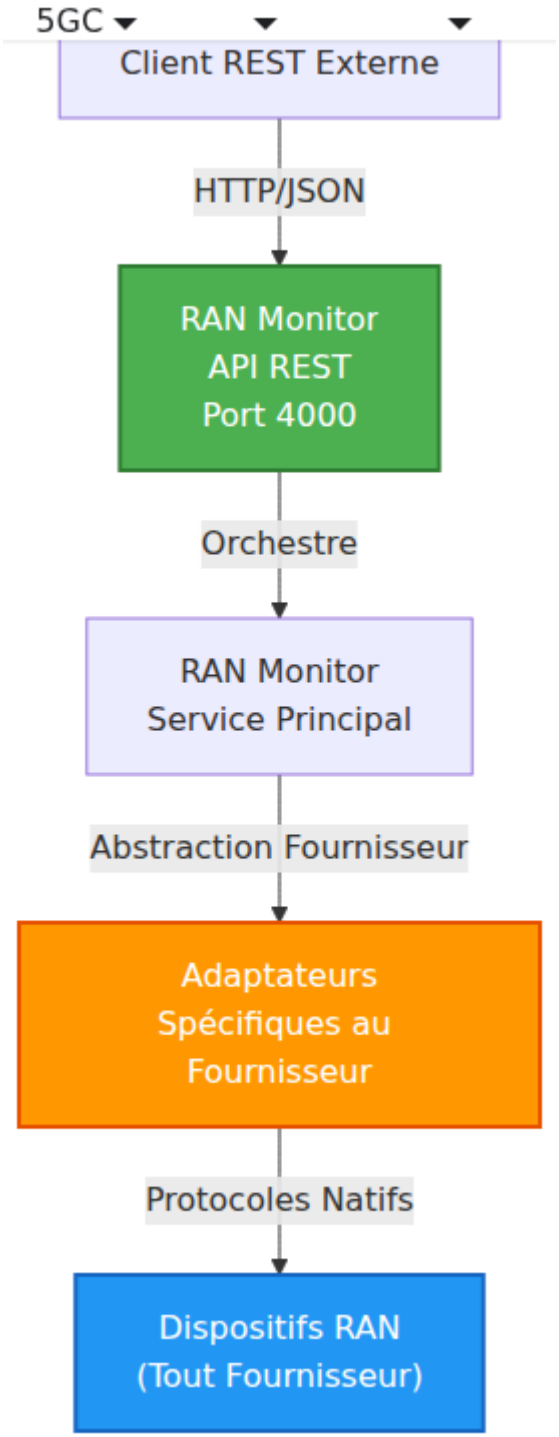
1. Aperçu
2. Architecture de l'API
3. Authentification & Accès
4. Référence des points de terminaison
5. Gestion de la configuration
6. Opérations de récupération de données
7. Flux de travail communs
8. Gestion des erreurs
9. Exemples d'API

Aperçu

RAN Monitor expose une API REST complète pour gérer la configuration des dispositifs RAN et interroger les données opérationnelles. L'API fournit une interface indépendante du fournisseur qui abstrait les protocoles de communication des dispositifs sous-jacents. L'API permet :

- **Gestion des dispositifs** - Enregistrer, désenregistrer et surveiller les dispositifs
- **Requêtes de configuration** - Récupérer les paramètres des dispositifs et l'état du système
- **Collecte de données** - Extraire des métriques de performance, des alarmes et une topologie
- **Contrôle de session** - Gérer les sessions de communication avec les dispositifs
- **Opérations réseau** - Automatiser les tâches de gestion de routine

Architecture de l'API



Fonctionnalités de l'API

- **Conception RESTful** - Méthodes HTTP standard (GET, POST, PUT, DELETE)
- **Format JSON** - Toutes les requêtes et réponses sont en JSON
- **Abstraction Fournisseur** - API unifiée à travers différents fournisseurs de dispositifs

- **Opérations Stateful** - Maintient les sessions et l'état des dispositifs
- **Gestion des erreurs** - Messages d'erreur détaillés et codes d'état
- **Traitement Asynchrone** - Requêtes non bloquantes pour les longues opérations

---

Authentification & Accès

Enregistrement de Dispositif

Avant toute opération, un dispositif doit être enregistré auprès de RAN Monitor. L'enregistrement établit la connexion entre RAN Monitor et le dispositif en utilisant le mécanisme d'authentification natif de chaque fournisseur.

Processus d'enregistrement :

1. Les identifiants du dispositif (nom d'utilisateur/mot de passe ou clés API) sont stockés en toute sécurité
2. Un test de connectivité initial vérifie que le dispositif est accessible
3. Le dispositif est enregistré et prêt pour les opérations
4. La surveillance continue de la santé commence

Contrôle d'accès à l'API

Actuellement, l'API RAN Monitor est accessible au sein du réseau de gestion. Pour les déploiements en production, envisagez :

- **Méthodes d'authentification :**
  - Clé API dans l'en-tête : `Authorization: Bearer <api-key>`
  - OAuth2 pour l'intégration avec les fournisseurs d'identité
  - Contrôle d'accès basé sur le réseau (pare-feu/VPN)
- **Limitation de taux :**
  - Limites par client pour prévenir les abus

    - Limites par dispositif pour la fréquence des opérations

- **Journalisation des audits :**
    - Tous les appels API sont enregistrés avec des horodatages et des informations sur l'utilisateur/client
    - Les changements de configuration sont suivis avec des valeurs avant/après

---

Référence des points de terminaison

Gestion des dispositifs

Lister tous les dispositifs

```
GET /api/v1/devices
```

Réponse :

```
{
  "data": [
    {
      "name": "SITE_A_BS1",
      "address": "192.168.1.100:8080",
      "registration_status": "registered",
      "session_status": "active",
      "bts_status": "connected",
      "vendor": "Nokia",
      "agent_type": "AirScale",
      "software_release": "BSC-2250.5.0",
      "hardware_version": "2.0",
      "agent_unique_id": "airscale-001",
      "manager_vendor": "Nokia",
      "manager_release": "NE3S-5.0",
      "license_required": false,
      "retention_hours": 720,
      "last_connected_at": "2025-12-10T14:30:00Z",
      "disconnected_at": null,
      "last_error_code": null,
      "last_error_string": null,
      "data": {
        "pm_points": 45320,
        "pm_last_write": "2025-12-10T14:15:00Z",
        "config_points": 1200,
        "config_last_write": "2025-12-10T14:30:00Z",
        "alarm_points": 15
      },
      "pm_warning": null
    }
  ],
  "meta": {
    "total": 50,
    "page": 1,
    "per_page": 25,
    "total_pages": 2
  },
  "status_counts": {
    "total": 50,
    "connected": 45,
    "waiting_for_pm": 2,
    "pending": 1,
    "registering": 0,
```

```
    "disconnected": 2
  }
}
```

Obtenir les détails d'un dispositif

```
GET /api/v1/devices/:id
```

Réponse :

```
{
  "device": {
    "id": "nokia_bs1",
    "name": "SITE_A_BS1",
    "vendor": "Nokia",
    "address": "192.168.1.100",
    "registration_status": "registered",
    "registration_key": "base64_encoded_key",
    "session_id": "nonuniquesession",
    "session_expiry": "2025-12-11T14:30:00Z",
    "device_info": {
      "type": "AirScale",
      "software_release": "5.0.0",
      "hardware_version": "2.0",
      "agent_unique_id": "airscale-001"
    }
  }
}
```

Enregistrer un dispositif

```
PUT /api/v1/devices/:id/register
Content-Type: application/json

{
  "address": "192.168.1.100:8080",
  "web_username": "admin",
  "web_password": "password",
  "webhook_url": "http://manager.example.com:9076/webhook",
  "private_key_path": "/etc/certs/private.key",
  "public_key_path": "/etc/certs/public.key"
}
```

Réponse :

```
{
  "result": "Success",
  "registration_key": "base64_encoded_nonce",
  "device_id": "nokia_bs1",
  "message": "Device registered successfully"
}
```

Codes d'état :

- `200` - Enregistrement réussi
- `400` - Paramètres invalides ou erreur de dispositif
- `409` - Dispositif déjà enregistré
- `500` - Erreur interne

Désenregistrer un dispositif

```
DELETE /api/v1/devices/:id
```

Réponse :

```
{
  "result": "Success",
  "message": "Device unregistered",
  "device_id": "nokia_bs1"
}
```

Gestion de session

Démarrer une session

```
PUT /api/v1/devices/:id/sessions
Content-Type: application/json

{
  "session_id": "session_unique_identifier"
}
```

Réponse :

```
{
  "result": "Success",
  "session_id": "session_unique_identifier",
  "session_timeout": 86400,
  "expires_at": "2025-12-11T14:30:00Z"
}
```

Durée de vie de la session :

- Délai d'expiration par défaut : 24 heures
- Keep-alive requis avant expiration
- Actualisation automatique toutes les 20 heures

Vérifier l'état de la session

```
GET /api/v1/devices/:id/sessions
```

Réponse :

```
{
  "session": {
    "active": true,
    "session_id": "session_unique_identifier",
    "expires_at": "2025-12-11T14:30:00Z",
    "time_remaining_seconds": 82400,
    "last_activity": "2025-12-10T14:30:00Z"
  }
}
```

Garder la session active

```
POST /api/v1/devices/:id/sessions/keep-alive
```

Réponse :

```
{
  "result": "Success",
  "new_expiry": "2025-12-11T14:30:00Z"
}
```

Gestion de la configuration

Interroger la configuration

Récupérer les paramètres de configuration du dispositif :

```
PUT /api/v1/devices/:id/config/upload
Content-Type: application/json

{
  "filter": {
    "uploadType": "configuration",
    "objects": [
      {
        "sdn": "/BSC-1/BTS-23/*",
        "depth": 100
      }
    ],
    "objectClass": ""
  }
}
```

Réponse :

```
{
  "result": "Success",
  "configuration": {
    "timestamp": "2025-12-10T14:30:00Z",
    "device_id": "nokia_bs1",
    "parameters": {
      "/BSC-1/BTS-23": {
        "BtsBasics": {
          "BtsName": "CELL_A",
          "BtsType": "MACRO",
          "EnvironmentalSpecifications": {
            "TemperatureRange": "Industrial"
          }
        },
        "CarrierAggregation": {
          "CarrierAggregationCapability": true,
          "MaxUECarriers": 5
        }
      }
    }
  }
}
```

Provisionner la configuration

Pousser un fichier de configuration à un dispositif, en effectuant le téléchargement, la validation et l'activation en une seule opération atomique. Une sauvegarde de la configuration actuelle en cours d'exécution est automatiquement enregistrée.

```
PUT /api/ne3s/function/provision
Content-Type: application/json

{
  "airscale_name": "nokia_bs1",
  "config_file": "/path/to/config.xml",
  "take_fallback": true,
  "block_local_changes": false
}
```

Réponse :

```
{
  "status": "success",
  "operation": "provision",
  "plan_id": "plan_17414844000000000000",
  "data": "<provisionResponse>...</provisionResponse>"
}
```

Paramètres :

Paramètre	Type	Requis	Par défaut	But
airscale_name	String	Oui	-	Nom du dispositif cible
config_file	String	Oui	-	Chemin vers le fichier de configuration XML sur le serveur
take_fallback	Boolean	Non	true	Sauvegarder la configuration actuelle comme fallback avant activation
block_local_changes	Boolean	Non	false	Bloquer les changements locaux pendant l'opération

Erreurs :

- `INVALID_FILE` - chemin config_file manquant ou fichier n'existe pas
- `TRANSPORT_ERROR` - Problème de connectivité réseau avec le dispositif
- `SESSION_ERROR` - Impossible d'établir une session NE3S
- Erreurs SOAP du dispositif (par exemple, erreurs de validation, violations de schéma)

Définir un paramètre de configuration

```
PUT /api/v1/devices/:id/config/set
Content-Type: application/json

{
  "parameter_path": "/BSC-1/BTS-23/BtsBasics/BtsName",
  "value": "NEW_CELL_NAME",
  "value_type": "string"
}
```

Réponse :

```
{
  "result": "Success",
  "parameter": "/BSC-1/BTS-23/BtsBasics/BtsName",
  "old_value": "CELL_A",
  "new_value": "NEW_CELL_NAME",
  "applied_at": "2025-12-10T14:30:45Z"
}
```

Paramètres de configuration courants :

Paramètre	Type	Exemple	But
BtsName	String	"SITE_A_Cell_1"	Identifiant de la cellule/station de base
MaxUEsServed	Integer	256	Nombre maximum d'UE simultanés
CellTXPower	Integer	40 (dBm)	Niveau de puissance d'émission
EnableCarrierAgg	Boolean	true	Support de l'agrégation de porteuses
HandoverHysteresis	Integer	3 (dB)	Sensibilité au transfert

Obtenir l'historique de configuration

```
GET /api/v1/devices/:id/config/history?limit=10&days=7
```

Réponse :


```
{
  "history": [
    {
      "timestamp": "2025-12-10T14:30:45Z",
      "change_type": "parameter_modified",
      "parameter": "/BSC-1/BTS-23/BtsBasics/BtsName",
      "old_value": "CELL_A",
      "new_value": "NEW_CELL_NAME",
      "reason": "Mise à jour manuelle de la configuration"
    }
  ]
}
```

Récupération de données

Obtenir des métriques de performance

Récupérer les données des compteurs de performance :

```
PUT /api/v1/devices/:id/metrics/upload
Content-Type: application/json

{
  "filter": {
    "uploadType": "measurement",
    "objects": [
      {
        "sdn": "*",
        "depth": 100
      }
    ]
  }
}
```

Réponse :

```
{
  "result": "Success",
  "metrics": {
    "timestamp": "2025-12-10T14:30:00Z",
    "measurement_interval": 300,
    "counters": [
      {
        "id": "M1C1",
        "name": "Débit Cellulaire DL",
        "value": 125.4,
        "unit": "Mbps",
        "cell_dn": "/BSC-1/BTS-23/Cell-1"
      },
      {
        "id": "M1C2",
        "name": "Débit Cellulaire UL",
        "value": 89.2,
        "unit": "Mbps",
        "cell_dn": "/BSC-1/BTS-23/Cell-1"
      }
    ]
  }
}
```

Obtenir les alarmes actives

```
PUT /api/v1/devices/:id/alarms/upload
Content-Type: application/json

{
  "filter": {
    "uploadType": "active_faults"
  }
}
```

Réponse :

```
{
  "result": "Success",
  "alarms": [
    {
      "alarm_id": "a1b2c3d4",
      "severity": "Critique",
      "probable_cause": "Cellule Indisponible",
      "specific_problem": "Échec de l'alimentation électrique",
      "affected_dn": "/BSC-1/BTS-23/Cell-1",
      "event_time": "2025-12-10T14:15:30Z",
      "description": "La cellule 1 est indisponible en raison d'un
échec de l'alimentation électrique"
    }
  ]
}
```

Obtenir la topologie du dispositif

```
PUT /api/v1/devices/:id/topology/upload
Content-Type: application/json

{
  "filter": {
    "uploadType": "topology",
    "objects": [
      {
        "sdn": "*",
        "depth": 100
      }
    ]
  }
}
```

Réponse :

```
{
  "result": "Success",
  "topology": {
    "device_dn": "/BSC-1",
    "managed_elements": [
      {
        "name": "BTS-23",
        "type": "BaseTransceiverStation",
        "dn": "/BSC-1/BTS-23",
        "cells": [
          {
            "name": "Cell-1",
            "type": "EUtranCell",
            "physical_cell_id": 100,
            "frequency": 2110
          }
        ]
      }
    ]
  }
}
```

Vérifications de santé

Ping du dispositif

```
PUT /api/v1/devices/:id/ping
```

Réponse :

```
{
  "result": "Success",
  "device_id": "nokia_bs1",
  "latency_ms": 45,
  "status": "reachable"
}
```

Obtenir des métriques système

```
GET /api/system-metrics
```

Renvoie les statistiques de l'écrivain par lots, l'état de la spool PM, les statistiques InfluxDB par dispositif et l'utilisation des ressources système.

Réponse :

```
{
  "data": {
    "batch_writer": {
      "queue_depth": 120,
      "queue_max": 50000,
      "flush_count": 8452,
      "points_written": 1250000,
      "bytes_written": 89000000
    },
    "pm_spool": {
      "pending_files": 3,
      "files_processed": 1420,
      "files_failed": 0,
      "points_written": 980000,
      "points_filtered": 4200000,
      "bytes_read": 650000000,
      "last_file_ms": 245,
      "started_at": "2025-12-10T08:00:00Z"
    },
    "influxdb_stats": [
      {
        "name": "2045_Booker",
        "total": 12500,
        "last_write": "2025-12-10T14:15:00Z",
        "performance_metrics": 11000,
        "configuration": 1200,
        "alarms": 300
      }
    ],
    "system": {
      "memory_total": 524288000,
      "memory_processes": 312000000,
      "memory_binary": 89000000,
      "memory_ets": 45000000,
      "process_count": 1250,
      "run_queue": 0
    }
  }
}
```


Obtenir la santé du système

```
GET /api/v1/health/status
```

Réponse :

```
{
  "status": "healthy",
  "devices": {
    "total": 50,
    "registered": 48,
    "active_sessions": 45,
    "unreachable": 2
  },
  "database": {
    "influxdb": "connected"
  },
  "timestamp": "2025-12-10T14:30:00Z"
}
```

Gestion de la configuration

Modèle de données de configuration

La configuration de l'eNodeB Nokia est organisée de manière hiérarchique :

```
/SystemFunctions
├── /BSC-1 (Contrôleur de Station de Base)
│   └── /BTS-23 (Station de Transception de Base)
│       ├── BtsBasics (Nom, type, emplacement)
│       ├── /Cell-1
│       │   ├── CellCommonData
│       │   ├── CellAdvanced
│       │   └── CarrierAggregation
│       └── /Cell-2
│           └── ...
└── /Connectivity
    ├── S1Interface
    ├── X2Interface
    └── NetworkConfiguration
```

Tâches de configuration courantes

Activer/Désactiver une cellule

```
{
  "parameter_path": "/BSC-1/BTS-23/Cell-
1/CellCommonData/AdminState",
  "value": "UNLOCKED",
  "value_type": "enum"
}
```

Valeurs possibles : `LOCKED`, `UNLOCKED`, `SHUTTING_DOWN`

Ajuster la puissance de la cellule

```
{
  "parameter_path": "/BSC-1/BTS-23/Cell-
1/CellAdvanced/CellTXPower",
  "value": "35",
  "value_type": "integer"
}
```

Plage : 0-46 dBm (dépendant du dispositif)

Configurer l'hystérésis de transfert

```
{
  "parameter_path": "/BSC-1/BTS-23/Cell-
1/CellAdvanced/HandoverHysteresis",
  "value": "3",
  "value_type": "integer"
}
```

Unité : dB, plage typique : 0-8 dB

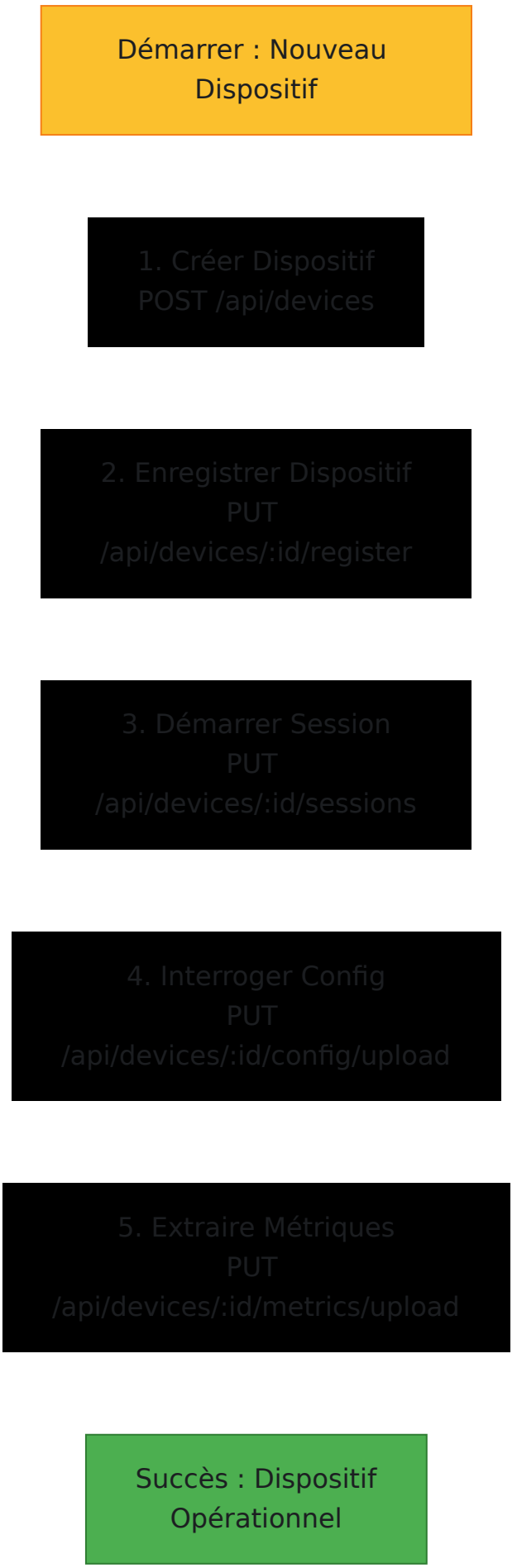
Définir le nombre maximum d'utilisateurs connectés

```
{
  "parameter_path": "/BSC-1/BTS-23/MaxUEsServed",
  "value": "256",
  "value_type": "integer"
}
```

Limite dépendante du dispositif

Flux de travail communs

Flux de travail 1 : Intégration de dispositif


Démarrer : Nouveau Dispositif
1. Créer Dispositif POST /api/devices
2. Enregistrer Dispositif PUT /api/devices/:id/register
3. Démarrer Session PUT /api/devices/:id/sessions
4. Interroger Config PUT /api/devices/:id/config/upload
5. Extraire Métriques PUT /api/devices/:id/metrics/upload
Succès : Dispositif Opérationnel

Exemple :

```
# 1. Créer une entrée de dispositif
curl -X POST http://localhost:4000/api/v1/devices \
  -H "Content-Type: application/json" \
  -d '{
    "id": "site_a_bs1",
    "name": "SITE_A_BS1",
    "vendor": "Nokia",
    "address": "192.168.1.100:8080",
    "credentials": {
      "username": "admin",
      "password": "password"
    }
  }'

# 2. Enregistrer avec le dispositif
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/register \
  -H "Content-Type: application/json" \
  -d '{
    "webhook_url": "http://manager.example.com:9076/webhook"
  }'

# 3. Démarrer la session
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/sessions \
  -H "Content-Type: application/json" \
  -d '{"session_id": "session_001"}'

# 4. Obtenir la configuration
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/config/upload \
  -H "Content-Type: application/json" \
  -d '{
    "filter": {
      "uploadType": "configuration",
      "objects": [{"sdn": "*", "depth": 100}]
    }
  }'
```

Flux de travail 2 : Mise à jour de la configuration

```
# 1. Interroger la valeur actuelle
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/config/upload \
  -H "Content-Type: application/json" \
  -d '{
    "filter": {
      "uploadType": "configuration",
      "objects": [{"sdn": "/BSC-1/BTS-23/Cell-1", "depth": 10}]
    }
  }' | jq '.configuration.parameters["/BSC-1/BTS-23/Cell-1"]'

# 2. Modifier le paramètre
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/config/set \
  -H "Content-Type: application/json" \
  -d '{
    "parameter_path": "/BSC-1/BTS-23/Cell-
1/CellAdvanced/CellTXPower",
    "value": "38",
    "value_type": "integer"
  }'

# 3. Vérifier le changement
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/config/upload \
  -H "Content-Type: application/json" \
  -d '{
    "filter": {
      "uploadType": "configuration",
      "objects": [{"sdn": "/BSC-1/BTS-23/Cell-1/CellAdvanced",
"depth": 5}]
    }
  }' | jq '.configuration.parameters["/BSC-1/BTS-23/Cell-
1/CellAdvanced/CellTXPower"]'
```

Flux de travail 3 : Surveillance de la

performance

```
# Boucle de surveillance continue (exemple de script)
#!/bin/bash

DEVICE="site_a_bs1"
INTERVAL=300  # 5 minutes

while true; do
  # Extraire les métriques
  METRICS=$(curl -s -X PUT
http://localhost:4000/api/v1/devices/$DEVICE/metrics/upload \
    -H "Content-Type: application/json" \
    -d '{
      "filter": {
        "uploadType": "measurement",
        "objects": [{"sdn": "*", "depth": 100}]
      }
    }')

  # Extraire les métriques clés
  DL=$(echo $METRICS | jq '.metrics.counters[] |
select(.id=="M1C1") | .value')
  CELLS=$(echo $METRICS | jq '.metrics.counters | length')

  echo "$(date): DL=$DL Mbps, Cells=$CELLS"

  # Vérifier les alarmes
  ALARMS=$(curl -s -X PUT
http://localhost:4000/api/v1/devices/$DEVICE/alarms/upload \
    -H "Content-Type: application/json" \
    -d '{
      "filter": {
        "uploadType": "active_faults"
      }
    }' | jq '.alarms | length')

  if [ "$ALARMS" -gt 0 ]; then
    echo "AVERTISSEMENT : $ALARMS alarmes actives"
  fi
```

```
  sleep $INTERVAL
done
```

Gestion des erreurs

Codes d'état HTTP

Code	Signification	Exemple
`200`	Succès	Configuration récupérée
`201`	Créé	Dispositif enregistré
`400`	Mauvaise demande	JSON ou paramètres invalides
`401`	Non autorisé	Clé API manquante/invalides
`404`	Non trouvé	Le dispositif n'existe pas
`409`	Conflit	Dispositif déjà enregistré
`500`	Erreur serveur	Échec de la connexion à la base de données
`503`	Indisponible	Mode maintenance

Format de réponse d'erreur

```
{
  "error": {
    "code": "DEVICE_NOT_FOUND",
    "message": "Dispositif 'site_a_bs1' non trouvé",
    "details": {
      "device_id": "site_a_bs1",
      "timestamp": "2025-12-10T14:30:00Z"
    }
  }
}
```

Erreurs courantes

Dispositif non enregistré :

```
{
  "error": {
    "code": "NOT_REGISTERED",
    "message": "Le dispositif doit être enregistré avant les
opérations",
    "solution": "Appelez PUT /api/devices/:id/register d'abord"
  }
}
```

Session expirée :

```
{
  "error": {
    "code": "SESSION_EXPIRED",
    "message": "La session du dispositif a expiré",
    "solution": "Appelez PUT /api/devices/:id/sessions pour
démarrer une nouvelle session"
  }
}
```

Paramètre de configuration invalide :

```
{
  "error": {
    "code": "INVALID_PARAMETER",
    "message": "Valeur du paramètre hors de portée",
    "details": {
      "parameter": "/BSC-1/BTS-23/Cell-
1/CellAdvanced/CellTXPower",
      "value": "99",
      "valid_range": "0-46 dBm"
    }
  }
}
```

Exemples d'API

Exemple de client Python

```
import requests
import json

class RanMonitorClient:
    def __init__(self, base_url="http://localhost:4000/api/v1"):
        self.base_url = base_url
        self.session = requests.Session()

    def register_device(self, device_id, address, username,
password):
        """Enregistrer un nouveau dispositif"""
        url = f"{self.base_url}/devices/{device_id}/register"
        payload = {
            "address": address,
            "web_username": username,
            "web_password": password,
            "webhook_url": "http://manager:9076/webhook"
        }
        response = self.session.put(url, json=payload)
        return response.json()

    def get_config(self, device_id, sdn="*", depth=100):
        """Récupérer la configuration du dispositif"""
        url = f"{self.base_url}/devices/{device_id}/config/upload"
        payload = {
            "filter": {
                "uploadType": "configuration",
                "objects": [{"sdn": sdn, "depth": depth}]
            }
        }
        response = self.session.put(url, json=payload)
        return response.json()

    def set_config(self, device_id, parameter_path, value,
value_type="string"):
        """Mettre à jour un paramètre de configuration"""
        url = f"{self.base_url}/devices/{device_id}/config/set"
        payload = {
```

```
            "parameter_path": parameter_path,
            "value": value,
            "value_type": value_type
        }
        response = self.session.put(url, json=payload)
        return response.json()

    def get_metrics(self, device_id):
        """Récupérer les métriques de performance"""
        url = f"
{self.base_url}/devices/{device_id}/metrics/upload"
        payload = {
            "filter": {
                "uploadType": "measurement",
                "objects": [{"sdn": "*", "depth": 100}]
            }
        }
        response = self.session.put(url, json=payload)
        return response.json()

# Exemple d'utilisation
client = RanMonitorClient()

# Enregistrer le dispositif
result = client.register_device(
    device_id="site_a_bs1",
    address="192.168.1.100:8080",
    username="admin",
    password="password"
)
print(f"Enregistrement : {result}")

# Obtenir la configuration
config = client.get_config("site_a_bs1")
print(f"Configuration : {json.dumps(config, indent=2)}")

# Mettre à jour le paramètre
update = client.set_config(
    "site_a_bs1",
    "/BSC-1/BTS-23/Cell-1/CellAdvanced/CellTXPower",
    "38",
    "integer"
```

```
)
print(f"Mise à jour : {update}")
```

Exemples cURL

Enregistrer le dispositif :

```
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/register \
  -H "Content-Type: application/json" \
  -d '{
    "address": "192.168.1.100:8080",
    "web_username": "admin",
    "web_password": "password",
    "webhook_url": "http://manager:9076/webhook"
  }'
```

Obtenir l'état du dispositif :

```
curl -X GET http://localhost:4000/api/v1/devices/site_a_bs1
```

Interroger la configuration :

```
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/config/upload \
  -H "Content-Type: application/json" \
  -d '{
    "filter": {
      "uploadType": "configuration",
      "objects": [{"sdn": "/BSC-1/*", "depth": 50}]
    }
  }' | jq '.'
```

Collection Baicells

État en direct + collecte KPI pour les eNB Baicells (basé sur le sondage)

Les eNB Baicells sont pris en charge dans RAN Monitor aux côtés de Nokia AirScale et Casa. Contrairement à ces deux derniers — qui **poussent** les PM vers RAN Monitor — le firmware QAFA de Baicells n'a pas d'exportation de fichier PM, donc RAN Monitor **sonde** l'API web locale de chaque cellule à intervalles réguliers. Ce guide couvre le fonctionnement de ce processus et comment le configurer, le déployer et le vérifier.

Vue d'ensemble

Les eNB de la série Nova de Baicells (par exemple, pBS4200, firmware `BaiBS_QAFA_*`) exposent une petite, **non authentifiée** API texte clé/valeur à `https://<cell>/fsmoam/` sur laquelle l'interface web Gargoyle est construite. Il n'y a pas de page de statistiques/PM locale et pas de poussée de fichiers — les données disponibles sont des **jauges en direct** (instantanées), pas des compteurs historiques 32.435.

Le `Baicells.Scheduler` de RAN Monitor sonde chaque cellule configurée à intervalles réguliers, lit les champs de dispositif/RF/synchronisation/WAN/UE/throughput/alarmes via `/fsmoam/`, et les écrit dans InfluxDB. Les champs d'état (cellule active, synchronisée, GPS, OMC, WAN) sont toujours émis sous forme de séries `0/1` afin que les tableaux de bord affichent une santé continue même lorsque la cellule n'est pas en service.

Élément	Valeur
Mécanisme	**Sondage** (pull) — `GET /fsmoam/...`, pas d'authentification, en lecture seule
Intervalle de sondage	`config :ran_monitor, :baicells, interval_ms:` (par défaut 60s)
Mesure InfluxDB	`BaicellsPerformanceMetrics`
Clé de cellule	id eNB / numéro de série (config)
Auth/écritures	aucune utilisée — le collecteur n'émet jamais d'appels `set.*`

> Seul le port TCP 443 est ouvert sur ces unités ; les lectures ne nécessitent pas de identifiants (des identifiants incorrects retournent également des données). Le collecteur est strictement en lecture seule.

Architecture

```
RanMonitor.Baicells.Scheduler         (GenServer, sonde chaque
interval_ms)
   └─ pour chaque cellule configurée :
        RanMonitor.Baicells.Collector (sonde chaque cellule)
          ├─ RanMonitor.Baicells.Fsmoam     GET /fsmoam/get.
<oid>?... (pas d'auth)
          ├─ construire la carte d'état
(up/sync/GPS/OMC/WAN/RF/alarmes)
          └─ construire les points InfluxDB
(BaicellsPerformanceMetrics)
        → RanMonitor.EnhancedInfluxDbConnection.write
        → RanMonitor.Database.InfluxDbStats.record_write
        → RanMonitor.Baicells.Ingest (dernier état de sondage pour
la page d'état)
```

Référence des composants :

Composant	Responsabilité
Fsmoam	Client/parser en lecture seule pour l'API clé-valeur `/fsmoam/`
Collecteur	Un sondage → carte d'état + cartes de points InfluxDB
Planificateur	Boucle de sondage à intervalles → Influx + statistiques + Ingest
Cellules	Registre de cellules basé sur la configuration
Ingest	État de dernier sondage en mémoire par cellule (pour la page d'état)
Page d'état Baicells	Page "État Baicells"

Métriques

Chaque sondage émet ces points (les noms de compteur réutilisent le style Casa/Nokia afin que les données soient compatibles avec les tableaux de bord) :

Toujours (état, 0/1 ou compte) : `CELL.OpStateUp`, `CELL.Synced`, `CELL.GpsInPosition`, `CELL.OmcConnected`, `CELL.WanLinkUp`, `FM.ActiveAlarms`

Lorsque la cellule est en service (jauges en direct) : `RRC.ConnMean` (UE actifs), `DRB.PdcpSduBitrateDl` / `DRB.PdcpSduBitrateUl` (kbps), `RRU.RssiUl`, `RRU.MaxTxPowerDbm`, `CARR.EarfcnDl`, `CARR.PhyCellId`

Forme du point (mesure `BaicellsPerformanceMetrics`) : champ `counterValue`, tags `metricCounter, enbName, enbId, site, host, metricMcc, metricMnc, vendor="Baicells", recordType`.

Configuration

```
config :ran_monitor, :baicells,
  interval_ms: 60_000,
  cells: [
    %{
      name: "baicells-nova-pbs4200",
      enb_id: "1202000091183FP0178",   # numéro de série / id eNB
(tag enbId + clé d'état)
      site: "Apex Lifestyle Lab",
      host: "10.7.15.70",
      scheme: "https"                   # https par défaut
    }
  ]
```

Réseau : RAN Monitor → cellule Baicells **TCP sortant 443**. Aucun port entrant n'est nécessaire (modèle de sondage).

Interface Web

État Baicells (`/baicells/status`) — une carte par cellule avec accessibilité, cellule active/inactive, synchronisation (`DISP` = synchronisé), GPS, OMC/ACS, WAN, UE actifs, DL/UL throughput, RSSI UL, EARFCN/PCI, puissance TX max, points écrits, et une liste de toutes les alarmes actives (avec gravité). Se rafraîchit automatiquement toutes les 5s.

Il n'y a **pas de page de filtre de compteur** pour Baicells — elle émet ~13 métriques fixes, donc il n'y a rien à élaguer (contrairement aux ~1065 compteurs de Casa).

Vérification

```
# Lecture directe fsmoam (ce que fait le collecteur) — pas
d'authentification :
curl -sk "https://10.7.15.70/fsmoam/get.0x08010005.0?
ModuleType:+SoftwareVersion:+SerialNumber"

# Données dans InfluxDB :
influx -database 'nokia-monitor' \
  -execute 'SELECT last("counterValue") FROM
"BaicellsPerformanceMetrics" GROUP BY "metricCounter"'
```

Ou regardez les journaux : `[Baicells.Scheduler] <name> (<host>): up=<bool> ue=<n> wrote <N> metric(s)`, et vérifiez la page **État Baicells**.

> Remarque : si la cellule est mal configurée/non en service (par exemple, plage `phyCellId` invalide → `cellUnavailableAlarm`), les jauges UE/throughput/RSSI en direct restent vides et seules les séries d'état `CELL.*` + alarmes sont écrites — par conception.

Documentation Connexe

- **Collection PM Casa** — fournisseur basé sur le push (et le guide "ajouter un fournisseur")
- **Prise en main** — déploiement initial
- **Intégration Grafana** — tableaux de bord
- **Guide des opérations** — aperçu opérationnel

Collection Casa PM

Ingestion de métriques de performance et gestion de flotte pour les femtocells Casa Systems

RAN Monitor est multi-fournisseur. Les eNB Casa Systems sont pris en charge aux côtés de Nokia AirScale et Baicells. Les femtocells Casa **s'auto-enregistrent** — une cellule s'annonce simplement en poussant des PM, et RAN Monitor apprend son identité (numéro de série) et l'adresse IP de gestion à partir de cette poussée. À partir de là, il peut également gérer l'unité via SSH (sauvegarde de configuration, accessibilité et poussée de la configuration de rapport PM). Ce guide couvre la collecte, l'auto-enregistrement, le nommage, la gestion SSH et la vérification.

Table des matières

1. Aperçu
2. Architecture
3. Configuration
4. Auto-enregistrement et nommage
5. Intégration d'une unité (bootstrap KPI)
6. Sauvegarde de configuration
7. Accessibilité
8. Filtrage des compteurs
9. Interface Web
10. API
11. Modèle de données
12. Vérification
13. Dépannage

Aperçu

Les eNB Casa expédient un `kpi_agent` intégré qui produit des fichiers XML PM 3GPP TS 32.435 et **les pousse** via HTTP (multipart, libcurl) vers un `serverURL` configurable. RAN Monitor reçoit ces poussées sur un point de terminaison dédié, enregistre chaque fichier sur disque, et un travailleur en arrière-plan analyse, filtre et écrit les compteurs dans InfluxDB.

Deux choses rendent le pipeline Casa **auto-enregistré** :

- Chaque nom de fichier PM porte le **numéro de série** de l'unité (son identité stable), et l' **adresse IP de gestion** est l'adresse source de la poussée. Ainsi, une cellule qui n'a jamais été configurée apparaît toujours — identifiée par le numéro de série, avec son IP apprise — au moment où elle pousse.
- Parce que le numéro de série + IP sont connus, RAN Monitor peut également atteindre l'unité via SSH pour sauvegarder sa configuration, vérifier l'accessibilité, et pousser la configuration de rapport PM (intégration). Les algorithmes SSH hérités requis par ces unités sont gérés automatiquement.

Les opérateurs ajoutent un **nom / site / ECID** convivial en tant que métadonnées identifiées par le numéro de série — le numéro de série ne change jamais même si l'IP de l'unité change.

Faits clés :

Élément	Valeur
Point de terminaison d'ingestion	`http://<ran-monitor>:9077/api/casa/pm/upload`
Transport (PM)	HTTP multipart POST (Casa `kpi_agent`)
Transport (mgmt)	SSH (Erlang `:ssh`, algorithmes Dropbear hérités)
Format PM	3GPP TS 32.435 (seaux de 60s)
Répertoire de spool	`/var/lib/ran_monitor/casa_pm_spool`
Mesure InfluxDB	`CasaPerformanceMetrics`
Clé de cellule	**numéro de série** (analysé à partir du nom de fichier PM)
IP de gestion	apprise à partir de l'adresse source de la poussée
Magasin d'enregistrement	`priv/casa_cell_registry.etf` (persisté)
Sauvegardes de configuration	`priv/casa_configs/<serial>/` (versionnées)

Architecture

```
Casa eNB kpi_agent
   │  HTTP multipart POST (32.435 PM XML)
   ▼
RanMonitor.Web.Casa.Endpoint            (port 9077)
   └─ Router → PmController.upload
        │  parse serial from filename, learn mgmt IP from source
addr
        ├─ RanMonitor.Casa.CellRegistry   record serial → mgmt IP
(self-register)
        ▼
RanMonitor.Casa.PmSpool
/var/lib/ran_monitor/casa_pm_spool
        ▼
RanMonitor.Casa.PmSpoolWorker            (polls every 1s)
   ├─ RanMonitor.Casa.PmParser           32.435 → point maps
(drops empty tags)
   ├─ RanMonitor.Casa.PmFilterStore      keep only selected
counters
   └─ RanMonitor.EnhancedInfluxDbConnection → InfluxDB
"CasaPerformanceMetrics"

Gestion SSH (RanMonitor.Casa.Ssh — Erlang :ssh, algorithmes
hérités) :
   ├─ RanMonitor.Casa.ConfigBackup       sauvegarde périodique
femtoconfig.ini → ConfigStorage
   ├─ RanMonitor.Casa.Reachability       sonde SSH échelonnée →
CellRegistry
   └─ RanMonitor.Casa.KpiBootstrap       pousse kpi_agent.ini +
redémarre (intégration)
```

Référence de module (`lib/ran_monitor/casa/`) :

Module	Responsabilité
`pm_spool.ex` / `pm_spool_worker.ex`	Spool disque ; vider → analyser → filtrer → écrire
`pm_parser.ex`	analyseur 32.435 → cartes de points InfluxDB (omet les balises de valeur vide)
`cell_registry.ex`	Magasin d'auto-enregistrement : numéro de série → IP de gestion + annotations nom/site/ECID, persisté
`ssh.ex`	Aide SSH via Erlang `:ssh` avec algorithmes Dropbear hérités
`config_storage.ex` / `config_backup.ex`	Sauvegarde versionnée de `femtoconfig.ini` via SSH
`reachability.ex`	Sonde d'accessibilité SSH en arrière-plan échelonnée
`kpi_bootstrap.ex`	Pousse la configuration de rapport PM `kpi_agent.ini` à une unité + redémarre
`pm_filter_store.ex`	Magasin ETS + disque des compteurs à conserver

Configuration

Le chemin d'ingestion PM nécessite **aucune configuration par cellule** — les cellules s'auto-enregistrent. La configuration fournit le point de terminaison, les identifiants de gestion et des semences de métadonnées optionnelles.

Configuration de gestion (clés de niveau supérieur séparées)

```
# config/config.exs — valeurs par défaut ; remplacer les éléments
spécifiques au déploiement dans runtime.exs
config :ran_monitor, :casa_ssh,
  username: "root", password: "<casa-root-pw>", port: 22,
connect_timeout_ms: 15_000

config :ran_monitor, :casa_monitor_ip, "10.4.2.250"   # hôte
serverURL pour le bootstrap
config :ran_monitor, :casa_backup, enabled: true, interval_ms:
3_600_000
config :ran_monitor, :casa_reachability, enabled: true,
interval_ms: 600_000, stagger_ms: 3_000
```

> Ceux-ci vivent sous **clés de niveau supérieur séparées**, pas imbriquées sous `:casa`, intentionnellement : `runtime.exs` définit `config :ran_monitor, casa: %{cells: [...]}` comme une **carte**, qui remplace toute la valeur `:casa` — tout ce qui est imbriqué là serait effacé. Gardez la configuration de gestion en dehors de `:casa`.

Cellules (semence de métadonnées optionnelle)

`config :ran_monitor, :casa, cells:` est maintenant **optionnel**. Les entrées sont des semences de métadonnées correspondant au numéro de série ; la source durable de vérité est l'ensemble d'annotations par numéro de série défini à partir de l'UI/API (voir ci-dessous). `mcc`/`mnc` proviennent du bloc partagé `general: %{mcc: "313", mnc: "380"}`.

Réseau / pare-feu

- Casa eNB → RAN Monitor : **TCP entrant 9077** (poussée PM)
- RAN Monitor → Casa eNB : **TCP sortant 22** (gestion SSH)
- RAN Monitor → InfluxDB : sortant 8086

Auto-enregistrement et nommage

Lorsqu'une unité pousse des PM, `CellRegistry` enregistre `serial → {mgmt IP, first seen, last push}` et le persiste. La cellule apparaît immédiatement sur la page de statut, signalée comme **non configurée** jusqu'à ce qu'elle soit nommée.

Le nommage est une **annotation identifiée par le numéro de série** — durable même si l'IP de l'unité change (le numéro de série ne change jamais). Chaque annotation contient :

- **nom** — nom convivial (par exemple `DUTB41CASA03`)
- **site** — emplacement / client (par exemple `Ptarmigan Road, Unalaska AK 99685`)
- **ECID** — l'identifiant de cellule E-UTRAN du plan RF (l'identifiant unique par cellule)

Définissez-les à partir du bouton **Nom** de la page de statut, ou de l'API :

```
PUT /api/casa/cells/<serial>
{ "name": "DUTB41CASA03", "site": "Ptarmigan Road...", "enb_id":
"43573" }
```

L'IP de gestion est affichée dans l'UI afin que vous puissiez reconnaître quelle unité physique un numéro de série fraîchement découvert correspond (croisez votre plan RF par IP), puis nommez-la en fonction du numéro de série.

Intégration d'une unité (bootstrap KPI)

Une unité qui n'a jamais rapporté n'a pas de `serverURL` défini. Pour la pointer vers ce moniteur, utilisez **Définir les paramètres KPI** sur la page de statut (ou l'API) avec l'IP de l'unité. RAN Monitor se connecte en SSH, sauvegarde le `kpi_agent.ini` existant, écrit les cinq tâches standard pointant vers `http://<monitor-ip>:9077/api/casa/pm/upload`, et redémarre l'agent.

```
POST /api/casa/bootstrap
{ "ip": "10.101.16.22" }          # ou { "serial": "<serial>" }
pour réutiliser une IP apprise
```

> **Remarque de redémarrage :** le `kpi_agent` n'a pas de superviseur, et l'arrêt de celui-ci déclenche le watchdog de l'unité en un redémarrage d'environ 1 minute, qui relit la nouvelle configuration à partir de la partition `/config` persistante. L'intégration redémarre donc brièvement la cellule. Après son retour, elle pousse des PM et s'auto-enregistre dans un délai d'environ 2 minutes.

L'équivalent manuel, si vous configurez l'unité directement, consiste à définir le `kpi_agent` `serverURL` sur le point de terminaison ci-dessus. Le nom de fichier PM porte le numéro de série comme son dernier jeton délimité par un underscore (`..._Accessibility_<serial>.xml`), ce qui est comment la cellule est identifiée.

Sauvegarde de configuration

`ConfigBackup` se connecte périodiquement à chaque unité connue et stocke son `/config/l3/femtoconfig.ini` via `ConfigStorage` — versionné et uniquement en cas de changement (une nouvelle version est écrite uniquement lorsque le contenu change), sous `priv/casa_configs/<serial>/`. Déclenchez une sauvegarde immédiate depuis la page de statut (**Sauvegarder**) ou `POST /api/casa/configs/<serial>/backup` ; visualisez le fichier actuel en ligne (**Voir**) ou récupérez les versions via l'API.

Accessibilité

`Reachability` exécute une sonde SSH en arrière-plan échelonnée de chaque unité connue et enregistre `reachable` / `last_probe` dans le registre, de sorte que la page de statut/API signale les unités qui sont devenues inactives (poussant mais inaccessibles via SSH, ou hors ligne). L'intervalle et l'échelonnement sont configurés sous `:casa_reachability`.

Filtrage des compteurs

Casa émet environ 1065 compteurs à travers cinq tâches PM (Accessibilité, Mobilité, Intégrité, Utilisation du système, Disponibilité). Seuls les compteurs dans l'ensemble **stocké** sont écrits dans InfluxDB ; les autres sont comptés et abandonnés.

- **Catalogue complet :** `priv/casa_pm_metrics.csv`
- **Valeurs par défaut :** `priv/casa_pm_counters.csv`
- **État en direct :** ETS, persisté dans `priv/casa_pm_filters.etf`

Gérez l'ensemble depuis la page **Filtres de données Casa**. Les modifications persistent et prennent effet lors du prochain fichier PM traité. Le filtre correspond à la balise `metricCounter`.

Interface Web

Statut Casa (`/casa/status`)

Piloté par le registre (cellules auto-enregistrées), par cellule :

- Statut PM (Actif / Inactif / Obsolète par dernière écriture) et points écrits / dernier PM
- nom / numéro de série / ECID, site, IP de gestion apprise
- badge d'accessibilité SSH (accessible / inaccessible / inconnu)
- nombre de sauvegardes de configuration + dernier temps de sauvegarde
- actions : **Nom** (définir nom/site/ECID), **Sauvegarder**, **Voir** (configuration en ligne)
- haut de page : formulaire **Définir les paramètres KPI** pour intégrer une unité par IP

Les cellules sans annotation sont signalées comme `non configurées`.

Filtres de données Casa (`/casa/pm-filters`)

Ajouter/retirer l'interface utilisateur pour choisir quels compteurs sont stockés.

API

Toujours disponible (indépendamment du basculement de navigation de l'UI) :

Méthode + chemin	But
`GET /api/casa/devices`	Cellules avec statut PM (reflète la page de statut)
`GET /api/casa/cells`	Cellules auto-enregistrées : numéro de série, IP de gestion, accessibilité, nom/site/ECID
`PUT /api/casa/cells/:serial`	Définir/modifier nom, site, ECID (identifié par numéro de série)
`GET /api/casa/configs`	Unités avec comptes de versions de sauvegarde
`GET /api/casa/configs/:serial`	Liste des versions pour une unité
`GET /api/casa/configs/:serial/current`	Télécharger la femtoconfig actuelle
`POST /api/casa/configs/:serial/backup`	Sauvegarder une unité maintenant
`POST /api/casa/bootstrap`	Pousser la configuration PM à une unité (`ip` ou `serial`) et redémarrer

---

Modèle de données

Chaque `(compteur, seau de 60s)` devient un point InfluxDB dans `CasaPerformanceMetrics` :

```
fields:  counterValue (float), measurementStart, measurementStop
(ISO8601)
tags:    metricCounter, metricJob, enbName, enbId, metricInterval,
         metricMcc, metricMnc, vendor="Casa",
recordType="performanceMetric"
         (site / host uniquement lorsque la cellule a cette
métadonnée)
timestamp: start-of-bucket (ns)
```

> **Les balises vides sont abandonnées.** Le protocole de ligne InfluxDB rejette une valeur de balise vide (`missing tag value`) et échoue tout le lot d'écriture. Une cellule auto-enregistrée sans métadonnées site/hôte émettrait autrement `site=`/`host=` ; le parseur omet toute balise de valeur vide afin que ces écritures réussissent.

Casa partage la base de données InfluxDB `nokia-monitor` avec un nom de mesure distinct afin que les fournisseurs ne se chevauchent jamais.

Vérification

```
# Sur le nœud en cours d'exécution — cellules auto-enregistrées +
points
bin/ran_monitor rpc 'RanMonitor.Casa.CellRegistry.all() |>
Enum.each(fn c ->
  {pts, _} =
RanMonitor.Database.InfluxDbStats.get_stats("CasaPerformanceMetrics",
c.serial)
  IO.puts("#{c.name || c.serial}  ip=#{c.mgmt_ip}  pts=#{pts}
reachable=#{inspect c.reachable}")
end)'
```

Journaux à attendre après une poussée :

```
[Casa.PmController] Poussée PM acceptée : 1 fichier(s) mis en
spool
[Casa.PmSpoolWorker] Traité <file>: <N> points écrits, <M> filtrés
```

Ou regardez les **Points Écrits** / **Dernier PM** de la cellule avancer sur la page de statut.

Dépannage

Points écrits = 0, `... N filtrés`, et le journal d'écriture montre un 400
Le lot a été rejeté par InfluxDB. Historiquement, cela était dû à `missing tag value` d'une balise `site=`/`host=` vide sur une cellule non configurée — le parseur abandonne maintenant les balises vides, donc assurez-vous que la version en cours d'exécution inclut cette correction.

Points écrits = 0 mais fichiers traités > 0 (pas d'erreur d'écriture)
Chaque compteur dans ce fichier a été filtré. Ajoutez les compteurs que vous souhaitez sur la page **Filtres de données Casa**.

La cellule affiche `non configurée` Elle s'est auto-enregistrée mais n'a pas été nommée. Utilisez le bouton **Nom** (ou `PUT /api/casa/cells/:serial`) pour définir nom/site/ECID par rapport à son numéro de série.

L'accessibilité affiche `inaccessible` mais la cellule pousse des PM La poussée PM (unité → :9077) et SSH (moniteur → :22) sont dans des directions opposées. L'unité peut pousser tout en refusant/bloquant SSH, ou être sur un segment que le moniteur ne peut pas atteindre en sortie. La sauvegarde/l'intégration nécessite le chemin SSH.

Intégration : l'unité ne commence pas à rapporter après le bootstrap
Le bootstrap redémarre l'agent via un redémarrage du watchdog (~1 min). Confirmez que l'unité est revenue et peut atteindre `<monitor-ip>:9077`. Vérifiez `bin/ran_monitor rpc` pour le numéro de série apparaissant dans `CellRegistry.all()`.

Fichiers s'accumulant dans le spool / sous-répertoire `failed/` Vérifiez les journaux du travailleur. Les fichiers non analysables sont déplacés vers `/var/lib/ran_monitor/casa_pm_spool/failed/` plutôt que supprimés.

Documentation Connexe

- **Prise en main** — déploiement initial
- **Collection Baicells** — Baicells (basé sur sondage)
- **Collecte de données PM** — pipeline PM Nokia
- **Guide de configuration d'exécution** — référence de configuration
- **Intégration Grafana** — tableaux de bord

Guide d'Archivage de Configuration

Versioning Automatisé et Suivi Historique pour les Configurations AirScale

---

Vue d'ensemble

Le système d'Archivage de Configuration suit et versionne automatiquement tous les fichiers de configuration des stations de base AirScale. Au lieu de stocker des instantanés de configuration dans InfluxDB, les configurations sont enregistrées sous forme de fichiers XML horodatés sur le serveur, fournissant une piste d'audit complète des changements de configuration.

Caractéristiques Clés

- **Versioning Automatique** - Nouvelles versions créées uniquement lorsque des changements de configuration
- **Interrogation Horaire** - Vérifie les changements de configuration toutes les heures (configurable)
- **Détection de Changements** - Comparaison intelligente détecte les changements réels, ignorant les espaces
- **Limites Basées sur la Taille** - Stockage maximum de 100 Mo par appareil (garde ~690 versions)
- **Interface Web** - Parcourir, télécharger et gérer les versions de configuration
- **Accès Rapide** - Stockage basé sur des fichiers pour une récupération instantanée
- **Aucune Charge InfluxDB** - Configurations non stockées dans la base de données de séries temporelles
- **Nettoyage Automatique** - Anciennes versions supprimées lorsque la limite de taille est atteinte

Comment Ça Fonctionne

Planification de l'Interrogation

La configuration est interrogée depuis chaque station de base AirScale enregistrée :

- **Intervalle :** Toutes les 1 heure (par défaut)
- **Première Interrogation :** Immédiatement au démarrage de l'application
- **Détection de Changements :** Compare le contenu avec la version précédente
- **Stockage :** N'enregistre que si changé ou première fois

Emplacement de Stockage

Les configurations sont stockées sur le système de fichiers du serveur RAN Monitor :

```
priv/airscale_configs/
└── <airscale-name>/
    ├── current.xml                                    #
Configuration la plus récente
    ├── ONS-Lab-Airscale_config_20251230_143522.xml   # Version du
30 déc, 14h35
    ├── ONS-Lab-Airscale_config_20251229_120000.xml   # Version
précédente
    ├── ONS-Lab-Airscale_config_20251228_093045.xml   # Version
plus ancienne
    └── ...                                            # Versions
conservées jusqu'à la limite de 100 Mo
```

Format de Nom de Fichier : `<AirScaleName>_config_YYYYMMDD_HHMMSS.xml`

Nommage de Répertoire : Les noms AirScale sont assainis (caractères spéciaux remplacés par des underscores, en minuscules)

Gestion des Versions

- **Dernière Version :** Toujours disponible sous `current.xml`
- **Versions Historiques :** Fichiers horodatés montrant quand la configuration a changé
- **Auto-Nettoyage :** Supprime les versions les plus anciennes lorsque la limite de taille de 100 Mo est atteinte
- **Nettoyage Manuel :** Supprimer des versions spécifiques via l'interface Web (sauf `current.xml`)
- **Protection de Stockage :** Limite basée sur la taille empêche une utilisation illimitée du disque
- **Rétention Flexible :** Plus de versions si les fichiers sont petits, moins si les fichiers sont grands

---

Protection de Stockage

Limite de Stockage Basée sur la Taille

Pour éviter une utilisation illimitée du disque, le système utilise une **limite basée sur la taille** au lieu d'un compte de versions :

- **Taille Maximale :** 100 Mo par appareil (configurable)
- **Nettoyage Automatique :** Les versions les plus anciennes sont supprimées lorsque la limite de taille est dépassée
- **Moment de Nettoyage :** Chaque fois qu'une nouvelle version de configuration est enregistrée
- **Fichiers Protégés :** `current.xml` et au moins une version toujours conservée
- **Flexible :** Garde ~690 versions à 145 Ko chacune, plus si les fichiers sont plus petits

Comment Ça Fonctionne

Lorsqu'une nouvelle version de configuration est enregistrée :

1. **Enregistrer nouvelle version** - Configuration écrite sous `<AirScale>_config_YYYYMMDD_HHMMSS.xml`
2. **Mettre à jour current** - `current.xml` mis à jour avec la dernière configuration
3. **Calculer la taille** - Le système additionne la taille totale de tous les fichiers versionnés
4. **Nettoyer les anciens** - Si total > 100 Mo, supprimer les versions les plus anciennes jusqu'à ce que cela soit sous la limite
5. **Journaliser l'activité** - Suppressions enregistrées avec l'espace libéré

Scénario d'Exemple

```
État initial : 95 Mo utilisés (655 versions à 145 Ko chacune)
├── ONS-Lab-Airscale_config_20240101_100000.xml  <- La plus
ancienne (145 Ko)
├── ONS-Lab-Airscale_config_20240102_100000.xml  (145 Ko)
├── ... (653 autres versions)
└── ONS-Lab-Airscale_config_20251230_100000.xml  <- La plus
récente (145 Ko)

Nouvelle configuration détectée le 2025-12-31 10:00:00 (145 Ko)

Actions :
1. Enregistrer : ONS-Lab-Airscale_config_20251231_100000.xml (145
Ko)
2. Taille totale maintenant : 95 Mo + 145 Ko = 95,14 Mo (toujours
sous la limite de 100 Mo)
3. Aucune suppression nécessaire
4. Final : 656 versions, 95,14 Mo utilisés

---

Plus tard : Changement de configuration important (nouvelles
fonctionnalités ajoutées, le fichier est maintenant de 500 Ko)

Actions :
1. Enregistrer : ONS-Lab-Airscale_config_20251231_150000.xml (500
Ko)
2. Taille totale maintenant : 95,14 Mo + 500 Ko = 95,64 Mo
(toujours sous la limite)
3. Aucune suppression nécessaire
4. Final : 657 versions, 95,64 Mo utilisés

---

Après de nombreux autres changements : Approche de la limite

État actuel : 99,8 Mo (685 versions)

Nouvelle configuration : 200 Ko
1. Enregistrer nouvelle version
2. Total serait : 100 Mo (dépasse la limite)
3. Supprimer les versions les plus anciennes jusqu'à ce que le
```

```
total < 100 Mo
4. Suppressions enregistrées : "Supprimé 3 versions, libéré 435
Ko"
5. Final : 682 versions, 99,6 Mo utilisés
```

Garanties de Stockage

Le nettoyage automatique garantit :

- **Stockage Limité :** Chaque appareil limité à 100 Mo maximum
- **Pas de Surprises :** Le stockage ne croîtra pas indéfiniment
- **Sécurisé en Production :** Aucune intervention manuelle requise
- **Historique Flexible :** Plus de versions pour de petites configurations, moins pour de grandes configurations
- **Toujours Disponible :** Au moins une version toujours conservée

Surveillance du Stockage

Vérifiez l'utilisation du stockage pour tous les appareils :

```
# Total de stockage utilisé
du -sh priv/airscale_configs/
# Exemple : 215M (pour 3 appareils avec une moyenne de 70 Mo
chacun)

# Stockage par appareil
du -sh priv/airscale_configs/*/
# Exemple :
# 95M     priv/airscale_configs/ons-lab-airscale/
# 68M     priv/airscale_configs/sector-1/
# 52M     priv/airscale_configs/sector-2/

# Vérifiez si un appareil est proche de la limite
find priv/airscale_configs -maxdepth 1 -type d -exec du -sm {} \;
| awk '$1 > 90 {print $2 " est à " $1 "Mo (approchant la limite de
100Mo)"}'
```

Utilisation de la Page d'Archivage de Configuration

Accéder à l'Archivage de Configuration

Interface Web : Naviguez vers **Nokia → Archivage de Configuration**

URL : `https://<ran-monitor-ip>:9443/nokia/config-archive`

L'interface d'Archivage de Configuration montrant le sélecteur de station de base, le tableau d'historique des versions avec des horodatages et des tailles de fichiers, et des informations de stockage.

Vue d'Ensemble de l'Interface

La page d'Archivage de Configuration a trois sections principales :

1. Sélecteur de Station de Base

- **Vue Grille** - Montre tous les appareils AirScale enregistrés
- **Nombre de Versions** - Nombre de versions de configuration stockées pour chacun
- **Sélection** - Cliquez sur un appareil pour voir son historique de configuration
- **Indicateur Visuel** - L'appareil sélectionné est mis en surbrillance en bleu

2. Tableau d'Histoire des Versions

Affiche toutes les versions de configuration pour la station de base sélectionnée :

Colonne	Description
Horodatage	Quand la configuration a été enregistrée (UTC)
Nom de Fichier	Nom de fichier de version (par exemple, `config_20251230_143522.xml`)
Taille	Taille du fichier en Ko ou Mo
Âge	Depuis combien de temps la version a été créée (par exemple, "il y a 2h", "il y a 3j")
Actions	Boutons Télécharger ou Supprimer

Tri : Les versions les plus récentes apparaissent en premier (décroissant par horodatage)

Configuration Actuelle : Le fichier `current.xml` ne peut pas être supprimé (mesure de sécurité)

3. Informations de Stockage

Panneau récapitulatif montrant :

- **Total des Versions** - Nombre de versions de configuration stockées
- **Taille Totale** - Taille combinée de toutes les versions

- **Chemin de Stockage** - Emplacement du système de fichiers sur le serveur

---

Opérations Courantes

Télécharger une Configuration

Objectif : Récupérer une version spécifique de configuration pour révision, sauvegarde ou comparaison

Étapes :

1. Naviguez vers la page d'Archivage de Configuration
2. Sélectionnez la station de base souhaitée
3. Trouvez la version que vous souhaitez dans le tableau
4. Cliquez sur le bouton **Télécharger**
5. Le fichier se télécharge avec le format : `<AirScaleName>_config_YYYYMMDD_HHMMSS.xml` (correspond au nom de fichier stocké)

Cas d'Utilisation :

- Création de sauvegardes hors ligne
- Comparaison des configurations entre les horodatages
- Rétrogradation vers une configuration précédente connue
- Analyse de la dérive de configuration au fil du temps

Supprimer des Anciennes Versions

Objectif : Supprimer des versions de configuration obsolètes pour libérer de l'espace de stockage

Étapes :

1. Naviguez vers la page d'Archivage de Configuration

2. Sélectionnez la station de base
3. Trouvez la version à supprimer
4. Cliquez sur le bouton **Supprimer**
5. Confirmez la suppression dans la boîte de dialogue contextuelle
6. La version est définitivement supprimée

Notes Importantes :

- Ne peut pas supprimer `current.xml` (version la plus récente protégée)
- La suppression est immédiate et ne peut pas être annulée
- La suppression manuelle n'affecte pas les paramètres de nettoyage automatique

Comparer des Configurations

Objectif : Identifier ce qui a changé entre deux versions de configuration

Comparaison Manuelle :

1. Téléchargez les deux versions que vous souhaitez comparer
2. Utilisez un outil de différence XML (par exemple, `xmldiff`, `Beyond Compare`, `WinMerge`)
3. Examinez les différences pour comprendre les changements

Exemple utilisant la ligne de commande :

```
# Télécharger les deux versions
wget https://<server>:9443/download/config/ONS-Lab-Airscale/ONS-
Lab-Airscale_config_20251230_143522.xml
wget https://<server>:9443/download/config/ONS-Lab-Airscale/ONS-
Lab-Airscale_config_20251229_120000.xml

# Comparer avec diff
diff ONS-Lab-Airscale_config_20251229_120000.xml ONS-Lab-
Airscale_config_20251230_143522.xml

# Ou utilisez xmldiff pour une sortie plus propre
xmldiff ONS-Lab-Airscale_config_20251229_120000.xml ONS-Lab-
Airscale_config_20251230_143522.xml
```

Flux de Travail de Gestion de Configuration

Enquête sur la Piste d'Audit

Scénario : Besoin de déterminer quand une configuration a changé

Étapes :

1. Ouvrir l'Archivage de Configuration
2. Sélectionner la station de base concernée
3. Examiner les horodatages des versions
4. Télécharger les versions pertinentes
5. Comparer pour identifier les changements exacts
6. Corréler avec des problèmes de performance ou des alarmes

Exemple :

```
Chronologie des Versions :
- ONS-Lab-Airscale_config_20251230_143522.xml (143 Ko) - La plus
récente
- ONS-Lab-Airscale_config_20251228_091045.xml (142 Ko) - Il y a 2
jours
- ONS-Lab-Airscale_config_20251225_180000.xml (142 Ko) - Il y a 5
jours

Analyse :
- La taille a augmenté de 142 Ko à 143 Ko le 30 déc
- Comparer le 28 déc vs le 30 déc pour trouver ce qui a été ajouté
- Vérifier si le timing correspond à un pic d'alarme
```

Rétrogradation de Configuration

Scénario : Un changement de configuration récent a causé des problèmes, besoin de restaurer la version précédente

Étapes :

1. Identifier la version de configuration connue comme bonne
2. Télécharger cette version depuis l'Archivage de Configuration
3. Naviguer vers la page de Gestion de Configuration (Interface Web)
4. Télécharger la configuration téléchargée → recevoir l'ID de Plan
5. Valider le plan → vérifier les erreurs
6. Si la validation réussit, activer le plan
7. Surveiller l'appareil pour la stabilité
8. Vérifier que la nouvelle configuration apparaît dans l'archive après la prochaine interrogation

Liste de Vérification de Sécurité :

- ✓ Version précédente correcte téléchargée
- ✓ Plan validé avant activation
- ✓ Coordination avec l'équipe des opérations
- ✓ Planifié pendant la fenêtre de maintenance
- ✓ Outils de surveillance prêts pour vérification

Gestion de Configuration de Base

Scénario : Maintenir une "configuration dorée" pour la standardisation

Meilleure Pratique :

1. Créer et valider la configuration de base
2. Appliquer à l'appareil de référence
3. Télécharger depuis l'Archivage de Configuration après la prochaine interrogation
4. Stocker externement comme modèle
5. Utiliser pour déployer de nouveaux appareils
6. Réviser et mettre à jour périodiquement la base

Détails Techniques

Algorithme de Détection de Changements

Le système utilise une comparaison de contenu intelligente pour éviter les faux positifs :

Processus de Normalisation :

1. Supprimer les espaces en début/fin
2. Réduire les espaces entre les balises XML
3. Normaliser les espaces internes
4. Comparer le contenu normalisé résultant

Avantages :

- Les changements de format ne déclenchent pas de nouvelles versions
- Seuls les changements réels de configuration créent des versions
- Réduit les besoins de stockage
- Fournit un historique de changement significatif

Exemple :

```
<!-- Ceux-ci sont considérés comme identiques -->

<!-- Version 1 (avec espaces supplémentaires) -->
<parameter>
    <name>cellId</name>
    <value>1</value>
</parameter>

<!-- Version 2 (compact) -->
<parameter><name>cellId</name><value>1</value></parameter>
```

Exigences de Stockage

Taille Typique de Configuration : ~145 Ko par version (basé sur des configurations AirScale réelles)

Planification de Capacité :

Appareils	Taille Max par Appareil	Versions Conservées (à 145 Ko)	Stockage Total Max
10	100 Mo	~690	1 Go
50	100 Mo	~690	5 Go
100	100 Mo	~690	10 Go
500	100 Mo	~690	50 Go
1000	100 Mo	~690	100 Go

Caractéristiques de Croissance :

- **Stockage maximum par appareil :** 100 Mo (configurable)
- **Versions typiques conservées :** ~690 (145 Ko chacune)

- **Si la configuration ne change jamais :** Croissance minimale (seulement current.xml à 145 Ko)
- **Si la configuration change fréquemment :** La croissance s'arrête à la limite de 100 Mo
- **Adaptatif :** Garde plus de versions pour de petites configurations, moins pour de grandes configurations

Protection Automatique :

- Anciennes versions supprimées lorsque la limite de taille est atteinte
- Aucune intervention manuelle nécessaire
- Utilisation de stockage strictement limitée par appareil
- Au moins une version toujours conservée

Politique de Rétention

Paramètres par Défaut :

- Stockage maximum de **100 Mo** par appareil
- Suppression automatique des versions les plus anciennes lorsque la limite est dépassée
- `current.xml` toujours conservé (exempt de nettoyage)
- Nettoyage se produit chaque fois qu'une nouvelle version est enregistrée
- Au moins un fichier versionné toujours conservé

Personnalisation de la Rétention :

La limite de stockage par défaut est de 100 Mo par appareil. Elle peut être ajustée à d'autres limites, par exemple 50 Mo (garde ~345 versions) ou 200 Mo (garde ~1380 versions). Contactez le support Omnitouch pour changer la limite de rétention, puis redémarrez RAN Monitor pour appliquer le changement.

Configuration de l'Interrogation

Intervalle par Défaut : 1 heure (3 600 000 millisecondes)

Pour Changer l'Intervalle d'Interrogation :

L'intervalle d'interrogation par défaut est de 1 heure (3 600 000 ms). Contactez le support Omnitouch pour le changer à une autre valeur.

Intervalles Courants :

- 30 minutes : `1_800_000`
- 1 heure : `3_600_000` (par défaut)
- 2 heures : `7_200_000`
- 4 heures : `14_400_000`
- 24 heures : `86_400_000`

Après le changement, recompilez et redémarrez RAN Monitor.

Dépannage

Aucune Version de Configuration Affichée

Symptômes :

- La page d'Archivage de Configuration montre "0 versions"
- L'appareil sélectionné montre un tableau vide

Causes Possibles :

1. **Appareil Non Enregistré**
    - Vérifiez la page des Stations de Base
    - Vérifiez que l'appareil montre le statut "ENREGISTRÉ"
    - Consultez les Journaux d'Application pour les erreurs d'enregistrement
2. **Session Non Active**
    - Vérifiez la vue des détails de l'appareil
    - Assurez-vous que le statut de session est "ACTIF"
    - Consultez les horodatages de session

3. **Configuration Pas Encore Interrogée**
    - Attendez le premier cycle d'interrogation horaire
    - Ou déclenchez manuellement : `Kernel.send(Process.whereis(RanMonitor.Nokia.Airscale.Manager), :get_airscale_config)`
4. **Problèmes de Chemin de Stockage**
    - Vérifiez que le répertoire `priv/airscale_configs/` existe
    - Vérifiez que RAN Monitor a les permissions d'écriture
    - Consultez les Journaux d'Application pour les erreurs de système de fichiers

Le Téléchargement Renvoie une Erreur 404

Symptômes :

- Cliquer sur Télécharger montre "Fichier de configuration non trouvé"
- Le navigateur montre une erreur 404

Causes Possibles :

1. **Incohérence de Chemin de Fichier**
    - Les noms de répertoires sont assainis (minuscules, caractères spéciaux remplacés)
    - Vérifiez le nom réel du répertoire dans `priv/airscale_configs/`
2. **Fichier Supprimé**
    - Vérifiez si le fichier a été supprimé manuellement du système de fichiers
    - Rafraîchissez la page d'Archivage de Configuration pour mettre à jour la liste
3. **Problèmes de Permission**

- Vérifiez que le processus du serveur web peut lire les fichiers de configuration
- Vérifiez les permissions de fichier sur le répertoire de configuration

Résolution :

```
# Vérifiez que le répertoire existe
ls -la priv/airscale_configs/

# Vérifiez que le fichier existe
ls -la priv/airscale_configs/<device-name>/

# Corrigez les permissions si nécessaire
chmod 755 priv/airscale_configs/
chmod 644 priv/airscale_configs/*/*.xml
```

La Configuration Ne Se Met Pas à Jour

Symptômes :

- Seul `current.xml` existe, aucune nouvelle version
- Le compte de versions reste à 1 même après des changements

Causes Possibles :

1. **La Configuration N'a Pas Changé**
   - Le système ne crée des versions que lorsque le contenu change
   - Consultez les journaux : `Configuration inchangée, aucune nouvelle version créée`
2. **L'Interrogation Ne Fonctionne Pas**
   - Vérifiez les Journaux d'Application pour les messages d'interrogation
   - Vérifiez que le processus Manager fonctionne
   - Vérifiez les erreurs lors de la récupération de la configuration
3. **Détection de Changements Trop Stricte**

- Les changements uniquement d'espaces sont ignorés (par conception)
- Vérifiez que les valeurs réelles des paramètres ont changé

Vérification :

```
# Vérifiez les journaux pour l'interrogation de configuration
grep "process_configuration" <log-file>

# Déclenchez manuellement le tirage de configuration
# Dans la console IEx :
Kernel.send(Process.whereis(RanMonitor.Nokia.Airscale.Manager),
:get_airscale_config)
```

Meilleures Pratiques

Sauvegardes Régulières

Recommandation : Créez des sauvegardes externes des configurations critiques

Exemple de Script de Sauvegarde Automatisée :

```
#!/bin/bash
# backup-configs.sh - Sauvegarde quotidienne de configuration vers
un stockage externe

BACKUP_DIR="/backup/ran-monitor/configs"
CONFIG_DIR="priv/airscale_configs"
DATE=$(date +%Y%m%d)

# Créer un répertoire de sauvegarde daté
mkdir -p "$BACKUP_DIR/$DATE"

# Copier toutes les configurations
rsync -av "$CONFIG_DIR/" "$BACKUP_DIR/$DATE/"

# Garder les 30 derniers jours
find "$BACKUP_DIR" -type d -mtime +30 -exec rm -rf {} +

echo "Sauvegarde terminée : $BACKUP_DIR/$DATE"
```

Planifiez avec cron :

```
0 2 * * * /path/to/backup-configs.sh
```

Documentation des Changements

Meilleure Pratique : Documenter pourquoi les configurations ont changé

Processus Suggéré :

1. Avant de faire des changements de configuration, documentez la raison
2. Créez un fichier de journal de changement à côté des configurations
3. Inclure : Date, Appareil, Changements, Justification, Approveur

Exemple de Journal de Changement :

```
# config_changes.log

2025-12-30 14:35:22 - ONS-Lab-Airscale
Changé Par : John Smith
Raison : Augmenter la puissance de cellule pour améliorer la
couverture dans le Secteur 1
Paramètres : txPower changé de 40dBm à 43dBm
Validé : Oui
Activé : 2025-12-30 14:40:00
Résultat : Couverture améliorée, aucune dégradation observée

2025-12-28 09:10:45 - ONS-Lab-Airscale
Changé Par : Jane Doe
Raison : Mettre à jour la liste des cellules voisines après le
déploiement d'un nouveau site
Paramètres : Ajouté cellules voisines 10, 11, 12
Validé : Oui
Activé : 2025-12-28 09:15:00
Résultat : Transferts fonctionnant correctement
```

Surveillance du Stockage

Recommandation : Surveillez l'utilisation du disque périodiquement

Vérifiez l'Utilisation du Stockage :

```
# Taille totale de l'archive de configuration
du -sh priv/airscale_configs/

# Taille par appareil
du -sh priv/airscale_configs/*/

# Nombre de versions par appareil
find priv/airscale_configs/ -name "*.xml" | \
  sed 's|/[^/]*\.xml||' | uniq -c
```

Configurer des Alertes :

- Alerte si la taille totale dépasse un seuil (par exemple, 500 Mo)
- Alerte si un appareil a un nombre de versions anormalement élevé

- Alerte si l'espace disque est inférieur à 10 % libre

Intégration avec la Gestion de Configuration

Le système d'Archivage de Configuration fonctionne aux côtés de la page de Gestion de Configuration :

Intégration des Flux de Travail

Télécharger la Configuration Actuelle :

- Utilisez l'Archivage de Configuration pour obtenir `current.xml`
- Ou utilisez le bouton "Télécharger" de la Gestion de Configuration (déclenche un tirage immédiat)

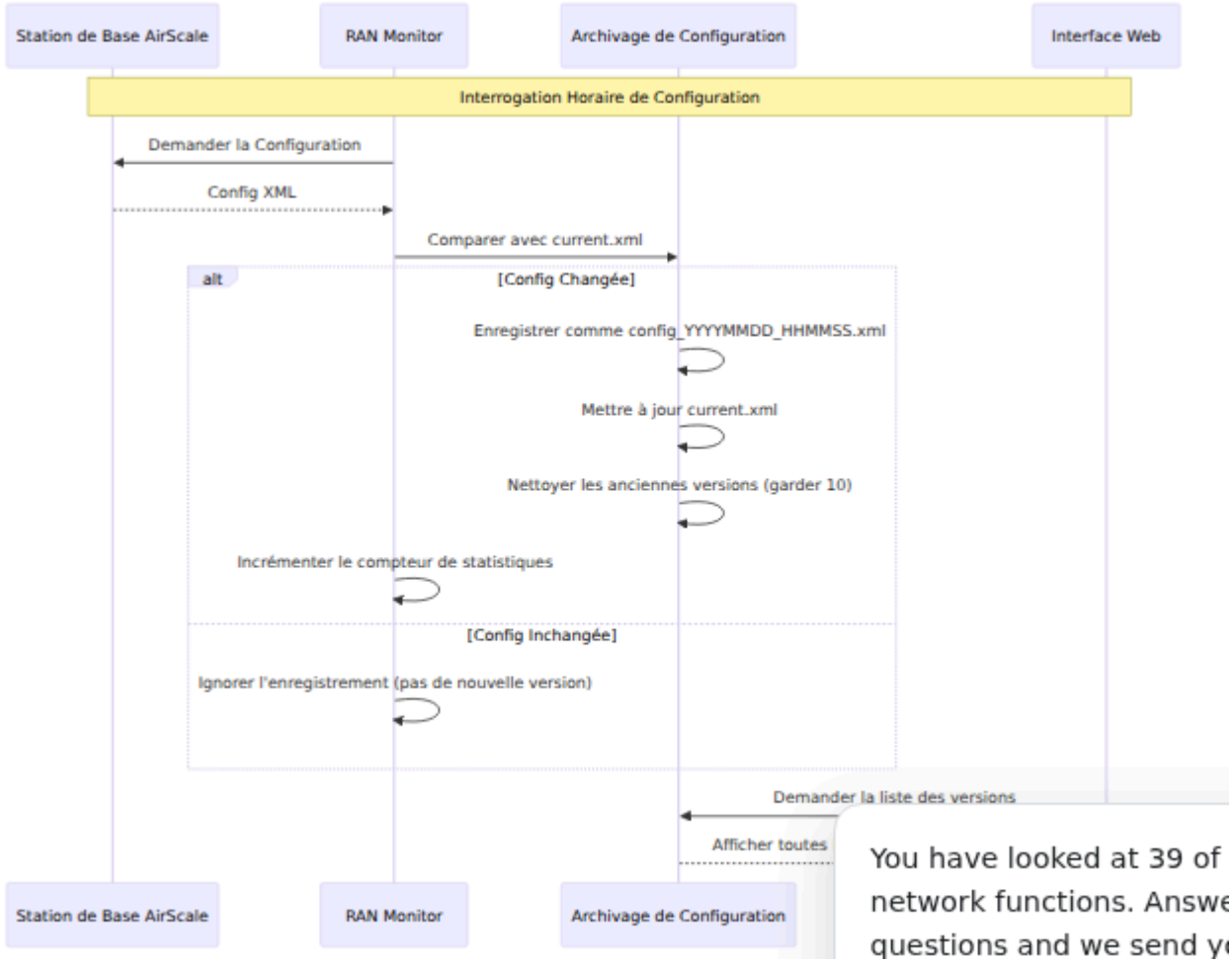
Télécharger une Configuration Modifiée :

- Utilisez la page de Gestion de Configuration
- Télécharger → Valider → Activer le flux de travail
- La nouvelle version apparaît dans l'Archive après la prochaine interrogation

Processus de Rétrogradation :

- Télécharger la version précédente depuis l'Archive
- Télécharger via la Gestion de Configuration
- Suivre le flux de travail Valider → Activer

Flux de Données



Accès API

Bien que l'Archivage de Configuration soit principalement accessible via l'Interface Web, les configurations peuvent également être téléchargées via des requêtes HTTP directes.

Points de Téléchargement

Configuration Actuelle :

```
curl -k "https://<server>:9443/download/config/<airscale-
name>/current.xml" \
  -o current_config.xml
```

Version Spécifique :

```
curl -k "https://<server>:9443/download/config/<airscale-
name>/ONS-Lab-Airscale_config_20251230_143522.xml" \
  -o ONS-Lab-Airscale_config_20251230_143522.xml
```

Remarque : Le nom AirScale dans l'URL doit correspondre au nom de répertoire assaini (minuscules, underscores pour les caractères spéciaux)

Accès Programmatique

Lister les Versions (depuis la console IEx) :

```
# Obtenir toutes les versions pour un appareil
RanMonitor.Nokia.Airscale.ConfigStorage.list_config_versions("ONS-
Lab-Airscale")

# Obtenir le contenu de la configuration actuelle
{:ok, xml} =
RanMonitor.Nokia.Airscale.ConfigStorage.get_current_config("ONS-
Lab-Airscale")

# Vérifier le compte de versions
RanMonitor.Nokia.Airscale.ConfigStorage.count_versions("ONS-Lab-
Airscale")
# Renvoie : 655

# Obtenir le paramètre de taille de stockage max
RanMonitor.Nokia.Airscale.ConfigStorage.max_storage_bytes()
# Renvoie : 104857600 (100 Mo en octets)

# Obtenir l'utilisation actuelle du stockage
RanMonitor.Nokia.Airscale.ConfigStorage.get_storage_usage("ONS-
Lab-Airscale")
# Renvoie : 99614055 (octets)

# Obtenir des statistiques de stockage détaillées
RanMonitor.Nokia.Airscale.ConfigStorage.get_storage_stats("ONS-
Lab-Airscale")
# Renvoie : %{version_count: 655, total_size_bytes: 99614055, ...}

# Nettoyage manuel (garder sous 50 Mo)
RanMonitor.Nokia.Airscale.ConfigStorage.cleanup_old_versions("ONS-
Lab-Airscale", 50 * 1024 * 1024)
# Renvoie : {:ok, 345, 50000000} - supprimé 345 versions, libéré
50 Mo

# Nettoyage en utilisant la valeur par défaut (100 Mo)
RanMonitor.Nokia.Airscale.ConfigStorage.cleanup_old_versions("ONS-
Lab-Airscale")
# Renvoie : {:ok, 0, 0} - aucun nettoyage nécessaire si sous la
limite
```

Voir Aussi

- **Guide de l'Interface Web** - Référence complète du panneau de contrôle
- **Guide de Configuration AirScale** - Configuration de la station de base
- **Guide des Opérations Courantes** - Tâches de gestion quotidiennes
- **Guide de Politique de Rétention des Données** - Gestion du stockage

Guide de Push de Configuration

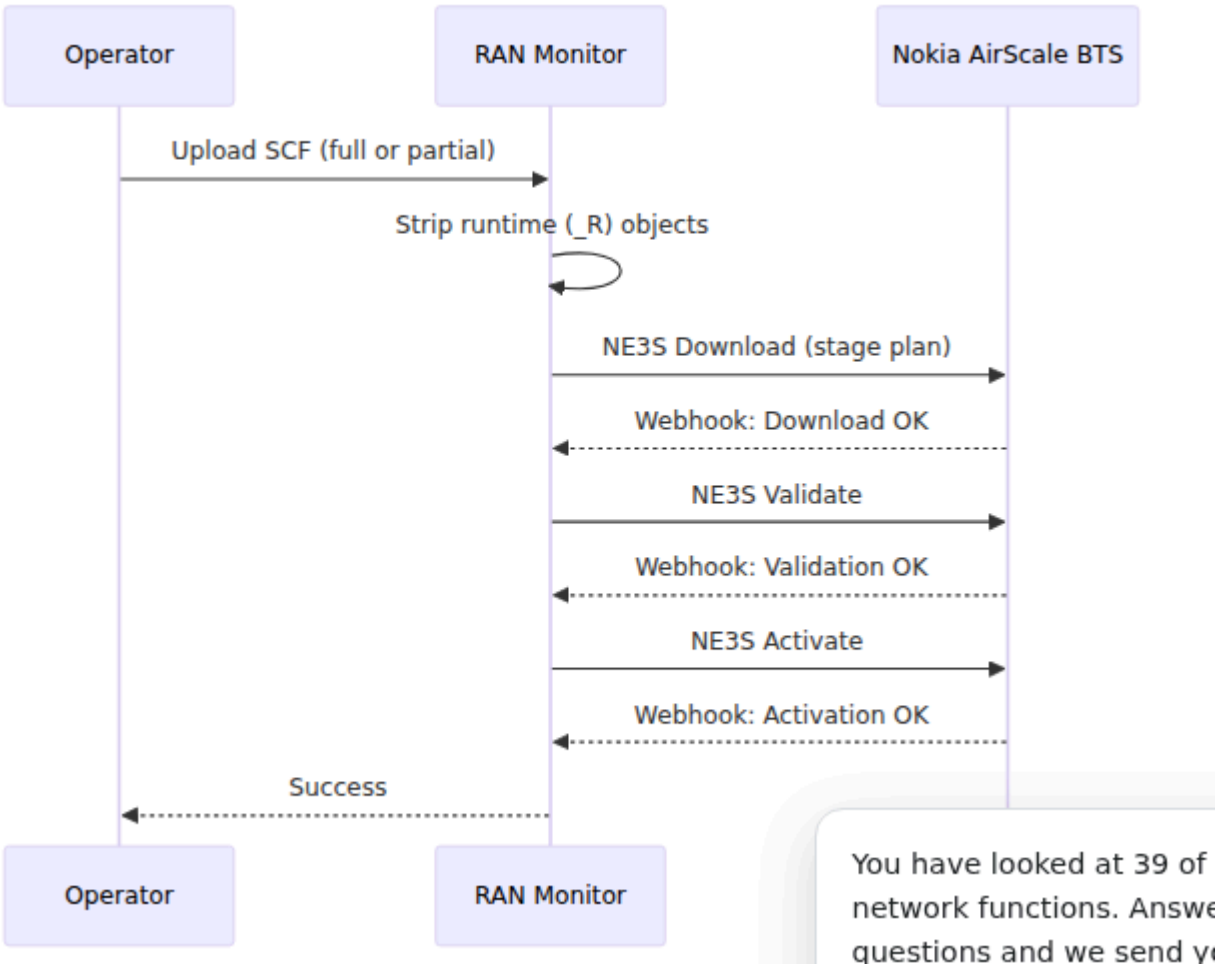
Pousser des modifications de configuration aux stations de base Nokia AirScale via RAN Monitor

---

Vue d'ensemble

RAN Monitor peut pousser des modifications de configuration aux stations de base Nokia AirScale en utilisant le protocole NE3S Bulk Operations. La configuration est exprimée sous forme de SCF (Site Configuration File) au format XML RAML 2.1. Le push suit un processus en trois étapes sur le BTS : **télécharger** (stager le plan), **valider** (vérifier les erreurs) et **activer** (appliquer les modifications). RAN Monitor gère automatiquement les trois étapes.

Un push de configuration peut être un **SCF complet** contenant chaque objet géré sur le BTS, ou une **mise à jour partielle** ciblant uniquement les paramètres spécifiques que vous souhaitez modifier. Les mises à jour partielles sont l'approche recommandée pour les modifications opérationnelles car elles sont plus rapides, moins risquées et évitent de déclencher des redémarrages inutiles du BTS.



Format XML SCF

Tous les fichiers de configuration utilisent le schéma XML RAML 2.1. La structure de base est :

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>

<!-- Les objets gérés vont ici -->

</cmData>
</raml>
```

Chaque objet géré est représenté comme un élément `<managedObject>` :

```
<managedObject class="NOKLTE:LNBTS" distName="MRBTS-256/LNBTS-256"
operation="update">
<p name="enbName">MY-SITE-NAME</p>
</managedObject>
```

Attributs Clés

Attribut	Description
`class`	Identifiant de classe d'objet Nokia (ex. `NOKLTE:LNCEL`, `com.nokia.srbts.tnl:IPIF`)
`distName`	Nom distinct — le chemin de l'objet dans l'arbre des objets gérés
`operation`	`create` pour un push SCF complet, `update` pour des modifications partielles

Format du Nom Distinct

Le `distName` suit un chemin hiérarchique :

```
MRBTS-{bts_id}                                  # Racine du BTS
MRBTS-{bts_id}/LNBTS-{bts_id}                   # LTE eNodeB
MRBTS-{bts_id}/LNBTS-{bts_id}/LNCEL-{cell_id}   # Cellule LTE
MRBTS-{bts_id}/GNBTS-{gsm_id}                   # BTS GSM
MRBTS-{bts_id}/GNBTS-{gsm_id}/GNCEL-{cell_id}   # Cellule GSM
MRBTS-{bts_id}/MNL-1/MNLENT-1/PMCADM-1          # Administration
PM
MRBTS-{bts_id}/EQM-1/APEQM-1                    # Gestion de
l'équipement
```

Push SCF Complet vs Mise à Jour Partielle

Push SCF Complet

Un SCF complet contient chaque objet géré sur le BTS (généralement 100-200 objets). Il utilise `operation="create"` sur chaque objet. Cela remplace l'ensemble de la configuration.

Quand l'utiliser : Provisionnement initial, récupération après sinistre, ou restauration d'une configuration connue à partir d'une sauvegarde.

Risque : Élevé. Un SCF complet contient généralement des objets de transport/IP qui déclencheront un redémarrage du BTS, rendant le site hors ligne pendant 3 à 5 minutes.

Mise à Jour Partielle

Un SCF partiel contient uniquement les objets et paramètres que vous souhaitez modifier. Il utilise `operation="update"` et n'inclut que les éléments `<p>` spécifiques à modifier.

Quand l'utiliser : Changements de paramètres opérationnels, réglage de cellule, activation de fonctionnalités, configuration PM.

Risque : Faible à néant, à condition d'éviter les classes d'objets déclenchant un redémarrage.

Différences Clés

	SCF Complet	Mise à Jour Partielle
Attribut d'opération	`operation="create"`	`operation="update"`
Objets inclus	Tous les objets gérés	Seulement les objets modifiés
Paramètres inclus	Tous les paramètres par objet	Seulement les paramètres modifiés
Risque de redémarrage	Presque certain	Dépend des classes d'objets
Cas d'utilisation typique	Provisionnement initial	Changements quotidiens

---

Impact du Redémarrage par Classe d'Objet

Objets Qui Déclenchent un Redémarrage du BTS

Modifier l'une de ces classes d'objets entraînera le redémarrage du BTS. Le site sera **hors ligne pendant 3 à 5 minutes** pendant le redémarrage.

Catégorie	Classes d'Objets
Transport / IP	`TNL`, `ETHIF`, `ETHLK`, `IPIF`, `IPADDRESSV4`, `IPRT`, `IPRTV6`, `VLANIF`, `L2SWI`, `BRGPRT`, `IBRGPRT`, `IPNO`, `ETHSVC`, `TNLSVC`, `IPSECC`, `FIREWALL`
Système / Matériel	`MRBTS`, `SMOD`, `BBMOD`
Plan de Gestion	`MPLANENW`, `CLOCK`, `SYNC`, `NTP`
Sécurité / Certificats	`SECADM`, `CERTH`, `CERTHENT`, `CMP`, `CMPECDSA`, `CMPFH`

Objets Sûrs à Modifier Sans Redémarrage

Ces classes d'objets peuvent être mises à jour sans déclencher un redémarrage. Certains changements de paramètres radio entraîneront une brève interruption de cellule (secondes) lors de la reconfiguration de la cellule.

Catégorie	Classes d'Objets	Remarques
Radio LTE	`LNCEL`, `LNCEL_FDD`, `LNBTS`, `LNBTS_FDD`	Certains paramètres causent une brève reconfiguration de cellule
Radio GSM	`GNBTS`, `GNCEL`, `GNBCF`	
Surveillance de Performance	`PMCADM`, `PMMNL`, `PMCCP`, `PMPLM`, `PMRNL`, `PMTNLINT`	
Fonctionnalités	`FEATCADM`, `FEATGADM`, `FEATLADM`	
ANR / Relations de Voisinage	`ANR`, `ANRPRL`	
RRC / DRX	`DRX`, `SDRX`, `SIB`	
S1 / Transport	`SCTP`, `TRSNW`, `LNMME`	
Autre	`ALARMSUPP`, `REDRT`, `CAGENB`, `CADPR`, `QOS`	

Objets d'Exécution (Lecture Seule)

Les classes d'objets se terminant par `_R` sont des **objets d'exécution** générés automatiquement par le BTS. Ils ne peuvent pas être poussés et sont automatiquement supprimés par RAN Monitor avant le téléchargement. Exemples : `EQM_R`, `APEQM_R`, `LNCEL_R`, `TNL_R`, `ETHIF_R`.

Exemples de Mise à Jour Partielle

Changer le Nom de l'eNB

Pas de redémarrage. Prend effet immédiatement.

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>
<managedObject class="NOKLTE:LNBTS" distName="MRBTS-256/LNBTS-256"
operation="update">
<p name="enbName">NICK-LAB-AIRSCALE</p>
</managedObject>
</cmData>
</raml>
```

Changer le Nom de la Cellule

Pas de redémarrage. Prend effet immédiatement.

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>
<managedObject class="NOKLTE:LNCEL" distName="MRBTS-256/LNBTS-
256/LNCEL-256" operation="update">
<p name="cellName">TRI-B5-1</p>
</managedObject>
</cmData>
</raml>
```

Changer l'ID de Cellule Physique

Pas de redémarrage. La cellule se reconfigurera brièvement.

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>
<managedObject class="NOKLTE:LNCEL_FDD" distName="MRBTS-256/LNBTS-
256/LNCEL-256/LNCEL_FDD-256" operation="update">
<p name="physCellId">120</p>
</managedObject>
</cmData>
</raml>
```

Changer l'EARFCN et la Largeur de Bande

Pas de redémarrage, mais la cellule sera **brièvement indisponible** (secondes) lors de la reconfiguration à la nouvelle fréquence.

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>
<managedObject class="NOKLTE:LNCEL_FDD" distName="MRBTS-256/LNBTS-
256/LNCEL-256/LNCEL_FDD-256" operation="update">
<p name="earfcnDL">1400</p>
<p name="dlChBw">10 MHz</p>
</managedObject>
</cmData>
</raml>
```

Changer l'Intervalle de Collecte PM

Pas de redémarrage. Prend effet lors du prochain cycle de collecte.

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>
<managedObject class="com.nokia.srbts.mnl:PMCADM" distName="MRBTS-256/MNL-1/MNLENT-1/PMCADM-1" operation="update">
<p name="rTPmCollInterval">60s</p>
</managedObject>
</cmData>
</raml>
```

Changer Plusieurs Paramètres à Travers des Objets

Plusieurs objets peuvent être inclus dans un seul SCF. Cet exemple change le nom de l'eNB et un paramètre de cellule en un seul push :

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>
<managedObject class="NOKLTE:LNBTS" distName="MRBTS-256/LNBTS-256" operation="update">
<p name="enbName">NICK-LAB-AIRSCALE</p>
</managedObject>
<managedObject class="NOKLTE:LNCEL" distName="MRBTS-256/LNBTS-256/LNCEL-256" operation="update">
<p name="cellName">TRI-B5-1</p>
<p name="pMax">331</p>
</managedObject>
</cmData>
</raml>
```

Changer une Adresse IP (Déclenche un Redémarrage)

Modifier des objets de transport/IP **déclenchera le redémarrage du BTS**. Le site sera hors ligne pendant 3 à 5 minutes.

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="actual" scope="all" domain="ALL">
<header>
<log dateTime="2026-03-21T00:00:00+00:00" action="created"></log>
</header>
<managedObject class="com.nokia.srbts.tnl:IPADDRESSV4"
distName="MRBTS-256/TNL-1/IPNO-1/IPIF-1/IPADDRESSV4-1"
operation="update">
<p name="localIpAddr">10.7.15.66</p>
</managedObject>
</cmData>
</raml>
```

Pousser la Configuration via l'Interface Web

1. Naviguez vers **État du BTS** dans le panneau de contrôle
2. Cliquez sur **Config Ops** sur le dispositif cible
3. Sélectionnez votre fichier XML SCF partiel (glisser-déposer ou parcourir)
4. Cliquez sur **Pousser la Configuration vers le Dispositif**
5. RAN Monitor supprime automatiquement les objets d'exécution, puis effectue le téléchargement, la validation et l'activation
6. Surveillez le message de résultat pour le succès ou les erreurs

Pour plus de contrôle, développez la section **Avancé : Étapes manuelles de téléchargement/validation/activation** pour stager un plan sans l'activer, puis validez et activez séparément.

Pousser la Configuration via l'API

```
PUT /api/ne3s/function/provision
Content-Type: application/json

{
  "airscale_name": "ons-Lab-Airscale",
  "config_file": "/path/to/partial-config.xml"
}
```

Le chemin `config_file` doit exister sur le serveur RAN Monitor. Copiez le fichier sur le serveur d'abord si nécessaire.

Réponse en cas de succès :

```
{
  "status": "success",
  "operation": "provision",
  "plan_id": "plan_17740417727216527 42",
  "data": "<activateResponse>...</activateResponse>"
}
```

Réponse en cas d'échec :

```
{
  "status": "error",
  "code": "PROVISION_FAILED",
  "message": "validate failed: Validation error details..."
}
```

Paramètres de l'API

Paramètre	Type	Requis	Par défaut	Description
`airscale_name`	String	Oui	-	Nom de l'appareil enregistré dans RAN Monitor
`config_file`	String	Oui	-	Chemin absolu vers le fichier XML SCF sur le serveur RAN Monitor

---

Meilleures Pratiques

1. **Téléchargez toujours une sauvegarde d'abord.** Utilisez le bouton "Télécharger la Config" de l'interface Web ou l'API pour sauvegarder la configuration actuelle avant d'apporter des modifications.

2. **Utilisez des mises à jour partielles pour les changements opérationnels.** Incluez uniquement les objets et paramètres que vous devez modifier. Cela minimise le risque et évite les redémarrages.

3. **Utilisez `operation="update"` pour des modifications partielles.** L'attribut `operation="create"` est destiné aux remplacements SCF complets et écrasera tous les paramètres de l'objet.

4. **Vérifiez la classe d'objet avant de pousser.** Si votre SCF inclut des objets de transport, système, gestion ou sécurité, le BTS redémarrera. Planifiez une fenêtre de maintenance en conséquence.

5. **Vérifiez que le `distName` correspond à votre BTS cible.** L'ID MRBTS, l'ID LNBTS et les ID de cellule doivent correspondre à l'appareil cible. Poussez le mauvais `distName` et le BTS rejettera la configuration avec une erreur de validation.

6. **Un changement à la fois pour les paramètres critiques.** Lors de la modification des paramètres radio qui affectent le service (EARFCN, largeur de bande, PCI), effectuez un changement par push afin de pouvoir isoler tout problème.

Dépannage

Validation Échouée : Objet Dupliqué

Symptômes : Le push échoue avec `Duplicated object MRBTS-256/EQM_R-1`

Cause : Le SCF contient des objets d'exécution (`_R`). Ceux-ci sont générés automatiquement par le BTS et ne peuvent pas être poussés.

Résolution : RAN Monitor supprime automatiquement les objets `_R`. Si vous voyez cette erreur, vérifiez que vous poussez via RAN Monitor et non directement au BTS.

Activation Échouée : Conflit d'Opération

Symptômes : Le push échoue avec `Operation could not execute because of operation conflict, RequestOperationType = {activate}, OngoingOperationType = {validate}`

Cause : L'activation a été envoyée avant que la validation ne soit terminée. Le BTS traite chaque étape de manière asynchrone.

Résolution : RAN Monitor attend la fin asynchrone entre les étapes automatiquement. Si cela se produit, réessayez le push. Si cela persiste, vérifiez qu'aucun autre système de gestion (NetAct, WebLM) ne pousse simultanément la configuration vers le même BTS.

BTS Redémarré de Manière Inattendue

Symptômes : Le BTS devient hors ligne après le push de configuration, le ping échoue pendant 3 à 5 minutes.

Cause : La configuration poussée incluait des objets de transport/IP, système ou sécurité qui déclenchent un redémarrage.

Résolution : Le BTS reviendra de lui-même après 3 à 5 minutes. Pour éviter cela à l'avenir, utilisez une mise à jour partielle qui n'inclut que les paramètres spécifiques que vous souhaitez modifier, en évitant les classes d'objets déclenchant un redémarrage énumérées ci-dessus.

Fichier de Plan Non Trouvé

Symptômes : L'activation échoue avec `Processing of attachment detail property file failed in agent`

Cause : Erreur interne du BTS lors de la lecture du fichier de plan mis en scène. Cela peut se produire lorsque plusieurs opérations de configuration se chevauchent.

Résolution : Attendez 30 secondes et réessayez le push. Si l'erreur persiste, redémarrez la session NE3S en utilisant le bouton "Forcer la reconnexion" dans l'interface Web avant de réessayer.

Guide de la Politique de Conservation des Données

Aperçu

L'application RAN Monitor inclut désormais un système complet de **Politique de Conservation des Données** qui vous permet de gérer la durée de stockage des métriques de performance, des données de configuration et des enregistrements d'alarme dans InfluxDB. Ce guide couvre tout ce que vous devez savoir sur la gestion de la conservation des données.

🚀 Démarrage Rapide

Accéder au Tableau de Bord de la Politique de Conservation

1. Accédez au **Panneau de Contrôle** : `https://localhost:9443`
2. Cliquez sur **Conservation des Données** dans le menu de navigation
3. Visualisez et gérez les paramètres de conservation pour tous les eNodeBs configurés

Définir une Période de Conservation Personnalisée

1. Trouvez l'eNodeB dans la liste
2. Mettez à jour le champ "Période de Conservation" (en heures)
3. Le paramètre est enregistré immédiatement
4. Revertit à la valeur par défaut globale si laissé vide

Nettoyer les Anciennes Données

1. Cliquez sur le bouton **Nettoyer les Anciennes Données** pour supprimer les enregistrements plus anciens que la période de conservation
2. Ou cliquez sur **Effacer Toutes les Données** pour supprimer tous les enregistrements pour cet eNodeB (à utiliser avec précaution !)

Capture d'Écran

Le tableau de bord de conservation des données montrant les paramètres de conservation et les comptes d'enregistrements pour chaque eNodeB

Fonctionnalités

Paramètres de Conservation Globaux

- **Période de Conservation par Défaut** : 720 heures (30 jours)

- **Configurables** : Changement dans `config/config.exs`
- **Repli** : Appliqué à tous les eNodeBs sans paramètres personnalisés

Conservation par eNodeB

- **Remplacer Global** : Définir une conservation personnalisée pour des eNodeBs spécifiques
- **Stocké dans la Base de Données** : Persisté dans la table `airscales`
- **Temps Réel** : Prend effet immédiatement

Nettoyage Automatique

- **Planifié** : S'exécute automatiquement chaque heure
- **Travailleur en Arrière-Plan** : `RanMonitor.Data.RetentionCleanupWorker`
- **Par eNodeB** : Respecte les paramètres de conservation individuels
- **Journalisé** : Tous les nettoyages sont enregistrés pour la traçabilité

Visibilité des Données

- **Comptes d'Enregistrements** : Voir combien d'enregistrements par type de mesure :
  - Métriques de Performance
  - Configuration
  - Alarmes
- **Résumé Total** : Voir le total des enregistrements par eNodeB
- **Temps Réel** : Mis à jour lors du rafraîchissement de la page

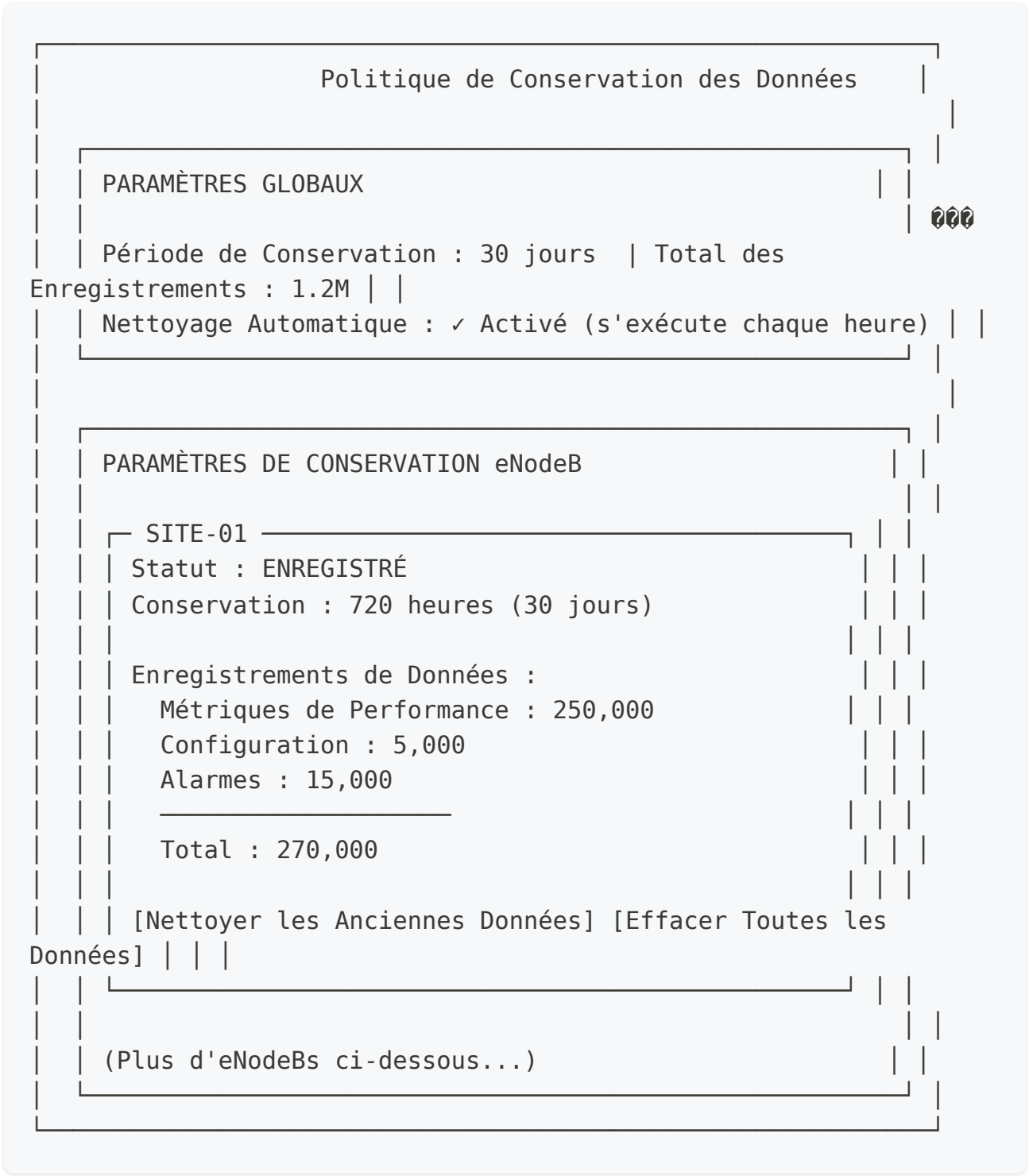
---

🖥️ Interface Utilisateur

Mise en Page du Tableau de Bord

Le tableau de bord de conservation des données montrant les paramètres globaux, les périodes de conservation par eNodeB et les comptes d'enregistrements

Aperçu de la Mise en Page :



Indicateurs de Statut

- **Vert (✓)** : eNodeB enregistré et actif
- **Rouge (✗)** : eNodeB en attente ou non enregistré
- **Désactivé** : Impossible de modifier les paramètres pour les eNodeBs non enregistrés

Boutons d'Action

Bouton	Action	Effet
Nettoyer les Anciennes Données	Supprimer les anciens enregistrements	Supprime les enregistrements plus anciens que la période de conservation
Effacer Toutes les Données	Effacement complet	Supprime TOUS les enregistrements (⚠ à utiliser avec précaution !)
Rafraîchir	Mettre à jour l'affichage	Récupère à nouveau les comptes d'enregistrements et les paramètres

---

⚙ Configuration

Configuration de Conservation Globale

Éditez `config/config.exs` :

```
config :ran_monitor,
  ecto_repos: [RanMonitor.Repo],
  generators: [context_app: :ran_monitor],
  data_retention_hours: 720  # 30 jours, ajustez si nécessaire
```

Valeurs de Temps Supportées

Période	Heures	Jours	Recommandé Pour
1 heure	1	0.04	Test uniquement
1 jour	24	1	Métriques à court terme
7 jours	168	7	Rapports hebdomadaires
14 jours	336	14	Rapports bi-hebdomadaires
30 jours	720	30	Rapports mensuels (par défaut)
90 jours	2160	90	Tendances à long terme
180 jours	4320	180	Rapports bi-annuels
1 an	8760	365	Rapports annuels

Variables d'Environnement

Remplacez éventuellement au moment de l'exécution :

```
export DATA_RETENTION_HOURS=1440  # 60 jours
mix phx.server
```

🔧 Comment Cela Fonctionne

Flux de Conservation des Données

```
1. INSERTION DE DONNÉES
   ├─ Métriques de Performance → InfluxDB
   ├─ Données de Configuration → InfluxDB
   └─ Alarmes → InfluxDB

2. NETTOYAGE AUTOMATIQUE (Horaire)
   ├─ RetentionCleanupWorker déclenché
   ├─ Pour chaque eNodeB :
   │  ├─ Obtenir la conservation effective (par eNodeB ou globale)
   │  ├─ Calculer le timestamp de coupure
   │  └─ Supprimer les enregistrements plus anciens que la coupure
   └─ Journaliser les résultats

3. NETTOYAGE MANUEL (À la Demande)
   ├─ L'utilisateur clique sur le bouton dans l'UI
   ├─ Politique de conservation appliquée
   ├─ Enregistrements supprimés immédiatement
   └─ Notification de succès/erreur affichée

4. SURVEILLANCE
   └─ Comptes d'enregistrements affichés dans l'UI
```

Logique de Conservation

Conservation Effective par eNodeB :

```
effective_retention = case airscale.retention_hours do
  nil -> Config.data_retention_hours()      # Utiliser la valeur
globale (720h)
  hours -> hours                             # Utiliser la valeur
personnalisée par eNodeB
end
```

Exemple :

- Valeur par défaut globale : 720 heures (30 jours)
- eNodeB "SITE-01" personnalisé : 168 heures (7 jours)
- eNodeB "SITE-02" personnalisé : nil → utilise 720 heures globales

Processus de Nettoyage

```
Timestamp de Coupure = Maintenant - (retention_hours * 3600
secondes)

Exemple avec une conservation de 30 jours :
├─ Actuel : 2025-12-11 10:00:00
├─ Conservation : 720 heures (30 jours)
├─ Coupure : 2025-11-11 10:00:00
└─ Supprimer tous les enregistrements avec timestamp < coupure
```

□ Surveillance & Journalisation

Entrées de Journal

Le système journalise toutes les activités de conservation. Recherchez :

```
[RetentionCleanupWorker] Démarrage du travailleur de nettoyage de
conservation
[RetentionCleanupWorker] Nettoyage des données pour SITE-01
(conservation : 720h)
[RetentionCleanupWorker] 15,000 enregistrements supprimés pour
SITE-01
[RetentionCleanupWorker] Cycle de nettoyage terminé : 5 réussis, 0
échoués, 75,000 total supprimés
```

Surveillance des Comptes d'Enregistrements

Visibilité en Temps Réel :

1. Ouvrez le tableau de bord de conservation des données

2. Visualisez les comptes d'enregistrements actuels par mesure par eNodeB
3. Cliquez sur "Rafraîchir" pour mettre à jour les comptes

Suivi Historique :

- Vérifiez les journaux de l'application pour les résumés de nettoyage
- Surveillez l'utilisation du disque InfluxDB au fil du temps
- Configurez des alertes basées sur la croissance des comptes d'enregistrements

---

Utilisation Avancée

Accès Programmatique

Utilisez le service de politique de conservation dans votre code :

```
alias RanMonitor.Data.RetentionPolicy
alias RanMonitor.Database.Nokia

# Obtenir la conservation effective pour un eNodeB
airscale = Nokia.get_airscale!(1)
hours = RetentionPolicy.get_retention_hours(airscale)
# => 720 (ou valeur personnalisée si définie)

# Obtenir les comptes d'enregistrements pour un eNodeB
counts = RetentionPolicy.get_record_counts("SITE-01")
# => %{"PerformanceMetrics" => 250000, "Configuration" => 5000,
"Alarms" => 15000}

# Obtenir le total des enregistrements
total = RetentionPolicy.get_total_record_count("SITE-01")
# => 270000

# Supprimer manuellement les anciens enregistrements
{:ok, deleted_count} = RetentionPolicy.delete_old_records("SITE-
01", 720)
# => {:ok, 50000}  (50k enregistrements supprimés)

# Effacer tous les enregistrements pour un eNodeB
{:ok, deleted_count} = RetentionPolicy.clear_all_records("SITE-
01")
# => {:ok, 270000}  (tous les 270k enregistrements supprimés)
```

Ajustement de l'Intervalle de Nettoyage

L'intervalle de nettoyage par défaut est de 1 heure (3,600,000 ms) et peut être ajusté, par exemple à 30 minutes (1,800,000 ms). Contactez le support Omnitouch pour le modifier.

Requêtes au Niveau de la Base de Données

Visualisez les paramètres de conservation directement :

```
SELECT name, retention_hours FROM airscales;
```

Mettez à jour la conservation via la base de données :

```
UPDATE airscales
SET retention_hours = 168
WHERE name = 'SITE-01';
```

Meilleures Pratiques

Sélection de la Période de Conservation

Court Terme (< 7 jours)

- Utilisé pour : Tests, environnements de staging
- Pas recommandé pour : Production
- Risque : Peut supprimer des données historiques importantes

Standard (7-30 jours)

- Utilisé pour : Déploiements en production avec stockage typique
- Meilleur pour : La plupart des cas d'utilisation
- Équilibre : Bonne histoire avec stockage gérable

Long Terme (> 30 jours)

- Utilisé pour : Analyse des tendances, exigences de conformité
- Coût : Exigences de stockage plus élevées
- Avantage : Données historiques étendues

Recommandé par Cas d'Utilisation

Cas d'Utilisation	Conservation	Raison
Rapports quotidiens	7-14 jours	Cycles de révision hebdomadaires
Rapports hebdomadaires	30-60 jours	Résumés mensuels
Rapports mensuels	90 jours	Analyse trimestrielle
Analyse des tendances	180-365 jours	Modèles à long terme
Conformité	Selon les besoins	Légal/réglementaire

Considérations de Stockage

Estimez les besoins en stockage :

- 1000 enregistrements ≈ 1-5 Ko (selon le type de mesure)
- 1 million d'enregistrements ≈ 1-5 Go
- Période de conservation × taux de collecte = stockage total

Surveillez la croissance avec :

```
# Vérifiez la taille du bucket InfluxDB
influx bucket list

# Ou vérifiez l'utilisation du disque
df -h /path/to/influxdb/data
```

🔒 Sécurité & Conformité

Confidentialité des Données

- **Pas de cryptage** au repos par défaut
- **Accès réseau** contrôlé via la sécurité InfluxDB
- **Journaux d'accès** disponibles dans les journaux de l'application

Conformité

- **Traçabilité** : Tous les nettoyages sont enregistrés avec un timestamp
- **Intégrité des données** : Suppressions douces, pas de suppressions définitives au niveau de l'application
- **Preuve de conservation** : Les journaux montrent ce qui a été conservé/supprimé

Recommandations

1. **Activer l'authentification InfluxDB** pour la production
2. **Surveiller les journaux de nettoyage** régulièrement
3. **Définir la conservation avec soin** pour équilibrer conformité et stockage
4. **Sauvegarder avant les opérations en masse** si des données critiques
5. **Tester les politiques de conservation** dans un environnement de staging d'abord

---

🔧 Dépannage

Problème : Nettoyage Non Exécuté

Symptômes :

- Enregistrements plus anciens que la période de conservation existent toujours

- Pas d'entrées de journal de nettoyage

Solutions :

1. Vérifiez que l'application fonctionne : `ps aux | grep mix`
2. Vérifiez que `RetentionCleanupWorker` a démarré :
   - Vérifiez les journaux pour `[RetentionCleanupWorker] Démarrage`
3. Vérifiez la connexion InfluxDB :
   - Visitez la page d'état InfluxDB : `https://localhost:9443/nokia/influx`
4. Vérifiez que les paramètres de conservation sont configurés :
   - Vérifiez `config/config.exs` pour `data_retention_hours`

Problème : Nettoyage Manuel Échoué

Symptômes :

- Message d'erreur lors du clic sur "Nettoyer les Anciennes Données"
- Enregistrements non supprimés

Solutions :

1. Vérifiez qu'InfluxDB est accessible :
   - Testez la connexion dans le tableau de bord
2. Vérifiez que les comptes d'enregistrements sont précis :
   - Cliquez sur "Rafraîchir" pour mettre à jour
3. Vérifiez les journaux de l'application pour les erreurs :
   - Recherchez les entrées d'erreur `[RetentionPolicy]`
4. Vérifiez que l'eNodeB est enregistré :
   - Vérifiez la page d'état BTS

Problème : Utilisation Élevée de la Mémoire Après Nettoyage

Symptômes :

- L'application devient lente après le nettoyage

- Les pics d'utilisation de la mémoire

Solutions :

1. Cela est normal pour de grandes suppressions
2. Laissez 5-10 minutes pour que la mémoire se normalise
3. Envisagez de réduire la fréquence de nettoyage :
   - Changez `@cleanup_interval_ms` (par défaut 1 heure)
4. Ou réduisez la période de conservation pour les eNodeBs affectés

Problème : Comptes d'Enregistrements Incorrects

Symptômes :

- Les comptes d'enregistrements ne correspondent pas à l'UI InfluxDB
- "Nettoyer les Anciennes Données" affiche des chiffres différents

Solutions :

1. Cliquez sur "Rafraîchir" pour forcer la mise à jour
2. Vérifiez la requête InfluxDB :
   - Peut prendre du temps pour refléter les suppressions récentes
3. Attendez une minute et réessayez :
   - InfluxDB peut traiter les opérations de suppression
4. Vérifiez que le nom de l'eNodeB correspond exactement :
   - Comparaison sensible à la casse

Documentation Connexe

- **Guide des Opérations** - Vue d'ensemble opérationnelle complète
- **Guide de l'Interface Web** - Référence et fonctionnalités du panneau de contrôle
- **Guide de Démarrage** - Guide de démarrage rapide
- **Guide des Opérations Courantes** - Tâches de gestion quotidiennes

- **Guide d'Intégration Grafana** - Analytique et tableaux de bord

---

Points d'Accès

- **Tableau de Bord de Conservation des Données** : `https://localhost:9443/nokia/retention`
- **État BTS** : `https://localhost:9443/nokia/status`
- **État InfluxDB** : `https://localhost:9443/nokia/influx`
- **Journaux en Direct** : `https://localhost:9443/nokia/logs`

FAQ

Q : Le nettoyage supprimera-t-il des données actives ?

R : Non. Seuls les enregistrements plus anciens que la période de conservation sont supprimés. Les données actuellement collectées ne sont jamais affectées.

Q : Puis-je définir une conservation différente pour différents eNodeBs ?

R : Oui ! Chaque eNodeB peut avoir son propre paramètre de conservation. S'il n'est pas défini, il utilise la valeur par défaut globale.

Q : À quelle fréquence le nettoyage automatique s'exécute-t-il ?

R : Chaque heure par défaut. Ajustez `@cleanup_interval_ms` dans le travailleur si nécessaire.

Q : Que se passe-t-il si j'efface toutes les données ?

R : Tous les enregistrements (Métriques de Performance, Configuration, Alarmes) pour cet eNodeB sont définitivement supprimés. Cela ne peut pas être annulé.

Q : Le nettoyage peut-il affecter la collecte de données ?

R : Non. Le nettoyage et la collecte de données sont indépendants. De nouvelles données continueront à être écrites pendant que les anciennes données sont supprimées.

Q : Combien de temps le nettoyage prend-il ?

R : Cela dépend du nombre d'enregistrements :

- Petit (< 100k) : < 1 seconde
- Moyen (100k-1M) : 1-10 secondes
- Grand (> 1M) : 10-60+ secondes

Q : Puis-je supprimer manuellement des enregistrements spécifiques ?

R : Pas via l'UI. Seul le nettoyage complet ou l'effacement complet est disponible. Pour des suppressions granulaires, utilisez directement l'API ou la CLI InfluxDB.

Q : Que se passe-t-il si InfluxDB n'est pas disponible ?

R : Le nettoyage échouera silencieusement et réessaiera l'heure suivante. La collecte de données continue sans être affectée.

Q : Le nettoyage affecte-t-il les performances ?

R : Impact mineur pendant le nettoyage (secondes à minutes selon la taille des données). L'intervalle horaire a été choisi pour minimiser l'impact.

Détails de Mise en Œuvre

Ce que Cela Ajoute

La fonctionnalité de conservation ajoute un paramètre de conservation par eNodeB, un paramètre de conservation global configuré dans `config/config.exs`, un travailleur de nettoyage en arrière-plan qui s'exécute chaque heure, une page d'interface de gestion, et une migration de base de données pour stocker les valeurs de conservation par eNodeB.

Fonctions Clés

Module RetentionPolicy :

- `get_retention_hours(airscale)` - Obtenir la conservation effective
- `get_record_counts(airscale_name)` - Récupérer les comptes d'enregistrements
- `get_total_record_count(airscale_name)` - Compte total
- `delete_old_records(name, hours)` - Nettoyer les anciens enregistrements
- `clear_all_records(name)` - Effacement complet

GenServer RetentionCleanupWorker :

- `start_link(opts)` - Démarrer le travailleur de nettoyage
- `init(:ok)` - Initialiser le travailleur
- `handle_info(:cleanup, state)` - Exécuter le cycle de nettoyage

🚀 Démarrer

Configuration (Une Fois)

1. **Exécutez la migration :**

   ```
   mix ecto.migrate
   ```

2. **Redémarrez l'application :**

   ```
   mix phx.server
   ```

3. **Vérifiez l'installation :**

   - Accédez à `https://localhost:9443/nokia/retention`
   - Vous devriez voir le tableau de bord de conservation des données

Première Utilisation

1. **Vérifiez les paramètres actuels :**
    - Visualisez la conservation globale (par défaut : 720 heures)
    - Visualisez les paramètres de conservation par eNodeB
2. **Personnalisez si nécessaire :**
    - Mettez à jour la conservation globale dans `config/config.exs`
    - Ou définissez par eNodeB via l'UI
3. **Surveillez le nettoyage :**
    - Regardez les journaux pour les entrées `[RetentionCleanupWorker]`
    - Vérifiez que les comptes d'enregistrements diminuent au fil du temps

---

Support

Besoin d'Aide ?

1. **Vérifiez les journaux :** Recherchez les entrées `[RetentionPolicy]` ou `[RetentionCleanupWorker]`
2. **Consultez ce guide :** La plupart des problèmes sont couverts dans la section Dépannage
3. **Vérifiez d'autres docs :** Référez-vous aux liens de documentation connexes ci-dessus
4. **Vérifiez la configuration :** Assurez-vous que la migration a été exécutée et que le travailleur a démarré

Signalement de Problèmes

Incluez :

- Message d'erreur de l'UI ou des journaux
- Nom de l'eNodeB affecté

- Paramètres de conservation actuels
- Comptes d'enregistrements avant/après
- Étapes pour reproduire

Ressources d'Apprentissage

Concepts Connexes

- **InfluxDB v2.x** : Base de données de séries temporelles avec politiques de conservation
- **Politique de Conservation** : Durée de conservation des données
- **Nettoyage** : Suppression automatisée des anciennes données
- **Types de Mesure** : Métriques de Performance, Configuration, Alarmes

Ressources Externes

- Documentation InfluxDB
- Guide GenServer d'Elixir
- Phoenix LiveView

Guide de Commissioning DHCP Nokia AirScale

Configuration de DHCP pour l'Intégration Automatique de la Station de Base

---

Table des Matières

1. Aperçu
2. Prérequis
3. Comment Ça Fonctionne
4. Configuration du Serveur DHCP
5. Configuration de la Station de Base
6. Vérification
7. Dépannage
8. Référence Technique de l'Option 43

Aperçu

Les stations de base Nokia AirScale peuvent découvrir et s'enregistrer automatiquement avec RAN Monitor via DHCP. Lorsque la station de base s'allume, elle envoie une requête DHCP contenant son identité. Le serveur DHCP répond avec la configuration IP de la station de base et l'adresse du serveur RAN Monitor encodée dans **l'Option DHCP 43** (Informations Spécifiques au Fournisseur).

Cela élimine le besoin de configurer manuellement chaque station de base avec l'adresse du serveur de gestion. La station de base complète le

handshake DHCP, puis initie une connexion de découverte d'agent NE3S à l'adresse IP RAN Monitor fournie dans la réponse DHCP.

Qui Devrait Utiliser Ce Guide

Important : Toute configuration de station de base Nokia AirScale est **effectuée par Omnitouch** dans le cadre du déploiement initial et du support continu. Ce guide est fourni pour :

- **Utilisateurs avancés** qui souhaitent comprendre le processus de commissioning DHCP
- **Déploiements autogérés** où les clients gèrent leur propre infrastructure DHCP
- **Dépannage** des problèmes d'autoconnection basés sur DHCP

Si vous êtes un client géré par Omnitouch, contactez le support Omnitouch pour le commissioning de la station de base et la configuration DHCP.

Prérequis

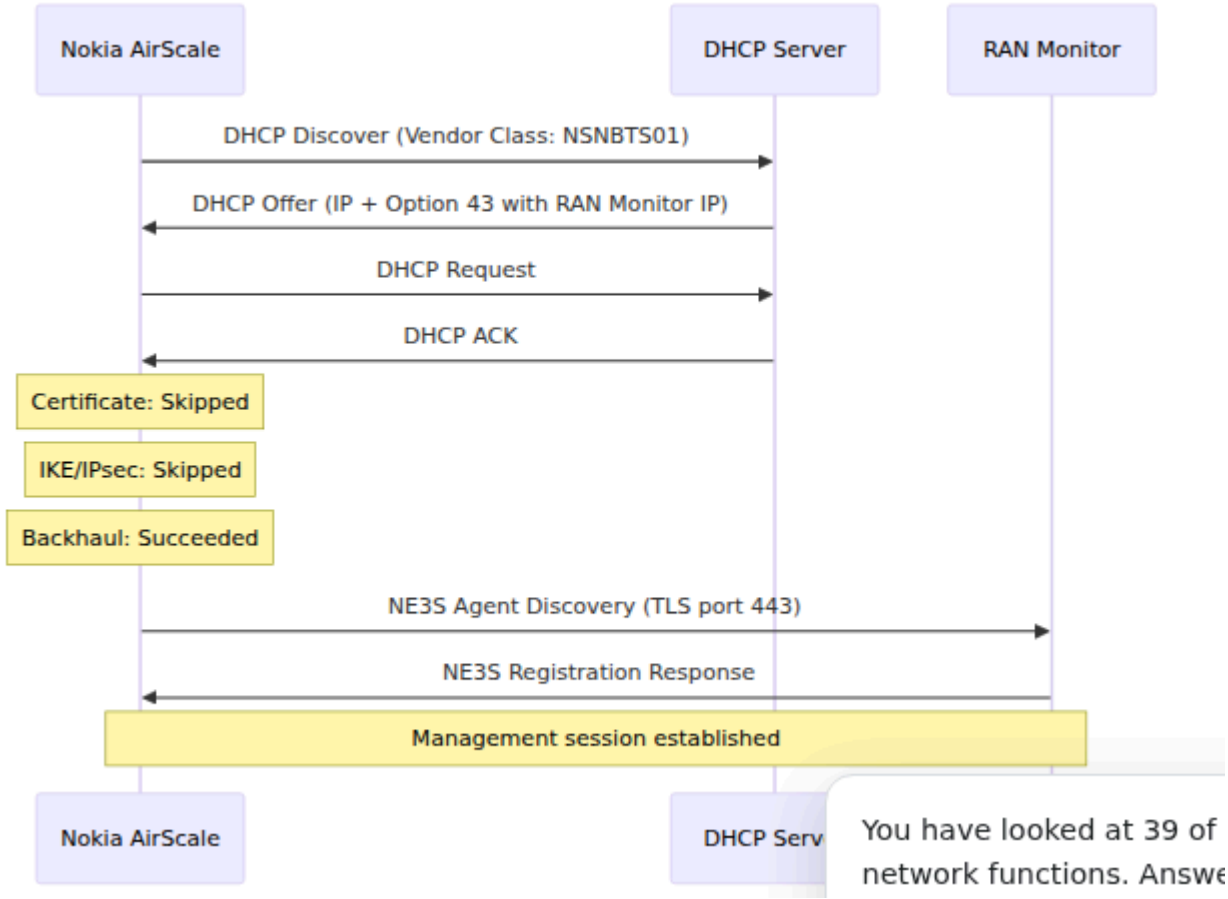
Avant de configurer le commissioning DHCP, assurez-vous d'avoir :

- **Serveur DHCP** — Un serveur DHCP sur le réseau de gestion de la station de base (MikroTik, ISC DHCP, dnsmasq, etc.)
- **RAN Monitor** — Une instance RAN Monitor en cours d'exécution accessible depuis le réseau de la station de base
- **Connectivité Réseau** — Connectivité de couche 2 entre le port OAM de la station de base et le serveur DHCP

Informations Requises :

Paramètre	Description	Exemple
IP RAN Monitor	Adresse IP où RAN Monitor est en cours d'exécution	10.179.2.139
Sous-réseau de Gestion	Sous-réseau pour les interfaces de gestion de la station de base	10.7.15.64/26
IP de la Passerelle	Passerelle par défaut pour le sous-réseau de gestion	10.7.15.65
Serveur DNS	IP du serveur DNS	10.7.15.65

Comment Ça Fonctionne



Flux d'Autoconnection

La station de base progresse à travers ces phases après avoir reçu un bail DHCP :

Phase	Statut	Description
DHCP	Réussi	Adresse IP et adresse RAN Monitor obtenues
Certificat	Ignoré	Aucun enregistrement de certificat requis (réseau privé)
IKE	Ignoré	Aucun tunnel IPsec requis (réseau privé)
Backhaul	Réussi	Connectivité réseau confirmée
Identification	Demandé	Découverte de l'agent NE3S initiée vers RAN Monitor

---

Configuration du Serveur DHCP

Encodage de l'Option 43

Les stations de base Nokia AirScale nécessitent que l'Option DHCP 43 (Informations Spécifiques au Fournisseur) contienne l'adresse IP de RAN Monitor. La station de base **rejette** les Offres DHCP sans une Option 43 correctement encodée.

Génération de la Valeur de l'Option 43

Exécutez ce script avec votre IP RAN Monitor pour générer la valeur hexadécimale nécessaire pour le serveur DHCP :

```
#!/bin/bash
# generate-nokia-option43.sh
# Usage: ./generate-nokia-option43.sh <ran-monitor-ip>
IP="${1:?Usage: $0 <ran-monitor-ip>}"
IFS='.' read -r a b c d <<< "$IP"
H=$(printf "%02x%02x%02x%02x" $a $b $c $d)
S=$(echo -n "$IP" | xxd -p)
L=$(printf "%02x" ${#IP})
echo "0x0104${H}0104${H}08${L}${S}0904706b69780b0101"
```

Exemple pour `10.179.2.139` :

```
$ ./generate-nokia-option43.sh 10.179.2.139
0x01040ab3028b04040ab3028b080c31302e3137392e322e3133390904706b69780b0
```

Utilisez la sortie comme la `value` dans la configuration du serveur DHCP ci-dessous.

MikroTik RouterOS 7

```
/ip dhcp-server option
add code=43 name=nokia-oms
value=0x01040ab3028b04040ab3028b080c31302e3137392e322e3133390904706b6

/ip dhcp-server option sets
add name=nokia-set options=nokia-oms

/ip dhcp-server network
set [find address=10.7.15.64/26] dhcp-option-set=nokia-set dns-
server=10.7.15.65 gateway=10.7.15.65
```

Paramètres :

Ligne	But
`code=43`	Option DHCP 43 (Informations Spécifiques au Fournisseur)
`value=0x...`	Charge utile de l'Option 43 encodée en hexadécimal contenant l'IP de RAN Monitor
`dhcp-option-set=nokia-set`	Attache l'ensemble d'options au réseau DHCP

dnsmasq

```
dhcp-
option=43,01:04:0a:b3:02:8b:04:04:0a:b3:02:8b:08:0c:31:30:2e:31:37:39
```

ISC DHCP

```
option vendor-encapsulated-options
01:04:0a:b3:02:8b:04:04:0a:b3:02:8b:08:0c:31:30:2e:31:37:39:2e:32:2e:
```

Configuration de la Station de Base

Mode d'Autoconnection

La station de base doit être réglée sur le mode **Réseau privé avec DHCP**. Cela se configure via le Web Element Manager :

1. Ouvrez le Web Element Manager de la station de base à `https://<base-station-ip>/`
2. Naviguez vers **Configuration Automatisation**
3. Réglez **Scénario** sur **Réseau privé avec DHCP**

4. Laissez **Supprimer les certificats d'opérateur** sur **Non**

Si la station de base est réglée sur **Réseau public**, elle **rejette** les Offres DHCP contenant des données de fournisseur de l'Option 43.

Port Ethernet

La station de base envoie DHCP sur son port OAM (Opérations, Administration, Maintenance) ethernet. Sur le module système SBTS, il s'agit généralement de **SystemModuleEIF3** ou du premier port connecté. La station de base détecte automatiquement quel port a un lien et interroge chacun d'eux en séquence.

Le port OAM doit être connecté au réseau de gestion où le serveur DHCP est accessible. Aucun balisage VLAN n'est requis pour les déploiements de réseau privé — la station de base envoie d'abord un DHCP non balisé sur l'interface simple, puis revient à l'interrogation VLAN si aucune offre valide n'est reçue.

Vérification

Bail DHCP

Après avoir configuré le serveur DHCP, vérifiez que la station de base obtient un bail. Sur MikroTik :

```
/ip dhcp-server lease print where server=<dhcp-server-name>
```

Le préfixe d'adresse MAC de la station de base est `78:F9:B4` (Nokia Solutions and Networks).

Journaux de la Station de Base

Le rapport d'autoconnection de la station de base (accessible via le Web Element Manager) devrait montrer :

```
Dhcp offer Accepted
Identification Server Ip1: 10.179.2.139
Certificate Skipped
Ike Skipped
BTS backhaul connection Succeeded
Started agent discovery with identification IP: 10.179.2.139
```

RAN Monitor

Dans l'interface Web de RAN Monitor :

1. Naviguez vers **Statut BTS**
2. La station de base devrait apparaître avec l'un des statuts suivants :
   - **Connecté** (vert) — enregistré, session active, config et données PM en cours
   - **En attente de données PM** (bleu) — session active, config reçue, en attente du premier cycle PM
   - **Session Active** (jaune) — enregistré avec session active, en attente de données
   - **Enregistrement** (jaune) — enregistrement NE3S en cours
   - **Déconnecté** (rouge) — non enregistré ou inaccessible

Dépannage

Station de Base Ne Pas Accepter DHCP

Symptôme : La station de base envoie des découvertes DHCP à plusieurs reprises mais n'accepte jamais l'Offre.

Vérifiez ceci dans l'ordre :

1. **L'Option 43 est-elle attachée au réseau DHCP ?** — L'option doit être liée via `dhcp-option-set`, pas seulement définie
2. **La station de base est-elle réglée sur "Réseau privé avec DHCP" ?** — Vérifiez la page Configuration Automatisation du Web Element Manager

3. **L'IP RAN Monitor est-elle accessible ?** — Vérifiez le routage entre le sous-réseau de la station de base et RAN Monitor

"Connexion au Serveur d'Identification échouée"

Symptôme : DHCP réussit mais la station de base ne peut pas se connecter à RAN Monitor.

Vérifiez :

- RAN Monitor est en cours d'exécution et accessible depuis le sous-réseau de la station de base
- Le port 443 est ouvert entre la station de base et RAN Monitor
- La station de base est ajoutée à la configuration des appareils de RAN Monitor

---

Ressources Supplémentaires

- Guide de Configuration Nokia AirScale — Configuration de la surveillance des performances après le commissioning
- Guide de Configuration Runtime — Configuration des appareils RAN Monitor
- Dépannage — Guide de dépannage général

Gestion du Firmware

Dépôt de Paquets Logiciels Nokia AirScale

Hébergez et servez des paquets de firmware pour des mises à jour logicielles à distance

---

Vue d'ensemble

La page de Gestion du Firmware fournit un dépôt centralisé pour les paquets logiciels des stations de base Nokia AirScale. Une fois qu'un paquet est téléchargé sur RAN Monitor, il peut être installé sur une station de base de deux manières :

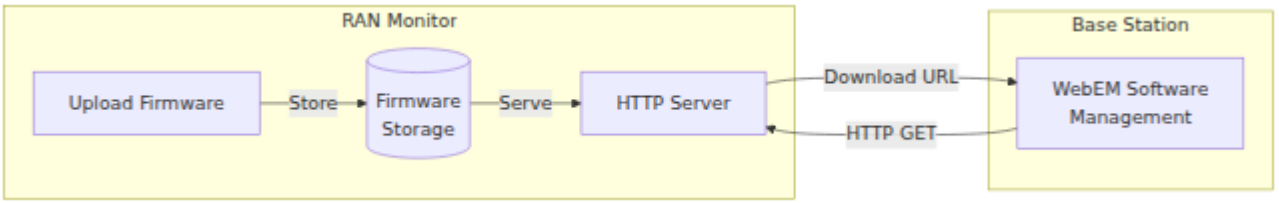
- **Installation directe** — RAN Monitor se connecte à la station de base et effectue le téléchargement, l'activation et le redémarrage du logiciel en votre nom. Piloté depuis la page Firmware ou l'API. Voir Installation du Firmware sur une Station de Base.
- **Récupération par la station de base** — le paquet est servi via HTTP et la station de base le récupère elle-même, soit via l'option "Serveur distant" de WebEM, soit déclenché par une poussée de configuration. Voir Flux de Mise à Jour Logicielle de la Station de Base et Mise à Jour Logicielle à Distance via Poussée de Configuration.

Fonctionnalités Clés

- **Télécharger des paquets de firmware** - Stocker des paquets logiciels .zip Nokia AirScale
- **Installation directe sur la station de base** - Télécharger, activer et revenir à une version précédente du logiciel depuis RAN Monitor sans se connecter à chaque site
- **Validation post-redémarrage** - Confirmer que la station de base a redémarré avec la version logicielle attendue après un réinitialisation

- **Service de fichiers HTTP** - Les stations de base téléchargent le firmware via des URL HTTP standard
- **Sommes de contrôle MD5** - Calcul automatique des sommes de contrôle pour la vérification de l'intégrité
- **Copie d'URL** - Copie en un clic des URL de téléchargement pour la configuration WebEM
- **Statistiques de stockage** - Surveiller l'utilisation du disque du dépôt de firmware

Vue d'ensemble du Flux de Travail



Accéder à la Page

URL : `https://<ran-monitor-ip>:9443/nokia/firmware`

Navigation : Barre latérale du Panneau de Contrôle > **Firmware**

La page de Gestion du Firmware avec la section de téléchargement et la liste des firmwares disponibles.

Configuration de Stockage

Chemin de Stockage par Défaut

Les fichiers de firmware sont stockés sur le système de fichiers du serveur RAN Monitor :

```
/var/firmware/nokia/
├── SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zi
├── SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zi
├──
SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip.me
├── SBTS24R1_ENB_0000_001093_000000_release_BTSSM_downloadable_A52.zi
├── SBTS24R1_ENB_0000_001093_000000_release_BTSSM_downloadable_A52.zi
├──
SBTS24R1_ENB_0000_001093_000000_release_BTSSM_downloadable_A52.zip.me
└── ...
```

Pour chaque paquet de firmware, les fichiers suivants sont créés :

- `.zip` - Le paquet de firmware
- `.md5` - Somme de contrôle MD5 mise en cache
- `.metadata.json` - Métadonnées mises en cache extraites du paquet

Chemin de Stockage Personnalisé

Configurez un emplacement de stockage alternatif dans `config/runtime.exs` :

```
config :ran_monitor,
  firmware_storage_path: "/data/firmware/nokia"
```

Paramètre	Type	Requis	Par défaut	De
`firmware_storage_path`	String	Non	`/var/firmware/nokia`	Chem répert stocka fichier firmw répert créé autom s'il n'e

Comportement de Repli

Si le chemin de stockage configuré ne peut pas être créé (par exemple, permission refusée), le système revient à `priv/firmware/nokia` dans le répertoire de l'application.

Référence de l'Interface Web

Vue d'ensemble du Stockage

La section supérieure affiche des statistiques du dépôt :

Mètre	Description
Fichiers de Firmware	Nombre total de paquets de firmware stockés
Taille Totale	Taille combinée de tous les fichiers de firmware
Chemin de Stockage	Emplacement actuel du système de fichiers pour le stockage des firmwares

Section de Téléchargement

Téléchargez des paquets de firmware Nokia AirScale :

1. Cliquez sur la zone de téléchargement ou faites glisser et déposez un fichier `.zip`
2. Vérifiez que le nom du fichier apparaît avec des informations de taille
3. Cliquez sur **Télécharger le Firmware** pour stocker le fichier

La progression du téléchargement affiche la vitesse de transfert et le temps estimé restant.

Fichiers supportés : uniquement les fichiers `.zip` (paquets logiciels Nokia)

Taille maximale du fichier : 15 Go

La progression du téléchargement affiche :

- Vitesse de téléchargement actuelle (par exemple, 15.37 Mo/s)
- Pourcentage complété
- Octets transférés / taille totale
- Temps estimé restant (ETA)

Format du nom de fichier : Les paquets de firmware Nokia suivent la convention de nommage :

```
SBTS<release>_ENB_<build>_<variant>_release_BTSSM_downloadable_<suffi
```

Exemple :
`SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip`

Liste des Firmwares

Le tableau affiche tous les paquets de firmware téléchargés :

Colonne	Description
Nom de Fichier	Nom complet du paquet de firmware
Version	Version de sortie extraite (par exemple, SBTS25R1)
Date de Construction	Horodatage de construction extrait des métadonnées du firmware
Info	Bouton pour voir les métadonnées détaillées du firmware
Taille	Taille du fichier au format lisible par l'homme
MD5	Somme de contrôle MD5 (cliquez pour copier)
Téléchargements	Nombre de fois que le firmware a été téléchargé
Actions	Boutons Copier l'URL, Télécharger, Supprimer

Métadonnées du Firmware

Cliquez sur le bouton **Info** sur n'importe quelle ligne de firmware pour voir les métadonnées détaillées extraites du paquet :

La modal des métadonnées affiche des détails complets sur le paquet de firmware.

Champ	Description
Nom de Fichier	Nom complet du paquet
Version	Version du logiciel de la station de base (par exemple, SBTS25R1)
Date de Construction	Horodatage lorsque le firmware a été construit
Taille	Taille du fichier
Fichier Modifié	Quand le fichier a été téléchargé sur RAN Monitor
Version du Logiciel	Chaîne de version complète du logiciel (par exemple, FTM_SBTS25R1_2025.05.27_0097)
Version PS	Version de la sortie du logiciel de la plateforme
Version du Noyau	Version du noyau Linux
Version LTE	Version du logiciel LTE (par exemple, FL19A)
Version WCDMA	Version du logiciel WCDMA (par exemple, WBTSFP20C)
Unités Matérielles Supportées	Liste des modules matériels compatibles (ASCE, ASCF, FCTJ, etc.)
Somme de Contrôle MD5	Somme de contrôle d'intégrité du fichier
URL de Téléchargement	URL complète pour les téléchargements de la station de base

Les métadonnées sont automatiquement extraites du paquet de firmware lors du téléchargement et mises en cache pour un accès rapide.

Boutons d'Action

Bouton	Description
Info	Voir les métadonnées détaillées du firmware dans une modal
Copier l'URL	Copier l'URL de téléchargement du firmware dans le presse-papiers
Télécharger	Télécharger le fichier de firmware directement
Supprimer	Supprimer le fichier de firmware du stockage

Ligne d'URL de Téléchargement

Sous chaque entrée de firmware, l'URL de téléchargement complète est affichée :

```
http://<ran-monitor-ip>:4000/firmware/nokia/<filename>.zip
```

Cette URL est saisie dans le champ d'URL "Serveur distant" de WebEM.

Sommes de Contrôle MD5

Calcul Automatique

Les sommes de contrôle MD5 sont calculées automatiquement lorsque les fichiers de firmware sont listés. La somme de contrôle est mise en cache dans un fichier `.md5` à côté du paquet de firmware pour des recherches rapides ultérieures.

Fichiers de Somme de Contrôle

Pour chaque paquet de firmware, un fichier `.md5` correspondant est créé :

```
/var/firmware/nokia/
├── SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zi
└──
SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip.md
```

Le fichier `.md5` contient la somme de contrôle hexadécimale en minuscules :

```
a1b2c3d4e5f6789012345678abcdef01
```

Vérification

Utilisez la somme de contrôle MD5 pour vérifier l'intégrité du firmware après le téléchargement :

Linux/macOS :

```
md5sum
SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip
```

Windows (PowerShell) :

```
Get-FileHash -Algorithm MD5
SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip
```

Installation du Firmware sur une Station de Base

RAN Monitor peut installer un paquet de firmware téléchargé directement sur une station de base — il n'est pas nécessaire de se connecter manuellement à

l'interface WebEM de chaque site. RAN Monitor se connecte à l'interface de gestion logicielle de la station de base et effectue le téléchargement, l'activation et le redémarrage du logiciel en votre nom, puis confirme que la station de base est revenue avec la version logicielle attendue.

La même opération peut être pilotée de deux manières :

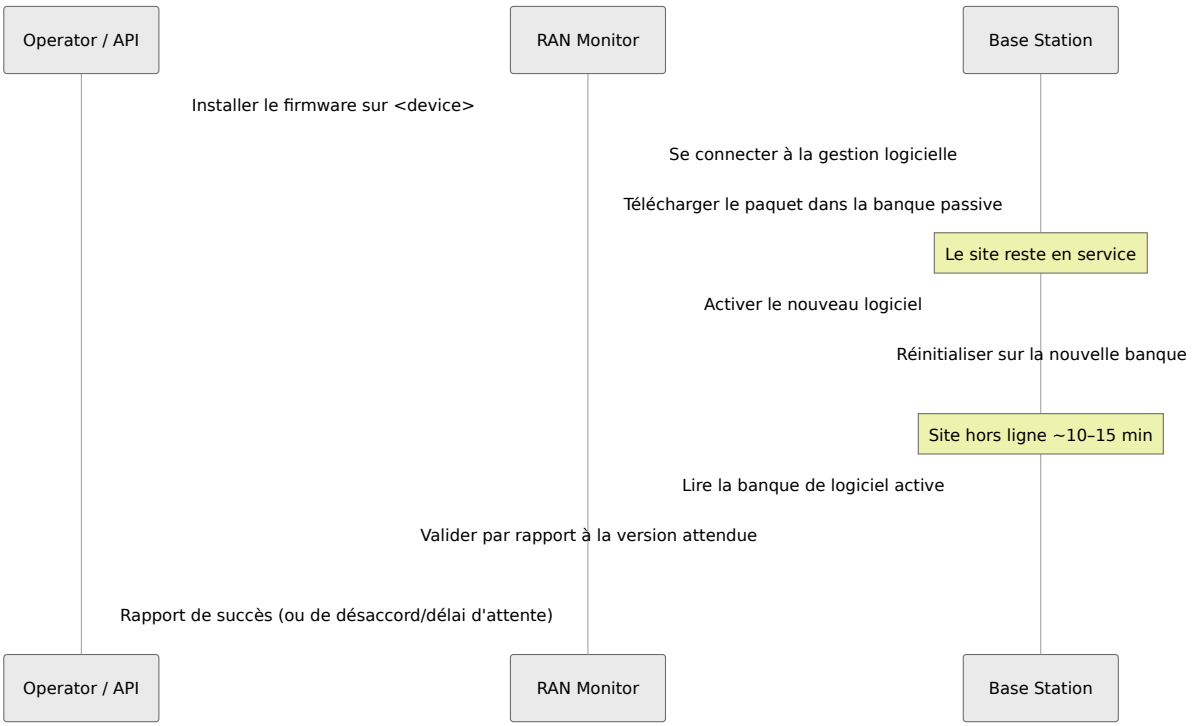
- Depuis la **page Firmware** dans l'interface web — pointer et cliquer. Voir Via l'Interface Web.
- Depuis l'**API JSON** — pour l'automatisation et les déploiements en masse. Voir Via l'API.

Étapes d'Installation

Une installation reflète le modèle logiciel à deux banques de la station de base :

Étape	Ce qui se passe	Impact sur le site
Téléchargement	Le nouveau logiciel est transféré dans la banque de logiciel passive (de secours) de la station de base.	Aucun — le site reste en service avec son logiciel actuel.
Activation	La station de base passe au nouveau logiciel téléchargé et se réinitialise dessus.	Le site est hors ligne pendant environ 10 à 15 minutes pendant la réinitialisation.

Vous pouvez exécuter les deux étapes ensemble (télécharger et activer en une seule opération) ou séparément — par exemple, télécharger avant une fenêtre de maintenance et activer plus tard.



Rétrogradation

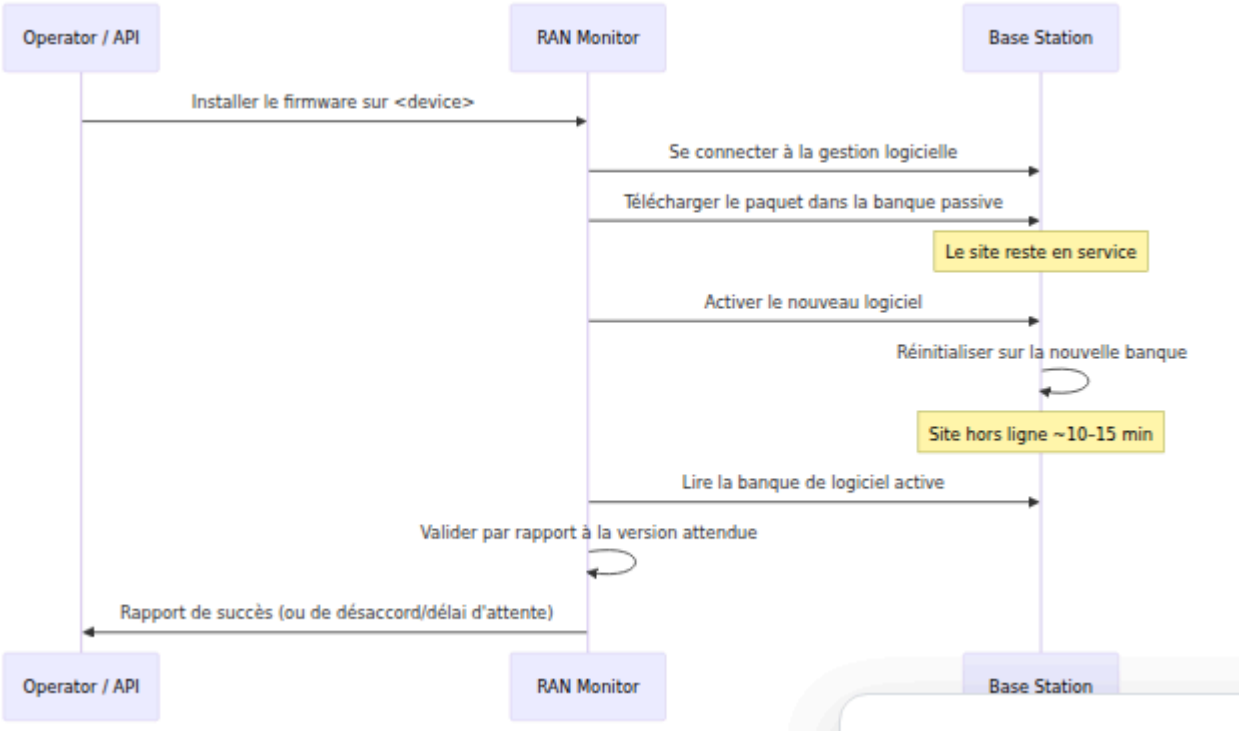
Une **rétrogradation** active la banque de logiciel passive de la station de base (le logiciel précédemment exécuté) et se réinitialise dessus. Utilisez-la pour annuler une mise à jour problématique. La rétrogradation n'implique pas de fichier de firmware — elle revient simplement au logiciel déjà présent dans la banque de secours.

Validation Post-Réinitialisation

Chaque fois qu'une opération réinitialise la station de base (une activation ou une rétrogradation), RAN Monitor attend que la station de base revienne et confirme que **la banque de logiciel active correspond à la version attendue**. L'opération n'est signalée comme **réussie** qu'une fois cela confirmé. Si la station de base redémarre sur une version différente, ou ne revient pas dans le temps imparti, l'opération est signalée comme **échouée** — donc un résultat vert signifie toujours que le logiciel cible fonctionne réellement.

Cycle de Vie de l'Opération

Étant donné qu'une installation peut prendre plusieurs minutes (téléchargement, activation, réinitialisation et validation), l'opération s'exécute en arrière-plan. L'interface web montre la progression en direct ; l'API renvoie un identifiant de travail que vous interrogez pour connaître l'état.



Statut	Signification
`running`	L'opération est en cours (téléchargement et/ou activation).
`validating`	La station de base a été réinitialisée et RAN Monitor confirme la version en cours d'exécution.
`succeeded`	L'opération est terminée et (si elle a réinitialisé la station de base) la version attendue a été confirmée.
`failed`	L'opération a échoué. Voir le champ `error` pour la raison (par exemple, erreur de transfert, désaccord de version, délai d'attente de validation).

Via l'Interface Web

Depuis la page Firmware :

1. Localisez le paquet de firmware dans la liste et cliquez sur **Pousser**.
2. Sélectionnez la **station de base cible** dans la liste des appareils (seules les stations de base enregistrées sont affichées).
3. Choisissez l'action :
   - **Télécharger sur BTS** — préparer le logiciel dans la banque passive uniquement (pas de réinitialisation ; le site reste en service).
   - **Activer sur BTS** — télécharger, passer au nouveau logiciel et réinitialiser (le site passe hors ligne pour la réinitialisation).
   - **Rétrograder vers le logiciel précédent** — réactiver la banque passive et réinitialiser.
4. La progression est affichée en direct — l'étape actuelle, une barre de progression de transfert et, après une réinitialisation, un indicateur "validant" pendant que RAN Monitor confirme que la station de base est revenue sur la version cible.
5. À l'achèvement, le résultat rapporte la version logicielle en cours confirmée (ou la raison de l'échec).

> **Remarque :** L'activation et la rétrogradation redémarrent la station de base. Le site est hors service pendant environ 10 à 15 minutes. Planifiez ces opérations pour une fenêtre de maintenance.

Via l'API

Les opérations `/api/nokia/firmware` sont servies sur HTTPS via l'API RAN Monitor (port `8443`). Le point de téléchargement est servi sur l'interface web (même origine que la page Firmware).

Télécharger un Paquet de Firmware

Stockez un paquet dans le dépôt avant de l'installer. Le corps de la requête est le fichier brut `.zip`.

Point de terminaison : `POST /api/firmware/upload?filename=<name>.zip`

```
curl -k -X POST \
  --data-binary
@SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip \
  "https://<ran-monitor-ip>:9443/api/firmware/upload?
filename=SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A
```

Réponse (200) :

```
{
  "ok": true,
  "path":
"/var/firmware/nokia/SBTS25R1_ENB_0000_001046_000000_release_BTSSM_do
  "bytes": 9602426993
}
```

Paramètre	Type	Requis	Par défaut	Description
`filename`	String (query)	Oui	-	Nom de fichier cible à stocker. Doit être un `.zip` et suivre la convention de nommage de Nokia. Renvoie `409 already_exists` si un fichier de ce nom est déjà présent.

Déclencher une Installation

Point de terminaison : `POST /api/nokia/firmware/install`

```
curl -k -X POST "https://<ran-monitor-
ip>:8443/api/nokia/firmware/install" \
  -H "Content-Type: application/json" \
  -d '{
    "device": "2057_Guymon_TOY",
    "filename":
"SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip",
    "activate": true
  }'
```

Réponse (202 Accepted) :


```
{
  "data": {
    "id": "6f1c8b2a-9d0e-4f3a-8c11-2b7e5a9d4c30",
    "status": "running",
    "device": "2057_Guymon_TOY",
    "filename":
"SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip",
    "activate": true,
    "status_url": "/api/nokia/firmware/install/6f1c8b2a-9d0e-4f3a-
8c11-2b7e5a9d4c30"
  }
}
```

Paramètre	Type	Requis	Par défaut	Description
`device`	String	Oui	-	Nom de la station de base tel qu'enregistré dans RAN Monitor.
`filename`	String	Oui	-	Nom de fichier de firmware `.zip` déjà téléchargé dans le dépôt.
`activate`	Boolean	Non	`true`	Lorsque `true`, la station de base passe au nouveau logiciel et se réinitialise. Lorsque `false`, le logiciel est uniquement préparé dans la banque passive (pas de réinitialisation, le site reste en service).

L'installation s'exécute en arrière-plan ; interrogez l'`status_url` pour connaître la progression. Les réponses d'erreur utilisent `{ "error": { "code", "message" } }` — par exemple `404 FIRMWARE_NOT_FOUND` ou `404 DEVICE_NOT_FOUND`.

Déclencher une Rétrogradation

Point de terminaison : `POST /api/nokia/firmware/rollback`

```
curl -k -X POST "https://<ran-monitor-
ip>:8443/api/nokia/firmware/rollback" \
  -H "Content-Type: application/json" \
  -d '{ "device": "2057_Guymon_TOY" }'
```

Réponse (202 Accepted) : même structure que l'installation, avec `"operation": "rollback"`.

Paramètre	Type	Requis	Par défaut	Description
`device`	String	Oui	-	Nom de la station de base à rétrograder vers sa banque de logiciel passive (précédente).

Interroger l'État de l'Opération

Point de terminaison : `GET /api/nokia/firmware/install/<id>`

```
curl -k "https://<ran-monitor-
ip>:8443/api/nokia/firmware/install/6f1c8b2a-9d0e-4f3a-8c11-
2b7e5a9d4c30"
```

Réponse (200) :


```
{
  "data": {
    "id": "6f1c8b2a-9d0e-4f3a-8c11-2b7e5a9d4c30",
    "operation": "install",
    "status": "validating",
    "device": "2057_Guymon_TOY",
    "filename":
"SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip",
    "activate": true,
    "step": "validating",
    "progress": 100,
    "status_line": "attente que BTS redémarre sur
SBTS25R1_ENB_0000_001046_000000",
    "validated": { "active": "SBTS25R1_ENB_0000_001046_000000",
"expected": "SBTS25R1_ENB_0000_001046_000000", "ok": true },
    "error": null
  }
}
```

Champ	Description
`operation`	`install` ou `rollback`.
`status`	État global : `running`, `validating`, `succeeded`, ou `failed`.
`step`	Phase actuelle (par exemple, `transfer`, `validating`).
`progress`	Progrès du transfert en pourcentage (0–100).
`status_line`	Description lisible par l'homme de l'activité actuelle.
`validated`	Vérification post-réinitialisation : `active` (version sur laquelle la station de base a redémarré), `expected` (version cible), et `ok` (si elles correspondent).
`error`	Raison de l'échec lorsque `status` est `failed` ; `null` sinon.

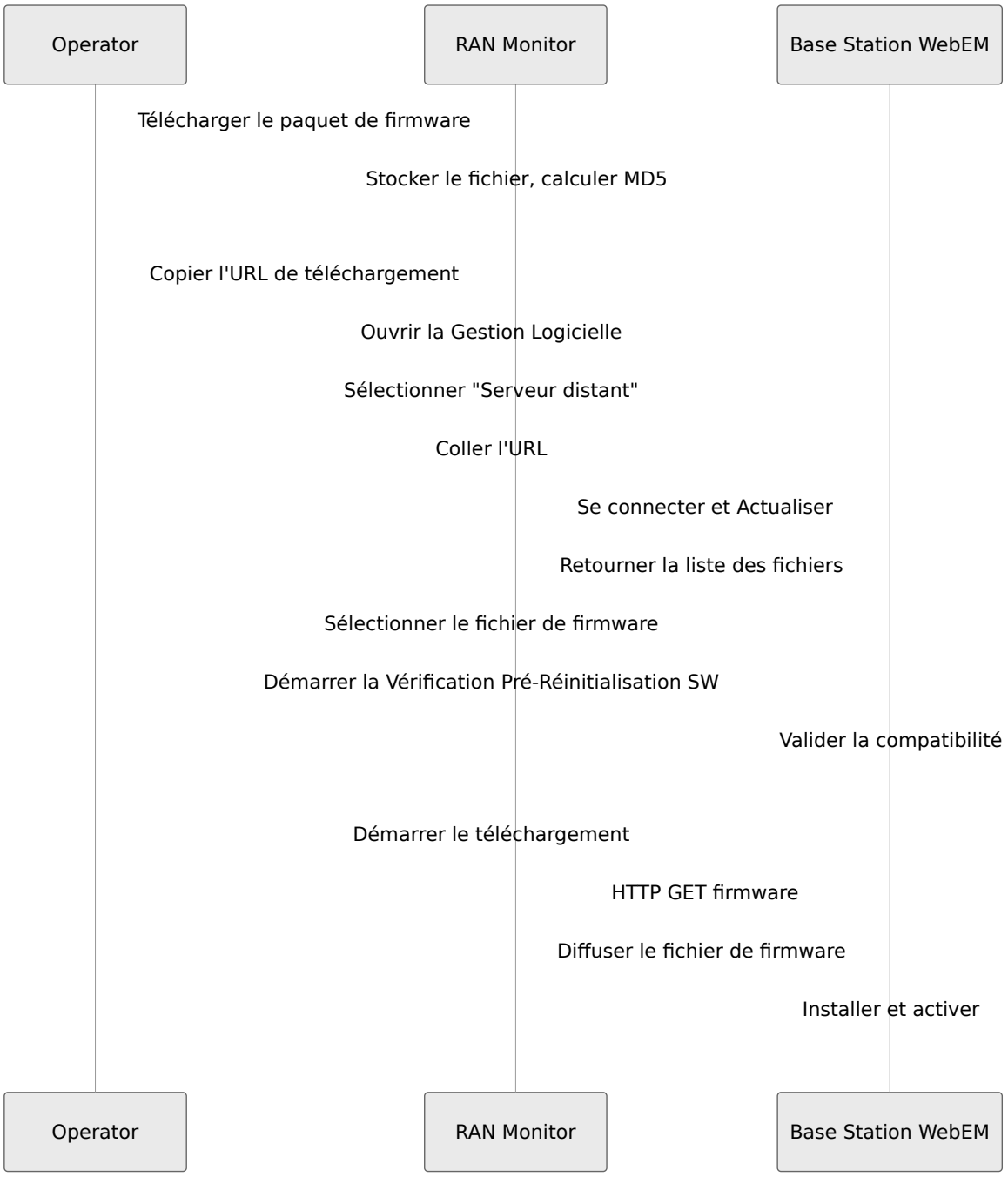
Flux de Mise à Jour Logicielle de la Station de Base

> Ceci est l'alternative manuelle, pilotée par la station de base, à l'installation directe ci-dessus. Utilisez-la lorsque vous préférez piloter WebEM vous-même, ou lorsque la station de base doit récupérer le paquet plutôt que d'être installé.

Prérequis

- Paquet de firmware téléchargé sur RAN Monitor
- Connectivité réseau de la station de base à RAN Monitor
- Accès à l'interface WebEM de la station de base

Processus Étape par Étape



Étapes Détailées

1. Télécharger le Firmware sur RAN Monitor

Naviguez vers la page de Gestion du Firmware et téléchargez le paquet logiciel :

- Allez à `https://<ran-monitor-ip>:9443/nokia/firmware`

- Téléchargez le paquet de firmware `.zip`
- Vérifiez que le fichier apparaît dans la liste des firmwares avec le bon MD5

2. Copier l'URL de Téléchargement

Cliquez sur **Copier l'URL** à côté du paquet de firmware. Le format de l'URL est :

```
http://<ran-monitor-ip>:4000/firmware/nokia/<filename>.zip
```

3. Accéder à la Gestion Logicielle WebEM

Ouvrez l'interface WebEM de la station de base :

- Allez à **Gestion Logicielle** > **Mise à Jour Logicielle**
- Voir les versions logicielles actuelles des BTS (Actif et Passif)

4. Configurer le Serveur Distant

Dans la section "Télécharger et activer le logiciel depuis" de WebEM :

1. Sélectionnez **Serveur distant**
2. Collez l'URL copiée dans le champ **URL**
3. Cliquez sur **Se connecter et Actualiser**

WebEM se connecte à RAN Monitor et récupère la liste des fichiers.

5. Sélectionner le Firmware et Démarrer la Mise à Jour

1. Sélectionnez le fichier de firmware dans le menu déroulant **Fichier logiciel**
2. Optionnellement, exécutez **Démarrer la Vérification Pré-Réinitialisation SW** pour vérifier la compatibilité
3. Cochez **Activer le logiciel après le téléchargement** si une activation immédiate est souhaitée
4. Cliquez sur **Démarrer** pour commencer la mise à jour logicielle

Vérification Post-Mise à Jour

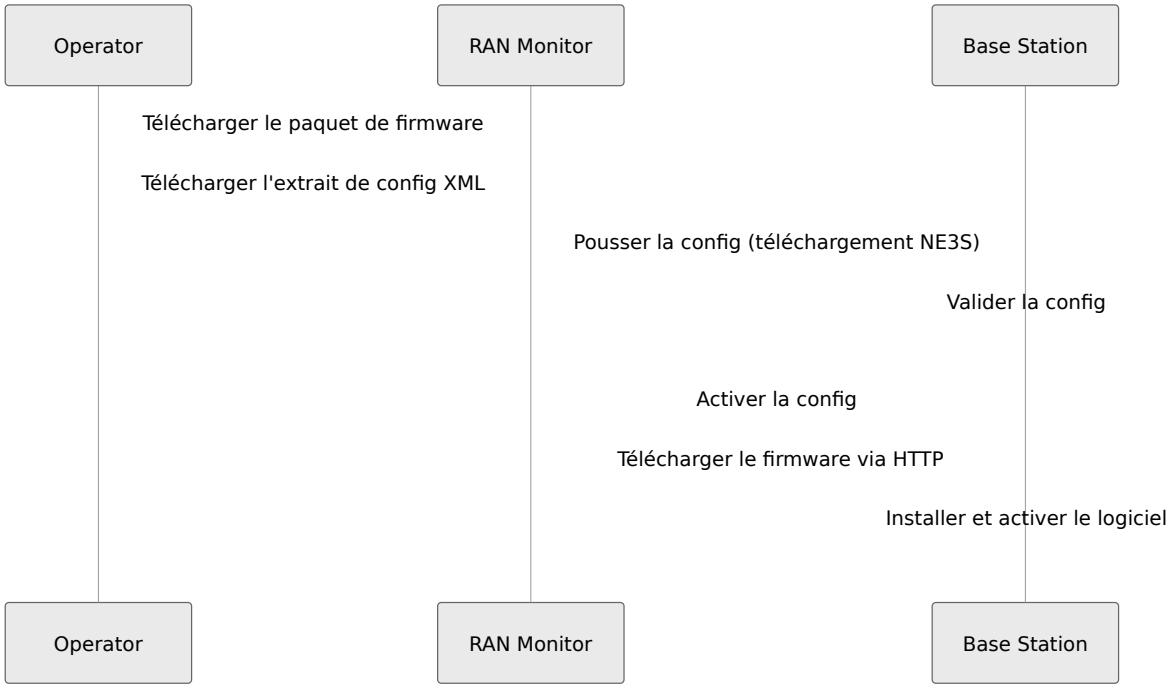
Après la mise à jour :

1. Vérifiez que la nouvelle version logicielle apparaît comme **Active** dans WebEM
2. Vérifiez RAN Monitor pour tout nouvel alarme de la station de base
3. Confirmez la restauration du service cellulaire via les KPI

Mise à Jour Logicielle à Distance via Poussée de Configuration

Au lieu d'accéder manuellement à WebEM sur chaque station de base, vous pouvez déclencher des mises à jour logicielles à distance en téléchargeant un extrait de configuration via la fonction de gestion de configuration de RAN Monitor.

Comment Cela Fonctionne



Extrait de Configuration

Créez un fichier XML contenant les paramètres de téléchargement du logiciel. La station de base récupérera le firmware à partir de l'URL spécifiée lorsque la configuration sera activée.

Exemple : `sw_update.xml`

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="plan" scope="changes">
<managedObject class="com.nokia.srbts.btsswm:BTSSWM" distName="MRBTS-
operation="update">
  <p name="swPkgUrl">http://{ran-monitor-
ip}:4000/firmware/nokia/SBTS25R1_ENB_0000_001046_000000_release_BTSSM
  <p name="swPkgActivate">true</p>
</managedObject>
</cmData>
</raml>
```

Remplacez :

- `{site_id}` - L'ID MRBTS de la station de base cible (par exemple, `256`, `2057`)
- `{ran-monitor-ip}` - L'adresse IP ou le nom d'hôte de RAN Monitor accessible depuis la station de base

Pousser la Configuration

1. Naviguez vers la page de détails de la station de base dans RAN Monitor
2. Cliquez sur **Opérations de Config** pour ouvrir les opérations de configuration
3. Téléchargez l'extrait `sw_update.xml`
4. Cliquez sur **Valider** pour vérifier la configuration
5. Cliquez sur **Activer** pour appliquer la configuration

La station de base téléchargera et installera automatiquement le firmware.

Mises à Jour en Masse

Pour mettre à jour plusieurs sites, créez un extrait XML séparé pour chaque site (avec le bon ID MRBTS) et poussez-les séquentiellement via RAN Monitor, ou utilisez l'API pour automatiser le processus.

Référence des Paramètres

Paramètre	Description
`swPkgUrl`	URL HTTP du paquet de firmware à télécharger
`swPkgActivate`	Défini sur `true` pour activer automatiquement après le téléchargement

---

Suivi des Téléchargements

RAN Monitor suit les téléchargements de firmware pour aider à identifier quelles stations de base ont récupéré des paquets logiciels.

Informations Suivies

Pour chaque téléchargement, les informations suivantes sont enregistrées :

Champ	Description
Adresse IP	Adresse IP distante du téléchargeur
Nom d'Hôte	Nom d'hôte résolu ou nom AirScale correspondant
Horodatage	Date et heure du téléchargement

Affichage de l'Historique des Téléchargements

La colonne **Téléchargements** dans la liste des firmwares montre le nombre total de téléchargements. Survolez le nombre pour voir les détails des téléchargements récents, y compris les adresses IP et les horodatages.

Les données de suivi des téléchargements sont persistées sur disque et survivent aux redémarrages de l'application.

Accès API

Lister les Fichiers de Firmware

Récupérez l'inventaire des firmwares via l'API REST :

Point de terminaison : `GET /api/firmware/nokia`

Réponse :

```
{
  "firmware": [
    {
      "filename": "SBTS25R1_ENB_0000_001046_000000_release_BTSSM_dowr
      "size": 1073741824,
      "size_formatted": "1.0 GB",
      "modified": "2025-01-15T10:30:00Z",
      "download_url": "http://ran-
monitor:4000/firmware/nokia/SBTS25R1_ENB_0000_001046_000000_release_E
      "metadata": {
        "release": "SBTS25R1",
        "build": "0000_001046_000000",
        "variant": "release",
        "suffix": "A54",
        "type": "BTS Software"
      }
    }
  ],
  "stats": {
    "file_count": 3,
    "total_size": 3221225472,
    "total_size_formatted": "3.0 GB",
    "storage_path": "/var/firmware/nokia"
  }
}
```


Télécharger un Fichier de Firmware

Point de terminaison : `GET /firmware/nokia/<filename>`

Réponse : Téléchargement de fichier binaire avec `Content-Type: application/zip`

Référence de Configuration

URL de Téléchargement de Base

Configurez l'URL de base accessible publiquement pour les téléchargements de firmware :

```
config :ran_monitor,
  firmware_base_url: "http://ran-monitor.example.com:4000"
```

Paramètre	Type	Requis	Par défaut	Descr
`firmware_base_url`	String	Non	`http://localhost:4000`	URL de utilisée la génér des URL téléchar Définiss sur le nc d'hôte/II accessib publique du serve Monitor.

Ce paramètre affecte les URL affichées dans l'interface web et renvoyées par l'API. Le service de fichiers réel utilise le port HTTP configuré de l'application.

Dépannage

Échec de Téléchargement

Symptômes : Le téléchargement du fichier montre une erreur ou ne se termine jamais

Causes possibles :

- Le fichier dépasse la taille maximale de 15 Go
- Le fichier n'est pas un fichier `.zip`
- Espace disque insuffisant dans le chemin de stockage
- Permission refusée sur le répertoire de stockage

Résolution :

1. Vérifiez que la taille du fichier est inférieure à 15 Go
2. Confirmez que l'extension du fichier est `.zip`
3. Vérifiez l'espace disque disponible : `df -h /var/firmware/nokia`
4. Vérifiez les permissions du répertoire : `ls -la /var/firmware`

La Station de Base Ne Peut Pas Télécharger

Symptômes : "Se connecter et actualiser" de WebEM échoue ou le téléchargement expire

Causes possibles :

- Problème de connectivité réseau entre la station de base et RAN Monitor
- Pare-feu bloquant le port HTTP 4000
- URL incorrecte (mauvaise IP ou nom d'hôte)

Résolution :

1. Vérifiez le chemin réseau : ping RAN Monitor depuis le réseau de la station de base
2. Vérifiez que le pare-feu autorise le port 4000 entrant

3. Confirmez que l'URL utilise la bonne IP/nom d'hôte accessible depuis la station de base
4. Testez l'URL dans un navigateur depuis le même segment de réseau

MD5 Montre "calcul en cours..."

Symptômes : La colonne MD5 affiche "calcul en cours..." et ne se met jamais à jour

Causes possibles :

- Fichier très volumineux encore en cours de traitement
- Problème de permission sur le système de fichiers empêchant la création du fichier `.md5`

Résolution :

1. Attendez que le calcul soit terminé (les fichiers volumineux prennent plus de temps)
2. Cliquez sur **Actualiser** pour recharger la page
3. Vérifiez que les permissions du répertoire de stockage permettent la création de fichiers

Erreur de Fichier Déjà Existant

Symptômes : Le téléchargement échoue avec une erreur "déjà existant"

Résolution :

1. Supprimez le fichier existant si le remplacement est prévu
2. Renommez le nouveau fichier si les deux versions sont nécessaires
3. Vérifiez que vous ne téléchargez pas accidentellement le même fichier à nouveau

Collection de la zone Flexi

Collecte de métriques de performance et d'alarmes pour les stations de base Nokia Flexi Zone classiques

RAN Monitor est multi-fournisseur. Les stations de base Nokia **Flexi Zone** classiques (FZM, par exemple le Flexi Zone Indoor Pico) sont prises en charge aux côtés de Nokia AirScale, Casa Systems et Baicells.

Les unités Flexi Zone sont intégrées via l'API, comme Casa. Vous soumettez l'adresse IP de la station de base et ses identifiants de gestion à RAN Monitor. RAN Monitor configure ensuite la station de base pour envoyer ses métriques de performance (PM) et ses alarmes à RAN Monitor via HTTP. Après l'intégration, l'unité rapporte d'elle-même sur un minuteur. Aucune action supplémentaire n'est nécessaire.

Table des matières

1. Aperçu
2. Architecture
3. Intégration d'une unité
4. Configuration
5. Ce qui est collecté
6. API
7. Métriques
8. Dépannage

Aperçu

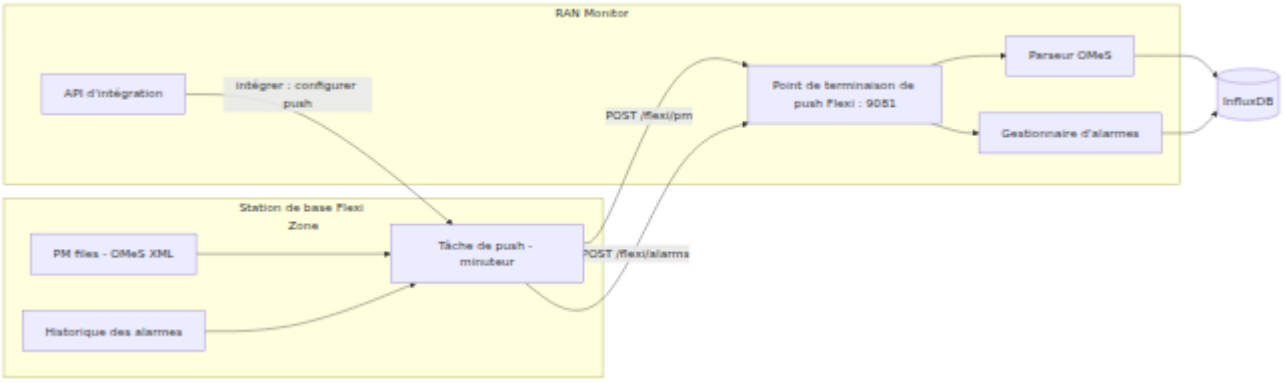
Une station de base Flexi Zone classique n'a pas l'interface webhook NE3S que utilise AirScale. RAN Monitor collecte à partir de celle-ci avec un modèle de **push** à la place :

- Vous intégrez l'unité une fois via l'API. Vous donnez à RAN Monitor l'adresse IP de la station de base et ses identifiants de gestion.
- RAN Monitor configure l'unité pour envoyer de nouveaux fichiers PM et un instantané d'alarme à RAN Monitor toutes les quelques minutes.
- RAN Monitor reçoit chaque push, analyse les compteurs et les écrit dans InfluxDB. Il enregistre également les alarmes actives.

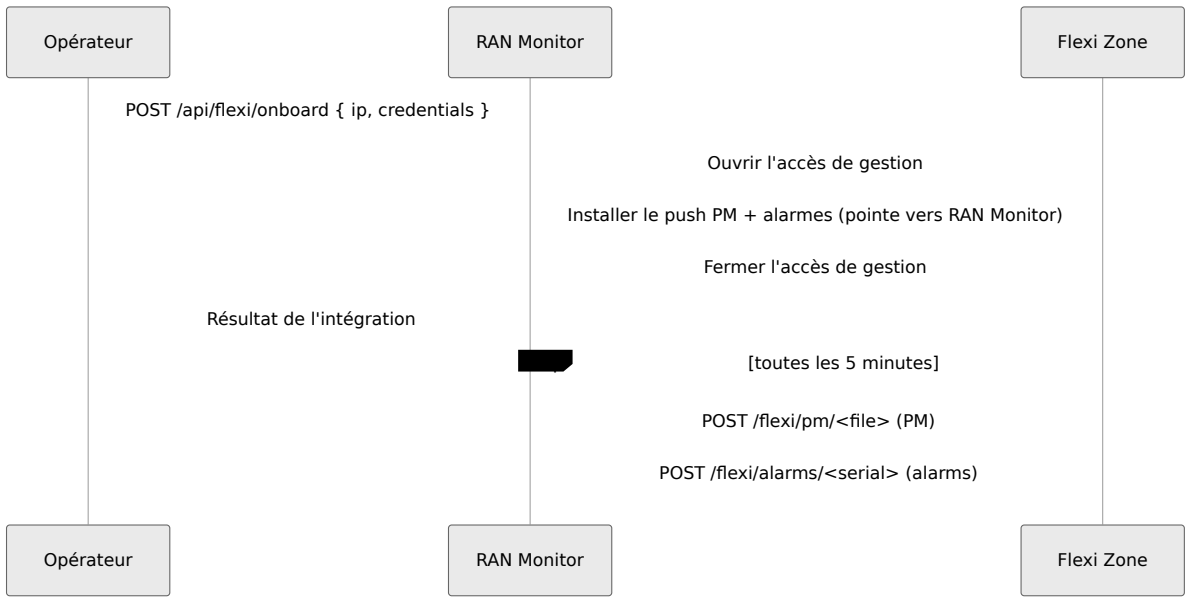
Les données PM utilisent le format XML **OMeS** de Nokia, le même format de compteur que AirScale. RAN Monitor réutilise le parseur OMeS existant, donc les compteurs Flexi Zone apparaissent à côté des autres fournisseurs sans configuration supplémentaire.

L'accès de gestion à la station de base est ouvert uniquement pendant l'intégration. RAN Monitor le ferme à nouveau à la fin. Le push régulier de PM et d'alarmes ne l'utilise pas.

Architecture



La séquence d'intégration :



Intégration d'une unité

Pour intégrer une Flexi Zone, soumettez son IP et ses identifiants de gestion à l'API :

```
POST /api/flexi/onboard
{
  "ip": "10.7.15.67",
  "bts_username": "Nemuadmin",
  "bts_password": "nemuuser",
  "ssh_password": "<service-account password>"
}
```

RAN Monitor effectue alors automatiquement les actions suivantes :

1. Il ouvre l'accès de gestion sur la station de base.
2. Il installe une petite tâche de push sur l'unité. La tâche envoie de nouveaux fichiers PM et l'instantané d'alarme à RAN Monitor.
3. Il démarre la tâche. La tâche s'exécute toutes les 5 minutes.
4. Il ferme à nouveau l'accès de gestion.

L'unité commence à rapporter dans quelques minutes. La station de base conserve la tâche de push après l'intégration.

Paramètres de la requête d'intégration :

Paramètre	Type	Requis	Par défaut	Description
`ip`	Chaîne	Oui	-	Adresse IP OAM de la station de base, accessible depuis RAN Monitor.
`bts_username`	Chaîne	Non	`Nemuadmin`	Nom d'utilisateur pour l'interface de gestion web de la station de base.
`bts_password`	Chaîne	Non	`nemuuser`	Mot de passe pour l'interface de gestion web de la station de base.
`ssh_username`	Chaîne	Non	Compte de service Nokia	Compte de service utilisé pour installer la tâche de push.
`ssh_password`	Chaîne	Non	Par défaut de Nokia	Mot de passe du compte de service. À définir lorsque l'opérateur l'a changé.
`push_interval`	Chaîne	Non	`5min`	Fréquence à laquelle la station de base pousse PM et alarmes. Utilisez une durée systemd, par exemple `5min` ou `15min`.
`keep_ssh`	Booléen	Non	`false`	Laisser l'accès de gestion ouvert après

Paramètre	Type	Requis	Par défaut	Description
				l'intégration. Gardez `false` en production.

RAN Monitor ne retourne jamais les identifiants dans la réponse. Une réponse de succès indique l'IP cible, l'adresse RAN Monitor à laquelle l'unité poussera, les étapes d'intégration et si l'accès de gestion a été laissé ouvert :

```
{
  "status": "ok",
  "ip": "10.7.15.67",
  "ranmon_host": "10.4.2.250",
  "ranmon_port": 9081,
  "ssh_left_enabled": false,
  "steps": ["activation de l'accès de gestion", "installation de
la tâche de push", "accès de gestion fermé"]
}
```

> **Remarque sur le redémarrage :** RAN Monitor ne redémarre pas l'unité pendant l'intégration. Le push commence immédiatement. Si la station de base redémarre plus tard, ou si un ingénieur la remet en service avec BTS Site Manager ou NetAct, relancez l'intégration pour restaurer la tâche de push.

Configuration

RAN Monitor reçoit les pushes Flexi Zone sur un point de terminaison dédié. Définissez le point de terminaison dans `runtime.exs` :

```
config :ran_monitor, :nokia,
  flexi_push: [
    port: 9081,
    advertised_host: "10.4.2.250"
  ]
```

Paramètres :

Paramètre	Type	Requis	Par défaut	Description
`port`	Entier	Non	9081	Port TCP pour les pushes PM et alarmes Flexi Zone entrants. Remplacez par la variable d'environnement `FLEXI_PUSH_P0RT`.
`advertised_host`	Chaîne	Non	Adresse locale de RAN Monitor	Adresse que RAN Monitor écrit dans la tâche de push de la station de base. La station de base l'utilise pour atteindre RAN Monitor. Définissez ceci lorsque RAN Monitor a plus d'une adresse ou est derrière un NAT.

La station de base doit atteindre `http://<advertised_host>:<port>`. Confirmez que les règles de pare-feu autorisent ce trafic depuis le réseau OAM de la station de base.

Ce qui est collecté

Métriques de performance. L'unité envoie des fichiers PM OMeS. Chaque fichier contient une ou plusieurs périodes de mesure. RAN Monitor écrit chaque compteur dans InfluxDB, tagué avec l'identité de la station de base. Les types de mesures de transport sont toujours présents. Les compteurs radio et de

cellule apparaissent lorsqu'une cellule transporte du trafic. Types de mesures typiques :

Type de mesure	Zone
`LTE_Ethernet_Link`	Lien Ethernet de retour
`LTE_ETHIF_stats`	Interface Ethernet
`LTE_IP_Stats`	Couche IP
`LTE_IP_Filtering`	Filtrage de paquets IP
`LTE_IPSec`	IPsec
`LTE_L2_SWITCH_Stats`	Commutateur de couche 2
`LTE_TAC_Stats`	Contrôle d'admission de transport

Pour les définitions de compteurs, voir la Référence des compteurs Nokia.

Alarmes. L'unité envoie sa liste de défauts actifs. RAN Monitor enregistre chaque défaut actif avec son identité de défaut, son nom, son objet source et son horodatage. Pour la gestion des alarmes, voir le Guide de gestion des alarmes.

API

Méthode + chemin	But
`POST /api/flexi/onboard`	Intégrer une station de base par IP. RAN Monitor configure l'unité pour pousser PM et alarmes, puis ferme l'accès de gestion.
`GET /api/flexi/devices`	Lister les unités Flexi Zone qui ont poussé. Affiche le numéro de série, l'IP source, le dernier temps PM et le dernier temps d'alarme.

Les deux points de terminaison sont sur le port de point de terminaison de push Flexi (par défaut 9081).

Métriques

RAN Monitor écrit les compteurs Flexi Zone dans InfluxDB dans les mêmes mesures que les autres sources Nokia. Interrogez-les par le tag d'identité de la station de base. Pour les métriques au niveau de l'application Prometheus que RAN Monitor expose concernant l'ingestion, voir la Référence des métriques.

Dépannage

L'unité n'apparaît pas après l'intégration

Symptômes : `GET /api/flexi/devices` ne liste pas la station de base.

Causes possibles :

- La station de base ne peut pas atteindre `advertised_host:port`.
- Un pare-feu bloque le trafic de push.
- Les identifiants de gestion dans la requête d'intégration sont incorrects.

Résolution :

1. Confirmez que `advertised_host` et `port` sont corrects dans `runtime.exs`.
2. Confirmez que le réseau OAM de la station de base peut atteindre RAN Monitor sur ce port.
3. Relancez l'intégration avec les identifiants de gestion corrects.

PM arrêté après un redémarrage de la station de base

Symptômes : L'unité a rapporté auparavant, mais s'est arrêtée après la maintenance.

Causes possibles :

- L'unité a redémarré. La tâche de push ne survit pas à un redémarrage.
- Un ingénieur a remis l'unité en service avec BTS Site Manager ou NetAct.

Résolution :

1. Relancez l'intégration pour cette station de base.

Les alarmes se mettent à jour mais PM ne le fait pas

Symptômes : L'heure de l'alarme avance, mais aucun nouveau PM n'arrive.

Causes possibles :

- L'unité n'a produit aucun nouveau fichier PM depuis le dernier push.
- Aucune cellule ne transporte de trafic, donc seuls des compteurs de transport sont produits.

Résolution :

1. Attendez la prochaine période PM.
2. Confirmez qu'une cellule est active si vous attendez des compteurs radio.

Introduction à RAN Monitor

Guide de démarrage rapide pour déployer et configurer RAN Monitor

Instructions étape par étape pour configurer RAN Monitor dans votre environnement

---

Table des matières

1. Aperçu
2. Prérequis
3. Processus de configuration initiale
4. Vérification
5. Étapes suivantes

Aperçu

Ce guide vous accompagne dans le déploiement initial de RAN Monitor, de la préparation de l'infrastructure à la première connexion de station de base.

Ce que vous accomplirez

À la fin de ce guide, vous aurez :

- ✓ Préparé l'infrastructure requise (MySQL, InfluxDB)
- ✓ Configuré RAN Monitor avec les détails de votre environnement
- ✓ Démarré l'application RAN Monitor
- ✓ Connecté votre première station de base Nokia AirScale
- ✓ Vérifié que les métriques sont envoyées à InfluxDB

- ✓ Accédé au tableau de bord de l'interface Web

Temps estimé : 30-60 minutes pour la configuration initiale

Prérequis

Avant de déployer RAN Monitor, assurez-vous d'avoir les éléments suivants :

Exigences d'infrastructure

Serveur de base de données MySQL

- Version : MySQL 5.7+ ou MariaDB 10.3+
- Accès : Connectivité réseau depuis le serveur RAN Monitor
- Permissions : Privilèges CREATE, SELECT, INSERT, UPDATE, DELETE
- Base de données : Base de données vide créée pour RAN Monitor
- Recommandation : Instance ou schéma de base de données dédié

Base de données InfluxDB Time-Series

- Version : InfluxDB 1.8+ ou 2.0+
- Accès : Connectivité réseau depuis le serveur RAN Monitor
- Bucket/Base de données : Créé et prêt pour le stockage des métriques
- Jeton API : Avec permissions d'écriture sur le bucket (InfluxDB 2.x)
- Stockage : Espace disque suffisant pour votre politique de rétention

Serveur RAN Monitor

- OS : Linux (Ubuntu 20.04+, CentOS 8+, ou similaire)
- RAM : 4 Go minimum, 8 Go recommandé
- CPU : 2 cœurs minimum, 4+ cœurs recommandé
- Disque : 20 Go minimum pour l'application et les journaux
- Réseau : Connectivité aux stations de base, MySQL et InfluxDB

Exigences réseau

Connectivité réseau

- RAN Monitor → Stations de base Nokia AirScale (port 8080)
- Stations de base Nokia → RAN Monitor (port 9076 pour webhooks)
- Femtocells Casa → RAN Monitor (port 9077 pour PM push) — voir Collecte PM Casa
- RAN Monitor → eNBs Baicells (sortant 443, basé sur le sondage) — voir Collecte Baicells
- RAN Monitor → gNBs OCUDU (sortant 8001, WebSocket) : voir Collecte OCUDU
- RAN Monitor → MySQL (port 3306)
- RAN Monitor → InfluxDB (port 8086)
- Opérateurs → Interface Web RAN Monitor (port 9443)

Règles de pare-feu

- Autoriser les connexions entrantes sur le port 8080 (communication avec la station de base)
- Autoriser les connexions entrantes sur le port 9076 (récepteur de webhook)
- Autoriser les connexions entrantes sur le port 9443 (interface Web HTTPS)
- Autoriser les connexions sortantes vers MySQL et InfluxDB

Exigences des stations de base Nokia

Pour chaque station de base :

- **Adresse IP** - Adresse réseau où la station de base est accessible
- **Port** - Port de l'interface de gestion (typiquement 8080)
- **Identifiants** - Nom d'utilisateur et mot de passe pour l'authentification WebLM
- **Route réseau** - Connectivité vérifiée (ping doit réussir)
- **Interface de gestion** - Activée et accessible

Clés d'authentification du gestionnaire

- **Clé privée** - Pour l'authentification du gestionnaire (format PEM)
- **Certificat public** - Certificat d'identité du gestionnaire (format DER)
- Fournis par Nokia ou générés avec OpenSSL

Grafana (optionnel mais recommandé)

- Version : Grafana 8.0+
- Accès : Connectivité réseau à InfluxDB
- Objectif : Tableaux de bord d'analytique et alertes

Processus de configuration initiale

Étape 1 : Préparer l'infrastructure

1.1 Configurer la base de données MySQL

Créez la base de données pour RAN Monitor :

```
CREATE DATABASE ran_monitor CHARACTER SET utf8mb4 COLLATE
utf8mb4_unicode_ci;
```

Créez un utilisateur dédié avec les privilèges appropriés :

```
CREATE USER 'ran_monitor_user'@'%' IDENTIFIED BY
'secure_password';
GRANT CREATE, SELECT, INSERT, UPDATE, DELETE ON ran_monitor.* TO
'ran_monitor_user'@'%';
FLUSH PRIVILEGES;
```

Vérifiez la connectivité depuis le serveur RAN Monitor :

```
mysql -h <mysql-host> -u ran_monitor_user -p ran_monitor
```

1.2 Déployer InfluxDB

Pour InfluxDB 1.x, créez la base de données :

```
influx -execute 'CREATE DATABASE "nokia-monitor"'
```

Pour InfluxDB 2.x, créez un bucket :

```
influx bucket create -n nokia-monitor -o your-org
```

Créez un jeton API avec des permissions d'écriture (InfluxDB 2.x) :

```
influx auth create --org your-org --write-buckets
```

Enregistrez le jeton pour l'utiliser dans la configuration.

1.3 Vérifier les routes réseau

Assurez-vous de la connectivité réseau vers toutes les stations de base :

```
# Tester la connectivité vers chaque station de base
ping 10.7.15.66

# Vérifier que le port de gestion est accessible
telnet 10.7.15.66 8080
```

Vérifiez que MySQL et InfluxDB sont accessibles :

```
# Tester la connectivité MySQL
telnet <mysql-host> 3306

# Tester la connectivité InfluxDB
curl http://<influxdb-host>:8086/ping
```

Étape 2 : Configurer RAN Monitor

Toute la configuration est gérée dans le fichier `config/runtime.exs`.

2.1 Configuration de la base de données

Modifiez `config/runtime.exs` et configurez la connexion MySQL :

```
config :ran_monitor, RanMonitor.Repo,
  username: "ran_monitor_user",
  password: "secure_password",
  hostname: "mysql-host",
  database: "ran_monitor",
  stacktrace: true,
  show_sensitive_data_on_connection_error: true,
  pool_size: 10
```

2.2 Configuration d'InfluxDB

Configurez la connexion InfluxDB :

```
config :ran_monitor, RanMonitor.InfluxDbConnection,
  auth: [
    username: "monitor",
    password: "influx_password"  # Ou jeton API pour InfluxDB 2.x
  ],
  database: "nokia-monitor",
  host: "influxdb-host"
```

2.3 Configuration des points de terminaison Web

Configurez les points de terminaison Web :

```
# Point de terminaison principal SOAP/API pour les stations de
base
config :ran_monitor, RanMonitor.Web.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 8080],
  check_origin: false,
  secret_key_base: "generate_with_mix_phx_gen_secret",
  server: true

# Interface Web du panneau de contrôle (HTTPS)
config :control_panel, ControlPanelWeb.Endpoint,
  url: [host: "0.0.0.0", port: 9443, scheme: "https"],
  https: [
    ip: {0, 0, 0, 0},
    port: 9443,
    keyfile: "priv/cert/omnitouch.pem",
    certfile: "priv/cert/omnitouch.crt"
  ]

# Point de terminaison webhook pour les notifications de station
de base
config :ran_monitor, RanMonitor.Web.Nokia.Airscale.Endpoint,
  url: [host: "0.0.0.0"],
  http: [ip: {0, 0, 0, 0}, port: 9076],
  server: true
```

2.4 Configuration Nokia

Configurez vos identifiants réseau et stations de base :

```
config :ran_monitor,
  general: %{
    mcc: "001",  # Votre code de pays mobile
    mnc: "001"   # Votre code de réseau mobile
  },
  nokia: %{
    ne3s: %{
      webhook_url: "http://<ran-monitor-ip>:9076/webhook",
      private_key: Path.join(Application.app_dir(:ran_monitor,
"priv"), "external/nokia/ne.key.pem"),
      public_key: Path.join(Application.app_dir(:ran_monitor,
"priv"), "external/nokia/ne.cert.der"),
      reregister_interval: 30
    },
    airscales: [
      %{
        address: "10.7.15.66",
        name: "Site-A-BS1",
        port: "8080",
        web_username: "admin",
        web_password: "password"
      }
    ]
  }
```

2.5 Générer des certificats SSL (si nécessaire)

Pour l'interface Web HTTPS, générez des certificats SSL :

```
# Certificat auto-signé pour laboratoire/test
openssl req -newkey rsa:2048 -nodes -keyout
priv/cert/omnitouch.pem \
  -x509 -days 365 -out priv/cert/omnitouch.crt
```

Pour la production, utilisez des certificats signés par une autorité.

Pour des options de configuration détaillées, voir le Guide de configuration d'exécution.

Étape 3 : Démarrer le système

Une fois configuré, démarrez RAN Monitor.

3.1 Exécuter les migrations de base de données

Initialisez le schéma de la base de données :

```
mix ecto.migrate
```

Cela crée toutes les tables nécessaires pour la gestion de l'état de session.

3.2 Démarrer RAN Monitor

Démarrez l'application :

```
mix phx.server
```

Ou pour le déploiement en production :

```
MIX_ENV=prod mix release
_build/prod/rel/ran_monitor/bin/ran_monitor start
```

3.3 Surveiller les journaux de démarrage

Surveillez les journaux pour un démarrage réussi :

```
[info] Running RanMonitor.Web.Endpoint with cowboy
[info] Running ControlPanelWeb.Endpoint with cowboy
[info] Running RanMonitor.Web.Nokia.Airscale.Endpoint with cowboy
[info] Starting RAN Monitor Manager
[info] Connecting to InfluxDB...
[info] InfluxDB connection established
[info] Attempting registration with device: Site-A-BS1
[info] Successfully registered with Site-A-BS1
```

Recherchez :

- Points de terminaison Web démarrés
- Connexions à la base de données établies
- Connectivité InfluxDB confirmée
- Tentatives d'enregistrement de la station de base

Vérification

Étape 4 : Vérifier le fonctionnement

Vérifiez que le système fonctionne correctement.

4.1 Accéder au tableau de bord de l'interface Web

Ouvrez votre navigateur et accédez à :

```
https://<ran-monitor-ip>:9443
```

Vous devriez voir le panneau de contrôle de RAN Monitor.

4.2 Vérifier l'état de la station de base

Dans l'interface Web :

1. Accédez à la page **Stations de base**
2. Vérifiez que votre station de base apparaît dans la liste
3. L'état doit être "Associé" (vert)
4. L'état d'enregistrement doit être "Enregistré"
5. Les informations de session doivent montrer une session active avec un temps d'expiration

Si l'état est rouge/échec, vérifiez :

- La connectivité réseau vers la station de base
- Les identifiants sont corrects
- L'interface de gestion de la station de base est accessible

- Les journaux de l'application pour les messages d'erreur

4.3 Confirmer que les métriques sont envoyées à InfluxDB

Dans l'interface Web :

1. Accédez à la page **État d'InfluxDB**
2. L'état de la connexion doit être vert
3. Les comptes de mesure doivent augmenter
4. Vérifiez les comptes de "Métriques de performance", "Configuration" et "Alarmes"

Alternativement, interrogez InfluxDB directement :

```
# InfluxDB 1.x
influx -database 'nokia-monitor' -execute 'SELECT COUNT(*) FROM
PerformanceMetrics'

# InfluxDB 2.x
influx query 'from(bucket:"nokia-monitor")
  |> range(start: -1h)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> count()'
```

4.4 Examiner les journaux de démarrage

Vérifiez les journaux de l'application pour toute erreur :

Dans l'interface Web :

1. Accédez à la page **Journaux de l'application**
2. Filtrer par niveau "Erreur"
3. Vérifiez qu'il n'y a pas d'erreurs critiques

Ou vérifiez la sortie de la console si vous exécutez via `mix phx.server`.

4.5 Vérifier les détails de l'appareil

Dans l'interface Web :

1. Cliquez sur votre station de base depuis la page Stations de base
2. Vérifiez :
   - Les détails d'enregistrement sont remplis
   - La session a un temps d'expiration valide
   - Les métriques récentes montrent des données
   - L'état de configuration montre les paramètres

Étapes suivantes

Maintenant que RAN Monitor fonctionne, voici les étapes suivantes recommandées :

Actions immédiates

1. **Ajouter plus de stations de base**
   - Ajoutez des appareils supplémentaires à `config/runtime.exs`
   - Redémarrez l'application pour prendre en compte les changements
   - Voir le Guide des opérations courantes
2. **Configurer les tableaux de bord Grafana**
   - Installez Grafana si ce n'est pas déjà déployé
   - Configurez la source de données InfluxDB
   - Importez ou créez des tableaux de bord
   - Voir le Guide d'intégration Grafana
3. **Configurer la rétention des données**
   - Définissez des périodes de rétention appropriées
   - Configurez la rétention par appareil si nécessaire
   - Voir le Guide de politique de rétention des données
4. **Configurer les alarmes et alertes**
   - Examinez les alarmes actives dans l'interface Web

    - Configurez des règles d'alerte Grafana
    - Configurez des canaux de notification
    - Voir le Guide de gestion des alarmes

Préparation opérationnelle

Revue de la documentation :

- Lisez le Guide de l'interface Web pour les opérations quotidiennes
- Consultez le Guide des opérations courantes pour les tâches de routine
- Étudiez le Guide de dépannage pour la résolution de problèmes

Formation de l'équipe :

- Parcourez l'interface Web avec l'équipe des opérations
- Pratiquez les flux de travail courants (vérification de santé quotidienne, enquête sur les alarmes)
- Passez en revue les procédures d'escalade pour les alarmes critiques

Configuration de la surveillance :

- Créez des tableaux de bord opérationnels dans Grafana
- Configurez des règles d'alerte pour les métriques critiques
- Configurez des canaux de notification (Slack, e-mail, PagerDuty)

Renforcement de la sécurité :

- Remplacez les certificats auto-signés par des certificats signés par une autorité
- Déplacez les identifiants vers des variables d'environnement
- Restreignez les permissions de fichiers sur `config/runtime.exs`
- Configurez les règles de pare-feu

Déploiement en production

Avant la production :

- Testez d'abord dans un environnement de staging
- Vérifiez que toutes les stations de base se connectent avec succès
- Confirmez que les métriques sont précises
- Testez les notifications d'alarme
- Documentez toute configuration personnalisée

Lancement en production :

- Déployez pendant une fenêtre de maintenance
- Surveillez de près pendant les 24 premières heures
- Ayez un plan de retour prêt
- Gardez les contacts de support disponibles

Opérations continues :

- Vérifications de santé quotidiennes via l'interface Web
- Revue hebdomadaire des tendances d'alarme
- Planification de capacité mensuelle avec Grafana
- Sauvegardes régulières de configuration

Obtenir de l'aide

Ressources de dépannage

- Guide de dépannage - Problèmes courants et solutions
- Guide de l'interface Web - Référence du panneau de contrôle
- Page des journaux d'application - Journaux système en temps réel

Documentation

- Guide des opérations - Référence opérationnelle complète
- Guide de configuration d'exécution - Détails de configuration
- Configuration AirScale - Configuration de la station de base

Problèmes courants pour les premières fois

Station de base non enregistrée :

- Vérifiez la connectivité réseau (ping)
- Vérifiez que les identifiants sont corrects
- Confirmez que le port 8080 est accessible
- Consultez les journaux de l'application pour les erreurs

Échec de la connexion à InfluxDB :

- Vérifiez qu'InfluxDB est en cours d'exécution
- Vérifiez la configuration de l'hôte et du port
- Confirmez que le jeton API a des permissions d'écriture
- Testez la connectivité : `curl http://<influxdb-host>:8086/ping`

Interface Web non accessible :

- Vérifiez que le port HTTPS 9443 est ouvert
- Vérifiez que les certificats SSL sont présents
- Confirmez que le point de terminaison Web a démarré dans les journaux
- Essayez d'accéder d'abord depuis la machine locale

Documentation connexe

- **Guide des opérations** - Vue d'ensemble opérationnelle complète
- **Guide de l'interface Web** - Guide utilisateur du panneau de contrôle
- **Guide des opérations courantes** - Tâches quotidiennes
- **Guide de configuration d'exécution** - Référence de configuration
- **Configuration AirScale** - Configuration de la station de base
- **Collecte PM Casa** - Ingestion PM des femtocells Casa (push)
- **Collecte Baicells** - Collecte en direct des eNB Baicells (sondage)
- **Collecte OCUDU** - Flux de métriques gNB OCUDU 5G (WebSocket)
- **Guide d'intégration Grafana** - Analytique et tableaux de bord

- **Guide de gestion des alarmes** - Gestion des alarmes
- **Guide de politique de rétention des données** - Gestion des données
- **Guide de dépannage** - Résolution de problèmes

Guide d'Intégration et d'Analyse Grafana

Création de Tableaux de Bord Opérationnels et d'Alerte pour la Surveillance RAN

Guide complet sur la création de tableaux de bord Grafana, les stratégies d'alerte et la visualisation des KPI

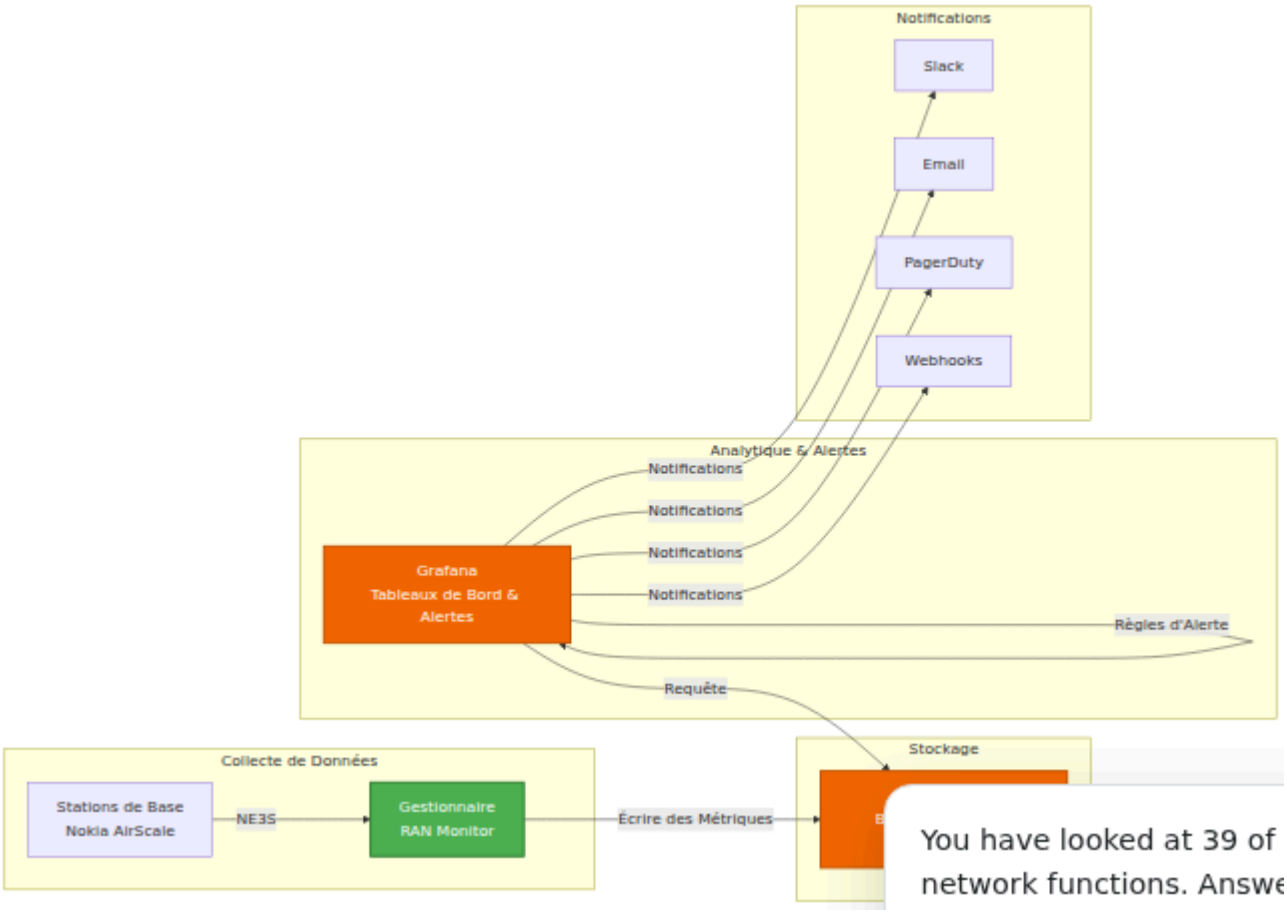
Table des Matières

1. Aperçu
2. Configuration de Grafana & InfluxDB
3. Configuration de la Source de Données
4. Modèles de Conception de Tableaux de Bord
5. Exemples de Requêtes
6. Règles d'Alerte & Escalade
7. Tableaux de Bord Opérationnels
8. Dépannage

Aperçu

Grafana est une plateforme de visualisation et d'alerte qui transforme les métriques collectées par RAN Monitor en informations exploitables pour les équipes d'opérations réseau.

Architecture de Surveillance



Avantages de Grafana

- **Visibilité en Temps Réel** - Tableaux de bord en direct montrant l'état actuel du réseau
- **Analyse Historique** - Analyse des tendances sur des jours/semaine/mois
- **Alertes** - Notifications proactives avant que les problèmes n'impactent les utilisateurs
- **Vues Personnalisées** - Tableaux de bord adaptés à différents rôles (direction, opérations, ingénierie)
- **Rapports** - Exportations instantanées et rapports programmés

Personnalisation des Tableaux de Bord

Important : Les tableaux de bord et visualisations décrits dans ce guide sont **des exemples et des modèles**. L'**équipe des opérations/NOC (ONS)**

concevra et construira des tableaux de bord Grafana en fonction de leurs exigences opérationnelles spécifiques, KPI et flux de travail de surveillance.

Ce guide fournit :

- Exemples de requêtes et modèles sur lesquels s'appuyer
- Meilleures pratiques pour l'organisation des tableaux de bord
- Modèles de configuration d'alerte
- Mappages de référence de compteurs (voir Référence de Compteur Nokia)

L'équipe ONS doit personnaliser :

- Dispositions et visualisations des panneaux
- Seuils d'alerte et politiques d'escalade
- Politiques de conservation pour leur volume de données (voir Politique de Conservation des Données)
- Fenêtres d'agrégation basées sur les besoins de surveillance
- Canaux de notification et routage

Pour les options de configuration d'exécution et les paramètres de collecte de données, reportez-vous au Guide de Configuration d'Exécution.

Configuration de Grafana & InfluxDB

Installation

Prérequis :

- InfluxDB 2.0+ avec un bucket créé pour RAN Monitor
- Jeton API InfluxDB avec permissions de lecture
- Connectivité réseau entre Grafana et InfluxDB

Exemple Docker Compose :

```yaml
version: '3.8'
services:
  influxdb:
    image: influxdb:2.7
    environment:
      INFLUXDB_DB: ran_metrics
      INFLUXDB_ADMIN_USER: admin
      INFLUXDB_ADMIN_PASSWORD: change_me
    ports:
      - "8086:8086"
    volumes:
      - influxdb_data:/var/lib/influxdb2

  grafana:
    image: grafana/grafana:latest
    environment:
      GF_SECURITY_ADMIN_PASSWORD: change_me
    ports:
      - "3000:3000"
    depends_on:
      - influxdb
    volumes:
      - grafana_data:/var/lib/grafana
      - ./provisioning:/etc/grafana/provisioning

volumes:
  influxdb_data:
  grafana_data:
```

Création d'un Jeton API InfluxDB

1. Ouvrir l'interface utilisateur InfluxDB (port 8086)
2. Naviguer vers les Jetons API
3. Créer un nouveau jeton avec les permissions :
    - Lecture : buckets, `ran_metrics` (votre bucket)
4. Copier la valeur du jeton
5. Utiliser dans la configuration de la source de données Grafana

---

Configuration de la Source de Données

Ajout d'InfluxDB en tant que Source de Données dans Grafana

1. **Accéder aux Sources de Données**
    - Grafana → Configuration → Sources de Données
2. **Créer une Nouvelle Source de Données**
    - Cliquer sur "Ajouter une source de données"
    - Sélectionner "InfluxDB"
3. **Configurer la Connexion**

Paramètre	Valeur	Remarques
Nom	RAN Monitor	Nom affiché dans Grafana
URL	`http://influxdb:8086`	Doit être accessible depuis Grafana
Accès	Serveur (par défaut)	Le backend Grafana accède à la DB
Organisation	omnitouch	Votre organisation InfluxDB
Jeton	(jeton API)	À partir de la création du jeton API
Bucket par Défaut	ran_metrics	Où RAN Monitor écrit
Intervalle de temps minimum	10s	Correspond à l'intervalle de sondage

4. **Tester la Connexion**
    - Cliquer sur le bouton "Tester"
    - Devrait afficher "La source de données fonctionne"

Remarque : Les paramètres de connexion InfluxDB (URL, organisation, nom du bucket) doivent correspondre à votre configuration RAN Monitor. Voir le Guide de Configuration d'Exécution pour des détails sur la configuration d'InfluxDB et Configuration AirScale pour l'enregistrement de la station de base.

Langage de Requête Flux

Grafana utilise Flux pour interroger InfluxDB. Syntaxe de base :

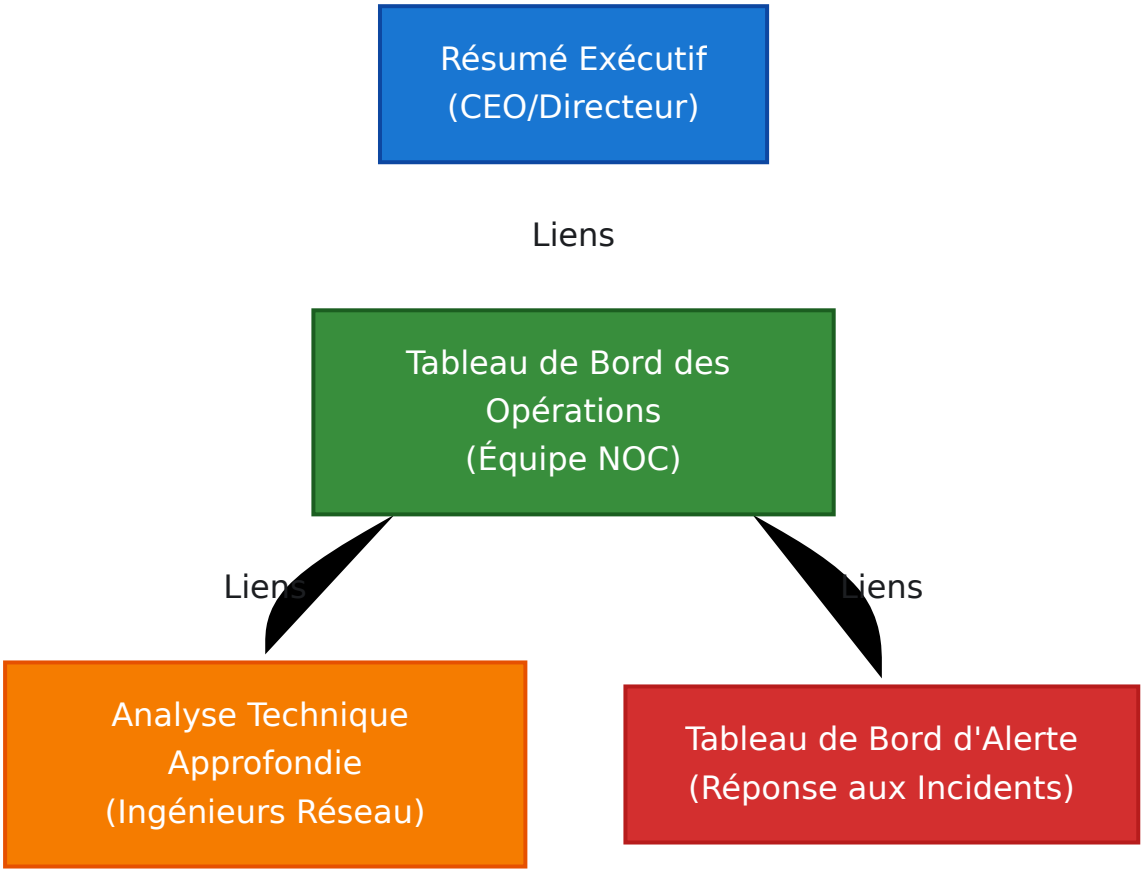
```
from(bucket:"ran_metrics")
  |> range(start: -7d, stop: now())
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r.device == "SITE_A_BS1")
  |> group(by: ["_field"])
  |> aggregateWindow(every: 1h, fn: mean)
```

Concepts Clés :

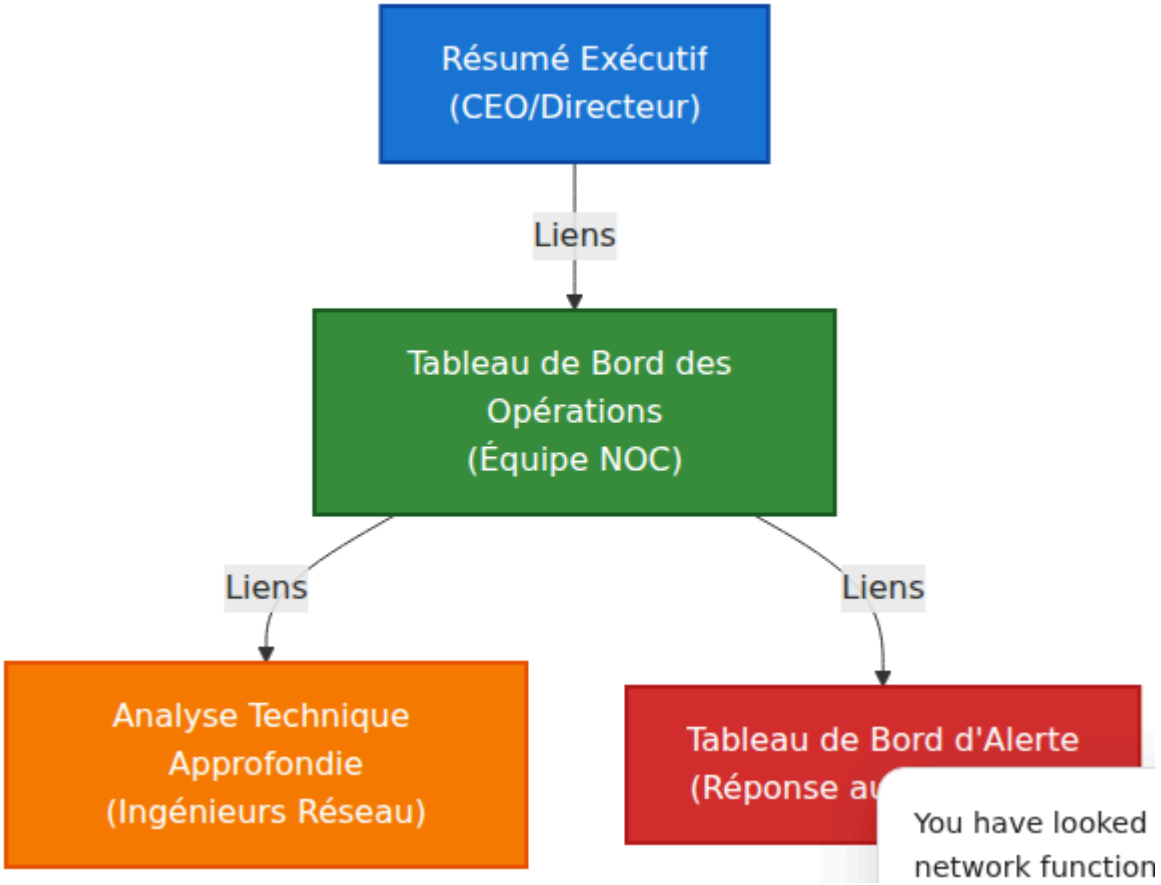
- `from()` - Sélectionner le bucket
- `range()` - Fenêtre temporelle
- `filter()` - Sélectionner les données
- `group()` - Organiser les résultats
- `aggregateWindow()` - Résumer les périodes temporelles

Modèles de Conception de Tableaux de Bord

Hiérarchie des Tableaux de Bord



Types de Panneaux & Cas d'Utilisation



Sections Standard des Tableaux de Bord

Section Supérieure : Métriques Clés (Indicateurs de Statut)

Afficher l'état actuel d'un coup d'œil :

```
┌──────────────────────────────────────────────────────────────────────┐
│ Instantané de la Santé du Réseau                                     │
├──────────────────┬──────────────────┬────────────────────────────────┤
│ Dispositifs En Ligne│ Alarmes Actives │ Disponibilité Moyenne des Cellules │
│ 48/50 (96%)      │ 3 Critiques      │ 98.5%                          │
├──────────────────┴──────────────────┴────────────────────────────────┤
│ Incident le Plus Récent : [il y a 2 heures] Résolu                   │
└──────────────────────────────────────────────────────────────────────┘
```

Objectif :

- Vérification rapide du statut (< 10 secondes pour évaluer)
- Indicateurs verts/rouges pour les problèmes immédiats
- Liens vers des tableaux de bord détaillés pour enquête

Section du Milieu : Tendances (Graphiques de Séries Temporelles)

Afficher les motifs et les changements au fil du temps :

```
┌──────────────────────────────────────────────────────┐
│ Modèles de Trafic (7 jours)                          │
│ [Grand graphique de surface avec motifs
quotidiens/hebdomadaires] │
│ Pic : 250 Gbps (Mercredi 14h)                        │
│ Creux : 80 Gbps (Dimanche 3h)                        │
└──────────────────────────────────────────────────────┘
```

Objectif :

- Identifier les contraintes de capacité
- Comprendre les motifs de trafic
- Prédire les heures de pointe
- Détecter les anomalies

Section Inférieure : Détails & Alertes (Tableaux)

Afficher des informations granulaires :

```
┌──────────────────────────────────────────────────────┐
│ Alarmes Actives (Triées par Sévérité)                │
├─────────┬─────────────┬──────────────┬───────────────┤
│ Niveau │ Dispositif   │ Problème     │ Durée         │
├─────────┼─────────────┼──────────────┼───────────────┤
│ □      │ SITE_A_BS1   │ Cellule Hors Ligne │ 45 minutes │
│ □      │ SITE_B_BS2   │ Température Élevée │ 2 heures    │
└─────────┘──────────────────────────────────────────────┘
```

Objectif :

- Actions immédiates

- Détails d'enquête
- Informations sur les tendances (durée, fréquence)

Exemples de Requêtes

Remarque : Les exemples de requêtes suivants utilisent des compteurs de performance spécifiques à Nokia. Pour des définitions détaillées des compteurs, des unités et des directives d'utilisation, reportez-vous à la Référence de Compteur Nokia. Pour configurer les intervalles de collecte de données et les paramètres InfluxDB, voir le Guide de Configuration d'Exécution.

Requêtes de Métriques de Performance

Disponibilité des Cellules par Dispositif (Dernières 24 Heures)

```
from(bucket:"ran_metrics")
  |> range(start: -24h)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r._field == "CellAvailability")
  |> group(by: ["device"])
  |> aggregateWindow(every: 1h, fn: mean)
  |> yield(name: "cell_availability")
```

Utilisation :

- Tableau de bord exécutif pour le reporting SLA
- Graphique de séries temporelles montrant les moyennes horaires
- Objectif : > 99.5% de disponibilité

Tendance du Débit de Trafic (7 Jours)

```
from(bucket:"ran_metrics")
  |> range(start: -7d)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r._field =~ /Throughput.*/)
  |> group(by: ["device", "_field"])
  |> aggregateWindow(every: 10m, fn: mean)
  |> yield(name: "traffic_trend")
```

Utilisation :

- Tableau de bord de planification de capacité
- Graphique de surface montrant le pic par rapport au creux
- Identifier les heures de pointe pour la planification

Utilisation des Ressources DL par Cellule

```
from(bucket:"ran_metrics")
  |> range(start: -1h)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r._field == "DLResourceUtilization")
  |> filter(fn: (r) => r.device == "SITE_A_BS1")
  |> aggregateWindow(every: 10s, fn: last)
  |> yield(name: "dl_resource")
```

Utilisation :

- Tableau de bord des opérations en temps réel
- Panneau de jauge avertissant à 80%, critique à 95%
- Identification rapide des cellules congestionnées

Requêtes d'Alerte

Alarmes Actives par Sévérité (Dernières 24 Heures)

```
from(bucket:"ran_metrics")
  |> range(start: -24h)
  |> filter(fn: (r) => r._measurement == "Alarms")
  |> filter(fn: (r) => r.status == "active")
  |> group(by: ["severity"])
  |> count()
  |> yield(name: "alarm_count")
```

Utilisation :

- Indicateur de statut montrant les comptes d'alerte
- Graphique circulaire de distribution
- Accès à la liste détaillée des alarmes

Taux d'Alerte (Alarmes par Heure)

```
from(bucket:"ran_metrics")
  |> range(start: -7d)
  |> filter(fn: (r) => r._measurement == "Alarms")
  |> group(by: ["severity"])
  |> aggregateWindow(every: 1h, fn: count)
  |> yield(name: "alarm_rate")
```

Utilisation :

- Graphique de tendance montrant quand les tempêtes d'alerte se produisent
- Identifier les moments de forte instabilité
- Corréler avec des changements de configuration

Alarmes Fréquemment Déclenchées

```
from(bucket:"ran_metrics")
  |> range(start: -7d)
  |> filter(fn: (r) => r._measurement == "Alarms")
  |> group(by: ["alarm_description"])
  |> count()
  |> sort(columns: ["_value"], desc: true)
  |> limit(n: 10)
  |> yield(name: "top_alarms")
```

Utilisation :

- Identifier les problèmes systémiques
- Prioriser les efforts d'ingénierie
- Analyse des causes profondes

Analytique Avancée

Prévision de Disponibilité des Cellules (Régression Linéaire)

```
from(bucket:"ran_metrics")
  |> range(start: -30d)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r._field == "CellAvailability")
  |> filter(fn: (r) => r.device == "SITE_A_BS1")
  |> aggregateWindow(every: 1h, fn: mean)
  |> statefulWindow(every: 1h, period: 24h)
    |> map(fn: (r) => ({r with _value: float(v: r._value)}))
    |> reduce(fn: (r, acc) => ({
        x: acc.x + [float(v: r._time)],
        y: acc.y + [r._value]
      }),
      initial: {x: [], y: []})
    |> yield(name: "availability_forecast")
```

Utilisation :

- Prédire quand le SLA pourrait être enfreint
- Planification de maintenance proactive

- Prévision de capacité

Corrélation du Succès de Transfert avec le Trafic

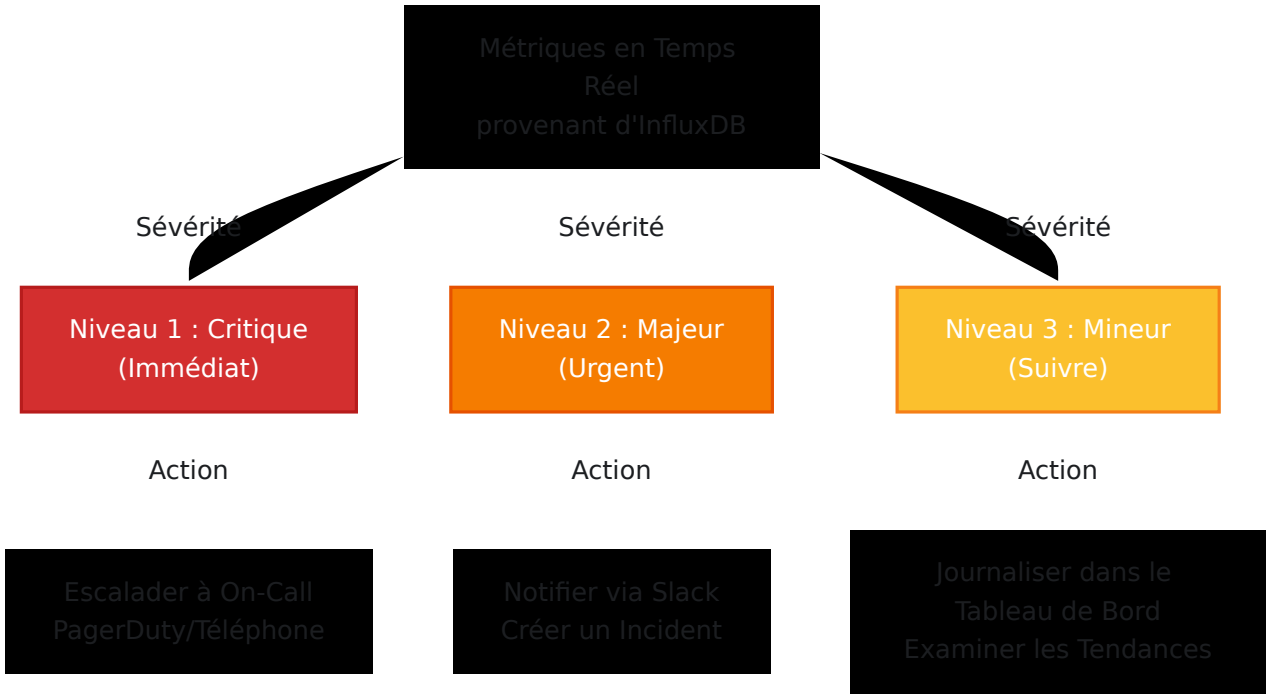
```
from(bucket:"ran_metrics")
  |> range(start: -7d)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r._field =~ /HandoverSuccess|Traffic/)
  |> group(by: ["device", "_field"])
  |> aggregateWindow(every: 1h, fn: mean)
  |> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn:
"_value")
  |> map(fn: (r) => ({r with correlation: float(v:
r.HandoverSuccess) * float(v: r.Traffic)}))
  |> yield(name: "ho_traffic_correlation")
```

Utilisation :

- Identifier si les problèmes de transfert sont liés à la charge
- Ajuster les seuils d'hystérésis de transfert
- Informations sur l'optimisation du r��seau

Règles d'Alerte & Escalade

Cadre de Stratégie d'Alerte



Création de Règles d'Alerte dans Grafana

Étape 1 : Créer une Règle d'Alerte

1. Ouvrir le Tableau de Bord
2. Cliquer sur le panneau à alerter
3. Panneau → Créer une alerte
4. Ou Alerte → Règles d'Alerte → Créer une nouvelle règle d'alerte

Étape 2 : Configurer les Critères d'Évaluation

Exemple 1 : Alerte de Disponibilité des Cellules

```
Condition : CellAvailability < 95%
Durée : 15 minutes
Fréquence d'Évaluation : Chaque minute
Pour : Les 15 dernières minutes
```

Raisonnement :

- Déclencher à 95% pour avertir avant une violation de SLA (99.5%)
- Fenêtre de 15 minutes pour éviter les faux positifs dus aux transitoires
- Surveiller chaque minute pour une réponse rapide

Exemple 2 : Détection de Tempête d'Alarme

```
Condition : count(active_alarms) > 10
Durée : 5 minutes
Fréquence d'Évaluation : Toutes les 2 minutes
Pour : Les 5 dernières minutes
```

Raisonnement :

- 10+ alarmes indiquent un problème systémique
- Détection rapide en 5 minutes pour une réponse rapide
- Vérifier fréquemment pour attraper l'escalade

Exemple 3 : Épuisement des Ressources DL

```
Condition : DLResourceUtilization > 90%
Durée : 30 minutes
Fréquence d'Évaluation : Toutes les 5 minutes
Pour : Les 30 dernières minutes
```

Raisonnement :

- Une utilisation soutenue élevée des ressources indique une congestion
- Fenêtre de 30 minutes pour prévenir les fausses alertes dues aux pics de trafic
- Surveiller toutes les 5 minutes pour attraper la congestion soutenue

Étape 3 : Configurer le Canal de Notification

1. Cliquer sur "Canal de Notification"
2. Sélectionner ou créer un canal (Slack, Email, PagerDuty, etc.)

3. Configurer le modèle de message

Exemple de Modèle de Message :

```
Alerte : {{ .AlertRuleName }}
Sévérité : {{ .Severity }}
Dispositif : {{ .Labels.device }}
Valeur : {{ .EvalMatches[0].Value }}
Durée : {{ .StartsAt }}

{{ .RuleUrl }}
```

Politiques d'Escalade

Alertes de Niveau 1 (Critique) :

- **Condition :** Impact sur le service (dispositif hors ligne, violation de SLA imminente)
- **Durée :** Immédiate (1-5 minutes)
- **Notification :** Appel téléphonique + SMS + Slack + PagerDuty
- **Propriétaire :** Ingénieur de garde
- **SLA :** Réponse en < 15 minutes

Alertes de Niveau 2 (Majeur) :

- **Condition :** Performance dégradée (qualité, disponibilité en baisse)
- **Durée :** 15-30 minutes
- **Notification :** Slack + Email + PagerDuty
- **Propriétaire :** Équipe NOC + ingénieur senior
- **SLA :** Réponse en < 30 minutes

Alertes de Niveau 3 (Mineur) :

- **Condition :** Informatif (tendances, limites approchées)
- **Durée :** 1+ heures
- **Notification :** Slack + Tableau de Bord
- **Propriétaire :** Planification de capacité / ingénierie

- **SLA :** Revue quotidienne

Canaux de Notification

Intégration Slack

```
1. Créer une application Slack dans l'espace de travail
2. Obtenir l'URL du webhook
3. Dans Grafana Alerte → Canaux de Notification
4. Ajouter le canal "Slack"
5. Coller l'URL du webhook
6. Tester la notification
```

Formatage du Message Slack :

```
 CRITIQUE : Cellule Hors Ligne - SITE_A_BS1_Cell1
Durée : 45 minutes
Impact : ~2000 abonnés
Dernière donnée réussie : 14h15

[Enquêter] [Reconnaître] [Tableau de Bord]
```

Intégration PagerDuty

```
1. Créer une clé d'intégration dans PagerDuty
2. Dans Grafana Alerte → Canaux de Notification
3. Ajouter le canal "PagerDuty"
4. Coller la clé d'intégration
5. Mapper les niveaux de sévérité :
   - Critique → Déclencher un incident
   - Majeur → Déclencher avec une urgence inférieure
   - Mineur → Ajouter à un incident existant
```

Intégration Email

```
1. Configurer SMTP dans la configuration de Grafana
2. Dans Alerte → Canaux de Notification
3. Ajouter le canal "Email"
4. Entrer les adresses des destinataires
5. Peut inclure un CSV de destinataires pour des listes de
distribution
```

Tableaux de Bord Opérationnels

Tableau de Bord 1 : Tableau de Bord de Santé Exécutif

Public : Direction, exécutifs
Fréquence de Rafraîchissement : 5 minutes
Objectif : Vue d'ensemble de la santé à haut niveau

Panneaux :

1. **Résumé de Statut (4 Panneaux Stat)**
    - Dispositifs En Ligne / Total
    - Alarmes Actives (codées par couleur selon la sévérité)
    - Disponibilité Moyenne des Cellules (%)
    - Trafic de Pointe Actuel (Gbps)
2. **Santé du Réseau (Série Temporelle)**
    - Tendance de Disponibilité des Cellules (7 jours)
    - Tendance du Taux d'Alerte (7 jours)
    - Prévision de Trafic vs. Réel
3. **Incidents Récents (Tableau)**
    - Heure, Durée, Cause Racine, Statut
    - Derniers 7 jours, triés par sévérité

4. **Grille de Statut des Dispositifs (Carte de Chaleur)**
    - Lignes : Dispositifs, Colonnes : Métriques de Santé
    - Vert (OK) → Jaune (Dégradé) → Rouge (Hors Ligne)

Exemple de Tableau de Bord :

Exemple montrant un aperçu de la station de base avec Dernier Rapporté, UEs Connectés, Données Transférées, Utilisation de PRB et métriques de Débit.

Tableau de Bord 2 : Tableau de Bord des Opérations NOC

Public : Équipe du centre d'opérations réseau
Fréquence de Rafraîchissement : 10 secondes
Objectif : Contrôle opérationnel en temps réel

Panneaux :

1. **Problèmes Actifs (Tableau)**
    - Heure, Sévérité, Dispositif, Problème, Durée
    - Tri par sévérité, clic pour approfondir
2. **Utilisation des Ressources (Jauges)**

- % Ressource DL (par site)
- % Ressource UL (par site)
- % CPU sur les dispositifs

3. **Aperçu du Trafic (Graphique de Surface)**
   - Débit DL/UL (dernières 24 heures)
   - Actuel vs. Moyenne sur 24 heures
   - Indicateurs d'heure de pointe
4. **Tendance des Alarmes (Graphique à Barres)**
   - Compte par sévérité (dernière heure, en cours)
   - Barres empilées montrant la distribution
5. **Statut des Dispositifs (Vue Rapide)**
   - Nom du dispositif, IP, Statut (vert/rouge)
   - Horodatage de la dernière mise à jour des métriques
   - Liens vers le tableau de bord spécifique au dispositif
6. **Événements Récents (Série Temporelle)**
   - Alarmes apparaissant/cessant
   - Changements de configuration
   - Changements de statut de session

Exemple de Tableau de Bord :

Exemple montrant un aperçu du statut 4G avec carte géographique, tableau des alarmes avec niveaux de sévérité, et statistiques de performance.

Tableau de Bord 3 : Analyse Approfondie des Ingénieurs

Public : Ingénieurs réseau
Fréquence de Rafraîchissement : 1 minute
Objectif : Analyse technique détaillée

Panneaux :

1. **Analyse des Modèles de Trafic (Multi-Séries)**
    - DL/UL par site pour comparaison
    - Baseline + superposition actuelle
    - Saisonnalité par heure de la journée
2. **Métriques de Qualité des Cellules (Multi-Séries)**
    - Distribution SINR (histogramme)
    - Distribution RSRP (histogramme)
    - Taux de succès de transfert

3. **Performance Radio (Série Temporelle)**
    - Taux de retransmission RLC (par site)
    - Taux de succès de configuration RRC
    - Taux de chute d'appel
4. **Audit de Configuration (Tableau)**
    - Dispositif, Date de Configuration, Paramètres Changés
    - Met en évidence les modifications récentes
5. **Analyse de Corrélation (Nuage de Points)**
    - Ressource DL vs. Trafic
    - Trafic vs. Succès de Transfert
    - Disponibilité vs. Compte d'Alerte

Tableau de Bord 4 : Tableau de Bord d'Alerte d'Appel

Public : Répondants aux incidents (en garde)
Fréquence de Rafraîchissement : 5 secondes
Objectif : Évaluation et réponse rapide aux incidents

Panneaux :

1. **Résumé des Alertes (Grand Stat)**
    - Compte des alertes critiques actives
    - Couleur de fond : Vert (OK) / Rouge (Problèmes)
2. **Problèmes Critiques (Tableau, Grand Texte)**
    - Dispositif, Problème, Durée
    - Défilement automatique pour les nouveaux en premier
3. **Métriques Associées (Série Temporelle)**
    - Trafic, Utilisation des ressources

- Métriques de qualité pour le dispositif affecté
- Auto-remplissage basé sur l'alerte

4. **Modifications Récentes (Tableau)**

   - Changements de configuration dans les 4 dernières heures
   - Versions logicielles
   - Modifications de paramètres

5. **Problèmes Similaires (Tableau)**

   - Même type de problème dans les 30 derniers jours
   - Temps de résolution
   - Causes racines identifiées

6. **Chemin d'Escalade (Panneau de Texte)**

   - Contact d'escalade de niveau supérieur
   - Informations sur la fenêtre de maintenance
   - Numéro de ticket/incident associé

Tableau de Bord 5 : Performance Détails de Nokia AirScale

Public : Ingénieurs RF, analystes de performance
Fréquence de Rafraîchissement : 30 secondes
Objectif : Métriques et KPI spécifiques à Nokia en profondeur

Ce tableau de bord utilise des compteurs de performance spécifiques à Nokia pour fournir une visibilité complète sur la performance des stations de base AirScale. Voir la Référence de Compteur Nokia pour des définitions détaillées des compteurs.

Panneau 1 : Vue d'Ensemble de l'Utilisation des Ressources (Jauges)

Montre l'utilisation actuelle des PRB (Blocs de Ressources Physiques) :

```
// Utilisation des PRB en Downlink
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8011C37")
  |> filter(fn: (r) => r._field == "counterValue")
  |> group()
  |> mean()
  |> map(fn: (r) => ({ r with _value: r._value / 10.0}))  //
Convertir en pourcentage
  |> rename(columns: {_value: "Utilisation PRB DL"})

// Utilisation des PRB en Uplink
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8011C24")
  |> filter(fn: (r) => r._field == "counterValue")
  |> group()
  |> mean()
  |> map(fn: (r) => ({ r with _value: r._value / 10.0}))  //
Convertir en pourcentage
  |> rename(columns: {_value: "Utilisation PRB UL"})
```

Visualisation : Panneaux de jauge avec seuils :

- Vert : 0-70%
- Jaune : 70-85%
- Rouge : 85-100%

Panneau 2 : Tendances de Débit (Série Temporelle)

Affiche le débit au niveau de la couche PDCP pour le downlink et l'uplink :

```
// Débit en Downlink
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8012C26")
  |> filter(fn: (r) => r._field == "counterValue")
  |> map(fn: (r) => ({ r with _value: r._value / 1000.0}))  //
Convertir en Mbps
  |> rename(columns: {_value: "Débit Downlink Mbps"})

// Débit en Uplink
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8012C23")
  |> filter(fn: (r) => r._field == "counterValue")
  |> map(fn: (r) => ({ r with _value: r._value / 1000.0}))  //
Convertir en Mbps
  |> rename(columns: {_value: "Débit Uplink Mbps"})
```

Compteurs Utilisés :

- **M8012C26** - Débit PDCP DL Moyen (kbit/s)
- **M8012C23** - Débit PDCP UL Moyen (kbit/s)

Panneau 3 : Compte d'UE Actifs (Série Temporelle)

Suit le nombre d'utilisateurs connectés :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8018C1")
  |> filter(fn: (r) => r._field == "counterValue")
  |> rename(columns: {_value: "UEs Connectés"})
```

Compteur Utilisé :

- **M8018C1** - UE Actifs par eNB max (compte)

Panneau 4 : Disponibilité des Cellules (Série Temporelle avec Alerte de Seuil)

Calcule et affiche le pourcentage de disponibilité des cellules :

```
import "strings"

from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8020C3" or
                       r["metricCounter"] == "M8020C6" or
                       r["metricCounter"] == "M8020C4")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> pivot(rowKey:["_time"], columnKey: ["metricCounter"],
valueColumn: "_value")
  |> map(fn: (r) => ({
      _time: r._time,
      "Disponibilité des Cellules": 100.0 * r.M8020C3 / (r.M8020C6
- r.M8020C4)
    }))
```

Compteurs Utilisés :

- **M8020C3** - Échantillons lorsque la cellule est disponible
- **M8020C6** - Dénominateur de disponibilité de la cellule
- **M8020C4** - Échantillons lorsque la cellule est prévue comme indisponible

Alerte de Seuil : Disponibilité des Cellules < 99%

Panneau 5 : Utilisation des PRB par Cellule (Multi-Séries Série Temporelle)

Montre l'utilisation des ressources décomposée par cellules individuelles :

```
import "strings"

// Utilisation des PRB en Uplink par cellule
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8011C24")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> map(fn: (r) => ({ r with _value: r._value / 10.0}))
  |> rename(columns: {"_value": "Utilisation Moyenne PRB Uplink"})

// Utilisation des PRB en Downlink par cellule
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8011C37")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> map(fn: (r) => ({ r with _value: r._value / 10.0 }))
  |> rename(columns: {"_value": "Utilisation Moyenne PRB
Downlink"})
```

Panneau 6 : Débit PDCP par Cellule (Multi-Séries Série Temporelle)

Débit PDCP décomposé par cellule :

```
import "strings"

// Débit PDCP en Downlink par cellule
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8012C26")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> rename(columns: {"_value": "Débit PDCP Downlink"})

// Débit PDCP en Uplink par cellule
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8012C23")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> rename(columns: {"_value": "Débit PDCP Uplink"})
```

Panneau 7 : RSSI (Indicateur de Force du Signal Reçu) (Multi-Séries Série Temporelle)

Affiche les statistiques de force du signal uplink :

```
import "strings"

// RSSI Minimum
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8005C0")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> rename(columns: {"_value": "RSSI Minimum"})

// RSSI Moyen
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8005C2")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> rename(columns: {"_value": "RSSI Moyen"})

// RSSI Maximum
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8005C1")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> rename(columns: {"_value": "RSSI Maximum"})
```

Compteurs Utilisés :

- **M8005C0** - RSSI pour PUCCH Min (dBm)
- **M8005C1** - RSSI pour PUCCH Max (dBm)

- **M8005C2** - RSSI pour PUCCH Moyen (dBm)

Panneau 8 : Latence (Série Temporelle)

Mesure du délai SDU PDCP :

```
import "strings"

from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8001C2")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> rename(columns: {"_value": "Latence"})
```

Compteur Utilisé :

- **M8001C2** - Délai SDU PDCP sur DL DTCH Moyen (ms)

Panneau 9 : Taux de Succès de Configuration de Connexion RRC (Série Temporelle avec Seuil d'Alerte)

Calcule le pourcentage de configurations de connexion réussies :

```
import "strings"

from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M8013C5" or
                       r["metricCounter"] == "M8013C17" or
                       r["metricCounter"] == "M8013C18" or
                       r["metricCounter"] == "M8013C19" or
                       r["metricCounter"] == "M8013C34" or
                       r["metricCounter"] == "M8013C31" or
                       r["metricCounter"] == "M8013C21" or
                       r["metricCounter"] == "M8013C93" or
                       r["metricCounter"] == "M8013C91")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${CellKey}"))
  |> group()
  |> pivot(rowKey:["_time"], columnKey: ["metricCounter"],
valueColumn: "_value")
  |> map(fn: (r) => ({
      _time: r._time,
      "Ratio de Succès de Configuration": 100.0 * r.M8013C5 /
(r.M8013C17 + r.M8013C18 + r.M8013C19 + r.M8013C34 + r.M8013C31 +
r.M8013C21 + r.M8013C93 + r.M8013C91)
    }))
```

Compteurs Utilisés :

- **M8013C5** - Achèvements de Configuration de Connexion de Signalisation
- **M8013C17-M8013C93** - Divers types de tentatives de connexion

Alerte de Seuil : Ratio de Succès de Configuration < 95%

Panneau 10 : VSWR (Rapport d'Ondes Stationnaires de Tension) par Antenne (Série Temporelle)

Surveillance de la santé matérielle pour les systèmes d'antenne :

```
import "strings"

from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M40001C0")
  |> filter(fn: (r) => r._field == "counterValue")
  |> filter(fn: (r) => strings.containsStr(v: r["DN"], substr:
"${RadioKey}"))
  |> map(fn: (r) => ({
      r with
      "DN": strings.split(v: r["DN"], t: "/")[5],
      "VSWR": r._value / 10.0
    }))
  |> group()
  |> pivot(rowKey: ["_time"], columnKey: ["DN"], valueColumn:
"VSWR")
```

Compteur Utilisé :

- **M40001C0** - VSWR par branche d'antenne (0.1 ratio)

Alerte de Seuil : VSWR > 2.0

Panneau 11 : Consommation d'Énergie (Série Temporelle)

Surveillance de l'utilisation d'énergie de la station de base :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["recordType"] == "performanceMetric")
  |> filter(fn: (r) => r["basebandName"] == "${Airscale}")
  |> filter(fn: (r) => r["metricCounter"] == "M40002C2")
  |> filter(fn: (r) => r._field == "counterValue")
  |> group()
  |> map(fn: (r) => ({ r with _value: r._value / 100000.0 }))
  |> rename(columns: {"_value": "Consommation d'Énergie"})
```

Compteur Utilisé :

- **M40002C2** - Consommation d'Énergie (facteur de 100000)

Variables de Tableau de Bord :

Ce tableau de bord utilise des variables de modèle Grafana pour un filtrage dynamique :

- **${Airscale}** - Sélecteur de station de base (menu déroulant)
- **${CellKey}** - Sélecteur de cellule pour les sites multi-cellules (menu déroulant)
- **${RadioKey}** - Sélecteur d'unité radio pour VSWR (menu déroulant)

Règles d'Alerte pour ce Tableau de Bord :

1. **Haute Utilisation de PRB** - Déclenche lorsque DL ou UL PRB > 85% pendant 5 minutes
2. **Basse Disponibilité des Cellules** - Déclenche lorsque la disponibilité < 99% pendant 10 minutes
3. **Mauvais Taux de Succès de Configuration** - Déclenche lorsque le succès de configuration RRC < 95% pendant 5 minutes
4. **Haute VSWR** - Déclenche lorsque VSWR > 2.0 pour toute antenne pendant 15 minutes
5. **Consommation d'Énergie Anormale** - Déclenche lorsque l'énergie dévie > 20% de la ligne de base

Utilisation de ce Tableau de Bord :

1. **Analyse de Capacité** - Surveiller l'utilisation de PRB pour identifier les cellules approchant de la capacité
2. **Dépannage de Performance** - Utiliser RSSI, latence et taux de succès de configuration pour diagnostiquer les problèmes
3. **Santé Matérielle** - Suivre VSWR et consommation d'énergie pour une maintenance proactive
4. **Assurance Qualité** - Surveiller la disponibilité et le débit pour la conformité SLA

Voir la Référence de Compteur Nokia pour des définitions complètes des compteurs et des directives d'utilisation.

Exemple de Tableau de Bord - Vue Détail :

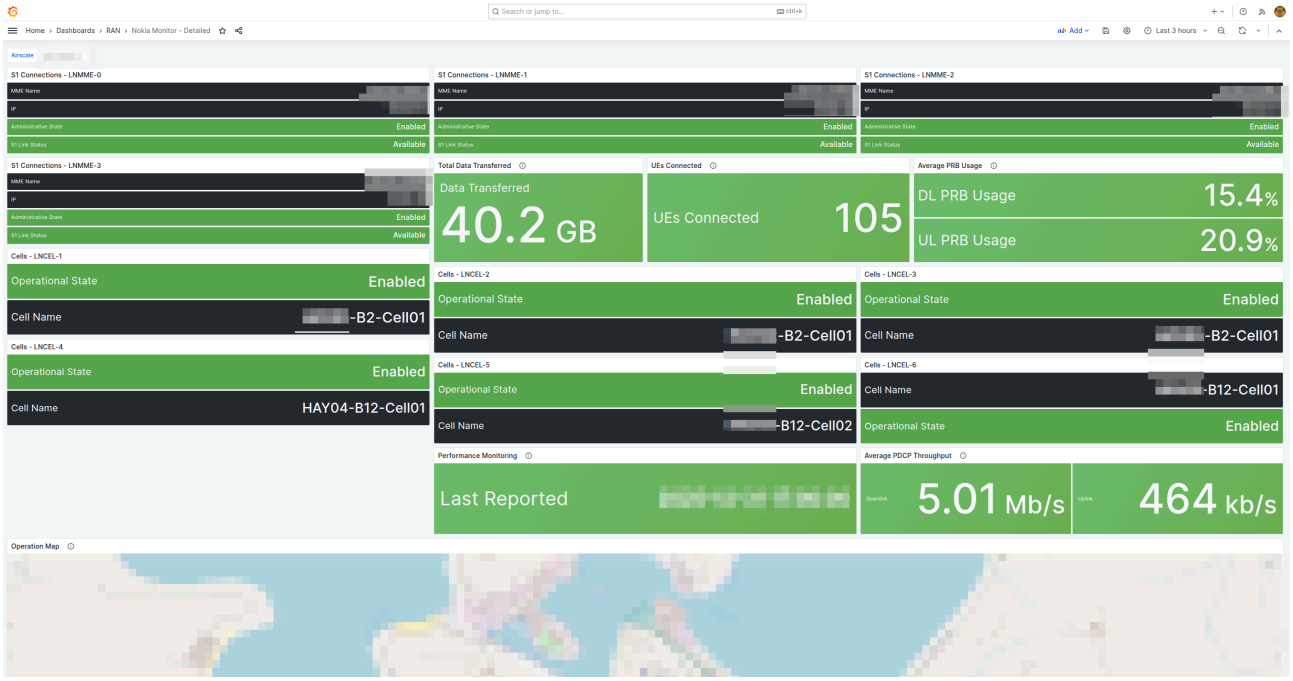


Tableau de bord détaillé de Nokia Monitor montrant les Connexions S1, état opérationnel, données transférées, UEs connectés, utilisation moyenne de PRB, métriques de surveillance de performance, et carte d'opération géographique.

Exemple de Tableau de Bord - Disponibilité des Cellules, Utilisation de PRB et Débit :

Graphiques de Disponibilité des Cellules par LNCEL, Utilisation de PRB LTE par TTI pour uplink/downlink, et graphiques de Débit PDCP montrant la performance à travers plusieurs cellules.

Exemple de Tableau de Bord - RSSI, Énergie, Latence et RRC :

Graphiques RSSI (Min/Moyen/Max), Consommation d'Énergie Combinée, Mesures de Latence, Ratio de Succès de Configuration RRC, et graphiques VSWR (RMOD) pour plusieurs cellules.

Exemple de Tableau de Bord - Panneaux de Performance Supplémentaires :

Panneaux de performance supplémentaires montrant la continuité du Ratio de Succès de Configuration RRC, les mesures de Latence, les graphiques VSWR RMOD, et les UEs Connectés au fil du temps.

Exemple de Tableau de Bord - Détail VSWR avec Infobulle :

Graphique détaillé VSWR RMOD-2 montrant les mesures d'antenne (ANTL-1, ANTL-2, ANTL-3, ANTL-4) avec infobulle interactive affichant l'horodatage et les valeurs.

Dépannage

Aucune Donnée N'apparaît dans les Panneaux

Symptômes :

- Le tableau de bord se charge mais les panneaux affichent "Aucune donnée"
- La source de données semble connectée

Diagnostic :

```
1. Vérifier que la requête InfluxDB est valide
2. Vérifier que le nom de mesure existe dans InfluxDB
3. Vérifier que la plage horaire inclut des points de données
4. Vérifier que les conditions de filtre correspondent aux balises
de données
```

Solution :

- Tester la requête directement dans l'interface utilisateur InfluxDB
- Ajuster la plage horaire (essayer les dernières 24 heures)
- Vérifier que les noms de balises correspondent à la sortie de RAN Monitor
- Activer l'inspecteur de requêtes pour voir les résultats réels

Chargement Lent du Tableau de Bord

Symptômes :

- Le tableau de bord prend > 5 secondes à charger
- Les panneaux apparaissent un par un lentement

Diagnostic :

```
1. Trop de panneaux (> 8)
2. Requêtes trop complexes/plage de données trop large
3. Problèmes de performance d'InfluxDB
4. Latence réseau
```

Solution :

- Réduire le nombre de panneaux
- Limiter la plage horaire (24h vs. 1 an)
- Pré-agréger les données dans InfluxDB
- Vérifier le CPU/mémoire d'InfluxDB
- Augmenter le délai d'attente de la requête

Alertes Non Déclenchées

Symptômes :

- La règle d'alerte est activée
- La condition devrait être remplie
- Aucune notification reçue

Diagnostic :

```
1. Vérifier que l'évaluation de l'alerte se produit
2. Vérifier que le canal de notification fonctionne
3. Vérifier la condition de la règle d'alerte
4. Examiner les journaux du canal de notification
```

Solution :

- Tester manuellement la règle d'alerte (icône de crayon → Tester)
- Vérifier le statut de la règle d'alerte dans Alerte → Règles d'Alerte
- Vérifier que le canal de notification a l'URL/clée correcte
- Vérifier les journaux Grafana pour des erreurs
- Retester le canal de notification avec un déclenchement manuel

Données Incorrectes dans les Tableaux de Bord

Symptômes :

- Les valeurs ne correspondent pas aux chiffres attendus
- Les données semblent décalées dans le temps
- Les agrégations semblent incorrectes

Diagnostic :

```
1. Vérifier les paramètres de fuseau horaire
2. Vérifier la fonction d'agrégation
3. Vérifier les filtres de balises/étiquettes
4. Examiner la requête pour des erreurs mathématiques
```

Solution :

- Définir le fuseau horaire du tableau de bord pour correspondre à InfluxDB
- Vérifier la fonction aggregateWindow (moyenne/somme/dernier)
- Tester les filtres directement dans InfluxDB
- Simplifier la requête pour isoler le problème

Problèmes de Conservation des Données

Symptômes :

- Données historiques manquantes ou incomplètes
- Les requêtes retournent moins de données que prévu
- Le tableau de bord montre des lacunes dans les séries temporelles

Solution :

- Vérifier les paramètres de politique de conservation dans Politique de Conservation des Données
- Vérifier que la période de conservation est suffisante pour votre plage horaire de requête
- Ajuster la conservation par eNodeB si nécessaire

Problèmes de Configuration

Symptômes :

- Erreurs de connexion InfluxDB
- Données eNodeB manquantes dans les requêtes
- Intervalles de collecte de données incorrects

Solution :

- Examiner le Guide de Configuration d'Exécution pour des paramètres appropriés
- Vérifier que la Configuration AirScale est correcte
- Vérifier le statut d'enregistrement de l'eNodeB

Documentation Connexe

- **Référence de Compteur Nokia** - Définitions complètes des compteurs de performance
- **Politique de Conservation des Données** - Gestion du cycle de vie et du stockage des données
- **Guide de Configuration d'Exécution** - Configuration et réglage du système
- **Configuration AirScale** - Configuration et enregistrement de la station de base

Guide des Opérations Courantes

Tâches de Gestion Quotidienne du Moniteur RAN

Guide pratique pour les tâches opérationnelles de routine et la gestion des appareils

---

Table des Matières

1. Aperçu
2. Ajout d'une Nouvelle Station de Base
3. Suppression d'une Station de Base
4. Mise à Jour des Identifiants de l'Appareil
5. Ajustement des Intervalles de Collecte
6. Gestion de la Configuration de l'Appareil
7. Surveillance de la Santé du Système
8. Gestion des Données
9. Sauvegarde et Récupération
10. Maintenance du Système

Aperçu

Ce guide couvre les tâches opérationnelles de routine pour la gestion du Moniteur RAN dans les opérations quotidiennes. Ces procédures sont conçues pour les équipes NOC, les administrateurs réseau et le personnel des opérations.

Prérequis

- Le Moniteur RAN est installé et en cours d'exécution
- Vous avez accès aux fichiers de configuration
- Vous pouvez redémarrer l'application Moniteur RAN
- Vous comprenez votre topologie réseau

Pour la configuration initiale, voir le Guide de Démarrage.

Ajout d'une Nouvelle Station de Base

Lors du déploiement de nouvelles stations de base Nokia AirScale, suivez ces étapes pour les ajouter à la surveillance.

Étape 1 : Vérifier la Connectivité Réseau

Avant d'ajouter l'appareil à la configuration, assurez-vous de la connectivité réseau :

```
# Tester la connectivité de base
ping <base-station-ip>

# Vérifier que le port de gestion est accessible
telnet <base-station-ip> 8080
```

Résultat Attendu : Réponses ping réussies et connexion telnet

Si Échec :

- Vérifiez les routes réseau
- Vérifiez que les règles de pare-feu permettent la connectivité
- Confirmez que la station de base est sous tension et opérationnelle

Étape 2 : Rassembler les Informations de l'Appareil

Collectez les informations suivantes :

Information	Exemple	Où Trouver
Adresse IP	10.7.15.67	Documentation réseau ou étiquette de l'appareil
Port	8080	Typiquement 8080 pour Nokia AirScale
Nom de l'Appareil	Site-B-Tower-1	Utilisez la convention de nommage du site
Nom d'utilisateur	admin	À partir de la provision de la station de base
Mot de passe	password123	À partir de la provision de la station de base

Meilleures Pratiques de Nommage des Appareils :

- Utilisez un nom descriptif et cohérent
- Incluez l'identifiant du site
- Incluez le type d'équipement si plusieurs au même site
- Exemples : `NYC-SiteA-BS1`, `LAX-Tower-Main`, `CHI-Indoor-DAS`

Étape 3 : Vérifier les Appareils Non Configurés

Avant d'ajouter manuellement, vérifiez si l'appareil a déjà tenté de se connecter :

1. Ouvrez l'interface Web : `https://<ran-monitor-ip>:9443`
2. Accédez à la page **eNodeBs Non Configurés**
3. Recherchez l'adresse IP ou l'ID Agent de votre appareil

4. Notez l'ID Agent s'il est trouvé

Cela aide à vérifier que l'appareil peut atteindre le Moniteur RAN.

Étape 4 : Ajouter l'Appareil à la Configuration

Modifiez `config/runtime.exs` et ajoutez le nouvel appareil à la liste `airscales` :

```
config :ran_monitor,
  nokia: %{
    ne3s: %{
      # ... configuration existante des ne3s ...
    },
    airscales: [
      # Appareils existants
      %{
        address: "10.7.15.66",
        name: "Site-A-BS1",
        port: "8080",
        web_username: "admin",
        web_password: "password1"
      },

      # Nouvel appareil
      %{
        address: "10.7.15.67",          # Adresse IP de la
nouvelle station de base
        name: "Site-B-Tower-1",          # Nom descriptif
        port: "8080",                    # Port de gestion
        web_username: "admin",           # Nom d'utilisateur WebLM
        web_password: "password123"      # Mot de passe WebLM
      }
    ]
  }
```

Important : Assurez-vous que la syntaxe Elixir est correcte - les virgules, l'indentation et la structure de la carte doivent être correctes.

Étape 5 : Valider la Configuration

Avant de redémarrer, validez la syntaxe de la configuration :

```
elixir -c config/runtime.exs
```

Sortie Attendue : Pas d'erreurs

Si Erreurs :

- Vérifiez les virgules manquantes
- Vérifiez que toutes les accolades `{` et crochets `[` d'ouverture sont fermés
- Assurez-vous que les chaînes sont correctement citées
- Vérifiez que l'indentation est cohérente

Étape 6 : Redémarrer le Moniteur RAN

Redémarrez l'application pour charger la nouvelle configuration :

```
# Si en développement
# Appuyez sur Ctrl+C deux fois, puis :
mix phx.server

# Si exécuté en tant que service
systemctl restart ran_monitor

# Si exécuté via release
/path/to/ran_monitor/bin/ran_monitor restart
```

Étape 7 : Vérifier l'Enregistrement de l'Appareil

Après le redémarrage, vérifiez que l'appareil est maintenant surveillé :

1. **Vérifiez les Journaux de l'Application :**

```
[info] Tentative d'enregistrement avec l'appareil : Site-B-
Tower-1
[info] Enregistrement réussi avec Site-B-Tower-1
```

2. **Vérifiez l'Interface Web :**
   - Accédez à la page **Stations de Base**
   - Trouvez votre nouvel appareil dans la liste
   - Le statut doit être "Associé" (vert)
   - L'état d'enregistrement doit être "Enregistré"
3. **Vérifiez les Détails de l'Appareil :**
   - Cliquez sur l'appareil
   - Vérifiez que les informations de session montrent une session active
   - Confirmez que le timestamp "Dernier Contact" est récent
4. **Vérifiez l'État d'InfluxDB :**
   - Accédez à la page **État d'InfluxDB**
   - Vérifiez que le nombre total d'enregistrements augmente
   - Les comptes de mesure devraient croître à mesure que les données sont collectées

Étape 8 : Configurer la Rétention des Données (Optionnel)

Si cet appareil nécessite une rétention différente de la valeur par défaut globale :

1. Accédez à la page **Rétention des Données**
2. Trouvez votre nouvel appareil dans la liste
3. Mettez à jour le champ "Période de Rétention" (en heures)
4. Le système enregistre automatiquement

Pour plus de détails, voir le Guide de Politique de Rétention des Données.

Étape 9 : Ajouter aux Tableaux de Bord Grafana

Mettez à jour les tableaux de bord Grafana pour inclure le nouvel appareil :

1. Modifiez les variables de modèle de tableau de bord
2. Ajoutez le nom de l'appareil aux sélecteurs déroulants
3. Créez un tableau de bord spécifique à l'appareil si nécessaire

Pour plus de détails, voir le Guide d'Intégration Grafana.

Suppression d'une Station de Base

Lors de la mise hors service d'une station de base, suivez ces étapes pour la retirer de la surveillance.

Étape 1 : Décider du Traitement des Données

Avant de supprimer, décidez quoi faire avec les données historiques :

Option A : Préserver les Données

- Désactiver la surveillance mais conserver les données historiques
- Utile pour l'équipement mis hors service mais potentiellement de retour

Option B : Supprimer les Données

- Supprimer toutes les données historiques pour l'appareil
- Libère de l'espace de stockage InfluxDB
- Irréversible - les données ne peuvent pas être récupérées

Étape 2 : Désactiver l'Appareil (Préserver les Données)

Pour arrêter la surveillance mais conserver les données historiques :

Modifiez `config/runtime.exs` et localisez l'appareil dans la liste `airscales`. Commentez-le ou retirez-le :

```
airscales: [
  %{
    address: "10.7.15.66",
    name: "Site-A-BS1",
    port: "8080",
    web_username: "admin",
    web_password: "password1"
  },

  # Appareil mis hors service - commenté pour préserver les
données
  # %{
  #   address: "10.7.15.67",
  #   name: "Site-B-Tower-1",
  #   port: "8080",
  #   web_username: "admin",
  #   web_password: "password123"
  # }
]
```

Étape 3 : Supprimer les Données (Optionnel)

Pour supprimer toutes les données historiques pour l'appareil :

1. Accédez à la page **Rétention des Données** dans l'interface Web
2. Trouvez l'appareil dans la liste
3. Cliquez sur le bouton **Effacer Toutes les Données**
4. Confirmez l'action

Avertissement : Ceci est permanent et ne peut pas être annulé.

Étape 4 : Redémarrer le Moniteur RAN

Redémarrez l'application pour appliquer les modifications de configuration :

```
systemctl restart ran_monitor
# ou
mix phx.server
```

Étape 5 : Vérifier la Suppression

Après le redémarrage :

1. **Vérifiez la Page des Stations de Base :**
    - L'appareil ne doit plus apparaître dans la liste active
    - Si les données ont été préservées, l'appareil peut encore apparaître dans les requêtes historiques
2. **Vérifiez les Journaux de l'Application :**
    - Aucune tentative d'enregistrement pour l'appareil supprimé
    - Pas d'erreurs concernant l'appareil manquant
3. **Vérifiez InfluxDB :**
    - Si les données ont été supprimées, les comptes d'enregistrements devraient être plus bas
    - L'appareil ne devrait pas apparaître dans les nouvelles métriques

Étape 6 : Mettre à Jour les Tableaux de Bord Grafana

Retirez l'appareil des configurations Grafana :

1. Modifiez les variables de modèle de tableau de bord
2. Supprimez le nom de l'appareil des déroulants
3. Supprimez les tableaux de bord spécifiques à l'appareil s'ils existent

---

Mise à Jour des Identifiants de l'Appareil

Lorsque les mots de passe des stations de base sont modifiés, mettez à jour la configuration du Moniteur RAN.

Étape 1 : Noter l'État Actuel

Avant de faire des changements :

1. Vérifiez que l'appareil est actuellement connecté (statut vert)
2. Notez les informations de session actuelles
3. Prenez une capture d'écran ou enregistrez l'état actuel pour comparaison

Étape 2 : Mettre à Jour la Configuration

Modifiez `config/runtime.exs` et mettez à jour les identifiants :

```
airscales: [
  %{
    address: "10.7.15.66",
    name: "Site-A-BS1",
    port: "8080",
    web_username: "admin",
    web_password: "new_password_here"  # Mot de passe mis à jour
  }
]
```

Étape 3 : Redémarrer le Moniteur RAN

Appliquez le changement de configuration :

```
systemctl restart ran_monitor
```

Étape 4 : Vérifier la Reconnexion

Après le redémarrage :

1. **Vérifiez les Journaux de l'Application :**

   ```
   [info] Tentative d'enregistrement avec l'appareil : Site-A-BS1
   [info] Enregistrement réussi avec Site-A-BS1
   ```

2. **Vérifiez l'Interface Web :**

   - Le statut de l'appareil doit être "Associé" (vert)
   - Une nouvelle session doit être établie
   - "Dernier Contact" doit être récent

Si l'Appareil Échoue à se Connecter :

- Vérifiez que les nouveaux identifiants sont corrects
- Vérifiez les fautes de frappe dans le mot de passe
- Confirmez que les identifiants fonctionnent directement sur la station de base
- Consultez les journaux de l'application pour des erreurs d'authentification

---

Ajustement des Intervalles de Collecte

Changez la fréquence à laquelle le Moniteur RAN collecte des données des stations de base.

Comprendre les Intervalles de Collecte

Le Moniteur RAN collecte trois types de données à différents intervalles :

Type de Données	Intervalle Par Défaut	Configurable	Impact d'un Intervalle Plus Court
Métriques de Performance	10 secondes	Oui	Données plus granulaires, utilisation réseau/de stockage plus élevée
Alarmes	10 secondes	Oui	Détection d'alarme plus rapide, plus de requêtes
Configuration	60 secondes	Oui	Instantanés de configuration plus fréquents, plus de stockage
Vérifications de Santé	30 secondes	Oui	Plus réactif aux problèmes de connectivité

Quand Ajuster les Intervalles

Raccourcir les Intervalles (Plus Fréquent) :

- Résolution de problèmes actifs
- Infrastructure critique de grande valeur
- Surveillance SLA avec des exigences strictes
- Tests et analyses de capacité

Allonger les Intervalles (Moins Fréquent) :

- Réduire le trafic réseau
- Réduire l'utilisation de stockage InfluxDB
- Environnements de test de moindre priorité
- Liens à bande passante limitée

Étape 1 : Modifier la Configuration

Les intervalles de collecte sont configurés dans le code de l'application, pas dans runtime.exs. Pour les changer, vous devrez modifier le code source et recompiler.

Les intervalles de collecte des métriques de performance, des alarmes et de la configuration sont chacun définis dans le code de l'application.

Remarque : Contactez le support Omnitouch pour obtenir de l'aide sur les changements d'intervalles de collecte, car cela nécessite des modifications du code source.

Étape 2 : Considérer l'Impact

Avant de changer les intervalles :

Impact Réseau :

- Calculez : appareils × compteurs × intervalle = requêtes par seconde
- Intervalles plus courts = plus de trafic réseau
- Assurez-vous que le réseau peut gérer la charge accrue

Impact de Stockage :

- Calculez : points de données par jour × période de rétention = stockage total
- Exemple : intervalle de 10s = 8,640 mesures/jour par compteur
- Assurez-vous qu'InfluxDB dispose de suffisamment d'espace disque

Performance du Système :

- Plus de sondages fréquents = utilisation CPU plus élevée sur le Moniteur RAN
- Surveillez les ressources système après les changements

Étape 3 : Surveiller Après les Changements

Après avoir ajusté les intervalles :

1. **Surveillez les Journaux de l'Application** pour toute erreur
2. **Surveillez les Ressources Système :**
   - Utilisation CPU sur le serveur Moniteur RAN
   - Utilisation de la bande passante réseau
   - I/O disque InfluxDB et croissance du stockage
3. **Vérifiez la Qualité des Données :**
   - Vérifiez InfluxDB pour la fréquence de mesure attendue
   - Vérifiez qu'il n'y a pas de lacunes dans les données
4. **Ajustez si Nécessaire :**
   - Revenez en arrière si le système est surchargé
   - Affinez en fonction des performances observées

Gestion de la Configuration de l'Appareil

Comment gérer en toute sécurité les configurations des stations de base via le Moniteur RAN.

Flux de Travail de Configuration

Pour des procédures de gestion de configuration détaillées, voir le Guide de l'Interface Web - Gestion de la Configuration.

Référence Rapide :

1. **Téléchargez** la configuration actuelle (sauvegarde)
2. **Modifiez** la configuration hors ligne
3. **Téléchargez** la nouvelle configuration - obtenez l'ID de Plan
4. **Validez** la configuration en utilisant l'ID de Plan
5. **Activez** si la validation réussit

6. **Vérifiez** que les changements ont pris effet

Meilleures Pratiques

Téléchargez Toujours en Premier :

- Conservez une sauvegarde de la configuration actuelle
- Permet le retour en arrière si nécessaire
- Documente la configuration avant le changement

Validez Avant d'Activer :

- Ne jamais activer sans valider
- La validation détecte les erreurs de syntaxe
- Évite les interruptions de service

Planifiez les Changements Appropriately :

- Utilisez des fenêtres de maintenance lorsque cela est possible
- Évitez les heures de pointe
- Ayez un plan de retour en arrière prêt

Documentez les Changements :

- Enregistrez ce qui a été changé et pourquoi
- Notez l'ID de Plan pour le suivi
- Documentez les résultats de vérification
- Mettez à jour le système de gestion des changements

Surveillez Après les Changements :

- Surveillez les alarmes
- Vérifiez que les métriques se normalisent
- Vérifiez la stabilité de l'appareil pendant 15-30 minutes
- Soyez prêt à revenir en arrière si des problèmes surviennent

---

Surveillance de la Santé du Système

Vérifications de routine pour s'assurer que le Moniteur RAN fonctionne correctement.

Vérification Quotidienne de la Santé

Effectuez ces vérifications au début de chaque quart :

1. Accédez au Tableau de Bord de l'Interface Web

```
https://<ran-monitor-ip>:9443
```

2. Vérifiez l'État du Système

- Tous les appareils affichent-ils un statut vert (associé) ?
- Des appareils rouges (échoués) nécessitant une enquête ?
- Le nombre d'alarmes est-il raisonnable pour l'heure de la journée ?

3. Vérifiez le Résumé des Alarmes

- Des alarmes critiques sont-elles actives ?
- Le taux d'alarme est-il en hausse ou en baisse ?
- Des alarmes répétées indiquant des problèmes systémiques ?

4. Vérifiez la Collecte de Données

- Accédez à la page État d'InfluxDB
- Les comptes de mesure augmentent-ils ?
- Le timestamp de la dernière mise à jour est-il récent ?

5. Vérifiez les Journaux Récents

- Accédez à la page des Journaux de l'Application
- Filtrez par niveau "Erreur"

- Des erreurs récurrentes ?

Pour des procédures de vérification de santé détaillées, voir le Guide de l'Interface Web - Flux de Travail de l'Interface Web.

Exemple : Tableau de Bord de Surveillance Grafana

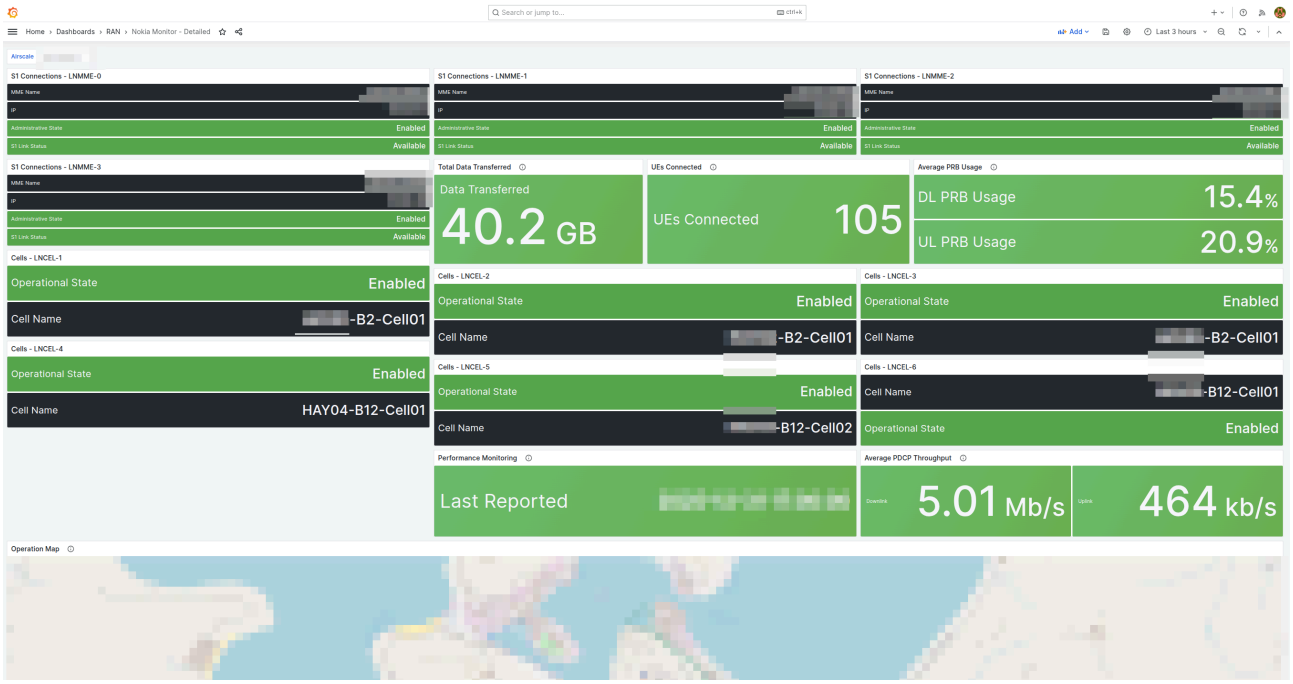


Tableau de bord de surveillance complet montrant l'état des connexions S1 par LNMME, état opérationnel, données transférées, UEs connectés, utilisation moyenne des PRB, métriques de surveillance de performance, et carte de couverture géographique. Ce tableau de bord fournit une visibilité instantanée sur la santé du réseau et l'état des appareils.

Revue Systématique Hebdomadaire

Vérification plus approfondie effectuée chaque semaine :

1. Vérifiez les Tendances des Alarmes

- Utilisez Grafana pour analyser le taux d'alarme au cours de la semaine passée
- Identifiez les tempêtes d'alarmes ou les modèles
- Corrélez avec la maintenance ou les changements

2. Vérifiez la Croissance du Stockage

- Utilisation du disque InfluxDB en tendance
- Taille de la base de données MySQL
- Tailles des fichiers journaux de l'application

3. Vérifiez la Connectivité des Appareils

- Des appareils avec des déconnexions fréquentes ?
- Problèmes de délai d'expiration de session ?
- Modèle de problèmes de connectivité ?

4. Utilisation des Ressources Système

- Utilisation CPU sur le serveur Moniteur RAN
- Tendances d'utilisation de la mémoire
- Consommation de bande passante réseau

5. Changements de Configuration

- Vérifiez tous les changements de configuration effectués
- Vérifiez que les changements ont été documentés
- Corrélez avec d'éventuels problèmes

Temps Requis : 30-45 minutes

Gestion des Données

Gestion de la Rétention des Données

Voir le Guide de Politique de Rétention des Données pour des détails complets.

Référence Rapide :

Voir la Rétention Actuelle :

- Accédez à la page Rétention des Données
- Vérifiez les paramètres par défaut globaux et par appareil

Ajuster la Période de Rétention :

- Mettez à jour les heures de rétention pour un appareil spécifique
- Ou modifiez la valeur par défaut globale dans `config/config.exs`

Nettoyer les Anciennes Données :

- Nettoyage manuel : Cliquez sur le bouton "Nettoyer les Anciennes Données"
- Le nettoyage automatique s'exécute toutes les heures

Planification de Stockage :

- Surveillez l'utilisation du disque InfluxDB chaque semaine
- Ajustez la rétention en fonction du stockage disponible
- Équilibrez la période de rétention avec la capacité de stockage

Exportation des Données

Exporter les Configurations des Appareils :

1. Accédez à la page de détails de l'appareil
2. Cliquez sur "Télécharger la Configuration"
3. Enregistrez le fichier XML à un endroit sûr
4. Étiquetez avec le nom de l'appareil et la date

Exporter les Métriques (via InfluxDB) :

```
# Exporter les données pour un appareil spécifique
influx -database 'nokia-monitor' -execute '
  SELECT * FROM PerformanceMetrics
  WHERE basebandName='''Site-A-BS1'''
  AND time > now() - 7d
' -format csv > export.csv
```

Exporter via Grafana :

- Ouvrez le tableau de bord
- Sélectionnez la plage horaire
- Cliquez sur "Partager" - "Exporter" - "CSV"

Sauvegarde et Récupération

Sauvegardes Régulières

Ce qu'il faut Sauvegarder :

1. Fichiers de Configuration

```
# Sauvegarder la configuration d'exécution
cp config/runtime.exs backups/runtime.exs.$(date +%Y%m%d)

# Sauvegarder l'ensemble du répertoire de configuration
tar -czf backups/config-$(date +%Y%m%d).tar.gz config/
```

2. Configurations des Appareils

- Téléchargez les configurations de tous les appareils via l'interface Web
- Stockez dans un contrôle de version ou un emplacement de sauvegarde
- Effectuez cela chaque semaine ou avant/après des changements

3. Base de Données MySQL

```
# Sauvegarder la base de données d'état de session
mysqldump -u ran_monitor_user -p ran_monitor >
backups/ran_monitor-$(date +%Y%m%d).sql
```

4. Données InfluxDB

```
# Sauvegarde InfluxDB 1.x
influxd backup -portable -database nokia-monitor
/backups/influx-$(date +%Y%m%d)

# Sauvegarde InfluxDB 2.x
influx backup /backups/influx-$(date +%Y%m%d)
```

5. Certificats SSL

```
cp priv/cert/* backups/certificates-$(date +%Y%m%d)/
```

Plan de Sauvegarde

Quotidien :

- Base de données MySQL (état de session)
- Fichiers de configuration s'ils ont été modifiés

Hebdomadaire :

- Données InfluxDB (ou selon la politique de rétention)
- Configurations des appareils de toutes les stations de base

Avant les Changements :

- Fichiers de configuration
- Configurations des appareils
- Instantané de la base de données

Processus de Récupération

Récupérer d'une Erreur de Configuration :

1. Arrêtez le Moniteur RAN

   ```
   systemctl stop ran_monitor
   ```

2. Restaurez le fichier de configuration

```
cp backups/runtime.exs.20251230 config/runtime.exs
```

3. Validez la configuration

```
elixir -c config/runtime.exs
```

4. Redémarrez le Moniteur RAN

```
systemctl start ran_monitor
```

5. Vérifiez que les appareils se reconnectent

Récupérer d'une Perte de Base de Données :

1. Arrêtez le Moniteur RAN

```
systemctl stop ran_monitor
```

2. Restaurez la base de données MySQL

```
mysql -u ran_monitor_user -p ran_monitor < backups/ran_monitor-
20251230.sql
```

3. Redémarrez le Moniteur RAN

```
systemctl start ran_monitor
```

4. Les appareils se réenregistreront automatiquement

5. La collecte de nouvelles métriques commence

6. Les données historiques restent dans InfluxDB

Récupérer d'une Perte Totale du Système :

1. Réinstallez le Moniteur RAN sur un nouveau serveur
2. Restaurez les fichiers de configuration
3. Restaurez la base de données MySQL
4. Restaurez les données InfluxDB
5. Restaurez les certificats SSL
6. Démarrez le Moniteur RAN
7. Vérifiez que tous les appareils se reconnectent
8. Vérifiez que les données historiques sont accessibles

Maintenance du Système

Tâches de Maintenance Routinières

Mensuel :

1. Vérifiez les Journaux

- Archivez les anciens journaux d'application
- Vérifiez les erreurs ou avertissements récurrents
- Nettoyez les fichiers journaux pour libérer de l'espace disque

2. Mettez à Jour la Documentation

- Documentez tous les changements de configuration
- Mettez à jour les diagrammes réseau si la topologie a changé
- Passez en revue et mettez à jour les procédures opérationnelles

3. Mises à Jour de Sécurité

- Appliquez les correctifs de sécurité du système d'exploitation
- Mettez à jour le logiciel de base de données si nécessaire
- Faites tourner les mots de passe selon la politique de sécurité

4. Revue de Performance

- Analysez les tendances des ressources système
- Identifiez toute dégradation de performance
- Planifiez des mises à niveau de capacité si nécessaire

Trimestriel :

1. Test de Récupération après Sinistre

- Testez le processus de restauration des sauvegardes
- Vérifiez que les procédures de récupération fonctionnent
- Mettez à jour la documentation de récupération après sinistre

2. Audit de Sécurité

- Vérifiez les journaux d'accès
- Vérifiez les autorisations des utilisateurs
- Mettez à jour les certificats SSL s'ils expirent bientôt

3. Planification de Capacité

- Passez en revue les tendances de croissance du stockage
- Prévoyez les besoins futurs en capacité
- Planifiez des mises à niveau matérielles si nécessaire

Annuel :

1. Renouvellement des Certificats SSL

- Remplacez les certificats SSL expirants
- Testez les nouveaux certificats avant l'expiration

2. Rotation des Mots de Passe

- Mettez à jour tous les identifiants des stations de base
- Mettez à jour les mots de passe de la base de données
- Mettez à jour les jetons API

3. Mise à Niveau du Système

- Planifiez la mise à niveau de version du Moniteur RAN
- Testez dans un environnement de staging
- Planifiez la mise à niveau en production

Fenêtres de Maintenance

Planification d'une Fenêtre de Maintenance :

1. **Planifiez Pendant un Trafic Faible :**
    - Les nuits ou les week-ends sont généralement les meilleurs
    - Évitez les heures de pointe identifiées dans Grafana
2. **Informez les Parties Prenantes :**
    - Informez l'équipe des opérations
    - Mettez à jour la page d'état
    - Fixez des attentes pour les temps d'arrêt
3. **Préparez un Plan de Retour en Arrière :**
    - Sauvegardez l'état actuel
    - Documentez les étapes de retour en arrière
    - Ayez la version précédente prête si vous mettez à niveau
4. **Effectuez la Maintenance :**
    - Suivez les procédures documentées
    - Surveillez de près les progrès
    - Documentez toute déviation
5. **Vérifiez la Santé du Système :**
    - Tous les appareils se reconnectent
    - Les métriques circulent normalement
    - Pas d'erreurs dans les journaux
    - Exécutez les procédures de vérification de santé

6. **Documentez les Résultats :**
    - Enregistrez ce qui a été fait
    - Notez les problèmes rencontrés
    - Mettez à jour les procédures si nécessaire

Documentation Connexe

- **Guide de Démarrage** - Procédures de configuration initiale
- **Guide de l'Interface Web** - Guide utilisateur du panneau de contrôle
- **Guide de Configuration d'Exécution** - Référence de configuration
- **Configuration AirScale** - Configuration de la station de base
- **Gestion des Firmwares** - Référentiel de paquets logiciels et mises à jour
- **Guide d'Intégration Grafana** - Analytique et tableaux de bord
- **Guide de Gestion des Alarmes** - Procédures de gestion des alarmes
- **Guide de Politique de Rétention des Données** - Gestion du cycle de vie des données
- **Guide de Dépannage** - Résolution de problèmes
- **Guide des Opérations** - Vue d'ensemble opérationnelle complète

Référence des Métriques Prometheus

Métriques au niveau de l'application pour la surveillance et l'alerte du RAN Monitor

---

Table des Matières

1. Aperçu
2. Point de terminaison des métriques
3. Architecture
4. Métriques de la file d'attente InfluxDB
5. Métriques de performance d'écriture InfluxDB
6. Métriques d'écriture par agent
7. Métriques de filtrage des compteurs PM
8. Métriques de traitement des Webhooks
9. Métriques d'état des dispositifs Nokia
10. Métriques d'état BTS
11. Métriques de spool PM
12. Métriques système
13. Métriques gNB OCUDU
14. Exemples de requêtes Prometheus
15. Exemples d'alerte

Aperçu

Le RAN Monitor expose des métriques Prometheus pour surveiller la santé et la performance du pipeline de collecte de données. Ces métriques fournissent une visibilité sur :

- **Ingestion de données** - Profondeur de la file d'attente, latence d'écriture et débit vers InfluxDB
- **Connectivité des dispositifs** - Statut d'enregistrement et de session pour les stations de base Nokia AirScale
- **Traitement des Webhooks** - Performance du traitement des Webhooks SOAP entrants
- **Utilisation des ressources** - Mémoire et nombre de processus de la VM Erlang

Métriques vs. Données de Performance RAN

Les **métriques Prometheus** (documentées ici) surveillent l'application RAN Monitor elle-même - profondeurs de file d'attente, latences d'écriture, statut de connectivité des dispositifs.

Les **données de séries temporelles InfluxDB** contiennent les véritables métriques de performance RAN des stations de base Nokia AirScale (compteurs PM, alarmes, configuration). Voir Intégration Grafana pour interroger les données InfluxDB.

Point de terminaison des métriques

URL : `GET http://<host>:4000/metrics`

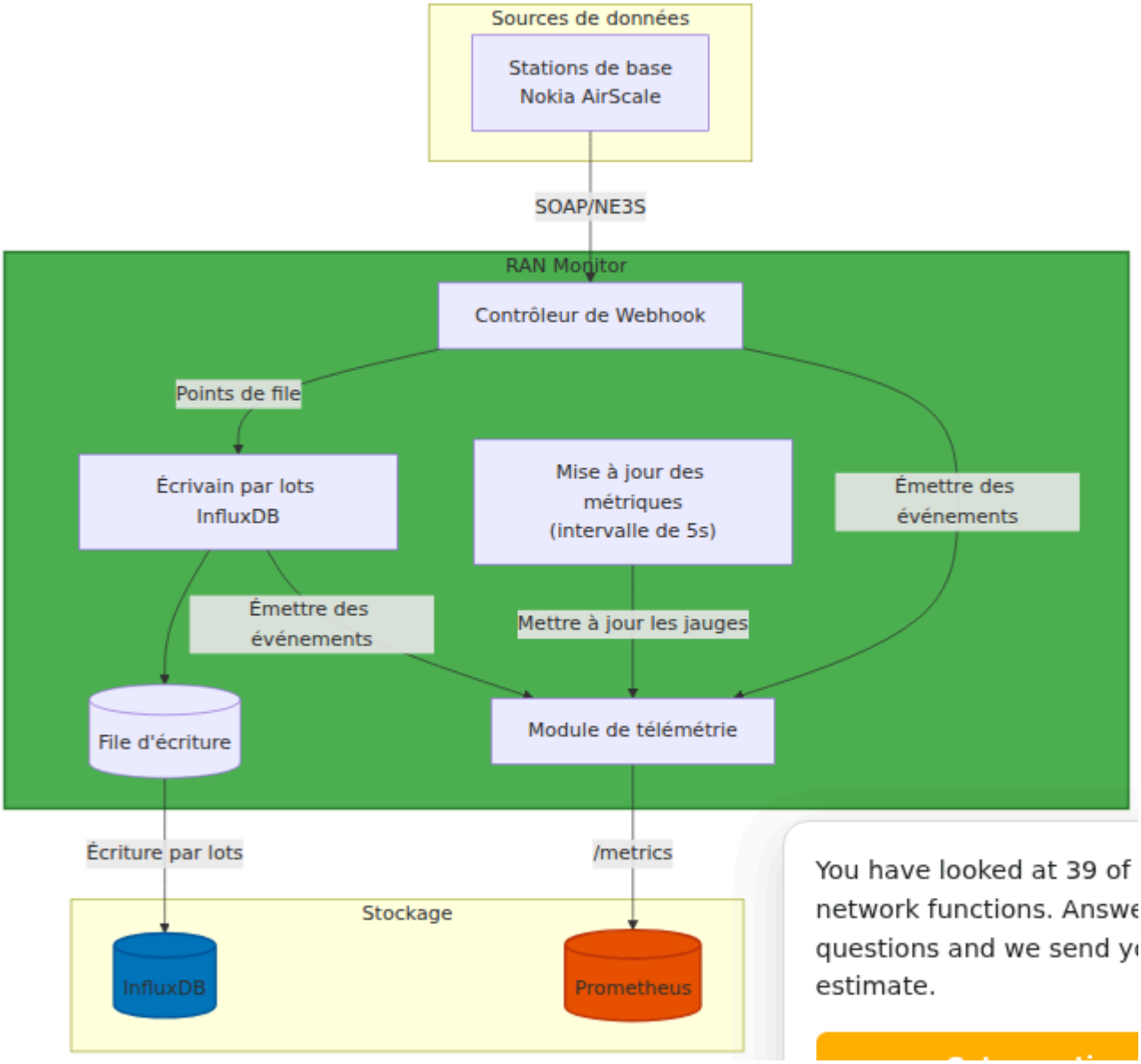
Format : Format d'exposition de texte Prometheus

Authentification : Aucune (réseau interne uniquement)

Configuration de Scrape

```yaml
# prometheus.yml
scrape_configs:
  - job_name: 'ran_monitor'
    static_configs:
      - targets: ['ran-monitor.internal:4000']
    scrape_interval: 15s
    scrape_timeout: 10s
```

Architecture



You have looked at 39 of
network functions. Answe
questions and we send y
estimate.

Mécanismes de mise à jour

Type de métrique	Déclencheur de mise à jour	Fréquence
Jauges	Polling de MetricsUpdater	Toutes les 5 secondes
Compteurs	Lors de l'occurrence d'un événement	Temps réel
Histogrammes	Lors de l'occurrence d'un événement	Temps réel

Métriques de la file d'attente InfluxDB

Ces métriques suivent la file d'écriture par lots qui tamponne les points de données avant de les écrire dans InfluxDB.

influxdb_queue_depth

Type : Jauge

Description : Nombre actuel de points de données en attente dans la file d'écriture InfluxDB.

Étiquettes : Aucune

Utilisation : Surveiller l'accumulation de la file d'attente indiquant des goulets d'étranglement d'écriture InfluxDB ou des problèmes de connectivité.

Seuils :

- Normal : < 5 000 points

- Avertissement : > 10 000 points
- Critique : > 40 000 points (approchant la capacité maximale)

---

influxdb_queue_max

Type : Jauge

Description : Taille maximale de la file avant que les points ne soient abandonnés. Fixé à 50 000 points.

Étiquettes : Aucune

Utilisation : Valeur de référence pour calculer le pourcentage d'utilisation de la file d'attente.

---

influxdb_queue_overflow_drops_total

Type : Compteur

Description : Nombre total de points de données abandonnés parce que la file a dépassé la capacité maximale.

Étiquettes :

Étiquette	Description
`agent_name`	Identifiant de la station de base (par exemple, `2045_Booker`, `2057_Guymon_TOY`)

Utilisation : Alerter sur toute augmentation - les abandons indiquent une perte de données et nécessitent une enquête.

Métriques de Performance d'Écriture InfluxDB

Ces métriques mesurent la performance des écritures par lots dans InfluxDB.

influxdb_write_duration_milliseconds

Type : Histogramme

Description : Durée des opérations d'écriture par lots InfluxDB en millisecondes.

Étiquettes :

Étiquette	Description
`status`	Résultat de l'écriture : `success` ou `error`

Seaux : 10, 25, 50, 100, 250, 500, 1000, 2500, 5000 ms

Utilisation : Surveiller la distribution de la latence d'écriture. Des latences élevées peuvent indiquer des problèmes de performance d'InfluxDB ou des problèmes de réseau.

---

influxdb_points_written_total

Type : Compteur

Description : Nombre total de points de données écrits avec succès dans InfluxDB.

Étiquettes :

Étiquette	Description
`measurement`	Type de données : `pm` (métriques de performance), `config`, ou `alarm`

Utilisation : Suivre le taux d'ingestion de données par catégorie. Des chutes soudaines indiquent des problèmes de collecte.

---

influxdb_bytes_written_total

Type : Compteur

Description : Nombre total d'octets écrits dans InfluxDB lors de toutes les écritures.

Étiquettes : Aucune

Utilisation : Surveiller le volume de données pour la planification de la capacité et l'estimation des coûts.

---

influxdb_flush_count_total

Type : Compteur

Description : Nombre total d'opérations de vidage par lots effectuées.

Étiquettes : Aucune

Utilisation : Suivre la fréquence d'écriture. Combiné avec points_written, indique la taille moyenne des lots.

Métriques d'Écriture par Agent

Ces métriques fournissent une visibilité par station de base sur la collecte de données.

influxdb_points_written_by_agent_total

Type : Compteur

Description : Nombre total de points de données écrits dans InfluxDB, décomposé par station de base et type de mesure.

Étiquettes :

Étiquette	Description
`agent_name`	Identifiant de la station de base (par exemple, `2045_Booker`)
`measurement`	Type de données : `pm`, `config`, ou `alarm`

Utilisation : Identifier quelles stations de base rapportent activement des données et détecter les pannes silencieuses.

---

influxdb_bytes_written_by_agent_total

Type : Compteur

Description : Nombre total d'octets écrits dans InfluxDB par station de base.

Étiquettes :

Étiquette	Description
`agent_name`	Identifiant de la station de base

Utilisation : Identifier les stations de base à fort volume pour la planification de la capacité.

---

influxdb_write_duration_by_agent_milliseconds

Type : Histogramme

Description : Durée des écritures InfluxDB par station de base en millisecondes.

Étiquettes :

Étiquette	Description
`agent_name`	Identifiant de la station de base
`status`	Résultat de l'écriture : `success` ou `error`

Seaux : 10, 25, 50, 100, 250, 500, 1000, 2500, 5000 ms

Utilisation : Identifier les stations de base avec des écritures systématiquement lentes qui peuvent impacter la performance globale.

Métriques de Filtre de Compteur PM

Ces métriques suivent le filtrage des compteurs de Métriques de Performance (PM) pour réduire le volume de stockage.

pm_points_filtered_total

Type : Compteur

Description : Nombre total de points de données PM abandonnés parce que le compteur n'était pas dans la liste blanche.

Étiquettes : Aucune

Utilisation : Surveiller l'efficacité du filtre. Des valeurs très élevées peuvent indiquer que la liste blanche doit être élargie.

---

pm_points_kept_total

Type : Compteur

Description : Nombre total de points de données PM conservés après filtrage par liste blanche.

Étiquettes : Aucune

Utilisation : Suivre le volume réel de données PM stockées.

---

pm_filter_allowed_count

Type : Jauge

Description : Nombre de compteurs PM actuellement dans la liste blanche de collecte.

Étiquettes : Aucune

Utilisation : Vérifier la configuration du filtre. Les changements indiquent des mises à jour de la liste blanche via l'interface utilisateur.

Source : Chargé depuis `priv/pm_counters.csv`, géré via la page Collecte de données PM.

---

config_points_filtered_total

Type : Compteur

Description : Nombre total de points de données de configuration abandonnés parce que la clé n'était pas dans la liste blanche.

Étiquettes :

Étiquette	Description
`agent_name`	Identifiant de la station de base

Utilisation : Surveiller l'activité du filtre de configuration par appareil. Des valeurs élevées sont normales — la plupart des clés de configuration sont filtrées.

---

config_filter_allowed_count

Type : Jauge

Description : Nombre de clés de configuration actuellement dans la liste blanche de collecte.

Étiquettes : Aucune

Utilisation : Vérifier la configuration du filtre de configuration.

Source : Chargé depuis `priv/config_keys.csv`.

Métriques de Traitement des Webhooks

Ces métriques suivent le traitement des Webhooks SOAP entrants des stations de base Nokia AirScale.

webhook_processing_duration_milliseconds

Type : Histogramme

Description : Temps pour traiter les charges utiles de Webhook entrants en millisecondes.

Étiquettes :

Étiquette	Description
`airscale_name`	Identifiant de la station de base
`message_type`	Type de charge utile : `PM`, `Config`, `Alarm`, ou `Feedback`

Seaux : 10, 50, 100, 250, 500, 1000, 2500, 5000, 10000 ms

Utilisation : Surveiller la performance du traitement des Webhooks. Un traitement lent peut indiquer des problèmes d'analyse ou des goulets d'étranglement en aval.

---

webhook_processing_total

Type : Compteur

Description : Nombre total de charges utiles de Webhook traitées.

Étiquettes :

Étiquette	Description
`airscale_name`	Identifiant de la station de base
`message_type`	Type de charge utile : `PM`, `Config`, `Alarm`, ou `Feedback`
`status`	Résultat du traitement : `success` ou `error`

Utilisation : Suivre le volume de Webhooks et les taux d'erreur par station de base.

Métriques d'État des Dispositifs Nokia

Ces métriques suivent la connectivité et le statut d'enregistrement des stations de base Nokia AirScale.

nokia_devices_registered

Type : Jauge

Description : Nombre de dispositifs Nokia actuellement enregistrés avec RAN Monitor.

Étiquettes : Aucune

Utilisation : Vérifier le nombre de dispositifs attendus. Des chutes indiquent des problèmes d'enregistrement.

---

nokia_devices_session_active

Type : Jauge

Description : Nombre de dispositifs Nokia avec des sessions de gestion actives.

Étiquettes : Aucune

Utilisation : Doit correspondre à `nokia_devices_registered` en fonctionnement normal. Des écarts indiquent des problèmes de session.

---

nokia_device_state

Type : Jauge

Description : Indicateur d'état de connectivité par dispositif.

Étiquettes :

Étiquette	Description
`device_name`	Identifiant de la station de base (par exemple, `2045_Booker`)

Valeurs :

Valeur	État
1	Connecté (enregistré ET session active)
0	Déconnecté

Utilisation : Alerter sur tout dispositif tombant à 0. Utiliser le filtrage par étiquette pour surveiller des dispositifs spécifiques.

Métriques d'État BTS

Ces métriques fournissent une vue d'état calculée qui prend en compte le flux de données, pas seulement la connectivité. Mis à jour toutes les 5 secondes par le MetricsUpdater.

bts_status_total

Type : Jauge

Description : Nombre total de sites BTS configurés.

Étiquettes : Aucune

---

bts_status_connected

Type : Jauge

Description : Sites BTS avec session active et à la fois configuration et données PM en cours de flux.

Étiquettes : Aucune

Utilisation : C'est le compte "sain". Doit être égal au total moins tout site en états transitoires.

---

bts_status_waiting_for_pm

Type : Jauge

Description : Sites BTS avec session active et données de configuration reçues, mais pas encore de données PM.

Étiquettes : Aucune

Utilisation : Les sites dans cet état attendent le prochain cycle de collecte PM de 15 minutes. S'ils restent ici pendant plus de 30 minutes, enquêter sur la collecte PM sur l'eNodeB.

---

bts_status_pending

Type : Jauge

Description : Sites BTS avec session active mais aucune donnée reçue (ni configuration ni PM).

Étiquettes : Aucune

---

bts_status_registering

Type : Jauge

Description : Sites BTS qui sont enregistrés mais la session n'est pas encore active.

Étiquettes : Aucune

---

bts_status_disconnected

Type : Jauge

Description : Sites BTS qui ne sont pas enregistrés.

Étiquettes : Aucune

Utilisation : Alerter si cela augmente de manière inattendue.

Métriques de Spool PM

Ces métriques suivent le spool de données PM basé sur le disque qui tamponne les charges utiles PM brutes sur le disque pour un traitement séquentiel. Cela élimine les abandons de débordement de file et maintient l'utilisation de la mémoire stable.

pm_spool_pending_files

Type : Jauge

Description : Nombre de fichiers de données PM en attente d'être traités dans le répertoire de spool.

Étiquettes : Aucune

Utilisation : Surveiller l'accumulation de retard. En fonctionnement normal, cela reste proche de zéro. Un nombre croissant indique que le travailleur de spool ne peut pas suivre les données PM entrantes.

Seuils :

- Normal : < 10 fichiers
- Avertissement : > 50 fichiers
- Critique : > 200 fichiers

---

pm_spool_files_processed_total

Type : Compteur

Description : Nombre total de fichiers de spool PM traités par le travailleur en arrière-plan.

Étiquettes : Aucune

Utilisation : Suivre le débit de traitement. Le taux doit correspondre au taux de fichiers entrants.

---

pm_spool_points_written_total

Type : Compteur

Description : Nombre total de points de données PM écrits dans InfluxDB via le travailleur de spool.

Étiquettes : Aucune

Utilisation : Suivre le volume de données PM circulant à travers le chemin de spool.

Métriques Système

Ces métriques suivent l'utilisation des ressources de la VM Erlang.

vm_memory_bytes

Type : Jauge

Description : Utilisation de la mémoire de la VM Erlang en octets.

Étiquettes :

Étiquette	Description
`type`	Catégorie de mémoire : `total`, `processes`, `binary`, `ets`

Utilisation : Surveiller la croissance de la mémoire indiquant des fuites ou un tamponnage excessif.

Seuils (guidance) :

- `total` : Alerter si > 80 % de la RAM système
- `binary` : Alerter si croissant continuellement (peut indiquer une accumulation de file de messages)
- `ets` : Alerter si croissant continuellement (peut indiquer une fuite de table)

---

vm_process_count

Type : Jauge

Description : Nombre de processus Erlang dans la VM.

Étiquettes : Aucune

Utilisation : La ligne de base doit être stable. Une croissance significative peut indiquer des fuites de processus ou des tempêtes de connexions.

Métriques gNB OCUDU

Le RAN Monitor exporte les métriques en direct de chaque gNB OCUDU configuré. Pour la description complète, voir Collecte OCUDU.

Métrique	Type	Étiquettes	Descriptio
`ocudu_metric`	Jauge	`gnb`, `scope`, `pci`, `rnti`, `counter`	La dernière valeur d'un échantillon du rapport de métriques JSON du gNB.
`ocudu_connected`	Jauge	`gnb`	`1` si le flux de métriques du gNB est actif. `0` s'il est inactif.
`ocudu_last_report_timestamp_seconds`	Jauge	`gnb`	Temps Unix du dernier rapport du gNB.

Exemples de Requêtes Prometheus

Pourcentage d'Utilisation de la File

```
influxdb_queue_depth / influxdb_queue_max * 100
```

Taux d'Erreur d'Écriture (fenêtre de 5 minutes)

```
sum(rate(influxdb_write_duration_milliseconds_count{status="error"}
[5m]))
/ sum(rate(influxdb_write_duration_milliseconds_count[5m])) * 100
```

Points Écrits Par Seconde

```
sum(rate(influxdb_points_written_total[5m]))
```

Latence d'Écriture au 95ème Percentile

```
histogram_quantile(0.95,
sum(rate(influxdb_write_duration_milliseconds_bucket[5m])) by
(le))
```

Dispositifs Déconnectés

```
count(nokia_device_state == 0)
```

Taux d'Erreur de Webhook par Dispositif

```
sum by (airscale_name) (
  rate(webhook_processing_total{status="error"}[5m])
) / sum by (airscale_name) (
  rate(webhook_processing_total[5m])
) * 100
```

Taux de Perte de Données (Abandons de File)

```
sum(rate(influxdb_queue_overflow_drops_total[5m]))
```

Tendance d'Utilisation de la Mémoire

```
vm_memory_bytes{type="total"}
```

Sites BTS Pas Complètement Connectés

```
bts_status_total - bts_status_connected
```

Retard de Spool PM

```
pm_spool_pending_files
```

Taux de Traitement de Spool PM

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

Efficacité du Filtre PM

```
pm_points_filtered_total / (pm_points_filtered_total +
pm_points_kept_total) * 100
```

Exemples d'Alerte

Critique : Perte de Données

```yaml
alert: InfluxDBQueueDrops
expr: increase(influxdb_queue_overflow_drops_total[5m]) > 0
for: 0m
labels:
  severity: critical
annotations:
  summary: "Points de données abandonnés en raison du débordement de la file"
  description: "{{ $value }} points abandonnés au cours des 5 dernières minutes pour {{ $labels.agent_name }}"
```

Critique : Dispositif Déconnecté

```yaml
alert: NokiaDeviceDisconnected
expr: nokia_device_state == 0
for: 5m
labels:
  severity: critical
annotations:
  summary: "Dispositif Nokia {{ $labels.device_name }} déconnecté"
  description: "Le dispositif a été déconnecté pendant plus de 5 minutes"
```

Avertissement : Accumulation de File

```
alert: InfluxDBQueueHigh
expr: influxdb_queue_depth / influxdb_queue_max * 100 > 50
for: 5m
labels:
  severity: warning
annotations:
  summary: "File d'écriture InfluxDB au-dessus de 50 %"
  description: "File à {{ $value }} % de capacité. Vérifiez la
connectivité et la performance d'InfluxDB."
```

Avertissement : Latence d'Écriture Élevée

```
alert: InfluxDBWriteLatencyHigh
expr: histogram_quantile(0.95,
sum(rate(influxdb_write_duration_milliseconds_bucket[5m])) by
(le)) > 1000
for: 5m
labels:
  severity: warning
annotations:
  summary: "La latence d'écriture InfluxDB dépasse 1 seconde
(p95)"
  description: "La latence d'écriture au 95ème percentile est de
{{ $value }}ms"
```

Avertissement : Erreurs de Traitement de Webhook

```
alert: WebhookProcessingErrors
expr: sum(rate(webhook_processing_total{status="error"}[5m])) >
0.1
for: 5m
labels:
  severity: warning
annotations:
  summary: "Erreurs de traitement de Webhook détectées"
  description: "{{ $value }} erreurs par seconde au cours des 5
dernières minutes"
```

Avertissement : Retard de Spool PM

```
alert: PmSpoolBacklog
expr: pm_spool_pending_files > 50
for: 5m
labels:
  severity: warning
annotations:
  summary: "Retard de spool PM croissant"
  description: "{{ $value }} fichiers en attente de traitement. Le
travailleur de spool peut être en retard."
```

Avertissement : Sites Bloqués en Attente de PM

```
alert: BtsSitesWaitingForPm
expr: bts_status_waiting_for_pm > 0
for: 30m
labels:
  severity: warning
annotations:
  summary: "{{ $value }} site(s) en attente de données PM pendant >30 minutes"
  description: "Les sites ont des sessions actives et des configurations mais pas de données PM. Vérifiez la collecte PM sur l'eNodeB."
```

Info : Utilisation Élevée de la Mémoire

```
alert: HighMemoryUsage
expr: vm_memory_bytes{type="total"} > 4e9
for: 10m
labels:
  severity: info
annotations:
  summary: "Utilisation de la mémoire de la VM Erlang supérieure à 4 Go"
  description: "Utilisation actuelle de la mémoire : {{ $value | humanize1024 }}B"
```

Documentation Connexe

- **Intégration Grafana** - Tableaux de bord et alertes pour les données de performance RAN
- **Collecte de données PM** - Gestion des compteurs PM collectés
- **Dépannage** - Problèmes courants et résolution
- **Guide de Configuration Runtime** - Configuration du système

Référence des Compteurs de Performance LTE Nokia

Guide complet sur les compteurs de mesure de performance Nokia AirScale/FlexiRadio

---

Table des Matières

1. Aperçu
2. Convention de Nom des Compteurs
3. Catégories de Compteurs
4. Compteurs d'Utilisation des Ressources
5. Compteurs de Débit
6. Compteurs d'Activité UE
7. Compteurs de Disponibilité de Cellule
8. Compteurs de Qualité Radio
9. Compteurs de Gestion de Connexion
10. Compteurs de Latence et QoS
11. Compteurs de Matériel et d'Unité Radio
12. Utilisation des Compteurs dans Grafana
13. Documentation Connexe

Aperçu

Les stations de base LTE Nokia (AirScale, FlexiRadio) rapportent des données de performance en utilisant un système de compteurs structuré. Chaque compteur

mesure un aspect spécifique de la performance du réseau, de l'utilisation des ressources à la qualité radio.

Qu'est-ce que les Compteurs de Performance ?

Les compteurs de performance sont des mesures numériques collectées par la station de base à intervalles réguliers. Ils fournissent une visibilité sur :

- À quel point le réseau est occupé (utilisation des ressources)
- À quel point il fonctionne bien (débit, qualité)
- Combien d'utilisateurs sont connectés (charge)
- Si les services sont disponibles (disponibilité)
- La qualité du signal et les conditions radio

Groupes de Mesure

Les compteurs sont organisés en groupes de mesure, chacun couvrant un domaine fonctionnel spécifique. L'ensemble complet des compteurs LTE Nokia comprend les groupes de mesure suivants :

Mesures de Performance de Base (M8xxx)

Mesure	Catégorie	Nombre de Compteurs	Focalisation Principale
M8000	Interface S1	33	Configuration de Contexte Initial, configuration/réinitialisation S1, contexte UE
M8001	Performance de Cellule	336	Délai PDCP, RACH, blocs de transport, distribution MCS
M8004	Interface X2	4	Volume de données X2, trafic inte eNB
M8005	Qualité Radio	237	RSSI, SINR, conditions radio, AMC
M8006	Support EPS	54	Configuration/modification/libérat de support
M8007	Support Radio de Données	14	Établissement et gestion de DRB
M8008	Rejet de Connexion RRC	14	Raisons et statistiques de rejet de connexion
M8009	Préparation de Transfert	8	Échecs de préparation de HO
M8010	Distribution CQI	27	Statistiques de l'indicateur de qualité de canal
M8011	Utilisation des Ressources	55	Utilisation PRB, allocation de ressources

Mesure	Catégorie	Nombre de Compteurs	Focalisation Principale
M8012	Débit	121	Débits de données PDCP, statistiques de volume
M8013	Connexion de Signalisation	21	Tentatives/réussites de configuration de connexion RRC
M8014	Transfert Inter-eNB	14	Procédures de transfert basées su X2
M8015	Transfert Intra-eNB	13	Transferts internes de cellule
M8016	Recul CS	18	Procédures de recul commuté par circuit
M8017	HO Inter-Système	10	Transfert vers d'autres RAT (3G/2(
M8018	Charge eNB	8	Comptes d'UE actifs, statistiques charge
M8019	NACC	4	Changement de Cellule Assisté pa Réseau
M8020	Disponibilit�� de Cellule	7	État de la cellule et échantillonna de disponibilité
M8021	HO Inter-Fréquence	17	Procédures de transfert inter-fréquence
M8022	Configuration X2	2	Établissement de l'interface X2

Mesure	Catégorie	Nombre de Compteurs	Focalisation Principale
M8023	Volume de Données	36	Volume SDU PDCP sur l'interface radio

Mesures d'Interface Réseau (M5xxx)

Mesure	Catégorie	Nombre de Compteurs	Focalisation Principale
M5112	Entrée d'Interface IP	112	Statistiques de paquets entrants, métriques d'interface
M5113	Ethernet RX	21	Statistiques de paquets Ethernet reçus

Mesures de Matériel (M4xxxx)

Mesure	Catégorie	Nombre de Compteurs	Focalisation Principale
M40001	Matériel Radio	Variable	VSWR, santé de l'antenne, métriques RF
M40002	Consommation d'Énergie	Variable	Utilisation d'énergie de la station de base

---

Convention de Nom des Compteurs

Les compteurs Nokia suivent un format de nommage standard :

```
M<mesure><type>C<compteur>
```

Exemple : M8011C24

- **M** - Préfixe fixe indiquant "Mesure"
- **8011** - Groupe de mesure (Ressource de Cellule)
- **C** - Séparateur fixe indiquant "Compteur"
- **24** - Compteur spécifique au sein du groupe (utilisation moyenne PRB UL)

Types Logiques

Chaque compteur a un type logique qui détermine comment il agrège les données :

- **Somme** - Compte cumulatif d'événements
- **Moyenne** - Valeur moyenne sur la période de mesure
- **Min** - Valeur minimale observée
- **Max** - Valeur maximale observée
- **Actuel** - Valeur échantillonnée actuelle
- **Dénominateur** - Utilisé pour les calculs de ratio

Catégories de Compteurs

Par Domaine Fonctionnel

Planification de Capacité :

- M8011Cxx - Utilisation PRB
- M8018Cxx - Comptes d'UE actifs
- M8012Cxx - Taux de débit

Surveillance de Performance :

- M8001Cxx - Latence et délai
- M8005Cxx - RSSI, SINR
- M8013Cxx - Taux de réussite de configuration

Suivi de Disponibilité :

- M8020Cxx - Disponibilité de cellule
- M8049Cxx - État de connexion

Dépannage :

- M8005Cxx - Problèmes de qualité radio
- M8001Cxx - Problèmes de file d'attente
- M8013Cxx - Échecs de configuration

Compteurs d'Utilisation des Ressources

M8011 - Mesures de Ressources de Cellule

Ces compteurs suivent l'utilisation des Blocs de Ressources Physiques (PRB), ce qui indique à quel point les ressources radio de la cellule sont occupées.

Compteur	Nom	Description	Unité	Type	Échelle
M8011C24	Utilisation PRB UL par TTI Moyenne	Utilisation moyenne des PRB montants par Intervalle de Temps de Transmission	0.1%	Moyenne	Diviser par 10 pour obtenir un pourcentage
M8011C37	Utilisation PRB DL par TTI Moyenne	Utilisation moyenne des PRB descendants par Intervalle de Temps de Transmission	0.1%	Moyenne	Diviser par 10 pour obtenir un pourcentage

Comprendre l'Utilisation des PRB :

- **Blocs de Ressources Physiques (PRB)** sont les plus petites unités d'allocation de ressources radio en LTE
- **TTI (Intervalle de Temps de Transmission)** = 1 milliseconde en LTE
- Une utilisation plus élevée = cellule plus occupée (plus de trafic)
- Une utilisation de 100% indique que la cellule est à pleine capacité

Plages de Valeurs :

- 0-1000 (représente 0.0% à 100.0%)
- Diviser la valeur du compteur par 10 pour obtenir le pourcentage
- Exemple : Valeur du compteur 453 = 45.3% d'utilisation des PRB

Utilisation dans la Planification de Capacité :

- < 50% - La cellule a une capacité disponible

- 50-70% - Cellule chargée normalement
- 70-85% - Fortement chargée, surveiller pour congestion
- > 85% - Proche de la capacité, envisager d'ajouter des secteurs/porteuses

Exemple de Requête Grafana :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] == "M8011C37")
  |> filter(fn: (r) => r._field == "counterValue")
  |> map(fn: (r) => ({ r with _value: r._value / 10.0}))  //
Convertir en pourcentage
```

Compteurs de Débit

M8012 - Mesures de Débit de Cellule

Ces compteurs mesurent le débit de la couche PDCP (Packet Data Convergence Protocol), indiquant les taux de transfert de données utilisateur réels.

Compteur	Nom	Description	Unité	Type	Déclencheur de Mise à Jour
M8012C23	Débit PDCP UL Moyenne	Débit PDCP montant moyen	kbit/s	Moyenne	Lorsque SDU PDCP reçu de l'UE
M8012C26	Débit PDCP DL Moyenne	Débit PDCP descendant moyen	kbit/s	Moyenne	Lorsque SDU PDCP transmis à l'UE

Comprendre le Débit PDCP :

- La couche **PDCP** est l'endroit où les paquets de données utilisateur sont traités
- Le débit est mesuré en kilobits par seconde (kbit/s)
- Représente le taux de transfert de données réelles pour le trafic utilisateur
- Mis à jour chaque seconde

Calcul du Débit :

- Mesuré comme une moyenne sur un intervalle d'échantillonnage de 1 seconde
- Prend en compte tous les utilisateurs actifs dans la cellule
- Inclut à la fois les porteuses VoLTE et de données

Repères de Performance :

Descendant (M8012C26) :

- < 10 Mbps - Faible trafic / peu d'utilisateurs
- 10-50 Mbps - Trafic modéré
- 50-100 Mbps - Fort trafic / de nombreux utilisateurs actifs
- > 100 Mbps - Trafic de pointe (dépend de la bande passante de la cellule)

Montant (M8012C23) :

- < 5 Mbps - Faible trafic
- 5-20 Mbps - Trafic modéré
- 20-40 Mbps - Fort trafic
- > 40 Mbps - Trafic de pointe

Exemple de Requête Grafana :

```
from(bucket: "nokia-monitor")
  |> range(start: -1h)
  |> filter(fn: (r) => r["metricCounter"] == "M8012C26")
  |> filter(fn: (r) => r._field == "counterValue")
  |> map(fn: (r) => ({ r with _value: r._value / 1000.0}))  //
Convertir en Mbps
```

Compteurs d'Activité UE

M8018 - Mesures de Charge eNB

Ces compteurs suivent le nombre de dispositifs d'Équipement Utilisateur (UE) actifs connectés à la station de base.

Compteur	Nom	Description	Unité	Type	Intervalle de Mise à Jour
M8018C1	UE Actifs par eNB max	Nombre maximum d'UE actifs par eNodeB	Entier	Max	1 seconde

Comprendre l'Activité UE :

- **UE Actif** = Un dispositif avec au moins un Support de Signalisation Radio (SRB) et un Support de Données Radio (DRB)
- Valeur maximale observée sur des périodes d'échantillonnage de 1 seconde
- Indique la charge utilisateur concurrente maximale

Niveaux de Charge :

UEs Actifs	Niveau de Charge	Recommandation
0-50	Faible	Fonctionnement normal
50-100	Modéré	Surveiller la capacité
100-150	Élevé	Évaluer l'ajout de capacité
> 150	Très Élevé	Besoin d'expansion de capacité

Remarques :

- La capacité réelle dépend de la configuration matérielle de la station de base
- Nokia AirScale peut généralement supporter 150-250 UE actifs concurrents par cellule
- Un nombre élevé d'UE peut impacter le débit par utilisateur

---

Compteurs de Disponibilité de Cellule

M8020 - Mesures de Disponibilité de Cellule

Ces compteurs calculent le pourcentage de disponibilité de la cellule en échantillonnant l'état de la cellule à intervalles réguliers.

Compteur	Nom	Description	Unité	Type	Int de
M8020C3	Échantillons lorsque la cellule est disponible	Nombre d'échantillons lorsque la cellule était disponible	Entier	Somme	~1 sec
M8020C4	Échantillons lorsque la cellule est prévue comme indisponible	Nombre d'échantillons lorsque la cellule était en maintenance planifiée	Entier	Somme	~1 sec
M8020C6	Dénominateur de disponibilité de cellule	Nombre total d'échantillons de vérification de disponibilité	Entier	Dénominateur	~1 sec

Calcul de la Disponibilité de Cellule :

```
Disponibilité de Cellule % = 100.0 × M8020C3 / (M8020C6 - M8020C4)
```

Explication de la Formule :

- **M8020C3** - Échantillons lorsque la cellule fonctionnait normalement
- **M8020C6** - Total des échantillons pris
- **M8020C4** - Échantillons d'indisponibilité planifiée (exclus du calcul)

Objectifs de Disponibilité :

Disponibilité	Classe	Statut
> 99.9%	Excellent	Respect de l'accord de niveau de service (SLA)
99.0-99.9%	Bon	Fonctionnement normal
95.0-99.0%	Passable	Enquête sur les problèmes
< 95.0%	Pauvre	Critique - action immédiate requise

Exemple de Requête Grafana :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] == "M8020C3" or
                       r["metricCounter"] == "M8020C6" or
                       r["metricCounter"] == "M8020C4")
  |> pivot(rowKey:["_time"], columnKey: ["metricCounter"],
valueColumn: "_value")
  |> map(fn: (r) => ({
      _time: r._time,
      "Disponibilité de Cellule": 100.0 * r.M8020C3 / (r.M8020C6 -
r.M8020C4)
    }))
```

Compteurs de Qualité Radio

M8005 - Mesures de Qualité Radio

Ces compteurs mesurent l'Indicateur de Force du Signal Reçu (RSSI) et le Rapport Signal sur Interférence et Bruit (SINR), fournissant un aperçu des conditions radio.

Mesures RSSI

Compteur	Nom	Description	Unité	Type
M8005C0	RSSI pour PUCCH Min	RSSI minimum sur le Canal de Contrôle Uplink Physique	dBm	Min
M8005C1	RSSI pour PUCCH Max	RSSI maximum sur le Canal de Contrôle Uplink Physique	dBm	Max
M8005C2	RSSI pour PUCCH Moyenne	RSSI moyen sur le Canal de Contrôle Uplink Physique	dBm	Moyenne

Comprendre le RSSI :

- **RSSI** = Indicateur de Force du Signal Reçu (puissance totale reçue)
- **PUCCH** = Canal de Contrôle Uplink Physique (transporte des informations de contrôle)
- Mesuré en dBm (décibel-milliwatts)
- Mis à jour lorsque les valeurs RSSI li��es à l'UE sont calculées

Interprétation des Valeurs RSSI :

Plage RSSI	Qualité	Description
> -70 dBm	Excellent	Signal très fort
-70 à -85 dBm	Bon	Signal fort, bonne performance
-85 à -100 dBm	Passable	Signal adéquat
-100 à -110 dBm	Pauvre	Signal faible, problèmes potentiels
< -110 dBm	Très Pauvre	Signal très faible, problèmes probables

Cas d'Utilisation :

- **Analyse de couverture** - Un faible RSSI indique des lacunes de couverture
- **Dépannage d'interférences** - Modèles RSSI inattendus
- **Planification RF** - Valider les prévisions de force du signal

---

Compteurs de Gestion de Connexion

M8013 - Établissement de Connexion de Signalisation

Ces compteurs suivent les tentatives et réussites d'établissement de connexion RRC (Radio Resource Control), des indicateurs clés de l'accessibilité du réseau.

Compteur	Nom	Description	Unité	Type
M8013C5	Établissements de Connexion de Signalisation Réussis	Établissements de connexion RRC réussis	Entier	Somme
M8013C17	Tentatives d'Établissement de Connexion de Signalisation MO-S	Tentatives de connexion - Signalisation Originaire Mobile	Entier	Somme
M8013C18	Tentatives d'Établissement de Connexion de Signalisation MT	Tentatives de connexion - Terminées Mobiles	Entier	Somme
M8013C19	Tentatives d'Établissement de Connexion de Signalisation MO-D	Tentatives de connexion - Données Originaire Mobile	Entier	Somme
M8013C21	Tentatives d'Établissement de Connexion de Signalisation Urgentes	Tentatives de connexion d'appel d'urgence	Entier	Somme
M8013C31	Tentatives d'Établissement de Connexion de Signalisation Haute Priorité	Tentatives de connexion de haute priorité	Entier	Somme
M8013C34	Tentatives d'Établissement de Connexion de	Tentatives de connexion	Entier	Somme

Compteur	Nom	Description	Unité	Type
	Signalisation Tolérantes au Délai	tolérantes au délai		
M8013C91	Tentatives d'Établissement de Connexion de Signalisation MO-V	Tentatives de connexion - Voix Originaire Mobile	Entier	Somme
M8013C93	Tentatives d'Établissement de Connexion de Signalisation MT-Accès	Tentatives de connexion - Accès MT	Entier	Somme

Calcul du Taux de Réussite de Configuration :

```
Taux de Réussite de Configuration % = 100.0 × M8013C5 / (M8013C17
+ M8013C18 + M8013C19 + M8013C34 + M8013C31 + M8013C21 + M8013C93
+ M8013C91)
```

Explication de la Formule :

- **M8013C5** - Achèvements réussis (Configuration de Connexion RRC Complète reçue)
- **Somme des compteurs de tentatives** - Total des tentatives de connexion dans toutes les catégories

Types de Connexion :

- **MO-S (M8013C17)** - Signalisation Originaire Mobile (SMS, mises à jour de localisation)
- **MT (M8013C18)** - Terminées Mobiles (appels/données entrants)
- **MO-D (M8013C19)** - Données Originaire Mobile (sessions de données)
- **MO-V (M8013C91)** - Voix Originaire Mobile (appels VoLTE)
- **Urgent (M8013C21)** - Appels d'urgence (911, 112)

Objectifs de Performance :

Taux de Réussite	Classe	Statut
> 99%	Excellent	Fonctionnement normal
95-99%	Bon	Performance acceptable
90-95%	Passable	Enquête recommandée
< 90%	Pauvre	Problème critique - dépannage immédiat

Causes Courantes d'Échec :

- Problèmes de couverture (signal faible)
- Congestion (cellule à pleine capacité)
- Erreurs de configuration
- Problèmes matériels
- Interférences

Compteurs de Latence et QoS

M8001 - Mesures de Performance de Cellule

Compteur	Nom	Description	Unité	Type
M8001C2	Délai SDU PDCP sur DL DTCH Moyenne	Temps de rétention moyen SDU PDCP descendant dans l'eNB	ms	Moyenne

Comprendre la Latence :

- **SDU PDCP** = Unité de Données de Service du Protocole de Convergence de Données de Paquet (paquet de données utilisateur)

- **Délai** = Temps que le paquet passe dans la station de base avant transmission
- **DL DTCH** = Canal de Trafic Dédié Descendant (canal de données utilisateur)
- Des valeurs plus basses = meilleure réactivité

Objectifs de Latence :

Latence	Classe	Impact sur l'Application
< 10 ms	Excellent	Idéal pour VoLTE, jeux, appels vidéo
10-20 ms	Bon	Acceptable pour la plupart des applications
20-50 ms	Passable	Remarquable dans les applications interactives
> 50 ms	Pauvre	Impact sur les applications en temps réel

Causes de Haute Latence :

- Congestion de file d'attente (trop d'utilisateurs)
- Problèmes de configuration du planificateur
- Mauvaises conditions radio (beaucoup de retransmissions)
- Retards de liaison montante

Compteurs d'Interface S1

M8000 - Mesures d'Interface S1

Ces compteurs suivent l'interface S1 entre l'eNodeB et le MME (Entité de Gestion de Mobilité), y compris la configuration de contexte, la gestion de connexion S1 et les procédures de signalisation.

Compteur	Nom	Description	Unité	Type
M8000C0	Demandes de Configuration de Contexte Initial	Nombre de tentatives de Configuration de Contexte Initial	Entier	Somme
M8000C1	Achèvements de Configuration de Contexte Initial	Configurations de Contexte Initial réussies	Entier	Somme
M8000C2	Échecs de Configuration - Réseau Radio	Échecs dus à des problèmes de réseau radio	Entier	Somme
M8000C3	Échecs de Configuration - Transport	Échecs dus à des problèmes de couche de transport	Entier	Somme
M8000C6	Demandes de Configuration S1	Tentatives d'établissement de l'interface S1	Entier	Somme
M8000C7	Achèvements de Configuration S1	Configurations S1 réussies	Entier	Somme
M8000C11	Demandes de Paging S1	Messages de paging de MME	Entier	Somme
M8000C12	Configuration de Connexion Logique S1 UE	Connexions S1 associées à l'UE établies	Entier	Somme
M8000C29	Transport NAS Montant	Messages NAS envoyés au MME	Entier	Somme

Compteur	Nom	Description	Unité	Type
M8000C30	Transport NAS Descendant	Messages NAS reçus du MME	Entier	Somme

Comprendre l'Interface S1 :

- L'interface **S1** connecte l'eNodeB au EPC (Noyau de Paquet Évolué)
- La **Configuration de Contexte Initial** établit le contexte pour une nouvelle connexion UE
- La **Configuration S1** est la poignée de main initiale entre l'eNodeB et le MME
- Les messages **NAS (Non-Access Stratum)** transportent le signalisation de couche supérieure

Calcul du Taux de Réussite :

```
Taux de Réussite de Configuration S1 = 100 × M8000C7 / M8000C6
Taux de Réussite de Contexte Initial = 100 × M8000C1 / M8000C0
```

Objectifs de Performance :

- Taux de Réussite de Configuration S1 : > 99%
- Taux de Réussite de Contexte Initial : > 95%

Compteurs de Support EPS

M8006 - Mesures de Support EPS

Ces compteurs suivent les procédures d'établissement, de modification et de libération de Support Radio d'Accès E-UTRAN (E-RAB) et de support EPS.

Compteurs Clés :

Compteur	Nom	Description	Unité	Type
M8006C0	Tentatives d'Établissement de Support EPS	Tentatives d'établissement de support	Entier	Somme
M8006C1	Achèvements d'Établissement de Support EPS	Établissements de support réussis	Entier	Somme
M8006C2-C5	Échecs de Configuration par Cause	Échecs classés par raison	Entier	Somme

Comprendre les Supports EPS :

- **Support** = Canal logique pour les données utilisateur entre l'UE et le réseau
- **Support par Défaut** = Support toujours actif pour la connectivité Internet
- **Support Dédié** = Supports supplémentaires pour des exigences QoS spécifiques (VoLTE, streaming vidéo)

Cas d'Utilisation :

- Surveiller les taux de réussite d'établissement de support
- Identifier les raisons des échecs de support
- Suivre l'allocation de support QoS pour des services premium

---

Compteurs de Transfert

M8009 - Mesures de Préparation de Transfert

M8014 - Mesures de Transfert Inter-eNB

M8015 - Mesures de Transfert Intra-eNB

M8021 - Mesures de Transfert Inter-Fréquence

Ces groupes de mesure suivent les procédures de transfert - le processus de transfert d'une connexion UE d'une cellule à une autre sans interrompre l'appel.

Types de Transfert :

Type	Description	Groupe de Mesure
Intra-eNB	Transfert entre cellules sur la même station de base	M8015
Inter-eNB	Transfert entre différentes stations de base (X2)	M8014
Inter-Fréquence	Transfert vers une fréquence porteuse différente	M8021
Inter-RAT	Transfert vers une technologie différente (LTE→3G/2G)	M8017

Métriques Clés :

Groupe de Compteurs	Focus	Compteurs Critiques
M8009	Échecs de préparation de transfert	Tentatives de préparation, échecs par cause
M8014	HO basé sur X2	Tentatives de préparation, exécutions, échecs
M8015	HO intra-cellule	Tentatives de préparation, exécutions, échecs
M8021	HO inter-fréquence	Tentatives, succès, échecs

Formule du Taux de Succès de Transfert :

```
Taux de Succès de HO = 100 × (Exécutions de HO) / (Tentatives de Préparation de HO)
```

Objectifs de Performance :

- Taux de Succès de HO Intra-eNB : > 99%
- Taux de Succès de HO Inter-eNB : > 98%
- Taux de Succès de HO Inter-Fréquence : > 95%

Causes Courantes d'Échec de Transfert :

- Congestion de la cellule cible (aucune ressource disponible)
- Mauvaises conditions radio à la cellule cible
- Expiration du minuteur (UE ne répond pas à temps)
- Lacunes de mesure empêchant une sélection correcte de la cellule

---

Mesures de Qualité de Canal

M8010 - Distribution du CQI (Indicateur de Qualité de Canal)

Ces compteurs suivent la distribution des rapports CQI des UE, fournissant un aperçu de la qualité du canal radio.

Comprendre le CQI :

- **CQI** = Indicateur de Qualité de Canal rapporté par l'UE à l'eNodeB
- **Plage :** CQI 0 (pire) à CQI 15 (meilleur)
- **Objectif :** Aide le planificateur à sélectionner le MCS approprié (Schéma de Modulation et de Codage)
- **Fréquence de Mise à Jour :** Toutes les quelques millisecondes en fonction des conditions de canal

Mapping CQI à Débit de Données :

Niveau CQI	Qualité de Canal	Débit Max Approximatif	Modulation
0-3	Très Mauvais	< 1 Mbps	QPSK
4-6	Mauvais	1-5 Mbps	QPSK
7-9	Passable	5-15 Mbps	16-QAM
10-12	Bon	15-40 Mbps	64-QAM
13-15	Excellent	40-150 Mbps	64-QAM

Compteurs M8010 :

- M8010C0 - M8010C15 : Compte des rapports CQI à chaque niveau (0-15)

Analyse de Performance :

```
CQI Moyen = Σ(CQI_niveau × M8010C[niveau]) / Σ(M8010C[niveau])
```

Interprétation de la Distribution du CQI :

- **CQI Élevé (10-15) :** Bonne couverture, potentiel de débit élevé
- **CQI Moyen (7-9) :** Couverture adéquate, débit modéré
- **CQI Faible (0-6) :** Problèmes de couverture, envisager l'optimisation de la cellule

---

Compteurs de Repli CS

M8016 - Mesures de Repli CS

Ces compteurs suivent les procédures de Repli Circuit-Switched (CSFB), où les UE LTE se replient sur des réseaux 2G/3G pour les appels vocaux.

Comprendre le CSFB :

- **Objectif :** Gérer les appels vocaux sur des réseaux sans VoLTE
- **Processus :** UE en LTE → Appel vocal → Passer temporairement à 2G/3G → Retour à LTE
- **Impact :** Délai de configuration d'appel, perte temporaire de données LTE

Compteurs Clés :

Compteur	Nom	Description
M8016C0	Tentatives CSFB avec Redirection	CSFB utilisant la méthode de redirection
M8016C1	Tentatives CSFB avec Handover	CSFB utilisant la méthode de transfert

Méthodes CSFB :

1. **Redirection :** UE se déconnecte de LTE, re-sélectionne 2G/3G (plus rapide mais interruption de service brève)
2. **Handover :** Transfert approprié de LTE à 2G/3G (plus lent mais sans interruption)

Métriques de Performance :

- Taux de Succès CSFB = Transitions réussies / Total des tentatives CSFB
- Objectif : > 98%

Compteurs de Volume de Données

M8023 - Mesures de Volume de Données PDCP SDU

Ces compteurs suivent le volume total de données utilisateur transmises sur l'interface radio.

Métriques Clés :

- Volume total de données (montant et descendant)
- Volume par QCI (Identifiant de Classe de Qualité de Service)
- Volume par type de bearer

Cas d'Utilisation :

- Planification de la capacité du réseau
- Estimation des revenus (suivi de l'utilisation des données)
- Analyse de la consommation de données par utilisateur
- Profilage du trafic de classe QoS

Relation avec M8012 (Débit) :

- **M8012 :** Débit instantané (kbit/s)
- **M8023 :** Volume de données cumulatif (octets)

Compteurs de l'Interface X2

M8004 - Mesures de Volume de Données X2

M8022 - Mesures de Configuration X2

Ces compteurs suivent l'interface X2 entre les eNodeBs, utilisée pour les transferts inter-eNB et l'équilibrage de charge.

M8004 - Volume de Données X2 :

- Mesure des données transférées entre les eNodeBs lors des transferts
- Suit le volume de trafic X2 entrant et sortant

M8022 - Configuration X2 :

- **M8022C0 :** Tentatives de Configuration X2
- **M8022C1 :** Succès de Configuration X2

Comprendre l'Interface X2 :

- **Objectif :** Communication directe entre les eNodeBs voisins
- **Fonctions :** Coordination des transferts, partage de charge, gestion des interférences
- **Avantage :** Réduit la charge du réseau central, transferts plus rapides

Taux de Succès de Configuration X2 :

```
Taux de Succès de Configuration X2 = 100 × M8022C1 / M8022C0
```

Objectif : > 95%

Groupes de Mesures Supplémentaires

M8007 - Mesures de Bearer Radio de Données (DRB)

Suit l'établissement, la modification et la libération des Bearers Radio de Données (DRBs) pour la transmission de données utilisateur.

Domaines de Focus :

- Taux de succès de configuration de DRB
- Procédures de modification de DRB
- Statistiques de libération de bearer

M8008 - Mesures de Rejet de Connexion RRC

Suit les demandes de connexion RRC qui sont rejetées, classées par cause de rejet.

Raisons Courantes de Rejet :

- Congestion du réseau (PRBs insuffisants)
- Limite maximale d'UE atteinte
- Redirection pour équilibrage de charge
- Restrictions de mobilité

M8019 - Changement de Cellule Assisté par le Réseau (NACC)

Suit les procédures NACC pour optimiser la re-sélection de cellules de LTE à GSM.

Objectif : Fournir des informations sur le système de cellules voisines GSM aux UE avant la re-sélection, accélérant ainsi la transition.

Mesures de l'Interface Réseau

M5112 - Mesures d'Entrée de l'Interface IP

M5113 - Mesures RX Ethernet

Ces groupes de mesures suivent les statistiques de l'interface de retour.

M5112 - Entrée de l'Interface IP (112 compteurs) :

- Comptes de paquets entrants
- Distribution de la taille des paquets
- Statistiques spécifiques au protocole
- Utilisation de l'interface

M5113 - RX Ethernet (21 compteurs) :

- Comptes de trames Ethernet reçues
- Distribution de la taille des trames
- Statistiques d'erreur (erreurs CRC, erreurs de trame)

Cas d'Utilisation :

- Surveillance de la capacité de retour
- Évaluation de la santé des liaisons de transport
- Dépannage des problèmes de connectivité
- Planification de la capacité pour les mises à niveau de transport

---

Compteurs de Matériel et d'Unité Radio

M40001 - Mesures de Matériel Radio

Compteur	Nom	Description	Unité	Type	Échelle
M40001C0	VSWR par branche d'antenne	Rapport d'Ondes Stationnaires de Tension	0.1	Moyenne	Diviser par 10

Comprendre le VSWR :

- **VSWR** = Rapport d'Ondes Stationnaires de Tension
- Mesure de l'efficacité du système d'antenne
- Indique un déséquilibre d'impédance et des problèmes potentiels de câble/antenne
- Valeurs plus basses = mieux

Interprétation du VSWR :

VSWR	Statut	Action
1.0-1.5	Excellent	Fonctionnement normal
1.5-2.0	Bon	Acceptable
2.0-3.0	Passable	Enquête
> 3.0	Mauvais	Problème de câble/antenne - dépannage immédiat

Causes Courantes d'un VSWR Élevé :

- Câbles coaxiaux endommagés

- Connecteurs desserrés
- Ingress d'eau
- Dommages à l'antenne
- Déséquilibre d'impédance

Exemple de Requête Grafana :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] == "M40001C0")
  |> filter(fn: (r) => r._field == "counterValue")
  |> map(fn: (r) => ({ r with "VSWR": r._value / 10.0}))
```

M40002 - Mesures de Consommation Électrique

Compteur	Nom	Description	Unité	Type	Écho
M40002C2	Consommation Électrique	Consommation électrique de la station de base	100000 facteur	Moyenne	Divis par 1000

Comprendre la Consommation Électrique :

- Mesure de la consommation totale d'énergie de la station de base
- Utile pour les calculs OPEX et la planification de la capacité
- Peut indiquer des problèmes matériels si anormalement élevé/bas

Exemple de Requête Grafana :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] == "M40002C2")
  |> filter(fn: (r) => r._field == "counterValue")
  |> map(fn: (r) => ({ r with "Power": r._value / 100000.0}))
```

Utilisation des Compteurs dans Grafana

Création de Tableaux de Bord Efficaces

1. Tableau de Bord d'Utilisation des Ressources

Combinez M8011C24 et M8011C37 pour montrer l'utilisation des PRB montant/descendant :

```
// Utilisation des PRB Montant
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] == "M8011C24")
  |> map(fn: (r) => ({ r with _value: r._value / 10.0}))
  |> rename(columns: {"_value": "Utilisation PRB Montant %"})

// Utilisation des PRB Descendant
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] == "M8011C37")
  |> map(fn: (r) => ({ r with _value: r._value / 10.0}))
  |> rename(columns: {"_value": "Utilisation PRB Descendant %"})
```

2. Tableau de Bord de Débit

Montrez les taux de transfert de données :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] == "M8012C23" or
r["metricCounter"] == "M8012C26")
  |> map(fn: (r) => ({ r with _value: r._value / 1000.0}))  //
Convertir en Mbps
  |> pivot(rowKey: ["_time"], columnKey: ["metricCounter"],
valueColumn: "_value")
  |> map(fn: (r) => ({
      _time: r._time,
      "Uplink Mbps": r.M8012C23,
      "Downlink Mbps": r.M8012C26
    }))
```

3. Tableau de Bord de Disponibilité

Calculez et affichez la disponibilité des cellules :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] =~ /M8020C(3|4|6)/)
  |> pivot(rowKey: ["_time"], columnKey: ["metricCounter"],
valueColumn: "_value")
  |> map(fn: (r) => ({
      _time: r._time,
      "Disponibilité %": 100.0 * r.M8020C3 / (r.M8020C6 -
r.M8020C4)
    }))
```

4. Tableau de Bord du Taux de Succès de Connexion

Suivez la performance de configuration RRC :

```
from(bucket: "nokia-monitor")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["metricCounter"] =~
/M8013C(5|17|18|19|21|31|34|91|93)/)
  |> pivot(rowKey: ["_time"], columnKey: ["metricCounter"],
valueColumn: "_value")
  |> map(fn: (r) => ({
      _time: r._time,
      "Taux de Succès de Configuration %": 100.0 * r.M8013C5 /
(r.M8013C17 + r.M8013C18 + r.M8013C19 + r.M8013C34 + r.M8013C31 +
r.M8013C21 + r.M8013C93 + r.M8013C91)
    }))
```

Meilleures Pratiques pour les Tableaux de Bord

Utilisez des Types de Visualisation Appropriés :

- Graphiques en série temporelle - Données de tendance (débit, utilisation des PRB)
- Jauges - Valeurs actuelles (pourcentage de disponibilité)
- Panneaux de statistiques uniques - Valeurs maximales (max UE actifs)
- Cartes thermiques - Données de distribution (niveaux RSSI)

Définissez des Seuils Significatifs :

- Vert : Fonctionnement normal
- Jaune : Avertissement (enquête)
- Rouge : Critique (action immédiate)

Configuration d'Exemple des Seuils :

- Utilisation des PRB : Vert < 70%, Jaune 70-85%, Rouge > 85%
- Disponibilité : Vert > 99%, Jaune 95-99%, Rouge < 95%
- Succès de configuration : Vert > 99%, Jaune 95-99%, Rouge < 95%

Groupez les Métriques Connexes :

- Créez des tableaux de bord séparés pour la capacité, la performance et la qualité
- Utilisez des variables de modèle pour la sélection de site/cellule
- Incluez des liens de forage vers des vues détaillées

Documentation Connexe

- Guide des Opérations - Opérations et flux de travail du RAN Monitor
- Guide d'Intégration Grafana - Configuration des tableaux de bord Grafana
- Guide de Configuration Runtime - Configuration du RAN Monitor
- Guide de Configuration AirScale - Configuration de la station de base
- Référence des Métriques - Structure des données InfluxDB

Tableau de Référence Rapide

Compteurs les Plus Couramment Utilisés

Compteur	Nom	Cas d'Utilisation	Unité
M8011C24	Utilisation PRB UL moyenne	Planification de capacité	0.1%
M8011C37	Utilisation PRB DL moyenne	Planification de capacité	0.1%
M8012C23	Débit PDCP UL	Suivi de performance	kbit/s
M8012C26	Débit PDCP DL	Suivi de performance	kbit/s
M8018C1	UEs Actifs max	Suivi de charge	compte
M8020C3	Échantillons de cellule disponibles	Suivi de disponibilité	compte
M8020C6	Dénominateur de disponibilité	Calcul de disponibilité	compte
M8013C5	Achèvements de configuration	Suivi du taux de succès	compte
M8005C0	RSSI min	Analyse de couverture	dBm
M8005C2	RSSI moyen	Analyse de couverture	dBm
M8001C2	Délai PDCP moyen	Suivi de latence	ms

Compteur	Nom	Cas d'Utilisation	Unité
M40001C0	VSWR	Santé du matériel	0.1 ratio

Sources :

- Mesures de Performance LTE Nokia FlexiRadio
- Spécifications des Compteurs de Performance Nokia AirScale
- Normes de Gestion de Performance LTE 3GPP

Annexe : Liste Complète des Compteurs

Ci-dessous se trouve la liste complète de référence de tous les 1,186 compteurs de performance LTE Nokia extraits de la spécification KPI de Nokia.

```
=========================================================================
NOKIA LTE PERFORMANCE COUNTER COMPLETE REFERENCE
=========================================================================

-------------------------------------------------------------------------
Measurement Group: M8000
-------------------------------------------------------------------------
M8000C0         | Initial Context Setup requests
M8000C1         | Initial Context Setup completions
M8000C2         | Initial Context Setup failures due to
M8000C3         | Initial Context Setup failures due to
M8000C4         | Initial Context Setup failures due to
M8000C5         | Initial Context Setup failures due to
M8000C6         | S1 setup requests
M8000C7         | S1 setup completions
M8000C8         | S1 setup failure due to timer expiration
M8000C9         | S1 setup failure due to MME rejection
M8000C11        | S1 Paging requests
M8000C12        | Number of UE-associated logical S1-
M8000C13        | Global S1 Reset initiated by the eNB
M8000C14        | Global S1 Reset initiated by the MME
M8000C15        | Partial S1 Reset initiated by the eNB
M8000C16        | Partial S1 Reset initiated by the MME
M8000C23        | UE Context modification attempts
M8000C24        | UE Context modification attempts due
M8000C25        | UE Context modification failures
M8000C29        | Number of Uplink NAS Transport
M8000C30        | Number of Downlink NAS Transport
M8000C31        | UE Context modification attempts due
M8000C32        | E-RAB Setup Requests for IMS
M8000C33        | E-RAB Setup Completions for IMS
M8000C34        | E-RAB setup failures for IMS
M8000C35        | Number of Location Reporting Control
M8000C36        | Number of Location Report messages
M8000C37        | Number of successful X2 IP address
M8000C38        | Number of attempted X2 IP address
M8000C39        | Number of WRITE-REPLACE
M8000C40        | Number of WRITE-REPLACE
M8000C41        | Number of KILL REQUEST messages
M8000C42        | Number of KILL RESPONSE

-------------------------------------------------------------------------
Measurement Group: M8001
```

```
-----------------------------------------------------------------------
M8001C0         | PDCP SDU delay on DL DTCH Min
M8001C1         | PDCP SDU delay on DL DTCH Max
M8001C2         | PDCP SDU delay on DL DTCH Mean
M8001C3         | PDCP SDU delay on UL DTCH Min
M8001C4         | PDCP SDU delay on UL DTCH Max
M8001C5         | PDCP SDU delay on UL DTCH Mean
M8001C6         | RACH setup attempts for small size
M8001C7         | RACH setup attempts for large size
M8001C8         | RACH setup completions
M8001C9         | Transmitted TBs on PCH
M8001C10        | Transmitted TBs on BCH
M8001C11        | Transmitted TBs on DL-SCH
M8001C12        | HARQ retransmissions on DL-SCH
M8001C13        | Correct non-duplicate UL-SCH TB with
M8001C14        | Correct UL-SCH TB with re-reception
M8001C15        | Erroneous UL-SCH TB receptions
M8001C16        | PUSCH transmissions using MCS0
M8001C17        | PUSCH transmissions using MCS1
M8001C18        | PUSCH transmissions using MCS2
M8001C19        | PUSCH transmissions using MCS3
M8001C20        | PUSCH transmissions using MCS4
M8001C21        | PUSCH transmissions using MCS5
M8001C22        | PUSCH transmissions using MCS6
M8001C23        | PUSCH transmissions using MCS7
M8001C24        | PUSCH transmissions using MCS8
M8001C25        | PUSCH transmissions using MCS9
M8001C26        | PUSCH transmissions using MCS10
M8001C27        | PUSCH transmissions using MCS11
M8001C28        | PUSCH transmissions using MCS12
M8001C29        | PUSCH transmissions using MCS13
M8001C30        | PUSCH transmissions using MCS14
M8001C31        | PUSCH transmissions using MCS15
M8001C32        | PUSCH transmissions using MCS16
M8001C33        | PUSCH transmissions using MCS17
M8001C34        | PUSCH transmissions using MCS18
M8001C35        | PUSCH transmissions using MCS19
M8001C36        | PUSCH transmissions using MCS20
M8001C37        | PUSCH transmissions using MCS21
M8001C38        | PUSCH transmissions using MCS22
M8001C39        | PUSCH transmissions using MCS23
M8001C40        | PUSCH transmissions using MCS24
M8001C41        | PUSCH transmissions using MCS25
M8001C42        | PUSCH transmissions using MCS26
```

```
M8001C43        | PUSCH transmissions using MCS27
M8001C44        | PUSCH transmissions using MCS28
M8001C45        | PDSCH transmissions using MCS0
M8001C46        | PDSCH transmissions using MCS1
M8001C47        | PDSCH transmissions using MCS2
M8001C48        | PDSCH transmissions using MCS3
M8001C49        | PDSCH transmissions using MCS4
M8001C50        | PDSCH transmissions using MCS5
M8001C51        | PDSCH transmissions using MCS6
M8001C52        | PDSCH transmissions using MCS7
M8001C53        | PDSCH transmissions using MCS8
M8001C54        | PDSCH transmissions using MCS9
M8001C55        | PDSCH transmissions using MCS10
M8001C56        | PDSCH transmissions using MCS11
M8001C57        | PDSCH transmissions using MCS12
M8001C58        | PDSCH transmissions using MCS13
M8001C59        | PDSCH transmissions using MCS14
M8001C60        | PDSCH transmissions using MCS15
M8001C61        | PDSCH transmissions using MCS16
M8001C62        | PDSCH transmissions using MCS17
M8001C63        | PDSCH transmissions using MCS18
M8001C64        | PDSCH transmissions using MCS19
M8001C65        | PDSCH transmissions using MCS20
M8001C66        | PDSCH transmissions using MCS21
M8001C67        | PDSCH transmissions using MCS22
M8001C68        | PDSCH transmissions using MCS23
M8001C69        | PDSCH transmissions using MCS24
M8001C70        | PDSCH transmissions using MCS25
M8001C71        | PDSCH transmissions using MCS26
M8001C72        | PDSCH transmissions using MCS27
M8001C73        | PDSCH transmissions using MCS28
M8001C74        | PUSCH transmission nacks using
M8001C75        | PUSCH transmission nacks using
M8001C76        | PUSCH transmission nacks using
M8001C77        | PUSCH transmission nacks using
M8001C78        | PUSCH transmission nacks using
M8001C79        | PUSCH transmission nacks using
M8001C80        | PUSCH transmission nacks using
M8001C81        | PUSCH transmission nacks using
M8001C82        | PUSCH transmission nacks using
M8001C83        | PUSCH transmission nacks using
M8001C84        | PUSCH transmission nacks using
M8001C85        | PUSCH transmission nacks using
M8001C86        | PUSCH transmission nacks using
```

M8001C87	PUSCH transmission nacks using
M8001C88	PUSCH transmission nacks using
M8001C89	PUSCH transmission nacks using
M8001C90	PUSCH transmission nacks using
M8001C91	PUSCH transmission nacks using
M8001C92	PUSCH transmission nacks using
M8001C93	PUSCH transmission nacks using
M8001C94	PUSCH transmission nacks using
M8001C95	PUSCH transmission nacks using
M8001C96	PUSCH transmission nacks using
M8001C97	PUSCH transmission nacks using
M8001C98	PUSCH transmission nacks using
M8001C99	PUSCH transmission nacks using
M8001C100	PUSCH transmission nacks using
M8001C101	PUSCH transmission nacks using
M8001C102	PUSCH transmission nacks using
M8001C103	PDSCH transmission nacks using
M8001C104	PDSCH transmission nacks using
M8001C105	PDSCH transmission nacks using
M8001C106	PDSCH transmission nacks using
M8001C107	PDSCH transmission nacks using
M8001C108	PDSCH transmission nacks using
M8001C109	PDSCH transmission nacks using
M8001C110	PDSCH transmission nacks using
M8001C111	PDSCH transmission nacks using
M8001C112	PDSCH transmission nacks using
M8001C113	PDSCH transmission nacks using
M8001C114	PDSCH transmission nacks using
M8001C115	PDSCH transmission nacks using
M8001C116	PDSCH transmission nacks using
M8001C117	PDSCH transmission nacks using
M8001C118	PDSCH transmission nacks using
M8001C119	PDSCH transmission nacks using
M8001C120	PDSCH transmission nacks using
M8001C121	PDSCH transmission nacks using
M8001C122	PDSCH transmission nacks using
M8001C123	PDSCH transmission nacks using
M8001C124	PDSCH transmission nacks using
M8001C125	PDSCH transmission nacks using
M8001C126	PDSCH transmission nacks using
M8001C127	PDSCH transmission nacks using
M8001C128	PDSCH transmission nacks using
M8001C129	PDSCH transmission nacks using
M8001C130	PDSCH transmission nacks using

```
M8001C131       | PDSCH transmission nacks using
M8001C132       | RLC SDUs on DL DTCH
M8001C133       | RLC SDUs on DL DCCH
M8001C135       | RLC SDUs on UL DTCH
M8001C136       | RLC SDUs on UL DCCH
M8001C137       | RLC PDU first transmissions
M8001C138       | RLC PDU re-transmissions
M8001C139       | RLC PDU reception
M8001C140       | DL RLC C-PDUs transmitted the first
M8001C141       | DL RLC Data PDUs transmitted first
M8001C142       | UL RLC PDUs received
M8001C143       | Duplicate UL RLC PDU received
M8001C144       | UL RLC PDU retransmission requested
M8001C145       | UL RLC PDUs discarded
M8001C146       | DL RLC SDU From PDCP
M8001C147       | Average number of UEs with buffered
M8001C148       | Max number of UEs with buffered data
M8001C150       | Average number of UEs with buffered
M8001C151       | Max number of UEs with buffered data
M8001C153       | PDCP SDUs in Uplink
M8001C154       | PDCP SDUs in Downlink
M8001C155       | Discarded PDCP SDUs in downlink
M8001C156       | Failed Transmission PDSCH MCS0
M8001C157       | Failed Transmission PDSCH MCS1
M8001C158       | Failed Transmission PDSCH MCS2
M8001C159       | Failed Transmission PDSCH MCS3
M8001C160       | Failed Transmission PDSCH MCS4
M8001C161       | Failed Transmission PDSCH MCS5
M8001C162       | Failed Transmission PDSCH MCS6
M8001C163       | Failed Transmission PDSCH MCS7
M8001C164       | Failed Transmission PDSCH MCS8
M8001C165       | Failed Transmission PDSCH MCS9
M8001C166       | Failed Transmission PDSCH MCS10
M8001C167       | Failed Transmission PDSCH MCS11
M8001C168       | Failed Transmission PDSCH MCS12
M8001C169       | Failed Transmission PDSCH MCS13
M8001C170       | Failed Transmission PDSCH MCS14
M8001C171       | Failed Transmission PDSCH MCS15
M8001C172       | Failed Transmission PDSCH MCS16
M8001C173       | Failed Transmission PDSCH MCS17
M8001C174       | Failed Transmission PDSCH MCS18
M8001C175       | Failed Transmission PDSCH MCS19
M8001C176       | Failed Transmission PDSCH MCS20
M8001C177       | Failed Reception PUSCH MCS0
```

```
M8001C178       | Failed Reception PUSCH MCS1
M8001C179       | Failed Reception PUSCH MCS2
M8001C180       | Failed Reception PUSCH MCS3
M8001C181       | Failed Reception PUSCH MCS4
M8001C182       | Failed Reception PUSCH MCS5
M8001C183       | Failed Reception PUSCH MCS6
M8001C184       | Failed Reception PUSCH MCS7
M8001C185       | Failed Reception PUSCH MCS8
M8001C186       | Failed Reception PUSCH MCS9
M8001C187       | Failed Reception PUSCH MCS10
M8001C188       | Failed Reception PUSCH MCS11
M8001C189       | Failed Reception PUSCH MCS12
M8001C190       | Failed Reception PUSCH MCS13
M8001C191       | Failed Reception PUSCH MCS14
M8001C192       | Failed Reception PUSCH MCS15
M8001C193       | Failed Reception PUSCH MCS16
M8001C194       | Failed Reception PUSCH MCS17
M8001C195       | Failed Reception PUSCH MCS18
M8001C196       | Failed Reception PUSCH MCS19
M8001C197       | Failed Reception PUSCH MCS20
M8001C199       | RRC Connected UEs Avg
M8001C200       | RRC Connected UEs Max
M8001C202       | Failed Transmission PDSCH MCS21
M8001C203       | Failed Transmission PDSCH MCS22
M8001C204       | Failed Transmission PDSCH MCS23
M8001C205       | Failed Transmission PDSCH MCS24
M8001C206       | Failed Transmission PDSCH MCS25
M8001C207       | Failed Transmission PDSCH MCS26
M8001C208       | Failed Transmission PDSCH MCS27
M8001C209       | Failed Transmission PDSCH MCS28
M8001C210       | Minimum queue length DL SRB
M8001C211       | Average queue length DL SRB
M8001C212       | Maximum queue length DL SRB
M8001C213       | Minimum queue length DL DRB
M8001C214       | Average queue length DL DRB
M8001C215       | Maximum queue length DL DRB
M8001C216       | Average number of available PRBs per
M8001C217       | Average number of available PRBs per
M8001C218       | RLC SDUs on BCCH
M8001C219       | RLC SDUs on DL CCCH
M8001C220       | RLC SDUs on PCCH
M8001C222       | RLC SDUs on UL CCCH
M8001C223       | Active UE per Cell average
M8001C224       | Active UE per Cell max
```

```
M8001C227       | UEs with buffered DL data for DRB with
M8001C228       | UEs with buffered DL data for QCI2
M8001C229       | UEs with buffered DL data for QCI3
M8001C230       | UEs with buffered DL data for QCI4
M8001C231       | Number of primary ETWS notifications
M8001C232       | Number of secondary ETWS
M8001C233       | Number of CMAS notifications
M8001C235       | UEs with buffered DL data for non-GBR
M8001C254       | Number of lost PDCP SDUs in UL
M8001C255       | Number of lost PDCP SDUs in UL for
M8001C256       | Number of lost PDCP SDUs in UL for
M8001C257       | Number of lost PDCP SDUs in UL for
M8001C258       | Number of lost PDCP SDUs in UL for
M8001C259       | Number of lost PDCP SDUs in DL
M8001C260       | Number of lost PDCP SDUs in DL for
M8001C261       | Number of lost PDCP SDUs in DL for
M8001C262       | Number of lost PDCP SDUs in DL for
M8001C263       | Number of lost PDCP SDUs in DL for
M8001C264       | Sum of Active UEs with buffered data in
M8001C265       | Denominator for Active UEs with
M8001C266       | Sum of Active UEs with buffered data in
M8001C267       | Denominator for Active UEs with
M8001C269       | Mean PDCP SDU delay on DL DTCH
M8001C270       | Mean PDCP SDU delay on DL DTCH
M8001C271       | PDCP SDU delay on DL DTCH Mean
M8001C272       | PDCP SDU delay on DL DTCH Mean
M8001C273       | PDCP SDU delay on DL DTCH Mean
M8001C286       | RACH setup attempts for dedicated
M8001C305       | PDCP SDU UL QCI 1
M8001C306       | PDCP SDU UL QCI 2
M8001C307       | PDCP SDU UL QCI 3
M8001C308       | PDCP SDU UL QCI 4
M8001C314       | PDCP SDU DL QCI 1
M8001C315       | PDCP SDU DL QCI 2
M8001C316       | PDCP SDU DL QCI 3
M8001C317       | PDCP SDU DL QCI 4
M8001C318       | Sum of RRC Connected UEs per cell
M8001C319       | Denominator for RRC Connected UEs
M8001C320       | Sum of Active UEs per cell
M8001C321       | Denominator for Active UEs per cell
M8001C323       | PDCP SDU discarded DL QCI 1
M8001C324       | PDCP SDU discarded DL QCI 2
M8001C325       | PDCP SDU discarded DL QCI 3
M8001C326       | PDCP SDU discarded DL QCI 4
```

```
M8001C419       | UEs with buffered UL data for DRB with
M8001C420       | UEs with buffered UL data for non-GBR
M8001C421       | Number of PDCCH order attempts
M8001C422       | Number of initial PDCCH order
M8001C423       | Number of successful PDCCH orders
M8001C424       | Unavailability of dedicated preamble
M8001C425       | Unavailability of dedicated preamble for
M8001C426       | Unavailability of dedicated preamble for
M8001C427       | Number of UE state transitions from
M8001C428       | Average number of UEs in UL-In-Sync
M8001C429       | Average number of UEs with unlimited
M8001C430       | UE UL-Out-Of-Sync time T in the range
M8001C431       | UE UL-Out-Of-Sync time T in the range
M8001C432       | UE UL-Out-Of-Sync time T in the range
M8001C433       | UE UL-Out-Of-Sync time T in the range
M8001C434       | UE UL-Out-Of-Sync time T larger than
M8001C435       | First transmissions on PUSCH using
M8001C436       | First transmissions on PUSCH using
M8001C437       | First transmissions on PUSCH using
M8001C438       | First transmissions on PUSCH using
M8001C439       | First transmissions on PUSCH using
M8001C440       | First transmissions on PUSCH using
M8001C441       | First transmissions on PUSCH using
M8001C442       | First transmissions on PUSCH using
M8001C443       | First transmissions on PUSCH using
M8001C444       | First transmissions on PUSCH using
M8001C445       | First transmissions on PUSCH using
M8001C446       | First transmissions on PUSCH using
M8001C447       | First transmissions on PUSCH using
M8001C448       | First transmissions on PUSCH using
M8001C449       | First transmissions on PUSCH using
M8001C450       | First transmissions on PUSCH using
M8001C451       | First transmissions on PUSCH using
M8001C452       | First transmissions on PUSCH using
M8001C453       | First transmissions on PUSCH using
M8001C454       | First transmissions on PUSCH using
M8001C455       | First transmissions on PUSCH using
M8001C456       | First transmissions on PUSCH using
M8001C457       | First transmissions on PUSCH using
M8001C458       | First transmissions on PUSCH using
M8001C459       | First transmissions on PUSCH using
M8001C460       | First transmission NACKs on PUSCH
M8001C461       | First transmission NACKs on PUSCH
M8001C462       | First transmission NACKs on PUSCH
```

```
M8001C463       | First transmission NACKs on PUSCH
M8001C464       | First transmission NACKs on PUSCH
M8001C465       | First transmission NACKs on PUSCH
M8001C466       | First transmission NACKs on PUSCH
M8001C467       | First transmission NACKs on PUSCH
M8001C468       | First transmission NACKs on PUSCH
M8001C469       | First transmission NACKs on PUSCH
M8001C470       | First transmission NACKs on PUSCH
M8001C471       | First transmission NACKs on PUSCH
M8001C472       | First transmission NACKs on PUSCH
M8001C473       | First transmission NACKs on PUSCH
M8001C474       | First transmission NACKs on PUSCH
M8001C475       | First transmission NACKs on PUSCH
M8001C476       | First transmission NACKs on PUSCH
M8001C477       | First transmission NACKs on PUSCH
M8001C478       | First transmission NACKs on PUSCH
M8001C479       | First transmission NACKs on PUSCH
M8001C480       | First transmission NACKs on PUSCH
M8001C481       | First transmission NACKs on PUSCH
M8001C482       | First transmission NACKs on PUSCH
M8001C483       | First transmission NACKs on PUSCH
M8001C484       | First transmission NACKs on PUSCH
M8001C485       | Failed Reception PUSCH MCS21
M8001C486       | Failed Reception PUSCH MCS22
M8001C487       | Failed Reception PUSCH MCS23
M8001C488       | Failed Reception PUSCH MCS24
M8001C494       | Average number of DL carrier
M8001C495       | Average number of UEs with a
M8001C496       | Average number of UEs with an

-------------------------------------------------------------------------
Measurement Group: M8004
-------------------------------------------------------------------------
M8004C0         | X2 data volume per eNB, incoming
M8004C1         | X2 data volume per eNB, outgoing
M8004C2         | Incoming u-plane X2 data volume per
M8004C3         | Outgoing u-plane X2 data volume per

-------------------------------------------------------------------------
Measurement Group: M8005
-------------------------------------------------------------------------
M8005C0         | RSSI for PUCCH Min
M8005C1         | RSSI for PUCCH Max
M8005C2         | RSSI for PUCCH Mean
```

```
M8005C3         | RSSI for PUSCH Min
M8005C4         | RSSI for PUSCH Max
M8005C5         | RSSI for PUSCH Mean
M8005C6         | RSSI for PUCCH Level 01
M8005C7         | RSSI for PUCCH Level 02
M8005C8         | RSSI for PUCCH Level 03
M8005C9         | RSSI for PUCCH Level 04
M8005C10        | RSSI for PUCCH Level 05
M8005C11        | RSSI for PUCCH Level 06
M8005C12        | RSSI for PUCCH Level 07
M8005C13        | RSSI for PUCCH Level 08
M8005C14        | RSSI for PUCCH Level 09
M8005C15        | RSSI for PUCCH Level 10
M8005C16        | RSSI for PUCCH Level 11
M8005C17        | RSSI for PUCCH Level 12
M8005C18        | RSSI for PUCCH Level 13
M8005C19        | RSSI for PUCCH Level 14
M8005C20        | RSSI for PUCCH Level 15
M8005C21        | RSSI for PUCCH Level 16
M8005C22        | RSSI for PUCCH Level 17
M8005C23        | RSSI for PUCCH Level 18
M8005C24        | RSSI for PUCCH Level 19
M8005C25        | RSSI for PUCCH Level 20
M8005C26        | RSSI for PUCCH Level 21
M8005C27        | RSSI for PUCCH Level 22
M8005C28        | RSSI for PUSCH Level 01
M8005C29        | RSSI for PUSCH Level 02
M8005C30        | RSSI for PUSCH Level 03
M8005C31        | RSSI for PUSCH Level 04
M8005C32        | RSSI for PUSCH Level 05
M8005C33        | RSSI for PUSCH Level 06
M8005C34        | RSSI for PUSCH Level 07
M8005C35        | RSSI for PUSCH Level 08
M8005C36        | RSSI for PUSCH Level 09
M8005C37        | RSSI for PUSCH Level 10
M8005C38        | RSSI for PUSCH Level 11
M8005C39        | RSSI for PUSCH Level 12
M8005C40        | RSSI for PUSCH Level 13
M8005C41        | RSSI for PUSCH Level 14
M8005C42        | RSSI for PUSCH Level 15
M8005C43        | RSSI for PUSCH Level 16
M8005C44        | RSSI for PUSCH Level 17
M8005C45        | RSSI for PUSCH Level 18
M8005C46        | RSSI for PUSCH Level 19
```

```
M8005C47        | RSSI for PUSCH Level 20
M8005C48        | RSSI for PUSCH Level 21
M8005C49        | RSSI for PUSCH Level 22
M8005C54        | UE Power Headroom for PUSCH Level
M8005C55        | UE Power Headroom for PUSCH Level
M8005C56        | UE Power Headroom for PUSCH Level
M8005C57        | UE Power Headroom for PUSCH Level
M8005C58        | UE Power Headroom for PUSCH Level
M8005C59        | UE Power Headroom for PUSCH Level
M8005C60        | UE Power Headroom for PUSCH Level
M8005C61        | UE Power Headroom for PUSCH Level
M8005C62        | UE Power Headroom for PUSCH Level
M8005C63        | UE Power Headroom for PUSCH Level
M8005C64        | UE Power Headroom for PUSCH Level
M8005C65        | UE Power Headroom for PUSCH Level
M8005C66        | UE Power Headroom for PUSCH Level
M8005C67        | UE Power Headroom for PUSCH Level
M8005C68        | UE Power Headroom for PUSCH Level
M8005C69        | UE Power Headroom for PUSCH Level
M8005C70        | UE Power Headroom for PUSCH Level
M8005C71        | UE Power Headroom for PUSCH Level
M8005C72        | UE Power Headroom for PUSCH Level
M8005C73        | UE Power Headroom for PUSCH Level
M8005C74        | UE Power Headroom for PUSCH Level
M8005C75        | UE Power Headroom for PUSCH Level
M8005C76        | UE Power Headroom for PUSCH Level
M8005C77        | UE Power Headroom for PUSCH Level
M8005C78        | UE Power Headroom for PUSCH Level
M8005C79        | UE Power Headroom for PUSCH Level
M8005C80        | UE Power Headroom for PUSCH Level
M8005C81        | UE Power Headroom for PUSCH Level
M8005C82        | UE Power Headroom for PUSCH Level
M8005C83        | UE Power Headroom for PUSCH Level
M8005C84        | UE Power Headroom for PUSCH Level
M8005C85        | UE Power Headroom for PUSCH Level
M8005C87        | UE Power Headroom PUSCH Min
M8005C88        | UE Power Headroom PUSCH Max
M8005C89        | UE Power Headroom PUSCH Mean
M8005C90        | SINR for PUCCH Min
M8005C91        | SINR for PUCCH Max
M8005C92        | SINR for PUCCH Mean
M8005C93        | SINR for PUSCH Min
M8005C94        | SINR for PUSCH Max
M8005C95        | SINR for PUSCH Mean
```

```
M8005C96        | SINR for PUCCH Level 1
M8005C97        | SINR for PUCCH Level 2
M8005C98        | SINR for PUCCH Level 3
M8005C99        | SINR for PUCCH Level 4
M8005C100       | SINR for PUCCH Level 5
M8005C101       | SINR for PUCCH Level 6
M8005C102       | SINR for PUCCH Level 7
M8005C103       | SINR for PUCCH Level 8
M8005C104       | SINR for PUCCH Level 9
M8005C105       | SINR for PUCCH Level 10
M8005C106       | SINR for PUCCH Level 11
M8005C107       | SINR for PUCCH Level 12
M8005C108       | SINR for PUCCH Level 13
M8005C109       | SINR for PUCCH Level 14
M8005C110       | SINR for PUCCH Level 15
M8005C111       | SINR for PUCCH Level 16
M8005C112       | SINR for PUCCH Level 17
M8005C113       | SINR for PUCCH Level 18
M8005C114       | SINR for PUCCH Level 19
M8005C115       | SINR for PUCCH Level 20
M8005C116       | SINR for PUCCH Level 21
M8005C117       | SINR for PUCCH Level 22
M8005C118       | SINR for PUSCH Level 1
M8005C119       | SINR for PUSCH Level 2
M8005C120       | SINR for PUSCH Level 3
M8005C121       | SINR for PUSCH Level 4
M8005C122       | SINR for PUSCH Level 5
M8005C123       | SINR for PUSCH Level 6
M8005C124       | SINR for PUSCH Level 7
M8005C125       | SINR for PUSCH Level 8
M8005C126       | SINR for PUSCH Level 9
M8005C127       | SINR for PUSCH Level 10
M8005C128       | SINR for PUSCH Level 11
M8005C129       | SINR for PUSCH Level 12
M8005C130       | SINR for PUSCH Level 13
M8005C131       | SINR for PUSCH Level 14
M8005C132       | SINR for PUSCH Level 15
M8005C133       | SINR for PUSCH Level 16
M8005C134       | SINR for PUSCH Level 17
M8005C135       | SINR for PUSCH Level 18
M8005C136       | SINR for PUSCH Level 19
M8005C137       | SINR for PUSCH Level 20
M8005C138       | SINR for PUSCH Level 21
M8005C139       | SINR for PUSCH Level 22
```

```
M8005C140       | UL AMC upgrades
M8005C141       | UL AMC downgrades
M8005C206       | Minimum of cell-wide RSSI on PUCCH
M8005C207       | Maximum of cell-wide RSSI on PUCCH
M8005C208       | Mean of cell-wide RSSI on PUCCH
M8005C209       | Cell-wide RSSI on PUCCH level 1
M8005C210       | Cell-wide RSSI on PUCCH level 2
M8005C211       | Cell-wide RSSI on PUCCH level 3
M8005C212       | Cell-wide RSSI on PUCCH level 4
M8005C213       | Cell-wide RSSI on PUCCH level 5
M8005C214       | Cell-wide RSSI on PUCCH level 6
M8005C215       | Cell-wide RSSI on PUCCH level 7
M8005C216       | Cell-wide RSSI on PUCCH level 8
M8005C217       | Cell-wide RSSI on PUCCH level 9
M8005C218       | Cell-wide RSSI on PUCCH level 10
M8005C219       | Cell-wide RSSI on PUCCH level 11
M8005C220       | Cell-wide RSSI on PUCCH level 12
M8005C221       | Cell-wide RSSI on PUCCH level 13
M8005C222       | Cell-wide RSSI on PUCCH level 14
M8005C223       | Cell-wide RSSI on PUCCH level 15
M8005C224       | Cell-wide RSSI on PUCCH level 16
M8005C225       | Cell-wide RSSI on PUCCH level 17
M8005C226       | Cell-wide RSSI on PUCCH level 18
M8005C227       | Cell-wide RSSI on PUCCH level 19
M8005C228       | Cell-wide RSSI on PUCCH level 20
M8005C229       | Cell-wide RSSI on PUCCH level 21
M8005C230       | Cell-wide RSSI on PUCCH level 22
M8005C231       | Minimum of cell-wide RSSI on PUSCH
M8005C232       | Maximum of cell-wide RSSI on PUSCH
M8005C233       | Mean of cell-wide RSSI on PUSCH
M8005C234       | Cell-wide RSSI on PUSCH level 1
M8005C235       | Cell-wide RSSI on PUSCH level 2
M8005C236       | Cell-wide RSSI on PUSCH level 3
M8005C237       | Cell-wide RSSI on PUSCH level 4
M8005C238       | Cell-wide RSSI on PUSCH level 5
M8005C239       | Cell-wide RSSI on PUSCH level 6
M8005C240       | Cell-wide RSSI on PUSCH level 7
M8005C241       | Cell-wide RSSI on PUSCH level 8
M8005C242       | Cell-wide RSSI on PUSCH level 9
M8005C243       | Cell-wide RSSI on PUSCH level 10
M8005C244       | Cell-wide RSSI on PUSCH level 11
M8005C245       | Cell-wide RSSI on PUSCH level 12
M8005C246       | Cell-wide RSSI on PUSCH level 13
M8005C247       | Cell-wide RSSI on PUSCH level 14
```

M8005C248 | Cell-wide RSSI on PUSCH level 15
M8005C249 | Cell-wide RSSI on PUSCH level 16
M8005C250 | Cell-wide RSSI on PUSCH level 17
M8005C251 | Cell-wide RSSI on PUSCH level 18
M8005C252 | Cell-wide RSSI on PUSCH level 19
M8005C253 | Cell-wide RSSI on PUSCH level 20
M8005C254 | Cell-wide RSSI on PUSCH level 21
M8005C255 | Cell-wide RSSI on PUSCH level 22
M8005C256 | Minimum of cell-wide SINR on PUCCH
M8005C257 | Maximum of cell-wide SINR on PUCCH
M8005C258 | Mean of cell-wide SINR on PUCCH
M8005C259 | Cell-wide SINR on PUCCH level 1
M8005C260 | Cell-wide SINR on PUCCH level 2
M8005C261 | Cell-wide SINR on PUCCH level 3
M8005C262 | Cell-wide SINR on PUCCH level 4
M8005C263 | Cell-wide SINR on PUCCH level 5
M8005C264 | Cell-wide SINR on PUCCH level 6
M8005C265 | Cell-wide SINR on PUCCH level 7
M8005C266 | Cell-wide SINR on PUCCH level 8
M8005C267 | Cell-wide SINR on PUCCH level 9
M8005C268 | Cell-wide SINR on PUCCH level 10
M8005C269 | Cell-wide SINR on PUCCH level 11
M8005C270 | Cell-wide SINR on PUCCH level 12
M8005C271 | Cell-wide SINR on PUCCH level 13
M8005C272 | Cell-wide SINR on PUCCH level 14
M8005C273 | Cell-wide SINR on PUCCH level 15
M8005C274 | Cell-wide SINR on PUCCH level 16
M8005C275 | Cell-wide SINR on PUCCH level 17
M8005C276 | Cell-wide SINR on PUCCH level 18
M8005C277 | Cell-wide SINR on PUCCH level 19
M8005C278 | Cell-wide SINR on PUCCH level 20
M8005C279 | Cell-wide SINR on PUCCH level 21
M8005C280 | Cell-wide SINR on PUCCH level 22
M8005C281 | Minimum of cell-wide SINR on PUSCH
M8005C282 | Maximum of cell-wide SINR on PUSCH
M8005C283 | Mean of cell-wide SINR on PUSCH
M8005C284 | Cell-wide SINR on PUSCH level 1
M8005C285 | Cell-wide SINR on PUSCH level 2
M8005C286 | Cell-wide SINR on PUSCH level 3
M8005C287 | Cell-wide SINR on PUSCH level 4
M8005C288 | Cell-wide SINR on PUSCH level 5
M8005C289 | Cell-wide SINR on PUSCH level 6
M8005C290 | Cell-wide SINR on PUSCH level 7
M8005C291 | Cell-wide SINR on PUSCH level 8

```
M8005C292       | Cell-wide SINR on PUSCH level 9
M8005C293       | Cell-wide SINR on PUSCH level 10
M8005C294       | Cell-wide SINR on PUSCH level 11
M8005C295       | Cell-wide SINR on PUSCH level 12
M8005C296       | Cell-wide SINR on PUSCH level 13
M8005C297       | Cell-wide SINR on PUSCH level 14
M8005C298       | Cell-wide SINR on PUSCH level 15
M8005C299       | Cell-wide SINR on PUSCH level 16
M8005C300       | Cell-wide SINR on PUSCH level 17
M8005C301       | Cell-wide SINR on PUSCH level 18
M8005C302       | Cell-wide SINR on PUSCH level 19
M8005C303       | Cell-wide SINR on PUSCH level 20
M8005C304       | Cell-wide SINR on PUSCH level 21
M8005C305       | Cell-wide SINR on PUSCH level 22

-------------------------------------------------------------------------
Measurement Group: M8006
-------------------------------------------------------------------------
M8006C0         | EPS Bearer setup attempts
M8006C1         | EPS Bearer setup completions
M8006C2         | EPS Bearer setup failures due to Radio
M8006C3         | EPS Bearer setup failures due to
M8006C4         | EPS Bearer setup failures due to Radio
M8006C5         | EPS Bearer setup failures due to Other
M8006C6         | EPC initiated EPS Bearer Release
M8006C7         | EPC initiated EPS Bearer Release
M8006C8         | EPC initiated EPS Bearer Release
M8006C9         | EPC initiated EPS Bearer Release
M8006C10        | eNB initiated EPS Bearer Release
M8006C12        | Released E-RABs due to Radio Link
M8006C13        | eNB initiated EPS Bearer Release
M8006C14        | eNB initiated EPS Bearer Release
M8006C15        | eNB initiated EPS Bearer Release
M8006C17        | Initial EPS Bearer setup attempts for
M8006C18        | Initial EPS Bearer setup attempts for
M8006C26        | Additional EPS Bearer setup attempts
M8006C35        | Initial EPS Bearer setup completions
M8006C36        | Initial EPS Bearer setup completions
M8006C44        | Additional EPS Bearer setup
M8006C89        | EPC initiated EPS Bearer Release
M8006C98        | EPC initiated EPS Bearer Release
M8006C107       | EPC initiated EPS Bearer Release
M8006C116       | EPC initiated EPS Bearer Release
M8006C125       | eNB initiated EPS Bearer Release
```

```
M8006C134       | eNB initiated EPS Bearer Release
M8006C143       | eNB initiated EPS Bearer Release
M8006C152       | eNB initiated EPS Bearer Release
M8006C161       | eNB initiated EPS Bearer Release
M8006C162       | Initial EPS Bearer setup attempts for
M8006C163       | Initial EPS Bearer setup attempts for
M8006C164       | Initial EPS Bearer setup attempts for
M8006C165       | Additional EPS Bearer setup attempts
M8006C166       | Additional EPS Bearer setup attempts
M8006C167       | Additional EPS Bearer setup attempts
M8006C168       | Initial EPS Bearer setup completions
M8006C169       | Initial EPS Bearer setup completions
M8006C170       | Initial EPS Bearer setup completions
M8006C171       | Additional EPS Bearer setup
M8006C172       | Additional EPS Bearer setup
M8006C173       | Additional EPS Bearer setup
M8006C174       | Pre-empted GBR bearers
M8006C175       | Pre-empted non-GBR bearers
M8006C176       | Released active ERABs QCI1
M8006C177       | Released active ERABs QCI2
M8006C178       | Released active ERABs QCI3
M8006C179       | Released active ERABs QCI4
M8006C180       | Released active non GBR ERABs
M8006C181       | In-session activity time for QCI1
M8006C182       | In-session activity time for QCI2
M8006C183       | In-session activity time for QCI3
M8006C184       | In-session activity time for QCI4
M8006C185       | In-session activity time for non-GBR

-----------------------------------------------------------------------
Measurement Group: M8007
-----------------------------------------------------------------------
M8007C0         | Number of Data Radio Bearers
M8007C1         | Number of Data Radio Bearers
M8007C2         | Number of Data Radio Bearers failed to
M8007C3         | Number of released Data Radio
M8007C4         | Number of released Data Radio
M8007C5         | Number of released Data Radio
M8007C6         | Number of released Data Radio
M8007C7         | SRB1 setup attempts
M8007C8         | SRB1 setup completions
M8007C9         | SRB1 setup failures
M8007C10        | SRB2 setup attempts
M8007C11        | SRB2 setup completions
```

```
M8007C12        | SRB2 setup failures
M8007C13        | Radio Bearer Release requests

-------------------------------------------------------------------------
Measurement Group: M8008
-------------------------------------------------------------------------
M8008C0         | Rejected RRC Connection re-
M8008C1         | RRC Paging requests
M8008C2         | Discarded RRC Paging requests
M8008C3         | RRC Paging messages
M8008C4         | Number of RRC Connection Re-
M8008C5         | Number of successful RRC Connection
M8008C6         | RRC Connection Re-establishment
M8008C7         | RRC Connection Re-establishment
M8008C8         | RRC Connection Re-establishment
M8008C9         | RRC Connection Re-establishment
M8008C10        | Number of Report CGI Requests
M8008C11        | Number of successful CGI Reports
M8008C15        | Number of UEs attempted to redirect to
M8008C16        | Number of RRC Pagings for ETWS or

-------------------------------------------------------------------------
Measurement Group: M8009
-------------------------------------------------------------------------
M8009C0         | Total not started Handover preparations
M8009C1         | Total Handover decisions
M8009C2         | Intra eNB Handover preparations
M8009C3         | Failed Intra eNB Handover
M8009C5         | Failed Intra-eNB Handover
M8009C6         | Attempted intra eNB HO
M8009C7         | Successful intra eNB HO
M8009C8         | Total intra eNB HO failures due to timer

-------------------------------------------------------------------------
Measurement Group: M8010
-------------------------------------------------------------------------
M8010C36        | UE Reported CQI Level 00
M8010C37        | UE Reported CQI Level 01
M8010C38        | UE Reported CQI Level 02
M8010C39        | UE Reported CQI Level 03
M8010C40        | UE Reported CQI Level 04
M8010C41        | UE Reported CQI Level 05
M8010C42        | UE Reported CQI Level 06
M8010C43        | UE Reported CQI Level 07
```

```
M8010C44        | UE Reported CQI Level 08
M8010C45        | UE Reported CQI Level 09
M8010C46        | UE Reported CQI Level 10
M8010C47        | UE Reported CQI Level 11
M8010C48        | UE Reported CQI Level 12
M8010C49        | UE Reported CQI Level 13
M8010C50        | UE Reported CQI Level 14
M8010C51        | UE Reported CQI Level 15
M8010C52        | CQI offset Min
M8010C53        | CQI offset Max
M8010C54        | CQI offset Mean
M8010C55        | MIMO Open Loop Diversity Mode
M8010C56        | MIMO Open Loop Spatial Multiplexing
M8010C57        | MIMO Closed Loop Single Codeword
M8010C58        | MIMO Closed Loop Double Codeword
M8010C59        | Open Loop MIMO mode switches
M8010C60        | Closed Loop MIMO mode switches
M8010C61        | PDCCH allocations for PDSCH
M8010C62        | PDCCH allocations for PDSCH

-------------------------------------------------------------------------
Measurement Group: M8011
-------------------------------------------------------------------------
M8011C12        | UL PRB utilization per TTI Level 1
M8011C13        | UL PRB utilization per TTI Level 2
M8011C14        | UL PRB utilization per TTI Level 3
M8011C15        | UL PRB utilization per TTI Level 4
M8011C16        | UL PRB utilization per TTI Level 5
M8011C17        | UL PRB utilization per TTI Level 6
M8011C18        | UL PRB utilization per TTI Level 7
M8011C19        | UL PRB utilization per TTI Level 8
M8011C20        | UL PRB utilization per TTI Level 9
M8011C21        | UL PRB utilization per TTI Level 10
M8011C22        | UL PRB utilization per TTI Min
M8011C23        | UL PRB utilization per TTI Max
M8011C24        | UL PRB utilization per TTI Mean
M8011C25        | DL PRB utilization per TTI Level 1
M8011C26        | DL PRB utilization per TTI Level 2
M8011C27        | DL PRB utilization per TTI Level 3
M8011C28        | DL PRB utilization per TTI Level 4
M8011C29        | DL PRB utilization per TTI Level 5
M8011C30        | DL PRB utilization per TTI Level 6
M8011C31        | DL PRB utilization per TTI Level 7
M8011C32        | DL PRB utilization per TTI Level 8
```

```
M8011C33        | DL PRB utilization per TTI Level 9
M8011C34        | DL PRB utilization per TTI Level 10
M8011C35        | DL PRB utilisation per TTI Min
M8011C36        | DL PRB utilisation per TTI Max
M8011C37        | DL PRB utilisation per TTI Mean
M8011C38        | CCEs available PDCCH scheduling
M8011C39        | AGG1 used PDCCH
M8011C40        | AGG2 used PDCCH
M8011C41        | AGG4 used PDCCH
M8011C42        | AGG8 used PDCCH
M8011C43        | AGG1 blocked PDCCH
M8011C44        | AGG2 blocked PDCCH
M8011C45        | AGG4 blocked PDCCH
M8011C46        | AGG8 blocked PDCCH
M8011C47        | PRB used UL total
M8011C49        | PRB used PUCCH
M8011C50        | PRB used PUSCH
M8011C51        | PRB used DL total
M8011C54        | PRB used PDSCH
M8011C55        | Average UEs per UL TTI
M8011C56        | Max UEs per UL TTI
M8011C57        | Average UEs per DL TTI
M8011C58        | Max UEs per DL TTI
M8011C59        | Number of subframes with 1 OFDM
M8011C60        | Number of subframes with 2 OFDM
M8011C61        | Number of subframes with 3 OFDM
M8011C62        | Average number of UEs configured for
M8011C63        | Number of UL grants for TTI Bundling
M8011C64        | Short UE retention time in TTI Bundling
M8011C65        | Medium UE retention time in TTI
M8011C66        | Long UE retention time in TTI Bundling
M8011C67        | Number of SCell configuration attempts
M8011C68        | Number of successful SCell
M8011C69        | High cell load Indicator for Load

-------------------------------------------------------------------
Measurement Group: M8012
-------------------------------------------------------------------
M8012C0         | Total volume of original transmissions
M8012C1         | Total volume of correct received UL-
M8012C2         | Total volume of retransmissions of DL-
M8012C3         | Total volume of correct non-duplicate
M8012C12        | RLC data volume on DL DCCH
M8012C16        | RLC data volume on UL DCCH
```

```
M8012C17        | RLC PDU volume received
M8012C18        | RLC PDU volume transmitted
M8012C19        | PDCP SDU data volume on eUu
M8012C20        | PDCP SDU data volume on eUu
M8012C21        | PDCP Throughput UL Min
M8012C22        | PDCP Throughput UL Max
M8012C23        | PDCP Throughput UL Mean
M8012C24        | PDCP Throughput DL Min
M8012C25        | PDCP Throughput DL Max
M8012C26        | PDCP Throughput DL Mean
M8012C27        | MAC PDU volume PDSCH MCS0
M8012C28        | MAC PDU volume PDSCH MCS1
M8012C29        | MAC PDU volume PDSCH MCS2
M8012C30        | MAC PDU volume PDSCH MCS3
M8012C31        | MAC PDU volume PDSCH MCS4
M8012C32        | MAC PDU volume PDSCH MCS5
M8012C33        | MAC PDU volume PDSCH MCS6
M8012C34        | MAC PDU volume PDSCH MCS7
M8012C35        | MAC PDU volume PDSCH MCS8
M8012C36        | MAC PDU volume PDSCH MCS9
M8012C37        | MAC PDU volume PDSCH MCS10
M8012C38        | MAC PDU volume PDSCH MCS11
M8012C39        | MAC PDU volume PDSCH MCS12
M8012C40        | MAC PDU volume PDSCH MCS13
M8012C41        | MAC PDU volume PDSCH MCS14
M8012C42        | MAC PDU volume PDSCH MCS15
M8012C43        | MAC PDU volume PDSCH MCS16
M8012C44        | MAC PDU volume PDSCH MCS17
M8012C45        | MAC PDU volume PDSCH MCS18
M8012C46        | MAC PDU volume PDSCH MCS19
M8012C47        | MAC PDU volume PDSCH MCS20
M8012C48        | MAC PDU volume PUSCH MCS0
M8012C49        | MAC PDU volume PUSCH MCS1
M8012C50        | MAC PDU volume PUSCH MCS2
M8012C51        | MAC PDU volume PUSCH MCS3
M8012C52        | MAC PDU volume PUSCH MCS4
M8012C53        | MAC PDU volume PUSCH MCS5
M8012C54        | MAC PDU volume PUSCH MCS6
M8012C55        | MAC PDU volume PUSCH MCS7
M8012C56        | MAC PDU volume PUSCH MCS8
M8012C57        | MAC PDU volume PUSCH MCS9
M8012C58        | MAC PDU volume PUSCH MCS10
M8012C59        | MAC PDU volume PUSCH MCS11
M8012C60        | MAC PDU volume PUSCH MCS12
```

```
M8012C61        | MAC PDU volume PUSCH MCS13
M8012C62        | MAC PDU volume PUSCH MCS14
M8012C63        | MAC PDU volume PUSCH MCS15
M8012C64        | MAC PDU volume PUSCH MCS16
M8012C65        | MAC PDU volume PUSCH MCS17
M8012C66        | MAC PDU volume PUSCH MCS18
M8012C67        | MAC PDU volume PUSCH MCS19
M8012C68        | MAC PDU volume PUSCH MCS20
M8012C69        | MAC SDU volume on UL-CCCH
M8012C70        | MAC SDU volume on UL-DCCH
M8012C71        | MAC SDU volume on UL-DTCH
M8012C74        | MAC SDU volume on DL-CCCH
M8012C75        | MAC SDU volume on DL-DCCH
M8012C76        | MAC SDU volume on DL-DTCH
M8012C77        | RRC UL volume
M8012C78        | RRC DL volume
M8012C79        | RLC SDU UL-DTCH volume
M8012C80        | RLC SDU DL-DTCH volume
M8012C81        | MAC PDU volume PDSCH MCS21
M8012C82        | MAC PDU volume PDSCH MCS22
M8012C83        | MAC PDU volume PDSCH MCS23
M8012C84        | MAC PDU volume PDSCH MCS24
M8012C85        | MAC PDU volume PDSCH MCS25
M8012C86        | MAC PDU volume PDSCH MCS26
M8012C87        | MAC PDU volume PDSCH MCS27
M8012C88        | MAC PDU volume PDSCH MCS28
M8012C89        | Number of TTIs in UL with at least one
M8012C90        | Number of TTIs in DL with at least one
M8012C91        | IP Throughput volume in UL for QCI 1
M8012C92        | IP Throughput time in UL for QCI 1
M8012C93        | IP Throughput volume in UL for QCI 2
M8012C94        | IP Throughput time in UL for QCI 2
M8012C95        | IP Throughput volume in UL for QCI 3
M8012C96        | IP Throughput time in UL for QCI 3
M8012C97        | IP Throughput volume in UL for QCI 4
M8012C98        | IP Throughput time in UL for QCI 4
M8012C99        | IP Throughput volume in UL for QCI 5
M8012C100       | IP Throughput time in UL for QCI 5
M8012C101       | IP Throughput volume in UL for QCI 6
M8012C102       | IP Throughput time in UL for QCI 6
M8012C103       | IP Throughput volume in UL for QCI 7
M8012C104       | IP Throughput time in UL for QCI 7
M8012C105       | IP Throughput volume in UL for QCI 8
M8012C106       | IP Throughput time in UL for QCI 8
```

```
M8012C107       | IP Throughput volume in UL for QCI 9
M8012C108       | IP Throughput time in UL for QCI 9
M8012C116       | PDCP UL throughput Mean for QCI 1
M8012C117       | IP Throughput volume in DL for QCI 1
M8012C118       | IP Throughput time in DL for QCI 1
M8012C119       | IP Throughput volume in DL for QCI 2
M8012C120       | IP Throughput time in DL for QCI 2
M8012C121       | IP Throughput volume in DL for QCI 3
M8012C122       | IP Throughput time in DL for QCI 3
M8012C123       | IP Throughput volume in DL for QCI 4
M8012C124       | IP Throughput time in DL for QCI 4
M8012C125       | IP Throughput volume in DL for QCI 5
M8012C126       | IP Throughput time in DL for QCI 5
M8012C127       | IP Throughput volume in DL for QCI 6
M8012C128       | IP Throughput time in DL for QCI 6
M8012C129       | IP Throughput volume in DL for QCI 7
M8012C130       | IP Throughput time in DL for QCI 7
M8012C131       | IP Throughput volume in DL for QCI 8
M8012C132       | IP Throughput time in DL for QCI 8
M8012C133       | IP Throughput volume in DL for QCI 9
M8012C134       | IP Throughput time in DL for QCI 9
M8012C143       | PDCP DL throughput Mean for QCI 1
M8012C144       | MAC PDU volume PUSCH MCS21
M8012C145       | MAC PDU volume PUSCH MCS22
M8012C146       | MAC PDU volume PUSCH MCS23
M8012C147       | MAC PDU volume PUSCH MCS24
M8012C151       | PCell RLC data volume in DL via SCell

-----------------------------------------------------------------------
Measurement Group: M8013
-----------------------------------------------------------------------
M8013C5         | Signaling Connection Establishment
M8013C6         | Signaling Connection Establishment
M8013C7         | Signaling Connection Establishment
M8013C8         | Signaling Connection Establishment
M8013C9         | EPC initiated transitions to ECM-IDLE
M8013C10        | EPC initiated transitions to ECM-IDLE
M8013C11        | EPC initiated transitions to ECM-IDLE
M8013C12        | EPC initiated transitions to ECM-IDLE
M8013C13        | eNB initiated transitions to ECM-IDLE
M8013C15        | eNB initiated transitions to ECM-IDLE
M8013C16        | eNB initiated transitions to ECM-IDLE
M8013C17        | Signaling Connection Establishment
M8013C18        | Signaling Connection Establishment
```

```
M8013C19        | Signaling Connection Establishment
M8013C20        | Signaling Connection Establishment
M8013C21        | Number of Signaling Connection
M8013C24        | Subframes of DRX Active UE
M8013C25        | Subframes of DRX Sleep UE
M8013C26        | Signaling Connection Establishment
M8013C27        | Signaling Connection Establishment
M8013C28        | Pre-empted UE contexts due to pre-

-------------------------------------------------------------------------
Measurement Group: M8014
-------------------------------------------------------------------------
M8014C0         | Inter eNB Handover preparations
M8014C2         | Failed Inter eNB Handover
M8014C3         | Failed Inter eNB Handover
M8014C5         | Failed Inter-eNB Handover
M8014C6         | Attempted inter eNB HO
M8014C7         | Successful inter eNB HO
M8014C8         | Number of Inter eNB Handover failures
M8014C14        | Inter eNB S1-Handover preparations
M8014C15        | Failed Inter eNB S1-Handover
M8014C16        | Failed Inter eNB S1-Handover
M8014C17        | Failed Inter-eNB S1-Handover
M8014C18        | Attempted inter eNB S1-HO
M8014C19        | Successful inter eNB S1-HO
M8014C20        | Inter eNB S1-HO failures due to timer

-------------------------------------------------------------------------
Measurement Group: M8015
-------------------------------------------------------------------------
M8015C0         | Failed Intra eNB HO preparations per
M8015C1         | Intra eNB HO attempts per neighbor
M8015C2         | Intra eNB HO successes per neighbor
M8015C5         | Number of failed Inter eNB Handover
M8015C6         | Failed Inter eNB Handover
M8015C7         | Failed Inter eNB Handover
M8015C8         | Number of Inter eNB Handover
M8015C9         | Number of successful Inter eNB
M8015C10        | Number of Inter eNB Handover failures
M8015C15        | Intra eNB HO failures per neighbor cell
M8015C16        | Number of Late Handover per neighbor
M8015C17        | Number of Early Handover Type1 per
M8015C18        | Number of Early Handover Type2 per
```

```
-------------------------------------------------------------------------
Measurement Group: M8016
-------------------------------------------------------------------------
M8016C11        | CS Fallback attempts with redirection
M8016C12        | CS Fallback attempts (UE in
M8016C13        | CS Fallback attempts for emergency
M8016C14        | Inter System Handover preparations
M8016C15        | Failed Inter System Handover
M8016C16        | Failed Inter System Handover
M8016C17        | Failed Inter-System Handover
M8016C21        | Inter System Handover attempts
M8016C23        | Successful Inter System Handover
M8016C25        | Failed Inter System Handover attempts
M8016C26        | Number of NACC from LTE to GSM
M8016C29        | Inter System Handover attempts to
M8016C30        | Successful Inter System Handover
M8016C31        | Failed Inter System Handover attempts
M8016C32        | CS Fallback attempts to UTRAN with
M8016C33        | Inter System Handover attempts to
M8016C34        | Successful Inter System Handover
M8016C35        | Failed Inter System Handover attempts

-------------------------------------------------------------------------
Measurement Group: M8017
-------------------------------------------------------------------------
M8017C4         | Failed Inter System Handover
M8017C5         | Failed Inter System Handover
M8017C6         | Failed Inter System Handover
M8017C7         | Inter System Handover attempts to
M8017C8         | Successful Inter System Handover
M8017C9         | Failed Inter System Handover attempts
M8017C10        | Inter System Handover preparations
M8017C11        | Inter System Handover attempts to
M8017C12        | Successful Inter System Handover
M8017C13        | Failed Inter System Handover attempts

-------------------------------------------------------------------------
Measurement Group: M8018
-------------------------------------------------------------------------
M8018C0         | Active UE per eNB average
M8018C1         | Active UE per eNB max
M8018C4         | UE Contexts released due to S1 Reset
M8018C5         | Active UE Contexts released due to S1
M8018C6         | UE Contexts released due to S1 Reset
```

```
M8018C7         | Active UE Contexts released due to S1
M8018C8         | Sum of Active UEs per eNB
M8018C9         | Denominator for Active UEs per eNB

-----------------------------------------------------------------------
Measurement Group: M8019
-----------------------------------------------------------------------
M8019C0         | Number of NACC from LTE to GSM
M8019C3         | Inter System Handover attempts to
M8019C4         | Successful Inter System Handover
M8019C5         | Failed Inter System Handover attempts

-----------------------------------------------------------------------
Measurement Group: M8020
-----------------------------------------------------------------------
M8020C0         | Number of cell state changes to "cell is
M8020C1         | Number of cell state changes to "cell is
M8020C2         | Number of cell state changes to "cell is
M8020C3         | Samples when the cell is available
M8020C4         | Samples when the cell is planned
M8020C5         | Samples when the cell is unplanned
M8020C6         | Cell availability denominator

-----------------------------------------------------------------------
Measurement Group: M8021
-----------------------------------------------------------------------
M8021C0         | Number of inter frequency Handover
M8021C1         | Number of inter frequency Handover
M8021C2         | Number of successful inter-frequency
M8021C3         | Number of successful inter-frequency
M8021C4         | Number of Handover failures per cause
M8021C5         | Number of Handover failures per cause
M8021C6         | Handover preparations for IMS
M8021C9         | Failed Handover preparations for IMS
M8021C12        | Handover attempts for IMS emergency
M8021C15        | Successful Handover completions for
M8021C18        | Number of Handover attempts for UEs
M8021C19        | Number of Handover completions for
M8021C20        | Number of Late Handover
M8021C21        | Number of Early Handover Type1
M8021C22        | Number of Early Handover Type2
M8021C23        | Number of load balancing Handover
M8021C24        | Number of successful load balancing
```

```
-------------------------------------------------------------------------
Measurement Group: M8022
-------------------------------------------------------------------------
M8022C0         | Number of X2 Setup attempts
M8022C1         | Number of failed X2 Setup attempts

-------------------------------------------------------------------------
Measurement Group: M8023
-------------------------------------------------------------------------
M8023C0         | PDCP SDU data volume on eUu
M8023C1         | PDCP SDU data volume on eUu
M8023C2         | PDCP SDU data volume on eUu
M8023C3         | PDCP SDU data volume on eUu
M8023C4         | PDCP SDU data volume on eUu
M8023C5         | PDCP SDU data volume on eUu
M8023C6         | PDCP SDU data volume on eUu
M8023C7         | PDCP SDU data volume on eUu
M8023C8         | PDCP SDU data volume on eUu
M8023C9         | PDCP SDU data volume on eUu
M8023C10        | PDCP SDU data volume on eUu
M8023C11        | PDCP SDU data volume on eUu
M8023C12        | Average Number of active UE of
M8023C13        | Average Number of active UE of
M8023C14        | Average Number of active UE of
M8023C15        | Average Number of active UE of
M8023C16        | Average Number of active UE of
M8023C17        | Average Number of active UE of
M8023C18        | Average Number of active UE of
M8023C19        | Average Number of active UE of
M8023C20        | Average Number of active UE of
M8023C21        | Average number of active UEs of QCI
M8023C22        | Average number of active UEs of QCI
M8023C23        | Average number of active UEs of QCI
M8023C24        | Average number of active UEs of QCI
M8023C25        | Average number of active UEs of QCI
M8023C26        | Average number of active UEs of QCI
M8023C27        | Number of QCI Counter Group
M8023C28        | Average number of active UEs of
M8023C29        | Average number of active UEs of
M8023C30        | Average number of active UEs of
M8023C31        | Average number of active UEs of
M8023C32        | Average number of active UEs of
M8023C33        | Average number of active UEs of
M8023C34        | Average number of active UEs of
```

```
M8023C35        | Average number of active UEs of

-------------------------------------------------------------------------
Measurement Group: M5112
-------------------------------------------------------------------------
M51120C0        | ifInPackets15
M51120C1        | ifInOctets15
M51120C2        | ifOutPackets15
M51120C3        | ifOutOctets15
M51120C4        | ifInErrors15
M51120C5        | ifOutDroppedPackets
M51120C6        | ifOutDroppedOctets
M51121C0        | ifOctets_EF
M51121C1        | ifPackets_EF
M51121C2        | ifDroppedOctets_EF
M51121C3        | ifDroppedPackets_EF
M51121C4        | ifOctets_AF4
M51121C5        | ifPackets_AF4
M51121C6        | ifDroppedOctets_AF4
M51121C7        | ifDroppedPackets_AF4
M51121C8        | ifOctets_AF3
M51121C9        | ifPackets_AF3
M51121C10       | ifDroppedOctets_AF3
M51121C11       | ifDroppedPackets_AF3
M51121C12       | ifOctets_AF2
M51121C13       | ifPackets_AF2
M51121C14       | ifDroppedOctets_AF2
M51121C15       | ifDroppedPackets_AF2
M51121C16       | ifOctets_AF1
M51121C17       | ifPackets_AF1
M51121C18       | ifDroppedOctets_AF1
M51121C19       | ifDroppedPackets_AF1
M51121C20       | ifOctets_BE
M51121C21       | ifPackets_BE
M51121C22       | ifDroppedOctets_BE
M51121C23       | ifDroppedPackets_BE
M51121C24       | ifRxOctets_EF
M51121C25       | ifRxPackets_EF
M51121C26       | ifRxOctets_AF4
M51121C27       | ifRxPackets_AF4
M51121C28       | ifRxOctets_AF3
M51121C29       | ifRxPackets_AF3
M51121C30       | ifRxOctets_AF2
M51121C31       | ifRxPackets_AF2
```

M51121C32	ifRxOctets_AF1
M51121C33	ifRxPackets_AF1
M51121C34	ifRxOctets_BE
M51121C35	ifRxPackets_BE
M51123C0	EthIfInOcts_15
M51123C1	EthIfOutOcts_15
M51123C2	EthIfInPkt_15
M51123C3	EthIfOutPkt_15
M51123C4	EthIfInPktErr_15
M51123C8	EthIfInDiscRateLimiting
M51123C16	ethIfInVlanMismatch
M51123C17	ethIfOutDiscShaping_Q5
M51123C18	ethIfOutDiscShaping_Q4
M51123C19	ethIfOutDiscShaping_Q3
M51123C20	ethIfOutDiscShaping_Q2
M51123C21	ethIfOutDiscShaping_Q1
M51123C22	ethIfOutDiscShaping_Q6
M51123C23	EthIfInBlocksDiscRateLimiting
M51125C0	Protected_ESPFramesTx
M51125C1	Protected_ESPFramesRx
M51125C2	Discarded_ESPFramesTx
M51125C3	Discarded_ESPFramesRx
M51125C4	Bypassed_FramesTx
M51125C5	Bypassed_FramesRx
M51126C0	ipRmDroppedPacketsRateLimiting
M51126C1	ipRmDroppedPacketsFiltering
M51127C0	ifInPackets15
M51127C1	ifInOctets15
M51127C2	ifOutPackets15
M51127C3	ifOutOctets15
M51127C4	ifInErrors15
M51127C5	ifOutDroppedPackets
M51127C6	ifOutDroppedOctets
M51128C0	ifOctets_EF
M51128C1	ifPackets_EF
M51128C2	ifDroppedOctets_EF
M51128C3	ifDroppedPackets_EF
M51128C4	ifOctets_AF4
M51128C5	ifPackets_AF4
M51128C6	ifDroppedOctets_AF4
M51128C7	ifDroppedPackets_AF4
M51128C8	ifOctets_AF3
M51128C9	ifPackets_AF3
M51128C10	ifDroppedOctets_AF3

```
M51128C11       | ifDroppedPackets_AF3
M51128C12       | ifOctets_AF2
M51128C13       | ifPackets_AF2
M51128C14       | ifDroppedOctets_AF2
M51128C15       | ifDroppedPackets_AF2
M51128C16       | ifOctets_AF1
M51128C17       | ifPackets_AF1
M51128C18       | ifDroppedOctets_AF1
M51128C19       | ifDroppedPackets_AF1
M51128C20       | ifOctets_BE
M51128C21       | ifPackets_BE
M51128C22       | ifDroppedOctets_BE
M51128C23       | ifDroppedPackets_BE
M51128C24       | ifRxOctets_EF
M51128C25       | ifRxPackets_EF
M51128C26       | ifRxOctets_AF4
M51128C27       | ifRxPackets_AF4
M51128C28       | ifRxOctets_AF3
M51128C29       | ifRxPackets_AF3
M51128C30       | ifRxOctets_AF2
M51128C31       | ifRxPackets_AF2
M51128C32       | ifRxOctets_AF1
M51128C33       | ifRxPackets_AF1
M51128C34       | ifRxOctets_BE
M51128C35       | ifRxPackets_BE
M51129C0        | rxEthernetPackets
M51129C1        | rxEhernetOctets
M51129C2        | txEthernetPackets
M51129C3        | txEthernetOctets

-------------------------------------------------------------------------
Measurement Group: M5113
-------------------------------------------------------------------------
M51130C0        | rxEthernetPackets
M51130C1        | rxEhernetOctets
M51130C2        | txEthernetPackets
M51130C3        | txEthernetOctets
M51130C4        | EthIfInUnknownVLAN_15
M51131C0        | ethIfOutDiscShaping
M51132C0        | avgRTT_15Min
M51132C1        | maxRTT_15Min
M51132C2        | minRTT_15Min
M51132C3        | lostTwampMessages
M51132C4        | txTwampMessages
```

```
M51136C0        | tacSuccessfulGbrNormal
M51136C1        | tacSuccessfulGbrHandover
M51136C2        | tacSuccessfulGbrEmergency
M51136C3        | tacRejectedGbrNormal
M51136C4        | tacRejectedGbrHandover
M51136C5        | tacRejectedGbrEmergency
M51137C0        | topRxFreqSyncMsg
M51137C1        | topMinFreqSyncError
M51137C2        | topAvgFreqSyncError
M51137C3        | topMaxFreqSyncError
```

Documentation Connexe

- **Intégration Grafana** - Création de tableaux de bord en utilisant ces compteurs
- **Politique de Conservation des Données** - Gestion du cycle de vie des données des compteurs
- **Guide de Configuration à l'Exécution** - Configuration des intervalles de collecte de données
- **Configuration AirScale** - Configuration et enregistrement de la station de base

Collection OCUDU

Métriques en direct pour les gNB OCUDU 5G via le WebSocket de télécommande

Le RAN Monitor collecte des métriques en direct des gNB **OCUDU**. OCUDU est le logiciel CU/DU (gNB) open source de la Linux Foundation OCUDU Ecosystem Foundation. Il a commencé comme un fork de srsRAN. Le RAN Monitor prend en charge OCUDU ainsi que Nokia, Casa, Baicells et Flexi Zone.

Retour au Guide des opérations.

Table des matières

1. Aperçu
2. Architecture
3. Prérequis gNB
4. Configuration
5. Données collectées
6. Métriques Prometheus
7. Données InfluxDB
8. Page d'état et API
9. Sécurité
10. Dépannage

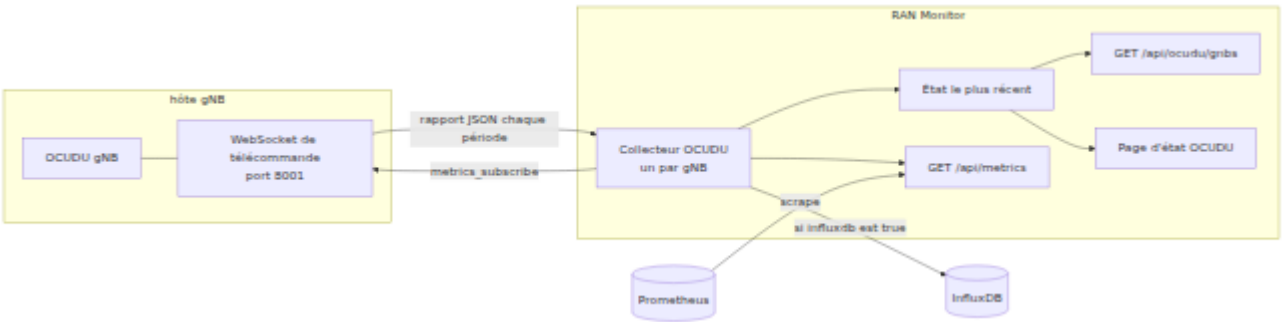
Aperçu

Un gNB OCUDU n'a pas d'interface de gestion SNMP, NETCONF ou REST. Son canal de gestion est le **WebSocket de télécommande** (RFC 6455). Lorsqu'un client s'abonne, le gNB envoie un rapport de métriques JSON à chaque période de rapport.

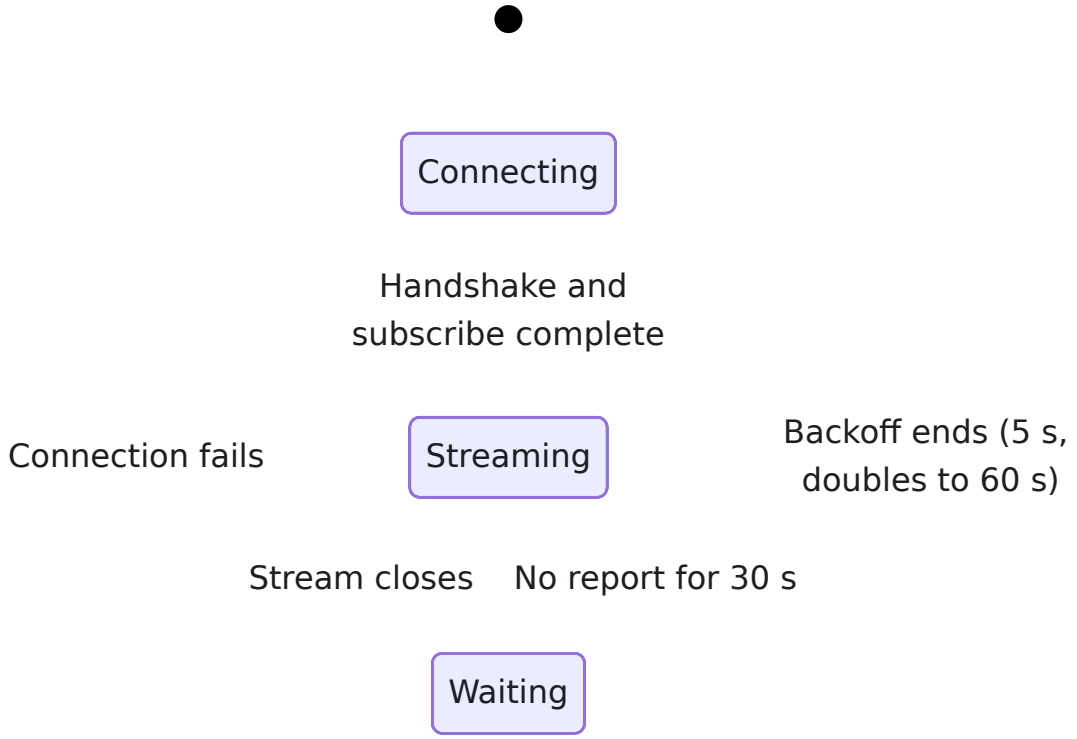
Le RAN Monitor maintient une connexion WebSocket ouverte vers chaque gNB configuré. Il s'abonne à la diffusion de métriques et n'envoie pas d'autres commandes.

Élément	Valeur
Mécanisme	Flux. Le RAN Monitor se connecte à `ws://<host>:<ws_port>` et envoie `metrics_subscribe`.
Taux de rapport	Le paramètre gNB `metrics.periodicity.du_report_period` (généralement 1 s).
Prometheus	`ocudu_metric`, `ocudu_connected` et `ocudu_last_report_timestamp_seconds` sur `GET /api/metrics`.
InfluxDB	Mesure `OcuduPerformanceMetrics`, uniquement si `influxdb` est `true`.
Commandes envoyées	`metrics_subscribe` uniquement.
Direction	Le RAN Monitor se connecte au gNB sur le port TCP `ws_port` (généralement 8001).

Architecture



Le collecteur pour chaque gNB passe par ces états :



- Lorsque le flux s'arrête, le RAN Monitor définit `ocudu_connected` à `0`.
- En même temps, il supprime la série Prometheus de ce gNB et efface les données du gNB sur la page d'état.
- Lorsqu'un rapport arrive, le backoff revient à 5 s.
- La vérification de 30 s trouve un gNB qui maintient la connexion TCP ouverte mais n'envoie aucun rapport.

Prérequis gNB

La configuration YAML du gNB doit activer la diffusion des métriques JSON et le serveur de télécommande. L'adresse `bind_addr` doit être une adresse que le RAN Monitor peut atteindre.

```yaml
metrics:
  enable_json: true
  layers:
    enable_sched: true
    enable_mac: true
    enable_ru: true
  periodicity:
    du_report_period: 1000

remote_control:
  enabled: true
  bind_addr: 172.29.5.227
  port: 8001
```

Paramètre	Type	Requis	Par défaut
`metrics.enable_json`	Booléen	Oui	`false`
`metrics.layers.enable_sched`	Booléen	Oui	`false`
`metrics.layers.enable_mac`	Booléen	Non	`false`
`metrics.layers.enable_ru`	Booléen	Non	`false`
`metrics.periodicity.du_report_period`	Entier	Non	`1000`
`remote_control.enabled`	Booléen	Oui	`false`

Paramètre	Type	Requis	Par défaut
`remote_control.bind_addr`	Chaîne	Oui	`127.0.0.1`
`remote_control.port`	Entier	Oui	`8001`

Un changement de ces paramètres prend effet uniquement après un redémarrage du gNB. Un redémarrage du gNB fait tomber la cellule.

Le RAN Monitor accepte également les autres couches de métriques OCUDU, par exemple `enable_ngap`, `enable_rrc`, `enable_pdcp` et `enable_app_usage`. Chaque champ numérique dans chaque rapport devient un compteur. Vous n'avez pas besoin de modifier le RAN Monitor lorsque vous activez une couche.

Configuration

Ajoutez la section `ocudu` à `config :ran_monitor` dans la configuration d'exécution.

```
ocudu: %{
  influxdb: false,
  gnbs: [
    %{name: "ocudu-gnb-riverside", host: "172.29.5.227", ws_port:
8001}
  ]
}
```

Paramètre	Type	Requis	Par défaut	Description
`influxdb`	Booléen	Oui	`false`	Si `true`, le RAN Monitor écrit également chaque échantillon dans InfluxDB sous `OcuduPerformanceMetrics`, par lots toutes les 10 s. L'exportation Prometheus est toujours activée.
`gnbs`	Liste	Oui	`[]`	Les gNB à surveiller. Voir Paramètres gNB.

Paramètres gNB

Paramètre	Type	Requis	Par défaut	Description
`name`	Chaîne	Oui	-	Nom du gNB. Le RAN Monitor l'utilise dans l'étiquette `gnb`, sur la page d'état et dans le chemin API. Chaque nom doit être unique.
`host`	Chaîne	Oui	-	Adresse IP ou nom d'hôte de l'hôte gNB. Cela doit être l'adresse dans `remote_control.bind_addr`, ou une adresse qui y achemine.
`ws_port`	Entier	Oui	-	Port du serveur de télécommande. Il doit être égal à `remote_control.port` sur le gNB.

Si une entrée gNB n'a pas un paramètre requis, le RAN Monitor ne démarre pas. Le message d'erreur indique le nom du gNB et le paramètre manquant.

Données collectées

Le RAN Monitor convertit chaque rapport JSON en échantillons. Chaque échantillon a un **scope**, un nom de **compteur** et une identité de cellule (PCI) et d'UE (RNTI) où ils s'appliquent.

Scope	Source dans le rapport	Identité	Contenu
`cell`	`cells[].cell_metrics`	`pci`	Compteurs du planificateur : Msg3 ok/nok, indications d'erreur, allocations PDCCH et UCI échouées, HARQs tardifs, latence du planificateur, utilisation de PUCCH.
`cell`	Calculé à partir de `cells[].ue_list`	`pci`	`nof_ues`, `dl_brate` et `ul_brate` : le nombre d'UE et la somme des d��bits binaires des UE.
`ue`	`cells[].ue_list[]`	`pci`, `rnti`	CQI, rang, MCS, débit binaire, HARQ ok/nok, SNR PUCCH, RSRP PUSCH, avance de synchronisation, BSR, PHR, délais.
`du`	`du.du_high.mac`	`pci`	Latence MAC et utilisation CPU.
`ru`	`ru.ofh`	`pci` où par cellule	Fronthaul : paquets en avance, à temps et en retard, messages perdus, erreurs de séquence eCPRI, débit, latence par étape.
Autre	`cu-cp`, `cu-up`, `app_resource_usage` et plus	Comme dans le rapport	Tous les champs numériques des couches que le gNB envoie.

- Le nom du compteur est le chemin du champ dans le rapport, avec des points entre les parties. Par exemple, `ofh.cells.ul.received_packets.late`.
- Le RAN Monitor ignore les listes de nombres, par exemple les histogrammes de latence.
- Le RNTI a le même format que sur la console gNB, par exemple `0x4603`.

Les termes NR 5G dans le tableau sont définis dans ces spécifications :

- CQI et rang : 3GPP TS 38.214.
- PUCCH, PUSCH et avance de synchronisation : 3GPP TS 38.213.
- BSR et PHR : 3GPP TS 38.321.

Métriques Prometheus

Le RAN Monitor sert les métriques à `GET /api/metrics`, avec ses autres métriques Prometheus.

Métrique : `ocudu_metric` **Type** : Jauge **Description** : La dernière valeur d'un échantillon OCUDU. **Étiquettes** :

- `gnb` - Le `nom` du gNB dans la configuration du RAN Monitor.
- `scope` - `cell`, `ue`, `du`, `ru` ou le nom d'un autre rapport.
- `pci` - ID de cellule physique. Vide si l'échantillon n'est pas pour une cellule.
- `rnti` - RNTI UE. Vide si l'échantillon n'est pas pour un UE.
- `counter` - Nom du compteur. Voir Données collectées.

Lorsqu'un UE quitte la cellule, le RAN Monitor supprime sa série. Lorsque le flux s'arrête, le RAN Monitor supprime toutes les séries de ce gNB.

Métrique : `ocudu_connected` **Type** : Jauge **Description** : `1` si le flux de métriques du gNB est actif. `0` s'il est inactif. **Étiquettes** :

- `gnb` - Le `nom` du gNB.

Métrique : `ocudu_last_report_timestamp_seconds` **Type** : Jauge **Description** : Temps Unix du dernier rapport du gNB. **Étiquettes** :

- `gnb` - Le `nom` du gNB.

Exemples de requêtes :

```
# UEs attachés par cellule
ocudu_metric{scope="cell", counter="nof_ues"}

# CQI par UE
ocudu_metric{scope="ue", counter="cqi"}

# Débit descendant de cellule en Mbit/s
ocudu_metric{scope="cell", counter="dl_brate"} / 1e6

# Paquets de fronthaul uplink en retard par rapport
ocudu_metric{scope="ru",
counter="ofh.cells.ul.received_packets.late"}

# gNBs sans rapport depuis plus de 60 s
time() - ocudu_last_report_timestamp_seconds > 60
```

Exemples d'alerte :

```
- alert: OcuduStreamDown
  expr: ocudu_connected == 0
  for: 2m
  labels:
    severity: major
  annotations:
    summary: "Pas de métriques de OCUDU gNB {{ $labels.gnb }}"

- alert: OcuduNoUEs
  expr: ocudu_metric{scope="cell", counter="nof_ues"} == 0
  for: 15m
  labels:
    severity: minor
  annotations:
    summary: "Pas d'UEs sur {{ $labels.gnb }} PCI {{ $labels.pci
}}"
```

Paramètre	Description
`alert`	Nom de la règle d'alerte.
`expr`	Condition PromQL qui déclenche l'alerte.
`for`	Temps que la condition doit rester vraie avant que l'alerte ne se déclenche.
`labels.severity`	Étiquette de gravité pour le routage dans Alertmanager.
`annotations.summary`	Texte de l'alerte.

Données InfluxDB

Si `influxdb` est `true`, le RAN Monitor écrit un point pour chaque échantillon dans la base de données InfluxDB configurée. Le format est le même que pour

les autres fournisseurs : un point pour chaque compteur, avec la valeur dans `counterValue`.

Élément	Valeur
Mesure	`OcuduPerformanceMetrics`
Champ	`counterValue` (flottant)
Étiquettes	`gnbName`, `host`, `vendor` (`OCUDU`), `recordType` (`performanceMetric`), `metricScope`, `metricCounter`, `pci`, `rnti`
Intervalle d'écriture	Toutes les 10 s, en un lot pour chaque gNB

Avec un rapport chaque seconde, une cellule avec 4 UEs génère environ 1 000 points dans chaque lot de 10 s.

Page d'état et API

La page **État OCUDU** (`/ocudu/status`) montre chaque gNB configuré :

- L'état du flux, l'adresse et l'heure du dernier rapport.
- Les compteurs du planificateur pour chaque cellule.
- Les compteurs de fronthaul pour chaque cellule.
- Un tableau avec une ligne pour chaque UE. Il a les mêmes valeurs que les métriques de la console gNB.

La page d'état OCUDU. Le gNB en direct `ocudu-gnb-riverside` montre ses compteurs de fronthaul et un UE attaché.

Les mêmes données sont disponibles au format JSON :

Requête	Résultat
`GET /api/ocudu/gnbs`	Tous les gNB configurés avec leur état de flux, cellules, UEs et autres compteurs.
`GET /api/ocudu/gnbs/{name}`	Un gNB. Si le nom n'est pas configuré, le résultat est `404` avec le code `GNB_NOT_FOUND`.

Sécurité

Ne pas ouvrir le port de télécommande à des réseaux que vous ne contrôlez pas. Le serveur de télécommande OCUDU n'a pas d'authentification et pas de TLS. Un client qui peut se connecter peut également envoyer des commandes. Le RAN Monitor envoie uniquement `metrics_subscribe`, mais d'autres clients peuvent envoyer n'importe quelle commande.

Commande	Effet
`quit`	Arrête le gNB.
`ssb_set`	Change la puissance du bloc SSB.
`rrm_policy_ratio_set`	Change le quota PRB d'une tranche.

Ne pas envoyer `ssb_set` ou `rrm_policy_ratio_set` à un gNB que le RAN Monitor surveille.

- Le serveur utilise un seul thread. Ces deux commandes arrêtent ce thread jusqu'à ce que le DU termine le changement, et il n'y a pas de délai d'attente.
- Si le DU ne termine pas le changement, le serveur arrête tout travail. Il n'accepte pas de nouvelles connexions et n'envoie pas de métriques.
- Seul un redémarrage du gNB efface cette condition.

Ce problème se produit avec le commit OCUDU `e1f308a`.

Dépannage

Le flux ne se connecte pas

Symptômes : `ocudu_connected` est `0`. La page d'état affiche `:econnrefused`.

Causes possibles :

- Le serveur de télécommande n'est pas activé sur le gNB.
- `remote_control.bind_addr` est `127.0.0.1`.
- `ws_port` dans le RAN Monitor n'est pas égal à `remote_control.port` sur le gNB.
- Le gNB n'est pas en cours d'exécution.

Résolution :

1. Assurez-vous que `remote_control.enabled` est `true` sur le gNB.
2. Assurez-vous que `remote_control.bind_addr` est une adresse que le RAN Monitor peut atteindre.
3. Assurez-vous que `ws_port` est égal à `remote_control.port`.
4. Assurez-vous que le service gNB est en cours d'exécution.

Le flux expire

Symptômes : La page d'état affiche `:timeout`, `:ehostunreach` ou `{:handshake, :timeout}`.

Causes possibles :

- Il n'y a pas de route du RAN Monitor vers l'hôte gNB.
- Le serveur de télécommande du gNB est bloqué. Voir Sécurité.

Résolution :

1. Assurez-vous que le RAN Monitor peut atteindre `host` sur `ws_port`.
2. Si la connexion TCP s'ouvre mais que le handshake expire, le serveur est bloqué. Redémarrez le gNB.

Pas de métriques pendant 30 s

Symptômes : Le journal du collecteur affiche `no metrics for 30s`. `ocudu_connected` change à `0` puis revient à `1` plusieurs fois.

Causes possibles :

- Le gNB a redémarré.

- `metrics.periodicity.du_report_period` est supérieur à 30000 ms.
- Le serveur de télécommande est bloqué. Voir Sécurité.

Résolution :

1. Assurez-vous que `du_report_period` est inférieur à 30000 ms.
2. Examinez le journal du service gNB pour un redémarrage.
3. Si le serveur est bloqué, redémarrez le gNB.

Connecté mais pas de lignes UE

Symptômes : `ocudu_connected` est `1`, mais la page d'état n'affiche pas de cellules ou pas d'UEs.

Causes possibles :

- `metrics.layers.enable_sched` est `false` sur le gNB.
- Aucun UE n'est attaché.

Résolution :

1. Assurez-vous que `metrics.layers.enable_sched` est `true` sur le gNB.
2. Examinez `ocudu_metric{scope="cell", counter="nof_ues"}`. Si la valeur est `0`, aucun UE n'est attaché.

Guide de Collecte de Données PM

> Cette page couvre le pipeline PM de **Nokia** et sa page "Filtres de Données". Pour les femtocells **Casa**, voir Collecte PM Casa — elle a son propre point de terminaison d'ingestion, sa page "Filtres de Données Casa" et sa page "Statut Casa".

Aperçu

La page de Collecte de Données PM vous permet de gérer quels compteurs de Métriques de Performance (PM) sont stockés dans InfluxDB. Les stations de base Nokia AirScale rapportent plus de **22 000 compteurs PM uniques**, mais les stocker tous n'est ni pratique ni nécessaire pour la plupart des cas d'utilisation.

Ce guide explique comment sélectionner quels compteurs collecter en fonction de vos besoins de surveillance.

Démarrage Rapide

Accéder à la Page de Collecte de Données PM

1. Naviguez vers le Panneau de Contrôle : `https://localhost:9443`
2. Cliquez sur **Filtres de Données** dans le menu de navigation
3. Affichez et gérez les paramètres de collecte des compteurs PM

Comprendre l'Interface

La page est divisée en deux sections principales :

Section	Description
Données PM Stockées (Gauche)	Compteurs actuellement collectés et stockés dans InfluxDB
Compteurs Disponibles (Droite)	Tous les 22 000+ compteurs disponibles à ajouter à votre collecte

---

Catégories de Compteurs

Les compteurs PM sont catégorisés par leur préfixe de code, qui indique la technologie et la fonction :

Catégorie	Préfixe de Code	Nombre	Description
LTE	M8xxx	~5 900	Compteurs LTE L1/L2/L3 (ERAB, RRC, transfert, etc.)
WCDMA	M5xxx	~885	Compteurs 3G WCDMA (couche MAC, CQI, HSDPA)
5G-NR	M55xxx	~14 500	Compteurs 5G NR (MIMO massif, formation de faisceaux, etc.)
5G-Mobilité	M51xxx	~500	Mobilité et mesures 5G
5G-Commun	M40xxx	~250	Compteurs 5G communs/partagés

Compteurs par Défaut

Au premier démarrage, des valeurs par défaut sensées sont chargées depuis `priv/pm_counters.csv`. Ces valeurs par défaut comprennent des compteurs essentiels pour :

- **Énergie** : Surveillance de la consommation d'énergie
- **Volume de Données** : Métriques de volume de trafic
- **Disponibilité** : Statistiques de disponibilité des cellules
- **Accessibilité** : Succès/échec de la connexion RRC
- **PRB** : Utilisation du Bloc de Ressources Physiques
- **Débit** : Métriques de débit UL/DL
- **RRC** : Statistiques de connexion RRC
- **ERAB** : Compteurs de configuration et de libération E-RAB
- **PDCP** : Métriques de couche PDCP
- **Transfert** : Statistiques de transfert inter-cellulaire
- **Interférence** : Mesures d'interférence UL

Gestion des Compteurs

Ajouter des Compteurs

1. Utilisez la **zone de recherche** ou le **filtre de catégorie** dans la section "Compteurs Disponibles"
2. Cliquez sur les lignes pour sélectionner des compteurs (la case à cocher apparaîtra cochée)
3. Utilisez **Tout Sélectionner** pour sélectionner tous les compteurs visibles
4. Cliquez sur **Ajouter Sélectionnés** pour les déplacer vers la collection stockée

Supprimer des Compteurs

1. Dans la section "Données PM Stockées", sélectionnez les compteurs à supprimer
2. Cliquez sur **Supprimer Sélectionnés** pour arrêter la collecte de ces compteurs

Filtrer et Rechercher

Les deux sections prennent en charge :

- **Recherche textuelle** : Filtrer par ID de compteur ou description
- **Filtre de catégorie** : Afficher uniquement les compteurs d'une catégorie spécifique (LTE, 5G-NR, etc.)

Réinitialiser aux Valeurs par Défaut

Cliquez sur **Réinitialiser aux Valeurs par Défaut** pour restaurer la liste originale des compteurs depuis `priv/pm_counters.csv`. Cela supprimera toutes les ajouts personnalisés.

Persistance

Les modifications de votre sélection de compteurs PM sont :

1. **Persistées sur disque** dans `priv/pm_filters.etf`
2. **Survivent aux redémarrages de l'application**
3. **Prennent effet immédiatement** (aucun redémarrage requis)

Le rédacteur de lots InfluxDB est informé des modifications et commence/arrête immédiatement de collecter les compteurs affectés.

Considérations de Stockage

Pourquoi Ne Pas Tout Collecter ?

Collecter tous les 22 000+ compteurs entraînerait :

Scénario	Impact
Stockage	~100-500 Go/mois par site (selon l'intervalle de collecte)
Charge d'Écriture	Pression d'écriture significative sur InfluxDB
Performance de Requête	Requêtes de tableau de bord plus lentes en raison du volume de données
Coût	Coûts de stockage et de calcul plus élevés

Approche Recommandée

1. **Commencez avec les valeurs par défaut** : Les compteurs préconfigurés couvrent la plupart des besoins de surveillance courants
2. **Ajoutez au besoin** : Lors de la création de nouveaux tableaux de bord, ajoutez des compteurs spécifiques dont vous avez besoin
3. **Révisez périodiquement** : Supprimez les compteurs qui ne sont plus utilisés

---

Référence de Compteurs

Trouver des Descriptions de Compteurs

La section "Compteurs Disponibles" montre la description officielle de Nokia pour chaque compteur. Utilisez la fonction de recherche pour trouver des

compteurs par :

- **ID de Compteur** (par exemple, `M8012C23`)
- **Mots-clés de Description** (par exemple, `débit`, `transfert`, `RSRP`)

Exemples Courants de Compteurs

Compteur	Catégorie	Description
M8012C23	LTE	Débit UL moyen par cellule
M8012C26	LTE	Débit DL moyen par cellule
M8001C2	LTE	Délai moyen SDU PDCP DL
M8011C24	LTE	Utilisation PRB UL
M8011C37	LTE	Utilisation PRB DL
M8013C17	LTE	Utilisateurs connectés RRC
M8020C3	LTE	Succès de transfert
M40001C0	5G	Consommation d'énergie

Fichiers de Configuration

pm_counters.csv

Compteurs par défaut chargés au premier démarrage :

```
# Format : compteur,catégorie,description
M8012C23,Débit,Débit montant moyen
M8012C26,Débit,Débit descendant moyen
M8001C2,Disponibilité,Disponibilité de la cellule
...
```

Emplacement : `priv/pm_counters.csv`

pm_metrics.csv

Référence complète de tous les compteurs disponibles :

```
# Format : PM_Code,Catégorie,Description
M8000C6,LTE,S1_SETUP_ATT
M8000C7,LTE,S1_SETUP_SUCC
...
```

Emplacement : `priv/pm_metrics.csv`

Dépannage

Compteurs Non Collectés

1. Vérifiez que le compteur est dans "Données PM Stockées" (côté gauche)
2. Vérifiez que l'eNodeB pousse les données PM (voir la page d'état InfluxDB)
3. Vérifiez que l'ID du compteur correspond exactement (sensible à la casse)

Changements Non Pris en Compte

1. Les changements de filtre sont appliqués immédiatement au rédacteur de lots
2. **Les nouvelles données n'apparaissent qu'après la prochaine poussée PM de l'eNodeB** (typiquement toutes les 15 minutes)
3. Vérifiez les journaux de l'application pour des erreurs `[PmFilterStore]`

4. Vérifiez que le disque est accessible en écriture pour le fichier de persistance

Descriptions de Compteurs Manquantes

1. Les descriptions de compteurs proviennent de `priv/pm_metrics.csv`
2. Assurez-vous que ce fichier est présent et correctement formaté
3. Vérifiez les problèmes d'encodage UTF-8

Documentation Connexe

- Politique de Conservation des Données - Combien de temps les données PM sont conservées
- Intégration Grafana - Création de tableaux de bord avec des données PM
- Requêtes InfluxDB - Interrogation des données PM

Points d'Accès

- **Collecte de Données PM** : `https://localhost:9443/nokia/pm-filters`
- **Conservation des Données** : `https://localhost:9443/nokia/retention`
- **État InfluxDB** : `https://localhost:9443/nokia/influx`

Guide de Configuration d'Exécution de RAN Monitor

Comprendre config/runtime.exs

Table des Matières

1. Aperçu
2. Configuration de la Base de Données
3. Points de Terminaison Web
4. Configuration du Logger
5. Intégration Nokia
6. Configuration d'InfluxDB
7. Meilleures Pratiques de Configuration

Aperçu

Le fichier `config/runtime.exs` est le fichier de configuration principal pour RAN Monitor. Il est évalué à l'exécution (lorsque l'application démarre), vous permettant de configurer tous les aspects du comportement du système.

Ce qui est Configuré :

- Connexions à la base de données (MySQL)
- Points de terminaison et ports du serveur web
- Détails de la station de base Nokia
- Base de données de séries temporelles InfluxDB
- Comportement de journalisation

- Informations d'identification de sécurité

Emplacement du Fichier :

```
config/runtime.exs
```

Qui Devrait Utiliser Ce Guide

Important : Toute la configuration de RAN Monitor est **effectuée par Omnitouch** dans le cadre du déploiement initial et du support continu. Ce guide est fourni pour :

- **Utilisateurs avancés** qui souhaitent comprendre la configuration du système
- **Déploiements autogérés** où les clients maintiennent leur propre configuration
- **Dépannage** et compréhension de la façon dont le système est configuré
- **Déploiements personnalisés** avec des exigences spécifiques

Si vous êtes un client géré par Omnitouch, contactez le support Omnitouch pour tout changement de configuration.

Pour comprendre quelles données sont collectées, consultez Référence des Compteurs Nokia. Pour la création de tableaux de bord, consultez Intégration Grafana.

Configuration de la Base de Données

Connexion MySQL/MariaDB

```
config :ran_monitor, RanMonitor.Repo,
  username: "omnitouch",
  password: "omnitouch2024",
  hostname: "localhost",
  database: "ran_monitor",
  stacktrace: true,
  show_sensitive_data_on_connection_error: true,
  pool_size: 10
```

But : Configure la connexion à la base de données MySQL utilisée pour la gestion de l'état de session et les données opérationnelles.

Paramètres Expliqués

username (String)

- Compte utilisateur de la base de données
- Valeur actuelle : `"omnitouch"`
- **Utilisation :** Doit avoir les privilèges CREATE, SELECT, INSERT, UPDATE, DELETE
- **Sécurité :** Envisagez d'utiliser un utilisateur dédié avec les privilèges minimaux requis

password (String)

- Mot de passe de la base de données pour l'authentification
- Valeur actuelle : `"omnitouch2024"`
- **Sécurité :** Doit être stocké dans des variables d'environnement en production
- **Recommandation :** Utilisez des mots de passe forts et uniques

hostname (String)

- Adresse du serveur de base de données
- Valeur actuelle : `"localhost"`
- **Options :**
  - `"localhost"` - Base de données sur la même machine
  - `"127.0.0.1"` - Connexion TCP à la machine locale
  - `"10.179.2.135"` - IP du serveur de base de données distant
  - `"db.example.com"` - Nom d'hôte de la base de données distante

database (String)

- Nom de la base de données à utiliser
- Valeur actuelle : `"ran_monitor"`
- **Remarque :** La base de données doit exister avant de démarrer RAN Monitor
- **Création :** `CREATE DATABASE ran_monitor CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;`

stacktrace (Boolean)

- Inclure les traces de pile dans les messages d'erreur
- Valeur actuelle : `true`
- **Développement :** `true` - Aide au débogage
- **Production :** `false` - Réduit le bruit dans les journaux

show_sensitive_data_on_connection_error (Boolean)

- Afficher les informations d'identification dans les messages d'erreur de connexion
- Valeur actuelle : `true`
- **Développement :** `true` - Dépannage plus facile
- **Production :** `false` - Empêche l'exposition des informations d'identification dans les journaux

pool_size (Integer)

- Nombre de connexions à la base de données à maintenir
- Valeur actuelle : `10`
- **Guide de Dimensionnement :**
  - 1-5 appareils : `pool_size: 5`
  - 6-20 appareils : `pool_size: 10`
  - 21-50 appareils : `pool_size: 15`
  - 50+ appareils : `pool_size: 20`
- **Formule :** Environ 2 connexions par station de base + 5 pour l'interface web

---

Points de Terminaison Web

RAN Monitor exécute plusieurs serveurs web pour différents objectifs.

Point de Terminaison SOAP/API Principal

```
config :ran_monitor, RanMonitor.Web.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 8080],
  check_origin: false,
  secret_key_base:
"v5tOS1/QRonjwOky7adGGfkBbrJmiJyXhpesJy/jvSZhqLZkREV+rlo1/pR8lkbu",
  server: true
```

But : Point de terminaison principal pour la communication avec les stations de base (interface SOAP pour le protocole Nokia NE3S).

ip (Tuple)

- Interface à lier
- Valeur actuelle : `{0, 0, 0, 0}` (toutes les interfaces)
- **Options :**
  - `{0, 0, 0, 0}` - Écouter sur toutes les interfaces réseau
  - `{127, 0, 0, 1}` - Écouter uniquement sur localhost
  - `{10, 179, 2, 135}` - Écouter sur une adresse IP spécifique

port (Integer)

- Numéro de port TCP
- Valeur actuelle : `8080`
- **Remarque :** Les stations de base doivent être configurées pour envoyer des données à ce port
- **Pare-feu :** Assurez-vous que le port est ouvert pour les IP des stations de base

check_origin (Boolean)

- Valider les en-têtes d'origine WebSocket/HTTP
- Valeur actuelle : `false`
- **Explication :** Défini sur `false` pour l'API SOAP (pas d'interface web visible par l'utilisateur)

secret_key_base (String)

- Clé de signature cryptographique pour les sessions
- Valeur actuelle : chaîne aléatoire de 64 caractères
- **Génération :** `mix phx.gen.secret`
- **Sécurité :** Gardez cela secret, ne jamais le commettre dans des dépôts publics
- **Impact :** Changer cela invalide toutes les sessions existantes

server (Boolean)

- Démarrer le point de terminaison lorsque l'application démarre
- Valeur actuelle : `true`
- **Toujours :** Doit être `true` dans runtime.exs

Interface Web du Panneau de Contrôle

```
# Obtenir le port HTTPS à partir de la variable d'environnement,
par défaut à 9443
https_port =
String.to_integer(System.get_env("CONTROL_PANEL_HTTPS_PORT") ||
"9443")

config :control_panel, ControlPanelWeb.Endpoint,
  url: [host: "0.0.0.0", port: https_port, scheme: "https"],
  https: [
    ip: {0, 0, 0, 0},
    port: https_port,
    keyfile: "priv/cert/omnitouch.pem",
    certfile: "priv/cert/omnitouch.crt"
  ]
```

But : Point de terminaison HTTPS pour l'interface web du panneau de contrôle.

Variables d'Environnement :

- **CONTROL_PANEL_HTTPS_PORT** - Numéro de port HTTPS (par défaut : 9443)
  - Définissez cette variable d'environnement pour changer le port HTTPS à l'exécution
  - Exemple : `export CONTROL_PANEL_HTTPS_PORT=8443`

url (Liste de mots-clés)

- Configuration de l'URL externe
- **host :** `"0.0.0.0"` - Accepter les connexions de n'importe quel hôte
- **port :** Utilise la variable `https_port` (configurable via CONTROL_PANEL_HTTPS_PORT)
- **scheme :** `"https"` - Utiliser le protocole HTTPS

https (Liste de mots-clés)

- Configuration du serveur HTTPS
- **ip :** `{0, 0, 0, 0}` - Lier à toutes les interfaces

- **port :** Utilise la variable `https_port` (doit correspondre au port de l'url)
- **keyfile :** Chemin vers la clé privée SSL
- **certfile :** Chemin vers le certificat SSL

Fichiers de Certificat SSL :

- Doivent être des certificats SSL/TLS valides
- Les certificats auto-signés fonctionnent pour les environnements de laboratoire
- La production doit utiliser des certificats signés par une CA
- Générer un certificat auto-signé :

```
openssl req -newkey rsa:2048 -nodes -keyout omnitouch.pem -x509
-days 365 -out omnitouch.crt
```

Point de Terminaison Webhook Nokia AirScale

```
config :ran_monitor, RanMonitor.Web.Nokia.Airscale.Endpoint,
  url: [host: "0.0.0.0"],
  http: [ip: {0, 0, 0, 0}, port: 9076],
  server: true
```

But : Reçoit des données de performance en temps réel des stations de base Nokia AirScale.

port (Integer)

- Valeur actuelle : `9076`
- **Remarque :** Doit correspondre au port configuré dans la station de base PMCADM (rTpmCollEntityPortNum)
- **Coordination :** Ce port doit correspondre à ce que vous avez configuré dans l'éditeur de paramètres Nokia WebLM

Configuration du Logger

```
config :logger,
  level: :info

config :logger, :console,
  format: "$time $metadata[$level] $message\n",
  metadata: [:request_id]
```

Niveau de Journalisation

level (Atom)

- Contrôle la verbosité de la journalisation
- Valeur actuelle : `:info`
- **Options :**
  - `:debug` - Extrêmement verbeux, tous les détails
  - `:info` - Opérations normales, recommandé pour la production
  - `:warning` - Uniquement les avertissements et les erreurs
  - `:error` - Uniquement les erreurs

Quand Utiliser Chaque Niveau :

- **Développement :** `:debug` - Voir toutes les opérations internes
- **Production :** `:info` - Équilibre entre visibilité et bruit
- **Dépannage :** Définir temporairement sur `:debug`, puis revenir
- **Production Silencieuse :** `:warning` - Alerter uniquement sur les problèmes

Format de la Console

format (String)

- Comment apparaissent les messages de journal
- Valeur actuelle : `"$time $metadata[$level] $message\n"`
- **Variables :**

    - `$time` - Horodatage
    - `$metadata` - Informations contextuelles
    - `$level` - Niveau de journal (info, erreur, etc.)
    - `$message` - Message de journal réel

metadata (Liste d'atomes)

- Contexte supplémentaire à inclure
- Valeur actuelle : `[:request_id]`
- **request_id :** Suit les requêtes HTTP individuelles à travers le système

---

Intégration Nokia

Cette section configure comment RAN Monitor communique avec les stations de base Nokia.

```
config :ran_monitor,
  general: %{
    mcc: "505",
    mnc: "57"
  },
  nokia: %{
    ne3s: %{
      webhook_url: "http://10.5.198.200:9076/webhook",
      private_key: Path.join(Application.app_dir(:ran_monitor,
"priv"), "external/nokia/ne.key.pem"),
      public_key: Path.join(Application.app_dir(:ran_monitor,
"priv"), "external/nokia/ne.cert.der"),
      reregister_interval: 30
    },
    airscales: [
      %{
        address: "10.7.15.67",
        name: "ONS-Lab-Airscale",
        port: "8080",
        web_username: "Nemuadmin",
        web_password: "nemuuser"
      }
    ]
  }
```

Paramètres Généraux

mcc (String)

- Code Pays Mobile
- Valeur actuelle : `"505"`
- **Utilisation :** Identifie le pays pour les réseaux 3GPP
- **Format :** 3 chiffres
- **Référence :** ITU-T E.212

mnc (String)

- Code Réseau Mobile
- Valeur actuelle : `"57"`

- **Utilisation :** Identifie l'opérateur de réseau spécifique
- **Format :** 2 ou 3 chiffres

Configuration NE3S (Protocole Nokia NE3S)

webhook_url (String)

- URL où les stations de base envoient des notifications
- Valeur actuelle : `"http://10.5.198.200:9076/webhook"`
- **Format :** `http://<ran-monitor-ip>:<port>/webhook`
- **Adresse IP :** Doit être l'adresse IP où RAN Monitor s'exécute
- **Port :** Doit correspondre au port de `RanMonitor.Web.Nokia.Airscale.Endpoint` (9076)
- **Chemin :** Toujours `/webhook`

private_key (String - Chemin de fichier)

- Clé privée pour l'authentification du gestionnaire
- Valeur actuelle : `priv/external/nokia/ne.key.pem`
- **Format :** Clé privée encodée en PEM
- **Sécurité :** Gardez ce fichier sécurisé, ne jamais partager
- **Génération :** Fournie par Nokia ou générée avec OpenSSL

public_key (String - Chemin de fichier)

- Certificat public pour l'identité du gestionnaire
- Valeur actuelle : `priv/external/nokia/ne.cert.der`
- **Format :** Certificat encodé en DER
- **Utilisation :** Envoyé à la station de base lors de l'enregistrement
- **Paire :** Doit correspondre à private_key

reregister_interval (Integer)

- À quelle fréquence se réenregistrer auprès des stations de base (secondes)
- Valeur actuelle : `30`

- **Explication :** Les sessions expirent, le réenregistrement périodique maintient la connexion
- **Plage :** 30-300 secondes
- **Recommandation :** 30 secondes pour une surveillance fiable

Stations de Base AirScale

airscales (Liste de cartes)

- Liste des stations de base Nokia AirScale à surveiller
- Valeur actuelle : Une station de base configurée

Chaque entrée de station de base nécessite :

address (String)

- Adresse IP de la station de base
- Valeur actuelle : `"10.7.15.66"`
- **Format :** Adresse IPv4 sous forme de chaîne
- **Réseau :** Doit être accessible depuis le serveur RAN Monitor
- **Vérification :** `ping 10.7.15.66` doit réussir

name (String)

- Nom convivial pour identification
- Valeur actuelle : `"ONS-Lab-Airscale"`
- **Utilisation :** Apparaît dans l'interface Web, les journaux et les balises InfluxDB
- **Recommandation :** Utilisez des noms descriptifs (codes de site, emplacements, etc.)
- **Exemples :**
  - `"NYC-Site-A-BS1"`
  - `"LAX-Tower-Main"`
  - `"TestLab-Airscale-01"`

port (String)

- Port de l'interface de gestion sur la station de base
- Valeur actuelle : `"8080"`
- **Standard :** Nokia AirScale utilise généralement 8080
- **Vérification :** Vérifiez la documentation de la station de base
- **Remarque :** La valeur est une chaîne, pas un entier

web_username (String)

- Nom d'utilisateur pour l'authentification WebLM
- Valeur actuelle : `"Nemuadmin"`
- **Utilisation :** Utilisé pour les appels API pour gérer la station de base
- **Privilèges :** Doit avoir un accès en lecture/écriture à la configuration
- **Remarque :** Sensible à la casse

web_password (String)

- Mot de passe pour l'authentification WebLM
- Valeur actuelle : `"nemuuser"`
- **Sécurité :** Doit être stocké dans des variables d'environnement en production
- **Rotation :** Changer régulièrement selon la politique de sécurité

Ajouter Plusieurs Stations de Base

Pour surveiller plusieurs stations de base, ajoutez des entrées supplémentaires à la liste `airscales` :

```
airscales: [
  %{
    address: "10.7.15.66",
    name: "ONS-Lab-Airscale",
    port: "8080",
    web_username: "Nemuadmin",
    web_password: "nemuuser"
  },
  %{
    address: "10.7.15.67",
    name: "Site-A-Tower-1",
    port: "8080",
    web_username: "admin",
    web_password: "password123"
  },
  %{
    address: "192.168.100.50",
    name: "Site-B-Indoor",
    port: "8080",
    web_username: "admin",
    web_password: "different_password"
  }
]
```

Configuration d'InfluxDB

```
config :ran_monitor, RanMonitor.InfluxDbConnection,
  auth: [
    username: "monitor",
    password: "sideunderTexasgalaxyview_61"
  ],
  database: "nokia-monitor",
  host: "10.179.2.135"
```

But : Configure la connexion à la base de données de séries temporelles InfluxDB pour stocker les métriques, les alarmes et les données de configuration.

Paramètres Expliqués

auth (Liste de mots-clés)

- Informations d'identification d'authentification pour InfluxDB
- **username :** Compte utilisateur InfluxDB (`"monitor"`)
- **password :** Mot de passe InfluxDB (`"sideunderTexasgalaxyview_61"`)
- **Remarque :** Pour InfluxDB 2.x, cela pourrait être un jeton API à la place

database (String)

- Nom du bucket/base de données dans InfluxDB
- Valeur actuelle : `"nokia-monitor"`
- **InfluxDB 1.x :** Nom de la base de données
- **InfluxDB 2.x :** Nom du bucket
- **Création :** Doit être créé avant de démarrer RAN Monitor

```
# InfluxDB 1.x
influx -execute 'CREATE DATABASE "nokia-monitor"'

# InfluxDB 2.x
influx bucket create -n nokia-monitor -o your-org
```

host (String)

- Adresse du serveur InfluxDB
- Valeur actuelle : `"10.179.2.135"`
- **Format :** Adresse IP ou nom d'hôte
- **Port :** Le port par défaut d'InfluxDB (8086) est supposé
- **Exemples :**
  - `"localhost"` - Même serveur que RAN Monitor
  - `"10.179.2.135"` - Serveur InfluxDB distant
  - `"influxdb.example.com"` - Nom d'hôte

Notes de Connexion InfluxDB

Accès Réseau :

- RAN Monitor doit pouvoir atteindre le serveur InfluxDB sur le port 8086
- Vérifiez : `curl http://10.179.2.135:8086/ping`

Politiques de Rétention :

- Définies via la page de rétention des données de l'interface Web
- Par défaut : 30 jours (720 heures)
- Peut être personnalisé par station de base

Performance d'Écriture :

- InfluxDB reçoit des écritures à chaque intervalle de collecte (60s par défaut)
- Chaque station de base génère des centaines de points de données par intervalle
- Surveillez régulièrement l'espace disque d'InfluxDB

Meilleures Pratiques de Configuration

Sécurité

1. Protéger les Données Sensibles

```
# Au lieu de mots de passe codés en dur :
password: "omnitouch2024"

# Utilisez des variables d'environnement :
password: System.get_env("DB_PASSWORD") || "default_password"
```

2. Restreindre les Permissions de Fichier

```
chmod 600 config/runtime.exs
chown ran_monitor:ran_monitor config/runtime.exs
```

3. Ne Jamais Commettre de Secrets

- Utilisez `.gitignore` pour runtime.exs s'il contient des secrets
- Utilisez des variables d'environnement ou des systèmes de gestion des secrets
- Faites tourner les mots de passe régulièrement

Performance

1. Dimensionnement du Pool de Base de Données

- Surveillez l'utilisation des connexions
- Augmentez pool_size si vous voyez des erreurs de délai d'attente de connexion
- Chaque appareil a besoin d'environ 2 connexions pendant le sondage actif

2. Intervalles de Collecte

- Équilibrez entre la granularité des données et la charge système
- Des intervalles de 60 secondes fonctionnent bien pour la plupart des déploiements
- Intervalles plus courts (15s) pour le dépannage

3. Optimisation d'InfluxDB

- Utilisez des politiques de rétention pour gérer l'utilisation du disque
- Surveillez la performance d'écriture d'InfluxDB
- Envisagez un serveur InfluxDB séparé pour les grands déploiements

Fiabilité

1. Configuration Réseau

- Utilisez des adresses IP statiques pour tous les composants
- Vérifiez les routes réseau entre RAN Monitor et les stations de base
- Testez la connectivité avant d'ajouter des appareils
- Configurez les règles de pare-feu de manière appropriée

2. Stratégie de Journalisation

- Développement : `:debug` pour un dépannage détaillé
- Production : `:info` pour une visibilité opérationnelle
- Systèmes critiques : Envisagez l'agrégation de journaux externe

3. Surveiller RAN Monitor

- Surveillez le moniteur (méta-surveillance)
- Surveillez les erreurs de connexion à la base de données
- Suivez les taux de réussite d'écriture d'InfluxDB
- Alertez sur les déconnexions de stations de base

Maintenance

1. Changements de Configuration

- Toujours sauvegarder runtime.exs avant les changements
- Testez la configuration d'abord en développement
- Documentez les changements avec des commentaires
- Redémarrez RAN Monitor après les changements de configuration

2. Ajouter des Stations de Base

```
# 1. Éditer runtime.exs
vim config/runtime.exs

# 2. Valider la syntaxe Elixir
elixir -c config/runtime.exs

# 3. Redémarrer l'application
systemctl restart ran_monitor
```

3. Considérations de Mise à l'Échelle

- Surveillez l'utilisation des ressources (CPU, mémoire, réseau)
- Augmentez la taille du pool de base de données à mesure que le nombre d'appareils augmente
- Envisagez une instance InfluxDB séparée à 50+ appareils
- Surveillez l'espace disque pour MySQL et InfluxDB

Exemple : Configuration Complète

Voici un exemple complet avec plusieurs stations de base et les meilleures pratiques appliquées :

```
import Config

#
==========================================================================
# Configuration de la Base de Données
#
==========================================================================

config :ran_monitor, RanMonitor.Repo,
  username: System.get_env("DB_USERNAME") || "ran_monitor_user",
  password: System.get_env("DB_PASSWORD") || "change_this_password",
  hostname: System.get_env("DB_HOST") || "localhost",
  database: "ran_monitor",
  stacktrace: false,  # Production : cacher les traces de pile
  show_sensitive_data_on_connection_error: false,  # Production : cac
informations d'identification
  pool_size: 15  # 6 stations de base * 2 + 3 de surcharge

#
==========================================================================
# Points de Terminaison Web
#
==========================================================================

config :ran_monitor, RanMonitor.Web.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 8080],
  check_origin: false,
  secret_key_base: System.get_env("SECRET_KEY_BASE") ||
"generate_with_mix_phx_gen_secret",
  server: true

config :control_panel, ControlPanelWeb.Endpoint,
  url: [host: "0.0.0.0", port: 9443, scheme: "https"],
  https: [
    ip: {0, 0, 0, 0},
    port: 9443,
    keyfile: "priv/cert/server.key",
    certfile: "priv/cert/server.crt"
  ]

config :ran_monitor, RanMonitor.Web.Nokia.Airscale.Endpoint,
  url: [host: "0.0.0.0"],
  http: [ip: {0, 0, 0, 0}, port: 9076],
```

```
  server: true

#
# Configuration du Logger
#

config :logger,
  level: :info  # Réglage de production

config :logger, :console,
  format: "$time $metadata[$level] $message\n",
  metadata: [:request_id]

#
# Configuration Nokia
#

config :ran_monitor,
  general: %{
    mcc: "001",
    mnc: "001"
  },
  nokia: %{
    ne3s: %{
      webhook_url: "http://10.179.2.135:9076/webhook",
      private_key: Path.join(Application.app_dir(:ran_monitor, "priv"
"external/nokia/ne.key.pem"),
      public_key: Path.join(Application.app_dir(:ran_monitor, "priv")
"external/nokia/ne.cert.der"),
      reregister_interval: 30
    },
    airscales: [
      # Site A - Tour Principale
      %{
        address: "10.7.15.66",
        name: "Site-A-Tour-Principale",
        port: "8080",
        web_username: "admin",
        web_password: System.get_env("BS_SITE_A_PASSWORD") || "passwo
      },
```

```
    # Site A - Tour de Secours
    %{
      address: "10.7.15.67",
      name: "Site-A-Tour-Secours",
      port: "8080",
      web_username: "admin",
      web_password: System.get_env("BS_SITE_A_PASSWORD") || "passwo
    },

    # Site B - Intérieur
    %{
      address: "10.7.16.10",
      name: "Site-B-Intérieur-DAS",
      port: "8080",
      web_username: "admin",
      web_password: System.get_env("BS_SITE_B_PASSWORD") || "passwo
    },

    # Site C - Toit
    %{
      address: "192.168.100.50",
      name: "Site-C-Toit",
      port: "8080",
      web_username: "admin",
      web_password: System.get_env("BS_SITE_C_PASSWORD") || "passwo
    },

    # Laboratoire - Équipement de Test
    %{
      address: "10.5.198.100",
      name: "Lab-Test-Airscale-01",
      port: "8080",
      web_username: "Nemuadmin",
      web_password: "nemuuser"
    },

    # Laboratoire - Développement
    %{
      address: "10.5.198.101",
      name: "Lab-Dev-Airscale-02",
      port: "8080",
      web_username: "Nemuadmin",
      web_password: "nemuuser"
```

```
      }
    ]
  }

#
# Configuration d'InfluxDB
#

config :ran_monitor, RanMonitor.InfluxDbConnection,
  auth: [
    username: System.get_env("INFLUX_USERNAME") || "monitor",
    password: System.get_env("INFLUX_PASSWORD") || "change_this_passw
  ],
  database: "nokia-monitor",
  host: System.get_env("INFLUX_HOST") || "10.179.2.135"
```

Documentation Connexe

- Guide des Opérations - Opérations quotidiennes
- Guide de Configuration AirScale - Configuration des stations de base
- Référence des Compteurs Nokia - Définitions des compteurs de performance
- Intégration Grafana - Création de tableaux de bord et d'alertes
- Points de Terminaison API - Référence de l'API REST
- Politique de Rétention des Données - Gestion du cycle de vie des données

Collecte de données MDT avec TCE

Entité de collecte de traces (TCE)

RAN Monitor comprend une entité de collecte de traces intégrée pour capturer et analyser les messages de protocole LTE/5G. Cela permet un dépannage détaillé, des tests de conduite et une optimisation RF.

Qu'est-ce que TCE ?

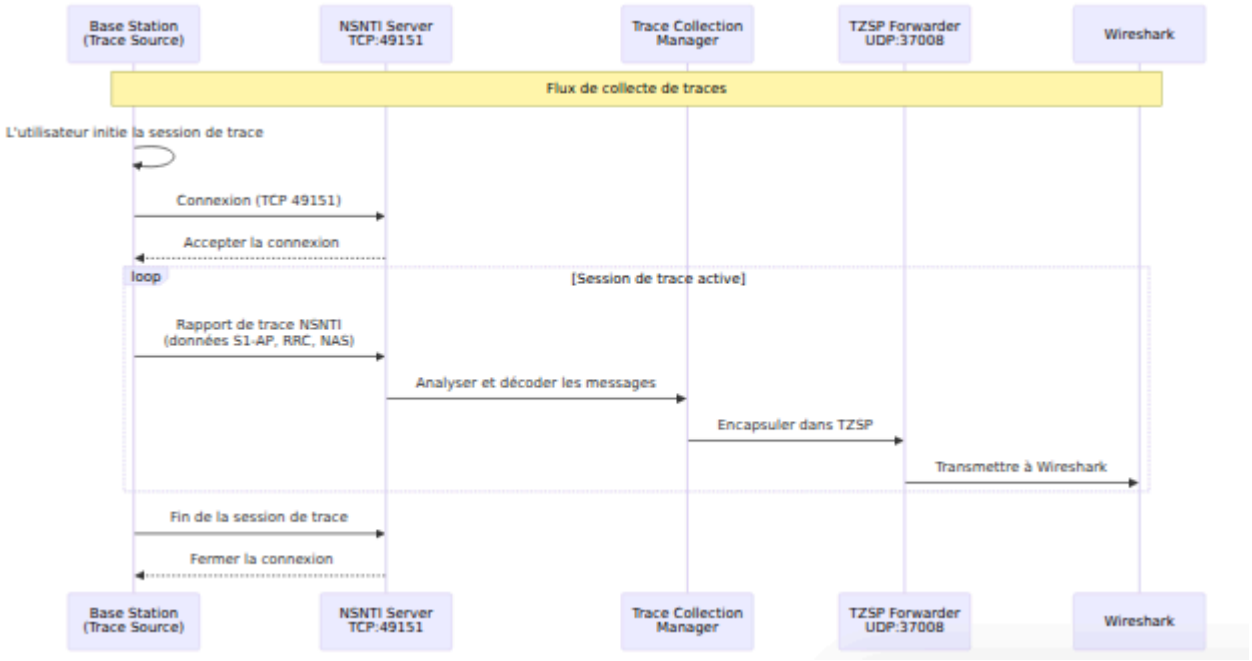
L'entité de collecte de traces reçoit des données de traces des stations de base Nokia AirScale contenant :

- **Messages S1-AP** - Signalisation du plan de contrôle entre eNodeB et EPC
- **Messages RRC** - Signalisation de contrôle des ressources radio
- **Messages NAS** - Signalisation du Stratum non d'accès
- **Données du plan utilisateur** - Informations sur le débit de la couche PDCP

Composants du TCE

Composant	Protocole	Port	Objectif
Serveur NSNTI	TCP	49151	Reçoit des messages de trace des stations de base
Serveur TZSP	UDP	37008	Transmet les traces à Wireshark pour une analyse en temps réel
Décodeurs de protocole	ASN.1	-	Décode les messages S1-AP et RRC

Comment ça fonctionne



La page de collecte de traces montre les connexions actives, le port d'écoute NSNTI (49151), la configuration TZSP et les stations de base connectées.

Configuration de la collecte de traces

1. **Vérifiez que TCE fonctionne :**

   ```
   ss -tlnp | grep 49151
   # Devrait afficher : LISTEN 0.0.0.0:49151
   ```

2. **Configurer la trace de la station de base :**

   - Définir l'IP de destination de la trace sur le serveur RAN Monitor
   - Définir le port de destination de la trace sur 49151
   - Activer les catégories de trace (S1-AP, RRC, NAS selon les besoins)
   - Démarrer la session de trace

3. **Configurer Wireshark :**

   Configuration de base :

   - Démarrer la capture sur l'interface recevant les paquets TZSP
   - Utiliser le filtre de capture : `udp port 37008`

   Configuration de décodage de protocole :

   RAN Monitor utilise des ports UDP spécifiques pour identifier différents types de protocoles et canaux RRC. Configurez la fonction "Décoder comme" de Wireshark pour décoder correctement ces protocoles :

   Méthode 1 : Utilisation de l'interface graphique de Wireshark

   i. Allez à **Analyser → Décoder comme...**
   ii. Cliquez sur le bouton **+** pour ajouter de nouvelles entrées
   iii. Configurez chaque ligne comme suit :

Champ	Valeur	Type	Actuel	Décoder comme
udp.port	36412	Entier	(aucun)	SCTP
sctp.port	36412	Entier	(aucun)	S1AP
udp.port	37000	Entier	(aucun)	TZSP
udp.port	37001	Entier	(aucun)	LTE RRC (DL-CCCH)
udp.port	37002	Entier	(aucun)	LTE RRC (DL-DCCH)
udp.port	37003	Entier	(aucun)	LTE RRC (BCCH)
udp.port	37004	Entier	(aucun)	LTE RRC (PCCH)
udp.port	37008	Entier	(aucun)	TZSP
udp.port	37011	Entier	(aucun)	LTE RRC (UL-CCCH)
udp.port	37012	Entier	(aucun)	LTE RRC (UL-DCCH)
udp.port	38000	Entier	(aucun)	MAC-LTE
udp.port	38001	Entier	(aucun)	MAC-LTE (DL)
udp.port	38002	Entier	(aucun)	MAC-LTE (BCH)
udp.port	38003	Entier	(aucun)	MAC-LTE (PCH)
udp.port	38011	Entier	(aucun)	MAC-LTE (UL)
udp.port	38012	Entier	(aucun)	MAC-LTE (RACH)

Méthode 2 : Utilisation du fichier decode_as_entries

Créez ou éditez `~/.config/wireshark/decode_as_entries` (Linux/Mac) ou `%APPDATA%\Wireshark\decode_as_entries` (Windows) :

```
# Mappages de ports TZSP de RAN Monitor
decode_as_entry: udp.port,36412,(none),SCTP
decode_as_entry: sctp.port,36412,(none),S1AP
decode_as_entry: udp.port,37000,(none),TZSP
decode_as_entry: udp.port,37001,(none),LTE RRC
decode_as_entry: udp.port,37002,(none),LTE RRC
decode_as_entry: udp.port,37003,(none),LTE RRC
decode_as_entry: udp.port,37004,(none),LTE RRC
decode_as_entry: udp.port,37008,(none),TZSP
decode_as_entry: udp.port,37011,(none),LTE RRC
decode_as_entry: udp.port,37012,(none),LTE RRC
decode_as_entry: udp.port,38000,(none),MAC-LTE
decode_as_entry: udp.port,38001,(none),MAC-LTE
decode_as_entry: udp.port,38002,(none),MAC-LTE
decode_as_entry: udp.port,38003,(none),MAC-LTE
decode_as_entry: udp.port,38011,(none),MAC-LTE
decode_as_entry: udp.port,38012,(none),MAC-LTE
```

Guide de référence des ports :

Port	Protocole	Canal/Type	Description
36412	S1AP	-	Plan de contrôle S1AP standard (eNodeB ↔ EPC)
37000	RRC	Générique	Fallback pour les types de canaux RRC inconnus
37001	RRC	DL-CCCH	Canal de contrôle commun de liaison descendante
37002	RRC	DL-DCCH	Canal de contrôle dédié de liaison descendante
37003	RRC	BCCH-DL-SCH	Canal de contrôle de diffusion (Informations système)
37004	RRC	PCCH	Canal de contrôle d'appel
37008	TZSP	-	Port d'écoute TZSP principal
37011	RRC	UL-CCCH	Canal de contrôle commun de liaison montante (Demande de connexion RRC)
37012	RRC	UL-DCCH	Canal de contrôle dédié de liaison montante (Rapports de mesure)
38000	MAC-LTE	Générique	Fallback pour les types de canaux MAC inconnus
38001	MAC-LTE	Descendant	Canal partagé de liaison descendante
38002	MAC-LTE	BCH	Canal de diffusion

Port	Protocole	Canal/Type	Description
38003	MAC-LTE	PCH	Canal d'appel
38011	MAC-LTE	Montant	Canal partagé de liaison montante
38012	MAC-LTE	RACH	Canal d'accès aléatoire

Filtres d'affichage utiles :

```
# Afficher tous les paquets TZSP
tzsp

# Afficher des protocoles spécifiques
s1ap || rrc || mac-lte

# Afficher uniquement les messages RRC en liaison montante
udp.port == 37011 || udp.port == 37012

# Afficher uniquement les messages RRC en liaison descendante
udp.port == 37001 || udp.port == 37002

# Afficher l'établissement de connexion RRC
rrc.rrcConnectionRequest || rrc.rrcConnectionSetup

# Afficher les messages de transfert
s1ap.HandoverRequired || s1ap.HandoverCommand
```

Cas d'utilisation

Tests de conduite :

- Capturer l'expérience RF de l'utilisateur final
- Analyser les performances de transfert
- Mesurer la qualité du signal (RSRP, RSRQ, SINR)
- Identifier les trous de couverture

Dépannage :

- Déboguer les échecs d'établissement d'appel
- Analyser les problèmes de transfert
- Enquêter sur les appels interrompus
- Examiner les événements de mobilité

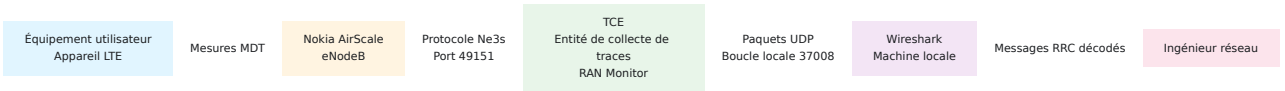
Optimisation RF :

- Validation de la planification PCI
- Optimisation des relations de voisinage
- Réglage des paramètres de transfert
- Analyse de la couverture et de la capacité

Aperçu

Minimisation des tests de conduite (MDT) vous permet de collecter des mesures radio (RSRP, RSRQ, données de couverture) directement à partir des UEs sans tests de conduite traditionnels. Ce guide vous montre comment capturer des données MDT à partir des stations de base Nokia AirScale en utilisant l'interface Web Omnitouch RAN Monitor et les visualiser dans Wireshark.

Architecture



L'entité de collecte de traces (TCE) est intégrée dans le RAN Monitor Omnitouch et gère la conversion des traces de protocole Ne3s spécifiques à Nokia en formats standard visibles dans Wireshark.

Prérequis

Licences requises

Le Nokia Airscale nécessite des activations de fonctionnalités, y compris **Données de mesure par appel** pour collecter ces données, et ces fonctionnalités doivent être activées et configurées.

Contactez ONS si vous avez besoin d'aide avec la licence ou si vous avez des questions sur votre déploiement spécifique.

Exigences système

- Omnitouch RAN Monitor avec TCE en cours d'exécution
- Wireshark 3.0+ installé sur votre machine
- Plugins Lua TCE installés dans Wireshark
- Connectivité réseau vers l'AirScale

Configuration de la traçabilité MDT

Le TCE intégré dans le RAN Monitor convertit les données Nokia entrantes en formats standard visibles dans Wireshark.

Étape 1 : Configurer l'entité de collecte de traces

Utilisez l'interface Web RAN Monitor pour configurer la station de base afin d'envoyer des traces au TCE :

1. Ouvrez l'interface Web : `https://<ran-monitor-ip>:9443`
2. Accédez à la page **Stations de base**
3. Cliquez sur l'appareil que vous souhaitez tracer
4. Allez à la section **Gestion de la configuration**
5. Téléchargez la configuration actuelle (sauvegarde)
6. Modifiez la configuration pour ajouter/mettre à jour les paramètres TCE :

    - **IP de l'entité de collecte de traces** : `<Votre IP RAN Monitor>`
    - **Port de l'entité de collecte de traces** : `49151`
7. Téléchargez la configuration modifiée
8. Validez la configuration (attendez que la validation soit terminée)
9. Activez la configuration

Pour obtenir de l'aide sur des paramètres de configuration spécifiques ou des versions logicielles AirScale, contactez ONS.

Étape 2 : Configurer MDT sur l'AirScale

Activez la traçabilité MDT sur votre station de base. Les options de configuration incluent :

- **Type de trace** : MDT immédiat (temps réel) ou MDT enregistré (mode inactif)
- **Portée de la zone** : Spécifique à la cellule, zone de suivi ou PLMN
- **Intervalle de mesure** : À quelle fréquence les UEs rapportent (par exemple, 5000 ms)
- **Type de mesure** : RSRP, RSRQ ou les deux
- **Profondeur de la trace** : Minimum, Moyen ou Maximum

Contactez ONS pour des conseils sur la configuration de ces paramètres pour votre cas d'utilisation spécifique.

Étape 3 : Activer la session de trace

Une fois configurée, activez la session de trace sur l'AirScale. La station de base commencera à envoyer des données MDT au TCE qui, à son tour, les transmettra à votre machine de surveillance.

Visualisation des données MDT dans Wireshark

Configurer la capture Wireshark

1. Démarrez Wireshark sur votre machine
2. Capturez sur l'**interface de boucle locale** (`lo` sur Linux, `lo0` sur macOS, `Loopback` sur Windows)
3. Définissez le filtre de capture : `udp port 37008`
4. Commencez à capturer

Exemple de capture Wireshark montrant des messages de plan de contrôle S1AP (InitialUEMessage, Demande d'attachement), des messages LTE RRC (RRCConnectionReject, RRCConnectionReestablishment) et divers flux de signalisation capturés via le TCE.

Filtrer pour les mesures MDT

Une fois les données en cours de flux, utilisez ces filtres d'affichage :

```
# Afficher tous les rapports de mesure RRC
lte-rrc.measurementReport

# Afficher tous les messages RRC en liaison montante
udp.dstport >= 37011 && udp.dstport <= 37012

# Filtrer par RSRP faible (< -100 dBm)
lte-rrc.rsrpResult < 40

# Filtrer par RSRQ faible (< -12 dB)
lte-rrc.rsrqResult < 22
```

Comprendre les données

Les mesures MDT apparaissent sous forme de messages **RRC MeasurementReport** contenant :

- **Mesures de cellule de service** : RSRP et RSRQ pour la cellule connectée
- **Mesures de cellules voisines** : RSRP et RSRQ pour les cellules à proximité
- **IDs de cellules** : IDs de cellules physiques pour corrélation
- **Localisation GPS** : Si configuré et pris en charge par l'UE

Développez le message RRC dans Wireshark pour voir les mesures détaillées :

```
Contrôle des ressources radio (RRC)
└─ UL-DCCH-Message
    └─ message: measurementReport
        └─ MeasurementReport
            └─ measResults
                ├─ measResultServCell (RSRP/RSRQ de la cellule de
service)
                └─ measResultNeighCells (mesures des cellules
voisines)
```

Exporter pour analyse

Pour analyser les données hors ligne :

1. **Fichier → Exporter les dissections de paquets → En tant que CSV**
2. Inclure les champs : `lte-rrc.rsrpResult`, `lte-rrc.rsrqResult`, `lte-rrc.physCellId`
3. Traitez dans Excel, Python ou d'autres outils

Cas d'utilisation courants

Analyse de couverture : Recherchez des zones avec un RSRP/RSRQ faible

```
lte-rrc.rsrpResult < 40 || lte-rrc.rsrqResult < 22
```

Analyse de transfert : Voir quelles cellules voisines les UEs rapportent

```
lte-rrc.MeasResultListEUTRA
```

Détection d'interférences : Bon RSRP mais mauvais RSRQ indique une interférence

```
lte-rrc.rsrpResult > 50 && lte-rrc.rsrqResult < 20
```

Dépannage

Pas de données dans Wireshark ?

- Vérifiez que TCE fonctionne : `ps aux | grep beam`
- Vérifiez que Wireshark capture la boucle locale avec le filtre `udp port 37008`
- Confirmez que la session de trace est active sur l'AirScale
- Vérifiez que l'IP/port TCE est configuré correctement sur la station de base

Données incomplètes ?

- Vérifiez que les licences sont actives (MDT + Mesure par appel)

- Augmentez la profondeur de trace à MAXIMUM
- Assurez-vous que les UEs prennent en charge MDT (LTE Release 10+)

Pour obtenir de l'aide sur la configuration, des problèmes de licence ou des questions spécifiques à AirScale, contactez ONS.

Liste de contrôle de démarrage rapide

- [ ] Vérifiez que les licences MDT et de mesure par appel sont actives
- [ ] Configurez l'IP TCE (IP RAN Monitor) et le port 49151 sur l'AirScale
- [ ] Démarrez TCE sur le serveur RAN Monitor
- [ ] Activez la session de trace MDT sur la station de base
- [ ] Démarrez la capture Wireshark sur la boucle locale avec le filtre `udp port 37008`
- [ ] Appliquez le filtre d'affichage : `lte-rrc.measurementReport`
- [ ] Analysez les mesures et exportez si nécessaire

Support

- **Omnitouch Network Services (ONS)** : Pour l'assistance à la configuration, à la licence et au déploiement d'AirScale

Guide de Dépannage

Résolution de Problèmes pour RAN Monitor

Problèmes courants, procédures de diagnostic et solutions

Table des Matières

1. Aperçu
2. Problèmes de Connexion des Dispositifs
3. Problèmes de Collecte de Données
4. Problèmes de l'Interface Web
5. Problèmes de Base de Données
6. Problèmes de Performance
7. Problèmes d'Alarme
8. Outils de Diagnostic
9. Obtenir de l'Aide

Aperçu

Ce guide vous aide à diagnostiquer et à résoudre les problèmes courants avec RAN Monitor. Chaque section fournit des symptômes, des étapes de diagnostic et des solutions.

Approche de Dépannage

1. Identifier le Symptom

- Qu'est-ce qui ne fonctionne pas comme prévu ?
- Quand le problème a-t-il commencé ?
- Qu'est-ce qui a changé récemment ?

2. Rassembler des Informations

- Vérifiez les journaux d'application
- Examinez l'état du dispositif dans l'interface Web
- Vérifiez la connectivité de la base de données
- Passez en revue les modifications de configuration récentes

3. Diagnostiquer la Cause Racine

- Utilisez des outils de diagnostic
- Examinez les messages d'erreur
- Testez les composants individuels
- Isolez le problème

4. Mettre en Œuvre la Solution

- Appliquez la correction en fonction du diagnostic
- Vérifiez que la solution résout le problème
- Surveillez la récurrence
- Documentez les résultats

Avant de Commencer

Vérifiez les Bases :

- RAN Monitor est-il en cours d'exécution ? (`ps aux | grep ran_monitor`)
- Les services requis sont-ils en cours d'exécution ? (MySQL, InfluxDB)
- La connectivité réseau fonctionne-t-elle ?
- Y a-t-il eu des changements récents ?

Problèmes de Connexion des Dispositifs

Problème : Dispositif Non Enregistré

Symptômes :

- Le dispositif affiche "Non Enregistré" dans l'interface Web
- Statut rouge (échec) dans la page des Stations de Base
- Aucune métrique n'est collectée à partir du dispositif
- Messages d'erreur dans les journaux d'application

Étapes de Diagnostic :

1. Vérifiez la Connectivité Réseau

```
# Testez la connectivité de base
ping <device-ip>

# Testez le port de gestion
telnet <device-ip> 8080
```

Attendu : Ping et connexion telnet réussis
Si Échec : Problème réseau - vérifiez les routes, le pare-feu, l'état du dispositif

2. Vérifiez la Configuration

Dans l'interface Web → Stations de Base → Cliquez sur le dispositif → Passez en revue la configuration :

- L'adresse IP est-elle correcte ?
- Le port est-il correct (généralement 8080) ?
- Les identifiants sont-ils configurés ?

Dans `config/runtime.exs` :

```
%{
  address: "10.7.15.66",  # IP correcte ?
  name: "Site-A-BS1",
  port: "8080",           # Port correct ?
  web_username: "admin",  # Nom d'utilisateur correct ?
  web_password: "password" # Mot de passe correct ?
}
```

3. Vérifiez les Journaux d'Application

Interface Web → Journaux d'Application → Filtrer par nom de dispositif

Recherchez :

- `[error] Authentication failed` → Identifiants incorrects
- `[error] Connection refused` → Problème de port/pare-feu
- `[error] Timeout` → Problème de connectivité réseau
- `[error] Certificate error` → Problème de clé/certificat du gestionnaire

Solutions :

Problème Réseau :

1. Vérifiez que le dispositif est sous tension et opérationnel
2. Vérifiez les routes réseau entre RAN Monitor et le dispositif
3. Vérifiez que le pare-feu autorise :
   - RAN Monitor → Port 8080 du dispositif
   - Dispositif → Port 9076 de RAN Monitor (webhooks)
4. Testez directement depuis le serveur RAN Monitor

Identifiants Incorrects :

1. Vérifiez que les identifiants fonctionnent directement sur l'interface WebLM du dispositif
2. Mettez à jour les identifiants dans `config/runtime.exs`
3. Redémarrez RAN Monitor
4. Surveillez les journaux pour une inscription réussie

Problème de Port/Pare-feu :

1. Vérifiez le port correct dans la configuration
2. Vérifiez les règles du pare-feu des deux côtés
3. Testez l'accessibilité du port : `telnet <device-ip> 8080`
4. Passez en revue les paramètres de sécurité côté dispositif

Problème de Clé/Certificat du Gestionnaire :

1. Vérifiez que les fichiers existent :
   - `priv/external/nokia/ne.key.pem`
   - `priv/external/nokia/ne.cert.der`
2. Vérifiez les permissions des fichiers (doivent être lisibles)
3. Vérifiez que les fichiers sont des identifiants valides du gestionnaire Nokia
4. Contactez le support Nokia si les clés sont invalides

Problème : La Session Expire en Continu

Symptômes :

- Le dispositif se déconnecte et se reconnecte en boucle
- Messages "Session expirée" dans les journaux
- Statut rouge/vert intermittent dans l'interface Web
- Lacunes dans la collecte des métriques

Étapes de Diagnostic :

1. Vérifiez les Informations de Session

Interface Web → Stations de Base → Cliquez sur le dispositif → Cycle de Vie de la Session :

- Quelle est la durée d'expiration de la session ?
- Le keep-alive fonctionne-t-il ?
- À quelle fréquence la session expire-t-elle ?

2. Vérifiez l'Intervalle de Keep-Alive

Dans `config/runtime.exs` :

```
nokia: %{
  ne3s: %{
    reregister_interval: 30  # Devrait être de 30 à 60 secondes
  }
}
```

3. Vérifiez la Stabilité du Réseau

- Y a-t-il des problèmes de réseau intermittents ?
- Vérifiez la perte de paquets : `ping <device-ip> -c 100`
- Passez en revue les journaux réseau pour des interfaces instables

4. Vérifiez la Synchronisation de l'Horloge

```
# Sur le serveur RAN Monitor
date

# Sur le dispositif (si accessible)
# Vérifiez que l'heure est synchronisée
```

Solutions :

Intervalle de Keep-Alive Trop Long :

1. Réduisez `reregister_interval` à 30 secondes
2. Redémarrez RAN Monitor
3. Surveillez la stabilité de la session

Instabilité Réseau :

1. Travaillez avec l'équipe réseau pour diagnostiquer
2. Vérifiez la connectivité intermittente
3. Passez en revue les journaux des commutateurs/routeurs
4. Envisagez des chemins réseau redondants

Synchronisation de l'Horloge :

1. Configurez NTP sur RAN Monitor et les dispositifs
2. Vérifiez que les horloges sont synchronisées
3. Vérifiez les grandes différences de temps

Problème Côté Dispositif :

1. Vérifiez les journaux du dispositif pour des erreurs
2. Vérifiez que l'interface de gestion du dispositif est stable
3. Envisagez de redémarrer le dispositif si un problème logiciel est suspecté

Problème : Les Métriques N'apparaissent Pas

Symptômes :

- Le dispositif apparaît comme "Associé" (vert) dans l'interface Web
- Mais aucune métrique n'apparaît dans InfluxDB
- Pas de données dans les tableaux de bord Grafana
- La page d'état d'InfluxDB affiche des comptes nuls ou faibles

Étapes de Diagnostic :

1. Vérifiez que le Dispositif est Associé

Interface Web → Stations de Base :

- Le statut du dispositif est-il vert ?
- L'horodatage du dernier contact est-il récent ?
- La session est-elle active ?

2. Vérifiez la Connexion à InfluxDB

Interface Web → État d'InfluxDB :

- Le statut de connexion est-il vert ?
- RAN Monitor peut-il écrire dans InfluxDB ?

Testez la connectivité :

```
# Depuis le serveur RAN Monitor
curl http://<influxdb-host>:8086/ping
```

3. Vérifiez les Journaux d'Application

Recherchez :

- `[error] InfluxDB write failed` → Problème de connexion ou de permission
- `[error] Failed to collect metrics` → Problème de communication avec le dispositif
- `[info] Metrics collected: 0` → Le dispositif ne renvoie pas de données

4. Vérifiez InfluxDB Directement

Interrogez InfluxDB pour des données récentes :

```
# InfluxDB 1.x
influx -database 'nokia-monitor' -execute '
  SELECT COUNT(*) FROM PerformanceMetrics
  WHERE basebandName='''Site-A-BS1'''
  AND time > now() - 1h
'

# InfluxDB 2.x
influx query 'from(bucket:"nokia-monitor")
  |> range(start: -1h)
  |> filter(fn: (r) => r.basebandName == "Site-A-BS1")
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> count()'
```

Solutions :

Problème de Connexion à InfluxDB :

1. Vérifiez qu'InfluxDB est en cours d'exécution
2. Vérifiez `config/runtime.exs` pour :
    - Adresse hôte

    - Port (8086)
    - Nom de la base de données/bucket
    - Identifiants/token API
3. Testez la connectivité depuis le serveur RAN Monitor
4. Vérifiez que le pare-feu autorise le port 8086
5. Redémarrez RAN Monitor après avoir corrigé la configuration

Problème de Permission InfluxDB :

1. Vérifiez que les identifiants ont la permission d'écriture dans le bucket/base de données
2. Vérifiez les journaux d'InfluxDB pour des erreurs d'authentification
3. Recréez le token API avec les permissions appropriées
4. Mettez à jour `config/runtime.exs` avec le nouveau token
5. Redémarrez RAN Monitor

InfluxDB Plein :

1. Vérifiez l'espace disque : `df -h`
2. Passez en revue les politiques de rétention
3. Nettoyez les anciennes données ou augmentez le stockage
4. Consultez le Guide de Politique de Rétention des Données

Le Dispositif Ne Renvoie Pas de Données :

1. Vérifiez que le dispositif est configuré pour envoyer des métriques
2. Vérifiez que l'URL du webhook est correcte dans la configuration du dispositif
3. Vérifiez les journaux du dispositif pour des erreurs
4. Vérifiez que le récepteur de webhook de RAN Monitor fonctionne (port 9076)

Problèmes de Collecte de Données

Problème : Lacunes dans les Données Historiques

Symptômes :

- Les tableaux de bord Grafana montrent des lacunes dans les séries temporelles
- Points de données manquants pour certaines périodes
- Les requêtes InfluxDB retournent des résultats incomplets

Étapes de Diagnostic :

1. Vérifiez le Temps de Fonctionnement de l'Application

Y a-t-il eu des interruptions de service pendant la période de lacune ?

```
# Vérifiez les journaux système pour les redémarrages
journalctl -u ran_monitor --since "2025-12-29" --until "2025-12-30"
```

2. Vérifiez l'Historique de Connectivité du Dispositif

Interface Web → Stations de Base → Dispositif → Passez en revue l'historique "Dernier Contact"

- Le dispositif était-il connecté pendant la période de lacune ?
- Y a-t-il des problèmes de connectivité ?

3. Vérifiez la Disponibilité d'InfluxDB

Y a-t-il eu des pannes d'InfluxDB pendant la période de lacune ?

- Vérifiez les journaux d'InfluxDB
- Passez en revue l'historique de surveillance/alerte

Solutions :

Temps d'Arrêt de RAN Monitor :

- La lacune de données est normale pendant une interruption de service
- Les données historiques ne peuvent pas être remplies
- Documentez l'incident et rétablissez le service

Déconnexion du Dispositif :

- Enquêtez sur la raison de la déconnexion du dispositif
- Corrigez le problème de connectivité
- La lacune de données est normale pendant la déconnexion
- Les futures données reprendront la collecte

Panne d'InfluxDB :

- Les métriques ont probablement été collectées mais non stockées
- Vérifiez les journaux de RAN Monitor pour des échecs d'écriture
- Rétablissez le service InfluxDB
- La lacune de données ne peut pas être récupérée

Prévention :

- Mettez en œuvre une surveillance pour le temps de fonctionnement de RAN Monitor
- Configurez des alertes pour les déconnexions prolongées
- Surveillez la santé d'InfluxDB
- Envisagez une HA/redondance pour les systèmes critiques

Problèmes de l'Interface Web

Problème : Impossible d'Accéder à l'Interface Web

Symptômes :

- Le navigateur ne peut pas se connecter à https://<ran-monitor-ip>:9443
- Délai d'attente ou connexion refusée
- Erreurs de certificat SSL

Étapes de Diagnostic :

1. Vérifiez que l'Interface Web Fonctionne

Vérifiez les journaux d'application :

```
[info] Running ControlPanelWeb.Endpoint with cowboy
```

Vérifiez le processus :

```
ps aux | grep control_panel
netstat -tulpn | grep 9443
```

2. Testez la Connectivité

Depuis une autre machine :

```
telnet <ran-monitor-ip> 9443
```

Depuis le serveur RAN Monitor lui-même :

```
curl -k https://localhost:9443
```

3. Vérifiez le Pare-feu

```
# Vérifiez si le port est ouvert
sudo iptables -L -n | grep 9443

# Ou
sudo firewall-cmd --list-ports
```

Solutions :

Port Non Ouvert :

1. Ajoutez une règle de pare-feu :

```
sudo firewall-cmd --add-port=9443/tcp --permanent
sudo firewall-cmd --reload
```

2. Testez l'accès à nouveau

Interface Web Non Démarrée :

1. Vérifiez `config/runtime.exs` pour la configuration du point de terminaison web
2. Vérifiez que les fichiers de certificat SSL existent
3. Vérifiez les journaux d'application pour des erreurs de démarrage
4. Redémarrez RAN Monitor

Problèmes de Certificat SSL :

1. Vérifiez que les fichiers de certificat existent et sont lisibles :

```
ls -l priv/cert/omnitouch.pem
ls -l priv/cert/omnitouch.crt
```

2. Vérifiez la validité du certificat :

```
openssl x509 -in priv/cert/omnitouch.crt -text -noout
```

3. Régénérez si expiré ou manquant
4. Redémarrez RAN Monitor

Mauvais Port :

1. Vérifiez `config/runtime.exs` pour le port configuré
2. Utilisez le bon port dans le navigateur
3. Ou définissez la variable d'environnement `CONTROL_PANEL_HTTPS_PORT`

Problème : L'Interface Web Charge Mais N'affiche Aucune Donnée

Symptômes :

- L'interface Web est accessible
- Les pages se chargent mais affichent des listes vides ou des comptes nuls
- Le tableau de bord ne montre aucun dispositif

Étapes de Diagnostic :

1. Vérifiez la Configuration du Dispositif

Y a-t-il quelque chose configuré dans `config/runtime.exs` ?

```
airscales: [
  # Doit avoir au moins un dispositif
]
```

2. Vérifiez la Connexion à la Base de Données

Les dispositifs sont-ils stockés dans MySQL ?

```
mysql -u ran_monitor_user -p ran_monitor -e "SELECT * FROM
airscales;"
```

3. Vérifiez les Journaux d'Application

Recherchez des erreurs de connexion à la base de données ou des échecs de requête.

Solutions :

Aucun Dispositif Configuré :

1. Ajoutez des dispositifs à `config/runtime.exs`
2. Redémarrez RAN Monitor
3. Les dispositifs devraient apparaître dans l'interface Web

Problème de Connexion à la Base de Données :

1. Vérifiez que MySQL est en cours d'exécution
2. Vérifiez la configuration de connexion dans `config/runtime.exs`
3. Testez la connexion à la base de données
4. Redémarrez RAN Monitor

Problèmes de Base de Données

Problème : Erreurs de Connexion MySQL

Symptômes :

- Les journaux d'application montrent des erreurs de connexion à la base de données
- L'interface Web affiche des erreurs lors du chargement des pages
- Messages "Délai d'attente de connexion à la base de données"

Étapes de Diagnostic :

1. Vérifiez que MySQL est en Cours d'Exécution

```
systemctl status mysql
# ou
systemctl status mariadb
```

2. Testez la Connexion

Depuis le serveur RAN Monitor :

```
mysql -h <mysql-host> -u <username> -p <database>
```

3. Vérifiez la Configuration

Dans `config/runtime.exs` :

```
config :ran_monitor, RanMonitor.Repo,
  username: "ran_monitor_user",
  password: "password",
  hostname: "localhost",
  database: "ran_monitor",
  pool_size: 10
```

Solutions :

MySQL Non Démarré :

1. Démarrez le service MySQL :
   ```
   systemctl start mysql
   ```
2. Vérifiez qu'il démarre correctement
3. RAN Monitor se reconnectera automatiquement

Erreur de Configuration de Connexion :

1. Vérifiez le nom d'hôte, le nom d'utilisateur, le mot de passe, le nom de la base de données
2. Testez la connexion manuellement
3. Mettez à jour `config/runtime.exs` si incorrect
4. Redémarrez RAN Monitor

Problème Réseau :

1. Vérifiez la connectivité réseau vers le serveur MySQL
2. Vérifiez que le pare-feu autorise le port 3306
3. Vérifiez l'adresse de liaison de MySQL (doit permettre les connexions distantes si nécessaire)

Trop de Connexions :

1. Vérifiez le paramètre max_connections de MySQL
2. Réduisez pool_size dans la configuration si nécessaire
3. Redémarrez RAN Monitor

Problèmes de Performance

Problème : Utilisation Élevée du CPU ou de la Mémoire

Symptômes :

- RAN Monitor utilise un CPU ou une RAM excessive
- Le système devient lent ou non réactif
- Les connexions à la base de données expirent
- Temps de réponse dégradé

Étapes de Diagnostic :

1. Vérifiez l'Utilisation des Ressources

```
# CPU et mémoire
top -p $(pgrep -f ran_monitor)

# Informations détaillées sur le processus
ps aux | grep ran_monitor
```

2. Vérifiez le Nombre de Dispositifs Surveillés

Combien de dispositifs sont configurés ?

- Plus de dispositifs = plus de ressources nécessaires
- Vérifiez si le nombre de dispositifs a récemment augmenté

3. Vérifiez les Intervalles de Collecte

Les intervalles de sondage sont-ils très fréquents ?

- Plus fréquent = plus d'utilisation du CPU/réseau
- La valeur par défaut est de 10 secondes pour les métriques

4. Vérifiez la Taille du Pool de Base de Données

Dans `config/runtime.exs` :

```
pool_size: 10  # Peut nécessiter un ajustement
```

Solutions :

Trop de Dispositifs pour les Ressources :

1. Surveillez les tendances d'utilisation des ressources
2. Augmentez les ressources du serveur (CPU/RAM)
3. Ou réduisez le nombre de dispositifs surveillés
4. Envisagez de mettre à l'échelle horizontalement (plusieurs instances)

Pool de Base de Données Trop Grand :

1. Réduisez pool_size dans la configuration
2. Règle générale : 2 connexions par dispositif + 5 pour l'interface Web
3. Redémarrez RAN Monitor
4. Surveillez l'utilisation des ressources

Fuite de Mémoire :

1. Surveillez l'utilisation de la mémoire au fil du temps
2. Si elle augmente continuellement, il peut s'agir d'une fuite de mémoire
3. Redémarrez RAN Monitor comme solution temporaire
4. Signalez le problème avec les journaux et les métriques

Performance d'Écriture d'InfluxDB :

1. Vérifiez l'utilisation des ressources d'InfluxDB
2. Vérifiez qu'InfluxDB n'est pas un goulot d'étranglement
3. Envisagez un serveur InfluxDB séparé
4. Passez en revue les politiques de rétention pour réduire le volume de données

---

Problème : Réponse Lente de l'Interface Web

Symptômes :

- L'interface Web prend beaucoup de temps à charger les pages
- Le tableau de bord est lent
- Délai d'attente lors de la consultation des détails du dispositif

Étapes de Diagnostic :

1. Vérifiez les Ressources du Serveur

Le serveur RAN Monitor est-il surchargé ?

```
top
free -h
df -h
```

2. Vérifiez la Performance de la Base de Données

Les requêtes de base de données sont-elles lentes ?

```
# Journal des requêtes lentes de MySQL
mysql -u root -p -e "SHOW VARIABLES LIKE 'slow_query_log%';"
```

3. Vérifiez la Latence Réseau

Y a-t-il une latence élev��e vers la base de données ou les clients ?

Solutions :

Problème de Ressources Serveur :

1. Réduisez la charge sur le serveur
2. Augmentez les ressources du serveur
3. Déplacez les bases de données vers des serveurs séparés

Performance de la Base de Données :

1. Optimisez la configuration de MySQL
2. Ajoutez des index si nécessaire (les tables devraient en avoir)
3. Augmentez les ressources du serveur de base de données

Latence Réseau :

1. Enquêtez sur le chemin réseau
2. Envisagez de rapprocher les composants
3. Utilisez une base de données locale si possible

Problèmes d'Alarme

Problème : Alarmes Non Apparentes

Symptômes :

- Des défauts connus n'apparaissent pas dans la page des Alarmes
- Le compte des alarmes est nul alors que des défauts existent
- Notifications d'alarme retardées

Étapes de Diagnostic :

1. Vérifiez que le Dispositif Envoie des Alarmes

Vérifiez dans l'interface de gestion du dispositif que les alarmes sont configurées pour être envoyées.

2. Vérifiez le Récepteur de Webhook

Le point de terminaison du webhook fonctionne-t-il ?

```
netstat -tulpn | grep 9076
```

Recherchez :

```
tcp  0  0.0.0.0:9076  0.0.0.0:*  LISTEN
```

3. Vérifiez la Configuration du Webhook

Dans la configuration du dispositif, vérifiez que l'URL du webhook pointe vers RAN Monitor :

```
http://<ran-monitor-ip>:9076/webhook
```

4. Vérifiez les Journaux d'Application

Recherchez des erreurs de récepteur de webhook ou des échecs d'analyse d'alarme.

5. Vérifiez InfluxDB

Les alarmes sont-elles écrites ?

```
influx -database 'nokia-monitor' -execute '
  SELECT COUNT(*) FROM Alarms WHERE time > now() - 1h
'
```

Solutions :

Récepteur de Webhook Non Fonctionnel :

1. Vérifiez `config/runtime.exs` pour la configuration du point de terminaison du webhook
2. Vérifiez que le port 9076 est configuré
3. Redémarrez RAN Monitor
4. Vérifiez que le port écoute

Dispositif Non Envoyant :

1. Configurez le dispositif pour envoyer des notifications d'alarme
2. Vérifiez l'URL du webhook dans la configuration du dispositif
3. Testez la génération d'alarme sur le dispositif

Pare-feu Bloquant :

1. Vérifiez que le dispositif peut atteindre le port 9076 de RAN Monitor
2. Ajoutez une règle de pare-feu si nécessaire
3. Testez la connectivité : `telnet <ran-monitor-ip> 9076` depuis le réseau du dispositif

Échec d'Écriture dans InfluxDB :

1. Vérifiez la connexion à InfluxDB
2. Vérifiez les permissions d'écriture
3. Vérifiez la capacité de stockage d'InfluxDB
4. Passez en revue les journaux d'application pour des erreurs d'écriture

---

Outils de Diagnostic

Journaux d'Application

Accéder via l'Interface Web :

1. Accédez à la page des Journaux d'Application
2. Filtrer par niveau de journal
3. Rechercher des mots-clés
4. Mettre en pause pour examiner des erreurs spécifiques

Accéder via la Ligne de Commande :

Si exécuté en tant que service systemd :

```
journalctl -u ran_monitor -f
```

Si exécuté via mix :

- Les journaux apparaissent dans la sortie de la console

Niveaux de Journal :

- Urgence/Alerte/Critique - Problèmes critiques pour le système
- Erreur - Erreurs nécessitant une attention
- Avertissement - Problèmes potentiels
- Info - Messages opérationnels normaux
- Débogage - Informations de diagnostic détaillées

Termes de Recherche Utiles :

- Nom du dispositif (par exemple, "Site-A-BS1")
- "error" ou "failed"
- "InfluxDB" ou "MySQL"
- "registration" ou "session"

Requêtes InfluxDB

Requête pour des métriques récentes :

```
influx -database 'nokia-monitor' -execute '
  SELECT * FROM PerformanceMetrics
  WHERE basebandName='''Site-A-BS1'''
  AND time > now() - 5m
  LIMIT 10
'
```

Compter les métriques par dispositif :

```
influx -database 'nokia-monitor' -execute '
  SELECT COUNT(*) FROM PerformanceMetrics
  GROUP BY basebandName
'
```

Requête pour les alarmes :

```
influx -database 'nokia-monitor' -execute '
  SELECT * FROM Alarms
  WHERE time > now() - 1h
'
```

Requêtes MySQL

Vérifiez les dispositifs configurés :

```
SELECT name, address, port, registration_status
FROM airscales;
```

Vérifiez les erreurs dans la base de données :

```
mysql -u ran_monitor_user -p ran_monitor -e "SHOW PROCESSLIST;"
```

Diagnostics Réseau

Testez la connectivité :

```
# Connectivité de base
ping <device-ip>

# Accessibilité du port
telnet <device-ip> 8080
nc -zv <device-ip> 8080

# Trace de route
traceroute <device-ip>
```

Vérifiez le pare-feu :

```
# Liste des règles
sudo iptables -L -n -v

# Vérifiez un port spécifique
sudo iptables -L -n | grep 8080
```

Obtenir de l'Aide

Avant de Contacter le Support

Rassemblez les informations suivantes :

1. Description du Problème

- Qu'est-ce qui ne fonctionne pas ?
- Quand cela a-t-il commencé ?
- Qu'est-ce qui a changé récemment ?

2. Messages d'Erreur

- Copiez les messages d'erreur exacts des journaux
- Incluez les horodatages
- Notez la fréquence des erreurs

3. Informations Système

- Version de RAN Monitor
- Système d'exploitation et version
- Versions de la base de données (MySQL, InfluxDB)
- Nombre de dispositifs surveillés

4. Résultats de Diagnostic

- Résultats des étapes de diagnostic ci-dessus
- Extraits de journaux pertinents

- Configuration (sanitisez les mots de passe)

5. Impact

- Combien de dispositifs sont affectés ?
- Cela bloque-t-il les opérations ?
- Quel est l'impact sur l'entreprise ?

Ressources Documentaires

- **Guide de l'Interface Web** - Référence du panneau de contrôle
- **Guide des Opérations Courantes** - Tâches de routine
- **Guide de Configuration d'Exécution** - Détails de configuration
- **Guide d'Intégration Grafana** - Configuration d'analytique
- **Guide de Gestion des Alarmes** - Gestion des alarmes
- **Guide de Politique de Rétention des Données** - Gestion des données
- **Guide des Opérations** - Vue d'ensemble complète

Ressources Autonomes

Vérifiez d'abord les Journaux :

- Page des Journaux d'Application dans l'interface Web
- Journaux système : `journalctl -u ran_monitor`
- Journaux de la base de données

Passez en Revue les Changements Récents :

- Modifications des fichiers de configuration
- Ajouts/suppressions de dispositifs
- Changements réseau
- Mises à jour logicielles

Testez la Fonctionnalité de Base :

- Pouvez-vous accéder à l'interface Web ?
- Les dispositifs apparaissent-ils comme connectés ?

- InfluxDB est-il accessible ?
- Les métriques circulent-elles ?

Escalade

Si vous ne pouvez pas résoudre le problème :

1. Documentez toutes les étapes de diagnostic effectuées
2. Rassemblez les informations énumérées ci-dessus
3. Contactez le support Omnitouch avec les détails
4. Soyez prêt à fournir :
    - Fichiers de configuration (sanitisés)
    - Extraits de journaux
    - Captures d'écran si pertinent
    - Étapes pour reproduire

Documentation Connexe

- **Guide des Opérations** - Vue d'ensemble opérationnelle complète
- **Guide de l'Interface Web** - Guide utilisateur du panneau de contrôle
- **Guide des Opérations Courantes** - Tâches quotidiennes
- **Guide de Gestion des Alarmes** - Procédures de gestion des alarmes
- **Guide de Configuration d'Exécution** - Référence de configuration
- **Guide d'Intégration Grafana** - Analytique et tableaux de bord
- **Guide de Politique de Rétention des Données** - Gestion du cycle de vie des données

Guide de l'interface utilisateur Web

Panneau de contrôle RAN Monitor - Référence de l'interface utilisateur

Guide complet pour utiliser le panneau de contrôle basé sur le web RAN Monitor

---

Table des matières

1. Aperçu
2. Accéder à l'interface utilisateur Web
3. Tableau de bord principal
4. Page des stations de base
5. Vue des détails de l'appareil
6. Page des alarmes
7. Gestion de la configuration
8. Page des eNodeBs non configurés
9. Page des journaux d'application
10. Page de la politique de conservation des données
11. Page d'état d'InfluxDB
12. Page des métriques système
13. Page de collecte de données PM
14. Page de gestion du firmware
15. Page de gestion des données
16. Flux de travail de l'interface utilisateur Web

Documentation connexe

- **Guide de gestion du firmware** - Documentation complète du référentiel de firmware

Aperçu

RAN Monitor comprend un panneau de contrôle basé sur le web pour la surveillance et la gestion opérationnelle en temps réel. L'interface utilisateur Web offre une visibilité immédiate sur l'état des appareils, les alarmes, la configuration et la santé du système.

Interface utilisateur Web vs. Grafana

L'interface utilisateur Web est idéale pour :

- Vérifications immédiates de l'état des appareils
- Surveillance des alarmes en temps réel
- Gestion de la configuration
- Dépannage des sessions
- Administration système

Grafana est idéal pour :

- Analyse des tendances historiques
- Tableaux de bord KPI personnalisés
- Planification de capacité à long terme
- Identification de motifs
- Rapports exécutifs

Pour les tableaux de bord et analyses Grafana, consultez le Guide d'intégration Grafana.

Accéder à l'interface utilisateur Web

Le panneau de contrôle est accessible via HTTPS :

URL : `https://<ran-monitor-ip>:9443`

Port par défaut : 9443 (configurable via la variable d'environnement `CONTROL_PANEL_HTTPS_PORT`)

Certificats SSL :

- Les certificats auto-signés fonctionnent pour les environnements de laboratoire
- La production doit utiliser des certificats signés par une autorité de certification
- Certificats configurés dans `config/runtime.exs`

Pour les détails de configuration, consultez le Guide de configuration d'exécution.

Actualisation automatique : La plupart des pages se rafraîchissent automatiquement toutes les 5 secondes pour afficher des données en temps réel.

Tableau de bord principal

Le tableau de bord fournit une vue d'ensemble de votre infrastructure RAN.

Sections clés

État du système

- Indicateurs de santé globaux
- Disponibilité et connectivité du système

Résumé des appareils

- Nombre d'appareils associés/échoués
- Vue d'ensemble de l'état d'enregistrement
- Instantané rapide de la santé des appareils

Alarmes actives

- Nombre actuel de pannes par gravité
- Niveaux de gravité codés par couleur (Critique, Majeur, Mineur, Avertissement)
- Liens rapides vers les détails des alarmes

Activité récente

- Derniers événements et changements
- Mises à jour de configuration
- Changements d'état de session

Fonctionnalités

- Actualisations automatiques toutes les 5 secondes
- Indicateurs d'état codés par couleur (vert = sain, rouge = problèmes)
- Navigation par clic vers des vues détaillées
- Mises à jour des métriques en temps réel

Page des stations de base

Voir tous les appareils gérés avec leur état actuel et les informations de session.

URL : `https://<ran-monitor-ip>:9443/nokia/enodeb`

La page d'état des BTS montrant la liste des appareils avec l'état de connexion, l'état de session et les boutons d'action.

Résumé des statistiques

La barre supérieure montre les comptes d'appareils agrégés :

Statistique	Description
Total des sites	Nombre de stations de base configurées
Connecté	Sites avec des sessions actives qui ont envoyé à la fois des données de configuration et des données PM depuis le dernier redémarrage
En attente	Sites qui sont enregistrés mais qui n'ont pas encore envoyé tous les types de données
Déconnecté	Sites qui ne sont pas enregistrés ou inaccessibles

Tableau des appareils

Colonne	Description
Nom	Nom du site tel que configuré
État	État de connexion (voir ci-dessous)
Adresse	Adresse IP de l'appareil et port
Session	État de la session : "Active" (vert) ou "Aucune" (gris)
Actions	Boutons d'action de l'appareil

États de statut

Statut	Icône	Description
Connecté		Enregistré, session active, à la fois les données de configuration et les données PM reçues depuis le dernier redémarrage
En attente de données PM		Session active et configuration reçue, mais pas encore de données PM (le cycle PM de l'eNodeB est généralement toutes les 15 minutes)
Session active		Enregistré avec une session active, en attente de l'envoi initial de données
Enregistrement		Enregistrement NE3S en cours
Déconnecté		Non enregistré ou inaccessibilité

Boutons d'action

Chaque ligne d'appareil a des boutons d'action :

Bouton	Description
Ping	Tester la connectivité réseau à l'appareil
Config	Voir la configuration actuelle de l'appareil
Config Ops	Accéder aux opérations de gestion de configuration (télécharger, télécharger, valider, activer)
Force Retry	Forcer une tentative de réenregistrement pour les appareils déconnectés

Panneau des détails de l'appareil

Cliquer sur une ligne d'appareil affiche des détails supplémentaires :

Champ	Description
ID du gestionnaire	Identifiant interne du gestionnaire
ID de session	Identifiant de session actuel
Type d'agent	Type d'agent de l'appareil (par exemple, COMA)
Fournisseur	Fournisseur de l'appareil (Nokia)

Filtrage et recherche

- Filtrer par état de connexion
- Rechercher par nom d'appareil ou adresse IP
- Trier par n'importe quelle colonne

Vue des détails de l'appareil

Cliquez sur n'importe quel appareil de la page des stations de base pour voir des informations complètes.

Détails d'enregistrement

- Identité du gestionnaire et état d'authentification
- Horodatage d'enregistrement
- Informations d'authentification utilisées
- Clés et certificats du gestionnaire

Cycle de vie de la session

- Heure de création de la session
- Heure d'expiration de la session
- Intervalle et état de maintien en vie
- Dernier horodatage de maintien en vie
- Temps restant jusqu'à l'expiration

Métriques récentes

- Derniers instantanés de données de performance
- Valeurs de compteur et horodatages
- État de collecte des métriques
- Intervalles de collecte de données

Alarmes actives

- Pannes actuelles pour cet appareil spécifique
- Gravité et description des alarmes
- Horodatages des alarmes
- Informations sur la cause probable

État de configuration

- Valeurs des paramètres actuels
- Changements récents de configuration
- Horodatage de configuration
- Historique des changements de paramètres

Page des alarmes

Surveillez toutes les pannes de votre réseau dans une vue centralisée.

Informations sur les alarmes

Niveaux de gravité :

- **Critique** (Rouge) - Affectant le service, action immédiate requise
- **Majeur** (Orange) - Dégradation significative, attention urgente nécessaire
- **Mineur** (Jaune) - Non affectant le service, doit être traité
- **Avertissement** (Bleu) - Informatif, surveiller les tendances
- **Résolu** (Vert) - Alarme précédemment active a été résolue

Détails de l'alarme :

- Description du problème
- Cause probable
- Système affecté (DN - Nom Distingué)
- Horodatages (quand l'alarme s'est produite et dernière mise à jour)

Fonctionnalités

Codage couleur :

- Identification visuelle immédiate de la gravité
- Rouge = Alarmes critiques

- Orange = Alarmes majeures
- Jaune = Alarmes mineures
- Bleu = Avertissements
- Vert = Résolu

Tri et filtrage :

- Trier par gravité, appareil ou temps
- Filtrer par type d'alarme
- Rechercher des problèmes spécifiques

Liens vers les appareils :

- Cliquez sur l'alarme pour voir les détails de l'appareil affecté
- Croiser avec les métriques de l'appareil
- Naviguer vers la configuration de l'appareil

Pour des procédures détaillées de gestion des alarmes, consultez le Guide de gestion des alarmes.

Gestion de la configuration

L'interface utilisateur Web fournit des outils pour gérer les configurations des appareils de manière sûre et efficace.

Télécharger la configuration

Objectif : Récupérer et sauvegarder la configuration actuelle

Étapes :

1. Naviguer vers la page de détails de l'appareil
2. Cliquez sur "Télécharger la configuration"
3. La configuration est récupérée depuis l'appareil
4. Enregistrez la configuration en tant que fichier XML

Meilleure pratique : Toujours télécharger et sauvegarder la configuration avant de faire des changements

Pousser la configuration (Provision)

Objectif : Appliquer une nouvelle configuration à un appareil en une seule opération

L'opération de provisionnement effectue le téléchargement, la validation et l'activation de manière atomique sur l'appareil. Un retour à la configuration en cours d'exécution est automatiquement sauvegardé avant l'application de la nouvelle configuration.

Étapes :

1. Cliquez sur "Config Ops" sur l'appareil cible
2. Sélectionnez un fichier de configuration XML (glisser-déposer ou cliquez pour parcourir)
3. Cliquez sur "Pousser la configuration vers l'appareil"
4. L'appareil télécharge, valide et active la configuration
5. Surveillez le message de résultat pour le succès ou les erreurs

Comment cela fonctionne :

- L'appareil reçoit le fichier de configuration et crée un plan interne
- Le plan est validé par rapport au schéma de l'appareil et à l'état actuel
- Si la validation réussit, la configuration en cours d'exécution est sauvegardée comme retour
- La nouvelle configuration est activée immédiatement
- Si l'activation échoue, l'appareil peut revenir au retour

Avancé : Flux manuel en 3 étapes

Pour les cas où vous avez besoin de plus de contrôle (par exemple, mettre en scène une configuration pour révision avant activation), la section avancée dans la boîte de dialogue Config Ops fournit les étapes individuelles :

1. **Mettre en scène (Télécharger)** - Téléchargez la configuration pour créer un plan sur l'appareil sans activer. Retourne un ID de plan.
2. **Valider** - Validez un plan mis en scène par son ID de plan. Confirme que la configuration est syntaxiquement et sémantiquement correcte.
3. **Activer** - Appliquez un plan validé par son ID de plan. Prend effet immédiatement.

L'ID de plan de l'étape de mise en scène est automatiquement rempli dans les champs de validation et d'activation.

Flux de travail de configuration

Processus recommandé :

1. Télécharger la configuration actuelle (sauvegarde)
2. Modifier la configuration hors ligne
3. Pousser la nouvelle configuration en utilisant l'opération de provision
4. Vérifier que les changements ont pris effet
5. Surveiller l'appareil pour la stabilité

Pour des détails de configuration des stations de base, consultez le Guide de configuration AirScale.

Page des eNodeBs non configurés

Découvrez et gérez les stations de base tentant de se connecter qui ne sont pas encore configurées dans le système.

Objectif

La page des eNodeBs non configurés vous aide à :

- Découvrir de nouvelles stations de base sur le réseau
- Identifier les appareils tentant des connexions non autorisées
- Vérifier les identifiants des appareils avant de les ajouter à la configuration

- Suivre les tentatives de connexion d'équipements inconnus

Informations affichées

ID de l'agent

- Identifiant de l'appareil détecté lors des tentatives de connexion
- Utilisez cet ID lors de l'ajout de l'appareil à la configuration

Dernière vue

- Horodatage de la dernière tentative de connexion
- Aide à identifier les appareils actifs vs inactifs

Occurrences

- Nombre de fois que l'appareil a tenté de se connecter
- Des tentatives fréquentes peuvent indiquer une mauvaise configuration

Première vue

- Quand l'appareil a été détecté pour la première fois
- Utile pour suivre les nouveaux équipements

Actions disponibles

Rafraîchir

- Recharger la liste des appareils non configurés
- Met à jour les horodatages et les comptes d'occurrences

Supprimer

- Supprimer des entrées individuelles de la liste
- Utile pour nettoyer les appareils anciens/déclassés

Tout effacer

- Supprimer tous les enregistrements d'appareils non configurés

- Nouveau départ pour la liste

Aide à la configuration

Lorsque des appareils apparaissent ici, suivez ces étapes :

1. **Notez l'ID de l'agent** de la table
2. **Ajoutez la configuration de l'appareil** à `config/runtime.exs` :

```
airscales: [
  %{
    address: "10.7.15.66",
    name: "Site-A-BS1",
    port: "8080",
    web_username: "admin",
    web_password: "password"
  }
]
```

3. **Redémarrez RAN Monitor** pour commencer à surveiller l'appareil

Pour des instructions de configuration détaillées, consultez le Guide de configuration d'exécution.

Cas d'utilisation

- **Découverte de réseau :** Trouver de nouvelles stations de base ajoutées au réseau
- **Sécurité :** Identifier les tentatives de connexion non autorisées
- **Provisionnement :** Vérifier les identifiants des appareils avant la configuration
- **Déclassement :** Suivre les tentatives d'appareils qui devraient être hors ligne

---

Page des journaux d'application

Tableau de bord de journalisation en temps réel pour le dépannage et la surveillance de l'activité du système.

Niveaux de journal

Filtrer par niveau de journal :

- **Urgent** - Pannes critiques pour le système
- **Alerte** - Action immédiate requise
- **Critique** - Conditions critiques
- **Erreur** - Conditions d'erreur
- **Avertissement** - Conditions d'avertissement
- **Notification** - Normal mais significatif
- **Info** - Messages informatifs
- **Débogage** - Informations détaillées de débogage

Remarque : Lors du filtrage, le niveau sélectionné et tous les niveaux de gravité supérieurs sont affichés.

Fonctionnalités

Recherche et filtrage :

- Recherche textuelle dans tous les messages de journal
- Diffusion de journaux en temps réel (derniers 500 messages)
- Filtrer par niveau de journal

Contrôles :

- **Pause/Reprendre** - Arrêter la diffusion en direct des journaux pour examiner les messages
- **Effacer** - Supprimer tous les journaux de l'affichage
- **Niveau système** - Changer dynamiquement le niveau de journalisation de l'application

Codage couleur :

- Rouge - Niveaux Urgent/Alerte/Critique
- Rouge clair - Niveau Erreur
- Jaune - Niveau Avertissement
- Cyan - Niveau Notification
- Bleu - Niveau Info
- Gris - Niveau Débogage

Cas d'utilisation

Dépanner les problèmes de connexion :

- Filtrer les erreurs provenant d'appareils spécifiques
- Rechercher des noms d'appareils ou des adresses IP
- Examiner les messages d'échec de connexion

Surveiller l'activité du système :

- Surveiller les journaux de niveau info pour les opérations normales
- Suivre les événements d'enregistrement des appareils
- Surveiller l'activité de collecte de données

Déboguer les problèmes :

- Définir temporairement le niveau de débogage
- Reproduire le problème
- Examiner les journaux détaillés
- Revenir au niveau info une fois terminé

Enquêter sur les pannes :

- Rechercher des messages d'erreur et des traces de pile
- Examiner les horodatages autour de l'heure de la panne
- Corréler avec les événements des appareils

Meilleures pratiques

- **Utiliser Pause** lors de l'examen de séquences d'erreur spécifiques
- **Définir le niveau de journal approprié :**
  - Info pour la production
  - Débogage pour le dépannage
  - Avertissement pour une production silencieuse
- **Rechercher efficacement** en utilisant des noms d'appareils ou des mots-clés d'erreur
- **Les changements de niveau de journal persistent** jusqu'au redémarrage de l'application

---

Page de la politique de conservation des données

Gérez combien de temps les données sont stockées dans InfluxDB pour chaque station de base.

Affichage des paramètres globaux

Période de conservation par défaut

- Politique de conservation à l'échelle du système en heures/jours
- Configuré dans `config/config.exs`
- Par défaut : 720 heures (30 jours)

Total des enregistrements

- Compte de tous les points de données à travers tous les appareils
- Mis à jour lors du rafraîchissement de la page

État de nettoyage automatique

- Montre les nettoyages effectués toutes les heures
- État du travail en arrière-plan

Paramètres par appareil

Pour chaque station de base configurée :

Informations sur l'appareil :

- Nom de l'appareil
- État d'enregistrement (Enregistré/Non enregistré)
- Paramètre de période de conservation actuel

Comptes d'enregistrements :

- **Métriques de performance** - Nombre de points de données PM stockés
- **Configuration** - Nombre de snapshots de configuration
- **Alarmes** - Nombre d'enregistrements d'alarmes
- **Total** - Somme de tous les enregistrements pour cet appareil

Actions :

- **Mettre à jour la période de conservation** - Changer les heures de conservation (s'applique uniquement à cet appareil)
- **Nettoyer les anciennes données** - Déclencher manuellement le nettoyage en fonction de la période de conservation
- **Effacer toutes les données** - Supprimer toutes les données pour cet appareil (irréversible)

Comment fonctionne la conservation

1. **Par défaut global** - Défini dans le fichier de configuration, s'applique à tous les appareils
2. **Remplacement par appareil** - Optionnellement définir une conservation personnalisée pour des appareils spécifiques
3. **Nettoyage automatique** - S'exécute toutes les heures, supprime les données plus anciennes que la période de conservation
4. **Nettoyage manuel** - Utilisez "Nettoyer les anciennes données" pour forcer un nettoyage immédiat

Périodes de conservation courantes

- **720 heures (30 jours)** - Surveillance opérationnelle à court terme
- **2160 heures (90 jours)** - Conservation standard pour la plupart des déploiements
- **4320 heures (180 jours)** - Conservation prolongée pour conformité
- **8760 heures (365 jours)** - Analyse historique à long terme

Cas d'utilisation

- Réduire l'utilisation de stockage en abaissant la période de conservation
- Conserver les données critiques des appareils plus longtemps que d'autres
- Nettoyer les données de test avant la production
- Gérer l'utilisation de l'espace disque d'InfluxDB

Avertissement : Effacer toutes les données est permanent et ne peut pas être annulé. Vérifiez toujours avant d'exécuter.

Pour des informations détaillées sur la politique de conservation, consultez le Guide de la politique de conservation des données.

Page d'état d'InfluxDB

Surveillez la santé et l'état de votre base de données de séries temporelles InfluxDB.

URL : `https://<ran-monitor-ip>:9443/nokia/influx`

La page d'état d'InfluxDB montrant l'état de connexion, les mesures, les performances de l'écrivain par lot et les informations de stockage.

État de connexion

Champ	Description
État de connexion	Indicateur vert lorsque connecté, rouge lorsque déconnecté
Base de données	Nom de bucket InfluxDB configuré
Version d'InfluxDB	Version de base de données détectée (2.x)

Mesures et points de données

Comptes de points de données en temps réel pour chaque type de mesure :

Mesure	Description
Métriques de performance	Points de données PM collectés à partir des appareils
Configuration	Snapshots de configuration stockés
Alarmes	Enregistrements d'alarmes dans la base de données
Total	Somme de tous les points de données

Performances de l'écrivain par lot

Statistiques pour le processus d'écrivain par lot d'InfluxDB qui gère toute l'ingestion de données :

Métrique	Description
Taille de la file d'attente	Points en attente d'écriture. Codé par couleur : vert (< 1000), jaune (< 10000), orange (< 20000), rouge (>= 20000)
Taux de filtrage	Pourcentage de points de données en double bloqués de l'écriture
PM filtré	Compte des compteurs PM filtrés (compteurs non tableau de bord non dans la liste des données PM stockées)
Chutes de file d'attente	Points abandonnés en raison d'un débordement de file d'attente (devrait être 0 en fonctionnement normal)
Cache de configuration	Nombre de hachages de configuration uniques mis en cache pour la détection de delta
Cache d'alarmes	Nombre d'alarmes actives mises en cache pour la détection de delta

Métriques supplémentaires :

Métrique	Description
Total écrit	Points cumulés écrits dans InfluxDB depuis le démarrage
Flushes	Nombre d'opérations de vidage par lot
Filtré	Total des points en double filtrés (non écrits)
Données écrites	Total des octets écrits dans InfluxDB
Débit	Débit d'écriture actuel (Ko/s ou Mo/s)
Uptime de l'écrivain	Temps écoulé depuis le démarrage de l'écrivain par lot
Dernier vidage	Temps écoulé depuis le dernier vidage réussi

Effacer les caches : Réinitialise les caches de détection de delta. Utilisez lorsque vous souhaitez forcer la réécriture de toutes les données (par exemple, après des changements de schéma).

Informations de stockage

Champ	Description
Politiques de conservation	Paramètres de conservation actuels (par défaut : Indéfini)
Utilisation du disque	Taille estimée de la base de données basée sur les comptes d'enregistrements
Activité	Horodatage de la dernière mise à jour

Détails de configuration

Champ	Description
Hôte	Nom d'hôte du serveur InfluxDB
Port	Port du serveur InfluxDB (par défaut : 8086)
Bucket	Nom de bucket InfluxDB
État	Badge d'état de connexion
Mesures	Nombre de types de mesures (3 : PerformanceMetrics, Configuration, Alarms)

Diagnostics de santé

Indicateurs d'état pour la santé du système :

- **Connectivité InfluxDB** - Base de données accessible et répondant
- **Collecte de données** - Métriques de performance collectées à partir des appareils
- **Conservation des données** - État actuel de la politique de conservation
- **Dernière synchronisation** - La synchronisation des données la plus récente

Actualisation automatique

La page se rafraîchit automatiquement toutes les 30 secondes.

Interprétation de l'état

Condition	Signification
Connecté + Comptes de données croissants	Système fonctionnant normalement
Connecté + Pas de données	Vérifiez l'enregistrement de l'appareil et la configuration des compteurs PM
Déconnecté	Vérifiez qu'InfluxDB fonctionne et la connectivité réseau
Taille de file d'attente élevée (jaune/rouge)	Problème de performance d'écriture InfluxDB ou latence réseau
Chutes de file d'attente élevées	Débordement de file d'attente - augmentez la taille du lot ou réduisez le taux de collecte
Taux de filtrage élevé	Bon - indique une détection efficace des doublons

Cas d'utilisation

- Vérifiez qu'InfluxDB reçoit des données
- Surveillez la santé et le débit de l'écrivain par lot
- Dépannez les problèmes de performance d'écriture
- Vérifiez l'efficacité du cache de détection de delta
- Confirmez que les données sont écrites

Page des métriques système

Surveillance de performance en temps réel pour l'écrivain par lot d'InfluxDB et les ressources système.

URL : `https://<ran-monitor-ip>:9443/nokia/metrics`

La page des métriques système montrant les statistiques de l'écrivain par lot d'InfluxDB et les comptes d'écriture par Airscale.

Écrivain par lot d'InfluxDB

Statistiques récapitulatives pour le processus d'écrivain par lot :

Métrique	Description
Taille de la file d'attente	Nombre de points de données en attente d'écriture dans InfluxDB
Nombre de vidages	Nombre total de vidages par lot depuis le démarrage
Total des points écrits	Points de données cumulés écrits dans InfluxDB
Dernier vidage	Temps écoulé depuis la dernière opération de vidage réussie

Statistiques d'écriture InfluxDB par Airscale

Répartition par appareil des données écrites dans InfluxDB :

Colonne	Description
Airscale	Nom de l'appareil
Métriques de performance	Compte des points de données PM écrits
Configuration	Compte des snapshots de configuration écrits
Alarmes	Compte des enregistrements d'alarmes écrits
Total des enregistrements	Somme de tous les points de données pour cet appareil
Dernière écriture	Horodatage de la dernière écriture pour cet appareil

La ligne des totaux en bas montre les comptes agrégés à travers tous les appareils.

Ressources système

Utilisation des ressources de la VM Erlang :

Métrique	Description
Mémoire totale	Mémoire totale allouée à la VM Erlang
Mémoire des processus	Mémoire utilisée par les processus Erlang
Mémoire binaire	Mémoire utilisée pour les données binaires (charges XML, JSON)
Mémoire des atomes	Mémoire utilisée pour les atomes
Nombre de processus	Nombre de processus Erlang actifs
File d'attente d'exécution	Nombre de processus en attente de temps CPU (0 est sain)

Actualisation automatique

La page se rafraîchit automatiquement toutes les 5 secondes.

Cas d'utilisation

- Surveillez la santé et le débit de l'écrivain par lot
- Identifiez les appareils avec un volume de données élevé
- Dépannez les problèmes de performance d'écriture
- Vérifiez que les données circulent depuis tous les appareils
- Surveillez l'utilisation des ressources système

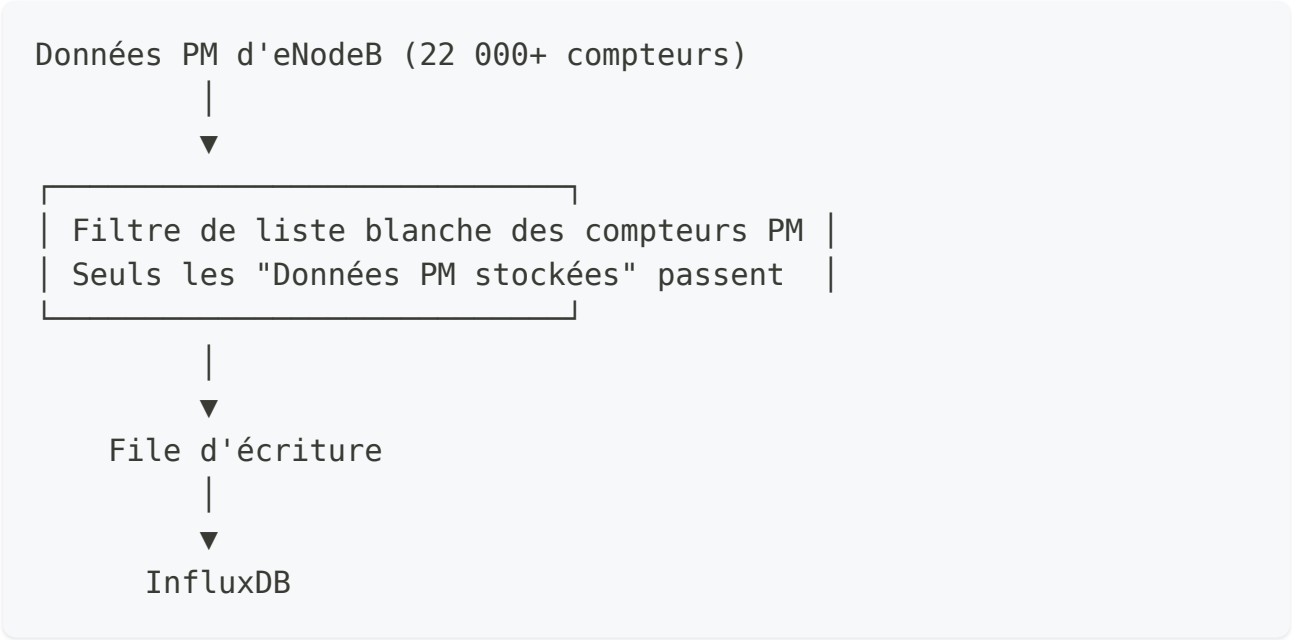
Page de collecte de données PM

Contrôlez quels compteurs de métriques de performance (PM) sont stockés dans InfluxDB. Les stations de base Nokia AirScale rapportent plus de 22 000 compteurs PM uniques, mais seuls un sous-ensemble est généralement nécessaire pour les tableaux de bord.

URL : `https://<ran-monitor-ip>:9443/nokia/pm-filters`

La page de collecte de données PM montrant les compteurs stockés (à gauche) et les compteurs disponibles (à droite) avec des filtres de catégorie.

Comment fonctionne le filtrage PM



L'écrivain par lot filtre les données PM entrantes par rapport à la liste des "Données PM stockées". Les compteurs non présents dans cette liste sont abandonnés avant la mise en file d'attente, réduisant le stockage et améliorant les performances des requêtes.

Mise en page de l'interface

Section	Description
Données PM stockées (Gauche)	Compteurs actuellement collectés et écrits dans InfluxDB
Compteurs disponibles (Droite)	Tous les 22 000+ compteurs disponibles à ajouter
Clés de configuration (Bas)	Paramètres de configuration suivis (depuis `config_keys.csv`)

Panneau des données PM stockées

Les compteurs de cette liste sont écrits dans InfluxDB lorsqu'ils sont reçus des appareils.

Filtres :

- **Recherche** : Filtrer par ID de compteur ou description
- **Catégorie** : Filtrer par technologie (LTE, 5G-NR, etc.)
- **Source** : Filtrer par Défaut (depuis CSV) ou Ajouté (ajouté par l'utilisateur)

Actions :

- **Supprimer sélectionnés** : Arrêter de collecter les compteurs sélectionnés
- **Sélectionner tout** : Sélectionner tous les compteurs visibles
- **Réinitialiser aux valeurs par défaut** : Restaurer la liste originale depuis `pm_counters.csv`

Panneau des compteurs disponibles

Parcourez et ajoutez des compteurs depuis la référence complète de PM de Nokia.

Filtres :

- **Recherche** : Trouver des compteurs par ID ou mots-clés de description
- **Catégorie** : Filtrer par catégorie technologique

Actions :

- **Ajouter sélectionnés** : Commencer à collecter les compteurs sélectionnés
- **Sélectionner tout** : Sélectionner tous les compteurs visibles (limité à 200 affichés)

Catégories de compteurs

Catégorie	Préfixe de code	Description
LTE	M8xxx	Compteurs LTE L1/L2/L3
WCDMA	M5xxx	Compteurs 3G WCDMA
5G-NR	M55xxx	Compteurs 5G NR
5G-Mobilité	M51xxx	Métriques de mobilité 5G
5G-Commun	M40xxx	Compteurs communs 5G

Persistance

Les changements sont :

- **Persistés sur disque** dans `priv/pm_filters.etf`
- **Survivent aux redémarrages de l'application**
- **Prennent effet immédiatement** (aucun redémarrage requis)

Statistiques connexes

La page d'état d'InfluxDB montre les statistiques de filtrage :

- **PM Filtré** : Compte des points PM abandonnés (non dans la liste blanche)
- **Taux de filtrage** : Pourcentage de points de configuration/alarmes en double bloqués

Pour des conseils détaillés sur la sélection de compteurs, consultez le Guide de collecte de données PM.

Page de gestion du firmware

Gérez les packages de firmware Nokia AirScale pour les mises à jour logicielles à distance.

URL : `https://<ran-monitor-ip>:9443/nokia/firmware`

Aperçu

La page de gestion du firmware fournit un référentiel centralisé pour les packages logiciels des stations de base. Téléchargez le firmware dans RAN Monitor et utilisez les URL HTTP générées dans l'option "Serveur distant" de WebEM pour effectuer des mises à jour logicielles.

Fonctionnalités clés

Fonctionnalité	Description
Télécharger	Stocker les packages de firmware .zip Nokia AirScale
URL de téléchargement	Copier les URL HTTP pour la configuration du serveur distant WebEM
Checksums MD5	Calcul automatique des checksums pour la vérification d'intégrité
Statistiques de stockage	Surveiller l'utilisation du disque du référentiel

Flux de travail rapide

1. Téléchargez le package de firmware dans RAN Monitor
2. Cliquez sur **Copier l'URL** pour obtenir l'URL de téléchargement
3. Dans la gestion des logiciels WebEM, sélectionnez **Serveur distant**
4. Collez l'URL et cliquez sur **Connecter et rafraîchir**

5. Sélectionnez le firmware et commencez la mise à jour

Pour une documentation complète incluant les options de configuration et le dépannage, consultez le **Guide de gestion du firmware**.

Page de gestion des données

Gérez les données mises en cache, les fichiers temporaires et le stockage persistant.

URL : `https://<ran-monitor-ip>:9443/nokia/data`

La page de gestion des données montrant le cache ETS, les fichiers temporaires et les options de nettoyage des données InfluxDB.

Cache ETS (En mémoire)

Caches volatils en mémoire qui sont effacés lors du redémarrage de l'application :

Cache	Description
Cache de configuration Nokia	Données de configuration des appareils mises en cache
Cache d'alarmes Nokia	Enregistrements d'alarmes actives mis en cache
Cache d'enregistrements de conservation	Comptes d'enregistrements de politique de conservation mis en cache
Cache d'état d'InfluxDB	État de connexion d'InfluxDB mis en cache

Effacer tout le cache ETS : Supprime toutes les entrées des caches en mémoire. Les données sont régénérées à la prochaine demande.

Fichiers temporaires

Fichiers créés lors de l'extraction et du traitement de la configuration :

- Extraire TAR des téléchargements de configuration d'appareil
- Archives temporaires créées lors du traitement

Effacer les fichiers temporaires : Supprime les fichiers temporaires du répertoire `/tmp`.

Données InfluxDB (Persistantes)

Données de séries temporelles stockées dans InfluxDB pour chaque appareil :

- Métriques de performance (compteurs PM)
- Snapshots de configuration
- Enregistrements d'alarmes

Effacement par appareil : Cliquez sur "Effacer les données" à côté d'un appareil pour supprimer toutes les données InfluxDB pour cet appareil.

Tout effacer : Supprime toutes les données InfluxDB pour tous les appareils. Utilisez avec prudence.

Registre des appareils

Montre le compte des appareils enregistrés. Les configurations des appareils sont chargées depuis `config/runtime.exs` au démarrage et stockées dans ETS.

Cas d'utilisation

- Libérer de la mémoire en effaçant les caches
- Nettoyer les fichiers temporaires après dépannage
- Supprimer les données de test avant utilisation en production
- Effacer les données pour les appareils déclassés

Flux de travail de l'interface utilisateur Web

Flux de travail opérationnels courants utilisant l'interface utilisateur Web.

Vérification quotidienne de la santé

Objectif : Vérifier la santé du système au début du quart

Étapes :

1. Ouvrir le tableau de bord principal
2. Vérifier que tous les appareils affichent un statut vert
3. Vérifier le nombre d'alarmes et leur gravité
4. Examiner les appareils rouges/échoués
5. Enquêter sur les problèmes si nécessaire
6. Documenter les actions prises

Temps : < 5 minutes

Enquête sur les alarmes

Objectif : Répondre et résoudre les alarmes

Étapes :

1. Ouvrir la page des alarmes
2. Trier par gravité (Critique d'abord)
3. Cliquez sur l'alarme pour des détails complets
4. Naviguer vers l'appareil affecté
5. Croiser avec les métriques récentes
6. Déterminer l'action requise
7. Mettre en œuvre la résolution
8. Vérifier que l'alarme s'efface

Pour des procédures détaillées de gestion des alarmes, consultez le Guide de gestion des alarmes.

Mise à jour de la configuration

Objectif : Mettre à jour en toute sécurité la configuration de l'appareil

Étapes :

1. Télécharger la configuration actuelle (sauvegarde)
2. Modifier la configuration hors ligne en utilisant les outils appropriés
3. Télécharger la nouvelle configuration sur l'appareil
4. Noter l'ID de plan retourné
5. Valider la configuration en utilisant l'ID de plan
6. Si la validation réussit, activer la configuration
7. Vérifier que les changements ont pris effet
8. Surveiller la stabilité de l'appareil pendant 15-30 minutes
9. Documenter le changement dans le système de gestion des changements

Notes de sécurité :

- Toujours valider avant d'activer
- Apporter des modifications pendant les fenêtres de maintenance si possible
- Avoir un plan de retour prêt
- Surveiller les comportements inattendus

Ajout d'une nouvelle station de base

Objectif : Ajouter une station de base nouvellement déployée à la surveillance

Étapes :

1. Vérifiez la page des eNodeBs non configurés pour l'appareil
2. Notez l'ID de l'agent et l'adresse IP
3. Ajoutez l'appareil à `config/runtime.exs`
4. Redémarrez l'application RAN Monitor
5. Vérifiez que l'appareil apparaît dans la page des stations de base
6. Confirmez que l'enregistrement réussit (statut vert)
7. Vérifiez que les métriques circulent vers InfluxDB
8. Définissez la politique de conservation si nécessaire
9. Ajoutez aux tableaux de bord Grafana

Pour des opérations détaillées, consultez le Guide des opérations courantes.

Dépannage de la connectivité de l'appareil

Objectif : Diagnostiquer et résoudre les problèmes de connexion de l'appareil

Étapes :

1. Vérifiez la page des stations de base pour l'état de l'appareil
2. Si rouge/échoué, cliquez sur l'appareil pour des détails
3. Examinez les informations de session et le dernier temps de contact
4. Vérifiez les journaux d'application pour des messages d'erreur
5. Vérifiez la connectivité réseau (ping de l'appareil)
6. Confirmez que les identifiants sont corrects
7. Vérifiez que l'appareil est accessible sur le port configuré

8. Examinez les journaux côté appareil si nécessaire
9. Redémarrez la connexion ou l'appareil si nécessaire
10. Vérifiez la récupération

Pour un dépannage détaillé, consultez le Guide de dépannage.

Documentation connexe

- **Guide de démarrage** - Configuration initiale et déploiement
- **Guide des opérations courantes** - Tâches opérationnelles quotidiennes
- **Guide de gestion des alarmes** - Gestion des alarmes et escalade
- **Guide de configuration d'exécution** - Configuration du système
- **Guide d'intégration Grafana** - Analyses et tableaux de bord
- **Guide de la politique de conservation des données** - Gestion du cycle de vie des données
- **Guide de dépannage** - Problèmes courants et solutions