Guide de Configuration Nokia AirScale

Configuration des Stations de Base pour l'Intégration avec RAN Monitor

---

Table des Matières

Aperçu

Pour permettre à RAN Monitor de collecter des métriques de performance, des alarmes et des données de configuration à partir des stations de base Nokia AirScale, vous devez configurer la station de base pour qu'elle rapporte des données au système RAN Monitor. Cela se fait par le biais de 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, consultez Nokia Counter Reference. Pour la configuration du système, consultez Runtime Configuration Guide.

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 Administrateurs** - Nom d'utilisateur et mot de passe avec privilèges de configuration
- **Détails de RAN Monitor** - Adresse IP et port où RAN Monitor écoute
- **Logiciel Supporté** - Version de logiciel de station de base Nokia AirScale compatible

Informations Requises :

Paramètre	Valeur	Exemple
Adresse IP de RAN Monitor	IP où RAN Monitor fonctionne	10.179.2.139
Port de RAN Monitor	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 Web Element Manager

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

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

   ou

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

3. Connectez-vous avec vos identifiants administrateurs

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'arborescence de configuration dans le panneau de gauche et l'éditeur de paramètres dans la fenêtre principale.

Configurer la Surveillance des Performances

Étape 1 : 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 2 : Configurer la Surveillance des Performances en Temps Réel

Faites défiler jusqu'à la section **Structure 1**, qui contient les paramètres de l'entité de collecte de surveillance des performances 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 des performances en temps réel	Adresse IP de RAN Monitor	Votre IP RAN Monitor (ex. : 10.179.2.139)
Numéro de Port de l'Entité de Collecte de Surveillance des Performances en Temps Réel	Port où RAN Monitor écoute	9076 (par défaut)
Intervalle de Collecte de Surveillance des Performances 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 pour conserver toutes les données)

Étape 3 : Enregistrer et Activer la Configuration

Après avoir configuré tous les paramètres :

1. **Vérifiez vos modifications** - Assurez-vous 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 l'extrait 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 RAN Monitor
- `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 RAN Monitor

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

Référence des Paramètres de Configuration

Aperçu de l'Objet PMCADM-1

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

Responsabilités Clés :

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

Entité de Collecte de Surveillance des Performances 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 de RAN Monitor

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 une 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 les environnements à fort volume

sdlNonce - Nonce SDL

- **Type :** Chaîne (8 chiffres)
- **But :** Identifiant unique pour la s��curité 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 nulles des rapports
- **Par Défaut :** false
- **Recommandation :** Garder false pour maintenir des données complètes pour les tendances

---

Vérification

Après avoir activé la configuration, vérifiez que la station de base envoie avec succès des données à RAN Monitor.

Vérifier l'Interface Web de RAN Monitor

1. Ouvrez l'interface Web de RAN Monitor : `http://<ran-monitor-ip>:4000/`
2. Accédez à la page **Statut eNodeB**
3. Localisez votre station de base dans la liste des appareils
4. Vérifiez que le statut indique **Connecté** (indicateur vert)
5. Vérifiez que **Session** indique **Active**

Statut Attendu :

- **Statut :** Connecté (vert)
- **Session :** Active
- **Adresse :** Correspond à l'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 de l'ID du gestionnaire et de la clé d'enregistrement
- RAN Monitor non configuré pour accepter cet appareil
- Problèmes de connectivité réseau

Si le Statut Indique Erreur de Connexion :

L'appareil ne peut pas atteindre RAN Monitor.

Causes possibles :

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

Vérifier la Collecte de Données

Vérifier le Statut InfluxDB :

1. Dans l'interface Web de RAN Monitor, accédez à **Statut InfluxDB**
2. Vérifiez que les points de données augmentent
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 aucun défaut actif

Vérifier la Rétention des Données :

1. Accédez à 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 RAN Monitor

Symptôme : L'appareil n'apparaît pas dans la page Statut eNodeB

Solutions :

1. **Vérifiez la connectivité réseau :**

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

2. **Vérifiez la configuration de RAN Monitor :**
   - 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 de RAN Monitor :**
   - Accédez à la page **Journaux en Direct**
   - Filtrez pour les messages d'erreur
   - Recherchez les tentatives de connexion de la station de base
4. **Vérifiez la configuration de la station de base :**
   - Revérifiez les paramètres PMCADM-1 dans WebLM
   - Confirmez que l'adresse IP de RAN Monitor est correcte
   - Assurez-vous que le port 9076 est spécifié

L'Appareil Affiche le 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 RAN Monitor correspond à l'attente de la station de base
   - Confirmez que les clés d'enregistrement sont correctement configurées
2. **Revoyez 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 à 60 secondes
    - Actualisez 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 à RAN Monitor
    - 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 RAN Monitor
3. **Vérifiez que RAN Monitor écoute :**

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

Pas de Métriques 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
    - Actualisez la page Statut InfluxDB
2. **Vérifiez la connexion InfluxDB :**
    - Accédez à la page Statut InfluxDB
    - Vérifiez que l'indicateur "Connecté" est vert
    - Confirmez que le nom du bucket est correct
3. **Consultez les journaux de RAN Monitor :**
    - Recherchez les erreurs d'écriture InfluxDB
    - Vérifiez les problèmes de parsing de données
    - Assurez-vous que le jeton 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 RAN Monitor 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 des Opérations - Documentation complète des opérations de RAN Monitor
- Guide de Configuration Runtime - Référence de configuration de RAN Monitor
- Nokia Counter Reference - 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 RAN Monitor

Support

Pour les problèmes non couverts dans ce guide :

1. Consultez les journaux d'application de RAN Monitor
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

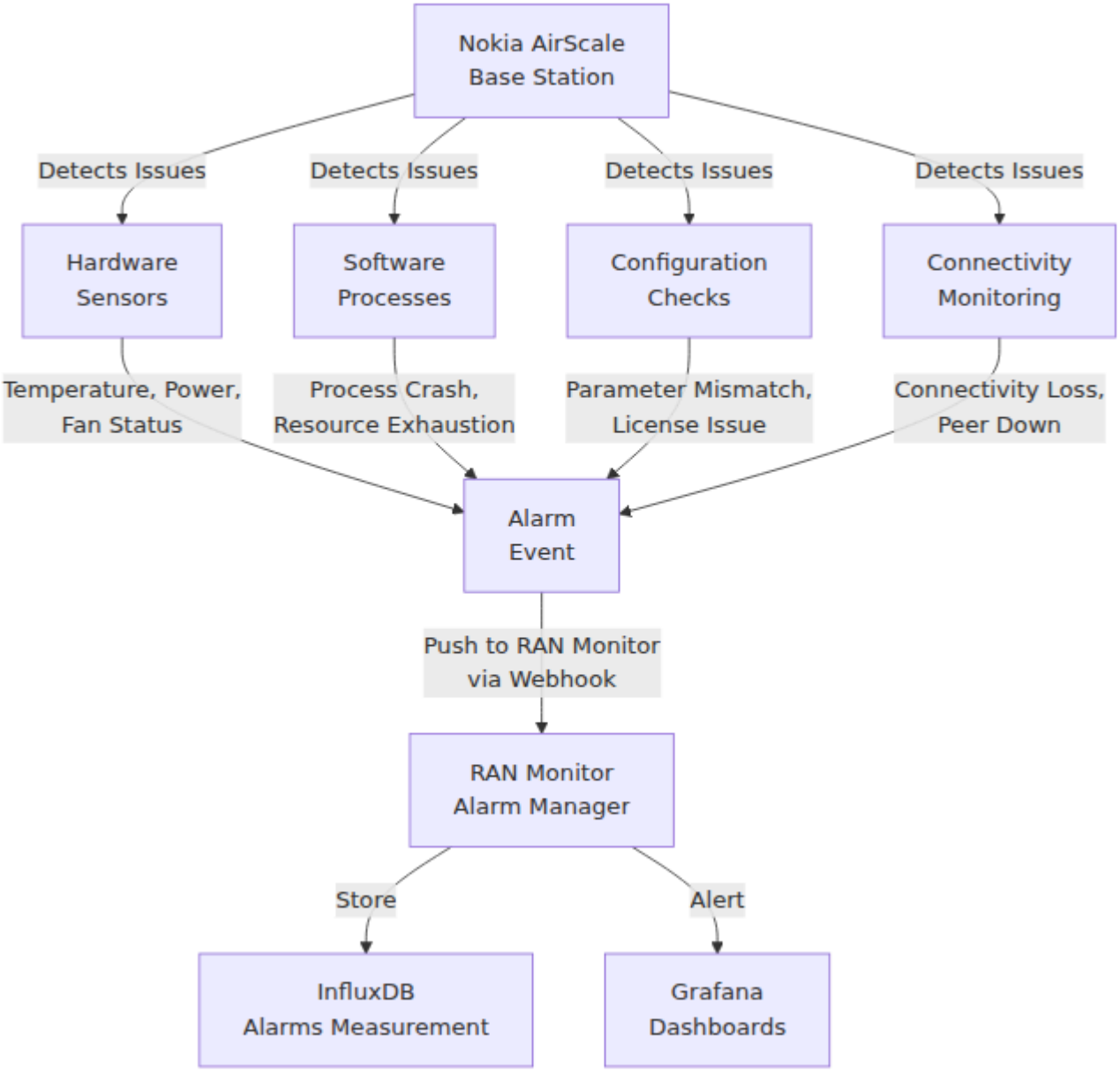
Aperçu

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



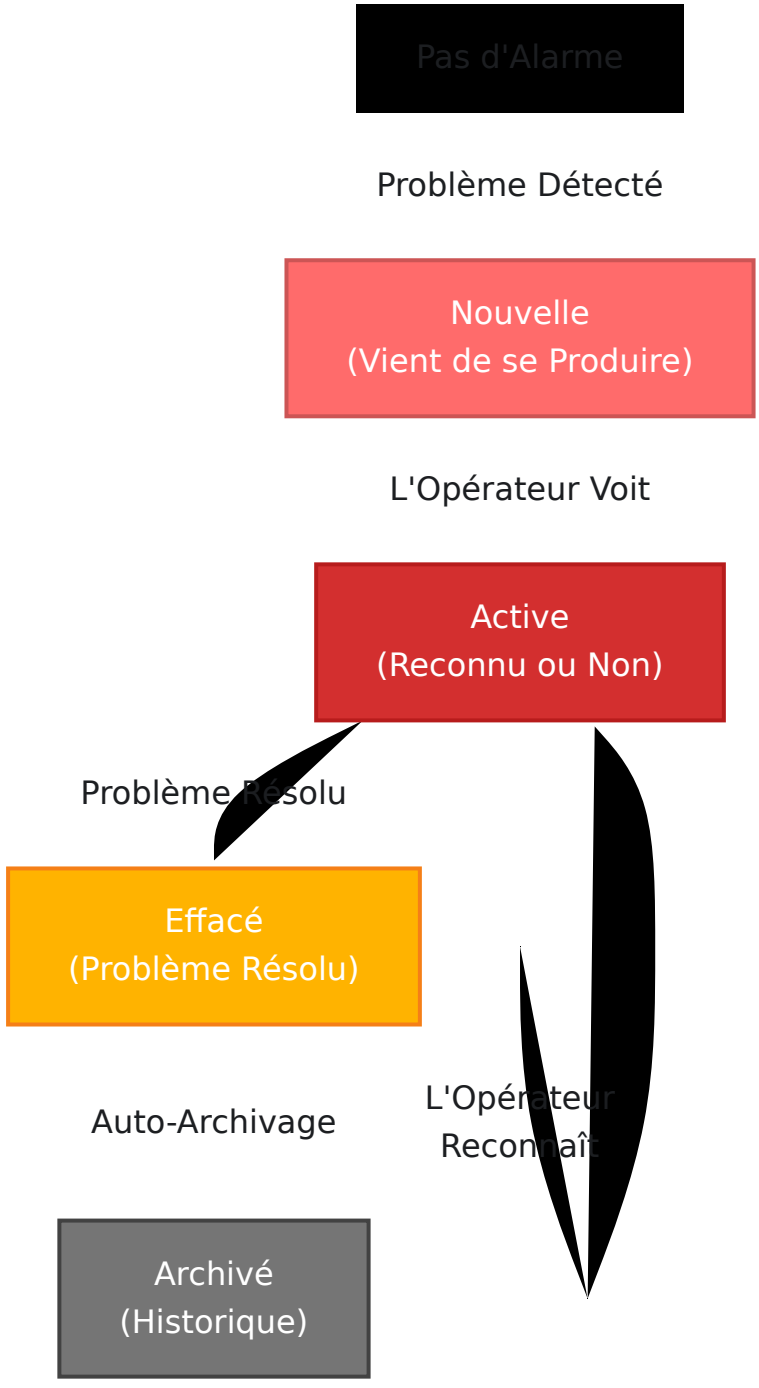
Attributs Clés des Alarmes

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

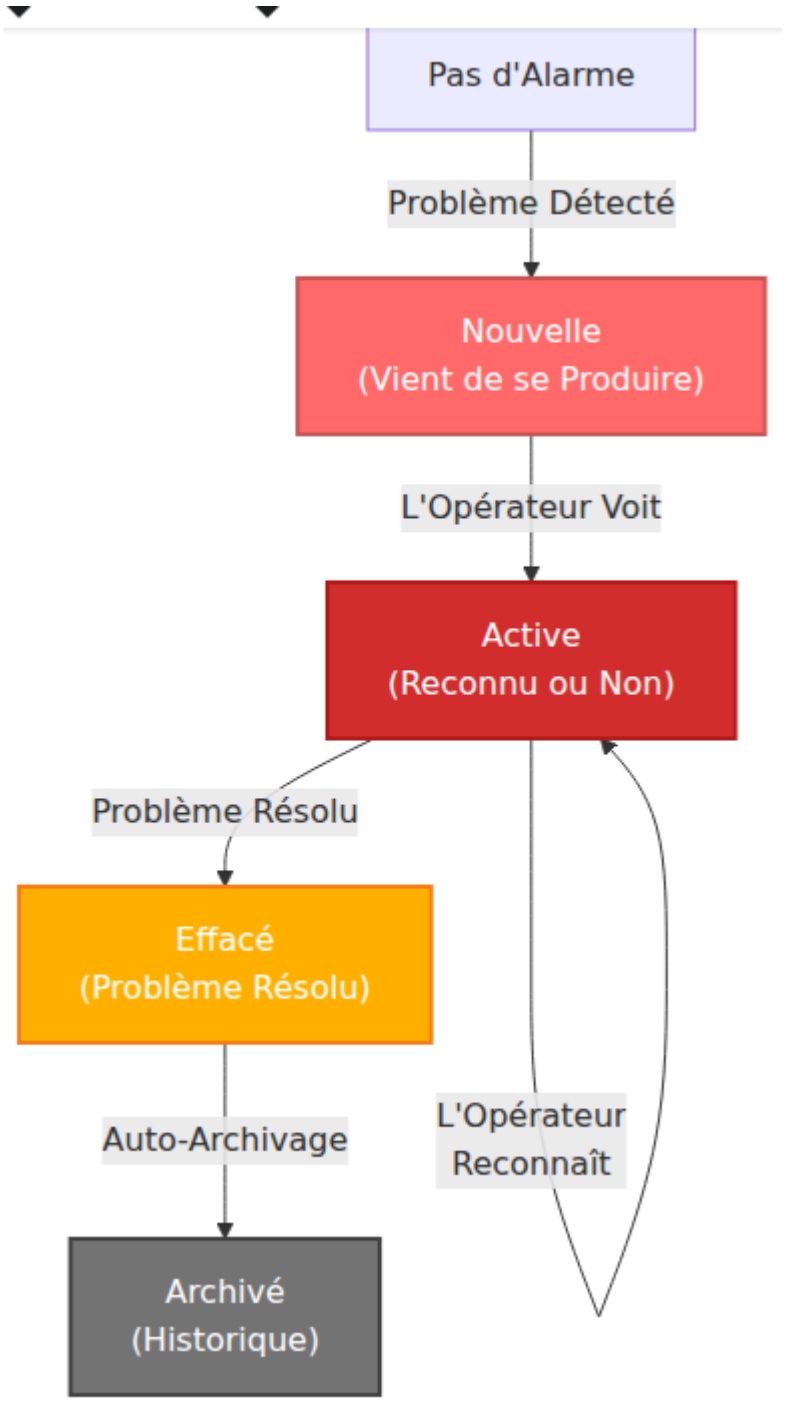
```
14:23:45 UTC - Problème Se Produit
            └─> La station de base détecte une perte de
connectivité
            └─> Génère une alarme : "Connexion S1 Perdue"
(Critique)

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

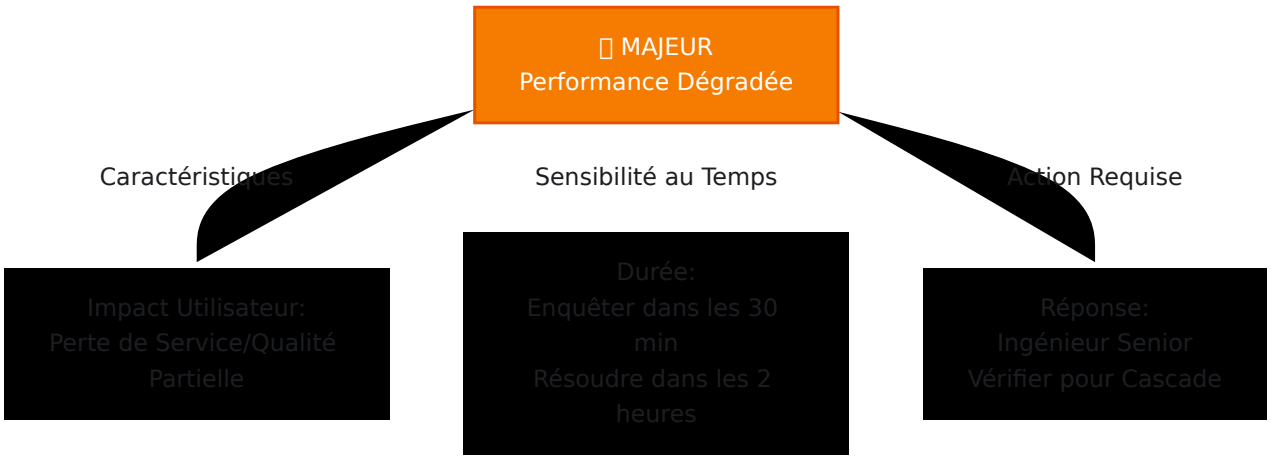
Escalade :

- 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 :

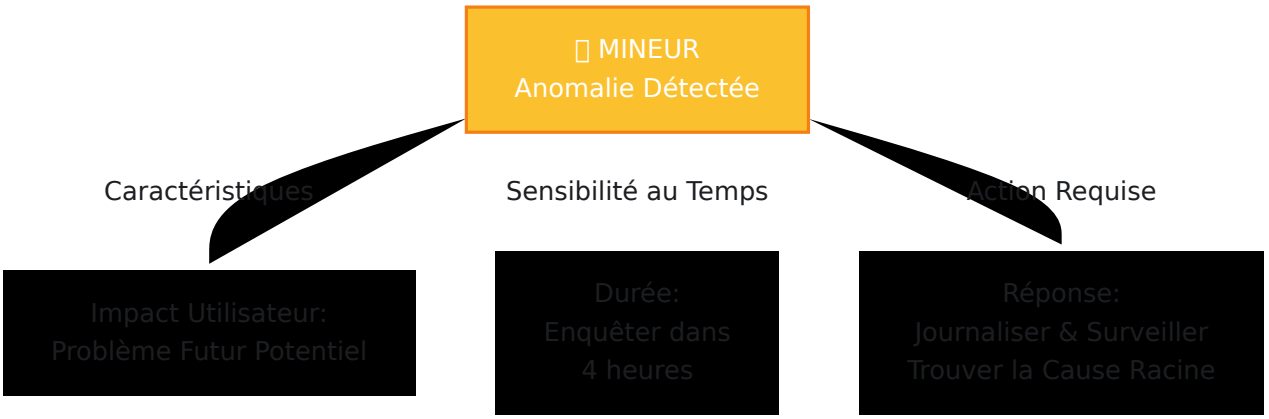
- Notifier l'équipe NOC + ingénieur senior
- Créer un incident dans la gestion des incidents

- 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

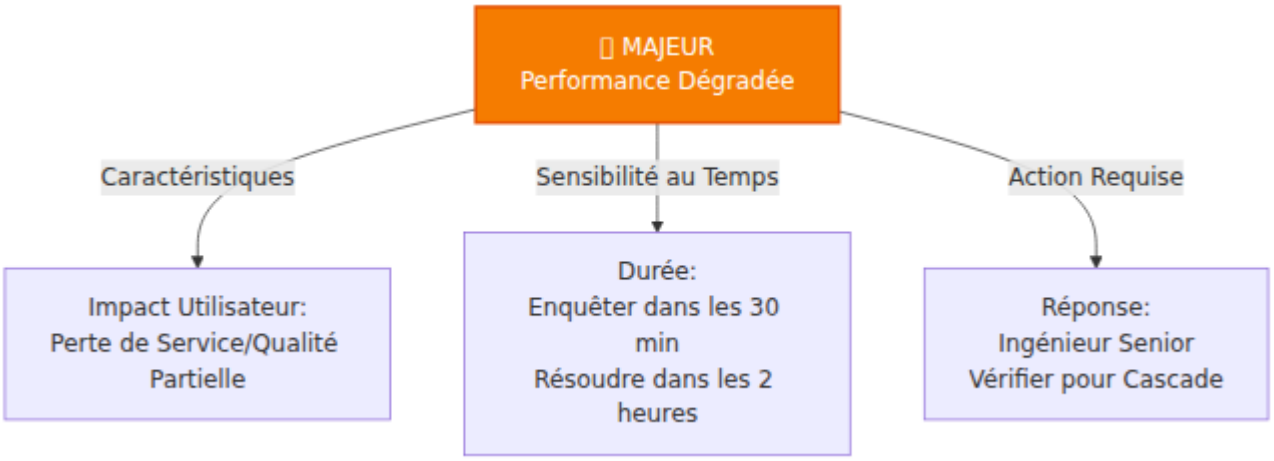
```
Catégorie : Interface Radio
Causes Probables :
  - Cellule Indisponible         → Pas de couverture/power radio
  - Ressource DL Bloquée      → Épuisement de capacité
  - Taux d'Échec de Transfert Élevé → Problème de configuration de
voisin
  - Mauvaise Qualité de Cellule        → Interférence RF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

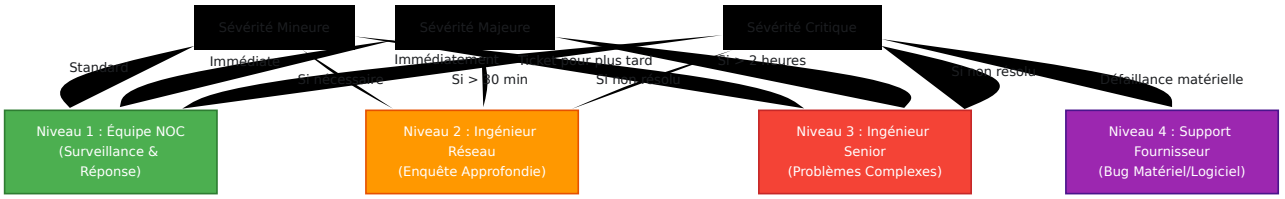
Documenter :

- 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 :

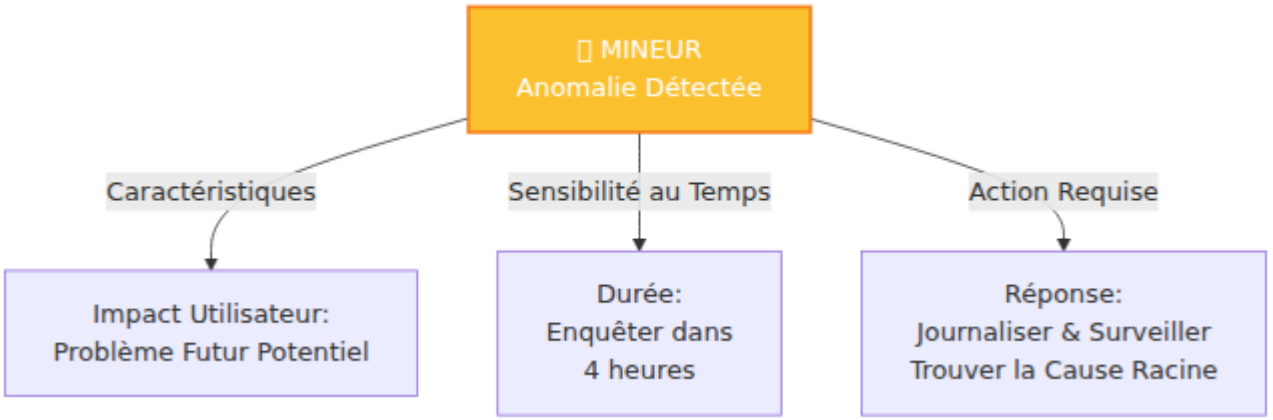
Questions à poser :

- 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

---

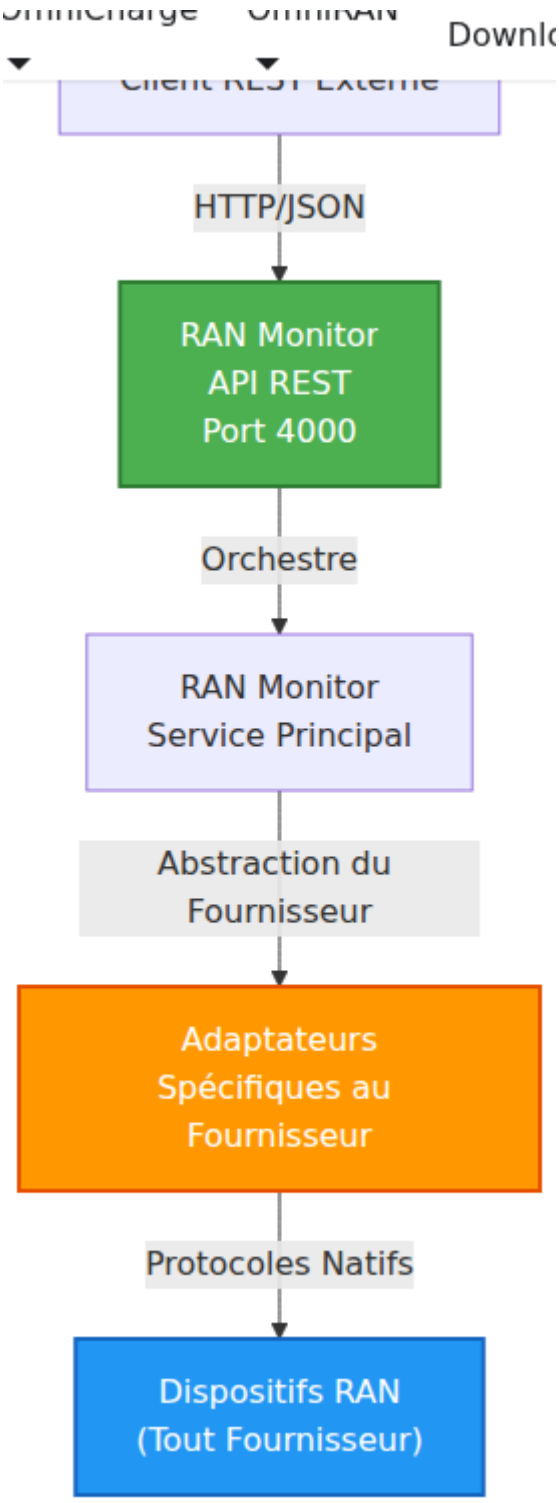
Table des matières

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 de la topologie
- **Contrôle de session** - Gérer les sessions de communication avec les dispositifs
- **Opérations réseau** - Automatiser les tâches de gestion routinières

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 du Fournisseur** - API unifiée à travers différents fournisseurs de dispositifs
- **Opérations avec État** - 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 opérations longues

---

Authentification & Accès

Enregistrement des dispositifs

Avant toute opération, un dispositif doit être enregistré avec 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 informations d'identification du dispositif (nom d'utilisateur/mot de passe ou clés API) sont stockées 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 débit :**

    - 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 utilisateur/client
    - Les modifications de configuration sont suivies avec des valeurs avant/après

---

Référence des points de terminaison

Gestion des dispositifs

Lister tous les dispositifs

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

Réponse :

```
{
  "devices": [
    {
      "id": "nokia_bs1",
      "name": "SITE_A_BS1",
      "vendor": "Nokia",
      "address": "192.168.1.100",
      "port": 8080,
      "status": "registered",
      "registered_at": "2025-12-10T14:30:00Z",
      "session_active": true,
      "software_version": "BSC-2250.5.0",
      "license_required": false
    }
  ]
}
```


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 des sessions

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
- Rafraîchissement 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
        }
      }
    }
  }
}
```


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 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'une défaillance 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 la santé du système

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

Réponse :

```
{
  "status": "healthy",
  "devices": {
    "total": 50,
    "registered": 48,
    "active_sessions": 45,
    "unreachable": 2
  },
  "database": {
    "mysql": "connected",
    "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

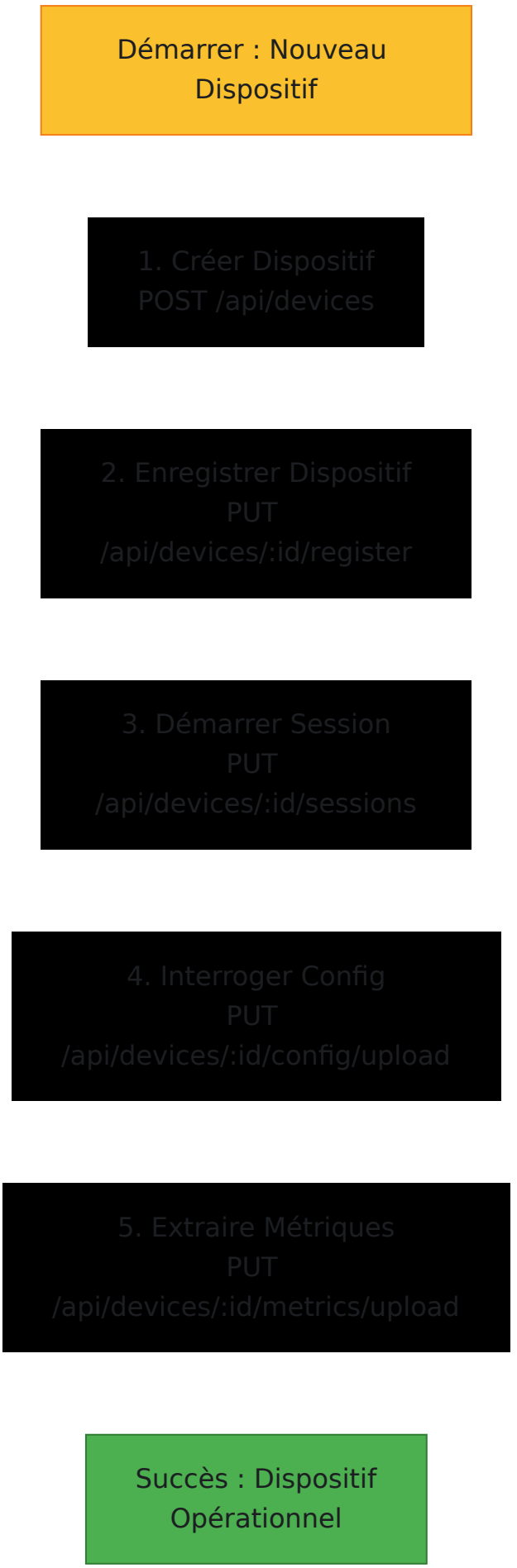
Définir le nombre maximum d'utilisateurs connectés

```
{
  "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 du 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 Requête	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 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": "Appeler PUT /api/devices/:id/register d'abord"
  }
}
```

Session expirée :

```
{
  "error": {
    "code": "SESSION_EXPIRED",
    "message": "La session du dispositif a expiré",
    "solution": "Appeler 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"Config : {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 '.'
```

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 sauvegardées sous forme de fichiers XML horodatés sur le serveur, fournissant une traçabilité complète des changements de configuration.

Caractéristiques Clés

- **Versioning Automatique** - Nouvelles versions créées uniquement lorsque des changements de configuration
- **Sondage Horaire** - Vérifie les changements de configuration toutes les heures (configurable)
- **Détection de Changements** - Comparaison intelligente détecte les changements réels, ignorant les espaces vides
- **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 du Sondage

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

- **Intervalle :** Toutes les 1 heure (par défaut)
- **Premier Sondage :** Immédiatement au démarrage de l'application
- **Détection de Changements :** Compare le contenu avec la version précédente
- **Stockage :** Ne sauvegarde 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                                    # Dernière
configuration
    ├── 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 :** Supprime des versions spécifiques via l'interface Web (sauf `current.xml`)
- **Protection de Stockage :** Limite basée sur la taille empêche l'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 Maximum :** 100 Mo par appareil (configurable)
- **Nettoyage Automatique :** Les versions les plus anciennes sont supprimées lorsque la limite de taille est dépassée
- **Timing de Nettoyage :** Chaque fois qu'une nouvelle version de configuration est sauvegardée
- **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 sauvegardée :

1. **Sauvegarder la 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 anciennes** - Si le total > 100 Mo, supprimer les versions les plus anciennes jusqu'à être sous la limite
5. **Journaliser l'activité** - Suppressions enregistrées avec l'espace libéré

Scénario 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. Sauvegarder : 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. Sauvegarder : 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. Sauvegarder la 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 un maximum de 100 Mo
- **Pas de Surprises :** Le stockage ne croîtra pas indéfiniment
- **Sécurisé en Production :** Aucune intervention manuelle requise
- **Historique Flexible :** Plus de versions pour les petites configurations, moins pour les 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 ayant en moyenne 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 horodatages et tailles de fichiers, et les 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 en 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** - Appareil sélectionné mis en surbrillance en bleu

2. Tableau d'Historique des Versions

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

Colonne	Description
Horodatage	Quand la configuration a été sauvegardée (UTC)
Nom de Fichier	Nom de fichier de version (ex : `config_20251230_143522.xml`)
Taille	Taille du fichier en Ko ou Mo
Âge	Depuis combien de temps la version a été créée (ex : "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 sur le système de fichiers du serveur

---

Opérations Courantes

Télécharger une Configuration

Objectif : Récupérer une version de configuration spécifique 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 à 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

Remarques Importantes :

- Impossible de 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 diff XML (ex : `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 Traçabilité

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 les problèmes de performance ou les 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 :
- Taille augmentée 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 récent de configuration 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 le prochain sondage

Liste de Contrôle de Sécurité :

- ✓ Version précédente correcte téléchargée
- ✓ Plan validé avant activation
- ✓ Coordination avec l'équipe des opérations
- ✓ Planification pendant la fenêtre de maintenance
- ✓ Outils de surveillance prêts pour la 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 le prochain sondage
4. Stocker à l'extérieur en tant que modèle
5. Utiliser pour déployer de nouveaux appareils
6. Revoir 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 vides en début/fin
2. Réduire les espaces vides 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 des 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 de Configuration Typique : ~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 les petites configurations, moins pour les 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 :

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

Personnalisation de la Rétention :

La limite de stockage est configurée dans le module ConfigStorage :

```
# Dans lib/ran_monitor/nokia/airscale/config_storage.ex
# Attribut de module en haut du fichier
@max_storage_bytes 100 * 1024 * 1024  # 100 Mo par défaut

# Changer à une limite différente :
@max_storage_bytes 50 * 1024 * 1024   # 50 Mo (garde ~345
versions)
@max_storage_bytes 200 * 1024 * 1024  # 200 Mo (garde ~1380
versions)

# La fonction de nettoyage utilise ce défaut
def cleanup_old_versions(airscale_name, max_size_bytes \
@max_storage_bytes)
```

Après modification, recompilez :

```
mix compile
# Redémarrez RAN Monitor pour appliquer les changements
```

Configuration de Sondage

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

Pour Changer l'Intervalle de Sondage :

Éditez `lib/ran_monitor/nokia/airscale/manager.ex` :

```
defp schedule_get_airscale_config do
  # Tirer la configuration toutes les 1 heure (3 600 000 ms)
  Process.send_after(self(), :get_airscale_config, 3_600_000)
end
```

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 modification, recompilez et redémarrez RAN Monitor.

Dépannage

Aucune Version de Configuration Affichée

Symptômes :

- La page d'Archivage de Configuration affiche "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 affiche le statut "ENREGISTRÉ"
    - Consultez les journaux d'application pour les erreurs d'enregistrement

2. **Session Non Active**
    - Vérifiez la vue détaillée de l'appareil
    - Assurez-vous que le statut de la session est "ACTIVE"
    - Consultez les horodatages de session
3. **Configuration Pas Encore Sondée**
    - Attendez le premier cycle de sondage 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 affiche "Fichier de configuration non trouvé"
- Le navigateur affiche une erreur 404

Causes Possibles :

1. **Incohérence du 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 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. **Sondage Non Exécuté**
   - Vérifiez les journaux d'application pour les messages de sondage

- Vérifiez que le processus Manager est en cours d'exécution
- 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 des paramètres ont réellement changé

Vérification :

```
# Vérifiez les journaux pour le sondage 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 : Documentez 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. Incluez : Date, Appareil, Changements, Justification, Approuveur

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 du cellulaire 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 : Ajout de cellules voisines 10, 11, 12
Validé : Oui
Activé : 2025-12-28 09:15:00
Résultat : Transferts fonctionnant correctement
```

Surveillance de 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
```

Mettez en Place des Alertes :

- Alerte si la taille totale dépasse un seuil (ex : 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 en parallèle avec 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)

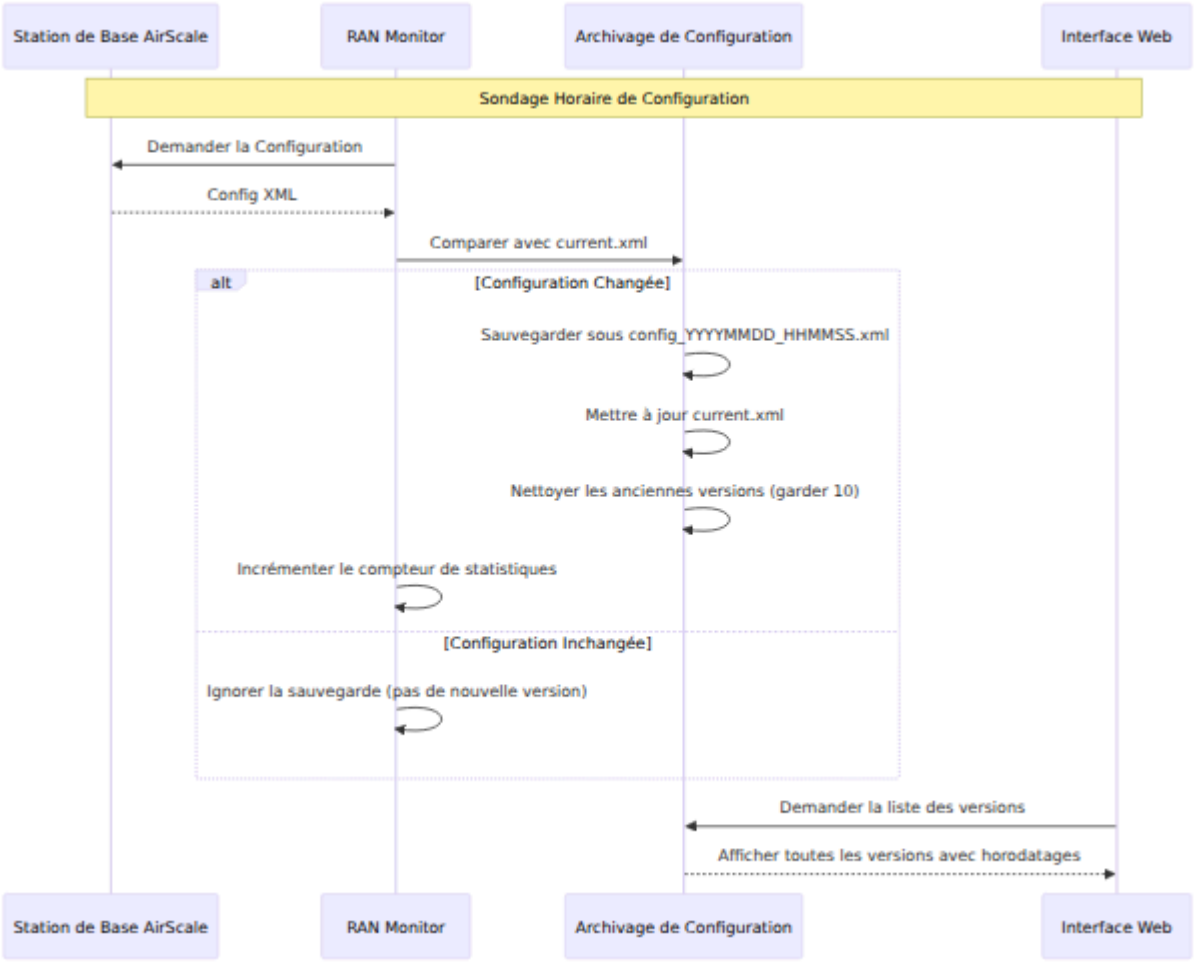
Télécharger une Configuration Modifiée :

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

Processus de Rétrogradation :

- Téléchargez la version précédente depuis l'Archive
- Téléchargez via la Gestion de Configuration
- Suivez 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")
# Retourne : 655

# Obtenir la taille de stockage maximale réglée
RanMonitor.Nokia.Airscale.ConfigStorage.max_storage_bytes()
# Retourne : 104857600 (100 Mo en octets)

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

# Obtenir des statistiques de stockage détaillées
RanMonitor.Nokia.Airscale.ConfigStorage.get_storage_stats("ONS-
Lab-Airscale")
# Retourne : %{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)
# Retourne : {:ok, 345, 50000000} - supprimé 345 versions, libéré
50 Mo

# Nettoyage utilisant le défaut (100 Mo)
RanMonitor.Nokia.Airscale.ConfigStorage.cleanup_old_versions("ONS-
Lab-Airscale")
# Retourne : {:ok, 0, 0} - aucun nettoyage nécessaire si sous
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 Politique de Conservation des Données

Vue d'ensemble

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 Conservation

1. Accédez au **Panneau de Contrôle** : `https://localhost:9443`
2. Cliquez sur **Conservation des Données** dans le menu de navigation
3. Affichez 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

Nettoyage des Anciennes Données

1. Cliquez sur le bouton **Nettoyer 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 prudence !)

Capture d'écran

Le tableau de bord de conservation des données affichant 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 toutes les heures
- **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** : Afficher le nombre total d'enregistrements par eNodeB
- **Temps Réel** : Mis à jour lors du rafraîchissement de la page

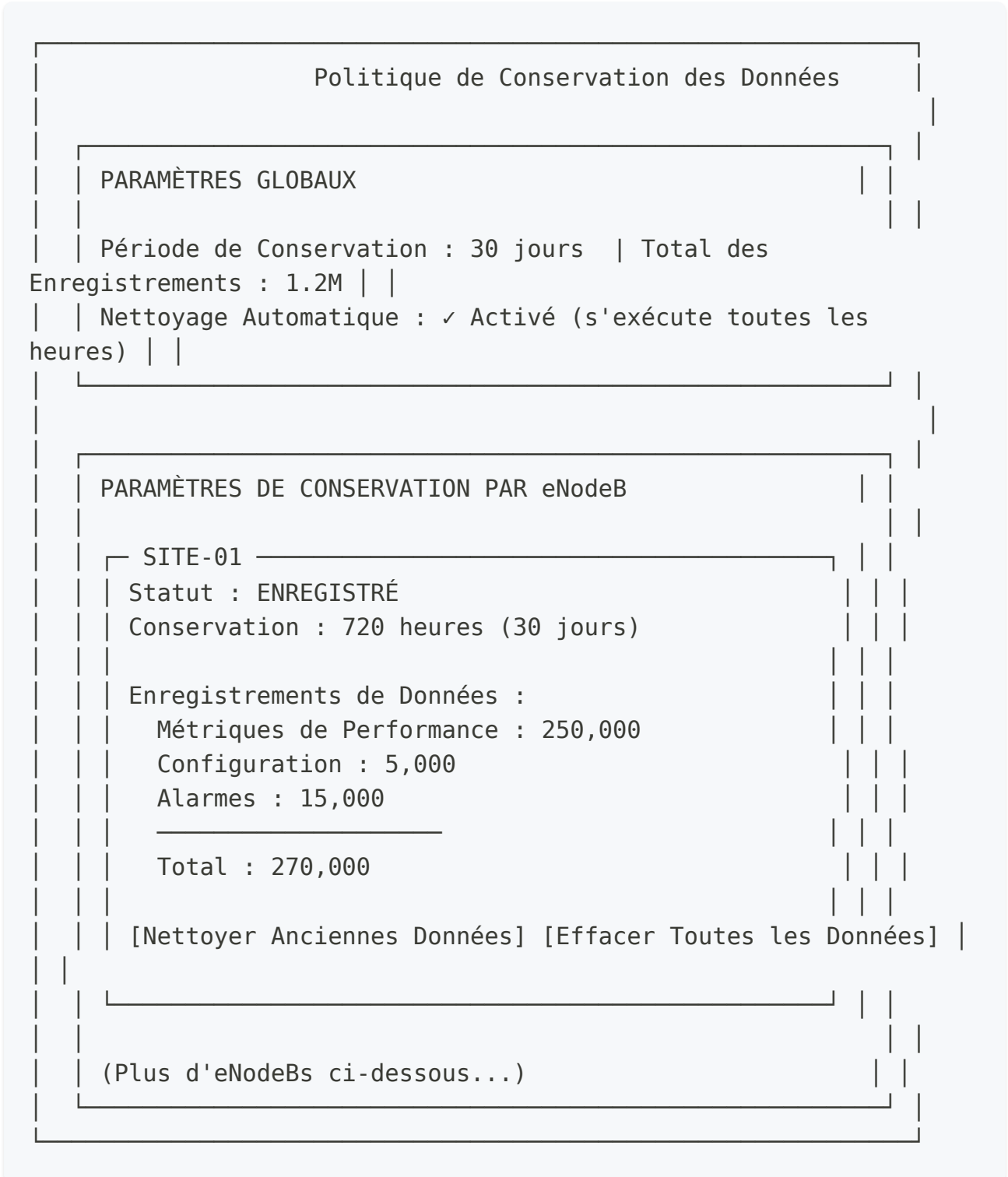
---

🖥️ Interface Utilisateur

Mise en Page du Tableau de Bord

Le tableau de bord de conservation des données affichant 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 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 prudence !)
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 Ça 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 déclenche
   ├─ 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 global
(720h)
  hours -> hours                             # Utiliser 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 global 720 heures

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] Supprimé 15,000 enregistrements 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. Affichez les comptes d'enregistrements actuels par mesure par eNodeB
3. Cliquez sur "Rafraîchir" pour mettre à jour les comptes

Suivi Historique :

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

Éditez `lib/ran_monitor/data/retention_cleanup_worker.ex` :

```
# Changer de 1 heure (3600000ms) à 30 minutes (1800000ms)
@cleanup_interval_ms 1800000  # 30 minutes
```

Puis recompilez :

```
mix compile
```

Requêtes au Niveau de la Base de Données

Voir les paramètres de conservation directement :

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

Mettre 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)

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

Standard (7-30 jours)

- Utiliser 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)

- Utiliser 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 chiffrement** au repos par défaut
- **Accès réseau** contrôlé via la sécurité InfluxDB
- **Journaux d'accès** disponibles dans les journaux d'application

Conformité

- **Traçabilité** : Tous les nettoyages sont enregistrés avec un timestamp
- **Intégrité des données** : Suppressions douces, pas de suppressions dures 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 données critiques
5. **Tester les politiques de conservation** en premier dans le staging

---

🔧 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 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 d'application pour les erreurs :
   - Recherchez les entrées d'erreur `[RetentionPolicy]`
4. Vérifiez que l'eNodeB est enregistré :
   - Vérifiez la page d'état de l'eNodeB

Problème : Utilisation Élevée de la Mémoire Après Nettoyage

Symptômes :

- L'application devient lente après le nettoyage
- Utilisation de la mémoire en forte hausse

Solutions :

1. C'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 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'UI Web** - Référence du panneau de contrôle et fonctionnalités
- **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 de l'eNodeB** : `https://localhost:9443/nokia/status`
- **État d'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 d'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 le 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

Fichiers Modifiés

Fichier	Changements
`lib/ran_monitor/database/nokia/airscale.ex`	Ajout du champ `retention_hours`
`lib/ran_monitor/config/config.ex`	Ajout du getter `data_retention_hours()`
`config/config.exs`	Ajout de la configuration de conservation globale et de la route de page
`lib/ran_monitor/application.ex`	Ajout du travailleur de nettoyage à l'arbre de supervision

Fichiers Créés

Fichier
`lib/ran_monitor/data/retention_policy.ex`
`lib/ran_monitor/data/retention_cleanup_worker.ex`
`lib/ran_monitor/web/live/retention_policy_live.ex`
`priv/repo/migrations/20251211065257_add_retention_hours_to_airscales.`

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

🚀 Démarrage

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 :**
    - Affichez la conservation globale (par défaut : 720 heures)
    - Affichez 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. **Revoyez ce guide :** La plupart des problèmes sont couverts dans la section Dépannage
3. **Vérifiez d'autres docs :** Consultez les liens de documentation connexes ci-dessus
4. **Vérifiez la configuration :** Assurez-vous que la migration a été exécutée et que le travailleur a démarré

Rapport 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 pendant laquelle les données sont conservées
- **Nettoyage** : Suppression automatisée des anciennes données
- **Types de Mesures** : Métriques de Performance, Configuration, Alarmes

Ressources Externes

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

Démarrer avec 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

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 de séries temporelles InfluxDB

- 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 les webhooks)
- RAN Monitor → MySQL (port 3306)
- RAN Monitor → InfluxDB (port 8086)
- Opérateurs → Interface Web RAN Monitor (port 9443)

Règles de pare-feu

- Autoriser l'entrée sur le port 8080 (communication avec la station de base)
- Autoriser l'entrée sur le port 9076 (récepteur de webhook)
- Autoriser l'entrée sur le port 9443 (interface Web HTTPS)
- Autoriser la sortie vers MySQL et InfluxDB

Exigences de la station 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 (le 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'analyse 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
```

Sauvegardez 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

Éditez `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 la
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, consultez 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 naviguez vers :

```
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 mesures 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. Filtrez 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
   - Consultez le Guide des opérations courantes
2. **Configurer des 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
   - Consultez le Guide d'intégration Grafana
3. **Configurer la rétention des données**
   - Définissez des périodes de rétention appropriées
   - Configurez la rétention par appareil si nécessaire
   - Consultez 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
    - Consultez 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 des 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)
- Révisez 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 la 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 de l'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 inaccessible :

- 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 de l'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
- **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 des problèmes

Guide d'Intégration et d'Analyse Grafana

Création de Tableaux de Bord Opérationnels et d'Alerte pour la Surveillance RAN

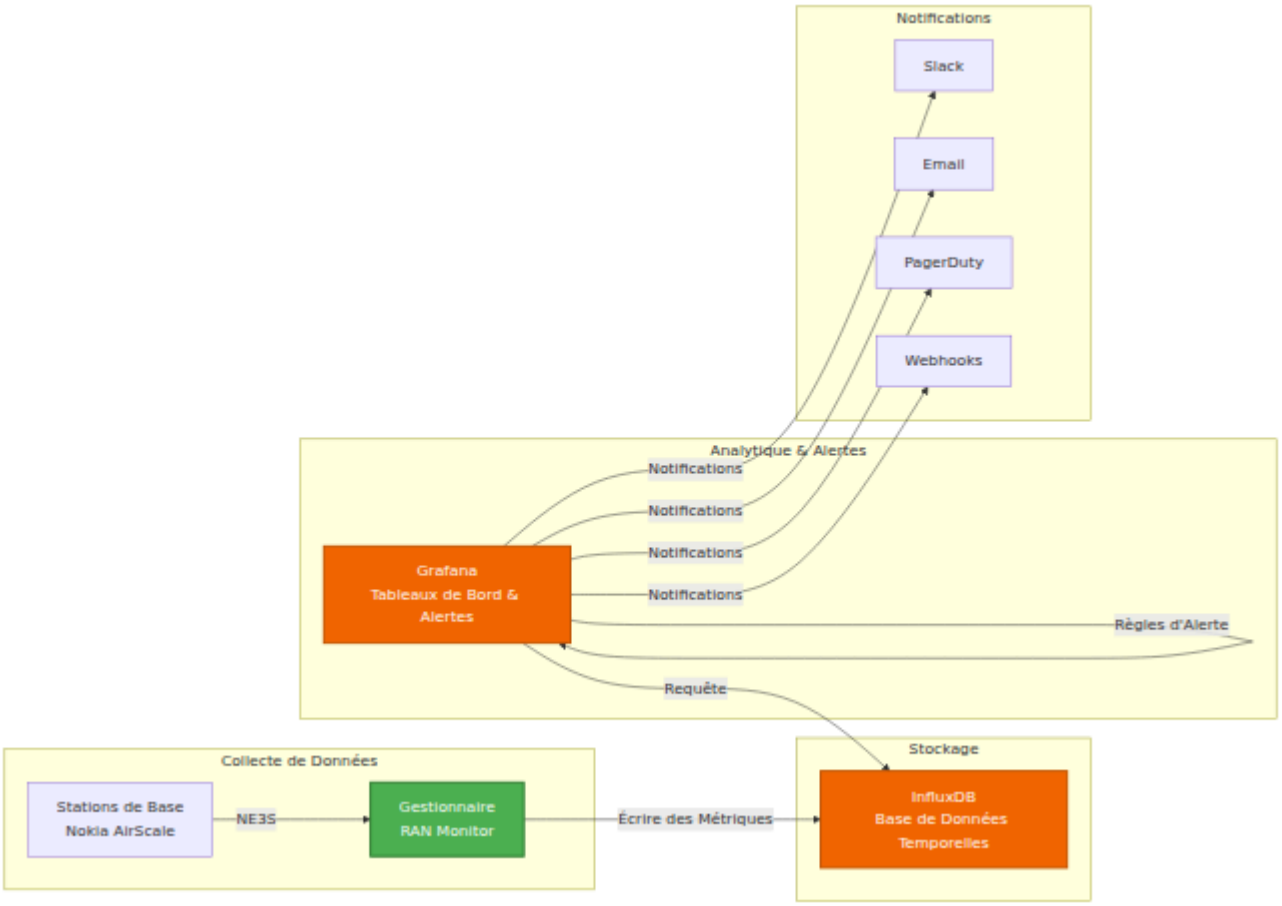
Guide complet sur la création de tableaux de bord Grafana, les stratégies d'alerte et la visualisation des KPI

Table des Matières

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 :

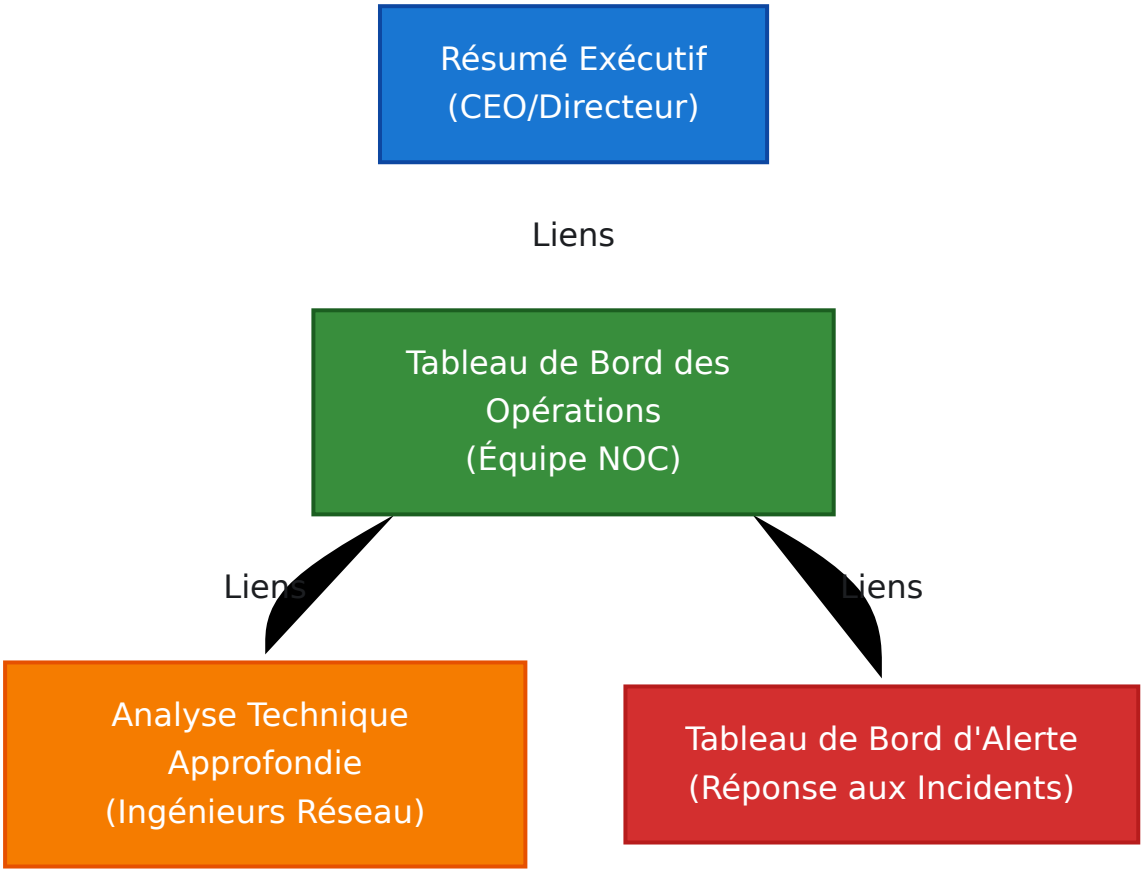
```
from(bucket:"ran_metrics")
  |> range(start: -7d, stop: now())
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r.device == "SITE_A_BS1")
  |> group(by: ["_field"])
  |> aggregateWindow(every: 1h, fn: mean)
```

Concepts Clés :

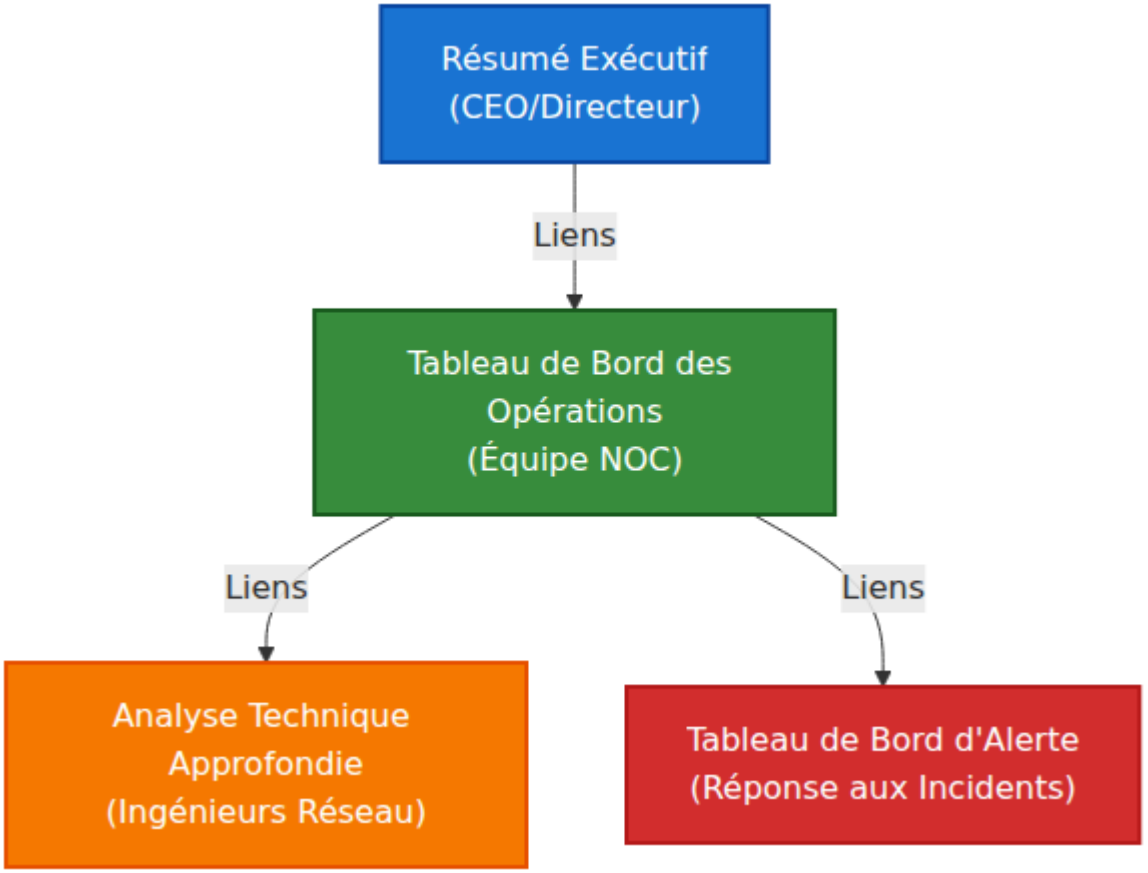
- `from()` - Sélectionner le bucket
- `range()` - Fenêtre temporelle
- `filter()` - Sélectionner les données
- `group()` - Organiser les résultats
- `aggregateWindow()` - Résumer les périodes temporelles

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

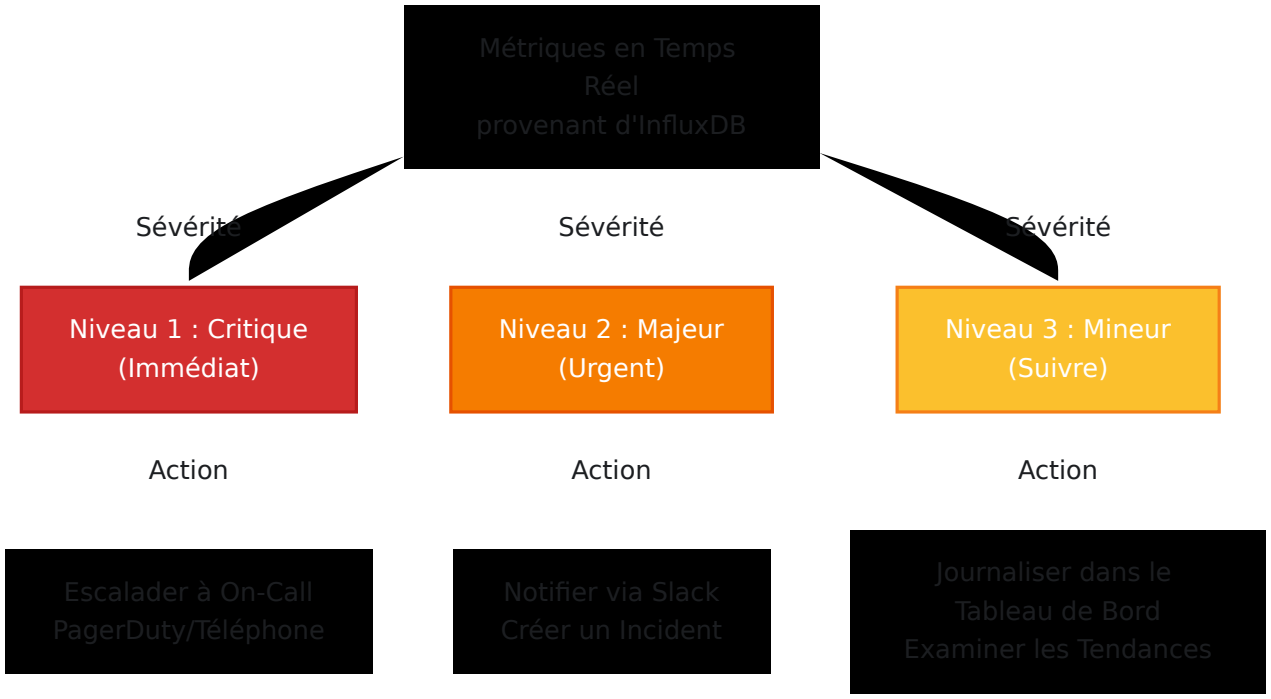
```
from(bucket:"ran_metrics")
  |> range(start: -7d)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r._field =~ /HandoverSuccess|Traffic/)
  |> group(by: ["device", "_field"])
  |> aggregateWindow(every: 1h, fn: mean)
  |> pivot(rowKey: ["_time"], columnKey: ["_field"], 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 du Moniteur RAN au Quotidien

Guide pratique pour les tâches opérationnelles de routine et la gestion des dispositifs

---

Table des Matières

Aperçu

Ce guide couvre les tâches opérationnelles de routine pour gérer le 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 la topologie de votre réseau

Pour la configuration initiale, consultez 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 le dispositif 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 du Dispositif

Collectez les informations suivantes :

Information	Exemple	Où Trouver
Adresse IP	10.7.15.67	Documentation réseau ou étiquette du dispositif
Port	8080	Typiquement 8080 pour Nokia AirScale
Nom du Dispositif	Site-B-Tower-1	Utilisez la convention de nommage du site
Nom d'utilisateur	admin	Provenant de la provision de la station de base
Mot de passe	password123	Provenant de la provision de la station de base

Meilleures Pratiques de Nommage des Dispositifs :

- Utilisez des noms descriptifs et cohérents
- 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 Dispositifs Non Configurés

Avant d'ajouter manuellement, vérifiez si le dispositif 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 d'Agent de votre dispositif
4. Notez l'ID d'Agent s'il est trouvé

Cela aide à vérifier que le dispositif peut atteindre le Moniteur RAN.

Étape 4 : Ajouter le Dispositif à la Configuration

Modifiez `config/runtime.exs` et ajoutez le nouveau dispositif à la liste `airscales` :

```
config :ran_monitor,
  nokia: %{
    ne3s: %{
      # ... configuration existante des ne3s ...
    },
    airscales: [
      # Dispositifs existants
      %{
        address: "10.7.15.66",
        name: "Site-A-BS1",
        port: "8080",
        web_username: "admin",
        web_password: "password1"
      },

      # Nouveau dispositif
      %{
        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 de la syntaxe Elixir 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 d'ouverture `{` et les crochets `[` 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 cours d'exécution en développement
# Appuyez sur Ctrl+C deux fois, puis :
mix phx.server

# Si en cours d'exécution en tant que service
systemctl restart ran_monitor

# Si en cours d'exécution via release
/path/to/ran_monitor/bin/ran_monitor restart
```

Étape 7 : Vérifier l'Enregistrement du Dispositif

Après le redémarrage, vérifiez que le dispositif est maintenant surveillé :

1. **Vérifiez les Journaux de l'Application :**

   ```
   [info] Tentative d'enregistrement avec le dispositif : 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 nouveau dispositif dans la liste
    - Le statut doit être "Associé" (vert)
    - L'état d'enregistrement doit être "Enregistré"
3. **Vérifiez les Détails du Dispositif :**
    - Cliquez sur le dispositif
    - 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 doivent croître à mesure que les données sont collectées

Étape 8 : Configurer la Conservation des Données (Optionnel)

Si ce dispositif nécessite une conservation différente de la valeur par défaut globale :

1. Accédez à la page **Conservation des Données**
2. Trouvez votre nouveau dispositif dans la liste
3. Mettez à jour le champ "Période de Conservation" (en heures)
4. Le système enregistre automatiquement

Pour plus de détails, consultez le Guide de Politique de Conservation des Données.

Étape 9 : Ajouter aux Tableaux de Bord Grafana

Mettez à jour les tableaux de bord Grafana pour inclure le nouveau dispositif :

1. Modifiez les variables de modèle de tableau de bord
2. Ajoutez le nom du dispositif aux sélecteurs déroulants
3. Créez un tableau de bord spécifique au dispositif si nécessaire

Pour plus de détails, consultez 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 des données historiques :

Option A : Préserver les Données

- Désactiver la surveillance mais garder 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 le dispositif
- Libère de l'espace de stockage InfluxDB
- Irréversible - les données ne peuvent pas être récupérées

Étape 2 : Désactiver le Dispositif (Préserver les Données)

Pour arrêter la surveillance mais garder les données historiques :

Modifiez `config/runtime.exs` et localisez le dispositif dans la liste `airscales`. Commentez-le ou supprimez-le :

```
airscales: [
  %{
    address: "10.7.15.66",
    name: "Site-A-BS1",
    port: "8080",
    web_username: "admin",
    web_password: "password1"
  },

  # Dispositif 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 le dispositif :

1. Accédez à la page **Conservation des Données** dans l'interface Web
2. Trouvez le dispositif 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 :**
    - Le dispositif ne doit plus apparaître dans la liste active
    - Si les données ont été préservées, le dispositif peut encore apparaître dans les requêtes historiques
2. **Vérifiez les Journaux de l'Application :**
    - Aucune tentative d'enregistrement pour le dispositif supprimé
    - Aucune erreur concernant un dispositif manquant
3. **Vérifiez InfluxDB :**
    - Si les données ont été supprimées, les comptes d'enregistrements doivent être plus bas
    - Le dispositif ne doit pas apparaître dans les nouvelles métriques

Étape 6 : Mettre à Jour les Tableaux de Bord Grafana

Retirez le dispositif des configurations Grafana :

1. Modifiez les variables de modèle de tableau de bord
2. Supprimez le nom du dispositif des sélecteurs déroulants
3. Supprimez les tableaux de bord spécifiques au dispositif s'ils existent

---

Mise à Jour des Identifiants du Dispositif

Lorsque les mots de passe des stations de base sont changés, mettez à jour la configuration du Moniteur RAN.

Étape 1 : Noter l'État Actuel

Avant d'apporter des modifications :

1. Vérifiez que le dispositif 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 le dispositif : Site-A-
   BS1
   [info] Enregistrement réussi avec Site-A-BS1
   ```

2. **Vérifiez l'Interface Web :**

   - Le statut du dispositif doit être "Associé" (vert)
   - Une nouvelle session doit être établie
   - "Dernier Contact" doit être récent

Si le Dispositif 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'alarmes 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.

Exemples d'emplacements (peuvent varier selon la version) :

- Métriques de performance : `lib/ran_monitor/nokia/airscale/manager.ex`
- Alarmes : `lib/ran_monitor/nokia/airscale/manager.ex`
- Configuration : `lib/ran_monitor/nokia/airscale/manager.ex`

Remarque : Contactez le support Omnitouch pour obtenir de l'aide concernant les modifications des intervalles de collecte, car cela nécessite des modifications du code source.

Étape 2 : Considérer l'Impact

Avant de changer les intervalles :

Impact Réseau :

- Calculez : dispositifs × 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 conservation = stockage total
- Exemple : intervalle de 10s = 8,640 mesures/jour par compteur
- Assurez-vous qu'InfluxDB dispose d'un espace disque suffisant

Performance du Système :

- Polling plus fréquent = 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 du Dispositif

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, consultez 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 :

- Gardez une sauvegarde de la configuration actuelle
- Permet un retour en arrière si nécessaire
- Documente la configuration avant 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 du dispositif 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 dispositifs affichent-ils un statut vert (associé) ?
- Des dispositifs 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'alarmes 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"

- Y a-t-il des erreurs récurrentes ?

Pour des procédures de vérification de santé détaillées, consultez 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, 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 une visibilité instantanée sur la santé du réseau et l'état des dispositifs.

Revue Systématique Hebdomadaire

Vérification plus approfondie effectuée chaque semaine :

1. Vérifiez les Tendances des Alarmes

- Utilisez Grafana pour analyser le taux d'alarmes 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

- Tendance d'utilisation du disque InfluxDB
- Taille de la base de données MySQL
- Tailles des fichiers journaux de l'application

3. Vérifiez la Connectivité des Dispositifs

- Des dispositifs 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 Conservation des Données

Consultez le Guide de Politique de Conservation des Données pour des détails complets.

Référence Rapide :

Voir la Conservation Actuelle :

- Accédez à la page de Conservation des Données
- Vérifiez la valeur par défaut globale et les paramètres par dispositif

Ajuster la Période de Conservation :

- Mettez à jour les heures de conservation pour un dispositif 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 conservation en fonction du stockage disponible
- Équilibrez la période de conservation avec la capacité de stockage

Exportation des Données

Exporter les Configurations des Dispositifs :

1. Accédez à la page de détails du dispositif
2. Cliquez sur "Télécharger la Configuration"
3. Enregistrez le fichier XML à un emplacement sûr
4. Étiquetez avec le nom du dispositif et la date

Exporter les Métriques (via InfluxDB) :

```
# Exporter des données pour un dispositif 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 de temps
- 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 tout le répertoire de configuration
tar -czf backups/config-$(date +%Y%m%d).tar.gz config/
```

2. Configurations des Dispositifs

- Téléchargez les configurations de tous les dispositifs via l'interface Web
- Stockez dans un contrôle de version ou un emplacement de sauvegarde
- Effectuez une sauvegarde hebdomadaire ou avant/après les 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)/
```

Planning de Sauvegarde

Quotidien :

- Base de données MySQL (état de session)
- Fichiers de configuration s'ils ont changé

Hebdomadaire :

- Données InfluxDB (ou selon la politique de conservation)
- Configurations des dispositifs de toutes les stations de base

Avant les Changements :

- Fichiers de configuration
- Configurations des dispositifs
- 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 dispositifs 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 dispositifs se réenregistreront automatiquement

5. La collecte de nouvelles métriques commence

6. Les données historiques restent dans InfluxDB

Récupérer d'une Perte Complète 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 dispositifs 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 de sauvegarde
- 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
- Prévoir 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 les Heures de Faible Trafic :**
    - 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 de statut
    - Fixez des attentes pour le 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 dispositifs 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 tout problème rencontré
    - 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
- **Guide d'Intégration Grafana** - Analytique et tableaux de bord
- **Guide de Gestion des Alarmes** - Procédures de gestion des alarmes
- **Guide de Politique de Conservation 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 Compteurs de Performance LTE de Nokia

Guide complet sur les compteurs de mesure de performance Nokia AirScale/FlexiRadio

---

Table des Matières

Aperçu

Les stations de base LTE de 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 de 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 inter-eNB
M8005	Qualité Radio	237	RSSI, SINR, conditions radio, AMC
M8006	Support EPS	54	Configuration/modification/libératio 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	55	Utilisation PRB, allocation de ressources

Mesure	Catégorie	Nombre de Compteurs	Focalisation Principale
	Ressources		
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 sur X2
M8015	Transfert Intra-eNB	13	Transferts internes de cellule
M8016	Retour en Circuit Commuté	18	Procédures de retour en circuit commuté
M8017	HO Inter-Système	10	Transfert vers d'autres RAT (3G/2G)
M8018	Charge eNB	8	Comptes d'UE actifs, statistiques de charge
M8019	NACC	4	Changement de cellule assisté par le réseau
M8020	Disponibilité de la Cellule	7	État de la cellule et échantillonnage de disponibilité
M8021	HO Inter-Fréquence	17	Procédures de transfert inter-fréquence

Mesure	Catégorie	Nombre de Compteurs	Focalisation Principale
M8022	Configuration X2	2	Établissement de l'interface X2
M8023	Volume de Données	36	Volume SDU PDCP sur l'interface ai

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	RX Ethernet	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 Énergétique	Variable	Utilisation de l'énergie de la station de base

---

Convention de Nommage 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 de 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 de 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 la cellule
- M8049Cxx - État de la 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 moyenne de PRB UL par TTI	Utilisation moyenne de PRB montante par Intervalle de Temps de Transmission	0.1%	Moyenne	Diviser par 10 pour obtenir un pourcentage
M8011C37	Utilisation moyenne de PRB DL par TTI	Utilisation moyenne de PRB descendante 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 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 de PRB

Utilisation dans la Planification de Capacité :

- < 50% - La cellule a une capacité disponible

- 50-70% - Cellule normalement chargée
- 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 réels des utilisateurs.

Compteur	Nom	Description	Unité	Type	Déclencheur de Mise à Jour
M8012C23	Débit PDCP UL moyen	Débit moyen de PDCP montante	kbit/s	Moyenne	Lorsque le SDU PDCP est reçu de l'UE
M8012C26	Débit PDCP DL moyen	Débit moyen de PDCP descendante	kbit/s	Moyenne	Lorsque le SDU PDCP est 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 réel 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 largeur de bande 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: v.timeRangeStart, stop: v.timeRangeStop)
  |> 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 de l'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	Nombre maximum d'UE actifs par eNodeB	Nombre maximum d'UE actifs par eNodeB	Entier	Max	1 seconde

Comprendre l'Activité de l'UE :

- **UE Actif** = Un dispositif avec au moins un Support Radio de Signalisation (SRB) et un Support Radio de Données (DRB)
- Valeur maximale observée sur des périodes d'échantillonnage de 1 seconde
- Indique la charge d'utilisateurs simultanés 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 simultanés par cellule
- Un nombre élevé d'UE peut avoir un impact sur le débit par utilisateur

---

Compteurs de Disponibilité de la Cellule

M8020 - Mesures de Disponibilité de la 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 prévue	Entier	Somme	~1 sec
M8020C6	Dénominateur de disponibilité de la cellule	Nombre total d'échantillons de vérification de disponibilité	Entier	Dénominateur	~1 sec

Calcul de la Disponibilité de la Cellule :

```
Disponibilité de la Cellule % = 100.0 × M8020C3 / (M8020C6 - M8020C4)
```

Explication de la Formule :

- **M8020C3** - Échantillons lorsque la cellule fonctionnait normalement
- **M8020C6** - Total des échantillons pris
- **M8020C4** - Échantillons de temps d'arrêt prévu (exclus du calcul)

Objectifs de Disponibilité :

Disponibilité	Note	Statut
> 99.9%	Excellent	Respect de l'accord de niveau de service
99.0-99.9%	Bon	Opérations normales
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 la 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 à 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 Mean	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 liées 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 prédictions de force du signal

---

Compteurs de Gestion des Connexions

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	Établissements de connexions RRC réussis	Entier	Somme
M8013C17	Tentatives d'Établissement de Connexion de Signalisation MO-S	Tentatives de connexion - Signalisation Origine Mobile	Entier	Somme
M8013C18	Tentatives d'Établissement de Connexion de Signalisation MT	Tentatives de connexion - Terminé Mobile	Entier	Somme
M8013C19	Tentatives d'Établissement de Connexion de Signalisation MO-D	Tentatives de connexion - Données Origine Mobile	Entier	Somme
M8013C21	Tentatives d'Établissement de Connexion de Signalisation Urgente	Tentatives de connexion d'appel d'urgence	Entier	Somme
M8013C31	Tentatives d'Établissement de Connexion de Signalisation Haute Priorité	Tentatives de connexion haute priorité	Entier	Somme
M8013C34	Tentatives d'Établissement de Connexion de	Tentatives de connexion tolérantes au délai	Entier	Somme

Compteur	Nom	Description	Unité	Type
	Signalisation Tolérant au Délai			
M8013C91	Tentatives d'Établissement de Connexion de Signalisation MO-V	Tentatives de connexion - Voix Origine Mobile	Entier	Somme
M8013C93	Tentatives d'Établissement de Connexion de Signalisation MT-Access	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 Origine Mobile (SMS, mises à jour de localisation)
- **MT (M8013C18)** - Terminé Mobile (appels/données entrants)
- **MO-D (M8013C19)** - Données Origine Mobile (sessions de données)
- **MO-V (M8013C91)** - Voix Origine Mobile (appels VoLTE)
- **Urgent (M8013C21)** - Appels d'urgence (911, 112)

Objectifs de Performance :

Taux de Réussite	Note	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 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 moyen	Temps de rétention moyen du 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	Note	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	Impacte les applications en temps réel

Causes de Haute Latence :

- Congestion de file d'attente (trop d'utilisateurs)
- Problèmes de configuration de planificateur
- Mauvaises conditions radio (beaucoup de retransmissions)
- Retards de backhaul

Compteurs d'Interface S1

M8000 - Mesures de l'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	Requêtes 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	Requêtes de Configuration S1	Tentatives d'établissement de l'interface S1	Entier	Somme
M8000C7	Achèvements de Configuration S1	Configurations S1 réussies	Entier	Somme
M8000C11	Requêtes de Paging S1	Messages de paging de MME	Entier	Somme
M8000C12	Configuration de Connexion S1 Logique 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 des signaux de couche supérieure

Calcul du Taux de Réussite de Configuration :

```
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 l'établissement, la modification et la libération des Porteuses Radio d'Accès E-UTRAN (E-RAB) et des procédures de support EPS.

Compteurs Clés :

Compteur	Nom	Description	Unité	Type
M8006C0	Tentatives de Configuration de Support EPS	Tentatives d'établissement de support	Entier	Somme
M8006C1	Achèvements de Configuration de Support EPS	Établissements de support réussis	Entier	Somme
M8006C2-C5	Échecs de Configuration par Cause	Échecs classés par raison	Entier	Somme

Comprendre les Porteuses EPS :

- **Porteuse** = Canal logique pour les données utilisateur entre l'UE et le réseau
- **Porteuse par Défaut** = Porteuse toujours active pour la connectivité Internet
- **Porteuse Dédiée** = Porteuses supplémentaires pour des exigences QoS spécifiques (VoLTE, streaming vidéo)

Cas d'Utilisation :

- Surveiller les taux de réussite de configuration de porteuse
- Identifier les raisons des échecs de porteuse
- Suivre l'allocation de porteuse QoS pour les 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	Focalisation	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, réussites, échecs

Formule du Taux de Réussite de Transfert :

```
Taux de Réussite de HO = 100 × (Exécutions de HO) / (Tentatives de Préparation de HO)
```

Objectifs de Performance :

- Taux de Réussite de HO Intra-eNB : > 99%
- Taux de Réussite de HO Inter-eNB : > 98%
- Taux de Réussite 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 (l'UE ne répond pas à temps)
- Lacunes de mesure empêchant une sélection correcte de la cellule

---

Mesures de Qualité de Canal

M8010 - Distribution de 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)
- **But :** Aide le planificateur à sélectionner le MCS (Schéma de Modulation et de Codage) approprié
- **Fréquence de Mise à Jour :** Toutes les quelques millisecondes en fonction des conditions du canal

Mapping CQI à Taux de Données :

Niveau CQI	Qualité du Canal	Taux Max Approximatif	Modulation
0-3	Très Pauvre	< 1 Mbps	QPSK
4-6	Pauvre	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 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

---

Mesures de Retour en Circuit Commuté

M8016 - Mesures de Retour en Circuit Commuté

Ces compteurs suivent les procédures de Retour en Circuit Commuté (CSFB), où les UE LTE retournent aux réseaux 2G/3G pour les appels vocaux.

Comprendre le CSFB :

- **But :** Gérer les appels vocaux sur des réseaux sans VoLTE
- **Processus :** UE en LTE → Appel vocal → Déplacement temporaire vers 2G/3G → Retour à LTE
- **Impact :** Délai de configuration d'appel, perte temporaire de données LTE

Compteurs Clés :

Compteur	Nom	Description
M8016C0	Tentatives de CSFB avec redirection	CSFB utilisant la méthode de redirection
M8016C1	Tentatives de CSFB avec transfert	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. **Transfert :** Transfert approprié de LTE vers 2G/3G (plus lent mais sans interruption)

Métriques de Performance :

- Taux de Réussite CSFB = Transitions réussies / Tentatives CSFB totales
- Objectif : > 98%

Compteurs de Volume de Données

M8023 - Mesures de Volume de Données SDU PDCP

Ces compteurs suivent le volume total de données utilisateur transmises sur l'interface air.

Métriques Clés :

- Volume total de données (montant et descendant)
- Volume par QCI (Identifiant de Classe de Service)
- Volume par type de porteuse

Cas d'Utilisation :

- Planification de 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 :** Taux de données instantané (kbit/s)
- **M8023 :** Volume de données cumulatif (octets)

Compteurs d'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 pendant les transferts
- Suivi du volume de trafic X2 entrant et sortant

M8022 - Configuration X2 :

- **M8022C0 :** Tentatives de Configuration X2
- **M8022C1 :** Succès de Configuration X2

Comprendre l'Interface X2 :

- **But :** Communication directe entre les eNodeBs voisins
- **Fonctions :** Coordination des transferts, partage de charge, gestion des interférences
- **Avantage :** Réduit la charge sur le réseau central, transferts plus rapides

Taux de Réussite de Configuration X2 :

```
Taux de Réussite de Configuration X2 = 100 × M8022C1 / M8022C0
```

Objectif : > 95%

Groupes de Mesure Supplémentaires

M8007 - Mesures de Support Radio de Données (DRB)

Suit l'établissement, la modification et la libération des Supports Radio de Données (DRB) pour la transmission de données utilisateur.

Domaines de Focalisation :

- Taux de réussite de configuration de DRB
- Procédures de modification de DRB
- Statistiques de libération de porteuse

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 (PRB insuffisants)
- Limite maximale d'UE atteinte
- Redirection d'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 cellule de LTE vers GSM.

But : Fournit des informations sur le système de cellules voisines GSM aux UE avant la re-sélection, accélérant la transition.

Mesures d'Interface Réseau

M5112 - Mesures d'Entrée d'Interface IP

M5113 - Mesures RX Ethernet

Ces groupes de mesure suivent les statistiques d'interface de backhaul.

M5112 - Entrée d'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 backhaul
- Évaluation de la santé du lien de transport
- Dépannage des problèmes de connectivité

- Planification de capacité pour des 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'onde stationnaire de tension	0.1	Moyenne	Diviser par 10

Comprendre le VSWR :

- **VSWR** = Rapport d'Onde Stationnaire de Tension
- Mesure de l'efficacité du système d'antenne
- Indique un déséquilibre d'impédance et des problèmes potentiels de câble/antenne
- Des 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	Pauvre	Problème de câble/antenne - dépannage immédiat

Causes Courantes de Haut VSWR :

- 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 Énergétique

Compteur	Nom	Description	Unité	Type	Éch
M40002C2	Consommation Énergétique	Consommation d'énergie de la station de base	100000 facteur	Moyenne	Divis par 100

Comprendre la Consommation Énergétique :

- Mesure de la consommation totale d'énergie de la station de base
- Utile pour les calculs OPEX et la planification de 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

Construire des Tableaux de Bord Efficaces

1. Tableau de Bord d'Utilisation des Ressources

Combinez M8011C24 et M8011C37 pour montrer l'utilisation des PRB montants/descendants :

```
// Utilisation 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 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,
      "Mbps Montant": r.M8012C23,
      "Mbps Descendant": r.M8012C26
    }))
```

3. Tableau de Bord de Disponibilité

Calculez et affichez la disponibilité de la cellule :

```
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 Réussite 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 Réussite 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 le Tableau de Bord

Utilisez des Types de Visualisation Appropriés :

- Graphiques de séries temporelles - Données de tendance (débit, utilisation de 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 de PRB : Vert < 70%, Jaune 70-85%, Rouge > 85%
- Disponibilité : Vert > 99%, Jaune 95-99%, Rouge < 95%
- Réussite 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 d'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 moyenne de PRB UL	Planification de capacité	0.1%
M8011C37	Utilisation moyenne de PRB DL	Planification de capacité	0.1%
M8012C23	Débit UL PDCP	Surveillance de performance	kbit/s
M8012C26	Débit DL PDCP	Surveillance de performance	kbit/s
M8018C1	Nombre maximum d'UE actifs	Surveillance de charge	compte
M8020C3	Échantillons de cellule disponible	Suivi de disponibilité	compte
M8020C6	Dénominateur de disponibilité	Calcul de disponibilité	compte
M8013C5	Achèvements de configuration	Suivi du taux de réussite	compte
M8005C0	RSSI min	Analyse de couverture	dBm
M8005C2	RSSI moyen	Analyse de couverture	dBm
M8001C2	Délai moyen PDCP	Surveillance de latence	ms

Compteur	Nom	Cas d'Utilisation	Unité
M40001C0	VSWR	Santé du matériel	0.1 ratio

Sources :

- Mesures de Performance LTE de Nokia FlexiRadio
- Spécifications des Compteurs de Performance Nokia AirScale
- Normes de Gestion de Performance LTE 3GPP

Annexe : Liste Complète des Compteurs

Voici la liste de référence complète de tous les 1,186 compteurs de performance LTE de Nokia extraits de la spécification KPI de Nokia.

```
================================================================================
RÉFÉRENCE COMPLÈTE DES COMPTEURS DE PERFORMANCE LTE NOKIA
================================================================================

--------------------------------------------------------------------------------
Groupe de Mesure : M8000
--------------------------------------------------------------------------------
M8000C0         | Requêtes de Configuration de Contexte Initial
entier
M8000C1         | Achèvements de Configuration de Contexte Initial
entier
M8000C2         | Échecs de Configuration de Contexte Initial dus à
M8000C3         | Échecs de Configuration de Contexte Initial dus à
M8000C4         | Échecs de Configuration de Contexte Initial dus à
M8000C5         | Échecs de Configuration de Contexte Initial dus à
M8000C6         | Requêtes de Configuration S1
M8000C7         | Achèvements de Configuration S1
M8000C8         | Échec de Configuration S1 dû à l'expiration du minu
entier
M8000C9         | Échec de Configuration S1 dû au rejet du MME
M8000C11        | Requêtes de Paging S1
M8000C12        | Nombre de S1 logiques associés à l'UE
M8000C13        | Réinitialisation globale S1 initiée par l'eNB
M8000C14        | Réinitialisation globale S1 initiée par le MME
M8000C15        | Réinitialisation partielle S1 initiée par l'eNB
M8000C16        | Réinitialisation partielle S1 initiée par le MME
M8000C23        | Tentatives de modification de contexte UE
M8000C24        | Tentatives de modification de contexte UE dues à
M8000C25        | Échecs de modification de contexte UE
M8000C29        | Nombre de Transport NAS Montant
M8000C30        | Nombre de Transport NAS Descendant
M8000C31        | Tentatives de modification de contexte UE dues à
M8000C32        | Requêtes de Configuration E-RAB pour IMS
M8000C33        | Achèvements de Configuration E-RAB pour IMS
M8000C34        | Échecs de configuration E-RAB pour IMS
M8000C35        | Nombre de contrôles de rapport de localisation
M8000C36        | Nombre de messages de rapport de localisation
M8000C37        | Nombre d'adresses IP X2 réussies
M8000C38        | Nombre d'adresses IP X2 tentées
M8000C39        | Nombre de WRITE-REPLACE
M8000C40        | Nombre de WRITE-REPLACE
M8000C41        | Nombre de messages de demande de KILL
M8000C42        | Nombre de réponses de KILL
```

```
-----------------------------------------------------------------------
Groupe de Mesure : M8001
-----------------------------------------------------------------------
M8001C0         | Délai SDU PDCP sur DL DTCH Min
M8001C1         | Délai SDU PDCP sur DL DTCH Max
M8001C2         | Délai SDU PDCP sur DL DTCH Moyenne
M8001C3         | Délai SDU PDCP sur UL DTCH Min
M8001C4         | Délai SDU PDCP sur UL DTCH Max
M8001C5         | Délai SDU PDCP sur UL DTCH Moyenne
M8001C6         | Tentatives de configuration RACH pour petite taille
entier
M8001C7         | Tentatives de configuration RACH pour grande taille
entier
M8001C8         | Achèvements de configuration RACH
M8001C9         | TBs transmis sur PCH
M8001C10        | TBs transmis sur BCH
M8001C11        | TBs transmis sur DL-SCH
M8001C12        | Retransmissions HARQ sur DL-SCH
M8001C13        | TB UL non dupliqués corrects avec
M8001C14        | TB UL corrects avec réception répétée
M8001C15        | Réceptions erronées de TB UL
M8001C16        | Transmissions PUSCH utilisant MCS0
M8001C17        | Transmissions PUSCH utilisant MCS1
M8001C18        | Transmissions PUSCH utilisant MCS2
M8001C19        | Transmissions PUSCH utilisant MCS3
M8001C20        | Transmissions PUSCH utilisant MCS4
M8001C21        | Transmissions PUSCH utilisant MCS5
M8001C22        | Transmissions PUSCH utilisant MCS6
M8001C23        | Transmissions PUSCH utilisant MCS7
M8001C24        | Transmissions PUSCH utilisant MCS8
M8001C25        | Transmissions PUSCH utilisant MCS9
M8001C26        | Transmissions PUSCH utilisant MCS10
M8001C27        | Transmissions PUSCH utilisant MCS11
M8001C28        | Transmissions PUSCH utilisant MCS12
M8001C29        | Transmissions PUSCH utilisant MCS13
M8001C30        | Transmissions PUSCH utilisant MCS14
M8001C31        | Transmissions PUSCH utilisant MCS15
M8001C32        | Transmissions PUSCH utilisant MCS16
M8001C33        | Transmissions PUSCH utilisant MCS17
M8001C34        | Transmissions PUSCH utilisant MCS18
M8001C35        | Transmissions PUSCH utilisant MCS19
M8001C36        | Transmissions PUSCH utilisant MCS20
M8001C37        | Transmissions PUSCH utilisant MCS21
```

```
M8001C38        | Transmissions PUSCH utilisant MCS22
M8001C39        | Transmissions PUSCH utilisant MCS23
M8001C40        | Transmissions PUSCH utilisant MCS24
M8001C41        | Transmissions PUSCH utilisant MCS25
M8001C42        | Transmissions PUSCH utilisant MCS26
M8001C43        | Transmissions PUSCH utilisant MCS27
M8001C44        | Transmissions PUSCH utilisant MCS28
M8001C45        | Transmissions PDSCH utilisant MCS0
M8001C46        | Transmissions PDSCH utilisant MCS1
M8001C47        | Transmissions PDSCH utilisant MCS2
M8001C48        | Transmissions PDSCH utilisant MCS3
M8001C49        | Transmissions PDSCH utilisant MCS4
M8001C50        | Transmissions PDSCH utilisant MCS5
M8001C51        | Transmissions PDSCH utilisant MCS6
M8001C52        | Transmissions PDSCH utilisant MCS7
M8001C53        | Transmissions PDSCH utilisant MCS8
M8001C54        | Transmissions PDSCH utilisant MCS9
M8001C55        | Transmissions PDSCH utilisant MCS10
M8001C56        | Transmissions PDSCH utilisant MCS11
M8001C57        | Transmissions PDSCH utilisant MCS12
M8001C58        | Transmissions PDSCH utilisant MCS13
M8001C59        | Transmissions PDSCH utilisant MCS14
M8001C60        | Transmissions PDSCH utilisant MCS15
M8001C61        | Transmissions PDSCH utilisant MCS16
M8001C62        | Transmissions PDSCH utilisant MCS17
M8001C63        | Transmissions PDSCH utilisant MCS18
M8001C64        | Transmissions PDSCH utilisant MCS19
M8001C65        | Transmissions PDSCH utilisant MCS20
M8001C66        | Transmissions PDSCH utilisant MCS21
M8001C67        | Transmissions PDSCH utilisant MCS22
M8001C68        | Transmissions PDSCH utilisant MCS23
M8001C69        | Transmissions PDSCH utilisant MCS24
M8001C70        | Transmissions PDSCH utilisant MCS25
M8001C71        | Transmissions PDSCH utilisant MCS26
M8001C72        | Transmissions PDSCH utilisant MCS27
M8001C73        | Transmissions PDSCH utilisant MCS28
M8001C74        | Transmissions PUSCH utilisant MCS0
M8001C75        | Transmissions PUSCH utilisant MCS1
M8001C76        | Transmissions PUSCH utilisant MCS2
M8001C77        | Transmissions PUSCH utilisant MCS3
M8001C78        | Transmissions PUSCH utilisant MCS4
M8001C79        | Transmissions PUSCH utilisant MCS5
M8001C80        | Transmissions PUSCH utilisant MCS6
M8001C81        | Transmissions PUSCH utilisant MCS7
```

M8001C82	Transmissions PUSCH utilisant MCS8
M8001C83	Transmissions PUSCH utilisant MCS9
M8001C84	Transmissions PUSCH utilisant MCS10
M8001C85	Transmissions PUSCH utilisant MCS11
M8001C86	Transmissions PUSCH utilisant MCS12
M8001C87	Transmissions PUSCH utilisant MCS13
M8001C88	Transmissions PUSCH utilisant MCS14
M8001C89	Transmissions PUSCH utilisant MCS15
M8001C90	Transmissions PUSCH utilisant MCS16
M8001C91	Transmissions PUSCH utilisant MCS17
M8001C92	Transmissions PUSCH utilisant MCS18
M8001C93	Transmissions PUSCH utilisant MCS19
M8001C94	Transmissions PUSCH utilisant MCS20
M8001C95	Transmissions PUSCH utilisant MCS21
M8001C96	Transmissions PUSCH utilisant MCS22
M8001C97	Transmissions PUSCH utilisant MCS23
M8001C98	Transmissions PUSCH utilisant MCS24
M8001C99	Transmissions PUSCH utilisant MCS25
M8001C100	Transmissions PUSCH utilisant MCS26
M8001C101	Transmissions PUSCH utilisant MCS27
M8001C102	Transmissions PUSCH utilisant MCS28
M8001C103	Transmissions PUSCH utilisant MCS29
M8001C104	Transmissions PUSCH utilisant MCS30
M8001C105	Transmissions PUSCH utilisant MCS31
M8001C106	Transmissions PUSCH utilisant MCS32
M8001C107	Transmissions PUSCH utilisant MCS33
M8001C108	Transmissions PUSCH utilisant MCS34
M8001C109	Transmissions PUSCH utilisant MCS35
M8001C110	Transmissions PUSCH utilisant MCS36
M8001C111	Transmissions PUSCH utilisant MCS37
M8001C112	Transmissions PUSCH utilisant MCS38
M8001C113	Transmissions PUSCH utilisant MCS39
M8001C114	Transmissions PUSCH utilisant MCS40
M8001C115	Transmissions PUSCH utilisant MCS41
M8001C116	Transmissions PUSCH utilisant MCS42
M8001C117	Transmissions PUSCH utilisant MCS43
M8001C118	Transmissions PUSCH utilisant MCS44
M8001C119	Transmissions PUSCH utilisant MCS45
M8001C120	Transmissions PUSCH utilisant MCS46
M8001C121	Transmissions PUSCH utilisant MCS47
M8001C122	Transmissions PUSCH utilisant MCS48
M8001C123	Transmissions PUSCH utilisant MCS49
M8001C124	Transmissions PUSCH utilisant MCS50
M8001C125	Transmissions PUSCH utilisant MCS51

M8001C126	Transmissions PUSCH utilisant MCS52
M8001C127	Transmissions PUSCH utilisant MCS53
M8001C128	Transmissions PUSCH utilisant MCS54
M8001C129	Transmissions PUSCH utilisant MCS55
M8001C130	Transmissions PUSCH utilisant MCS56
M8001C131	Transmissions PUSCH utilisant MCS57
M8001C132	Transmissions PUSCH utilisant MCS58
M8001C133	Transmissions PUSCH utilisant MCS59
M8001C134	Transmissions PUSCH utilisant MCS60
M8001C135	Transmissions PUSCH utilisant MCS61
M8001C136	Transmissions PUSCH utilisant MCS62
M8001C137	Transmissions PUSCH utilisant MCS63
M8001C138	Transmissions PUSCH utilisant MCS64
M8001C139	Transmissions PUSCH utilisant MCS65
M8001C140	Transmissions PUSCH utilisant MCS66
M8001C141	Transmissions PUSCH utilisant MCS67
M8001C142	Transmissions PUSCH utilisant MCS68
M8001C143	Transmissions PUSCH utilisant MCS69
M8001C144	Transmissions PUSCH utilisant MCS70
M8001C145	Transmissions PUSCH utilisant MCS71
M8001C146	Transmissions PUSCH utilisant MCS72
M8001C147	Transmissions PUSCH utilisant MCS73
M8001C148	Transmissions PUSCH utilisant MCS74
M8001C149	Transmissions PUSCH utilisant MCS75
M8001C150	Transmissions PUSCH utilisant MCS76
M8001C151	Transmissions PUSCH utilisant MCS77
M8001C152	Transmissions PUSCH utilisant MCS78
M8001C153	Transmissions PUSCH utilisant MCS79
M8001C154	Transmissions PUSCH utilisant MCS80
M8001C155	Transmissions PUSCH utilisant MCS81
M8001C156	Transmissions PUSCH utilisant MCS82
M8001C157	Transmissions PUSCH utilisant MCS83
M8001C158	Transmissions PUSCH utilisant MCS84
M8001C159	Transmissions PUSCH utilisant MCS85
M8001C160	Transmissions PUSCH utilisant MCS86
M8001C161	Transmissions PUSCH utilisant MCS87
M8001C162	Transmissions PUSCH utilisant MCS88
M8001C163	Transmissions PUSCH utilisant MCS89
M8001C164	Transmissions PUSCH utilisant MCS90
M8001C165	Transmissions PUSCH utilisant MCS91
M8001C166	Transmissions PUSCH utilisant MCS92
M8001C167	Transmissions PUSCH utilisant MCS93
M8001C168	Transmissions PUSCH utilisant MCS94
M8001C169	Transmissions PUSCH utilisant MCS95

```
M8001C170       | Transmissions PUSCH utilisant MCS96
M8001C171       | Transmissions PUSCH utilisant MCS97
M8001C172       | Transmissions PUSCH utilisant MCS98
M8001C173       | Transmissions PUSCH utilisant MCS99
M8001C174       | Transmissions PUSCH utilisant MCS100
M8001C175       | Transmissions PUSCH utilisant MCS101
M8001C176       | Transmissions PUSCH utilisant MCS102
M8001C177       | Transmissions PUSCH utilisant MCS103
M8001C178       | Transmissions PUSCH utilisant MCS104
M8001C179       | Transmissions PUSCH utilisant MCS105
M8001C180       | Transmissions PUSCH utilisant MCS106
M8001C181       | Transmissions PUSCH utilisant MCS107
M8001C182       | Transmissions PUSCH utilisant MCS108
M8001C183       | Transmissions PUSCH utilisant MCS109
M8001C184       | Transmissions PUSCH utilisant MCS110
M8001C185       | Transmissions PUS
```

Guide de Collecte des Données PM

Vue d'ensemble

La page de collecte des 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 stocker tous ces compteurs n'est ni pratique ni nécessaire pour la plupart des cas d'utilisation.

Ce guide explique comment sélectionner les compteurs à collecter en fonction de vos exigences de surveillance.

Démarrage Rapide

Accéder à la Page de Collecte des Données PM

1. Naviguez vers le Panneau de Contrôle : `https://localhost:9443`
2. Cliquez sur **Filtres de Données** dans le menu de navigation
3. Visualisez 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 collection

---

Catégories de Compteurs

Les compteurs PM sont classés 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 incluent 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 des Blocs 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 la 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 **Sélectionner Tout** 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

Filtrage et Recherche

Les deux sections supportent :

- **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 changements apportés à votre sélection de compteurs PM sont :

1. **Persistés sur disque** dans `priv/pm_filters.etf`
2. **Survivent aux redémarrages de l'application**
3. **Prennent effet immédiatement** (aucun redémarrage requis)

Le rédacteur de lot InfluxDB est informé des changements et commence/arrête immédiatement la collecte des 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 des Requêtes	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 des 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 SDU PDCP DL moyen
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 de liaison montante moyen
M8012C26,Débit,Débit de liaison descendante 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 Prendre Effet

1. Les changements de filtre sont appliqués immédiatement au rédacteur de lot
2. **Les nouvelles données n'apparaissent qu'après le prochain envoi de PM de l'eNodeB** (typiquement toutes les 15 minutes)
3. Vérifiez les journaux de l'application pour les 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 des 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

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 ?

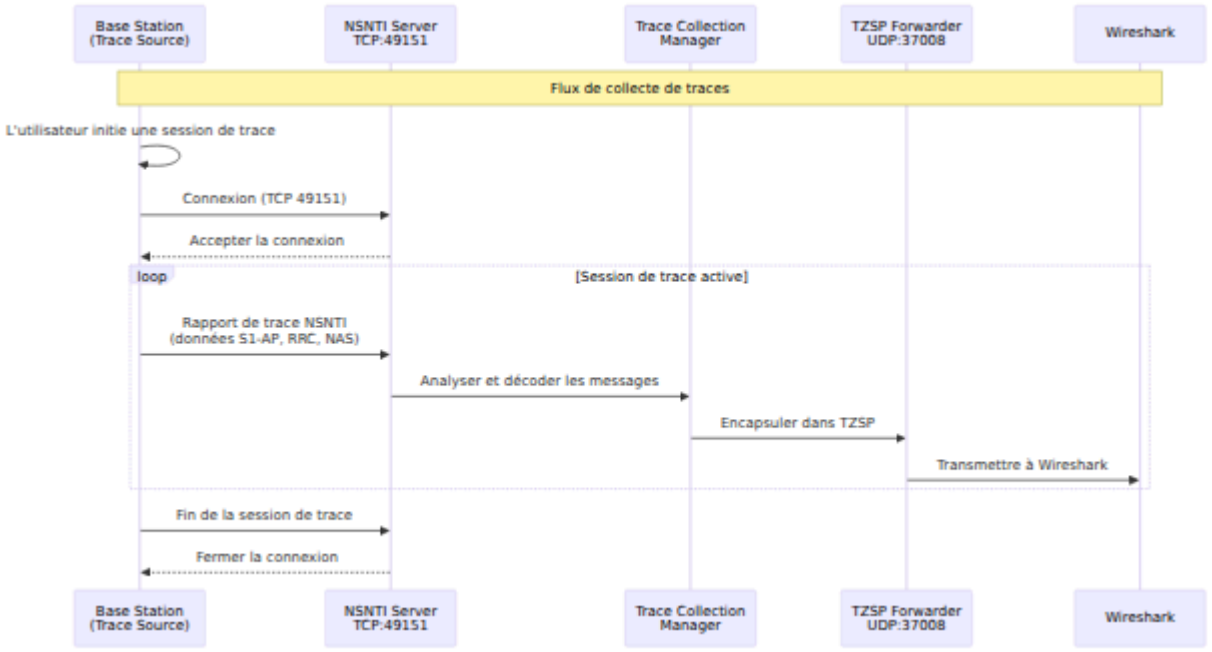
L'Entité de collecte de traces reçoit des données de trace des stations de base Nokia AirScale contenant :

- **Messages S1-AP** - Signalisation du plan de contrôle entre eNodeB et EPC
- **Messages RRC** - Signalisation du 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 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 montrer : 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 du 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 dans **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 modifiez `~/.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 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 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 :

```
# Montrer tous les paquets TZSP
tzsp

# Montrer des protocoles spécifiques
s1ap || rrc || mac-lte

# Montrer uniquement les messages RRC en liaison montante
udp.port == 37011 || udp.port == 37012

# Montrer uniquement les messages RRC en liaison descendante
udp.port == 37001 || udp.port == 37002

# Montrer l'établissement de connexion RRC
rrc.rrcConnectionRequest || rrc.rrcConnectionSetup

# Montrer 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 perdus
- 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 UE 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'TCE (Entité de collecte de traces) est intégrée dans le RAN Monitor Omnitouch et gère la conversion des traces de protocole Ne3s spécifiques à Nokia en formats standard visualisables 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 les licences 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 (voir TCE README)
- 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 visualisables 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 dans 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 immédiate (temps réel) ou MDT enregistrée (mode inactif)
- **Portée de la zone** : Spécifique à la cellule, zone de suivi ou PLMN
- **Intervalle de mesure** : À quelle fréquence les UE 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.

Visualiser les données MDT dans Wireshark

Configurer la capture Wireshark

1. Démarrez Wireshark sur votre machine
2. Capturez sur l'**interface de boucle** (`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 de connexion), 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 :

```
# Montrer tous les rapports de mesure RRC
lte-rrc.measurementReport

# Montrer 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 cellule physique 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
        └─ Rapport de mesure
            └─ 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. Traiter 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 UE 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 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 la trace à MAXIMUM

- Assurez-vous que les UE 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 vérification 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 avec le filtre `udp port 37008`
- [ ] Appliquez le filtre d'affichage : `lte-rrc.measurementReport`
- [ ] Analysez les mesures et exportez au besoin

Support

- **Omnitouch Network Services (ONS)** : Pour l'assistance à la configuration, aux licences et au déploiement d'AirScale

Guide de Dépannage

Résolution de Problèmes pour RAN Monitor

Problèmes courants, procédures de diagnostic et solutions

Table des Matières

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 de RAN Monitor

---

Table des matières

Aperçu

RAN Monitor comprend un panneau de contrôle intégré basé sur le Web pour la surveillance et la gestion opérationnelles 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 de session
- Administration système

Grafana est idéal pour :

- Analyse des tendances historiques
- Tableaux de bord KPI personnalisés
- Planification de capacité à long terme
- Identification de modèles
- Reporting exécutif

Pour les tableaux de bord et analyses Grafana, voir 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 CA
- Certificats configurés dans `config/runtime.exs`

Pour les détails de configuration, voir 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 du système et connectivité

Résumé des appareils

- Nombre d'appareils associés/échoués
- Aperçu 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

- Se rafraîchit automatiquement toutes les 5 secondes
- Indicateurs d'état codés par couleur (vert = sain, rouge = problèmes)
- Navigation par clic vers des vues détaillées
- Mises à jour 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 eNodeB NOKIA 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 agrégés des appareils :

Statistique	Description
Total des appareils	Nombre d'appareils configurés
Connectés	Appareils avec des sessions actives
En attente	Appareils en attente d'enregistrement
Déconnectés	Appareils sans session active

Tableau des appareils

Colonne	Description
Nom	Nom de l'appareil tel que configuré
État	État de connexion : "Connecté" (vert) ou "Déconnecté" (rouge)
Adresse	Adresse IP de l'appareil et port
Session	État de la session : "Active" (vert) ou "Inactive" (gris)
Actions	Boutons d'action de l'appareil

Boutons d'action

Chaque ligne d'appareil a des boutons d'action :

Bouton	Description
Ping	Tester la connectivité réseau vers l'appareil
Config	Voir la configuration actuelle de l'appareil
Config Ops	Accéder aux opérations de gestion de la configuration (télécharger, télécharger, valider, activer)
Force Retry	Forcer une nouvelle tentative d'enregistrement pour les appareils déconnectés

Panneau de détails de l'appareil

Cliquer sur une ligne d'appareil montre 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 ex., 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 détaillée 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 en cours d'utilisation
- Clés et certificats du gestionnaire

Cycle de vie de la session

- Heure de création de la session
- Heure d'expiration de la session
- Intervalle de maintien en vie et état

- Dernier horodatage de maintien en vie
- Temps restant avant 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 de l'alarme et description
- Horodatages des alarmes
- Informations sur la cause probable

État de la configuration

- Valeurs de paramètres actuelles
- Changements de configuration récents
- Horodatage de la 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) - Affecte le service, action immédiate requise
- **Majeur** (Orange) - Dégradation significative, attention urgente nécessaire

- **Mineur** (Jaune) - N'affecte pas 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, voir 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. Cliquer sur "Télécharger la configuration"
3. La configuration est récupérée depuis l'appareil
4. Sauvegarder la configuration sous forme de fichier XML

Meilleure pratique : Toujours télécharger et sauvegarder la configuration avant de faire des changements

Télécharger la configuration

Objectif : Appliquer une nouvelle configuration à l'appareil

Étapes :

1. Sélectionner le fichier de configuration XML
2. Cliquer sur "Télécharger la configuration"
3. La configuration est téléchargée sur l'appareil (crée un "plan")
4. Le système retourne un ID de plan pour le suivi

Important : Le téléchargement ne crée qu'un plan - il n'active pas la configuration

Valider la configuration

Objectif : Vérifier que la configuration est valide avant activation

Étapes :

1. Entrer l'ID de plan du téléchargement
2. Cliquer sur "Valider"
3. L'appareil valide la syntaxe et les paramètres
4. Le système confirme la préparation à l'activation ou signale des erreurs

Remarque : Toujours valider avant d'activer pour éviter les erreurs de configuration

Activer la configuration

Objectif : Appliquer le plan de configuration validé

Étapes :

1. Entrer l'ID de plan validé
2. Cliquer sur "Activer la configuration"
3. Les changements prennent effet immédiatement sur l'appareil
4. Surveiller l'état pour succès/échec

Avertissement : L'activation est immédiate et peut affecter le service - s'assurer que la validation a réussi d'abord

Flux de travail de configuration

Processus recommandé :

1. Télécharger la configuration actuelle (sauvegarde)
2. Modifier la configuration hors ligne
3. Télécharger la nouvelle configuration (obtenir l'ID de plan)
4. Valider la configuration (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 l'appareil pour la stabilité

Pour des détails sur la configuration de la station de base, voir 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/décommissionnés

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** dans le tableau
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, voir 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
- **Provisioning :** Vérifier les identifiants des appareils avant la configuration
- **Décommissionnement :** 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 système.

Niveaux de journal

Filtrer par niveau de journal :

- **Urgent** - Échecs critiques pour le système
- **Alerte** - Action immédiate requise
- **Critique** - Conditions critiques
- **Erreur** - Conditions d'erreur
- **Avertissement** - Conditions d'avertissement
- **Avis** - 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

- Flux de journal en temps réel (derniers 500 messages)
- Filtrer par niveau de journal

Contrôles :

- **Pause/Reprendre** - Arrêter le flux de journal en direct pour examiner les messages
- **Effacer** - Supprimer tous les journaux de l'affichage
- **Niveau système** - Changer dynamiquement le niveau de journal à l'échelle de l'application

Codage couleur :

- Rouge - Urgent/Alerte/Niveaux critiques
- Rouge clair - Niveau d'erreur
- Jaune - Niveau d'avertissement
- Cyan - Niveau d'avis
- Bleu - Niveau d'info
- Gris - Niveau de 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 système :

- Surveiller les journaux de niveau info pour les opérations normales
- Suivre les événements d'enregistrement d'appareils
- Surveiller l'activité de collecte de données

Déboguer des problèmes :

- Définir temporairement le niveau de débogage

- Reproduire le problème
- Examiner les journaux détaillés
- Revenir au niveau d'info lorsque c'est terminé

Enquêter sur les échecs :

- Rechercher des messages d'erreur et des traces de pile
- Examiner les horodatages autour du moment de l'échec
- Corréler avec les événements de l'appareil

Meilleures pratiques

- **Utilisez Pause** lors de l'examen de séquences d'erreurs spécifiques
- **Définissez 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

- Nombre 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 que les nettoyages s'exécutent toutes les heures
- État du travailleur 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. **Surcharge 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 diminuant 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 InfluxDB

Avertissement : Effacer toutes les données est permanent et ne peut pas être annulé. Toujours vérifier avant d'exécuter.

Pour des informations détaillées sur la politique de conservation, voir 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 lorsqu'il est déconnecté
Base de données	Nom du bucket InfluxDB configuré
Version d'InfluxDB	Version de la 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 depuis les 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 d'écriture
PM Filtrés	Nombre de compteurs PM filtrés (compteurs non-dashboard non dans la liste des données PM stockées)
Chutes de file d'attente	Points abandonnés en raison d'un débordement de file d'attente (doit être 0 en fonctionnement normal)
Cache de configuration	Nombre de hachages de configuration uniques mis en cache pour la détection des deltas
Cache d'alarmes	Nombre d'alarmes actives mises en cache pour la détection des deltas

Métriques supplémentaires :

Métrique	Description
Total écrit	Points cumul��s écrits dans InfluxDB depuis le démarrage
Flushes	Nombre d'opérations de vidage par lot
Filtrés	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 des deltas. 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 du bucket InfluxDB
État	Badge d'état de connexion
Mesures	Nombre de types de mesures (3 : PerformanceMetrics, Configuration, Alarmes)

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 depuis les appareils
- **Conservation des données** - État de la politique de conservation actuelle
- **Dernière synchronisation** - La dernière synchronisation des données

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 du compteur 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
- Dépanner les problèmes de performance d'écriture
- Vérifiez l'efficacité du cache de détection des deltas
- Confirmez que les données sont écrites

Page des métriques système

Surveillance des performances 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 résumées 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	Nombre de points de données PM écrits
Configuration	Nombre de snapshots de configuration écrits
Alarmes	Nombre d'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 (XML, charges utiles 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

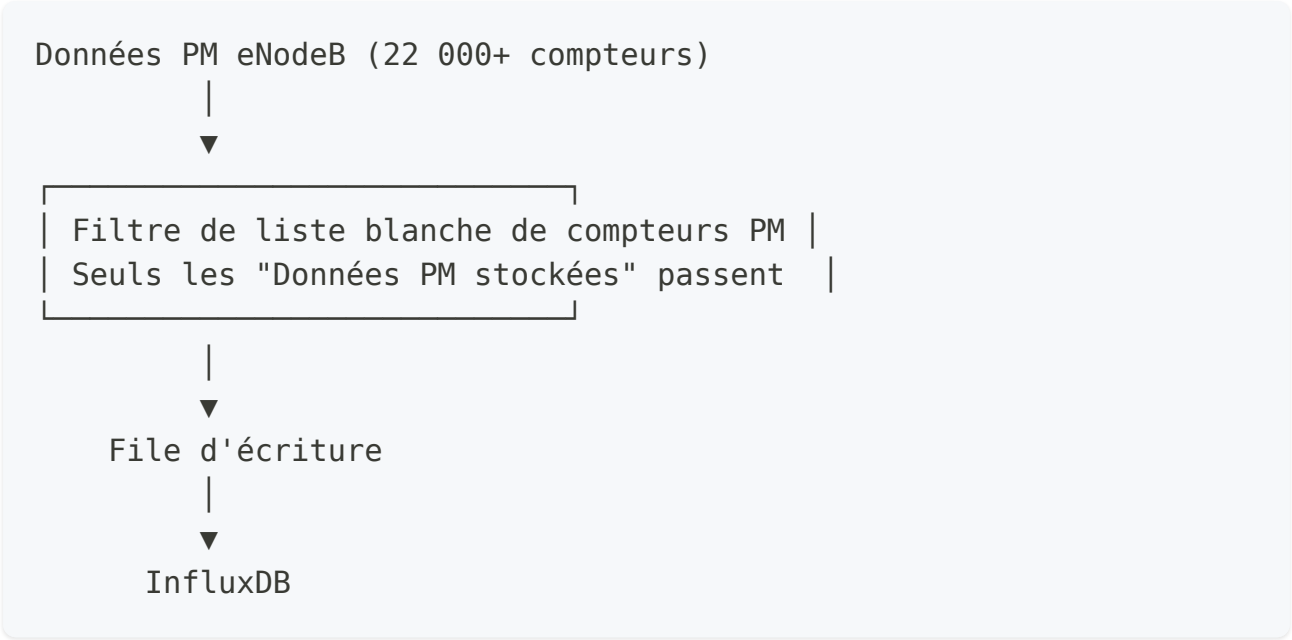
Page de collecte de données PM

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 de requête.

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 la sélection** : Arrêter de collecter les compteurs sélectionnés
- **Sélectionner tout** : Sélectionner tous les compteurs visibles
- **Réinitialiser aux valeurs par défaut** : Restaurer la liste d'origine depuis `pm_counters.csv`

Panneau des compteurs disponibles

Parcourez et ajoutez des compteurs depuis la référence complète des PM de Nokia.

Filtres :

- **Recherche** : Trouver des compteurs par ID ou mots-clés de description
- **Catégorie** : Filtrer par catégorie technologique

Actions :

- **Ajouter la sélection** : 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 des statistiques de filtrage :

- **PM Filtrés** : Nombre de 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 des compteurs, voir le Guide de collecte de données PM.

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 d'appareil mises en cache
Cache d'alarmes Nokia	Enregistrements d'alarmes actives mis en cache
Cache d'enregistrement 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 lors de la prochaine demande.

Fichiers temporaires

Fichiers créés lors de l'extraction et du traitement de la configuration :

- Extractions 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

Nettoyage 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 nombre d'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 décommissionnés

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 service

Étapes :

1. Ouvrir le tableau de bord principal
2. Vérifier que tous les appareils affichent un état 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 en premier)
3. Cliquer 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 se dissipe

Pour des procédures détaillées de gestion des alarmes, voir 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 (état 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, voir le Guide des opérations courantes.

Dépannage des problèmes de 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 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, voir 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 et escalade des alarmes
- **Guide de configuration d'exécution** - Configuration du système
- **Guide d'intégration Grafana** - Analytique 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

Guide des opérations du Moniteur RAN

Plateforme de surveillance et de gestion du Réseau d'Accès Radio (RAN)

par Omnitouch Network Services

Table des matières

Aperçu

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

Fonctionnalités 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 les 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	Objectif	Accès
Gestionnaire de Moniteur RAN	Application principale gérant les connexions des stations de base	Service en arrière-plan
Panneau de contrôle de l'interface Web	Tableau de bord opérationnel en temps réel	https://<server>:9443
Base de données MySQL	État de session et configuration des appareils	Interne
InfluxDB	Stockage des métriques temporelles	http://<server>:8086
Grafana	Tableaux de bord analytiques 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

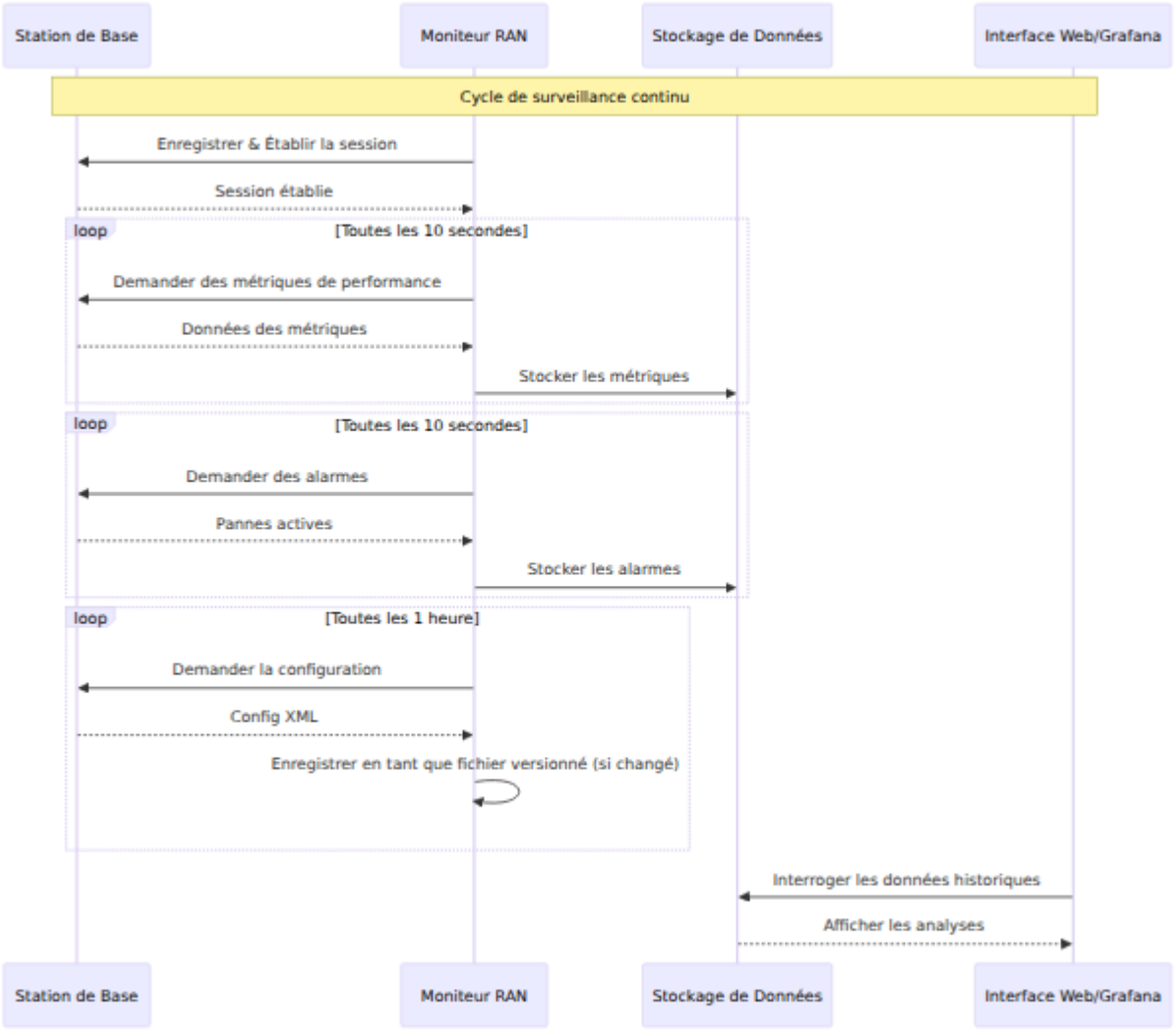
Tableau de bord de surveillance complet montrant l'état des connexions S1 par LNMME, l'état opérationnel, les données transférées, les UEs connectés, l'utilisation moyenne des PRB, les métriques de surveillance de performance et la carte de couverture géographique. Ce tableau de bord fournit aux opérateurs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

Ce que fait le Moniteur RAN

Le Moniteur RAN fonctionne en continu en arrière-plan pour :

1. **Enregistrer et se connecter** - Établit des connexions sécurisées avec vos stations de base Nokia
2. **Collecter des données de performance** - Rassemble des 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 temporelle
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 des cellules
- Débit de trafic (montant/descendant)
- Utilisation des ressources (utilisation des PRB)
- Taux de réussite de mise en place des appels
- Performance des transferts
- Mesures de qualité radio

Alarmes :

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

Configuration :

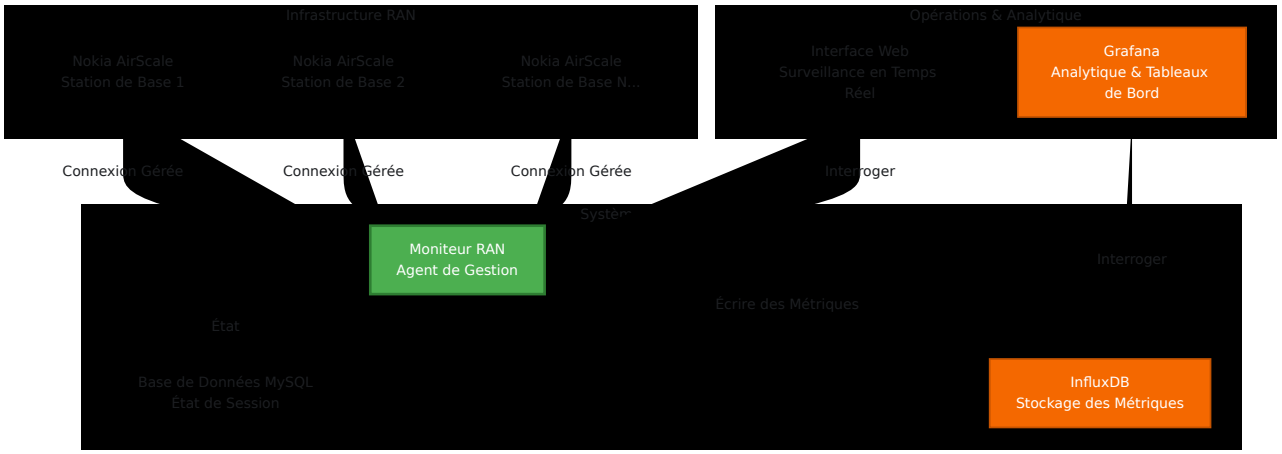
- Instantanés complets de configuration XML (stockés en tant que fichiers versionnés)
- Détection automatique des changements et versionnage
- Historique de configuration et piste d'audit
- Dernières 10 versions conservées par appareil

Pour les détails de gestion de configuration, voir le Guide d'archive de configuration.

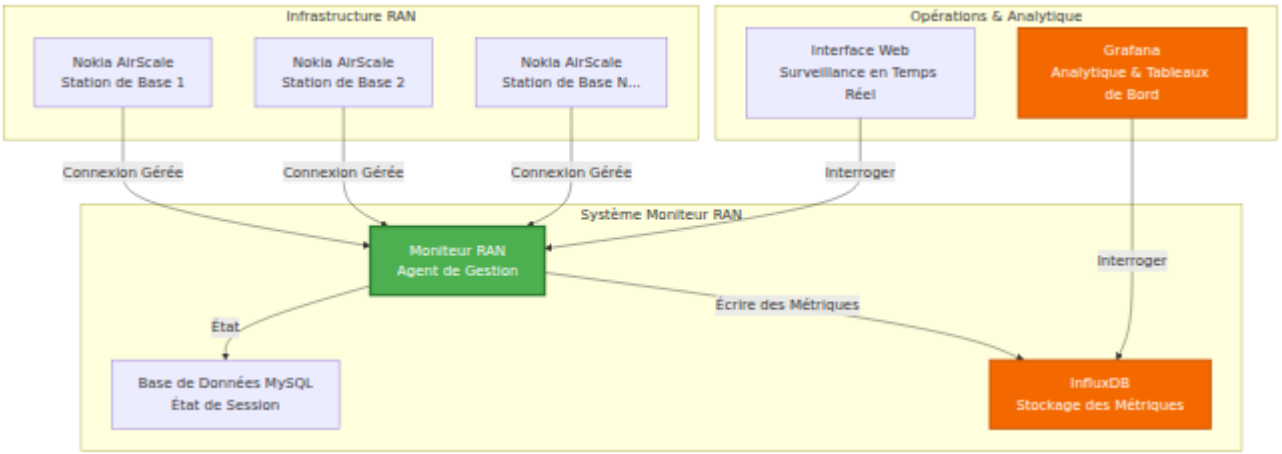
Pour des définitions de compteurs détaillées, voir le Référence des compteurs Nokia.

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)

Le Moniteur RAN 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 le 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-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 des appels
- 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

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

Le Moniteur RAN comprend une interface Web intégrée pour la surveillance et la gestion opérationnelle 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 appareils et les alarmes actives.

Pages clés

Tableau de bord principal

Aperçu du système en temps réel avec :

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

Actualisations automatiques toutes les 5 secondes pour une visibilité en temps réel.

Page des Stations de Base

Voir tous les appareils 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 appareil 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 sur votre réseau :

- Codage couleur par 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.

Archive de configuration : Tous les changements de configuration sont automatiquement suivis et versionnés. Consultez les configurations historiques, téléchargez des versions précédentes ou comparez les changements via la page d'archive de configuration.

Pour des procédures détaillées, voir le Guide de l'interface Web - Gestion de la configuration et le Guide d'archive de configuration.

---

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 de la dernière vue
- Nombre de tentatives de connexion
- Actions : Actualiser, Supprimer, Tout effacer

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 dans tous les messages
- Mettre en pause/Reprendre le streaming en direct
- Changer dynamiquement le niveau de journal système
- Codage couleur par gravité

Pour les procédures de dépannage, voir le Guide de dépannage.

Politique de conservation des données

Gérez la durée de stockage des données dans InfluxDB :

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

Pour des informations complètes sur la conservation des données, voir le Guide de politique de conservation des données.

État d'InfluxDB

Surveillez la santé de la base de données temporelle :

- Indicateur de statut de connexion
- Comptes de mesures par type
- Informations de stockage
- Version et configuration de la base de données
- Actualisations automatiques toutes les 5 minutes

Interprétation de l'état :

- Connecté + Comptes croissants = Fonctionnement normal
- Connecté + Pas de données = Vérifiez l'enregistrement de l'appareil
- 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 modèles 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 appareils
- 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 de résumé exécutif :

- Aperçu de la santé du réseau
- Nombre total d'alarmes par gravité

- Disponibilité moyenne des cellules sur tous les sites
- Métriques agrégées de débit et de capacité
- Grille d'état des appareils

Tableau de bord des opérations NOC :

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

Tableau de bord d'analyse approfondie d'ingénierie :

- Analyse des modèles de trafic
- Métriques de qualité des cellules (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 appareils affichent un statut vert
3. Vérifier le nombre d'alarmes et leur gravité
4. Examiner les appareils 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 l'appareil 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 appareils

Ajout d'une nouvelle station de base :

1. Vérifier la connectivité réseau avec l'appareil
2. Vérifier la page des eNodeBs non configurés pour l'appareil
3. Ajouter l'appareil à `config/runtime.exs`
4. Redémarrer le Moniteur RAN
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 préserver ou de supprimer les données historiques
2. Commenter ou supprimer l'appareil de `config/runtime.exs`
3. Optionnellement, effacer les données via la page de conservation des données
4. Redémarrer le Moniteur RAN
5. Mettre à jour les tableaux de bord Grafana

Mise à jour des identifiants de l'appareil :

1. Noter l'état actuel de l'appareil
2. Mettre à jour les identifiants dans `config/runtime.exs`
3. Redémarrer le Moniteur RAN
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 sécurisée :

1. **Télécharger** la configuration actuelle (sauvegarde) - ou récupérer depuis l'archive de configuration
2. **Modifier** la configuration hors ligne
3. **Télécharger** sur l'appareil → 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 de l'appareil pendant 15-30 minutes
8. **Confirmer** que la nouvelle version apparaît dans l'archive de configuration (dans l'heure)

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

Rollback de configuration : Si des problèmes surviennent, téléchargez une version précédente depuis l'archive 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'archive de configuration.

Index de documentation

La documentation du Moniteur RAN est organisée par public et cas d'utilisation :

Pour les équipes d'opérations (NOC, Administrateurs)

Document	Objectif	Quand l'utiliser
Guide de l'interface Web	Référence complète du panneau de contrôle	Opérations quotidiennes, surveillance des appareils
Guide des opérations courantes	Tâches de gestion quotidiennes	Ajout d'appareils, gestion des configs, sauvegardes
Guide d'archive de configuration	Versionnage et historique de la config	Suivi des changements de config, rollback, audit
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 d'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	Objectif	Quand l'utiliser
Guide d'intégration Grafana	Tableaux de bord, requêtes et alertes	Création de tableaux de bord, configuration des alertes
Référence des compteurs Nokia	Définitions des compteurs de performance	Comprendre les métriques, créer des requêtes
Guide de configuration AirScale	Configuration et mise en place des stations de base	Configurer des appareils, comprendre les paramètres
Guide de collecte de données TCE MDT	Collecte de traces MDT et analyse Wireshark	Collecte de données de tests 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 d'exécution	Référence complète de configuration	Configuration initiale, modification des paramètres

Démarrage rapide

Nouveau dans le Moniteur RAN ?

1. Commencez par le Guide de l'interface Web pour apprendre l'interface
2. Consultez le Guide des opérations courantes pour les tâches de routine
3. Étudiez le Guide de gestion des alarmes pour la gestion des alarmes
4. Gardez le Guide de dépannage en favori pour les problèmes

Configuration de la surveillance ?

1. Consultez le Guide d'intégration Grafana pour les tableaux de bord
2. Référez-vous à la Référence des 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 analytiques 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 de session :

- Le Moniteur RAN établit des sessions avec les stations de base
- Les sessions ont des temps d'expiration et nécessitent un maintien en vie
- La réinscription se produit 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
- Les instantanés de configuration sont pris toutes les 1 heure (sauvegardés en tant que fichiers versionnés lorsqu'ils changent)
- 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 effectué chaque heure
- Nettoyage manuel disponible via l'interface Web

Pour des détails de configuration, voir le Guide de configuration d'exécution.

Flux de travail courants

Vérification de santé quotidienne :

1. Ouvrir l'interface Web → Tableau de bord
2. Vérifier l'état des appareils (tous verts ?)
3. Examiner le nombre d'alarmes
4. Enquêter sur les problèmes

Répondre à une alarme critique :

1. Interface Web → Alarmes → Trier par gravité
2. Cliquer sur l'alarme pour des détails
3. Naviguer vers l'appareil
4. Examiner les métriques récentes et les changements de configuration
5. Mettre en œuvre la résolution
6. Vérifier que l'alarme se dissipe

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 le Moniteur RAN
5. Vérifier l'enregistrement (statut 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 détaillée de l'appareil	État de session, problèmes d'enregistrement
Page d'état d'InfluxDB	Vérification de la collecte de données

Étapes de diagnostic rapides

Appareil ne se connectant 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 des erreurs

Pas de métriques dans Grafana :

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

L'interface Web ne se 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 des erreurs de démarrage de l'interface Web

Pour des procédures de dépannage complètes, voir 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)
- Changements de configuration récents
- Version du Moniteur RAN et OS

Contact :

Pour assistance avec le Moniteur RAN :

- Support d'Omnitouch Network Services
- Inclure les informations de diagnostic rassemblées
- Fournir des 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 changements de configuration récents
4. Tester la connectivité et la fonctionnalité de base
5. Consulter les guides de documentation pertinents

Carte de documentation