Guia de Operações do Monitor RAN

Plataforma de Monitoramento e Gerenciamento de Rede de Acesso Rádio (RAN)

por Omnitouch Network Services

Índice

Visão Geral

O Monitor RAN é uma plataforma de gerenciamento e monitoramento para estações base Nokia AirScale em redes 3GPP LTE e 5G. Ele fornece visibilidade em tempo real sobre a saúde, desempenho e configuração do seu equipamento RAN.

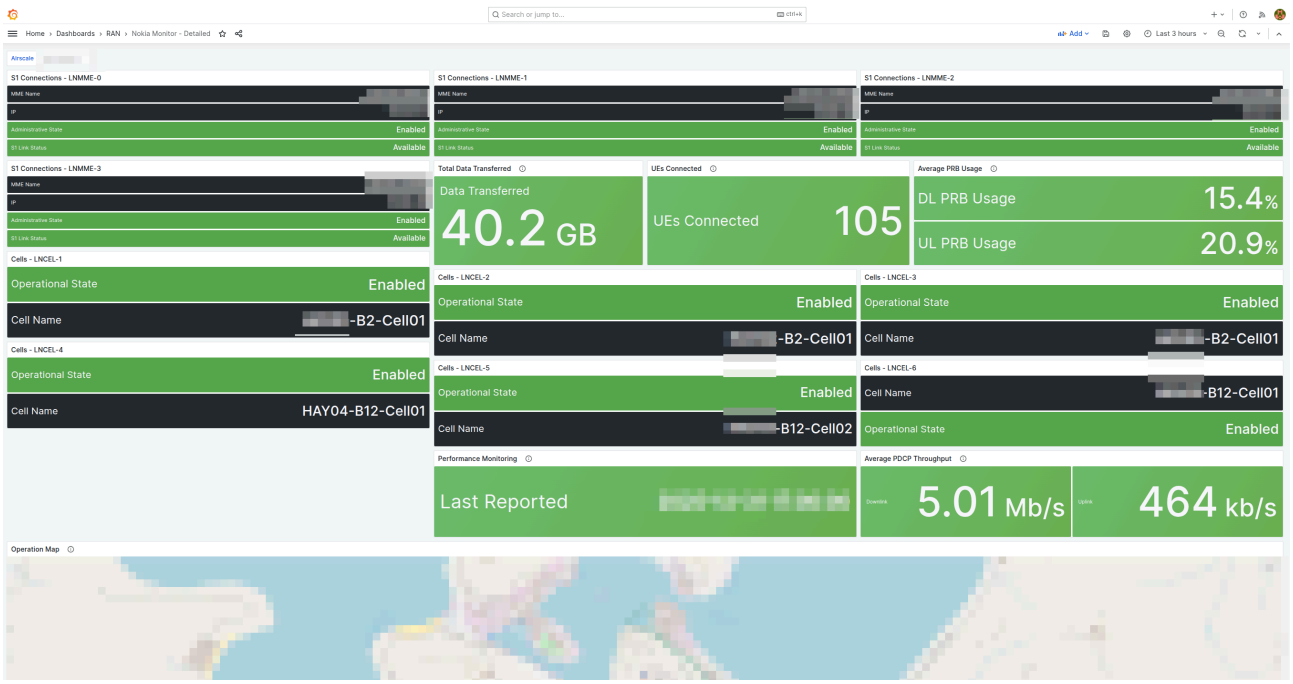
Principais Recursos

- **Monitoramento em Tempo Real** - Coleta contínua de métricas de desempenho e alarmes
- **Gerenciamento Automatizado** - Mantém conexões persistentes com estações base
- **Análise Histórica** - Armazena dados para análise de tendências e planejamento de capacidade
- **Painel Web** - Visibilidade operacional em tempo real através da interface Web integrada
- **Integração com Grafana** - Análises avançadas e painéis personalizados

Componentes do Sistema

Componente	Propósito	Acesso
Gerenciador do Monitor RAN	Aplicativo central que gerencia conexões com estações base	Serviço em segundo plano
Painel de Controle da Interface Web	Painel operacional em tempo real	https://<servidor>:9443
Banco de Dados MySQL	Estado da sessão e configuração do dispositivo	Interno
InfluxDB	Armazenamento de métricas de séries temporais	http://<servidor>:8086
Grafana	Painéis de análise e alertas	http://<servidor>:3000
Servidor TCE NSNTI	Coleta de rastreamento de estações base	Porta TCP 49151
Encaminhador TCE TZSP	Exportação de rastreamento em tempo real para Wireshark	Porta UDP 37008

Exemplo: Painel de Monitoramento Detalhado



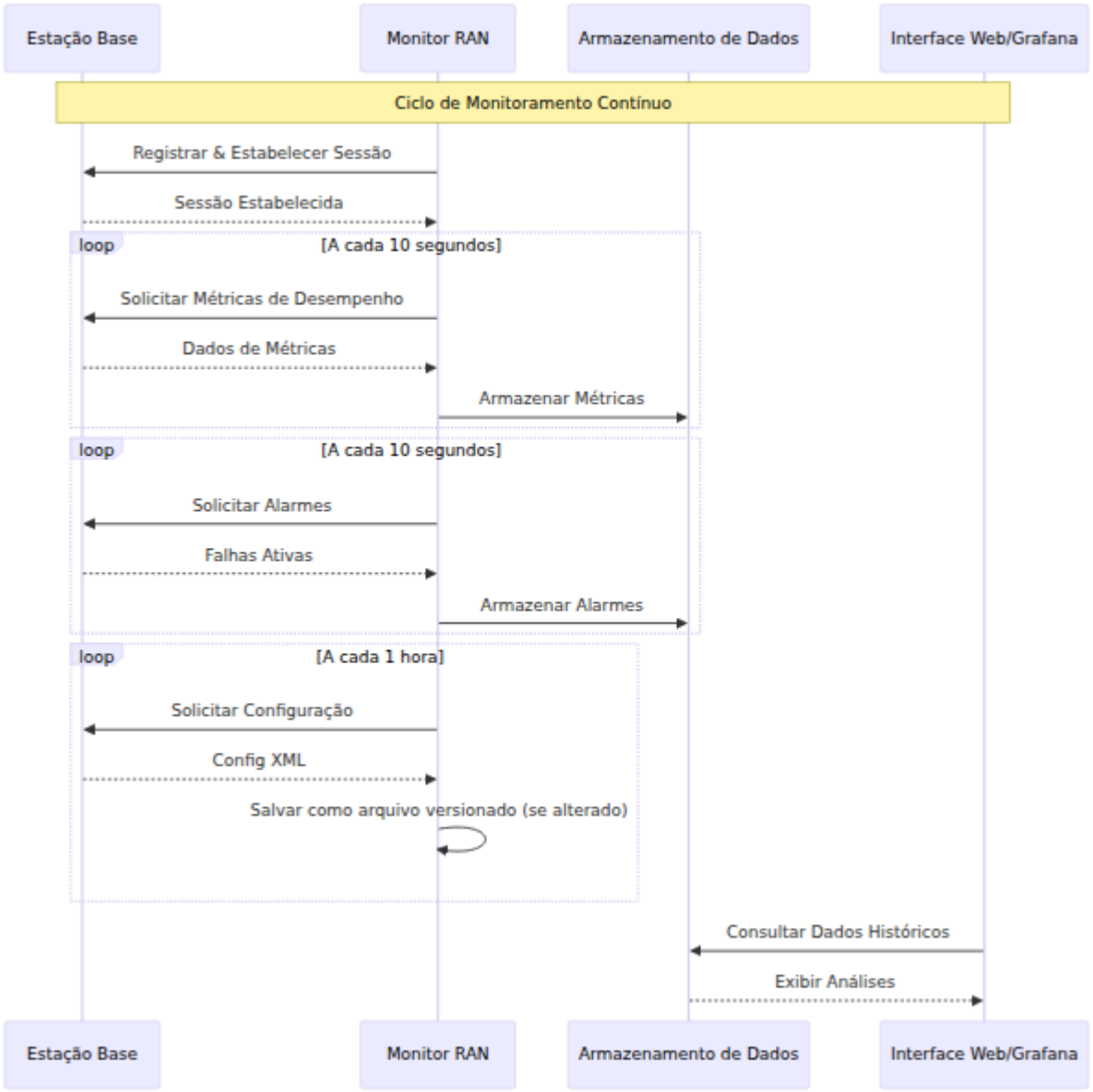
Painel de monitoramento abrangente mostrando o status das conexões S1 por LNMME, estado operacional, dados transferidos, UEs conectados, uso médio de PRB, métricas de monitoramento de desempenho e mapa de cobertura geográfica. Este painel fornece aos operadores de rede visibilidade instantânea sobre a saúde do dispositivo, status de conectividade e indicadores-chave de desempenho.

O que o Monitor RAN Faz

O Monitor RAN opera continuamente em segundo plano para:

1. **Registrar e Conectar** - Estabelece conexões seguras com suas estações base Nokia
2. **Coletar Dados de Desempenho** - Coleta KPIs a cada 10 segundos (configurável)
3. **Monitorar Alarmes** - Acompanha falhas e seus níveis de severidade
4. **Rastrear Configuração** - Registra o estado do sistema e mudanças de parâmetros
5. **Armazenar Dados Históricos** - Preserva métricas em banco de dados de séries temporais
6. **Fornecer Visibilidade** - Exibe status em tempo real através da interface Web e Grafana

Fluxo de Dados



O que é Coletado

Métricas de Desempenho:

- Disponibilidade e tempo de atividade da célula
- Taxa de transferência de tráfego (uplink/downlink)
- Utilização de recursos (uso de PRB)
- Taxas de sucesso na configuração de chamadas
- Desempenho de transferência
- Medições de qualidade de rádio

Alarmes:

- Severidade da falha (Crítica, Maior, Menor, Aviso)
- Sistemas e componentes afetados
- Causa provável e descrições
- Marcas de tempo e durações

Configuração:

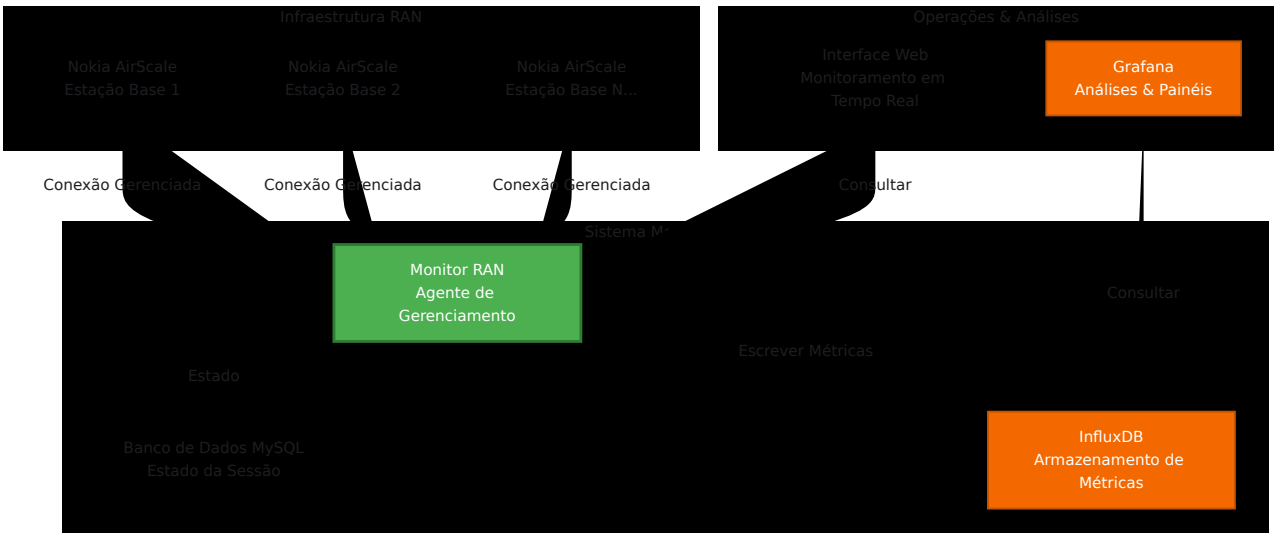
- Capturas completas de configuração XML (armazenadas como arquivos versionados)
- Detecção automática de mudanças e versionamento
- Histórico de configuração e trilha de auditoria
- Últimas 10 versões retidas por dispositivo

Para detalhes sobre gerenciamento de configuração, consulte o Guia de Arquivo de Configuração.

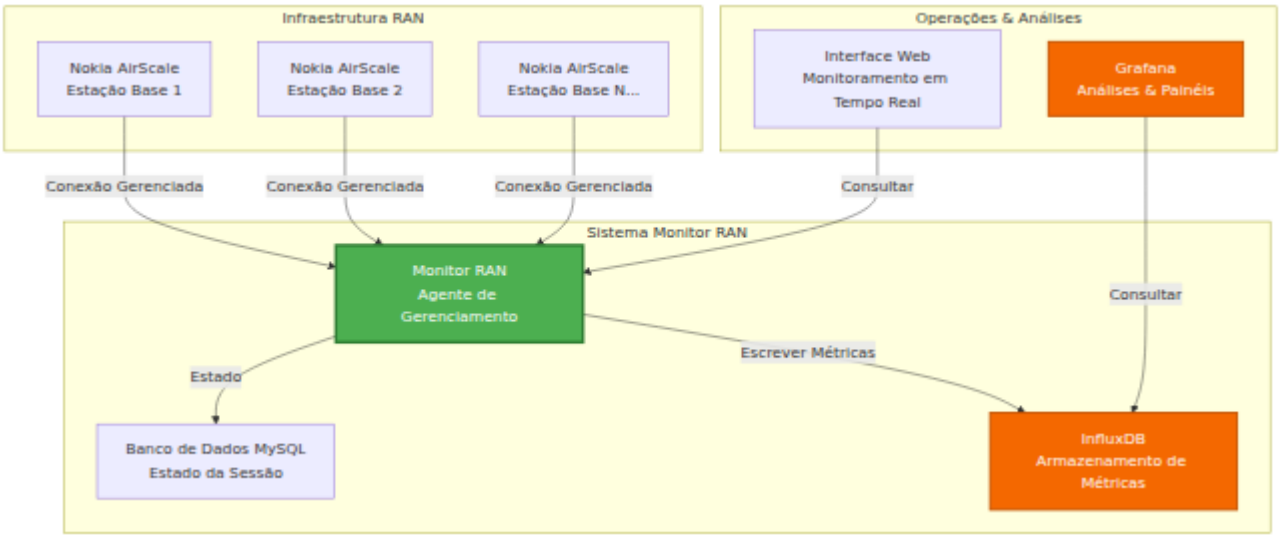
Para definições detalhadas de contadores, consulte a Referência de Contadores Nokia.

Arquitetura do Sistema

Visão Geral da Infraestrutura



Visão Geral da Configuração



Para detalhes completos da configuração, consulte o Guia de Configuração em Tempo de Execução.

Entidade de Coleta de Rastreio (TCE)

O Monitor RAN inclui uma Entidade de Coleta de Rastreio integrada para capturar e analisar mensagens de protocolo LTE/5G. Isso permite uma solução de problemas detalhada, testes de drive e otimização de RF.

O que é TCE?

A Entidade de Coleta de Rastreio recebe dados de rastreio das estações base Nokia AirScale contendo:

- **Mensagens S1-AP** - Sinalização do plano de controle entre eNodeB e EPC
- **Mensagens RRC** - Sinalização de Controle de Recursos de Rádio
- **Mensagens NAS** - Sinalização do Estrato Não Acessível
- **Dados do Plano do Usuário** - Informações de taxa de transferência da camada PDCP

Casos de Uso

Teste de Drive:

- Capturar a experiência de RF do usuário final
- Analisar o desempenho de transferência
- Medir a qualidade do sinal (RSRP, RSRQ, SINR)
- Identificar buracos de cobertura

Solução de Problemas:

- Depurar falhas na configuração de chamadas
- Analisar problemas de transferência
- Investigar chamadas perdidas
- Revisar eventos de mobilidade

Otimização de RF:

- Validação do planejamento de PCI
- Otimização de relações de vizinhança
- Ajuste de parâmetros de transferência
- Análise de cobertura e capacidade

Para procedimentos completos de coleta de rastreio e análise com Wireshark, consulte o **Guia de Coleta de Dados TCE MDT**.

Visão Geral da Interface Web

O Monitor RAN inclui uma interface Web integrada para monitoramento e gerenciamento operacional em tempo real.

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

O painel principal fornece visibilidade instantânea sobre a saúde do sistema, status do dispositivo e alarmes ativos.

Páginas Principais

Painel Principal

Visão geral do sistema em tempo real com:

- Indicadores de saúde do sistema
- Resumo do status do dispositivo (contagens associadas/falhadas)
- Contagens de alarmes ativos por severidade
- Atividade e eventos recentes

Atualiza automaticamente a cada 5 segundos para visibilidade em tempo real.

Página de Estações Base

Visualize todos os dispositivos gerenciados com seu status atual:

- Status da conexão (verde = associado, vermelho = falhado)
- Estado de registro e informações da sessão
- Marca de tempo do último contato
- Capacidades de filtragem, pesquisa e ordenação

Clique em qualquer dispositivo para ver informações detalhadas, incluindo detalhes de registro, ciclo de vida da sessão, métricas recentes e alarmes ativos.

Página de Alarmes

Monitore todas as falhas em sua rede:

- Colorido por severidade (Vermelho = Crítico, Laranja = Maior, Amarelo = Menor, Azul = Aviso, Verde = Resolvido)
- Detalhes do alarme, causa provável, sistema afetado
- Marcas de tempo e rastreamento de duração
- Ordenar por severidade e capacidades de filtragem

Para procedimentos de manuseio de alarmes, consulte o Guia de Gerenciamento de Alarmes.

Gerenciamento de Configuração

Gerencie com segurança as configurações das estações base:

1. **Baixar** a configuração atual (backup)
2. **Enviar** nova configuração → receber ID do Plano
3. **Validar** a configuração usando o ID do Plano
4. **Ativar** a configuração validada
5. **Verificar** se as mudanças surtiram efeito

Sempre valide antes de ativar para evitar interrupções no serviço.

Arquivo de Configuração: Todas as mudanças de configuração são automaticamente rastreadas e versionadas. Visualize as configs históricas, baixe versões anteriores ou compare mudanças através da página de Arquivo de Configuração.

Para procedimentos detalhados, consulte o Guia da Interface Web - Gerenciamento de Configuração e o Guia de Arquivo de Configuração.

- **Guia de Envio de Configuração** - Enviando mudanças de configuração totais ou parciais para estações base (impacto de reinicialização, atualizações parciais, formato SCF)

---

eNodeBs Não Configurados

Descubra estações base tentando se conectar que ainda não estão configuradas:

- ID do Agente (use ao adicionar à configuração)
- Marca de tempo da última visualização
- Número de tentativas de conexão
- Ações: Atualizar, Excluir, Limpar Tudo

Caso de Uso: Quando novas estações base são implantadas, elas aparecem aqui. Copie o ID do Agente e adicione-o ao `config/runtime.exs`.

Logs da Aplicação

Painel de logs em tempo real para solução de problemas:

- Filtrar por nível de log (Emergência a Depuração)
- Pesquisar em todas as mensagens
- Pausar/Retomar transmissão ao vivo
- Alterar dinamicamente o nível de log do sistema
- Colorido por severidade

Para procedimentos de solução de problemas, consulte o Guia de Solução de Problemas.

Política de Retenção de Dados

Gerencie por quanto tempo os dados são armazenados no InfluxDB:

- Visualize a política de retenção global e contagens totais de registros
- Defina períodos de retenção por dispositivo
- Visualize contagens de registros por tipo de medição (Métricas de Desempenho, Configuração, Alarmes)
- Acione manualmente a limpeza ou limpe todos os dados de um dispositivo

Para informações completas sobre retenção de dados, consulte o Guia de Política de Retenção de Dados.

Status do InfluxDB

Monitore a saúde do banco de dados de séries temporais:

- Indicador de status da conexão
- Contagens de medições por tipo
- Informações de armazenamento
- Versão e configuração do banco de dados
- Atualiza automaticamente a cada 5 minutos

Interpretando o Status:

- Conectado + Contagens Crescentes = Operação Normal
- Conectado + Sem Dados = Verifique o registro do dispositivo
- Desconectado = Verifique a conectividade do InfluxDB

Guia Completo da Interface Web

Para documentação abrangente da Interface Web, incluindo todos os recursos, fluxos de trabalho e melhores práticas, consulte:

Guia da Interface Web - Referência completa do painel de controle

---

Monitoramento com Grafana

Enquanto a Interface Web fornece visibilidade em tempo real, o Grafana permite uma análise histórica profunda e painéis personalizados.

Por que Usar o Grafana?

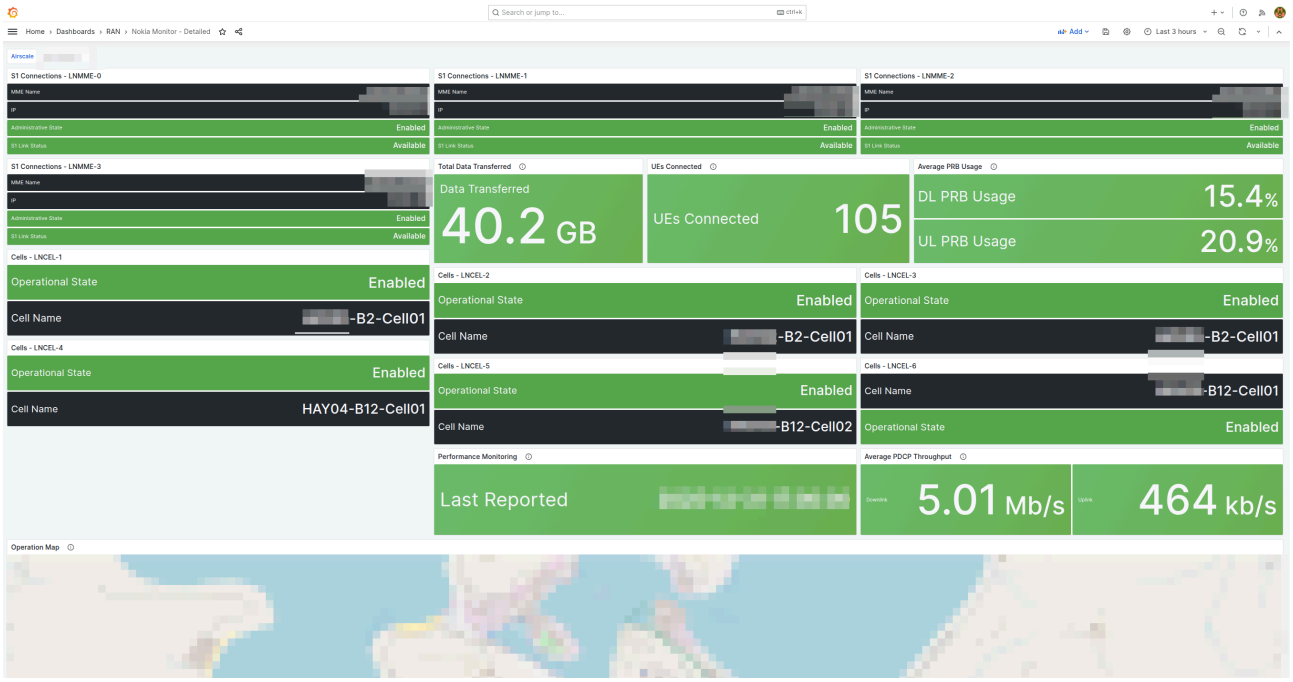
Grafana é Melhor Para:

- Análise de tendências históricas ao longo de dias/semanas/meses
- Painéis KPI personalizados adaptados às suas necessidades

- Planejamento de capacidade a longo prazo
- Identificação de padrões e detecção de anomalias
- Relatórios executivos e rastreamento de SLA
- Alertas avançados com canais de notificação

A Interface Web é Melhor Para:

- Verificações imediatas de status do dispositivo
- Monitoramento de alarmes em tempo real
- Gerenciamento de configuração
- Solução de problemas de sessão
- Tarefas de administração do sistema



Exemplo de painel Grafana mostrando disponibilidade da célula, tendências de taxa de transferência e utilização de recursos

Tipos de Painéis

Painel de Resumo Executivo:

- Visão geral da saúde da rede
- Contagem total de alarmes por severidade
- Disponibilidade média da célula em todos os sites

- Métricas agregadas de taxa de transferência e capacidade
- Grade de status do dispositivo

Painel de Operações NOC:

- Tabela de problemas ativos em tempo real
- Medidores de utilização de recursos
- Visão geral do tráfego (últimas 24 horas)
- Gráficos de tendência de alarmes
- Visão rápida do status do dispositivo

Painel de An��lise Profunda de Engenharia:

- Análise de padrões de tráfego
- Métricas de qualidade da célula (distribuições de SINR, RSRP)
- Desempenho de rádio (retransmissão RLC, sucesso na configuração RRC)
- Trilhas de auditoria de configuração
- Análise de correlação

Painel de Desempenho Nokia AirScale:

- Utilização de PRB (DL/UL)
- Tendências de taxa de transferência (camada PDCP)
- Contagens de UE ativas
- Cálculos de disponibilidade da célula
- Quebras de recursos por célula
- Medições de RSSI
- Sucesso na configuração de conexão RRC
- VSWR por antena
- Consumo de energia

Para exemplos completos de painéis, padrões de consulta e definições de contadores, consulte:

Guia de Integração Grafana - Guia completo de análises e painéis

Referência de Contadores Nokia - Definições de contadores de desempenho

---

Operações Comuns

Operações Diárias

Verificação de Saúde Diária (5-10 minutos):

1. Abra o painel da Interface Web
2. Verifique se todos os dispositivos mostram status verde
3. Verifique a contagem e severidade dos alarmes
4. Revise quaisquer dispositivos falhados
5. Investigue problemas conforme necessário

Para procedimentos detalhados, consulte o Guia da Interface Web - Fluxos de Trabalho.

Investigação de Alarmes:

1. Abra a página de Alarmes, ordene por severidade
2. Clique no alarme para detalhes completos
3. Navegue até o dispositivo afetado
4. Consulte as métricas
5. Determine a ação necessária e resolva

Para procedimentos de manuseio de alarmes, consulte o Guia de Gerenciamento de Alarmes.

Gerenciamento de Dispositivos

Adicionando uma Nova Estação Base:

1. Verifique a conectividade de rede com o dispositivo

2. Verifique a página de eNodeBs Não Configurados para o dispositivo
3. Adicione o dispositivo ao `config/runtime.exs`
4. Reinicie o Monitor RAN
5. Verifique se o registro é bem-sucedido (status verde)
6. Confirme se as métricas estão fluindo para o InfluxDB

Removendo uma Estação Base:

1. Decida se deseja preservar ou excluir dados históricos
2. Comente ou remova o dispositivo de `config/runtime.exs`
3. Opcionalmente, limpe os dados pela página de Retenção de Dados
4. Reinicie o Monitor RAN
5. Atualize os painéis do Grafana

Atualizando Credenciais do Dispositivo:

1. Anote o status atual do dispositivo
2. Atualize as credenciais em `config/runtime.exs`
3. Reinicie o Monitor RAN
4. Verifique se a reconexão é bem-sucedida

Para procedimentos operacionais completos, consulte:

Guia de Operações Comuns - Tarefas diárias de gerenciamento

Gerenciamento de Configuração

Fluxo de Trabalho Seguro para Atualização de Configuração:

1. **Baixar** a configuração atual (backup) - ou recuperar do Arquivo de Configuração
2. **Modificar** a configuração offline
3. **Enviar** para o dispositivo → obter ID do Plano
4. **Validar** usando o ID do Plano → verificar se não há erros
5. **Ativar** se a validação for bem-sucedida
6. **Verificar** se as mudanças surtiram efeito
7. **Monitorar** a estabilidade do dispositivo por 15-30 minutos
8. **Confirmar** que a nova versão aparece no Arquivo de Configuração (dentro de 1 hora)

Importante: Sempre valide antes de ativar. Programe mudanças durante janelas de manutenção sempre que possível.

Rollback de Configuração: Se ocorrerem problemas, baixe uma versão anterior do Arquivo de Configuração e envie-a usando o mesmo fluxo de

trabalho.

Para detalhes sobre configuração de estações base, consulte o Guia de Configuração AirScale.

Para histórico de configuração e versionamento, consulte o Guia de Arquivo de Configuraç��o.

Índice de Documentação

A documentação do Monitor RAN está organizada por público e caso de uso:

Para Equipes de Operações (NOC, Administradores)

Documento	Propósito	Quando Usar
Guia da Interface Web	Referência completa do painel de controle	Operações diárias, monitoramento de dispositivos
Guia de Operações Comuns	Tarefas diárias de gerenciamento	Adicionando dispositivos, gerenciando configs, backups
Guia de Arquivo de Configuração	Versionamento e histórico de configuração	Rastreando mudanças de configuração, rollback, auditoria
Guia de Gerenciamento de Firmware	Repositório de pacotes de software	Enviando firmware, atualizações de software da estação base
Guia de Gerenciamento de Alarmes	Manuseio e escalonamento de alarmes	Investigando falhas, respondendo a alertas
Guia de Solução de Problemas	Procedimentos de resolução de problemas	Quando ocorrem problemas, diagnóstico de erros
Guia de Política de Retenção de Dados	Gerenciamento do ciclo de vida dos dados	Gerenciando armazenamento, definindo períodos de retenção

Para Engenharia e Análise

Documento	Propósito	Quando Usar
Guia de Integração Grafana	Painéis, consultas e alertas	Construindo painéis, configurando alertas
Referência de Contadores Nokia	Definições de contadores de desempenho	Entendendo métricas, criando consultas
Guia de Configuração AirScale	Configuração e configuração da estação base	Configurando dispositivos, entendendo parâmetros
Guia de Comissionamento DHCP	Onboarding de estações base baseadas em DHCP	Comissionando novas estações base via DHCP Option 43
Guia de Coleta de Dados TCE MDT	Coleta de rastreio MDT e análise com Wireshark	Coletando dados de teste de drive, otimização de cobertura
Referência de Endpoints da API	Documentação da API REST	Integrações, automação, scripting

Para Configuração e Implantação

Documento	Propósito	Quando Usar
Guia de Configuração em Tempo de Execução	Referência completa de configuração	Configuração inicial, modificação de configurações

Início Rápido

Novo no Monitor RAN?

1. Comece com o Guia da Interface Web para aprender a interface
2. Revise o Guia de Operações Comuns para tarefas rotineiras
3. Estude o Guia de Gerenciamento de Alarmes para manuseio de alarmes
4. Mantenha o Guia de Solução de Problemas marcado para problemas

Configurando Monitoramento?

1. Consulte o Guia de Integração Grafana para painéis
2. Referencie a Referência de Contadores Nokia para métricas
3. Revise o Guia de Política de Retenção de Dados para gerenciamento de armazenamento

---

Referência Rápida

Pontos de Acesso

Serviço	URL	Propósito
Painel da Interface Web	`https://<servidor>:9443`	Monitoramento e gerenciamento em tempo real
Grafana	`http://<servidor>:3000`	Painéis de análise e alertas
InfluxDB	`http://<servidor>:8086`	Banco de dados de métricas (geralmente acesso interno apenas)

Caminhos Importantes

Caminho	Propósito
`config/runtime.exs`	Arquivo de configuração principal (dispositivos, bancos de dados, configurações)
`priv/cert/`	Certificados SSL para a Interface Web HTTPS
`priv/external/nokia/`	Chaves de autenticação do gerenciador
`priv/airscale_configs/`	Arquivo de configuração (arquivos XML versionados)

Conceitos Chave

Gerenciamento de Sessão:

- O Monitor RAN estabelece sessões com estações base
- As sessões têm tempos de expiração e requerem keep-alive
- A re-registro acontece automaticamente (padrão: a cada 30 segundos)
- O estado da sessão é armazenado no banco de dados MySQL

Fluxo de Dados:

- Métricas coletadas a cada 10 segundos (configurável)
- Alarmes coletados a cada 10 segundos via polling + webhooks em tempo real
- Capturas de configuração a cada 1 hora (salvas como arquivos versionados quando alteradas)
- Métricas de desempenho e alarmes escritos no InfluxDB para armazenamento histórico

Retenção de Dados:

- Padrão global: 720 horas (30 dias)
- Sobrescritas por dispositivo disponíveis

- Limpeza automática ocorre a cada hora
- Limpeza manual disponível via Interface Web

Para detalhes de configuração, consulte o Guia de Configuração em Tempo de Execução.

Fluxos de Trabalho Comuns

Verificação de Saúde Diária:

1. Abra a Interface Web → Painel
2. Verifique o status do dispositivo (todos verdes?)
3. Revise a contagem de alarmes
4. Investigue quaisquer problemas

Responder a Alarme Crítico:

1. Interface Web → Alarmes → Ordenar por severidade
2. Clique no alarme para detalhes
3. Navegue até o dispositivo
4. Revise métricas recentes e mudanças de configuração
5. Implemente a resolução
6. Verifique se o alarme é limpo

Adicionar Novo Dispositivo:

1. Verifique a conectividade de rede
2. Edite `config/runtime.exs`
3. Adicione o dispositivo à lista de airscales
4. Reinicie o Monitor RAN
5. Verifique o registro (status verde)

Suporte

Recursos de Solução de Problemas

Recurso	Usar Para
Guia de Solução de Problemas	Problemas comuns e soluções
Página de Logs da Aplicação	Logs e erros do sistema em tempo real
Visualização de Detalhes do Dispositivo	Status da sessão, problemas de registro
Página de Status do InfluxDB	Verificação de coleta de dados

Passos Rápidos de Diagnóstico

Dispositivo Não Conectando:

1. Verifique a página de Estações Base → status do dispositivo
2. Verifique a conectividade de rede: `ping <device-ip>`
3. Verifique as credenciais em `config/runtime.exs`
4. Revise os Logs da Aplicação para erros

Sem Métricas no Grafana:

1. Verifique se o dispositivo está associado (status verde)
2. Verifique se a página de Status do InfluxDB mostra contagens crescentes
3. Teste a conectividade do InfluxDB
4. Verifique a configuração da fonte de dados do Grafana

Interface Web Não Carregando:

1. Verifique se a porta 9443 é acessível
2. Verifique se o firewall permite tráfego HTTPS

3. Verifique se os certificados SSL existem
4. Revise os logs da aplicação para erros de inicialização da Interface Web

Para procedimentos completos de solução de problemas, consulte o Guia de Solução de Problemas.

Obtendo Ajuda

Antes de Contatar o Suporte:

Reúna estas informações:

- Descrição do problema e quando começou
- Mensagens de erro dos Logs da Aplicação
- Dispositivos afetados (nomes/IPs)
- Mudanças de configuração recentes
- Versão do Monitor RAN e OS

Contato:

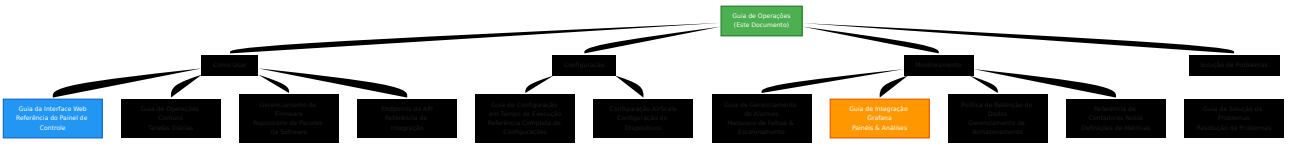
Para assistência com o Monitor RAN:

- Suporte da Omnitouch Network Services
- Inclua informações diagnósticas coletadas
- Forneça arquivos de configuração (sanitize senhas)
- Inclua trechos relevantes dos logs

Autoatendimento:

1. Pesquise no Guia de Solução de Problemas
2. Verifique os Logs da Aplicação para erros específicos
3. Revise mudanças de configuração recentes
4. Teste conectividade e funcionalidade básica
5. Consulte guias de documentação relevantes

Mapa da Documentação



Guia de Configuração do Nokia AirScale

Configurando Estações Base para Integração com o RAN Monitor

Índice

Visão Geral

Para permitir que o RAN Monitor colete métricas de desempenho, alarmes e dados de configuração das estações base Nokia AirScale, você deve configurar a estação base para relatar dados ao sistema RAN Monitor. Isso é realizado através da interface Nokia Web Element Manager (WebLM).

Este guia orienta o processo de configuração do objeto gerenciado Performance Measurement Common Administration (PMCADM), que controla como a estação base envia dados de desempenho para sistemas externos.

Quem Deve Usar Este Guia

Importante: Toda a configuração da estação base Nokia AirScale é **realizada pela Omnitouch** como parte da implantação inicial e suporte contínuo. Este

guia é fornecido para:

- **Usuários avançados** que desejam entender a configuração da estação base
- **Implantações autogeridas** onde os clientes configuram suas próprias estações base
- **Solução de problemas** e compreensão da configuração atual
- **Integração adicional de estações base** em ambientes autogeridos

Se você é um cliente gerenciado pela Omnitouch, entre em contato com o suporte da Omnitouch para configuração e integração da estação base.

Para entender as métricas que estão sendo coletadas, consulte Referência de Contadores Nokia. Para configuração do sistema, consulte Guia de Configuração em Tempo de Execução.

Pré-requisitos

Antes de configurar a estação base, certifique-se de que você possui:

- **Acesso à Rede** - Conectividade com a interface de gerenciamento da estação base
- **Credenciais de Administrador** - Nome de usuário e senha com privilégios de configuração
- **Detalhes do RAN Monitor** - Endereço IP e porta onde o RAN Monitor está ouvindo
- **Software Suportado** - Versão de software da estação base Nokia AirScale compatível

Informações Necessárias:

Parâmetro	Valor	Exemplo
Endereço IP do RAN Monitor	IP onde o RAN Monitor está em execução	10.179.2.139
Porta do RAN Monitor	Porta de coleta (padrão: 9076)	9076
Intervalo de Coleta	Com que frequência enviar métricas	60 segundos

---

Acessando a Interface WebLM

Passo 1: Abra o Gerenciador de Elementos Web

1. Abra um navegador da web
2. Navegue até a interface de gerenciamento da estação base:

   ```
   http://<endereço-ip-da-estação-base>/
   ```

   ou

   ```
   https://<endereço-ip-da-estação-base>/
   ```

3. Faça login com suas credenciais de administrador

Passo 2: Navegue até o Gerenciamento de Configuração

Uma vez logado:

1. Clique em **Configuração** na barra de menu superior
2. Selecione **Gerenciamento de Configuração** no menu suspenso

3. Clique na guia **Editor de Parâmetros**

Agora você deve ver a árvore de configuração no painel esquerdo e o editor de parâmetros na janela principal.

Configurando Monitoramento de Desempenho

Passo 1: Desabilitar OAM TLS

Importante: Antes de configurar o monitoramento de desempenho, você deve desabilitar a aplicação do OAM TLS na estação base. Por padrão, o objeto gerenciado `oamTls` está definido como `forced`, o que impede a comunicação não criptografada com sistemas de gerenciamento externos.

No painel de navegação à esquerda (árvore de Objetos):

1. Expanda **Configuração Atual da BTS**
2. Expanda **CURRENT_BTS_CONF-1**
3. Expanda **MRBTS-X** (onde X é o ID da sua estação base)
4. Localize o objeto gerenciado **oamTls**
5. Altere o valor de `forced` para `off`

Parâmetro	Valor Padrão	Valor Necessário
oamTls	forced	off

Nota: Esta configuração deve ser alterada antes que o RAN Monitor possa estabelecer comunicação com a estação base. Se permanecer na configuração padrão `forced`, a estação base rejeitará conexões não TLS.

Passo 2: Localizar o Objeto Gerenciado PMCADM

No painel de navegação à esquerda (árvore de Objetos):

1. Expanda **Configuração Atual da BTS**
2. Expanda **CURRENT_BTS_CONF-1**
3. Expanda **MRBTS-X** (onde X é o ID da sua estação base)
4. Expanda **MNL-1** (Link de Gerenciamento)
5. Expanda **MNLENT-1** (Entidade de Link de Gerenciamento)
6. Clique em **PMCADM-1** (Administração Comum de Medição de Desempenho)

O editor de parâmetros exibirá os parâmetros de configuração do PMCADM-1.

Passo 3: Configurar Monitoramento de Desempenho em Tempo Real

Role para baixo até a seção **Estrutura 1**, que contém as configurações da Entidade de Coleta de Monitoramento de Desempenho em Tempo Real. Configure os seguintes parâmetros:

Parâmetros Necessários:

Parâmetro	Descrição	Valor Recomendado
Tipo de certificado para autenticação TLS	Tipo de certificado de segurança	RSA (se TLS habilitado)
Host da entidade de coleta de monitoramento de desempenho em tempo real	Endereço IP do RAN Monitor	Seu IP do RAN Monitor (ex: 10.179.2.139)
Número da Porta da Entidade de Coleta de Monitoramento de Desempenho em Tempo Real	Porta onde o RAN Monitor escuta	9076 (padrão)
Intervalo de Coleta de Monitoramento de Desempenho em Tempo Real	Com que frequência enviar métricas	60s (ajustar conforme requisitos)
Habilitar TLS	Usar conexão criptografada	false (para configuração inicial)

Parâmetros Opcionais:

Parâmetro	Descrição	Valor Padrão
Número máximo de arquivos de upload SDL	Máximo de uploads simultâneos	1
Nonce SDL	Identificador único para segurança	12345678
Habilitar supressão de contadores com valor zero	Suprimir contadores com valor 0	false (recomendado manter todos os dados)

Passo 4: Salvar e Ativar a Configuração

Após configurar todos os parâmetros:

1. **Revise suas alterações** - Verifique se todos os endereços IP e portas estão corretos

2. **Crie um plano de configuração:**

    - Clique no botão **Criar Plano** na parte superior
    - O sistema validará suas alterações
    - Anote o ID do Plano fornecido

3. **Valide o plano:**

    - Clique no botão **Validar Plano**
    - Insira o ID do Plano
    - Aguarde a validação ser concluída
    - Resolva quaisquer erros de validação

4. **Ative a configuração:**

    - Clique no botão **Ativar Plano**
    - Insira o ID do Plano
    - Confirme a ativação
    - A estação base aplicará a nova configuração

Alternativa: Configuração XML

Para usuários avançados ou implantações automatizadas, a configuração do PMCADM pode ser aplicada usando XML. Este é o trecho de configuração que corresponde à configuração manual acima:

```
<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>
```

Parâmetros Chave em XML:

- `rTPmCollEntityHost` - Defina para o seu endereço IP do RAN Monitor
- `rTPmCollEntityPortNum` - Defina para 9076 (porta padrão do webhook)
- `rTPmCollInterval` - Intervalo de coleta (60s recomendado)
- `tlsEnabled` - Defina como false para configuração inicial
- `sdlPrimaryDestIp` - Defina para o seu endereço IP do RAN Monitor

Nota: Substitua `10.179.2.139` pelo seu endereço IP real do RAN Monitor e ajuste `MRBTS-132` para corresponder ao seu ID da estação base.

Referência de Parâmetros de Configuração

Parâmetros de Medição de Desempenho LNBTS

O objeto gerenciado LNBTS (LTE NodeB) contém parâmetros que controlam quais grupos de medição de desempenho são coletados. Esses parâmetros

devem ser habilitados para coletar certas categorias de contadores de PM.

actL1PM - Ativar Medições de Desempenho da Camada 1

Configuração	Valor
Parâmetro	actL1PM
Localização	Objeto gerenciado NOKLTE:LNBTS
Tipo	Booleano (true/false)
Padrão	false
Necessário para	Contadores RTWP (M8005C306-339)

Descrição: Habilita medições de desempenho da Camada 1 (camada física), incluindo RTWP (Received Total Wideband Power) por antena. Quando desabilitado, a estação base não relatará RTWP, interferência e outras medições de rádio de baixo nível.

Contadores Afetados:

- M8005C306-309: AVG_RTWP_RX_ANT_1 até AVG_RTWP_RX_ANT_4
- M8005C310-313: AVG_RTWP_RX_ANT_5 até AVG_RTWP_RX_ANT_8
- M8005C314: MAX_RTWP
- M8005C317-325: UL_IOT_PUSCH bins de distribuição
- M8005C326-335: AVG_SIR bins de distribuição

Configuração via XML:

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

Configuração via WebLM:

1. Navegue até Configuração > Gerenciamento de Configuração > Editor de Parâmetros
2. Expanda MRBTS-X > LNBTS-X
3. Localize o parâmetro `actL1PM`
4. Defina o valor como `true`
5. Crie, valide e ative o plano de configuração

actPCMDReport - Ativar Relatório de Dados de Medição por Chamada

Configuração	Valor
Parâmetro	actPCMDReport
Localização	Objeto gerenciado NOKLTE:LNBTS
Tipo	Booleano (true/false)
Padrão	false
Necessário para	Dados de medição por chamada

Descrição: Habilita o relatório de Dados de Medição por Chamada (PCMD), que fornece medições detalhadas para sessões de chamadas individuais.

Configuração via XML:

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

Visão Geral do Objeto PMCADM-1

O objeto gerenciado PMCADM (Administração Comum de Medição de Desempenho) controla como os dados de desempenho são coletados e

relatados a partir da estação base.

Principais Responsabilidades:

- Configurar destinos de monitoramento de desempenho em tempo real
- Definir intervalos de coleta para relatórios de métricas
- Controlar formato de dados e parâmetros de transmissão
- Gerenciar configurações de segurança para transmissão de dados

Parâmetros Chave do PMCADM

reportingIntervalPm - Intervalo de Relatório de PM

Configuração	Valor
Parâmetro	reportingIntervalPm
Localização	objeto gerenciado com.nokia.srbts.mnl:PMCADM
Tipo	Enumeração
Opções	5min, 15min, 30min, 60min
Recomendado	5min ou 15min para monitoramento em tempo real

Descrição: Controla com que frequência a estação base envia dados de medição de desempenho. Valores mais baixos fornecem dados mais granulares, mas aumentam o tráfego de rede e os requisitos de armazenamento.

Impacto na Coleta de Dados:

- **5min** - Melhor para monitoramento em tempo real e solução de problemas
- **15min** - Bom equilíbrio entre granularidade e uso de recursos
- **60min** - Adequado apenas para tendências de longo prazo

Configuração via XML:

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

Configuração via WebLM:

1. Navegue até Configuração > Gerenciamento de Configuração > Editor de Parâmetros
2. Expanda MRBTS-X > MNL-1 > MNLENT-1 > PMCADM-1
3. Localize o parâmetro `reportingIntervalPm`
4. Defina o valor para o intervalo desejado (ex: `5min`)
5. Crie, valide e ative o plano de configuração

Entidade de Coleta de Monitoramento de Desempenho em Tempo Real

Esta subestrutura define onde e como a estação base envia métricas de desempenho em tempo real.

certTypeForTlsAuth - Tipo de Certificado para Autenticação TLS

- **Tipo:** Enumeração (RSA, DSA, ECDSA)
- **Objetivo:** Especifica o tipo de certificado quando TLS está habilitado
- **Padrão:** RSA
- **Uso:** Somente relevante quando tlsEnabled = true

rTpmCollEntityHost - Host da Entidade de Coleta

- **Tipo:** Endereço IP (IPv4 ou IPv6)
- **Objetivo:** Endereço IP de destino para métricas de desempenho
- **Necessário:** Sim
- **Exemplo:** 10.179.2.139
- **Notas:** Deve ser acessível a partir da rede de gerenciamento da estação base

rTpmCollEntityPortNum - Número da Porta da Entidade de Coleta

- **Tipo:** Inteiro (1-65535)
- **Objetivo:** Porta TCP onde o sistema de coleta escuta
- **Padrão:** 9076
- **Notas:** Deve corresponder à configuração do RAN Monitor

rTpmCollInterval - Intervalo de Coleta

- **Tipo:** Tempo (segundos)
- **Objetivo:** Frequência de transmissão de dados de desempenho
- **Opções:** 15s, 30s, 60s, 300s, 900s, 1800s
- **Padrão:** 60s
- **Recomendação:** 60s para monitoramento padrão, 15s para solução de problemas detalhada

tlsEnabled - Habilitar TLS

- **Tipo:** Booleano (true/false)
- **Objetivo:** Criptografar dados de desempenho em trânsito
- **Padrão:** false
- **Notas:** Requer certificados válidos em ambos os lados se habilitado

sdlMaxUploadFileNumber - Número Máximo de Arquivos de Upload SDL

- **Tipo:** Inteiro
- **Objetivo:** Número máximo de uploads de arquivos simultâneos
- **Padrão:** 1
- **Notas:** Aumentar para ambientes de alto volume

sdlNonce - SDL Nonce

- **Tipo:** String (8 dígitos)
- **Objetivo:** Identificador único para segurança do protocolo SDL
- **Padrão:** 12345678
- **Notas:** Pode ser alterado por motivos de segurança

suppressZeroValueCount - Suprimir Contadores de Valor Zero

- **Tipo:** Booleano (true/false)
- **Objetivo:** Omitir contadores com valores zero dos relatórios
- **Padrão:** false
- **Recomendação:** Manter false para manter dados completos para tendências

---

Verificação

Após ativar a configuração, verifique se a estação base está enviando dados com sucesso para o RAN Monitor.

Verificar Interface Web do RAN Monitor

1. Abra a interface Web do RAN Monitor: `http://<endereço-ip-do-ran-monitor>:4000/`
2. Navegue até a página **Status da BTS**
3. Localize sua estação base na lista de dispositivos
4. Verifique se o status mostra **Conectado** (indicador verde) — isso significa que o site tem uma sessão ativa E enviou tanto a configuração quanto os dados de PM
5. Se o status mostrar **Aguardando Dados de PM**, a sessão está ativa, mas o site ainda não enviou métricas de desempenho (aguarde o próximo ciclo de PM de 15 minutos)

Status Esperado:

- **Status:** Conectado (verde)
- **Sessão:** Ativa
- **Endereço:** Corresponde ao IP da estação base
- **Ações:** Todos os botões habilitados

Se o Status Mostrar Pendente:

O dispositivo está tentando se registrar, mas não completou a autenticação.

Causas possíveis:

- Mismatch do ID do gerente e chave de registro
- RAN Monitor não configurado para aceitar este dispositivo
- Problemas de conectividade de rede

Se o Status Mostrar Erro de Conexão:

O dispositivo não consegue alcançar o RAN Monitor.

Causas possíveis:

- Endereço IP incorreto na configuração do PMCADM
- Problemas de roteamento de rede
- Firewall bloqueando a porta 8080
- Serviço do RAN Monitor não está em execução

Verificar Coleta de Dados

Verificar Status do InfluxDB:

1. Na interface Web do RAN Monitor, navegue até **Status do InfluxDB**
2. Verifique se os pontos de dados estão aumentando
3. Confira se a contagem de **Métricas de Desempenho** está crescendo
4. Confirme se o timestamp de **Última Atualização** é recente

Métricas Esperadas:

- **Métricas de Desempenho:** Contagem aumentando regularmente
- **Configuração:** Pontos de dados presentes
- **Alarmes:** Podem ser 0 se não houver falhas ativas

Verificar Retenção de Dados:

1. Navegue até a página **Política de Retenção de Dados**
2. Localize sua estação base
3. Verifique as contagens de **Métricas de Desempenho**, **Configuração** e **Alarmes**

Solução de Problemas

Estação Base Não Aparecendo no RAN Monitor

Sintoma: O dispositivo não aparece na página de Status da BTS

Soluções:

1. **Verifique a conectividade da rede:**

```
ping <endereço-ip-da-estação-base>
```

2. **Verifique a configuração do RAN Monitor:**
   - Certifique-se de que o dispositivo está adicionado ao `config/runtime.exs`
   - Verifique se o endereço IP corresponde à estação base
   - Confirme se as credenciais estão corretas
3. **Revise os logs do RAN Monitor:**
   - Navegue até a página **Logs Ao Vivo**
   - Filtre por mensagens de erro
   - Procure tentativas de conexão da estação base
4. **Verifique a configuração da estação base:**
   - Revise as configurações do PMCADM-1 no WebLM
   - Confirme se o endereço IP do RAN Monitor está correto
   - Assegure-se de que a porta 9076 está especificada

Dispositivo Mostra Status "Pendente"

Sintoma: O dispositivo aparece, mas o status é amarelo "Pendente"

Soluções:

1. **Verifique o registro do gerente:**
   - Verifique se o ID do gerente no RAN Monitor corresponde à expectativa da estação base
   - Confirme se as chaves de registro estão configuradas corretamente
2. **Revise a autenticação:**
   - Verifique as credenciais em runtime.exs
   - Assegure-se de que o nome de usuário/senha correspondem às configurações da estação base

3. **Aguarde o ciclo de registro:**
    - O registro pode levar de 30 a 60 segundos
    - Atualize a página após aguardar

Erros de Conexão

Sintoma: "Erro de rede: enetunreach" ou similar

Soluções:

1. **Verifique o caminho da rede:**
    - Teste a conectividade da estação base ao RAN Monitor
    - Verifique tabelas de roteamento
    - Confirme se VLANs/sub-redes estão configuradas corretamente
2. **Verifique as regras do firewall:**
    - Assegure-se de que a porta 9076 está aberta (para dados de desempenho em tempo real)
    - Assegure-se de que a porta 8080 está aberta (para comunicação da API SOAP)
    - Verifique se não há ACLs bloqueando o tráfego
    - Verifique as regras do iptables no servidor do RAN Monitor
3. **Verifique se o RAN Monitor está ouvindo:**

```
# Verifique os endpoints da API SOAP e do webhook
netstat -tlnp | grep -E '8080|9076'
```

Contadores RTWP ou da Camada 1 Ausentes

Sintoma: A estação base está relatando dados, mas os contadores RTWP (M8005C306-339) estão ausentes do InfluxDB

Causa: O parâmetro `actL1PM` está definido como `false` na configuração do LNBTS, o que desabilita as medições de desempenho da Camada 1.

Solução:

1. **Verifique a configuração atual:**
    - Exporte a configuração da estação base
    - Pesquise por `actL1PM` na seção LNBTS
    - Se o valor for `false`, esta é a causa
2. **Habilite PM da Camada 1:**
    - Acesse o WebLM na estação base
    - Navegue até MRBTS-X > LNBTS-X
    - Defina `actL1PM` como `true`
    - Crie, valide e ative o plano de configuração
3. **Verifique após a ativação:**
    - Aguarde o próximo intervalo de coleta (tipicamente 60 segundos)
    - Verifique o InfluxDB para os contadores M8005C306-309
    - Os dados RTWP devem agora aparecer

Parâmetros Relacionados:

- `actPCMDReport` - Dados de Medição por Chamada (também pode precisar ser habilitado)

Sem Métricas no InfluxDB

Sintoma: O dispositivo está conectado, mas não há dados no banco de dados

Soluções:

1. **Verifique o intervalo de coleta:**
    - Verifique a configuração do PMCADM-1 rTpmCollInterval
    - Aguarde pelo menos um período completo do intervalo
    - Atualize a página de Status do InfluxDB

2. **Verifique a conexão com o InfluxDB:**
    - Navegue até a página de Status do InfluxDB
    - Verifique se o indicador "Conectado" está verde
    - Confirme se o nome do bucket está correto
3. **Revise os logs do RAN Monitor:**
    - Procure por erros de gravação no InfluxDB
    - Verifique se há problemas de análise de dados
    - Confirme se o token da API tem permissões de gravação

Problemas de TLS/Certificado

Sintoma: A conexão falha quando o TLS está habilitado

Soluções:

1. **Verifique se os certificados estão instalados:**
    - Verifique se a estação base possui um certificado válido
    - Assegure-se de que o RAN Monitor possui o certificado CA correspondente
2. **Tente sem TLS primeiro:**
    - Defina tlsEnabled = false
    - Verifique se a conectividade básica funciona
    - Rehabilite o TLS após confirmar a funcionalidade
3. **Verifique a validade do certificado:**
    - Verifique se os certificados não estão expirados
    - Confirme se os nomes dos sujeitos do certificado correspondem
    - Verifique se a cadeia de certificados está completa

Recursos Adicionais

Documentação Relacionada

- Guia de Operações - Documentação completa de operações do RAN Monitor
- Guia de Configuração em Tempo de Execução - Referência de configuração do RAN Monitor
- Referência de Contadores Nokia - Definições de contadores de desempenho
- Integração com Grafana - Construindo painéis com métricas coletadas
- Endpoints da API - Referência da API REST para gerenciamento de dispositivos
- Política de Retenção de Dados - Gerenciamento de dados de desempenho armazenados

Arquivos de Configuração

- **config/runtime.exs** - Configuração do dispositivo do RAN Monitor

Suporte

Para problemas não cobertos neste guia:

1. Revise os logs da aplicação do RAN Monitor
2. Verifique a documentação da estação base Nokia para sua versão de software
3. Confirme a configuração da infraestrutura de rede
4. Consulte a equipe de operações de rede

Gerenciamento de Alarmes & Escalonamento

Tratamento de Falhas, Níveis de Severidade e Resposta Operacional

Guia para gerenciar alarmes, investigar falhas e escalar problemas

---

Índice

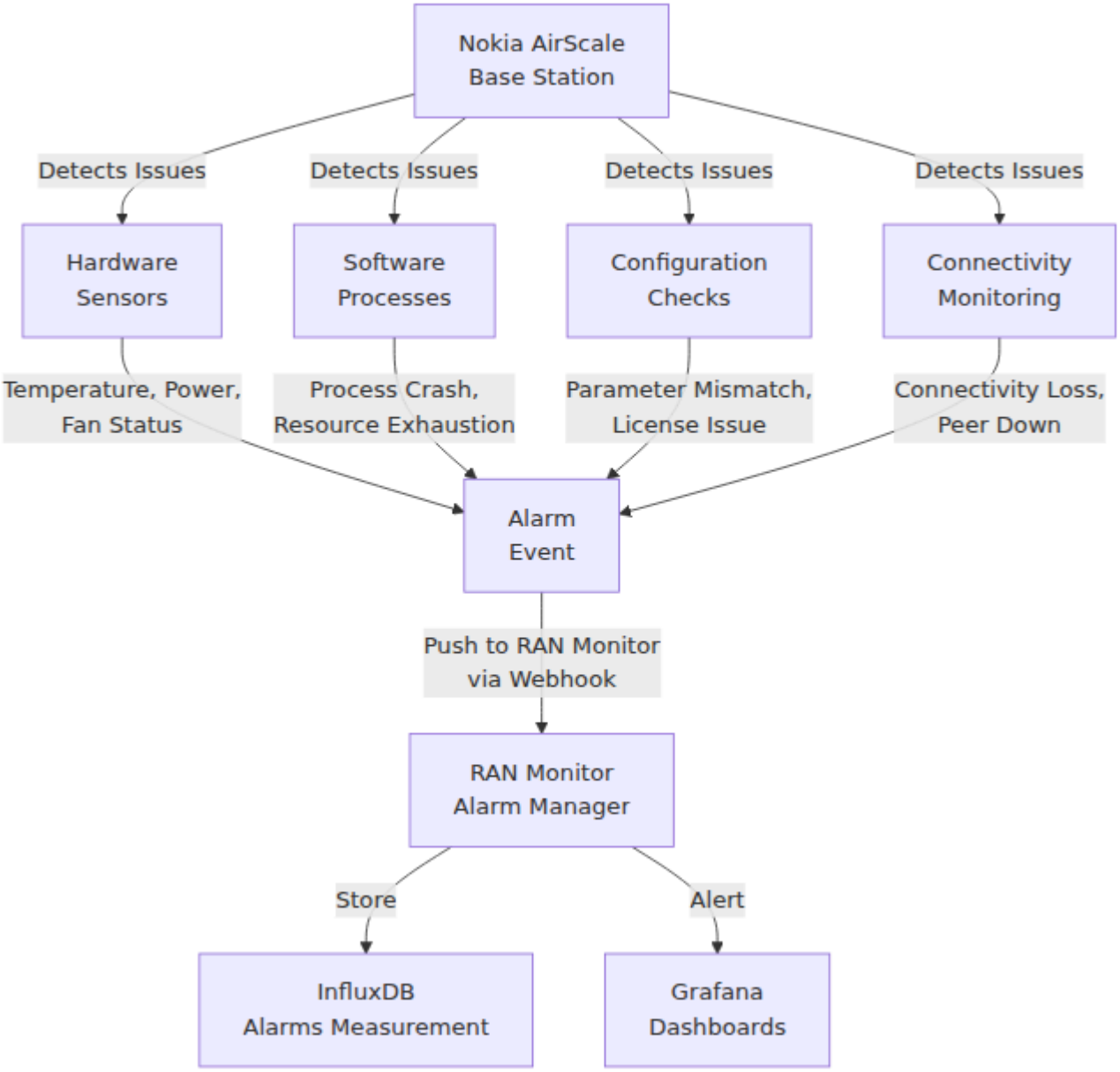
Visão Geral

Alarmes (também chamados de "falhas") representam problemas ou anomalias detectadas nas estações base Nokia AirScale. O RAN Monitor monitora continuamente alarmes ativos e rastreia seu ciclo de vida desde a geração até a resolução.

Exemplo de Painel de Alarmes:

Exemplo mostrando o Status 4G com uma tabela de visão geral de alarmes exibindo o status do alarme (ativo/limpo), níveis de severidade (crítico/aviso), timestamps e descrições de alarmes para falhas de interface óptica.

Fontes de Alarmes



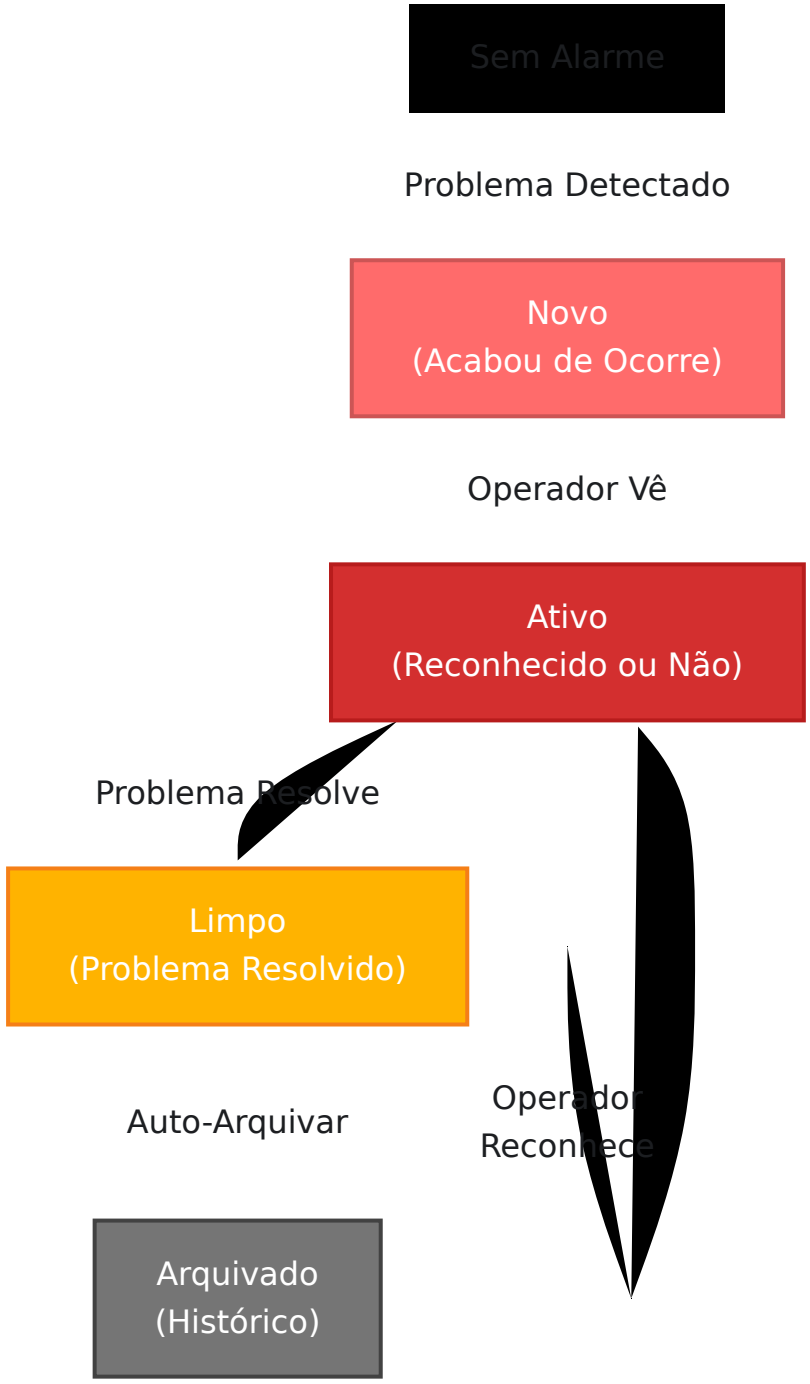
Principais Atributos do Alarme

Todo alarme contém:

Atributo	Exemplo	Propósito
ID do Alarme	a1b2c3d4-e5f6-...	Identificador único
Severidade	Crítico, Maior, Menor	Nível de prioridade
Causa Provável	"Célula Indisponível"	Categoria da causa raiz
Problema Específico	"Conexão S1 Perdida"	Problema detalhado
Sistema Afetado	/BSC-1/BTS-23/Célula-A	O que está impactado (DN)
Hora do Evento	2025-12-10 14:23:45	Quando foi detectado
Status	Ativo / Limpo	Estado atual

Ciclo de Vida do Alarme

Transições de Estado



Exemplo de Linha do Tempo do Alarme

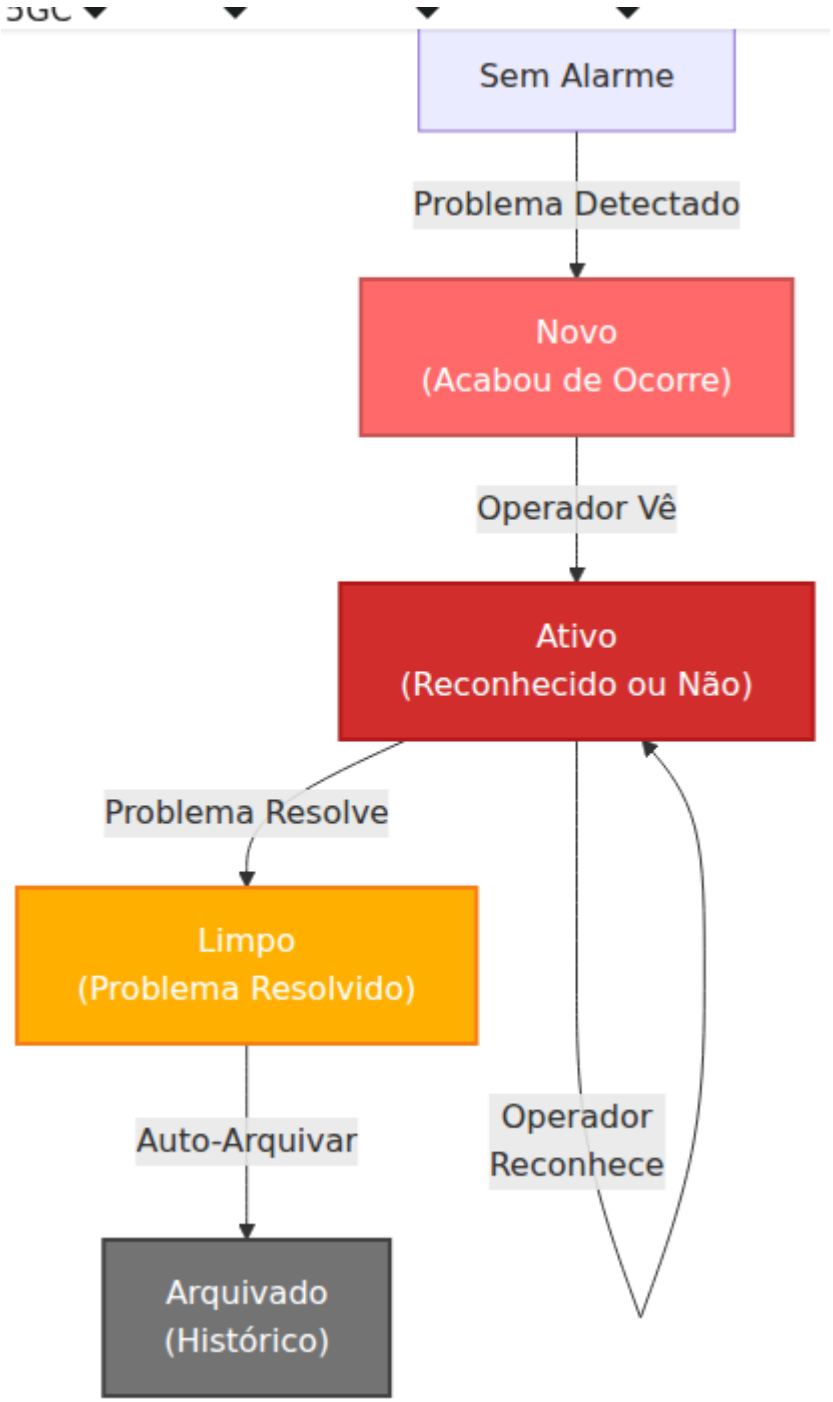
```
14:23:45 UTC - Ocorre o Problema
            └─> Estação base detecta perda de conectividade
            └─> Gera alarme: "Conexão S1 Perdida" (Crítico)

14:23:47 UTC - Alarme Enviado para o RAN Monitor
            └─> Notifica��ão de webhook NE3S recebida
            └─> Armazenado no InfluxDB
            └─> Regra de alerta acionada

14:23:50 UTC - Notificação Enviada
            └─> Alerta do Grafana acionado
            └─> Mensagem Slack para a equipe NOC
            └─> Incidente do PagerDuty criado

14:24:15 UTC - Operador Reconhece
            └─> Equipe NOC marca como reconhecido
            └─> Início do rastreamento de duração

14:28:35 UTC - Problema Auto-Resolve
            └─> Conectividade restaurada
            └─> Estação base limpa alarme
            └─> RAN Monitor registra "Limpo"

14:28:36 UTC - Alarme Fechado
            └─> Duração registrada: 5 minutos 51 segundos
            └─> Rastreado para relatório de SLA
            └─> Arquivado após 30 dias
```

Níveis de Severidade

O RAN Monitor rastreia cinco níveis de severidade, cada um com impacto operacional e requisitos de escalonamento diferentes:

Severidade Crítica

Definição: Impacta o serviço, requer ação imediata



Exemplos:

- Dispositivo completamente inacessível (perda de conectividade)
- Todas as células fora do ar (falha de banda base)
- Interface do plano de controle fora do ar (S1 perdido)
- Falha completa de encaminhamento de dados
- Estação base não respondendo à gestão

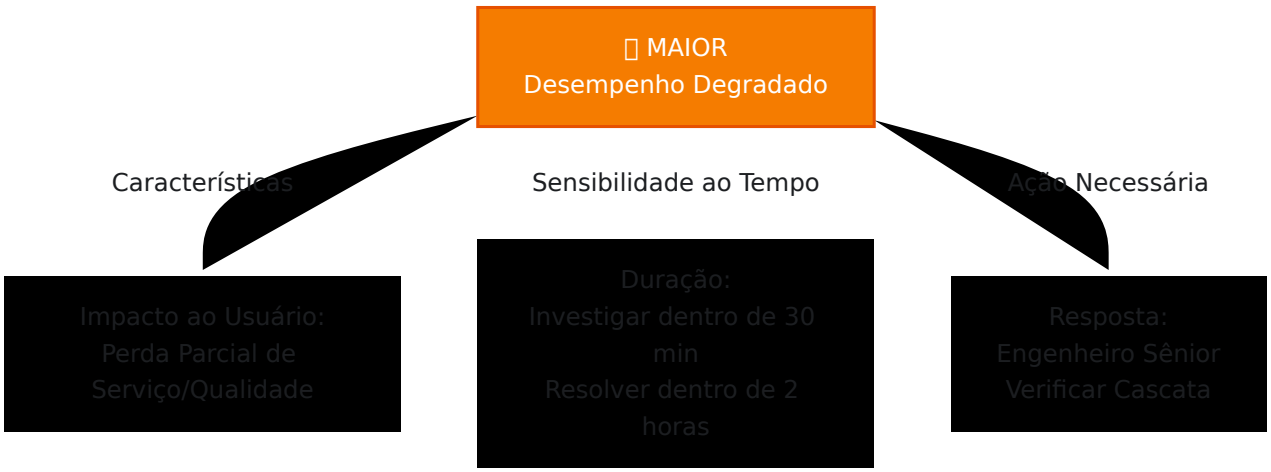
Escalonamento:

- Notificar engenheiro de plantão imediatamente (ligação telefônica)
- Criar incidente no sistema de gerenciamento de incidentes
- Atualizar página de status
- Informar a gestão se o SLA for afetado

SLA de Resposta: < 15 minutos

Severidade Maior

Definição: Desempenho degradado, requer investigação urgente



Exemplos:

- Disponibilidade da célula < 95% por > 15 minutos
- Taxa de sucesso de transferência < 95%
- Recurso DL/UL bloqueado (> 95% de utilização sustentada)
- Taxa de retransmissão RLC > 5%
- Múltiplas células apresentando baixa qualidade
- Degradação de link (aumentando erros E1/T1)

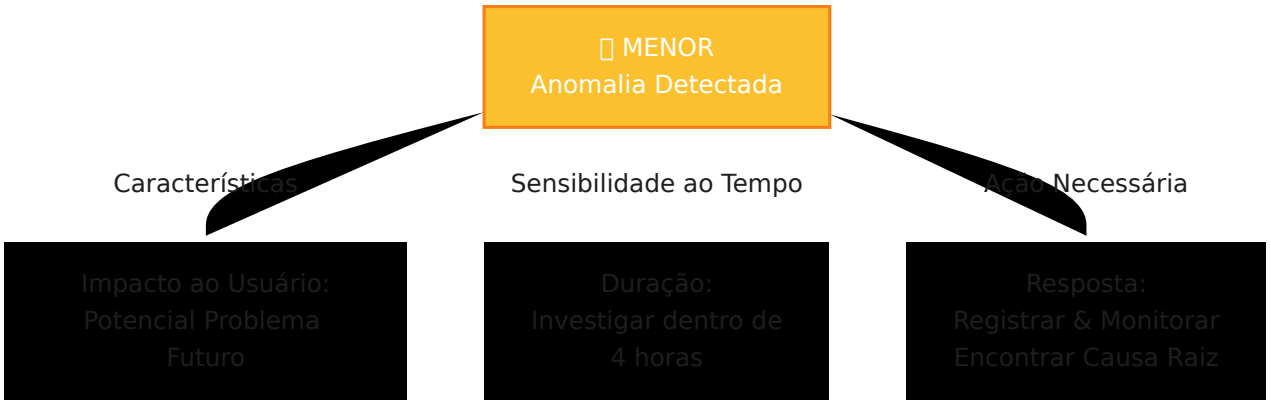
Escalonamento:

- Notificar equipe NOC + engenheiro sênior
- Criar incidente no gerenciamento de incidentes
- Notificar equipe de engenharia se ainda estiver aberto após 30 minutos
- Verificar problemas em cascata para outras células/sites

SLA de Resposta: < 30 minutos de investigação

Severidade Menor

Definição: Degradação, rastrear e investigar



Exemplos:

- Disponibilidade da célula 95-98% (tendência de queda)
- Aviso de alta temperatura no amplificador
- Capacidade de licença se aproximando do limite
- Problemas de consistência de configuração
- Desempenho lento na interface de gerenciamento
- Alarmes intermitentes (< 5 ocorrências/hora)

Escalonamento:

- Registrar no painel para conscientização
- Atribuir à engenharia para investigação
- Agendar para a próxima janela de manutenção, se necessário
- Criar ticket para análise de tendência

SLA de Resposta: Revisão no mesmo dia

Severidade de Aviso

Definição: Informacional, monitorar tendências

Exemplos:

- Disponibilidade da célula > 98% mas tendência de queda
- Temperatura/potência na faixa normal, mas elevada
- Recursos em 60-70% de utilização
- Inconsistência de configuração (parâmetros não críticos)
- Primeira ocorrência de novo tipo de falha

Escalonamento:

- Visibilidade apenas no painel
- Sem notificações automáticas
- Revisão manual em cadência

Limpo

Definição: Alarme anteriormente ativo agora resolvido

Propósito:

- Documenta que o problema foi resolvido
- Rastreia o tempo médio para reparo (MTTR)
- Permite relatórios de conformidade com SLA
- Identifica problemas recorrentes

Categorias de Alarmes

Alarmes de Conectividade

```
Categoria: Conectividade Externa
Causas Prováveis:
  - Conexão S1 Perdida       → MME/SGW inacessível
  - Link de Backhaul Fora    → Falha de transporte IP
  - Erro de Interface USIM    → Problema de conectividade HSS
  - Sincronização NTP Perdida → Problema de rede de sincronização
de tempo

Impacto: Interrupção de serviço, falhas na configuração de
chamadas
Investigação:
  1. Verificar conectividade de rede entre dispositivos
  2. Verificar se as regras de firewall permitem os protocolos
necessários
  3. Verificar status e erros do dispositivo par
  4. Revisar estatísticas da interface de rede
```

Alarmes de Hardware & Ambientais

```
Categoria: Infraestrutura Física
Causas Prováveis:
  - Aviso de Alta Temperatura  → Sistema de resfriamento degradado
  - Fonte de Alimentação Degradada → Problema de UPS/PSU
  - Falha do Ventilador         → Mau funcionamento do ventilador
de resfriamento
  - Espaço em Disco Baixo       → Armazenamento se aproximando do
limite
  - Exaustão de Memória         → Vazamento de memória do processo

Impacto: Falhas em cascata potenciais, perda de dados
Investigação:
  1. Verificar status do hardware via interface de gerenciamento
  2. Revisar tendências de temperatura
  3. Verificar operação do sistema de resfriamento
  4. Monitorar utilização de memória e CPU
```

Alarmes de Software & Processos

```
Categoria: Camada de Aplicação
Causas Prováveis:
  - Falha de Processo            → Erro de software ou OOM
  - Alta Utilização de CPU      → Gargalo de desempenho
  - Sobrecarga de Fila          → Acúmulo de processamento de
mensagens
  - Violação de Licença         → Capacidade excedida

Impacto: Degradação ou interrupção do serviço
Investigação:
  1. Verificar status do processo
  2. Revisar logs em busca de mensagens de erro
  3. Monitorar CPU/memória/profundidade da fila
  4. Verificar status da licença
```

Alarmes de Recursos de Rádio

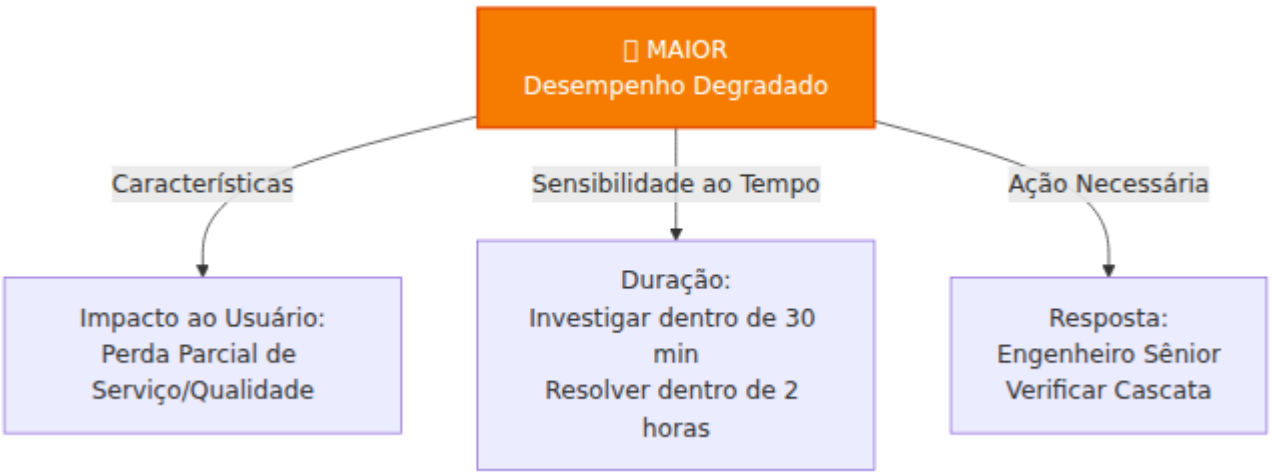
```
Categoria: Interface de Ar
Causas Prováveis:
  - Célula Indisponível         → Sem cobertura/potência de rádio
  - Recurso DL Bloqueado       → Exaustão de capacidade
  - Alta Taxa de Falha de Handover → Problema de configuração do
vizinho
  - Baixa Qualidade da Célula   → Interferência RF ou perda de
caminho

Impacto: Degradação da experiência do usuário
Investigação:
  1. Verificar parâmetros físicos da célula
  2. Revisar configuração da célula vizinha
  3. Analisar métricas de qualidade RF
  4. Verificar alinhamento da antena
```

Alarmes de Configuração

```
Categoria: Estado do Sistema
Causas Prováveis:
  - Inconsistência de Parâmetro       → Inconsistência de
configuração
  - Licença Expirada                   → Problema de licenciamento
  - Erro de Checksum de Configuração   → Corrupção ou conflito
  - Recurso Não Licenciado             → Uso de recurso excede
licença

Impacto: Indisponibilidade ou degradação de recurso
Investigação:
  1. Revisar alterações de configuração
  2. Comparar configuração atual vs. pretendida
  3. Verificar arquivo de licença e expiração
  4. Verificar compatibilidade da versão de software
```

Investigação & Solução de Problemas

Fluxo de Trabalho de Investigação



Etapa 1: Revisar Detalhes do Alarme

Quando um alarme é acionado, comece reunindo informações:

O que coletar:

- ID do Alarme e identificador único
- Severidade e causa provável
- Sistema DN afetado (dispositivo/célula/componente)
- Hora do evento (quando ocorreu)
- Duração (quanto tempo está ativo)
- Descrição completa do alarme e texto

Ferramentas:

- RAN Monitor Web UI → Página de Alarmes
- Grafana → Tabela de Alarmes Ativos
- InfluxDB → Consultar registro bruto do alarme

Etapa 2: Pesquisar Causa Provável

Cada tipo de alarme tem causas conhecidas e investigações:

Conhecimento Documentado:

- Guias de solução de problemas Nokia AirScale
- Histórico de tickets anteriores (problemas semelhantes)
- Runbooks documentados do RAN Monitor
- Especialização da equipe (especialistas no assunto)

Etapa 3: Verificar Métricas Relacionadas

Correlacione alarmes com métricas de desempenho para entender o impacto:

```
Exemplo: Alarme "Recurso DL Bloqueado"
├─ Verificar Utilização de Recurso DL (deve ser > 95%)
├─ Verificar Taxa de Tráfego (tendência de alta?)
├─ Verificar Sucesso na Configuração de Chamadas (desconexões?)
├─ Verificar Sucesso no Handover (afetado?)
└─ Verificar Disponibilidade da Célula (fora do ar?)
```

Ferramentas:

- Grafana → Painel específico do dispositivo
- Web UI → Página de detalhes do dispositivo → Seção de Métricas
- Consultas diretas do InfluxDB para correlação

Etapa 4: Correlacionar com Mudanças Recentes

Muitos problemas são causados por modificações recentes:

```
Linha do Tempo:
├─ Alterações de configuração (últimas 4 horas)
├─ Atualizações de software (últimas 24 horas)
├─ Ajustes de parâmetros de recurso (últimos 7 dias)
├─ Atividades de manutenção (últimos 7 dias)
├─ Mudanças na rede (últimos 7 dias)
└─ Mudanças de terceiros (rede externa)
```

Ferramentas:

- RAN Monitor → Histórico de configuração
- Sistema de gerenciamento de mudanças
- Histórico de incidentes (problemas semelhantes antes)
- Logs de notificação entre equipes

Etapa 5: Diagnosticar Causa Raiz

Com base na investigação, identifique a causa raiz:

Exemplo de Árvore de Decisão: Alarme "Célula Indisponível"

```
Alarme Célula Indisponível
│
├─ O dispositivo está respondendo à gestão?
│  ├─ NÃO → Verificar conectividade do dispositivo, reiniciar se
necessário
│  └─ SIM → Continuar
│
├─ Todas as células estão fora do ar ou célula específica?
│  ├─ Todas as células → Verificar hardware de banda base/fonte de
alimentação
│  └─ Célula específica → Continuar
│
├─ A célula está transmitindo potência?
│  ├─ NÃO → Verificar Amplificador de Potência, conexão da antena
│  └─ SIM → Continuar
│
├─ As células vizinhas estão reportando esta célula?
│  ├─ SIM → Outros dispositivos veem esta célula como indisponível
│  │       → Verificar alinhamento da antena, conexão do cabo
│  └─ NÃO → Célula está fora do ar por razão interna
│           → Verificar módulo de banda base, status do DSP
│
└─ Verificar logs em busca de mensagens de erro
   → Falha de software
   → Violação de licença
   → Erro de parâmetro
```

Etapa 6: Implementar Resolução

Uma vez que a causa raiz é identificada, implemente a correção:

Tipos de Resoluções:

Tipo	Método	Exemplo
Imediata	Reiniciar/reboot	Reiniciar dispositivo para limpar processo travado
Configuração	Ajustar parâmetros	Alterar limite de handover
Hardware	Substituir/reparar	Trocar fonte de alimentação com falha
Software	Atualizar/patch	Instalar correção de bug de software
Rede	Corrigir conectividade	Restaurar rota BGP, corrigir firewall

Etapa 7: Verificar Resolução

Após implementar a correção, verifique:

```
Lista de Verificação de Verificação:
□ Alarme limpo no RAN Monitor
□ Métricas relacionadas se normalizaram
□ Sem alarmes secundários/cascata
□ Métricas de desempenho retornaram ao normal
□ Relatórios de clientes (se aplicável) resolvidos
□ Sistema está estável (> 30 minutos de observação)
```

Etapa 8: Documentar Aprendizado

Registre as descobertas para referência futura:

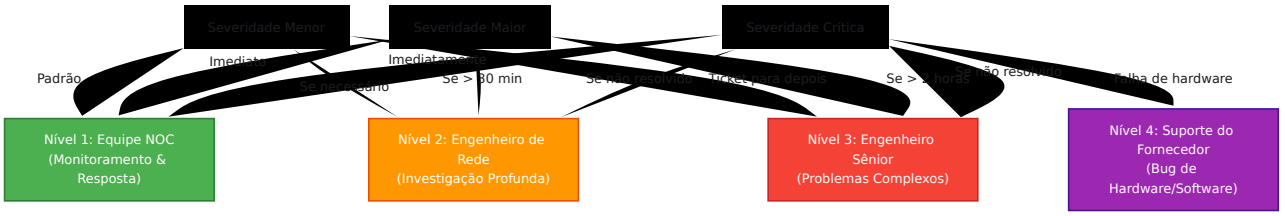
Documentar:

- Causa raiz e fatores contribuintes
- Passos tomados para resolver

- Tempo gasto (para rastreamento de SLA)
- Medidas preventivas tomadas
- Conhecimento compartilhado com a equipe

Procedimentos de Escalonamento

Escalonamento em Níveis



Gatilhos de Escalonamento

Escalonar para o Nível 2 se:

- Alarme crítico não limpo após 15 minutos
- Alarme maior não limpo após 30 minutos
- Problema está fora da especialização da equipe NOC
- Requer reinicialização do dispositivo/mudança significativa
- Afeta > 1 site simultaneamente

Escalonar para o Nível 3 se:

- Nível 2 incapaz de diagnosticar após 1 hora
- Problema crítico persiste > 30 minutos
- Falha de hardware suspeita
- Problemas em cascata detectados
- Requer envolvimento do fornecedor

Contatar o Fornecedor (Nível 4) se:

- Falha de hardware confirmada (PSU, CMON, etc.)

- Bug de software suspeito (crash irreversível)
- Problema de licença/ativação
- Problema documentado em questões conhecidas do fornecedor
- Múltiplos níveis de escalonamento incapazes de resolver

Comunicação de Escalonamento

Modelo para Escalonar para o Nível 2:

```
Assunto: Escalonamento - [Severidade] - [Dispositivo] - [Problema]

Hora do Alerta: [2025-12-10 14:30 UTC]
Duração: [15 minutos]
Dispositivo: [SITE_A_BS1]
Problema: [Célula Indisponível]

Sintomas:
- Célula A1 não respondendo à gestão
- Todas as células reportando célula indisponível
- Ping do dispositivo bem-sucedido

Investigação Realizada:
- Conectividade do dispositivo verificada
- Status do módulo de banda base verificado
- Status da fonte de alimentação: OK
- Temperatura: Normal

Métricas:
- Disponibilidade da célula: 0%
- Sem tráfego na célula
- Plano de controle: Conectado

Análise Inicial:
- Possível falha do módulo de banda base
- Ou problema de hardware do amplificador de potência

Próximos Passos Recomendados:
- Diagnósticos de hardware
- Troca de módulo se disponível
- Reiniciar dispositivo como último recurso

Link de Escalonamento: [Link do Painel]
```

Rastreamento de Resolução

Rastreamento de SLA

Rastrear o tempo até a resolução para conformidade com o SLA:

```
Linha do Tempo do Alarme:
├─ Hora do Evento: 14:23:45 ← Quando o problema ocorreu
├─ Hora da Detecção: 14:23:47 (2 seg) ← Gestão detectou
├─ Hora do Alerta: 14:23:50 (5 seg) ← Operações notificadas
├─ Hora de Reconhecimento: 14:24:15 (30 seg) ← Operador reconheceu
├─ Investigação: 14:24:15 → 14:28:00 (3,75 min)
├─ Resolução: 14:28:00 → 14:28:35 (35 seg de correção +
verificação)
└─ Hora de Limpeza: 14:28:36 ← Alarme limpo
    └─ Duração Total: 5 min 51 seg

Métricas de SLA:
├─ Latência de Detecção: 2 segundos
├─ Alerta para ACK: 30 segundos
├─ Tempo para Resolver: 5 min 51 seg
└─ Status do SLA: APROVADO (< 15 min alvo)
```

Análise de Tendências

Rastrear padrões nos dados de alarmes:

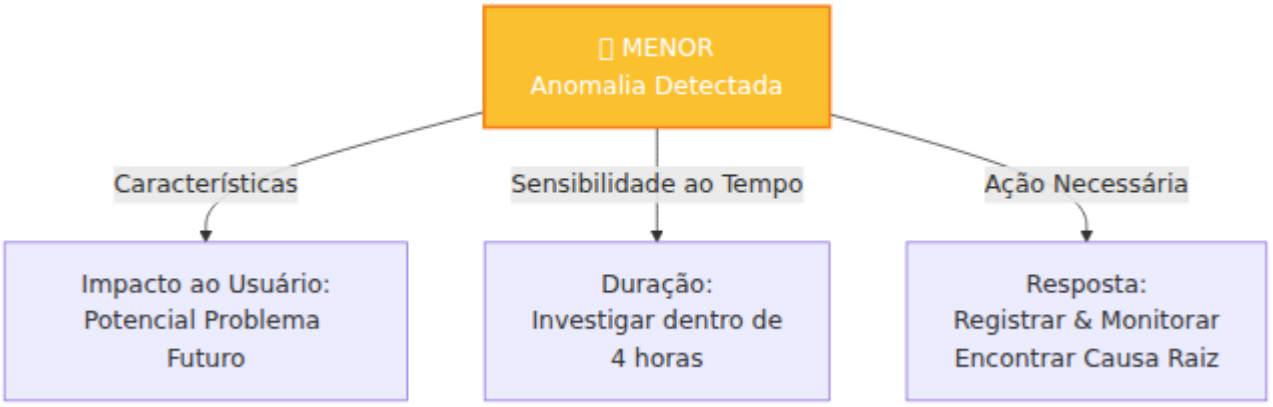
Perguntas a serem feitas:

- Estamos vendo o mesmo alarme repetidamente?
- A taxa de alarmes está aumentando/diminuindo?
- Os alarmes se agrupam em horários específicos?
- Múltiplos sites estão afetados simultaneamente?
- O MTTR está melhorando ao longo do tempo?

Ferramentas:

- Grafana → Painel de tendências de alarmes
- Relatório de principais alarmes (semanal)
- Rastreamento de MTTR por dispositivo/tipo

Prevenindo Problemas Repetidos



Melhores Práticas

Excelência Operacional

1. Prevenção da Fadiga de Alarmes

- Definir limites significativos (não muito sensíveis)
- Usar janelas de duração (não apenas picos únicos)
- Agregar alarmes relacionados
- Suprimir falsos positivos conhecidos

2. Resposta Rápida

- Manter runbooks atualizados
- Treinar a equipe sobre problemas comuns
- Usar automação para reinicializações rotineiras
- Ter contatos de escalonamento prontamente disponíveis

3. Documentação de Qualidade

- Documentar cada incidente
- Compartilhar aprendizados com a equipe
- Atualizar runbooks com base em incidentes
- Treinar cruzadamente membros da equipe

4. Monitoramento Proativo

- Observar avisos antes de críticos
- Análise de tendências para planejamento de capacidade
- Verificações de saúde regulares
- Estabelecimento de linha de base de desempenho

Desenvolvimento de Runbook

Todo alarme frequente deve ter um runbook:

Modelo:

```
Alarme: [Célula Indisponível]
Probabilidade: [Alta]
MTTR: [5-15 minutos]
Meta de SLA: [Resolvido dentro de 30 minutos]

Sintomas:
- Alarme: "Célula Indisponível"
- Usuários: Incapazes de conectar
- Métricas: Disponibilidade da célula 0%

Diagnóstico Rápido (< 5 minutos):
1. O dispositivo está respondendo ao ping?
2. Outras células estão funcionando?
3. O módulo de banda base está funcionando (verificar logs)?

Passos de Resolução:
Passo 1: Verificação de Conectividade do Dispositivo
  - Ping dispositivo: ping 192.168.1.100
  - Se não houver resposta → Verificar conectividade de rede

Passo 2: Status do Hardware
  - Verificar status do Amplificador de Potência
  - Verificar LEDs do módulo de banda base
  - Verificar conexão da antena

Passo 3: Reiniciar Célula
  - Reiniciar célula via interface de gerenciamento
  - Aguardar 60 segundos para inicialização
  - Verificar normalização das métricas

Passo 4: Se Ainda Estiver Fora do Ar
  - Escalonar para Nível 2
  - Preparar para reinicialização do dispositivo
  - Notificar cliente

Escalonamento:
- Se > 15 minutos → Escalonar para [Nome do Engenheiro]
- Se > 30 minutos → Escalonar para [Engenheiro Sênior]
- Se falha de hardware → Contatar Suporte Nokia

Prevenção:
- Atualizações regulares de firmware de banda base
```

```
- Substituição preventiva da fonte de alimentação
- Inspeção da conexão da antena trimestralmente
```

Endpoints da API e Gerenciamento de Configuração

API REST para Gerenciar Configuração e Operações de Dispositivos RAN

Guia para gerenciar a configuração da estação base, consultar o estado do dispositivo e automatizar operações RAN usando a API independente de fornecedor

---

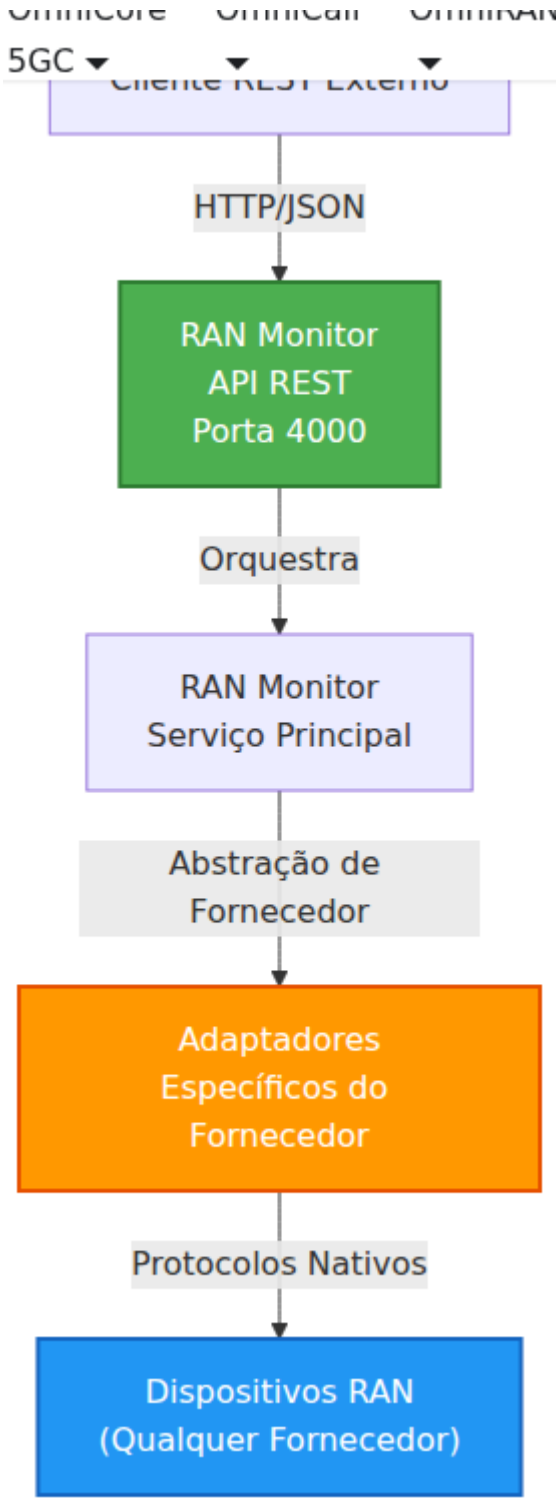
Índice

Visão Geral

O RAN Monitor expõe uma API REST abrangente para gerenciar a configuração de dispositivos RAN e consultar dados operacionais. A API fornece uma interface independente de fornecedor que abstrai os protocolos de comunicação de dispositivos subjacentes. A API permite:

- **Gerenciamento de Dispositivos** - Registrar, cancelar registro e monitorar dispositivos
- **Consultas de Configuração** - Recuperar parâmetros de dispositivos e estado do sistema
- **Coleta de Dados** - Extrair métricas de desempenho, alarmes e topologia
- **Controle de Sessão** - Gerenciar sessões de comunicação com dispositivos
- **Operações de Rede** - Automatizar tarefas de gerenciamento rotineiras

Arquitetura da API



Recursos da API

- **Design RESTful** - Métodos HTTP padrão (GET, POST, PUT, DELETE)
- **Formato JSON** - Todas as requisições e respostas são em JSON

- **Abstração de Fornecedor** - API unificada entre diferentes fornecedores de dispositivos
- **Operações Stateful** - Mantém sessões e estado do dispositivo
- **Tratamento de Erros** - Mensagens de erro detalhadas e códigos de status
- **Processamento Assíncrono** - Requisições não bloqueantes para operações longas

---

Autenticação e Acesso

Registro de Dispositivo

Antes de qualquer operação, um dispositivo deve ser registrado no RAN Monitor. O registro estabelece a conexão entre o RAN Monitor e o dispositivo usando o mecanismo de autenticação nativo de cada fornecedor.

Processo de Registro:

1. Credenciais do dispositivo (nome de usuário/senha ou chaves de API) são armazenadas com segurança
2. O teste de conectividade inicial verifica se o dispositivo é acessível
3. O dispositivo é registrado e está pronto para operações
4. O monitoramento contínuo de saúde começa

Controle de Acesso à API

Atualmente, a API do RAN Monitor é acessível dentro da rede de gerenciamento. Para implantações em produção, considere:

- **Métodos de Autenticação:**
  - Chave de API no cabeçalho: `Authorization: Bearer <api-key>`
  - OAuth2 para integração com provedores de identidade
  - Controle de acesso baseado em rede (firewall/VPN)
- **Limitação de Taxa:**

    - Limites por cliente para prevenir abusos
    - Limites por dispositivo para frequência de operações

- **Registro de Auditoria:**
    - Todas as chamadas da API são registradas com timestamps e informações do usuário/cliente
    - Mudanças de configuração são rastreadas com valores antes/depois

---

Referência de Endpoint

Gerenciamento de Dispositivos

Listar Todos os Dispositivos

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

Resposta:

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

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

Obter Detalhes do Dispositivo

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

Resposta:

```
{
  "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"
    }
  }
}
```

Registrar um Dispositivo

```
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"
}
```

Resposta:

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

Códigos de Status:

- `200` - Registro bem-sucedido
- `400` - Parâmetros inválidos ou erro no dispositivo
- `409` - Dispositivo já registrado
- `500` - Erro interno

Cancelar Registro de um Dispositivo

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

Resposta:

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

Gerenciamento de Sessão

Iniciar uma Sessão

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

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

Resposta:

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

Duração da Sessão:

- Tempo limite padrão: 24 horas
- Manter-alive necessário antes do tempo limite
- Atualização automática a cada 20 horas

Verificar Status da Sessão

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

Resposta:

```
{
  "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"
  }
}
```

Manter a Sessão Ativa

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

Resposta:

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

Gerenciamento de Configuração

Consultar Configuração

Recuperar parâmetros de configuração do dispositivo:

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

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

Resposta:

```
{
  "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
        }
      }
    }
  }
}
```

Provisionar Configuração

Enviar um arquivo de configuração para um dispositivo, realizando download, validação e ativação em uma única operação atômica. Um fallback da configuração atual em execução é salvo automaticamente.

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

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

Resposta:

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

Parâmetros:

Parâmetro	Tipo	Requerido	Padrão	Propósito
airscale_name	String	Sim	-	Nome do dispositivo alvo
config_file	String	Sim	-	Caminho para o arquivo de configuração XML no servidor
take_fallback	Boolean	Não	true	Salvar a configuração atual como fallback antes da ativação
block_local_changes	Boolean	Não	false	Bloquear alterações locais durante a operação

Erros:

- `INVALID_FILE` - caminho do config_file ausente ou arquivo não existe
- `TRANSPORT_ERROR` - Problema de conectividade de rede com o dispositivo
- `SESSION_ERROR` - Não foi possível estabelecer a sessão NE3S
- Falhas SOAP do dispositivo (por exemplo, erros de validação, violações de esquema)

Definir Parâmetro de Configuração

```
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"
}
```

Resposta:

```
{
  "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"
}
```

Parâmetros de Configuração Comuns:

Parâmetro	Tipo	Exemplo	Propósito
BtsName	String	"SITE_A_Cell_1"	Identificador da célula/estação base
MaxUEsServed	Inteiro	256	Máximo de UEs simultâneos
CellTXPower	Inteiro	40 (dBm)	Nível de potência de transmissão
EnableCarrierAgg	Boolean	true	Suporte à agregação de portadora
HandoverHysteresis	Inteiro	3 (dB)	Sensibilidade de transferência

Obter Histórico de Configuração

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

Resposta:

```
{
  "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": "Atualização de configuração manual"
    }
  ]
}
```

Recuperação de Dados

Obter Métricas de Desempenho

Recuperar dados de contadores de desempenho:

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

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

Resposta:

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

Obter Alarmes Ativos

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

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

Resposta:


```
{
  "result": "Success",
  "alarms": [
    {
      "alarm_id": "a1b2c3d4",
      "severity": "Critical",
      "probable_cause": "Célula Indisponível",
      "specific_problem": "Falha na Fonte de Alimentação",
      "affected_dn": "/BSC-1/BTS-23/Cell-1",
      "event_time": "2025-12-10T14:15:30Z",
      "description": "Célula 1 está indisponível devido a falha na
fonte de alimentação"
    }
  ]
}
```


Obter Topologia do Dispositivo

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

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

Resposta:

```
{
  "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
          }
        ]
      }
    ]
  }
}
```

Verificações de Saúde

Ping no Dispositivo

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

Resposta:

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

Obter Métricas do Sistema

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

Retorna estatísticas do gravador em lote, status do spool PM, estatísticas do InfluxDB por dispositivo e uso de recursos do sistema.

Resposta:

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


Obter Saúde do Sistema

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

Resposta:

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

Gerenciamento de Configuração

Modelo de Dados de Configuração

A configuração do eNodeB da Nokia é organizada hierarquicamente:

```
/SystemFunctions
├── /BSC-1 (Controlador da Estação Base)
│   └── /BTS-23 (Estação Transceptora Base)
│       ├── BtsBasics (Nome, tipo, localização)
│       ├── /Cell-1
│       │   ├── CellCommonData
│       │   ├── CellAdvanced
│       │   └── CarrierAggregation
│       └── /Cell-2
│           └── ...
└── /Connectivity
    ├── S1Interface
    ├── X2Interface
    └── NetworkConfiguration
```

Tarefas Comuns de Configuração

Habilitar/Desabilitar uma Célula

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

Valores possíveis: `LOCKED`, `UNLOCKED`, `SHUTTING_DOWN`

Ajustar Potência da Célula

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

Faixa: 0-46 dBm (dependente do dispositivo)

Configurar Histerese de Transferência

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

Unidade: dB, faixa típica: 0-8 dB

Definir Máximo de Usuários Conectados

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

Limite dependente do dispositivo

Fluxos de Trabalho Comuns

Fluxo de Trabalho 1: Onboarding de

Dispositivo


Início: Novo Dispositivo
1. Criar Dispositivo
POST /api/devices
2. Registrar Dispositivo
PUT
/api/devices/:id/register
3. Iniciar Sessão
PUT
/api/devices/:id/sessions
4. Consultar Config
PUT
/api/devices/:id/config/upload
5. Extrair Métricas
PUT
/api/devices/:id/metrics/upload
Sucesso: Dispositivo
Operacional

Exemplo:

```
# 1. Criar entrada de dispositivo
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. Registrar com o dispositivo
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. Iniciar sessão
curl -X PUT
http://localhost:4000/api/v1/devices/site_a_bs1/sessions \
  -H "Content-Type: application/json" \
  -d '{"session_id": "session_001"}'

# 4. Obter configuração
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}]
    }
  }'
```

Fluxo de Trabalho 2: Atualização de Configuração

```
# 1. Consultar valor atual
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. Modificar parâmetro
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. Verificar mudança
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"]'
```

Fluxo de Trabalho 3: Monitoramento de

Desempenho

```
# Loop de monitoramento contínuo (exemplo de script)
#!/bin/bash

DEVICE="site_a_bs1"
INTERVAL=300  # 5 minutos

while true; do
  # Extrair métricas
  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}]
      }
    }')

  # Extrair métricas chave
  DL=$(echo $METRICS | jq '.metrics.counters[] |
select(.id=="M1C1") | .value')
  CELLS=$(echo $METRICS | jq '.metrics.counters | length')

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

  # Verificar 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 "AVISO: $ALARMS alarmes ativos"
  fi
```

```
  sleep $INTERVAL
done
```

Tratamento de Erros

Códigos de Status HTTP

Código	Significado	Exemplo
`200`	Sucesso	Configuração recuperada
`201`	Criado	Dispositivo registrado
`400`	Solicitação Inválida	JSON ou parâmetros inválidos
`401`	Não Autorizado	Chave de API ausente/inválida
`404`	Não Encontrado	Dispositivo não existe
`409`	Conflito	Dispositivo já registrado
`500`	Erro do Servidor	Falha na conexão com o banco de dados
`503`	Indisponível	Modo de manutenção

Formato de Resposta de Erro

```
{
  "error": {
    "code": "DEVICE_NOT_FOUND",
    "message": "Dispositivo 'site_a_bs1' não encontrado",
    "details": {
      "device_id": "site_a_bs1",
      "timestamp": "2025-12-10T14:30:00Z"
    }
  }
}
```

Erros Comuns

Dispositivo Não Registrado:

```
{
  "error": {
    "code": "NOT_REGISTERED",
    "message": "O dispositivo deve ser registrado antes das
operações",
    "solution": "Chame PUT /api/devices/:id/register primeiro"
  }
}
```

Sessão Expirada:

```
{
  "error": {
    "code": "SESSION_EXPIRED",
    "message": "A sessão do dispositivo expirou",
    "solution": "Chame PUT /api/devices/:id/sessions para iniciar
nova sessão"
  }
}
```

Parâmetro de Configuração Inválido:

```
{
  "error": {
    "code": "INVALID_PARAMETER",
    "message": "Valor do parâmetro fora do intervalo",
    "details": {
      "parameter": "/BSC-1/BTS-23/Cell-
1/CellAdvanced/CellTXPower",
      "value": "99",
      "valid_range": "0-46 dBm"
    }
  }
}
```

Exemplos da API

Exemplo de Cliente 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):
        """Registrar um novo dispositivo"""
        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):
        """Recuperar configuração do dispositivo"""
        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"):
        """Atualizar um parâmetro de configuração"""
        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):
        """Recuperar métricas de desempenho"""
        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()

# Exemplo de uso
client = RanMonitorClient()

# Registrar dispositivo
result = client.register_device(
    device_id="site_a_bs1",
    address="192.168.1.100:8080",
    username="admin",
    password="password"
)
print(f"Registro: {result}")

# Obter configuração
config = client.get_config("site_a_bs1")
print(f"Config: {json.dumps(config, indent=2)}")

# Atualizar parâmetro
update = client.set_config(
    "site_a_bs1",
    "/BSC-1/BTS-23/Cell-1/CellAdvanced/CellTXPower",
    "38",
    "integer"
```

```
)
print(f"Atualização: {update}")
```

Exemplos de cURL

Registrar Dispositivo:

```
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"
  }'
```

Obter Status do Dispositivo:

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

Consultar Configuração:

```
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 '.'
```

Guia do Arquivo de Configuração

Versionamento Automatizado e Rastreamento Histórico para Configurações AirScale

---

Visão Geral

O sistema de Arquivo de Configuração rastreia e versiona automaticamente todos os arquivos de configuração da estação base AirScale. Em vez de armazenar instantâneas de configuração no InfluxDB, as configurações são salvas como arquivos XML com timestamp no servidor, fornecendo um completo histórico de auditoria das mudanças de configuração.

Principais Recursos

- **Versionamento Automático** - Novas versões criadas apenas quando há mudanças na configuração
- **Polling Horário** - Verifica mudanças de configuração a cada hora (configurável)
- **Detecção de Mudanças** - Comparação inteligente detecta mudanças reais, ignorando espaços em branco
- **Limites Baseados em Tamanho** - Armazenamento máximo de 100 MB por dispositivo (mantém ~690 versões)
- **Interface Web** - Navegue, baixe e gerencie versões de configuração
- **Acesso Rápido** - Armazenamento baseado em arquivos para recuperação instantânea
- **Zero Carga no InfluxDB** - Configurações não são mais armazenadas no banco de dados de séries temporais
- **Limpeza Automática** - Versões antigas excluídas quando o limite de tamanho é atingido

---

Como Funciona

Cronograma de Polling

A configuração é consultada de cada estação base AirScale registrada:

- **Intervalo:** A cada 1 hora (padrão)
- **Primeiro Poll:** Imediatamente na inicialização do aplicativo
- **Detecção de Mudanças:** Compara o conteúdo com a versão anterior
- **Armazenamento:** Salva apenas se houver mudança ou na primeira vez

Localização de Armazenamento

As configurações são armazenadas no sistema de arquivos do servidor RAN Monitor:

```
priv/airscale_configs/
└── <airscale-name>/
    ├── current.xml                                    # Última
configuração
    ├── ONS-Lab-Airscale_config_20251230_143522.xml   # Versão de
30 de Dez, 14:35
    ├── ONS-Lab-Airscale_config_20251229_120000.xml   # Versão
anterior
    ├── ONS-Lab-Airscale_config_20251228_093045.xml   # Versão
mais antiga
    └── ...                                            # Versões
mantidas até o limite de 100 MB
```

Formato do Nome do Arquivo:
`<AirScaleName>_config_YYYYMMDD_HHMMSS.xml`

Nomeação de Diretórios: Nomes AirScale são sanitizados (caracteres especiais substituídos por sublinhados, minúsculas)

Gerenciamento de Versões

- **Última Versão:** Sempre disponível como `current.xml`
- **Versões Históricas:** Arquivos com timestamp mostrando quando a configuração mudou
- **Limpeza Automática:** Exclui as versões mais antigas quando o limite de 100 MB é atingido
- **Limpeza Manual:** Exclua versões específicas via UI Web (exceto `current.xml`)
- **Proteção de Armazenamento:** Limite baseado em tamanho previne uso ilimitado do disco
- **Retenção Flexível:** Mais versões se os arquivos forem pequenos, menos se os arquivos forem grandes

---

Proteção de Armazenamento

Limite de Armazenamento Baseado em Tamanho

Para prevenir o uso ilimitado do disco, o sistema utiliza um **limite baseado em tamanho** em vez de uma contagem de versões:

- **Tamanho Máximo:** 100 MB por dispositivo (configurável)
- **Limpeza Automática:** Versões mais antigas excluídas quando o limite de tamanho é excedido
- **Tempo de Limpeza:** Cada vez que uma nova versão de configuração é salva
- **Arquivos Protegidos:** `current.xml` e pelo menos uma versão sempre mantida
- **Flexível:** Mantém ~690 versões a 145KB cada, mais se os arquivos forem menores

Como Funciona

Quando uma nova versão de configuração é salva:

1. **Salvar nova versão** - Configuração escrita como `<AirScale>_config_YYYYMMDD_HHMMSS.xml`
2. **Atualizar atual** - `current.xml` atualizado com a última configuração
3. **Calcular tamanho** - O sistema soma o tamanho total de todos os arquivos versionados
4. **Limpar antigos** - Se o total > 100 MB, exclui as versões mais antigas até ficar abaixo do limite
5. **Registrar atividade** - Exclusões registradas com espaço liberado

Cenário Exemplo

```
Estado inicial: 95 MB usados (655 versões a 145KB cada)
├── ONS-Lab-Airscale_config_20240101_100000.xml  <- Mais antiga
(145KB)
├── ONS-Lab-Airscale_config_20240102_100000.xml  (145KB)
├── ... (653 mais versões)
└── ONS-Lab-Airscale_config_20251230_100000.xml  <- Mais nova
(145KB)

Nova configuração detectada em 2025-12-31 10:00:00 (145KB)

Ações:
1. Salvar: ONS-Lab-Airscale_config_20251231_100000.xml (145KB)
2. Tamanho total agora: 95 MB + 145KB = 95.14 MB (ainda abaixo do
limite de 100 MB)
3. Nenhuma exclusão necessária
4. Final: 656 versões, 95.14 MB usados

---

Mais tarde: Grande mudança de configuração (novos recursos
adicionados, arquivo agora é 500KB)

Ações:
1. Salvar: ONS-Lab-Airscale_config_20251231_150000.xml (500KB)
2. Tamanho total agora: 95.14 MB + 500KB = 95.64 MB (ainda abaixo
do limite)
3. Nenhuma exclusão necessária
4. Final: 657 versões, 95.64 MB usados

---

Após muitas outras mudanças: Aproximando-se do limite

Estado atual: 99.8 MB (685 versões)

Nova configuração: 200KB
1. Salvar nova versão
2. O total seria: 100 MB (excede o limite)
3. Excluir as versões mais antigas até que o total < 100 MB
```

```
4. Exclusões registradas: "Excluídas 3 versões, liberados 435 KB"
5. Final: 682 versões, 99.6 MB usados
```

Garantias de Armazenamento

A limpeza automática garante:

- **Armazenamento Limitado:** Cada dispositivo limitado a 100 MB no máximo
- **Sem Surpresas:** O armazenamento não crescerá indefinidamente
- **Seguro para Produção:** Nenhuma intervenção manual necessária
- **Histórico Flexível:** Mais versões para configurações pequenas, menos para configurações grandes
- **Sempre Disponível:** Pelo menos uma versão sempre mantida

Monitorando Armazenamento

Verifique o uso de armazenamento para todos os dispositivos:

```
# Total de armazenamento usado
du -sh priv/airscale_configs/
# Exemplo: 215M (para 3 dispositivos com média de 70 MB cada)

# Armazenamento por dispositivo
du -sh priv/airscale_configs/*/
# Exemplo:
# 95M     priv/airscale_configs/ons-lab-airscale/
# 68M     priv/airscale_configs/sector-1/
# 52M     priv/airscale_configs/sector-2/

# Verifique se algum dispositivo está próximo do limite
find priv/airscale_configs -maxdepth 1 -type d -exec du -sm {} \;
| awk '$1 > 90 {print $2 " está em " $1 "MB (aproximando-se do
limite de 100MB)"}'
```

Usando a Página do Arquivo de Configuração

Acessando o Arquivo de Configuração

UI Web: Navegue até **Nokia → Arquivo de Configuração**

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

Interface do Arquivo de Configuração mostrando o seletor de estação base, tabela de histórico de versões com timestamps e tamanhos de arquivo, e informações de armazenamento.

Visão Geral da Interface

A página do Arquivo de Configuração tem três seções principais:

1. Seletor de Estação Base

- **Visualização em Grade** - Mostra todos os dispositivos AirScale registrados
- **Contagem de Versões** - Número de versões de configuração armazenadas para cada um
- **Seleção** - Clique em um dispositivo para ver seu histórico de configuração
- **Indicador Visual** - Dispositivo selecionado destacado em azul

2. Tabela de Histórico de Versões

Exibe todas as versões de configuração para a estação base selecionada:

Coluna	Descrição
Timestamp	Quando a configuração foi salva (UTC)
Filename	Nome do arquivo da versão (ex: `config_20251230_143522.xml`)
Size	Tamanho do arquivo em KB ou MB
Age	Há quanto tempo a versão foi criada (ex: "2h atrás", "3d atrás")
Actions	Botões de Download ou Excluir

Ordenação: As versões mais novas aparecem primeiro (decrescente por timestamp)

Configuração Atual: O arquivo `current.xml` não pode ser excluído (medida de segurança)

3. Informações de Armazenamento

Painel de resumo mostrando:

- **Total de Versões** - Número de versões de configuração armazenadas
- **Tamanho Total** - Tamanho combinado de todas as versões

- **Caminho de Armazenamento** - Localização do sistema de arquivos no servidor

---

Operações Comuns

Baixando uma Configuração

Propósito: Recuperar uma versão específica da configuração para revisão, backup ou comparação

Passos:

1. Navegue até a página do Arquivo de Configuração
2. Selecione a estação base desejada
3. Encontre a versão que você deseja na tabela
4. Clique no botão **Baixar**
5. O arquivo é baixado com o formato: `<AirScaleName>_config_YYYYMMDD_HHMMSS.xml` (corresponde ao nome do arquivo armazenado)

Casos de Uso:

- Criando backups offline
- Comparando configurações entre timestamps
- Revertendo para uma configuração anterior conhecida como boa
- Analisando a deriva de configuração ao longo do tempo

Excluindo Versões Antigas

Propósito: Remover versões de configuração desatualizadas para liberar espaço de armazenamento

Passos:

1. Navegue até a página do Arquivo de Configuração

2. Selecione a estação base
3. Encontre a versão a ser excluída
4. Clique no botão **Excluir**
5. Confirme a exclusão no diálogo popup
6. A versão é removida permanentemente

Notas Importantes:

- Não é possível excluir `current.xml` (última versão protegida)
- A exclusão é imediata e não pode ser desfeita
- A exclusão manual não afeta as configurações de limpeza automática

Comparando Configurações

Propósito: Identificar o que mudou entre duas versões de configuração

Comparação Manual:

1. Baixe ambas as versões que você deseja comparar
2. Use uma ferramenta de diff XML (ex: `xmldiff`, `Beyond Compare`, `WinMerge`)
3. Revise as diferenças para entender as mudanças

Exemplo usando linha de comando:

```
# Baixe ambas as versões
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

# Compare com diff
diff ONS-Lab-Airscale_config_20251229_120000.xml ONS-Lab-
Airscale_config_20251230_143522.xml

# Ou use xmldiff para uma saída mais limpa
xmldiff ONS-Lab-Airscale_config_20251229_120000.xml ONS-Lab-
Airscale_config_20251230_143522.xml
```

Fluxos de Trabalho de Gerenciamento de Configuração

Investigação de Rastro de Auditoria

Cenário: Necessidade de determinar quando uma configuração mudou

Passos:

1. Abra o Arquivo de Configuração
2. Selecione a estação base afetada
3. Revise os timestamps das versões
4. Baixe as versões relevantes
5. Compare para identificar mudanças exatas
6. Correlacione com problemas de desempenho ou alarmes

Exemplo:

```
Linha do Tempo das Versões:
- ONS-Lab-Airscale_config_20251230_143522.xml (143KB) - Mais
recente
- ONS-Lab-Airscale_config_20251228_091045.xml (142KB) - 2 dias
atrás
- ONS-Lab-Airscale_config_20251225_180000.xml (142KB) - 5 dias
atrás

Análise:
- O tamanho aumentou de 142KB para 143KB em 30 de Dez
- Compare 28 de Dez vs 30 de Dez para encontrar o que foi
adicionado
- Verifique se o tempo correlaciona com o pico de alarme
```

Reversão de Configuração

Cenário: Mudança recente de configuração causou problemas, necessidade de restaurar a versão anterior

Passos:

1. Identifique a versão de configuração conhecida como boa
2. Baixe essa versão do Arquivo de Configuração
3. Navegue até a página de Gerenciamento de Configuração (UI Web)
4. Faça o upload da configuração baixada → receba o ID do Plano
5. Valide o plano → verifique se há erros
6. Se a validação for bem-sucedida, ative o plano
7. Monitore o dispositivo para estabilidade
8. Verifique se a nova configuração aparece no arquivo após o próximo polling

Lista de Verificação de Segurança:

- ✓ Baixou a versão anterior correta
- ✓ Validou o plano antes da ativação
- ✓ Coordenou com a equipe de operações
- ✓ Agendado durante a janela de manutenção
- ✓ Ferramentas de monitoramento prontas para verificação

Gerenciamento de Configuração Base

Cenário: Manter uma "configuração padrão" para padronização

Melhor Prática:

1. Crie e valide a configuração base
2. Aplique ao dispositivo de referência
3. Baixe do Arquivo de Configuração após o próximo polling
4. Armazene externamente como template
5. Use para implantar novos dispositivos
6. Revise e atualize periodicamente a base

Detalhes Técnicos

Algoritmo de Detecção de Mudanças

O sistema utiliza comparação inteligente de conteúdo para evitar falsos positivos:

Processo de Normalização:

1. Remover espaços em branco iniciais/finais
2. Colapsar espaços em branco entre tags XML
3. Normalizar espaços internos
4. Comparar o conteúdo normalizado resultante

Benefícios:

- Mudanças de formatação não acionam novas versões
- Apenas mudanças reais na configuração criam versões
- Reduz as necessidades de armazenamento
- Fornece um histórico de mudanças significativo

Exemplo:

```
<!-- Estes são considerados idênticos -->

<!-- Versão 1 (com espaço extra) -->
<parameter>
    <name>cellId</name>
    <value>1</value>
</parameter>

<!-- Versão 2 (compacta) -->
<parameter><name>cellId</name><value>1</value></parameter>
```

Requisitos de Armazenamento

Tamanho Típico da Configuração: ~145 KB por versão (com base nas configurações reais do AirScale)

Planejamento de Capacidade:

Dispositivos	Tamanho Máximo por Dispositivo	Versões Mantidas (a 145KB)	Armazenamento Total Máximo
10	100 MB	~690	1 GB
50	100 MB	~690	5 GB
100	100 MB	~690	10 GB
500	100 MB	~690	50 GB
1000	100 MB	~690	100 GB

Características de Crescimento:

- **Armazenamento máximo por dispositivo:** 100 MB (configurável)
- **Versões típicas retidas:** ~690 (145KB cada)
- **Se a configuração nunca mudar:** Crescimento mínimo (apenas current.xml a 145KB)
- **Se a configuração mudar frequentemente:** O crescimento para ao atingir o limite de 100 MB
- **Adaptativo:** Mantém mais versões para configurações pequenas, menos para configurações grandes

Proteção Automática:

- Versões antigas excluídas quando o limite de tamanho é atingido
- Nenhuma intervenção manual necessária
- Uso de armazenamento estritamente limitado por dispositivo

- Pelo menos uma versão sempre retida

Política de Retenção

Configurações Padrão:

- Armazenamento máximo de **100 MB** por dispositivo
- Exclusão automática das versões mais antigas quando o limite é excedido
- `current.xml` sempre retido (isento de limpeza)
- A limpeza ocorre toda vez que uma nova versão é salva
- Pelo menos um arquivo versionado sempre mantido

Personalizando a Retenção:

O limite de armazenamento é configurado no módulo ConfigStorage:

```
# Em lib/ran_monitor/nokia/airscale/config_storage.ex
# Atributo do módulo no topo do arquivo
@max_storage_bytes 100 * 1024 * 1024  # 100 MB padrão

# Mudar para um limite diferente:
@max_storage_bytes 50 * 1024 * 1024   # 50 MB (mantém ~345
versões)
@max_storage_bytes 200 * 1024 * 1024  # 200 MB (mantém ~1380
versões)

# A função de limpeza usa este padrão
def cleanup_old_versions(airscale_name, max_size_bytes \
@max_storage_bytes)
```

Após modificar, recompilar:

```
mix compile
# Reinicie o RAN Monitor para aplicar as mudanças
```

Configuração de Polling

Intervalo Padrão: 1 hora (3.600.000 milissegundos)

Para Alterar o Intervalo de Polling:

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

```
defp schedule_get_airscale_config do
  # Puxar configuração a cada 1 hora (3.600.000 ms)
  Process.send_after(self(), :get_airscale_config, 3_600_000)
end
```

Intervalos Comuns:

- 30 minutos: `1_800_000`
- 1 hora: `3_600_000` (padrão)
- 2 horas: `7_200_000`
- 4 horas: `14_400_000`
- 24 horas: `86_400_000`

Após a alteração, recompilar e reiniciar o RAN Monitor.

Resolução de Problemas

Nenhuma Versão de Configuração Mostrando

Sintomas:

- A página do Arquivo de Configuração mostra "0 versões"
- O dispositivo selecionado mostra tabela vazia

Possíveis Causas:

1. **Dispositivo Não Registrado**
    - Verifique a página de Estações Base
    - Verifique se o dispositivo mostra status "REGISTRADO"
    - Revise os Logs do Aplicativo para erros de registro

2. **Sessão Não Ativa**
    - Verifique a visualização de detalhes do dispositivo
    - Assegure-se de que o status da sessão é "ATIVA"
    - Revise os timestamps da sessão
3. **Configuração Ainda Não Consultada**
    - Aguarde o primeiro ciclo de polling horário
    - Ou acione manualmente: `Kernel.send(Process.whereis(RanMonitor.Nokia.Airscale.Manager), :get_airscale_config)`
4. **Problemas de Caminho de Armazenamento**
    - Verifique se o diretório `priv/airscale_configs/` existe
    - Verifique se o RAN Monitor tem permissões de gravação
    - Revise os Logs do Aplicativo para erros de sistema de arquivos

Download Retorna Erro 404

Sintomas:

- Clicar em Baixar mostra "Arquivo de configuração não encontrado"
- O navegador mostra erro 404

Possíveis Causas:

1. **Desvio de Caminho do Arquivo**
    - Nomes de diretórios são sanitizados (minúsculas, caracteres especiais substituídos)
    - Verifique o nome real do diretório em `priv/airscale_configs/`
2. **Arquivo Excluído**
    - Verifique se o arquivo foi excluído manualmente do sistema de arquivos
    - Atualize a página do Arquivo de Configuração para atualizar a lista

3. **Problemas de Permissão**
    - Verifique se o processo do servidor web pode ler os arquivos de configuração
    - Verifique as permissões de arquivo no diretório de configuração

Resolução:

```
# Verifique se o diretório existe
ls -la priv/airscale_configs/

# Verifique se o arquivo existe
ls -la priv/airscale_configs/<device-name>/

# Corrija as permissões se necessário
chmod 755 priv/airscale_configs/
chmod 644 priv/airscale_configs/*/*.xml
```

Configuração Não Atualizando

Sintomas:

- Apenas `current.xml` existe, nenhuma nova versão
- Contagem de versões permanece em 1 mesmo após mudanças

Possíveis Causas:

1. **Configuração Não Mudou**
    - O sistema só cria versões quando o conteúdo muda
    - Revise os logs: `Configuração inalterada, nenhuma nova versão criada`
2. **Polling Não Está Rodando**
    - Verifique os Logs do Aplicativo para mensagens de polling
    - Verifique se o processo do Gerente está em execução
    - Verifique se há erros durante a recuperação da configuração

3. **Detecção de Mudança Muito Rigorosa**
    - Mudanças apenas de espaços em branco são ignoradas (por design)
    - Verifique se os valores reais dos parâmetros mudaram

Verificação:

```
# Verifique os logs para polling de configuração
grep "process_configuration" <log-file>

# Acione manualmente o pull de configuração
# No console IEx:
Kernel.send(Process.whereis(RanMonitor.Nokia.Airscale.Manager),
:get_airscale_config)
```

Melhores Práticas

Backups Regulares

Recomendação: Crie backups externos de configurações críticas

Exemplo de Script de Backup Automatizado:

```
#!/bin/bash
# backup-configs.sh - Backup diário de configuração para
armazenamento externo

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

# Crie diretório de backup datado
mkdir -p "$BACKUP_DIR/$DATE"

# Copie todas as configurações
rsync -av "$CONFIG_DIR/" "$BACKUP_DIR/$DATE/"

# Mantenha os últimos 30 dias
find "$BACKUP_DIR" -type d -mtime +30 -exec rm -rf {} +

echo "Backup concluído: $BACKUP_DIR/$DATE"
```

Agende com cron:

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

Documentação de Mudanças

Melhor Prática: Documente o motivo das mudanças nas configurações

Processo Sugerido:

1. Antes de fazer mudanças na configuração, documente o motivo
2. Crie um arquivo de log de mudanças ao lado das configurações
3. Inclua: Data, Dispositivo, Mudanças, Justificativa, Aprovador

Exemplo de Log de Mudanças:

```
# config_changes.log

2025-12-30 14:35:22 - ONS-Lab-Airscale
Alterado Por: John Smith
Razão: Aumentar potência da célula para melhorar cobertura no
Setor 1
Parâmetros: txPower alterado de 40dBm para 43dBm
Validado: Sim
Ativado: 2025-12-30 14:40:00
Resultado: Cobertura melhorada, nenhuma degradação observada

2025-12-28 09:10:45 - ONS-Lab-Airscale
Alterado Por: Jane Doe
Razão: Atualizar lista de células vizinhas após implantação de
novo site
Parâmetros: Células vizinhas 10, 11, 12 adicionadas
Validado: Sim
Ativado: 2025-12-28 09:15:00
Resultado: Transferências funcionando corretamente
```

Monitoramento de Armazenamento

Recomendação: Monitore o uso do disco periodicamente

Verifique o Uso de Armazenamento:

```
# Tamanho total do arquivo de configuração
du -sh priv/airscale_configs/

# Tamanho por dispositivo
du -sh priv/airscale_configs/*/

# Número de versões por dispositivo
find priv/airscale_configs/ -name "*.xml" | \
  sed 's|/[^/]*\.xml||' | uniq -c
```

Configure Alertas:

- Alerta se o tamanho total exceder o limite (ex: 500MB)
- Alerta se algum dispositivo tiver contagem de versões incomumente alta

- Alerta se o espaço em disco estiver abaixo de 10% livre

Integração com Gerenciamento de Configuração

O sistema de Arquivo de Configuração funciona em conjunto com a página de Gerenciamento de Configuração:

Integração de Fluxo de Trabalho

Baixar Configuração Atual:

- Use o Arquivo de Configuração para obter `current.xml`
- Ou use o botão "Baixar" na Gerência de Configuração (aciona pull imediato)

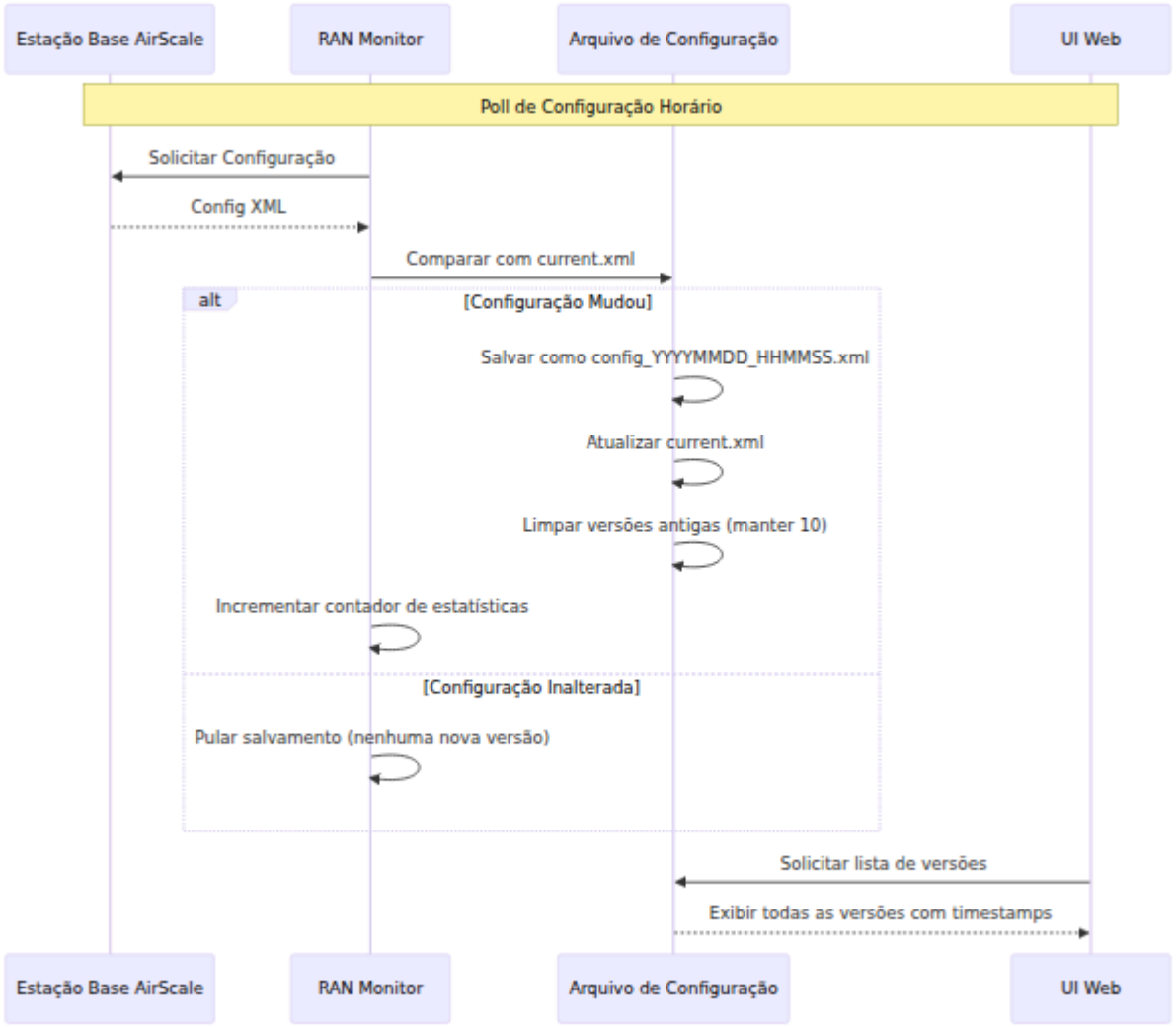
Fazer Upload de Configuração Modificada:

- Use a página de Gerenciamento de Configuração
- Fazer upload → Validar → Ativar fluxo de trabalho
- Nova versão aparece no Arquivo após o próximo polling

Processo de Reversão:

- Baixe a versão anterior do Arquivo
- Faça upload via Gerenciamento de Configuração
- Siga o fluxo de trabalho Validar → Ativar

Fluxo de Dados



Acesso à API

Embora o Arquivo de Configuração seja acessado principalmente via UI Web, as configurações também podem ser baixadas por meio de solicitações HTTP diretas.

Endpoints de Download

Configuração Atual:

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

Versão Específica:

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

Nota: O nome AirScale na URL deve corresponder ao nome do diretório sanitizado (minúsculas, sublinhados para caracteres especiais)

Acesso Programático

Listar Versões (do console IEx):

```
# Obter todas as versões para um dispositivo
RanMonitor.Nokia.Airscale.ConfigStorage.list_config_versions("ONS-
Lab-Airscale")

# Obter conteúdo da configuração atual
{:ok, xml} =
RanMonitor.Nokia.Airscale.ConfigStorage.get_current_config("ONS-
Lab-Airscale")

# Verificar contagem de versões
RanMonitor.Nokia.Airscale.ConfigStorage.count_versions("ONS-Lab-
Airscale")
# Retorna: 655

# Obter configuração de tamanho máximo de armazenamento
RanMonitor.Nokia.Airscale.ConfigStorage.max_storage_bytes()
# Retorna: 104857600 (100 MB em bytes)

# Obter uso atual de armazenamento
RanMonitor.Nokia.Airscale.ConfigStorage.get_storage_usage("ONS-
Lab-Airscale")
# Retorna: 99614055 (bytes)

# Obter estatísticas detalhadas de armazenamento
RanMonitor.Nokia.Airscale.ConfigStorage.get_storage_stats("ONS-
Lab-Airscale")
# Retorna: %{version_count: 655, total_size_bytes: 99614055, ...}

# Limpeza manual (manter abaixo de 50 MB)
RanMonitor.Nokia.Airscale.ConfigStorage.cleanup_old_versions("ONS-
Lab-Airscale", 50 * 1024 * 1024)
# Retorna: {:ok, 345, 50000000} - excluiu 345 versões, liberou
50MB

# Limpeza usando o padrão (100 MB)
RanMonitor.Nokia.Airscale.ConfigStorage.cleanup_old_versions("ONS-
Lab-Airscale")
# Retorna: {:ok, 0, 0} - nenhuma limpeza necessária se estiver
abaixo do limite
```

Veja Também

- **Guia da UI Web** - Referência completa do painel de controle
- **Guia de Configuração AirScale** - Configuração da estação base
- **Guia de Operações Comuns** - Tarefas de gerenciamento do dia a dia
- **Guia de Política de Retenção de Dados** - Gerenciamento de armazenamento

Guia de Push de Configuração

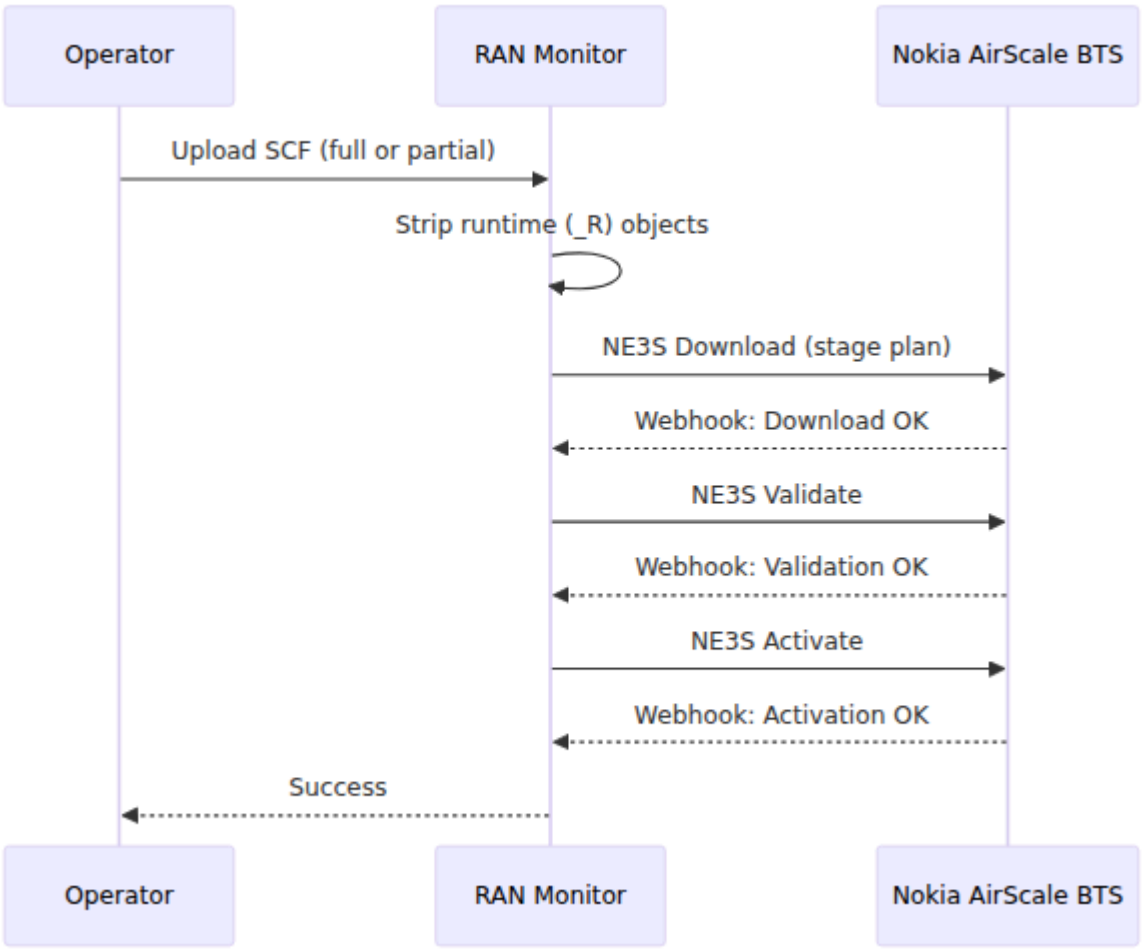
Enviando alterações de configuração para estações base Nokia AirScale via RAN Monitor

---

Visão Geral

O RAN Monitor pode enviar alterações de configuração para estações base Nokia AirScale usando o protocolo NE3S Bulk Operations. A configuração é expressa como um SCF (Site Configuration File) no formato XML RAML 2.1. O push segue um processo de três etapas na BTS: **download** (preparar o plano), **validar** (verificar erros) e **ativar** (aplicar alterações). O RAN Monitor gerencia automaticamente todas as três etapas.

Um push de configuração pode ser um **SCF completo** contendo todos os objetos gerenciados na BTS, ou uma **atualização parcial** direcionando apenas os parâmetros específicos que você deseja alterar. Atualizações parciais são a abordagem recomendada para mudanças operacionais porque são mais rápidas, de menor risco e evitam a reinicialização desnecessária da BTS.



Formato XML do SCF

Todos os arquivos de configuração usam o esquema XML RAML 2.1. A estrutura básica é:

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

<!-- Objetos gerenciados vão aqui -->

</cmData>
</raml>
```

Cada objeto gerenciado é representado como um elemento `<managedObject>`:

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

Atributos Chave

Atributo	Descrição
`class`	Identificador da classe de objeto Nokia (por exemplo, `NOKLTE:LNCEL`, `com.nokia.srbts.tnl:IPIF`)
`distName`	Nome distinto — o caminho do objeto na árvore de objetos gerenciados
`operation`	`create` para push de SCF completo, `update` para alterações parciais

Formato do Nome Distinto

O `distName` segue um caminho hierárquico:

```
MRBTS-{bts_id}                                  # Raiz da BTS
MRBTS-{bts_id}/LNBTS-{bts_id}                   # LTE eNodeB
MRBTS-{bts_id}/LNBTS-{bts_id}/LNCEL-{cell_id}   # Célula LTE
MRBTS-{bts_id}/GNBTS-{gsm_id}                   # BTS GSM
MRBTS-{bts_id}/GNBTS-{gsm_id}/GNCEL-{cell_id}   # Célula GSM
MRBTS-{bts_id}/MNL-1/MNLENT-1/PMCADM-1          # Administração
de PM
MRBTS-{bts_id}/EQM-1/APEQM-1                    # Gestão de
Equipamentos
```

Push Completo de SCF vs Atualização Parcial

Push Completo de SCF

Um SCF completo contém todos os objetos gerenciados na BTS (tipicamente 100-200 objetos). Ele usa `operation="create"` em cada objeto. Isso substitui toda a configuração.

Quando usar: Provisionamento inicial, recuperação de desastres ou restauração de uma configuração conhecida a partir do backup.

Risco: Alto. Um SCF completo normalmente contém objetos de transporte/IP que irão acionar uma reinicialização da BTS, levando o site offline por 3-5 minutos.

Atualização Parcial

Um SCF parcial contém apenas os objetos e parâmetros que você deseja alterar. Ele usa `operation="update"` e inclui apenas os elementos `<p>` específicos que estão sendo modificados.

Quando usar: Alterações de parâmetros operacionais, ajuste de células, ativação de recursos, configuração de PM.

Risco: Baixo a nenhum, desde que você evite classes de objetos que acionam reinicializações.

Principais Diferenças

	Push Completo de SCF	Atualização Parcial
Atributo de operação	`operation="create"`	`operation="update"`
Objetos incluídos	Todos os objetos gerenciados	Apenas objetos que estão sendo alterados
Parâmetros incluídos	Todos os parâmetros por objeto	Apenas parâmetros que estão sendo alterados
Risco de reinicialização	Quase certo	Depende das classes de objetos
Caso de uso típico	Provisionamento inicial	Alterações do dia a dia

---

Impacto da Reinicialização por Classe de Objeto

Objetos Que Acionam uma Reinicialização da BTS

Alterar qualquer uma dessas classes de objetos fará com que a BTS reinicie. O site ficará **offline por 3-5 minutos** durante a reinicialização.

Categoria	Classes de Objetos
Transporte / IP	`TNL`, `ETHIF`, `ETHLK`, `IPIF`, `IPADDRESSV4`, `IPRT`, `IPRTV6`, `VLANIF`, `L2SWI`, `BRGPRT`, `IBRGPRT`, `IPNO`, `ETHSVC`, `TNLSVC`, `IPSECC`, `FIREWALL`
Sistema / Hardware	`MRBTS`, `SMOD`, `BBMOD`
Plano de Gerenciamento	`MPLANENW`, `CLOCK`, `SYNC`, `NTP`
Segurança / Certificados	`SECADM`, `CERTH`, `CERTHENT`, `CMP`, `CMPECDSA`, `CMPFH`

Objetos Seguros para Alterar Sem Reinicialização

Essas classes de objetos podem ser atualizadas sem acionar uma reinicialização. Algumas alterações de parâmetros de rádio causarão uma breve interrupção da célula (segundos) enquanto a célula é reconfigurada.

Categoria	Classes de Objetos	Notas
Rádio LTE	`LNCEL`, `LNCEL_FDD`, `LNBTS`, `LNBTS_FDD`	Alguns parâmetros causam breve reconfiguração da célula
Rádio GSM	`GNBTS`, `GNCEL`, `GNBCF`	
Monitoramento de Desempenho	`PMCADM`, `PMMNL`, `PMCCP`, `PMPLM`, `PMRNL`, `PMTNLINT`	
Recursos	`FEATCADM`, `FEATGADM`, `FEATLADM`	
ANR / Relações de Vizinhança	`ANR`, `ANRPRL`	
RRC / DRX	`DRX`, `SDRX`, `SIB`	
S1 / Transporte	`SCTP`, `TRSNW`, `LNMME`	
Outros	`ALARMSUPP`, `REDRT`, `CAGENB`, `CADPR`, `QOS`	

Objetos de Tempo de Execução (Somente Leitura)

Classes de objetos que terminam em `_R` são **objetos de tempo de execução** gerados automaticamente pela BTS. Eles não podem ser enviados e são removidos automaticamente pelo RAN Monitor antes do upload. Exemplos: `EQM_R`, `APEQM_R`, `LNCEL_R`, `TNL_R`, `ETHIF_R`.

Exemplos de Atualização Parcial

Mudando o Nome do eNB

Sem reinicialização. Entra em vigor imediatamente.

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

Mudando o Nome da Célula

Sem reinicialização. Entra em vigor imediatamente.

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

Mudando o ID Físico da Célula

Sem reinicialização. A célula será brevemente reconfigurada.

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

Mudando EARFCN e Largura de Banda

Sem reinicialização, mas a célula ficará **brevemente indisponível** (segundos) enquanto se reconfigura para a nova frequência.

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

Mudando o Intervalo de Coleta de PM

Sem reinicialização. Entra em vigor no próximo ciclo de coleta.

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

Mudando Múltiplos Parâmetros em Objetos

Múltiplos objetos podem ser incluídos em um único SCF. Este exemplo muda o nome do eNB e um parâmetro da célula em um único push:

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

Mudando um Endereço IP (Aciona Reinicialização)

Alterar objetos de transporte/IP **irá reiniciar a BTS**. O site ficará offline por 3-5 minutos.

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

Enviando Configuração via a Interface Web

1. Navegue até **Status da BTS** no painel de controle
2. Clique em **Config Ops** no dispositivo alvo
3. Selecione seu arquivo XML SCF parcial (arraste e solte ou navegue)
4. Clique em **Enviar Configuração para o Dispositivo**
5. O RAN Monitor remove automaticamente os objetos de tempo de execução, em seguida, realiza download, validação e ativação
6. Monitore a mensagem de resultado para sucesso ou erros

Para mais controle, expanda a seção **Avançado: Passos manuais de download/validação/ativação** para preparar um plano sem ativá-lo, em seguida, valide e ative separadamente.

Enviando Configuração via API

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

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

O caminho `config_file` deve existir no servidor RAN Monitor. Copie o arquivo para o servidor primeiro, se necessário.

Resposta em caso de sucesso:

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

Resposta em caso de falha:

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

Parâmetros da API

Parâmetro	Tipo	Requerido	Padrão	Descrição
`airscale_name`	String	Sim	-	Nome do dispositivo registrado no RAN Monitor
`config_file`	String	Sim	-	Caminho absoluto para o arquivo SCF XML no servidor RAN Monitor

---

Melhores Práticas

1. **Sempre faça o download de um backup primeiro.** Use o botão "Download Config" da Interface Web ou a API para salvar a configuração atual antes de fazer alterações.

2. **Use atualizações parciais para alterações operacionais.** Inclua apenas os objetos e parâmetros que você precisa alterar. Isso minimiza o risco e evita reinicializações.

3. **Use `operation="update"` para alterações parciais.** O atributo `operation="create"` é para substituições completas de SCF e irá sobrescrever todos os parâmetros no objeto.

4. **Verifique a classe do objeto antes de enviar.** Se seu SCF incluir qualquer objeto de transporte, sistema, gerenciamento ou segurança, a BTS irá reiniciar. Planeje uma janela de manutenção de acordo.

5. **Verifique se o `distName` corresponde à sua BTS alvo.** O ID MRBTS, ID LNBTS e IDs de células devem corresponder ao dispositivo alvo. Envie o `distName` errado e a BTS rejeitará a configuração com um erro de validação.

6. **Uma alteração por vez para parâmetros críticos.** Ao alterar parâmetros de rádio que afetam o serviço (EARFCN, largura de banda, PCI), faça uma alteração por push para que você possa isolar quaisquer problemas.

Solução de Problemas

Validação Falhou: Objeto Duplicado

Sintomas: O push falha com `Duplicated object MRBTS-256/EQM_R-1`

Causa: O SCF contém objetos de tempo de execução (`_R`). Esses objetos são gerados automaticamente pela BTS e não podem ser enviados.

Resolução: O RAN Monitor remove automaticamente os objetos `_R`. Se você ver esse erro, verifique se está enviando através do RAN Monitor e não diretamente para a BTS.

Ativação Falhou: Conflito de Operação

Sintomas: O push falha com `Operation could not execute because of operation conflict, RequestOperationType = {activate}, OngoingOperationType = {validate}`

Causa: A ativação foi enviada antes que a validação fosse concluída. A BTS processa cada etapa de forma assíncrona.

Resolução: O RAN Monitor aguarda a conclusão assíncrona entre as etapas automaticamente. Se isso ocorrer, tente novamente o push. Se persistir, verifique se nenhum outro sistema de gerenciamento (NetAct, WebLM) está simultaneamente enviando configuração para a mesma BTS.

BTS Reiniciou Inesperadamente

Sintomas: A BTS fica offline após o push de configuração, o ping falha por 3-5 minutos.

Causa: A configuração enviada incluía objetos de transporte/IP, sistema ou segurança que acionam uma reinicialização.

Resolução: A BTS voltará sozinha após 3-5 minutos. Para evitar isso no futuro, use uma atualização parcial que inclua apenas os parâmetros específicos que você deseja alterar, evitando as classes de objetos que acionam reinicializações listadas acima.

Arquivo do Plano Não Encontrado

Sintomas: A ativação falha com `Processing of attachment detail property file failed in agent`

Causa: Erro interno da BTS ao ler o arquivo do plano preparado. Pode ocorrer quando várias operações de configuração se sobrepõem.

Resolução: Aguarde 30 segundos e tente novamente o push. Se o erro persistir, reinicie a sessão NE3S usando o botão "Force Reconnect" na Interface Web antes de tentar novamente.

Guia de Política de Retenção de Dados

Visão Geral

O aplicativo RAN Monitor agora inclui um sistema abrangente de **Política de Retenção de Dados** que permite gerenciar por quanto tempo métricas de desempenho, dados de configuração e registros de alarmes são armazenados no InfluxDB. Este guia cobre tudo o que você precisa saber sobre como gerenciar a retenção de dados.

□ Início Rápido

Acessando o Painel de Controle da Política de Retenção

1. Navegue até o **Painel de Controle**: `https://localhost:9443`
2. Clique em **Retenção de Dados** no menu de navegação
3. Visualize e gerencie as configurações de retenção para todos os eNodeBs configurados

Definindo um Período de Retenção Personalizado

1. Encontre o eNodeB na lista
2. Atualize o campo "Período de Retenção" (em horas)
3. A configuração é salva imediatamente
4. Retorna ao padrão global se deixado em branco

Limpando Dados Antigos

1. Clique no botão **Limpar Dados Antigos** para remover registros mais antigos que o período de retenção
2. Ou clique em **Limpar Todos os Dados** para excluir todos os registros desse eNodeB (use com cautela!)

Captura de Tela

O painel de retenção de dados mostrando as configurações de retenção e contagens de registros para cada eNodeB

Recursos

Configurações de Retenção Global

- **Período de Retenção Padrão**: 720 horas (30 dias)

- **Configurável**: Alterar em `config/config.exs`
- **Fallback**: Aplicado a todos os eNodeBs sem configurações personalizadas

Retenção por eNodeB

- **Substituir Global**: Defina retenção personalizada para eNodeBs específicos
- **Armazenado no Banco de Dados**: Persistido na tabela `airscales`
- **Em Tempo Real**: Tem efeito imediato

Limpeza Automática

- **Agendado**: Executa automaticamente a cada hora
- **Trabalhador em Segundo Plano**: `RanMonitor.Data.RetentionCleanupWorker`
- **Por eNodeB**: Respeita as configurações de retenção individuais
- **Registrado**: Todas as limpezas são registradas para trilha de auditoria

Visibilidade de Dados

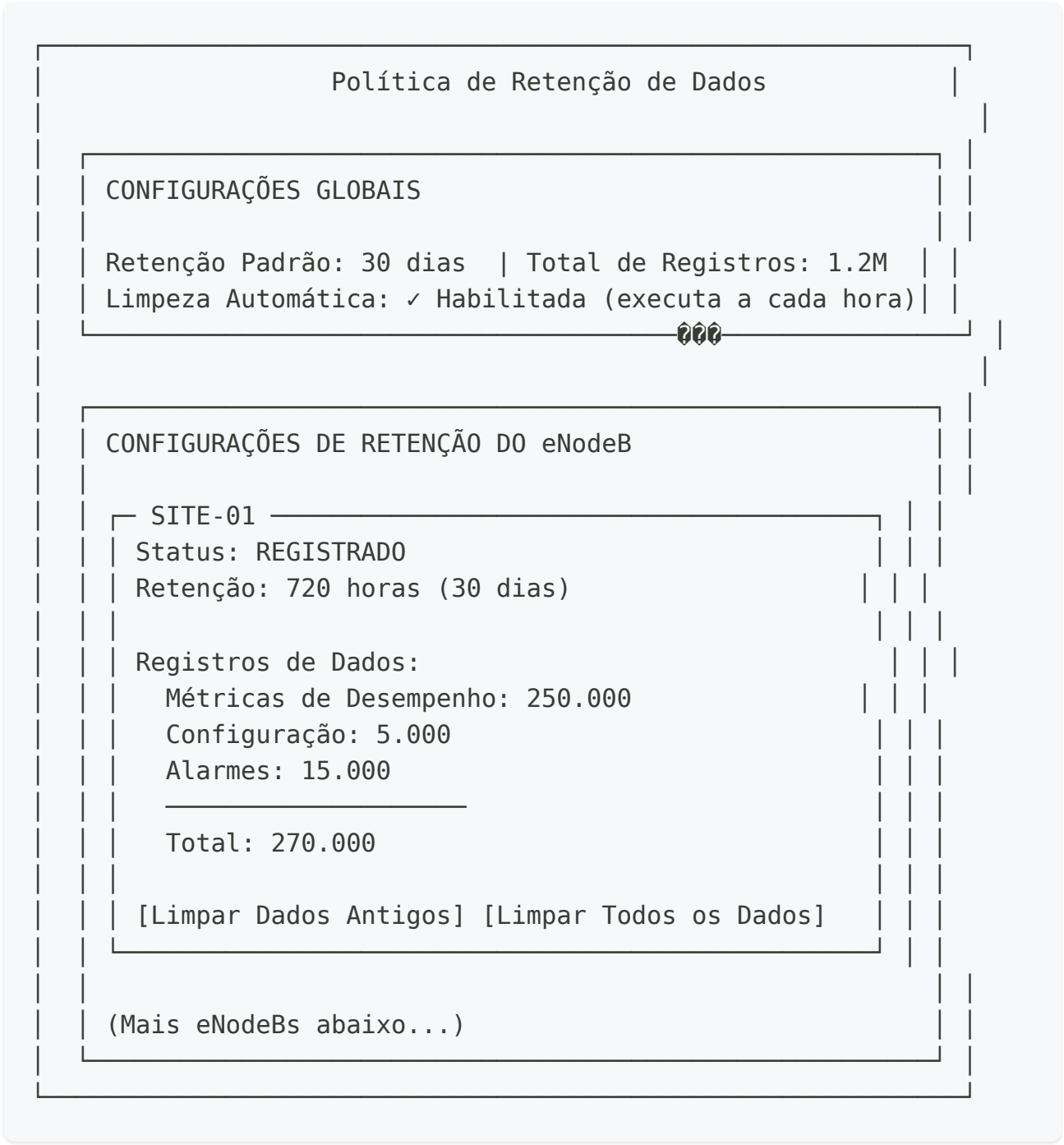
- **Contagem de Registros**: Veja quantos registros por tipo de medição:
  - Métricas de Desempenho
  - Configuração
  - Alarmes
- **Resumo Total**: Visualize o total de registros por eNodeB
- **Em Tempo Real**: Atualizado na atualização da página

🖥️ Interface do Usuário

Layout do Painel

O painel de retenção de dados mostrando configurações globais, períodos de retenção por eNodeB e contagens de registros

Visão Geral do Layout:



Indicadores de Status

- **Verde (✓)**: eNodeB registrado e ativo
- **Vermelho (✗)**: eNodeB pendente ou não registrado
- **Desativado**: Não é possível modificar configurações para eNodeBs não registrados

Botões de Ação

Botão	Ação	Efeito
Limpar Dados Antigos	Remover registros antigos	Exclui registros mais antigos que o período de retenção
Limpar Todos os Dados	Limpeza completa	Exclui TODOS os registros (⚠ use com cautela!)
Atualizar	Atualizar exibição	Rebusca contagens de registros e configurações

---

⚙ Configuração

Configuração Global de Retenção

Edite `config/config.exs`:

```
config :ran_monitor,
  ecto_repos: [RanMonitor.Repo],
  generators: [context_app: :ran_monitor],
  data_retention_hours: 720  # 30 dias, ajuste conforme necessário
```

Valores de Tempo Suportados

Período	Horas	Dias	Recomendado Para
1 hora	1	0.04	Apenas para testes
1 dia	24	1	Métricas de curto prazo
7 dias	168	7	Relatórios semanais
14 dias	336	14	Relatórios quinzenais
30 dias	720	30	Relatórios mensais (padrão)
90 dias	2160	90	Tendências de longo prazo
180 dias	4320	180	Relatórios semestrais
1 ano	8760	365	Relatórios anuais

Variáveis de Ambiente

Opcionalmente, substitua em tempo de execução:

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

□ Como Funciona

Fluxo de Retenção de Dados

```
1. INSERÇÃO DE DADOS
   ├─ Métricas de Desempenho → InfluxDB
   ├─ Dados de Configuração → InfluxDB
   └─ Alarmes → InfluxDB

2. LIMPEZA AUTOMÁTICA (Horária)
   ├─ RetentionCleanupWorker é acionado
   ├─ Para cada eNodeB:
   │  ├─ Obter retenção efetiva (por eNodeB ou global)
   │  ├─ Calcular timestamp de corte
   │  └─ Excluir registros mais antigos que o corte
   └─ Registrar resultados

3. LIMPEZA MANUAL (Sob Demanda)
   ├─ Usuário clica no botão na UI
   ├─ Política de retenção aplicada
   ├─ Registros excluídos imediatamente
   └─ Notificação de sucesso/erro exibida

4. MONITORAMENTO
   └─ Contagens de registros exibidas na UI
```

Lógica de Retenção

Retenção Efetiva por eNodeB:

```
effective_retention = case airscale.retention_hours do
  nil -> Config.data_retention_hours()      # Usa global (720h)
  hours -> hours                             # Usa valor
personalizado por eNodeB
end
```

Exemplo:

- Padrão global: 720 horas (30 dias)

- eNodeB "SITE-01" personalizado: 168 horas (7 dias)
- eNodeB "SITE-02" personalizado: nil → usa global 720 horas

Processo de Limpeza

```
Timestamp de Corte = Agora - (retention_hours * 3600 segundos)

Exemplo com retenção de 30 dias:
├─ Atual: 2025-12-11 10:00:00
├─ Retenção: 720 horas (30 dias)
├─ Corte: 2025-11-11 10:00:00
└─ Excluir todos os registros com timestamp < corte
```

□ Monitoramento & Registro

Entradas de Log

O sistema registra todas as atividades de retenção. Procure por:

```
[RetentionCleanupWorker] Iniciando trabalhador de limpeza de
retenção
[RetentionCleanupWorker] Limpando dados para SITE-01 (retenção:
720h)
[RetentionCleanupWorker] Excluídos 15.000 registros para SITE-01
[RetentionCleanupWorker] Ciclo de limpeza completo: 5 bem-
sucedidos, 0 falhados, 75.000 total excluídos
```

Monitorando Contagens de Registros

Visibilidade em Tempo Real:

1. Abra o painel de retenção de dados
2. Veja as contagens atuais de registros por medição por eNodeB
3. Clique em "Atualizar" para atualizar as contagens

Rastreamento Histórico:

- Verifique os logs do aplicativo para resumos de limpeza
- Monitore o uso de disco do InfluxDB ao longo do tempo
- Configure alertas com base no crescimento da contagem de registros

---

Uso Avançado

Acesso Programático

Use o serviço de política de retenção em seu código:

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

# Obter retenção efetiva para um eNodeB
airscale = Nokia.get_airscale!(1)
hours = RetentionPolicy.get_retention_hours(airscale)
# => 720 (ou valor personalizado se definido)

# Obter contagens de registros para um eNodeB
counts = RetentionPolicy.get_record_counts("SITE-01")
# => %{"PerformanceMetrics" => 250000, "Configuration" => 5000,
"Alarms" => 15000}

# Obter total de registros
total = RetentionPolicy.get_total_record_count("SITE-01")
# => 270000

# Excluir registros antigos manualmente
{:ok, deleted_count} = RetentionPolicy.delete_old_records("SITE-
01", 720)
# => {:ok, 50000}  (50k registros excluídos)

# Limpar todos os registros para um eNodeB
{:ok, deleted_count} = RetentionPolicy.clear_all_records("SITE-
01")
# => {:ok, 270000}  (todos os 270k registros excluídos)
```

Ajustando o Intervalo de Limpeza

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

```
# Mudar de 1 hora (3600000ms) para 30 minutos (1800000ms)
@cleanup_interval_ms 1800000  # 30 minutos
```

Então recompile:

```
mix compile
```

Consultas em Nível de Banco de Dados

Visualize as configurações de retenção diretamente:

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

Atualize a retenção via banco de dados:

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

□ Melhores Práticas

Seleção do Período de Retenção

Curto prazo (< 7 dias)

- Use para: Testes, ambientes de homologação
- Não recomendado para: Produção
- Risco: Pode excluir dados históricos importantes

Padrão (7-30 dias)

- Use para: Implantações em produção com armazenamento típico
- Melhor para: A maioria dos casos de uso
- Equilíbrio: Boa história com armazenamento gerenciável

Longo prazo (> 30 dias)

- Use para: Análise de tendências, requisitos de conformidade
- Custo: Requisitos de armazenamento mais altos
- Benefício: Dados históricos estendidos

Recomendado por Caso de Uso

Caso de Uso	Retenção	Motivo
Relatórios diários	7-14 dias	Ciclos de revisão semanais
Relatórios semanais	30-60 dias	Resumos mensais
Relatórios mensais	90 dias	Análise trimestral
Análise de tendências	180-365 dias	Padrões de longo prazo
Conformidade	Conforme necessário	Legal/regulatório

Considerações de Armazenamento

Estime as necessidades de armazenamento:

- 1000 registros ≈ 1-5 KB (dependendo do tipo de medição)
- 1 milhão de registros ≈ 1-5 GB
- Período de retenção × taxa de coleta = armazenamento total

Monitore o crescimento com:

```
# Verifique o tamanho do bucket do InfluxDB
influx bucket list

# Ou verifique o uso do disco
df -h /path/to/influxdb/data
```

Segurança & Conformidade

Privacidade de Dados

- **Sem criptografia** em repouso por padrão
- **Acesso à rede** controlado via segurança do InfluxDB
- **Logs de acesso** disponíveis nos logs do aplicativo

Conformidade

- **Trilha de auditoria**: Todas as limpezas registradas com timestamp
- **Integridade dos dados**: Exclusões suaves, sem limpezas duras no nível do aplicativo
- **Prova de retenção**: Logs mostram o que foi retido/excluído

Recomendações

1. **Ative a autenticação do InfluxDB** para produção
2. **Monitore os logs de limpeza** regularmente
3. **Defina retenção com cuidado** para equilibrar conformidade e armazenamento
4. **Faça backup antes de operações em massa** se dados críticos
5. **Teste políticas de retenção** em homologação primeiro

🔧 Solução de Problemas

Problema: Limpeza Não Executada

Sintomas:

- Registros mais antigos que o período de retenção ainda existem
- Sem entradas de log de limpeza

Soluções:

1. Verifique se o aplicativo está em execução: `ps aux | grep mix`
2. Verifique se o `RetentionCleanupWorker` foi iniciado:
   - Verifique os logs por `[RetentionCleanupWorker] Iniciando`
3. Verifique a conexão com o InfluxDB:
   - Visite a página de Status do InfluxDB: `https://localhost:9443/nokia/influx`
4. Verifique se as configura��ões de retenção estão configuradas:
   - Verifique `config/config.exs` para `data_retention_hours`

Problema: Limpeza Manual Falhou

Sintomas:

- Mensagem de erro ao clicar em "Limpar Dados Antigos"
- Registros não excluídos

Soluções:

1. Verifique se o InfluxDB é acessível:
   - Teste a conexão no painel
2. Verifique se as contagens de registros estão precisas:
   - Clique em "Atualizar" para atualizar
3. Verifique os logs do aplicativo em busca de erros:
   - Procure por entradas de erro `[RetentionPolicy]`
4. Verifique se o eNodeB está registrado:
   - Verifique a página de Status do BTS

Problema: Alto Uso de Memória Após Limpeza

Sintomas:

- O aplicativo fica lento após a limpeza
- Uso de memória aumenta

Soluções:

1. Isso é normal para exclusões grandes
2. Permita 5-10 minutos para a memória se normalizar
3. Considere reduzir a frequência de limpeza:
   - Mude `@cleanup_interval_ms` (padrão 1 hora)
4. Ou reduza o período de retenção para eNodeBs afetados

Problema: Contagens de Registros Incorretas

Sintomas:

- Contagens de registros não correspondem à UI do InfluxDB
- "Limpar Dados Antigos" mostra números diferentes

Soluções:

1. Clique em "Atualizar" para forçar a atualização
2. Verifique a consulta do InfluxDB:
   - Pode levar tempo para refletir exclusões recentes
3. Espere um minuto e tente novamente:
   - O InfluxDB pode estar processando operações de exclusão
4. Verifique se o nome do eNodeB corresponde exatamente:
   - Comparação sensível a maiúsculas e minúsculas

Documentação Relacionada

- **Guia de Operações** - Visão geral operacional completa

- **Guia da Interface Web** - Referência e recursos do painel de controle
- **Guia de Introdução** - Guia de início rápido
- **Guia de Operações Comuns** - Tarefas de gerenciamento do dia a dia
- **Guia de Integração com Grafana** - Análises e painéis

Pontos de Acesso

- **Painel de Retenção de Dados**: `https://localhost:9443/nokia/retention`
- **Status do BTS**: `https://localhost:9443/nokia/status`
- **Status do InfluxDB**: `https://localhost:9443/nokia/influx`
- **Logs ao Vivo**: `https://localhost:9443/nokia/logs`

Perguntas Frequentes

Q: A limpeza excluirá dados ativos?

A: Não. Apenas registros mais antigos que o período de retenção são excluídos. Dados que estão sendo coletados atualmente nunca são afetados.

Q: Posso definir retenção diferente para diferentes eNodeBs?

A: Sim! Cada eNodeB pode ter sua própria configuração de retenção. Se não for definido, usa o padrão global.

Q: Com que frequência a limpeza automática é executada?

A: A cada hora por padrão. Ajuste `@cleanup_interval_ms` no trabalhador se necessário.

Q: O que acontece se eu limpar todos os dados?

A: Todos os registros (Métricas de Desempenho, Configuração, Alarmes) para esse eNodeB são excluídos permanentemente. Isso não pode ser desfeito.

Q: A limpeza pode afetar a coleta de dados?

A: Não. A limpeza e a coleta de dados são independentes. Novos dados continuarão sendo gravados enquanto dados antigos são excluídos.

Q: Quanto tempo a limpeza leva?

A: Depende da contagem de registros:

- Pequeno (< 100k): < 1 segundo
- Médio (100k-1M): 1-10 segundos
- Grande (> 1M): 10-60+ segundos

Q: Posso excluir manualmente registros específicos?

A: Não via UI. Apenas limpeza completa ou limpeza total disponível. Para exclusões granulares, use o CLI ou API do InfluxDB diretamente.

Q: E se o InfluxDB estiver indisponível?

A: A limpeza falhará silenciosamente e tentará novamente na próxima hora. A coleta de dados continua sem ser afetada.

Q: A limpeza afeta o desempenho?

A: Impacto menor durante a limpeza (segundos a minutos dependendo do tamanho dos dados). O intervalo de uma hora foi escolhido para minimizar o impacto.

🔧 Detalhes da Implementação

Arquivos Modificados

Arquivo	Alterações
`lib/ran_monitor/database/nokia/airscale.ex`	Adicionado campo `retention_hours`
`lib/ran_monitor/config/config.ex`	Adicionado getter `data_retention_hours()`
`config/config.exs`	Adicionada configuração de retenção global e rota de página
`lib/ran_monitor/application.ex`	Adicionado trabalhador de limpeza à árvore de supervisão

Arquivos Criados

Arquivo
`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.`

Funções Principais

Módulo RetentionPolicy:

- `get_retention_hours(airscale)` - Obter retenção efetiva
- `get_record_counts(airscale_name)` - Buscar contagens de registros
- `get_total_record_count(airscale_name)` - Contagem total
- `delete_old_records(name, hours)` - Limpar registros antigos
- `clear_all_records(name)` - Limpeza completa

GenServer RetentionCleanupWorker:

- `start_link(opts)` - Iniciar trabalhador de limpeza
- `init(:ok)` - Inicializar trabalhador
- `handle_info(:cleanup, state)` - Executar ciclo de limpeza

🚀 Começando

Configuração (Uma Vez)

1. **Execute a migração:**

   ```
   mix ecto.migrate
   ```

2. **Reinicie o aplicativo:**

   ```
   mix phx.server
   ```

3. **Verifique a instalação:**

   - Navegue até `https://localhost:9443/nokia/retention`
   - Deve ver o painel de retenção de dados

Primeiro Uso

1. **Verifique as configurações atuais:**
    - Veja a retenção global (padrão: 720 horas)
    - Veja as configurações de retenção por eNodeB
2. **Personalize se necessário:**
    - Atualize a retenção global em `config/config.exs`
    - Ou defina por eNodeB via UI
3. **Monitore a limpeza:**
    - Observe os logs para entradas `[RetentionCleanupWorker]`
    - Verifique se as contagens de registros diminuem ao longo do tempo

---

Suporte

Precisa de Ajuda?

1. **Verifique os logs:** Procure por entradas `[RetentionPolicy]` ou `[RetentionCleanupWorker]`
2. **Revise este guia:** A maioria dos problemas está coberta na seção de Solução de Problemas
3. **Verifique outros docs:** Consulte os links de documentação relacionada acima
4. **Verifique a configuração:** Certifique-se de que a migração foi executada e o trabalhador foi iniciado

Relatando Problemas

Inclua:

- Mensagem de erro da UI ou logs
- Nome do eNodeB afetado

- Configurações de retenção atuais
- Contagens de registros antes/depois
- Passos para reproduzir

Recursos de Aprendizado

Conceitos Relacionados

- **InfluxDB v2.x**: Banco de dados de séries temporais com políticas de retenção
- **Política de Retenção**: Quanto tempo os dados são mantidos
- **Limpeza**: Exclusão automatizada de dados antigos
- **Tipos de Medição**: Métricas de Desempenho, Configuração, Alarmes

Recursos Externos

- Documentação do InfluxDB
- Guia do GenServer do Elixir
- Phoenix LiveView

Guia de Comissionamento DHCP da Nokia AirScale

Configurando DHCP para Onboarding Automático da Estação Base

Índice

Visão Geral

As estações base Nokia AirScale podem descobrir e registrar automaticamente com o RAN Monitor através do DHCP. Quando a estação base é ligada, ela envia uma solicitação DHCP contendo sua identidade. O servidor DHCP responde com a configuração IP da estação base e o endereço do servidor RAN Monitor codificado na **Opção DHCP 43** (Informações Específicas do Fornecedor).

Isso elimina a necessidade de configurar manualmente cada estaç��o base com o endereço do servidor de gerenciamento. A estação base completa o handshake DHCP e, em seguida, inicia uma conexão de descoberta do agente NE3S com o IP do RAN Monitor fornecido na resposta DHCP.

Quem Deve Usar Este Guia

Importante: Toda a configuração da estação base Nokia AirScale é **realizada pela Omnitouch** como parte da implantação inicial e suporte contínuo. Este guia é fornecido para:

- **Usuários avançados** que desejam entender o processo de comissionamento DHCP
- **Implantações autogeridas** onde os clientes gerenciam sua própria infraestrutura DHCP
- **Solução de problemas** de questões de autoconexão baseadas em DHCP

Se você é um cliente gerenciado pela Omnitouch, entre em contato com o suporte da Omnitouch para o comissionamento da estação base e configuração do DHCP.

Pré-requisitos

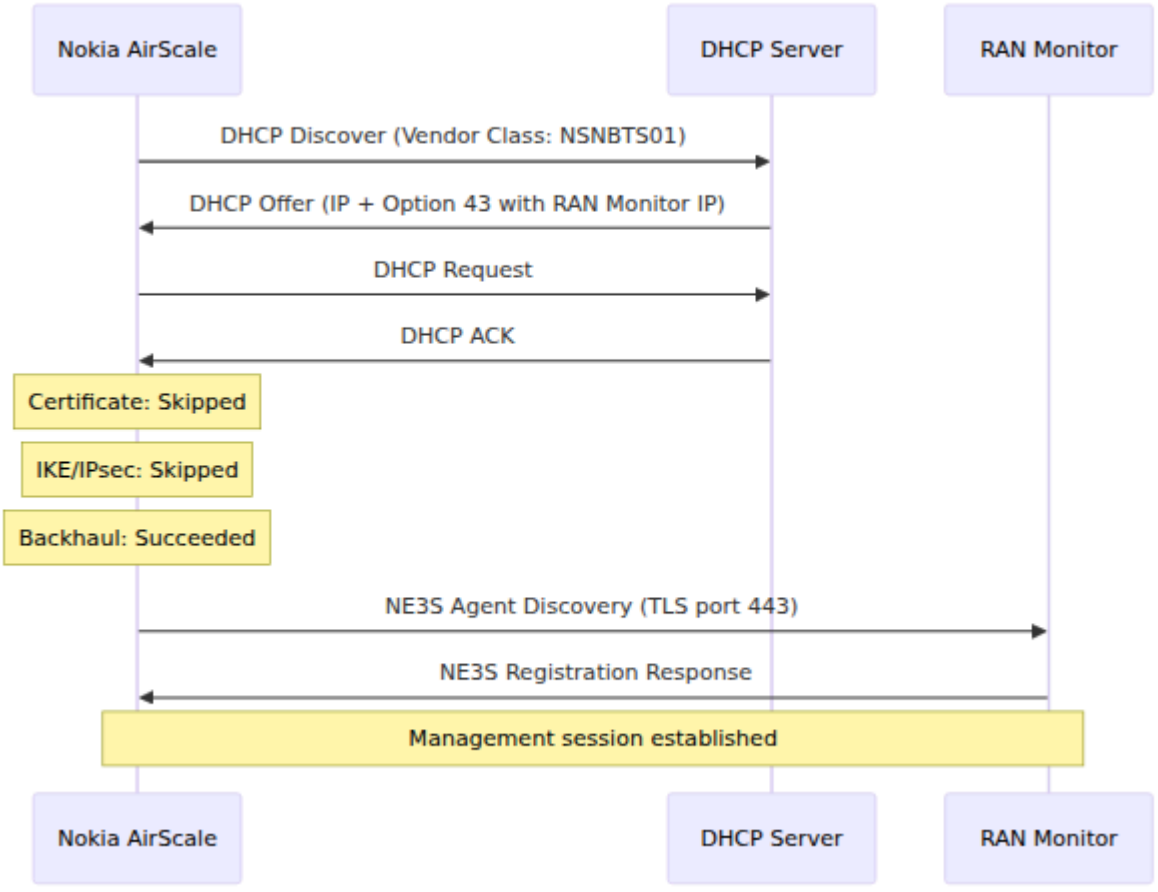
Antes de configurar o comissionamento DHCP, certifique-se de ter:

- **Servidor DHCP** — Um servidor DHCP na rede de gerenciamento da estação base (MikroTik, ISC DHCP, dnsmasq, etc.)
- **RAN Monitor** — Uma instância do RAN Monitor em execução acessível a partir da rede da estação base
- **Conectividade de Rede** — Conectividade de camada 2 entre a porta OAM da estação base e o servidor DHCP

Informações Necessárias:

Parâmetro	Descrição	Exemplo
IP do RAN Monitor	Endereço IP onde o RAN Monitor está em execução	10.179.2.139
Sub-rede de Gerenciamento	Sub-rede para interfaces de gerenciamento da estação base	10.7.15.64/26
IP do Gateway	Gateway padrão para a sub-rede de gerenciamento	10.7.15.65
Servidor DNS	IP do servidor DNS	10.7.15.65

Como Funciona



Fluxo de Autoconexão

A estação base avança por essas fases após receber um lease DHCP:

Fase	Status	Descrição
DHCP	Sucedido	Endereço IP e endereço do RAN Monitor obtidos
Certificado	Ignorado	Nenhum registro de certificado necessário (rede privada)
IKE	Ignorado	Nenhum túnel IPsec necessário (rede privada)
Backhaul	Sucedido	Conectividade de rede confirmada
Identificação	Solicitado	Descoberta do agente NE3S iniciada para o RAN Monitor

---

Configuração do Servidor DHCP

Codificação da Opção 43

As estações base Nokia AirScale requerem que a Opção 43 do DHCP (Informações Específicas do Fornecedor) contenha o endereço IP do RAN Monitor. A estação base **rejeita** Ofertas DHCP sem uma Opção 43 corretamente codificada.

Gerando o Valor da Opção 43

Execute este script com seu IP do RAN Monitor para gerar o valor hexadecimal necessário para o servidor DHCP:

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

Exemplo para `10.179.2.139`:

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

Use a saída como o `value` na configuração do servidor DHCP abaixo.

MikroTik RouterOS 7

```
/ip dhcp-server option
add code=43 name=nokia-oms
value=0x01040ab3028b04040ab3028b080c31302e3137392e322e3133390904706b0

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

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

Parâmetros:

Linha	Propósito
`code=43`	Opção DHCP 43 (Informações Específicas do Fornecedor)
`value=0x...`	Payload da Opção 43 codificado em hexadecimal contendo o IP do RAN Monitor
`dhcp-option-set=nokia-set`	Anexa o conjunto de opções à rede DHCP

dnsmasq

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

ISC DHCP

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

Configuração da Estação Base

Modo de Autoconexão

A estação base deve ser configurada para o modo **Rede privada com DHCP**. Isso é configurado através do Web Element Manager:

1. Abra o Web Element Manager da estação base em `https://<base-station-ip>/`
2. Navegue até **Automação de Configuração**
3. Defina **Cenário** como **Rede privada com DHCP**

4. Deixe **Excluir certificados do operador** como **N��o**

Se a estação base estiver configurada para **Rede pública**, ela **rejeitará** Ofertas DHCP que contenham dados do fornecedor da Opção 43.

Porta Ethernet

A estação base envia DHCP em sua porta OAM (Operações, Administração, Manutenção). No módulo do sistema SBTS, isso é tipicamente **SystemModuleEIF3** ou a primeira porta conectada. A estação base detecta automaticamente qual porta tem link e testa cada uma em sequência.

A porta OAM deve estar conectada à rede de gerenciamento onde o servidor DHCP é acessível. Nenhuma marcação de VLAN é necessária para implantações de rede privada — a estação base envia DHCP não marcado na interface simples primeiro, e depois recua para a sondagem de VLAN se nenhuma oferta válida for recebida.

Verificação

Lease DHCP

Após configurar o servidor DHCP, verifique se a estação base obtém um lease. No MikroTik:

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

O prefixo do endereço MAC da estação base é `78:F9:B4` (Nokia Solutions and Networks).

Logs da Estação Base

O relatório de autoconexão da estação base (acessível via Web Element Manager) deve mostrar:

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

RAN Monitor

Na interface Web do RAN Monitor:

1. Navegue até **Status da BTS**
2. A estação base deve aparecer com um dos seguintes status:
   - **Conectado** (verde) — registrado, sessão ativa, dados de configuração e PM fluindo
   - **Aguardando Dados de PM** (azul) — sessão ativa, configuração recebida, aguardando o primeiro ciclo de PM
   - **Sessão Ativa** (amarelo) — registrado com sessão ativa, aguardando dados
   - **Registrando** (amarelo) — registro NE3S em andamento
   - **Desconectado** (vermelho) — não registrado ou inacessível

---

Solução de Problemas

Estação Base Não Aceitando DHCP

Sintoma: A estação base envia DHCP Discover repetidamente, mas nunca aceita a Oferta.

Verifique isso na ordem:

1. **A Opção 43 está anexada à rede DHCP?** — A opção deve estar vinculada via `dhcp-option-set`, não apenas definida
2. **A estação base está configurada para "Rede privada com DHCP"?** — Verifique a página de Automação de Configuração do Web Element

Manager

3. **O IP do RAN Monitor é acessível?** — Verifique o roteamento entre a sub-rede da estação base e o RAN Monitor

"Conexão com o Servidor de Identificação malsucedida"

Sintoma: DHCP é bem-sucedido, mas a estação base não consegue se conectar ao RAN Monitor.

Verifique:

- O RAN Monitor está em execução e acessível a partir da sub-rede da estação base
- A porta 443 está aberta entre a estação base e o RAN Monitor
- A estação base está adicionada à configuração de dispositivo do RAN Monitor

---

Recursos Adicionais

- Guia de Configuração da Nokia AirScale — Configurando monitoramento de desempenho após o comissionamento
- Guia de Configuração em Tempo de Execução — Configuração de dispositivo do RAN Monitor
- Solução de Problemas — Guia geral de solução de problemas

Gerenciamento de Firmware

Repositório de Pacotes de Software Nokia AirScale

Hospede e sirva pacotes de firmware para atualizações de software remotas

---

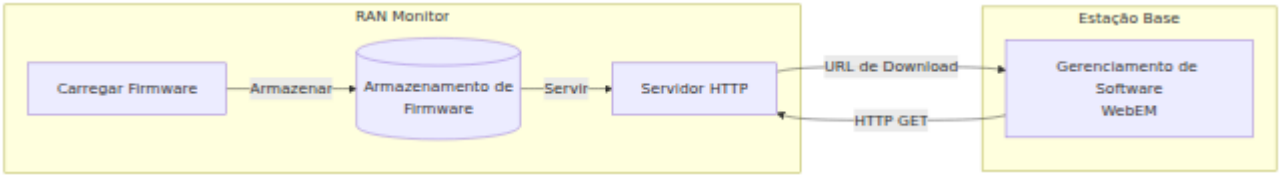
Visão Geral

A página de Gerenciamento de Firmware fornece um repositório centralizado para pacotes de software da estação base Nokia AirScale. Os arquivos de firmware carregados no RAN Monitor são servidos via HTTP, permitindo que as estações base baixem atualizações de software diretamente do RAN Monitor usando a opção "Servidor remoto" do WebEM.

Principais Recursos

- **Carregar pacotes de firmware** - Armazenar pacotes de software .zip da Nokia AirScale
- **Serviço de arquivos HTTP** - As estações base baixam firmware via URLs HTTP padrão
- **Checksums MD5** - Cálculo automático de checksum para verificação de integridade
- **Cópia de URL** - Cópia com um clique de URLs de download para configuração do WebEM
- **Estatísticas de armazenamento** - Monitorar o uso do disco do repositório de firmware

Visão Geral do Fluxo de Trabalho



Acessando a Página

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

Navegação: Barra lateral do Painel de Controle > **Firmware**

Página de Gerenciamento de Firmware com seção de upload e lista de firmware disponível.

Configuração de Armazenamento

Caminho de Armazenamento Padrão

Os arquivos de firmware são armazenados no sistema de arquivos do servidor RAN Monitor:

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

Para cada pacote de firmware, os seguintes arquivos são criados:

- `.zip` - O pacote de firmware
- `.md5` - Checksum MD5 em cache
- `.metadata.json` - Metadados em cache extraídos do pacote

Caminho de Armazenamento Personalizado

Configure um local de armazenamento alternativo em `config/runtime.exs`:

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

Parâmetro	Tipo	Necessário	Padrão	
`firmware_storage_path`	String	Não	`/var/firmware/nokia`	C d a d fi d a s

Comportamento de Retorno

Se o caminho de armazenamento configurado não puder ser criado (por exemplo, permissão negada), o sistema recorre a `priv/firmware/nokia` dentro do diretório da aplicação.

Referência da Interface Web

Visão Geral do Armazenamento

A seção superior exibe estatísticas do repositório:

Métrica	Descrição
Arquivos de Firmware	Número total de pacotes de firmware armazenados
Tamanho Total	Tamanho combinado de todos os arquivos de firmware
Caminho de Armazenamento	Localização atual do sistema de arquivos para armazenamento de firmware

Seção de Upload

Carregue pacotes de firmware Nokia AirScale:

1. Clique na área de upload ou arraste e solte um arquivo `.zip`
2. Verifique se o nome do arquivo aparece com informações de tamanho
3. Clique em **Carregar Firmware** para armazenar o arquivo

O progresso do upload exibe a velocidade de transferência e o tempo estimado restante.

Arquivos suportados: apenas arquivos `.zip` (pacotes de software Nokia)

Tamanho máximo do arquivo: 15 GB

O progresso do upload exibe:

- Velocidade de upload atual (por exemplo, 15.37 MB/s)
- Porcentagem concluída
- Bytes transferidos / tamanho total
- Tempo estimado restante (ETA)

Formato do nome do arquivo: Pacotes de firmware Nokia seguem a convenção de nomenclatura:

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

Exemplo:
`SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip`

Lista de Firmware

A tabela exibe todos os pacotes de firmware carregados:

Coluna	Descrição
Nome do Arquivo	Nome completo do pacote de firmware
Release	Versão de release extraída (por exemplo, SBTS25R1)
Data de Construção	Timestamp de construção extraído dos metadados do firmware
Info	Botão para visualizar metadados detalhados do firmware
Tamanho	Tamanho do arquivo em formato legível por humanos
MD5	Checksum MD5 (clique para copiar)
Downloads	Número de vezes que o firmware foi baixado
Ações	Botões Copiar URL, Baixar, Excluir

Metadados do Firmware

Clique no botão **Info** em qualquer linha de firmware para visualizar metadados detalhados extraídos do pacote:

O modal de metadados exibe detalhes abrangentes do pacote de firmware.

Campo	Descrição
Nome do Arquivo	Nome completo do pacote
Release	Versão do software da estação base (por exemplo, SBTS25R1)
Data de Construção	Timestamp quando o firmware foi construído
Tamanho	Tamanho do arquivo
Arquivo Modificado	Quando o arquivo foi carregado no RAN Monitor
Versão do Software	String completa da versão do software (por exemplo, FTM_SBTS25R1_2025.05.27_0097)
Versão do PS	Versão do release do software da plataforma
Versão do Kernel	Versão do kernel Linux
Versão do LTE	Release de software LTE (por exemplo, FL19A)
Versão do WCDMA	Release de software WCDMA (por exemplo, WBTSFP20C)
Unidades de Hardware Suportadas	Lista de módulos de hardware compatíveis (ASCE, ASCF, FCTJ, etc.)
Checksum MD5	Checksum de integridade do arquivo
URL de Download	URL completa para downloads da estação base

Os metadados são extraídos automaticamente do pacote de firmware no upload e armazenados em cache para acesso rápido.

Botões de Ação

Botão	Descrição
Info	Visualizar metadados detalhados do firmware em um modal
Copiar URL	Copiar a URL de download do firmware para a área de transferência
Baixar	Baixar o arquivo de firmware diretamente
Excluir	Remover o arquivo de firmware do armazenamento

Linha da URL de Download

Abaixo de cada entrada de firmware, a URL de download completa é exibida:

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

Esta URL é inserida no campo de URL do "Servidor remoto" do WebEM.

Checksums MD5

Cálculo Automático

Os checksums MD5 são calculados automaticamente quando os arquivos de firmware são listados. O checksum é armazenado em cache em um arquivo `.md5` ao lado do pacote de firmware para buscas subsequentes rápidas.

Arquivos de Checksum

Para cada pacote de firmware, um arquivo correspondente `.md5` é criado:

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

O arquivo `.md5` contém o checksum hexadecimal em minúsculas:

```
a1b2c3d4e5f6789012345678abcdef01
```

Verificação

Use o checksum MD5 para verificar a integridade do firmware após o download:

Linux/macOS:

```
md5sum
SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip
```

Windows (PowerShell):

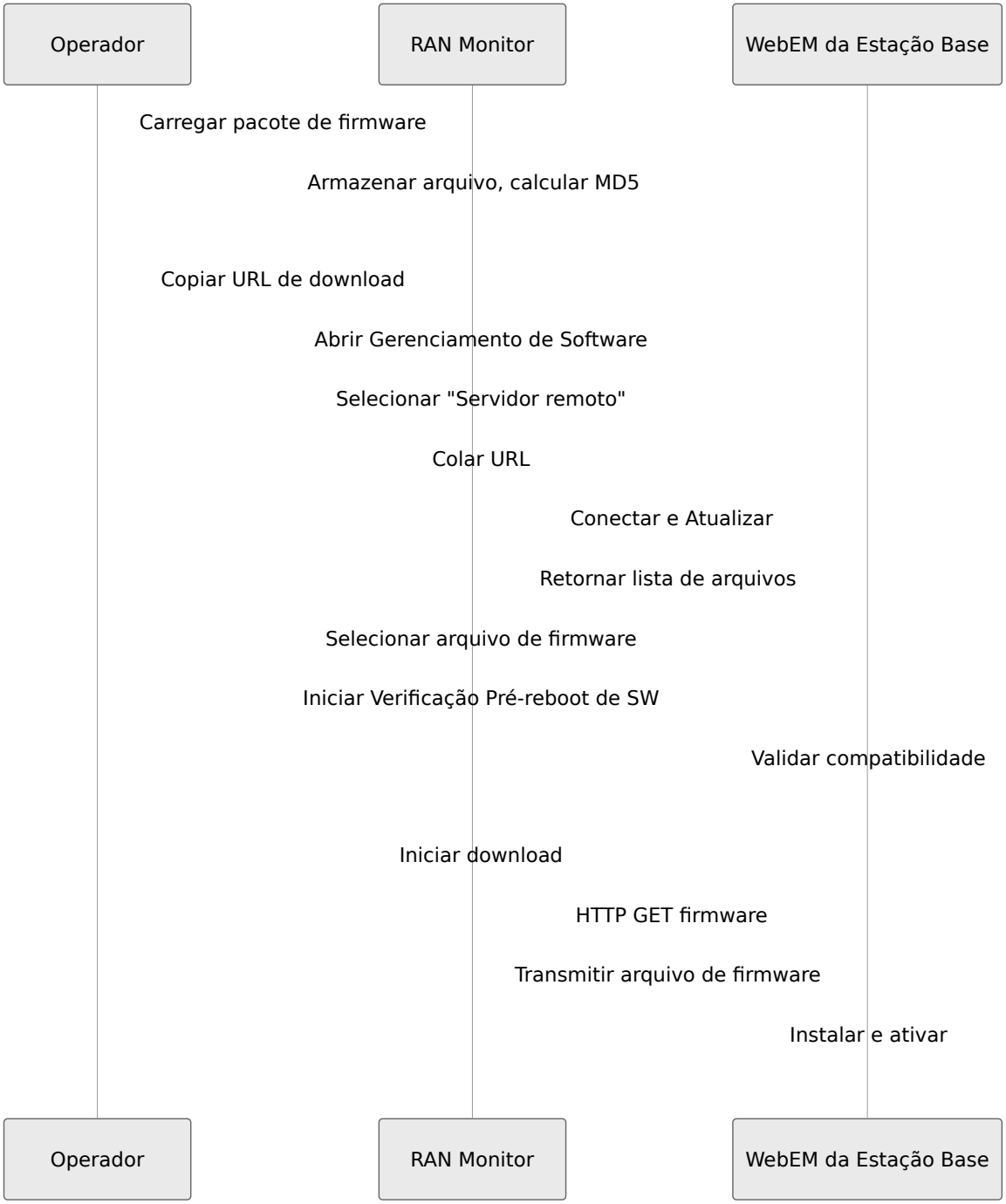
```
Get-FileHash -Algorithm MD5
SBTS25R1_ENB_0000_001046_000000_release_BTSSM_downloadable_A54.zip
```

Fluxo de Atualização de Software da Estação Base

Pré-requisitos

- Pacote de firmware carregado no RAN Monitor
- Conectividade de rede da estação base para o RAN Monitor
- Acesso à interface WebEM da estação base

Processo Passo a Passo



Etapas Detalhadas

1. Carregar Firmware no RAN Monitor

Navegue até a página de Gerenciamento de Firmware e carregue o pacote de software:

- Vá para `https://<ran-monitor-ip>:9443/nokia/firmware`
- Carregue o pacote de firmware `.zip`
- Verifique se o arquivo aparece na lista de firmware com o MD5 correto

2. Copiar a URL de Download

Clique em **Copiar URL** ao lado do pacote de firmware. O formato da URL é:

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

3. Acessar o Gerenciamento de Software do WebEM

Abra a interface WebEM da estação base:

- Navegue até **Gerenciamento de Software** > **Atualização de Software**
- Visualize as versões atuais do software da BTS (Ativas e Passivas)

4. Configurar Servidor Remoto

Na seção "Baixar e ativar software de" do WebEM:

1. Selecione **Servidor remoto**
2. Cole a URL copiada no campo **URL**
3. Clique em **Conectar e Atualizar**

O WebEM se conecta ao RAN Monitor e recupera a lista de arquivos.

5. Selecionar Firmware e Iniciar Atualização

1. Selecione o arquivo de firmware no dropdown **Arquivo de Software**
2. Opcionalmente, execute **Iniciar Verificação Pré-reboot de SW** para verificar a compatibilidade
3. Marque **Ativar software após download** se a ativação imediata for desejada
4. Clique em **Iniciar** para começar a atualização de software

Verificação Pós-Atualização

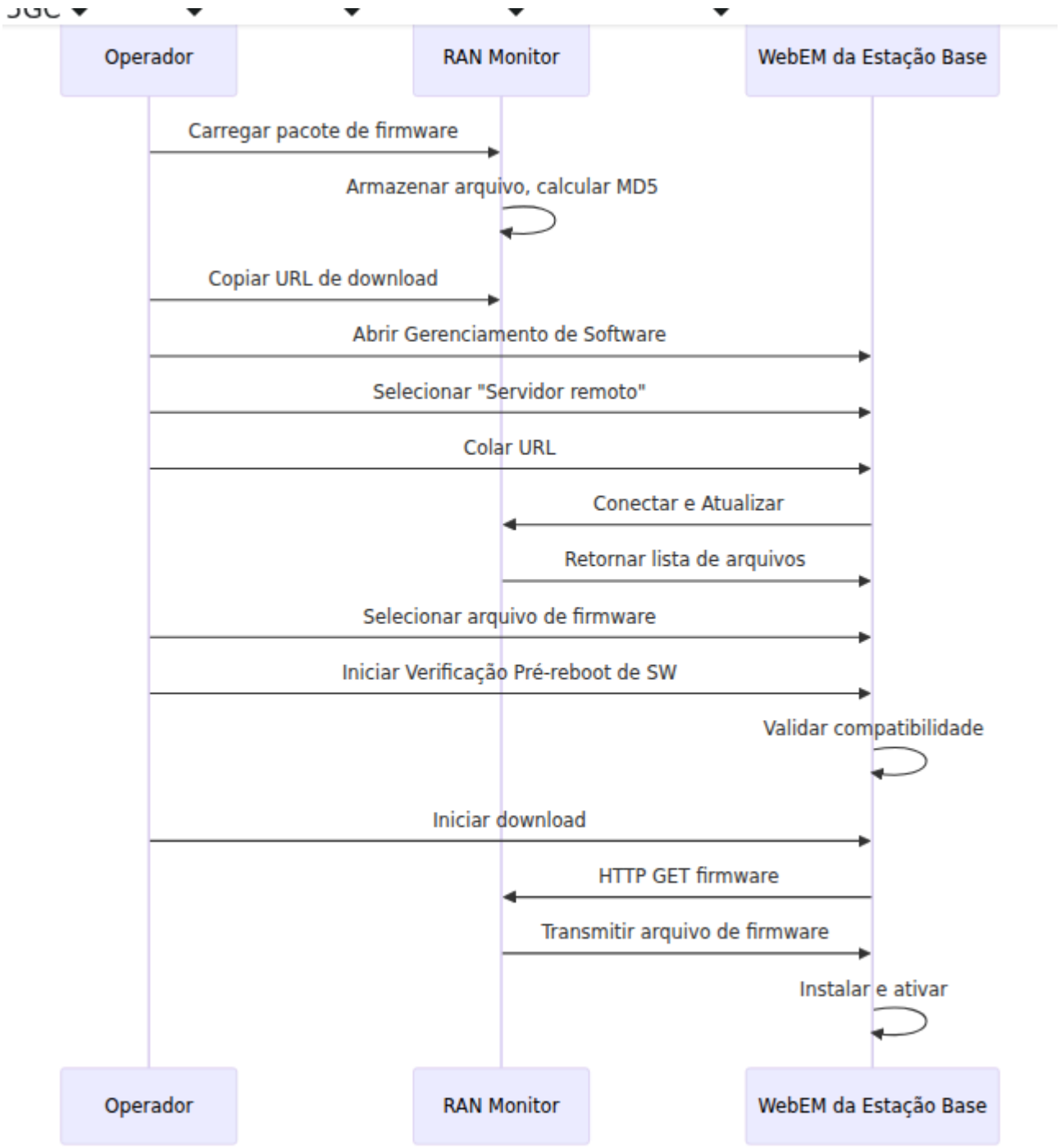
Após a conclusão da atualização:

1. Verifique se a nova versão do software aparece como **Ativa** no WebEM
2. Verifique o RAN Monitor para quaisquer novos alarmes da estação base
3. Confirme a restauração do serviço celular via KPIs

Atualização de Software Remota via Push de Configuração

Em vez de acessar manualmente o WebEM em cada estação base, você pode acionar atualizações de software remotamente carregando um trecho de configuração através do recurso de gerenciamento de configuração do RAN Monitor.

Como Funciona



Trecho de Configuração

Crie um arquivo XML contendo os parâmetros de download do software. A estação base buscará o firmware da URL especificada quando a configuração for ativada.

Exemplo: `sw_update.xml`

```
<?xml version="1.0" encoding="UTF-8"?>
<raml xmlns="raml21.xsd" version="2.1">
<cmData type="plan" scope="changes">
<managedObject class="com.nokia.srbts.btsswm:BTSSWM" distName="MRBTS-
operation="update">
  <p name="swPkgUrl">http://{ran-monitor-
ip}:4000/firmware/nokia/SBTS25R1_ENB_0000_001046_000000_release_BTSSM
  <p name="swPkgActivate">true</p>
</managedObject>
</cmData>
</raml>
```

Substitua:

- `{site_id}` - O ID do MRBTS da estação base alvo (por exemplo, `256`, `2057`)
- `{ran-monitor-ip}` - O endereço IP ou nome do host do RAN Monitor acessível a partir da estação base

Enviando a Configuração

1. Navegue até a página de detalhes da estação base no RAN Monitor
2. Clique em **Config Ops** para abrir operações de configuração
3. Carregue o trecho `sw_update.xml`
4. Clique em **Validar** para verificar a configuração
5. Clique em **Ativar** para aplicar a configuração

A estação base fará o download e instalará o firmware automaticamente.

Atualizações em Lote

Para atualizar vários sites, crie um trecho XML separado para cada site (com o ID MRBTS correto) e envie-os sequencialmente através do RAN Monitor, ou use a API para automatizar o processo.

Referência de Parâmetros

Parâmetro	Descrição
`swPkgUrl`	URL HTTP do pacote de firmware a ser baixado
`swPkgActivate`	Defina como `true` para ativar automaticamente após o download

---

Rastreamento de Downloads

O RAN Monitor rastreia downloads de firmware para ajudar a identificar quais estações base recuperaram pacotes de software.

Informações Rastreadas

Para cada download, as seguintes informações são registradas:

Campo	Descrição
Endereço IP	Endereço IP remoto do downloader
Nome do Host	Nome do host resolvido ou nome correspondente do AirScale
Timestamp	Data e hora do download

Visualizando o Histórico de Downloads

A coluna **Downloads** na lista de firmware mostra a contagem total de downloads. Passe o mouse sobre a contagem para ver detalhes recentes de downloads, incluindo endereços IP e timestamps.

Os dados de rastreamento de downloads são persistidos em disco e sobrevivem a reinicializações da aplicação.

Acesso à API

Listar Arquivos de Firmware

Recupere o inventário de firmware via API REST:

Endpoint: `GET /api/firmware/nokia`

Resposta:


```
{
  "firmware": [
    {
      "filename": "SBTS25R1_ENB_0000_001046_000000_release_BTSSM_dowr
      "size": 1073741824,
      "size_formatted": "1.0 GB",
      "modified": "2025-01-15T10:30:00Z",
      "download_url": "http://ran-
monitor:4000/firmware/nokia/SBTS25R1_ENB_0000_001046_000000_release_E
      "metadata": {
        "release": "SBTS25R1",
        "build": "0000_001046_000000",
        "variant": "release",
        "suffix": "A54",
        "type": "BTS Software"
      }
    }
  ],
  "stats": {
    "file_count": 3,
    "total_size": 3221225472,
    "total_size_formatted": "3.0 GB",
    "storage_path": "/var/firmware/nokia"
  }
}
```

Baixar Arquivo de Firmware

Endpoint: `GET /firmware/nokia/<filename>`

Resposta: Download de arquivo binário com `Content-Type: application/zip`

Referência de Configuração

URL Base de Download

Configure a URL base acessível externamente para downloads de firmware:

```
config :ran_monitor,
  firmware_base_url: "http://ran-monitor.example.com:4000"
```

Parâmetro	Tipo	Necessário	Padrão	D
`firmware_base_url`	String	Não	`http://localhost:4000`	URI usa ger de Def con do ace ext do RAI

Essa configuração afeta as URLs exibidas na interface web e retornadas pela API. O serviço de arquivos real usa a porta HTTP configurada da aplicação.

Solução de Problemas

Upload Falha

Sintomas: O upload do arquivo mostra erro ou nunca é concluído

Possíveis causas:

- O arquivo excede o tamanho máximo de 15 GB
- O arquivo não é um arquivo `.zip`
- Espaço em disco insuficiente no caminho de armazenamento
- Permissão negada no diretório de armazenamento

Resolução:

1. Verifique se o tamanho do arquivo está abaixo de 15 GB
2. Confirme se a extensão do arquivo é `.zip`
3. Verifique o espaço em disco disponível: `df -h /var/firmware/nokia`
4. Verifique as permissões do diretório: `ls -la /var/firmware`

Estação Base Não Consegue Baixar

Sintomas: "Conectar e Atualizar" do WebEM falha ou o download expira

Possíveis causas:

- Problema de conectividade de rede entre a estação base e o RAN Monitor
- Firewall bloqueando a porta HTTP 4000
- URL incorreta (IP ou nome do host errado)

Resolução:

1. Verifique o caminho da rede: ping RAN Monitor a partir da rede da estação base
2. Verifique se o firewall permite a porta 4000 de entrada
3. Confirme se a URL usa o IP/nome do host correto acessível a partir da estação base

4. Teste a URL no navegador a partir do mesmo segmento de rede

MD5 Mostra "calculando..."

Sintomas: A coluna MD5 mostra "calculando..." e nunca atualiza

Possíveis causas:

- Arquivo muito grande ainda sendo processado
- Problema de permissão no sistema de arquivos impedindo a criação do arquivo `.md5`

Resolução:

1. Aguarde a conclusão do cálculo (arquivos grandes demoram mais)
2. Clique em **Atualizar** para recarregar a página
3. Verifique se as permissões do diretório de armazenamento permitem a criação de arquivos

Erro de Arquivo Já Existe

Sintomas: Upload falha com erro "já existe"

Resolução:

1. Exclua o arquivo existente se a substituição for pretendida
2. Renomeie o novo arquivo se ambas as versões forem necessárias
3. Verifique se você não está acidentalmente re-enviando o mesmo arquivo

Introdução ao RAN Monitor

Guia Rápido para Implantação e Configuração do RAN Monitor

Instruções passo a passo para configurar o RAN Monitor em seu ambiente

---

Índice

Visão Geral

Este guia o orienta através da implantação inicial do RAN Monitor, desde a preparação da infraestrutura até a conexão da primeira estação base.

O Que Você Vai Conquistar

Ao final deste guia, você terá:

- ✓ Preparado a infraestrutura necessária (MySQL, InfluxDB)
- ✓ Configurado o RAN Monitor com os detalhes do seu ambiente
- ✓ Iniciado o aplicativo RAN Monitor
- ✓ Conectado sua primeira estação base Nokia AirScale
- ✓ Verificado que as métricas estão fluindo para o InfluxDB
- ✓ Acessado o painel da interface Web UI

Tempo Estimado: 30-60 minutos para configuração inicial

Pré-requisitos

Antes de implantar o RAN Monitor, certifique-se de que você possui o seguinte:

Requisitos de Infraestrutura

Servidor de Banco de Dados MySQL

- Versão: MySQL 5.7+ ou MariaDB 10.3+
- Acesso: Conectividade de rede a partir do servidor do RAN Monitor
- Permissões: Privilégios CREATE, SELECT, INSERT, UPDATE, DELETE
- Banco de Dados: Banco de dados vazio criado para o RAN Monitor
- Recomendação: Instância ou esquema de banco de dados dedicado

Banco de Dados de Série Temporal InfluxDB

- Versão: InfluxDB 1.8+ ou 2.0+
- Acesso: Conectividade de rede a partir do servidor do RAN Monitor
- Bucket/Banco de Dados: Criado e pronto para armazenamento de métricas
- Token de API: Com permissões de gravação no bucket (InfluxDB 2.x)
- Armazenamento: Espaço em disco suficiente para sua política de retenção

Servidor do RAN Monitor

- SO: Linux (Ubuntu 20.04+, CentOS 8+, ou similar)
- RAM: 4GB mínimo, 8GB recomendado
- CPU: 2 núcleos mínimo, 4+ núcleos recomendados
- Disco: 20GB mínimo para aplicativo e logs
- Rede: Conectividade com estações base, MySQL e InfluxDB

Requisitos de Rede

Conectividade de Rede

- RAN Monitor → Estações base Nokia AirScale (porta 8080)
- Estações base Nokia → RAN Monitor (porta 9076 para webhooks)
- RAN Monitor → MySQL (porta 3306)
- RAN Monitor → InfluxDB (porta 8086)
- Operadores → Web UI do RAN Monitor (porta 9443)

Regras de Firewall

- Permitir entrada na porta 8080 (comunicação da estação base)
- Permitir entrada na porta 9076 (receptor de webhook)
- Permitir entrada na porta 9443 (Web UI HTTPS)
- Permitir saída para MySQL e InfluxDB

Requisitos da Estação Base Nokia

Para Cada Estação Base:

- **Endereço IP** - Endereço de rede onde a estação base é acessível
- **Porta** - Porta da interface de gerenciamento (tipicamente 8080)
- **Credenciais** - Nome de usuário e senha para autenticação WebLM
- **Rota de Rede** - Conectividade verificada (ping deve ter sucesso)
- **Interface de Gerenciamento** - Habilitada e acessível

Chaves de Autenticação do Gerente

- **Chave Privada** - Para autenticação do gerente (formato PEM)
- **Certificado Público** - Certificado de identidade do gerente (formato DER)
- Fornecido pela Nokia ou gerado com OpenSSL

Grafana (Opcional, mas Recomendado)

- Versão: Grafana 8.0+
- Acesso: Conectividade de rede ao InfluxDB
- Propósito: Painéis de análise e alertas

Processo de Configuração Inicial

Passo 1: Preparar a Infraestrutura

1.1 Configurar o Banco de Dados MySQL

Crie o banco de dados para o RAN Monitor:

```
CREATE DATABASE ran_monitor CHARACTER SET utf8mb4 COLLATE
utf8mb4_unicode_ci;
```

Crie um usuário dedicado com privilégios apropriados:

```
CREATE USER 'ran_monitor_user'@'%' IDENTIFIED BY
'secure_password';
GRANT CREATE, SELECT, INSERT, UPDATE, DELETE ON ran_monitor.* TO
'ran_monitor_user'@'%';
FLUSH PRIVILEGES;
```

Verifique a conectividade a partir do servidor do RAN Monitor:

```
mysql -h <mysql-host> -u ran_monitor_user -p ran_monitor
```

1.2 Implantar o InfluxDB

Para InfluxDB 1.x, crie o banco de dados:

```
influx -execute 'CREATE DATABASE "nokia-monitor"'
```

Para InfluxDB 2.x, crie um bucket:

```
influx bucket create -n nokia-monitor -o your-org
```

Crie um token de API com permissões de gravação (InfluxDB 2.x):

```
influx auth create --org your-org --write-buckets
```

Salve o token para uso na configuração.

1.3 Verificar Rotas de Rede

Assegure a conectividade de rede para todas as estações base:

```
# Testar conectividade para cada estação base
ping 10.7.15.66

# Verificar se a porta de gerenciamento está acessível
telnet 10.7.15.66 8080
```

Verifique se o MySQL e o InfluxDB são acessíveis:

```
# Testar conectividade do MySQL
telnet <mysql-host> 3306

# Testar conectividade do InfluxDB
curl http://<influxdb-host>:8086/ping
```

Passo 2: Configurar o RAN Monitor

Toda a configuração é gerenciada no arquivo `config/runtime.exs`.

2.1 Configuração do Banco de Dados

Edite `config/runtime.exs` e configure a conexão 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 Configuração do InfluxDB

Configure a conexão do InfluxDB:

```
config :ran_monitor, RanMonitor.InfluxDbConnection,
  auth: [
    username: "monitor",
    password: "influx_password"  # Ou token de API para InfluxDB
2.x
  ],
  database: "nokia-monitor",
  host: "influxdb-host"
```

2.3 Configuração dos Endpoints Web

Configure os endpoints web:

```
# Endpoint SOAP/API principal para estações 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

# Painel de Controle Web UI (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"
  ]

# Endpoint de webhook para notificações da estação 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 Configuração da Nokia

Configure seus identificadores de rede e estações base:

```
config :ran_monitor,
  general: %{
    mcc: "001",  # Seu Código de País Móvel
    mnc: "001"   # Seu Código de Rede Móvel
  },
  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 Gerar Certificados SSL (se necessário)

Para a Web UI HTTPS, gere certificados SSL:

```
# Certificado autoassinado para laboratório/teste
openssl req -newkey rsa:2048 -nodes -keyout
priv/cert/omnitouch.pem \
  -x509 -days 365 -out priv/cert/omnitouch.crt
```

Para produção, use certificados assinados por CA.

Para opções de configuração detalhadas, consulte o Guia de Configuração em Tempo de Execução.

Passo 3: Iniciar o Sistema

Uma vez configurado, inicie o RAN Monitor.

3.1 Executar Migrações do Banco de Dados

Inicialize o esquema do banco de dados:

```
mix ecto.migrate
```

Isso cria todas as tabelas necessárias para o gerenciamento do estado da sessão.

3.2 Iniciar o RAN Monitor

Inicie o aplicativo:

```
mix phx.server
```

Ou para implantação em produção:

```
MIX_ENV=prod mix release
_build/prod/rel/ran_monitor/bin/ran_monitor start
```

3.3 Monitorar os Logs de Inicialização

Observe os logs para um início bem-sucedido:

```
[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
```

Procure por:

- Endpoints web iniciados
- Conexões de banco de dados estabelecidas
- Conectividade do InfluxDB confirmada
- Tentativas de registro da estação base

Verificação

Passo 4: Verificar a Operação

Verifique se o sistema está funcionando corretamente.

4.1 Acessar o Painel da Web UI

Abra seu navegador e navegue até:

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

Você deve ver o painel de controle do RAN Monitor.

4.2 Verificar o Status da Estação Base

Na Web UI:

1. Navegue até a página **Estações Base**
2. Verifique se sua estação base aparece na lista
3. O status deve mostrar como "Associado" (verde)
4. O estado de registro deve ser "Registrado"
5. As informações da sessão devem mostrar uma sessão ativa com tempo de expiração

Se o status estiver vermelho/falhado, verifique:

- Conectividade de rede com a estação base

- As credenciais estão corretas
- A interface de gerenciamento da estação base está acessível
- Logs do aplicativo para mensagens de erro

4.3 Confirmar que as Métricas estão Fluindo para o InfluxDB

Na Web UI:

1. Navegue até a página **Status do InfluxDB**
2. O status da conexão deve ser verde
3. As contagens de medições devem estar aumentando
4. Verifique as contagens de "Métricas de Desempenho", "Configuração" e "Alarmes"

Alternativamente, consulte o InfluxDB diretamente:

```
# 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 Revisar os Logs de Inicialização

Verifique os logs do aplicativo para quaisquer erros:

Na Web UI:

1. Navegue até a página **Logs do Aplicativo**
2. Filtre por nível "Erro"
3. Verifique se não há erros críticos

Ou verifique a saída do console se estiver executando via `mix phx.server`.

4.5 Verificar Detalhes do Dispositivo

Na Web UI:

1. Clique na sua estação base na página de Estações Base
2. Verifique:
    - Os detalhes de registro estão preenchidos
    - A sessão tem um tempo de expiração válido
    - Métricas recentes mostram dados
    - O estado de configuração mostra parâmetros

Próximos Passos

Agora que o RAN Monitor está em funcionamento, aqui estão os próximos passos recomendados:

Ações Imediatas

1. **Adicionar Mais Estações Base**
    - Adicione dispositivos adicionais ao `config/runtime.exs`
    - Reinicie o aplicativo para aplicar as alterações
    - Consulte o Guia de Operações Comuns
2. **Configurar Painéis do Grafana**
    - Instale o Grafana se ainda não estiver implantado
    - Configure a fonte de dados do InfluxDB
    - Importe ou crie painéis
    - Consulte o Guia de Integração do Grafana
3. **Configurar Retenção de Dados**
    - Defina períodos de retenção apropriados
    - Configure a retenção por dispositivo, se necessário
    - Consulte o Guia de Política de Retenção de Dados
4. **Configurar Alarmes e Alertas**

    - Revise alarmes ativos na Web UI
    - Configure regras de alerta no Grafana
    - Configure canais de notificação
    - Consulte o Guia de Gerenciamento de Alarmes

Prontidão Operacional

Revisão da Documentação:

- Leia o Guia da Web UI para operações diárias
- Revise o Guia de Operações Comuns para tarefas rotineiras
- Estude o Guia de Solução de Problemas para resolução de problemas

Treinamento da Equipe:

- Faça uma apresentação da Web UI com a equipe de operações
- Pratique fluxos de trabalho comuns (verificação de saúde diária, investigação de alarmes)
- Revise procedimentos de escalonamento para alarmes críticos

Configuração de Monitoramento:

- Crie painéis operacionais no Grafana
- Configure regras de alerta para métricas críticas
- Configure canais de notificação (Slack, e-mail, PagerDuty)

Fortalecimento da Segurança:

- Substitua certificados autoassinados por certificados assinados por CA
- Mova credenciais para variáveis de ambiente
- Restrinja permissões de arquivo em `config/runtime.exs`
- Configure regras de firewall

Implantação em Produção

Antes da Produção:

- Teste primeiro no ambiente de staging
- Verifique se todas as estações base se conectam com sucesso
- Confirme se as métricas estão precisas
- Teste notificações de alarmes
- Documente qualquer configuração personalizada

Lançamento em Produção:

- Implemente durante a janela de manutenção
- Monitore de perto nas primeiras 24 horas
- Tenha um plano de reversão pronto
- Mantenha contatos de suporte disponíveis

Operações Contínuas:

- Verificações diárias de saúde via Web UI
- Revisão semanal das tendências de alarmes
- Planejamento de capacidade mensal com Grafana
- Backups regulares da configuração

Obtendo Ajuda

Recursos de Solução de Problemas

- Guia de Solução de Problemas - Problemas comuns e soluções
- Guia da Web UI - Referência do painel de controle
- Página de Logs do Aplicativo - Logs do sistema em tempo real

Documentação

- Guia de Operações - Referência operacional completa
- Guia de Configuração em Tempo de Execu��ão - Detalhes de configuração
- Configuração AirScale - Configuração da estação base

Problemas Comuns de Primeira Vez

Estação Base Não Registrando:

- Verifique a conectividade de rede (ping)
- Verifique se as credenciais estão corretas
- Confirme se a porta 8080 está acessível
- Revise os logs do aplicativo para erros

Falha na Conexão com o InfluxDB:

- Verifique se o InfluxDB está em execução
- Verifique a configuração de host e porta
- Confirme se o token de API tem permissões de gravação
- Teste a conectividade: `curl http://<influxdb-host>:8086/ping`

Web UI Não Acessível:

- Verifique se a porta HTTPS 9443 está aberta
- Verifique se os certificados SSL estão presentes
- Confirme se o endpoint web foi iniciado nos logs
- Tente acessar a partir da máquina local primeiro

Documentação Relacionada

- **Guia de Operações** - Visão geral operacional completa
- **Guia da Web UI** - Guia do usuário do painel de controle
- **Guia de Operações Comuns** - Tarefas do dia a dia
- **Guia de Configuração em Tempo de Execução** - Referência de configuração
- **Configuração AirScale** - Configuração da estação base
- **Guia de Integração do Grafana** - Análise e painéis
- **Guia de Gerenciamento de Alarmes** - Tratamento de alarmes
- **Guia de Política de Retenção de Dados** - Gerenciamento de dados

- **Guia de Solução de Problemas** - Resolução de problemas

Guia de Integração e Análise do Grafana

Construindo Painéis Operacionais e Alertas para Monitoramento de RAN

Guia completo para criação de dashboards no Grafana, estratégias de alerta e visualização de KPIs

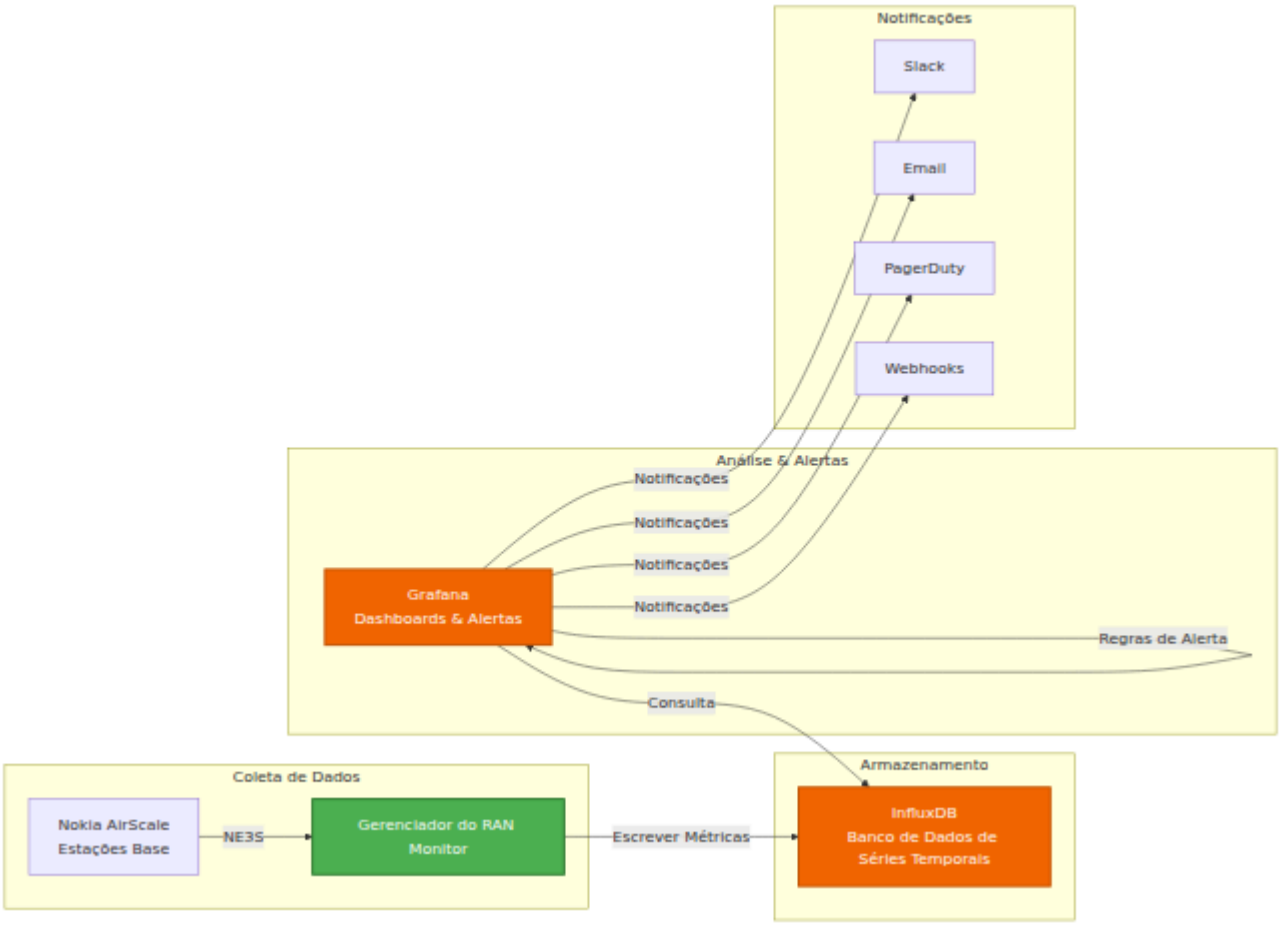
---

Índice

Visão Geral

Grafana é uma plataforma de visualização e alerta que transforma as métricas coletadas pelo RAN Monitor em insights acionáveis para equipes de operações de rede.

Arquitetura de Monitoramento



Benefícios do Grafana

- **Visibilidade em Tempo Real** - Dashboards ao vivo mostrando o estado atual da rede
- **Análise Histórica** - Análise de tendências ao longo de dias/semanas/meses
- **Alertas** - Notificações proativas antes que problemas impactem os usuários
- **Visões Personalizadas** - Dashboards adaptados a diferentes funções (executivo, operações, engenharia)
- **Relatórios** - Exportações instantâneas e relatórios programados

Personalização do Dashboard

Importante: Os dashboards e visualizações descritos neste guia são **exemplos e modelos**. A **equipe de Operações/NOC (ONS)** projetará e construirá dashboards do Grafana de acordo com seus requisitos operacionais específicos, KPIs e fluxos de trabalho de monitoramento.

Este guia fornece:

- Exemplos de consultas e padrões para se basear
- Melhores práticas para organização de dashboards
- Modelos de configuração de alertas
- Mapeamentos de referência de contadores (veja Referência de Contadores da Nokia)

A equipe ONS deve personalizar:

- Layouts de painel e visualizações
- Limiares de alerta e políticas de escalonamento
- Políticas de retenção para seu volume de dados (veja Política de Retenção de Dados)
- Janelas de agregação com base nas necessidades de monitoramento
- Canais de notificação e roteamento

Para opções de configuração em tempo de execução e configurações de coleta de dados, consulte o Guia de Configuração em Tempo de Execução.

Configuração do Grafana & InfluxDB

Instalação

Pré-requisitos:

- InfluxDB 2.0+ com bucket criado para o RAN Monitor

- Token da API do InfluxDB com permissões de leitura
- Conectividade de rede entre Grafana e InfluxDB

Exemplo de Docker Compose:

```
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:
```

Criando um Token da API do InfluxDB

1. Abra a interface do InfluxDB (porta 8086)
2. Navegue até Tokens da API
3. Crie um novo token com permissões:
    - Leitura: buckets, `ran_metrics` (seu bucket)

4. Copie o valor do token
5. Use na configuração da fonte de dados do Grafana

Configuração da Fonte de Dados

Adicionando o InfluxDB como Fonte de Dados no Grafana

1. **Acessar Fontes de Dados**
    - Grafana → Configuração → Fontes de Dados
2. **Criar Nova Fonte de Dados**
    - Clique em "Adicionar fonte de dados"
    - Selecione "InfluxDB"
3. **Configurar Conexão**

Configuração	Valor	Notas
Nome	RAN Monitor	Nome exibido no Grafana
URL	`http://influxdb:8086`	Deve ser acessível a partir do Grafana
Acesso	Servidor (padrão)	O backend do Grafana acessa o DB
Organização	omnitouch	Sua organização no InfluxDB
Token	(token da API)	Da criação do token da API
Bucket Padrão	ran_metrics	Onde o RAN Monitor escreve
Intervalo de tempo mínimo	10s	Corresponde ao intervalo de polling

4. **Testar Conexão**
    - Clique no botão "Testar"
    - Deve mostrar "Fonte de Dados está funcionando"

Nota: As configurações de conexão do InfluxDB (URL, organização, nome do bucket) devem corresponder à sua configuração do RAN Monitor. Consulte o Guia de Configuração em Tempo de Execução para detalhes sobre a configuração do InfluxDB e a Configuração do AirScale para registro da estação base.

Linguagem de Consulta Flux

O Grafana usa Flux para consultar o InfluxDB. Sintaxe básica:

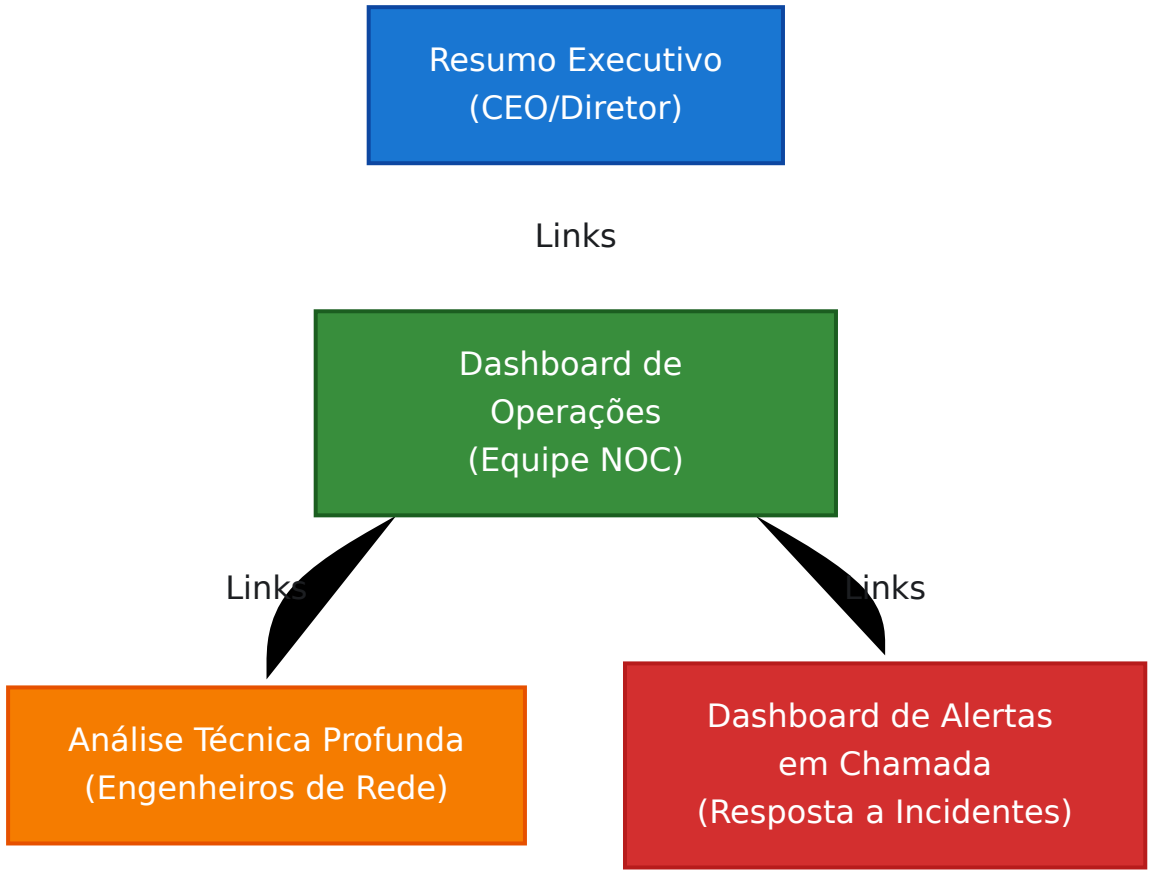
```
from(bucket:"ran_metrics")
  |> range(start: -7d, stop: now())
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r.device == "SITE_A_BS1")
  |> group(by: ["_field"])
  |> aggregateWindow(every: 1h, fn: mean)
```

Conceitos Chave:

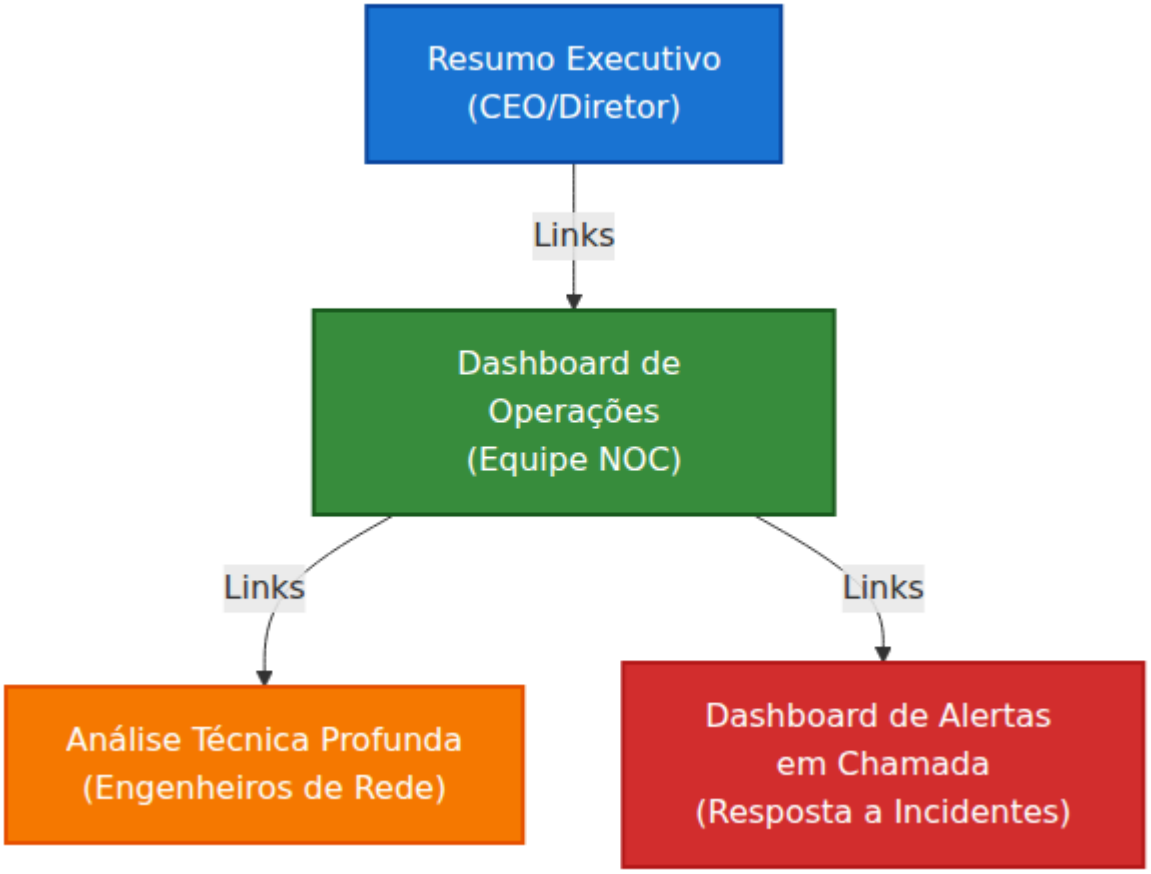
- `from()` - Seleciona o bucket
- `range()` - Janela de tempo
- `filter()` - Seleciona dados
- `group()` - Organiza resultados
- `aggregateWindow()` - Resume períodos de tempo

Padrões de Design de Dashboard

Hierarquia do Dashboard



Tipos de Painéis & Casos de Uso



Seções Padrão do Dashboard

Seção Superior: Métricas Chave (Indicadores de Status)

Mostre o estado atual de forma rápida:

```
┌──────────────────────────────────────────────────────┐
│ Instantâneo da Saúde da Rede                         │
├──────────────────┬──────────────────┬────────────────┤
│ Dispositivos Ativos │ Alarmes Ativos │ Média de Disponibilidade
da Célula │
│ 48/50 (96%)   │ 3 Críticos     │ 98.5%            │
├──────────────────┴──────────────────┴────────────────┤
│ Incidente Mais Recente: [2 horas atrás] Resolvido │
└──────────────────────────────────────────────────────┘
```

Propósito:

- Verificação rápida de status (< 10 segundos para avaliar)
- Indicadores verdes/vermelhos para problemas imediatos
- Links para dashboards detalhados para investigação

Seção do Meio: Tendências (Gráficos de Séries Temporais)

Mostre padrões e mudanças ao longo do tempo:

```
┌──────────────────────────────────────────────────────┐
│ Padrões de Tráfego (7 dias)                          │
│ [Grande gráfico de área com padrões diários/semanal] │
│ Pico: 250 Gbps (Quarta-feira 14h)                    │
│ Vale: 80 Gbps (Domingo 3h)                           │
└──────────────────────────────────────────────────────┘
```

Propósito:

- Identificar restrições de capacidade
- Compreender padrões de tráfego
- Prever horários de pico
- Detectar anomalias

Seção Inferior: Detalhes & Alertas (Tabelas)

Mostre informações granulares:

```
┌──────────────────────────────────────────────────────┐
│ Alarmes Ativos (Classificados por Severidade)        │
├──────────┬──────────────────┬──────────────┬─────────┤
│ Nível    │ Dispositivo      │ Problema     │ Duração │
├──────────┼──────────────────┼──────────────┼─────────┤
│ □        │ SITE_A_BS1       │ Célula Fora  │ 45 minutos │
│ □        │ SITE_B_BS2       │ Alta Temperatura │ 2 horas │
└──────────┴──────────────────┴──────────────┴─────────┘
```

Propósito:

- Itens de ação imediata

- Detalhes de investigação
- Informações de tendência (duração, frequência)

Exemplos de Consultas

Nota: Os seguintes exemplos de consultas usam contadores de desempenho específicos da Nokia. Para definições detalhadas de contadores, unidades e diretrizes de uso, consulte a Referência de Contadores da Nokia. Para configurar intervalos de coleta de dados e configurações do InfluxDB, veja o Guia de Configuração em Tempo de Execução.

Consultas de Métricas de Desempenho

Disponibilidade da Célula por Dispositivo (Últimas 24 Horas)

```
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")
```

Uso:

- Dashboard executivo para relatórios de SLA
- Gráfico de séries temporais mostrando médias horárias
- Meta: > 99.5% de disponibilidade

Tendência de Throughput de Tráfego (7 Dias)

```
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")
```

Uso:

- Dashboard de planejamento de capacidade
- Gráfico de área mostrando pico vs. vale
- Identificar horários de pico para agendamento

Utilização de Recursos DL por Célula

```
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")
```

Uso:

- Dashboard de operações em tempo real
- Painel de medidor com aviso em 80%, crítico em 95%
- Identificação rápida de células congestionadas

Consultas de Alarmes

Alarmes Ativos por Severidade (Últimas 24 Horas)

```
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")
```

Uso:

- Indicador de status mostrando contagens de alarmes
- Gráfico de pizza de distribuição
- Clique para ver lista detalhada de alarmes

Taxa de Alarmes (Alarmes por Hora)

```
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")
```

Uso:

- Gráfico de tendência mostrando quando ocorrem tempestades de alarmes
- Identificar momentos de alta instabilidade
- Correlacionar com mudanças de configuração

Alarmes Frequentemente Acionados

```
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")
```

Uso:

- Identificar problemas sistêmicos
- Priorizar esforços de engenharia
- Foco na análise de causa raiz

Análises Avançadas

Previsão de Disponibilidade da Célula (Regressão Linear)

```
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")
```

Uso:

- Prever quando o SLA pode ser violado
- Agendamento proativo de manutenção

- Previsão de capacidade

Correlação de Sucesso de Handover com Tráfego

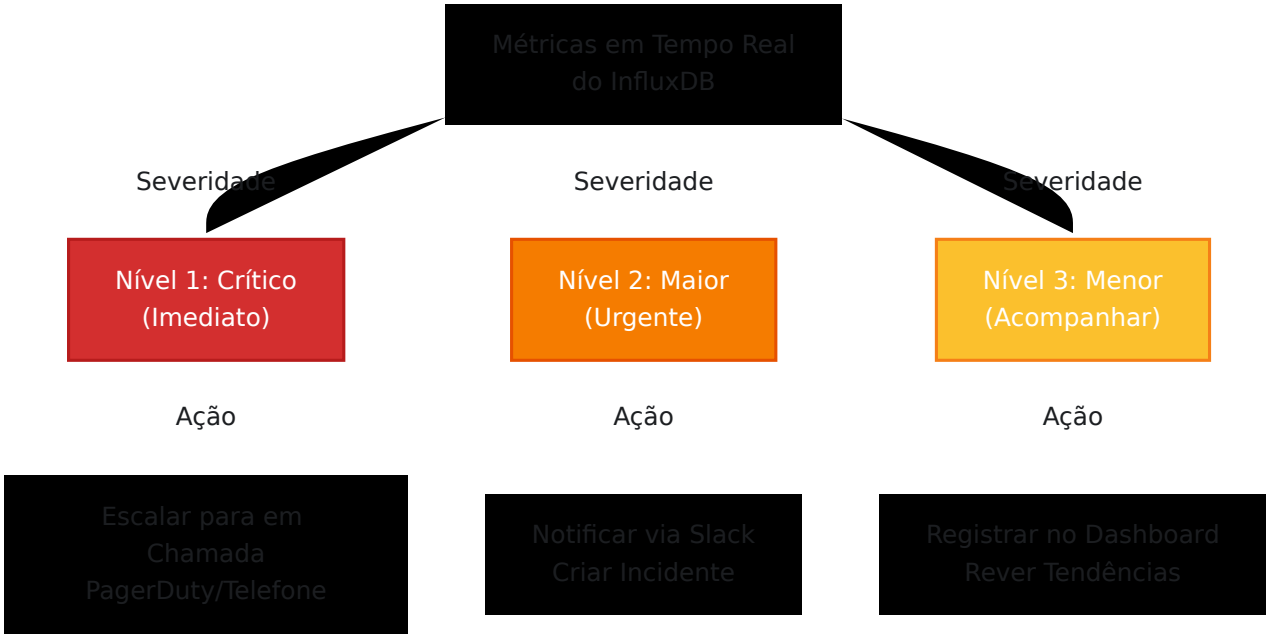
```
from(bucket:"ran_metrics")
  |> range(start: -7d)
  |> filter(fn: (r) => r._measurement == "PerformanceMetrics")
  |> filter(fn: (r) => r._field =~ /HandoverSuccess|Traffic/)
  |> group(by: ["device", "_field"])
  |> aggregateWindow(every: 1h, fn: mean)
  |> pivot(rowKey: ["_time"], columnKey: ["_field"], valueColumn:
"_value")
  |> map(fn: (r) => ({r with correlation: float(v:
r.HandoverSuccess) * float(v: r.Traffic)}))
  |> yield(name: "ho_traffic_correlation")
```

Uso:

- Identificar se problemas de handover estão relacionados à carga
- Ajustar limiares de histerese de handover
- Insights de otimização de rede

Regras de Alerta & Escalonamento

Estrutura de Estratégia de Alerta



Criando Regras de Alerta no Grafana

Passo 1: Criar Regra de Alerta

1. Abra o Dashboard
2. Clique no painel para alertar
3. Painel → Criar alerta
4. Ou Alerta → Regras de Alerta → Criar nova regra de alerta

Passo 2: Configurar Critérios de Avaliação

Exemplo 1: Alerta de Disponibilidade da Célula

```
Condição: CellAvailability < 95%
Duração: 15 minutos
Frequência de Avaliação: A cada 1 minuto
Por: Os últimos 15 minutos
```

Justificativa:

- Acionar em 95% para avisar antes da violação do SLA (99.5%)
- Janela de 15 minutos para evitar falsos positivos de transientes
- Monitorar a cada minuto para resposta rápida

Exemplo 2: Detecção de Tempestade de Alarmes

```
Condição: count(active_alarms) > 10
Duração: 5 minutos
Frequência de Avaliação: A cada 2 minutos
Por: Os últimos 5 minutos
```

Justificativa:

- 10+ alarmes indicam problema sistêmico
- Detecção rápida de 5 minutos para resposta ágil
- Verificar frequentemente para capturar escalonamento

Exemplo 3: Exaustão de Recursos DL

```
Condição: DLResourceUtilization > 90%
Duração: 30 minutos
Frequência de Avaliação: A cada 5 minutos
Por: Os últimos 30 minutos
```

Justificativa:

- Uso sustentado de recursos altos indica congestionamento
- Janela de 30 minutos evita alertas falsos de picos de tráfego
- Monitorar a cada 5 minutos para capturar congestionamento sustentado

Passo 3: Configurar Canal de Notificação

1. Clique em "Canal de Notificação"
2. Selecione ou crie um canal (Slack, Email, PagerDuty, etc.)
3. Configure o modelo de mensagem

Exemplo de Modelo de Mensagem:

```
Alerta: {{ .AlertRuleName }}
Severidade: {{ .Severity }}
Dispositivo: {{ .Labels.device }}
Valor: {{ .EvalMatches[0].Value }}
Duração: {{ .StartsAt }}

{{ .RuleUrl }}
```

Políticas de Escalonamento

Alertas de Nível 1 (Críticos):

- **Condição:** Impacto no serviço (dispositivo fora, violação de SLA iminente)
- **Duração:** Imediato (1-5 minutos)
- **Notificação:** Ligação + SMS + Slack + PagerDuty
- **Responsável:** Engenheiro em chamada
- **SLA:** Resposta em < 15 minutos

Alertas de Nível 2 (Maiores):

- **Condição:** Desempenho degradado (qualidade, disponibilidade em tendência de queda)
- **Duração:** 15-30 minutos
- **Notificação:** Slack + Email + PagerDuty
- **Responsável:** Equipe NOC + engenheiro sênior
- **SLA:** Resposta em < 30 minutos

Alertas de Nível 3 (Menores):

- **Condição:** Informativo (tendências, limites se aproximando)
- **Duração:** 1+ horas
- **Notificação:** Slack + Dashboard
- **Responsável:** Planejamento de capacidade / engenharia
- **SLA:** Revisão diária

Canais de Notificação

Integração com Slack

```
1. Crie um aplicativo Slack no workspace
2. Obtenha a URL do webhook
3. No Grafana Alerta → Canais de Notificação
4. Adicione o canal "Slack"
5. Cole a URL do webhook
6. Teste a notificação
```

Formatação da Mensagem do Slack:

```
 CRÍTICO: Célula Fora - SITE_A_BS1_Cell1
Duração: 45 minutos
Impacto: ~2000 assinantes
Último dado bem-sucedido: 14h15

[Investigar] [Reconhecer] [Dashboard]
```

Integração com PagerDuty

```
1. Crie uma chave de integração no PagerDuty
2. No Grafana Alerta → Canais de Notificação
3. Adicione o canal "PagerDuty"
4. Cole a chave de integração
5. Mapeie os níveis de severidade:
   - Crítico → Acionar incidente
   - Maior → Acionar com menor urgência
   - Menor → Adicionar a incidente existente
```

Integração por Email

```
1. Configure SMTP na configuração do Grafana
2. No Alerta → Canais de Notificação
3. Adicione o canal "Email"
4. Insira os endereços dos destinatários
5. Pode incluir CSV de destinatários para listas de distribuição
```

Dashboards Operacionais

Dashboard 1: Dashboard de Saúde Executiva

Público: Gestão, executivos
Taxa de Atualização: 5 minutos
Propósito: Visão geral de saúde em alto nível

Painéis:

1. **Resumo de Status (4 Painéis de Estatísticas)**
    - Dispositivos Ativos / Total
    - Alarmes Ativos (codificados por cor conforme severidade)
    - Média de Disponibilidade da Célula (%)
    - Tráfego Pico Atual (Gbps)
2. **Saúde da Rede (Série Temporal)**
    - Tendência de Disponibilidade da Célula (7 dias)
    - Tendência da Taxa de Alarmes (7 dias)
    - Previsão de Tráfego vs. Real
3. **Incidentes Recentes (Tabela)**
    - Hora, Duração, Causa Raiz, Status
    - Últimos 7 dias, classificados por severidade
4. **Grade de Status do Dispositivo (Mapa de Calor)**
    - Linhas: Dispositivos, Colunas: Métricas de Saúde
    - Verde (OK) → Amarelo (Degradado) → Vermelho (Fora)

Exemplo de Dashboard:

Exemplo mostrando visão geral da estação base com Último Reportado, UEs Conectados, Dados Transferidos, Utilização de PRB e métricas de Throughput.

Dashboard 2: Dashboard de Operações do NOC

Público: Equipe do centro de operações de rede
Taxa de Atualização: 10 segundos
Propósito: Controle operacional em tempo real

Painéis:

1. **Problemas Ativos (Tabela)**
    - Hora, Severidade, Dispositivo, Problema, Duração
    - Classificar por severidade, clique para aprofundar
2. **Utilização de Recursos (Medidores)**
    - % de Recursos DL (por site)
    - % de Recursos UL (por site)
    - % de CPU em dispositivos
3. **Visão Geral do Tráfego (Gráfico de Área)**
    - Throughput DL/UL (últimas 24 horas)

- Atual vs. média de 24 horas
- Indicadores de hora de pico

4. **Tendência de Alarmes (Gráfico de Barras)**
    - Contagem por severidade (última hora, rolando)
    - Barra empilhada mostrando distribuição
5. **Status do Dispositivo (Visão Rápida)**
    - Nome do dispositivo, IP, Status (verde/vermelho)
    - Timestamp da última atualização de métrica
    - Links para dashboard específico do dispositivo
6. **Eventos Recentes (Série Temporal)**
    - Alarmes aparecendo/limpando
    - Mudanças de configuração
    - Mudanças de status de sessão

Exemplo de Dashboard:

Exemplo mostrando visão geral do Status 4G com mapa geográfico, tabela de alarmes com níveis de severidade e estatísticas de desempenho.

Dashboard 3: Análise Técnica Profunda

Público: Engenheiros de rede
Taxa de Atualização: 1 minuto
Propósito: Análise técnica detalhada

Painéis:

1. **Análise de Padrão de Tráfego (Multi-Série)**
    - DL/UL por site para comparação
    - Linha de base + sobreposição atual
    - Sazonalidade por hora do dia
2. **Métricas de Qualidade da Célula (Multi-Série)**
    - Distribuição de SINR (histograma)
    - Distribuição de RSRP (histograma)
    - Tendências da taxa de sucesso de handover
3. **Desempenho de Rádio (Série Temporal)**
    - Taxa de retransmissão RLC (por site)
    - Taxa de sucesso de configuração RRC
    - Taxa de queda de chamadas
4. **Auditoria de Configuração (Tabela)**
    - Dispositivo, Data de Configuração, Parâmetros Alterados
    - Destaques de modificações recentes
5. **Análise de Correlação (Dispersão)**
    - Recurso DL vs. Tráfego
    - Tráfego vs. Sucesso de Handover
    - Disponibilidade vs. Contagem de Alarmes

Dashboard 4: Dashboard de Alertas em Chamada

Público: Respondedores de incidentes (em chamada)
Taxa de Atualização: 5 segundos
Propósito: Avaliação e resposta rápida a incidentes

Painéis:

1. **Resumo de Alertas (Grande Estatística)**
    - Contagem de alertas críticos ativos
    - Cor de fundo: Verde (OK) / Vermelho (Problemas)
2. **Problemas Críticos (Tabela, Texto Grande)**
    - Dispositivo, Problema, Duração
    - Rolagem automática para os mais recentes primeiro
3. **Métricas Relacionadas (Série Temporal)**
    - Tráfego, Utilização de Recursos
    - Métricas de qualidade para dispositivo afetado
    - Auto-preenchimento com base no alerta
4. **Mudanças Recentes (Tabela)**
    - Mudanças de configuração nas últimas 4 horas
    - Versões de software
    - Modificações de parâmetros
5. **Problemas Semelhantes (Tabela)**
    - Mesmo tipo de problema nos últimos 30 dias
    - Tempo para resolução
    - Causas raízes identificadas
6. **Caminho de Escalonamento (Painel de Texto)**
    - Contato de escalonamento de próximo nível

- Informações sobre a janela de manutenção
- Número de ticket/incidente relacionado

Dashboard 5: Desempenho Detalhado do Nokia AirScale

Público: Engenheiros RF, analistas de desempenho
Taxa de Atualização: 30 segundos
Propósito: Métricas e KPIs específicos da Nokia em profundidade

Este dashboard usa contadores de desempenho específicos da Nokia para fornecer visibilidade abrangente sobre o desempenho da estação base AirScale. Consulte a Referência de Contadores da Nokia para definições detalhadas de contadores.

Painel 1: Visão Geral da Utilização de Recursos (Medidores)

Mostra a utilização atual de PRB (Bloco de Recursos Físicos):

```
// Utilização de PRB 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}))  //
Converter para porcentagem
  |> rename(columns: {_value: "Utilização de PRB DL"})

// Utilização de PRB 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}))  //
Converter para porcentagem
  |> rename(columns: {_value: "Utilização de PRB UL"})
```

Visualização: Painéis de medidor com limiares:

- Verde: 0-70%
- Amarelo: 70-85%
- Vermelho: 85-100%

Painel 2: Tendências de Throughput (Série Temporal)

Exibe throughput da camada PDCP para downlink e uplink:

```
// Throughput 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}))  //
Converter para Mbps
  |> rename(columns: {_value: "Throughput DL em Mbps"})

// Throughput 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}))  //
Converter para Mbps
  |> rename(columns: {_value: "Throughput UL em Mbps"})
```

Contadores Usados:

- **M8012C26** - Throughput PDCP DL Médio (kbit/s)
- **M8012C23** - Throughput PDCP UL Médio (kbit/s)

Painel 3: Contagem de UEs Ativas (Série Temporal)

Acompanha o número de usuários conectados:

```
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 Conectados"})
```

Contador Usado:

- **M8018C1** - UE Ativas por eNB máximo (contagem)

Painel 4: Disponibilidade da Célula (Série Temporal com Alerta de Limite)

Calcula e exibe a porcentagem de disponibilidade da célula:

```
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,
      "Taxa de Disponibilidade da Célula": 100.0 * r.M8020C3 /
(r.M8020C6 - r.M8020C4)
    }))
```

Contadores Usados:

- **M8020C3** - Amostras quando a célula está disponível
- **M8020C6** - Denominador de disponibilidade da célula
- **M8020C4** - Amostras quando a célula está planejada como indisponível

Alerta de Limite: Disponibilidade da Célula < 99%

Painel 5: Utilização de PRB por Célula (Série Temporal Multi-Série)

Mostra a utilização de recursos dividida por células individuais:

```
import "strings"

// Uplink PRB por célula
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": "Utilização Média de PRB Uplink"})

// Downlink PRB por célula
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": "Utilização Média de PRB
Downlink"})
```

Painel 6: Throughput por Célula (Série Temporal Multi-Série)

Throughput PDCP dividido por célula:

```
import "strings"

// Throughput PDCP Downlink por célula
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": "Throughput PDCP Downlink"})

// Throughput PDCP Uplink por célula
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": "Throughput PDCP Uplink"})
```

Painel 7: RSSI (Índice de Força do Sinal Recebido) (Série Temporal Multi-Série)

Exibe estatísticas de força do sinal uplink:

```
import "strings"

// RSSI Mínimo
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 Mínimo"})

// RSSI Médio
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 Médio"})

// RSSI Máximo
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 Máximo"})
```

Contadores Usados:

- **M8005C0** - RSSI para PUCCH Mínimo (dBm)
- **M8005C1** - RSSI para PUCCH Máximo (dBm)

- **M8005C2** - RSSI para PUCCH Médio (dBm)

Painel 8: Latência (Série Temporal)

Medição de atraso do 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": "Latência"})
```

Contador Usado:

- **M8001C2** - Atraso do SDU PDCP no DL DTCH Médio (ms)

Painel 9: Taxa de Sucesso de Configuração RRC (Série Temporal com Limite de Alerta)

Calcula a porcentagem de configurações de conexão bem-sucedidas:

```
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,
      "Taxa de Sucesso de Configuração": 100.0 * r.M8013C5 /
(r.M8013C17 + r.M8013C18 + r.M8013C19 + r.M8013C34 + r.M8013C31 +
r.M8013C21 + r.M8013C93 + r.M8013C91)
    }))
```

Contadores Usados:

- **M8013C5** - Conclusões de Estabelecimento de Conexão de Sinalização
- **M8013C17-M8013C93** - Vários tipos de tentativas de conexão

Alerta de Limite: Taxa de Sucesso de Configuração < 95%

Painel 10: VSWR (Relação de Onda Estacionária de Tensão) por Antena (Série Temporal)

Monitoramento de saúde de hardware para sistemas de antena:

```
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")
```

Contador Usado:

- **M40001C0** - VSWR por ramo de antena (0.1 de relação)

Alerta de Limite: VSWR > 2.0

Painel 11: Consumo de Energia (Série Temporal)

Monitoramento do uso de energia da estação 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": "Consumo de Energia"})
```

Contador Usado:

- **M40002C2** - Consumo de Energia (fator de 100000)

Variáveis do Dashboard:

Este dashboard usa variáveis de modelo do Grafana para filtragem dinâmica:

- **${Airscale}** - Seletor de estação base (dropdown)
- **${CellKey}** - Seletor de célula para sites multi-célula (dropdown)
- **${RadioKey}** - Seletor de unidade de rádio para VSWR (dropdown)

Regras de Alerta para este Dashboard:

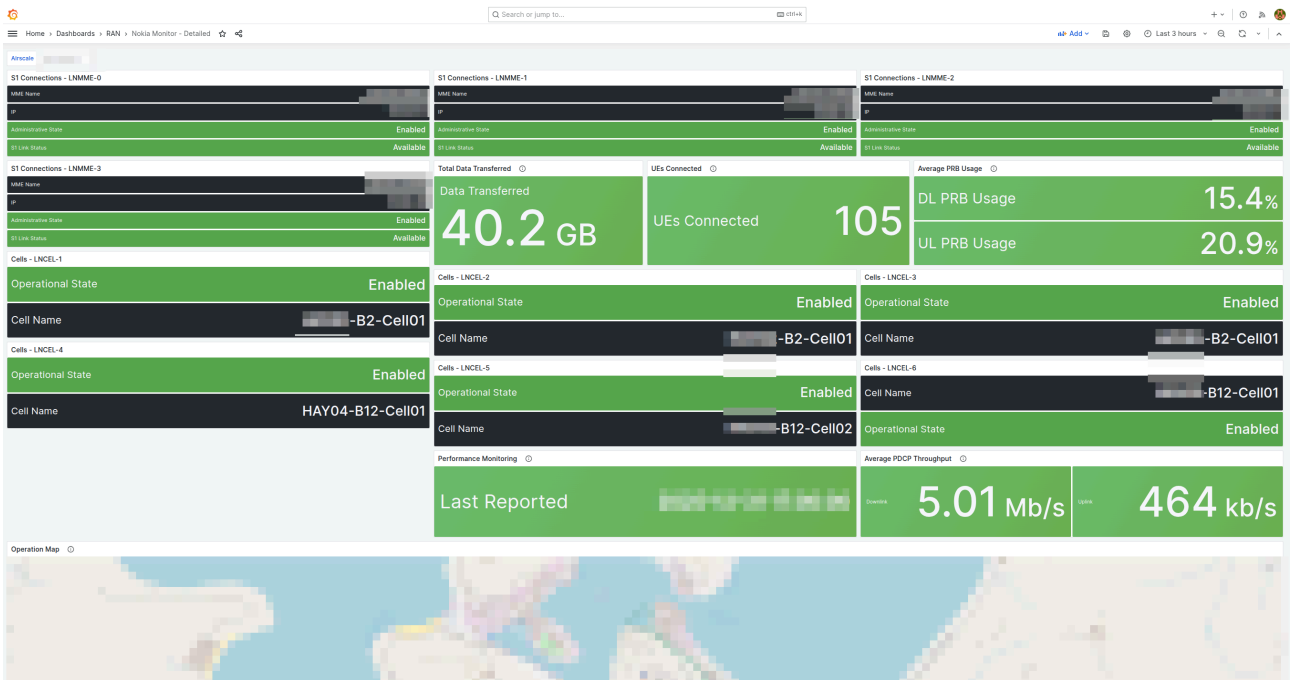
1. **Alta Utilização de PRB** - Aciona quando DL ou UL PRB > 85% por 5 minutos
2. **Baixa Disponibilidade da Célula** - Aciona quando a disponibilidade < 99% por 10 minutos
3. **Baixa Taxa de Sucesso de Configuração** - Aciona quando a taxa de sucesso de configuração RRC < 95% por 5 minutos
4. **Alto VSWR** - Aciona quando VSWR > 2.0 para qualquer antena por 15 minutos
5. **Consumo de Energia Anormal** - Aciona quando o consumo desvia > 20% da linha de base

Usando este Dashboard:

1. **Análise de Capacidade** - Monitore a utilização de PRB para identificar células se aproximando da capacidade
2. **Solução de Problemas de Desempenho** - Use RSSI, latência e taxa de sucesso de configuração para diagnosticar problemas
3. **Saúde do Hardware** - Acompanhe VSWR e consumo de energia para manutenção proativa
4. **Garantia de Qualidade** - Monitore disponibilidade e throughput para conformidade com SLA

Consulte a Referência de Contadores da Nokia para definições completas de contadores e diretrizes de uso.

Exemplo de Dashboard - Visão Detalhada:



Dashboard detalhado do monitor Nokia mostrando Conexões S1, estado operacional, dados transferidos, UEs conectados, utilização média de PRB, métricas de monitoramento de desempenho e mapa de operação geográfica.

Exemplo de Dashboard - Disponibilidade da Célula, Utilização de PRB e Throughput:

Gráficos de Disponibilidade da Célula por LNCEL, Utilização de PRB LTE por TTI para uplink/downlink, e gráficos de Throughput PDCP mostrando desempenho em várias células.

Exemplo de Dashboard - RSSI, Energia, Latência e RRC:

Gráficos de RSSI (Mínimo/Médio/Máximo), Consumo de Energia Combinado, medições de Latência, Taxa de Sucesso de Configuração RRC e gráficos de VSWR (RMOD) para várias células.

Exemplo de Dashboard - Painéis de Desempenho Adicionais:

Painéis de desempenho adicionais mostrando continuação da Taxa de Sucesso de Configuração RRC, medições de Latência, gráficos de VSWR RMOD e UEs

Conectados ao longo do tempo.

Exemplo de Dashboard - Detalhe do VSWR com Tooltip:

Gráfico detalhado de VSWR RMOD-2 mostrando medições de antena (ANTL-1, ANTL-2, ANTL-3, ANTL-4) com tooltip interativo exibindo timestamp e valores.

Solução de Problemas

Nenhum Dado Aparecendo nos Painéis

Sintomas:

- O dashboard carrega, mas os painéis mostram "Sem dados"
- A fonte de dados parece conectada

Diagnóstico:

```
1. Verifique se a consulta do InfluxDB é válida
2. Verifique se o nome da medição existe no InfluxDB
3. Verifique se o intervalo de tempo inclui pontos de dados
4. Verifique se as condições de filtro correspondem às tags de
dados
```

Solução:

- Teste a consulta diretamente na interface do InfluxDB
- Ajuste o intervalo de tempo (tente as últimas 24 horas)
- Verifique se os nomes das tags correspondem à saída do RAN Monitor
- Ative o inspetor de consultas para ver os resultados reais

Carregamento Lento do Dashboard

Sintomas:

- O dashboard leva > 5 segundos para carregar
- Os painéis aparecem um a um lentamente

Diagnóstico:

```
1. Muitos painéis (> 8)
2. Consultas muito complexas/faixa de dados grande
3. Problemas de desempenho do InfluxDB
4. Latência de rede
```

Solução:

- Reduza o número de painéis
- Limite o intervalo de tempo (24h vs. 1 ano)
- Pré-agregue dados no InfluxDB
- Verifique CPU/memória do InfluxDB
- Aumente o tempo limite da consulta

Alertas Não Disparando

Sintomas:

- A regra de alerta está habilitada
- A condição deveria ser atendida
- Nenhuma notificação recebida

Diagnóstico:

```
1. Verifique se a avaliação do alerta está acontecendo
2. Verifique se o canal de notificação está funcionando
3. Verifique a condição da regra de alerta
4. Revise os logs do canal de notificação
```

Solução:

- Teste a regra de alerta manualmente (ícone de lápis → Testar)
- Verifique o status da regra de alerta em Alerta → Regras de Alerta
- Verifique se o canal de notificação tem a URL/chave correta
- Verifique os logs do Grafana em busca de erros
- Re-teste o canal de notificação com acionamento manual

Dados Incorretos nos Dashboards

Sintomas:

- Os valores não correspondem aos números esperados
- Os dados parecem deslocados no tempo
- As agregações parecem erradas

Diagnóstico:

```
1. Verifique as configurações de fuso horário
2. Verifique a função de agregação
3. Verifique filtros de tags/rótulos
4. Revise a consulta em busca de erros matemáticos
```

Solução:

- Defina o fuso horário do dashboard para corresponder ao do InfluxDB
- Verifique a função aggregateWindow (média/soma/última)
- Teste filtros diretamente no InfluxDB
- Simplifique a consulta para isolar o problema

Problemas de Retenção de Dados

Sintomas:

- Dados históricos ausentes ou incompletos
- Consultas retornam menos dados do que o esperado
- O dashboard mostra lacunas na série temporal

Solução:

- Verifique as configurações da política de retenção em Política de Retenção de Dados
- Verifique se o período de retenção é suficiente para seu intervalo de consulta
- Ajuste a retenção por eNodeB, se necessário

Problemas de Configuração

Sintomas:

- Erros de conexão do InfluxDB
- Dados de eNodeB ausentes nas consultas
- Intervalos de coleta de dados incorretos

Solução:

- Revise o Guia de Configuração em Tempo de Execução para configurações adequadas
- Verifique se a Configuração do AirScale está correta
- Verifique o status de registro do eNodeB

Documentação Relacionada

- **Referência de Contadores da Nokia** - Definições completas de contadores de desempenho

- **Política de Retenção de Dados** - Gerenciamento do ciclo de vida e armazenamento de dados
- **Guia de Configuração em Tempo de Execução** - Configura��ão e ajuste do sistema
- **Configuração do AirScale** - Configuração e registro da estação base

Guia de Operações Comuns

Tarefas de Gerenciamento do Monitor RAN no Dia a Dia

Guia prático para tarefas operacionais de rotina e gerenciamento de dispositivos

---

Índice

Visão Geral

Este guia cobre tarefas operacionais de rotina para gerenciar o Monitor RAN nas operações do dia a dia. Esses procedimentos são projetados para equipes de NOC, administradores de rede e pessoal de operações.

Pré-requisitos

- O Monitor RAN está instalado e em execução

- Você tem acesso aos arquivos de configuração
- Você pode reiniciar o aplicativo Monitor RAN
- Você entende a topologia da sua rede

Para configuração inicial, consulte o Guia de Introdução.

Adicionando uma Nova Estação Base

Ao implantar novas estações base Nokia AirScale, siga estas etapas para adicioná-las ao monitoramento.

Etapa 1: Verificar Conectividade de Rede

Antes de adicionar o dispositivo à configuração, verifique a conectividade de rede:

```
# Testar conectividade básica
ping <base-station-ip>

# Verificar se a porta de gerenciamento está acessível
telnet <base-station-ip> 8080
```

Resultado Esperado: Respostas de ping bem-sucedidas e conexão telnet

Se Falhar:

- Verifique as rotas de rede
- Verifique se as regras do firewall permitem conectividade
- Confirme se a estação base está ligada e operacional

Etapa 2: Coletar Informações do Dispositivo

Colete as seguintes informações:

Informação	Exemplo	Onde Encontrar
Endereço IP	10.7.15.67	Documentação da rede ou etiqueta do dispositivo
Porta	8080	Normalmente 8080 para Nokia AirScale
Nome do Dispositivo	Site-B-Tower-1	Use a convenção de nomenclatura do site
Nome de Usuário	admin	Da provisão da estação base
Senha	password123	Da provisão da estação base

Melhores Práticas de Nomenclatura de Dispositivos:

- Use nomes descritivos e consistentes
- Inclua identificador do site
- Inclua tipo de equipamento se houver múltiplos no mesmo site
- Exemplos: `NYC-SiteA-BS1`, `LAX-Tower-Main`, `CHI-Indoor-DAS`

Etapa 3: Verificar Dispositivos Não Configurados

Antes de adicionar manualmente, verifique se o dispositivo já tentou se conectar:

1. Abra a interface Web: `https://<ran-monitor-ip>:9443`
2. Navegue até a página **eNodeBs Não Configurados**
3. Procure o endereço IP ou ID do Agente do seu dispositivo
4. Anote o ID do Agente se encontrado

Isso ajuda a verificar se o dispositivo pode alcançar o Monitor RAN.

Etapa 4: Adicionar Dispositivo à Configuração

Edite `config/runtime.exs` e adicione o novo dispositivo à lista `airscales`:

```
config :ran_monitor,
  nokia: %{
    ne3s: %{
      # ... configuração existente de ne3s ...
    },
    airscales: [
      # Dispositivos existentes
      %{
        address: "10.7.15.66",
        name: "Site-A-BS1",
        port: "8080",
        web_username: "admin",
        web_password: "password1"
      },

      # Novo dispositivo
      %{
        address: "10.7.15.67",          # Endereço IP da nova
estação base
        name: "Site-B-Tower-1",          # Nome descritivo
        port: "8080",                    # Porta de gerenciamento
        web_username: "admin",           # Nome de usuário do
WebLM
        web_password: "password123"      # Senha do WebLM
      }
    ]
  }
```

Importante: Certifique-se de que a sintaxe do Elixir esteja correta - vírgulas, indentação e estrutura do mapa devem estar corretas.

Etapa 5: Validar Configuração

Antes de reiniciar, valide a sintaxe da configuração:

```
elixir -c config/runtime.exs
```

Saída Esperada: Sem erros

Se Houver Erros:

- Verifique se há vírgulas ausentes
- Verifique se todas as chaves de abertura `{` e colchetes `[` estão fechados
- Certifique-se de que as strings estão devidamente entre aspas
- Verifique se a indentação é consistente

Etapa 6: Reiniciar o Monitor RAN

Reinicie o aplicativo para carregar a nova configuração:

```
# Se estiver executando em desenvolvimento
# Pressione Ctrl+C duas vezes, então:
mix phx.server

# Se estiver executando como um serviço
systemctl restart ran_monitor

# Se estiver executando via release
/path/to/ran_monitor/bin/ran_monitor restart
```

Etapa 7: Verificar Registro do Dispositivo

Após a reinicialização, verifique se o dispositivo agora está monitorado:

1. **Verifique os Logs do Aplicativo:**

   ```
   [info] Tentando registro com o dispositivo: Site-B-Tower-1
   [info] Registrado com sucesso com Site-B-Tower-1
   ```

2. **Verifique a Interface Web:**

   - Navegue até a página **Estações Base**
   - Encontre seu novo dispositivo na lista
   - O status deve ser "Associado" (verde)

- O estado de registro deve ser "Registrado"

3. **Verifique os Detalhes do Dispositivo:**
   - Clique no dispositivo
   - Verifique se as informações da sessão mostram sessão ativa
   - Confirme que o timestamp de "Último Contato" é recente
4. **Verifique o Status do InfluxDB:**
   - Navegue até a página **Status do InfluxDB**
   - Verifique se a contagem total de registros está aumentando
   - As contagens de medições devem crescer à medida que os dados são coletados

Etapa 8: Configurar Retenção de Dados (Opcional)

Se este dispositivo requer uma retenção diferente da padrão global:

1. Navegue até a página **Retenção de Dados**
2. Encontre seu novo dispositivo na lista
3. Atualize o campo "Período de Retenção" (em horas)
4. O sistema salva automaticamente

Para mais detalhes, consulte o Guia de Política de Retenção de Dados.

Etapa 9: Adicionar aos Painéis do Grafana

Atualize os painéis do Grafana para incluir o novo dispositivo:

1. Edite as variáveis do modelo do painel
2. Adicione o nome do dispositivo aos seletores suspensos
3. Crie um painel específico para o dispositivo, se necessário

Para mais detalhes, consulte o Guia de Integração do Grafana.

Removendo uma Estação Base

Ao descomissionar uma estação base, siga estas etapas para removê-la do monitoramento.

Etapa 1: Decidir sobre o Manuseio de Dados

Antes de remover, decida o que fazer com os dados históricos:

Opção A: Preservar Dados

- Desabilitar monitoramento, mas manter dados históricos
- Útil para equipamentos descomissionados, mas potencialmente retornando

Opção B: Remover Dados

- Excluir todos os dados históricos para o dispositivo
- Libera espaço de armazenamento no InfluxDB
- Irreversível - os dados não podem ser recuperados

Etapa 2: Desabilitar Dispositivo (Preservar Dados)

Para parar o monitoramento, mas manter os dados históricos:

Edite `config/runtime.exs` e localize o dispositivo na lista `airscales`. Comente ou remova:

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

  # Dispositivo descomissionado - comentado para preservar dados
  # %{
  #   address: "10.7.15.67",
  #   name: "Site-B-Tower-1",
  #   port: "8080",
  #   web_username: "admin",
  #   web_password: "password123"
  # }
]
```

Etapa 3: Remover Dados (Opcional)

Para excluir todos os dados históricos para o dispositivo:

1. Navegue até a página **Retenção de Dados** na interface Web
2. Encontre o dispositivo na lista
3. Clique no botão **Limpar Todos os Dados**
4. Confirme a ação

Aviso: Isso é permanente e não pode ser desfeito.

Etapa 4: Reiniciar o Monitor RAN

Reinicie o aplicativo para aplicar as alterações de configuração:

```
systemctl restart ran_monitor
# ou
mix phx.server
```

Etapa 5: Verificar Remoção

Após a reinicialização:

1. **Verifique a Página de Estações Base:**
    - O dispositivo não deve mais aparecer na lista ativa
    - Se os dados foram preservados, o dispositivo pode ainda aparecer em consultas históricas
2. **Verifique os Logs do Aplicativo:**
    - Nenhuma tentativa de registro para o dispositivo removido
    - Nenhum erro sobre dispositivo ausente
3. **Verifique o InfluxDB:**
    - Se os dados foram excluídos, as contagens de registros devem estar mais baixas
    - O dispositivo não deve aparecer em novas métricas

Etapa 6: Atualizar Painéis do Grafana

Remova o dispositivo das configurações do Grafana:

1. Edite as variáveis do modelo do painel
2. Remova o nome do dispositivo dos seletores
3. Exclua painéis específicos do dispositivo, se existirem

Atualizando Credenciais do Dispositivo

Quando as senhas das estações base são alteradas, atualize a configuração do Monitor RAN.

Etapa 1: Anotar o Status Atual

Antes de fazer alterações:

1. Verifique se o dispositivo está atualmente conectado (status verde)
2. Anote as informações da sessão atual
3. Tire uma captura de tela ou registre o estado atual para comparação

Etapa 2: Atualizar Configuração

Edite `config/runtime.exs` e atualize as credenciais:

```
airscales: [
  %{
    address: "10.7.15.66",
    name: "Site-A-BS1",
    port: "8080",
    web_username: "admin",
    web_password: "new_password_here"  # Senha atualizada
  }
]
```

Etapa 3: Reiniciar o Monitor RAN

Aplique a alteração de configuração:

```
systemctl restart ran_monitor
```

Etapa 4: Verificar Reconexão

Após a reinicialização:

1. **Verifique os Logs do Aplicativo:**

   ```
   [info] Tentando registro com o dispositivo: Site-A-BS1
   [info] Registrado com sucesso com Site-A-BS1
   ```

2. **Verifique a Interface Web:**
    - O status do dispositivo deve ser "Associado" (verde)
    - Uma nova sessão deve ser estabelecida
    - "Último Contato" deve ser recente

Se o Dispositivo Não Conectar:

- Verifique se as novas credenciais estão corretas
- Verifique se há erros de digitação na senha
- Confirme se as credenciais funcionam diretamente na estação base
- Revise os logs do aplicativo para erros de autenticação

Ajustando Intervalos de Coleta

Altere com que frequência o Monitor RAN coleta dados das estações base.

Entendendo Intervalos de Coleta

O Monitor RAN coleta três tipos de dados em diferentes intervalos:

Tipo de Dado	Intervalo Padrão	Configurável	Impacto de Intervalo Mais Curto
Métricas de Desempenho	10 segundos	Sim	Dados mais granulares, maior uso de rede/armazenamento
Alarmes	10 segundos	Sim	Detecção de alarmes mais rápida, mais consultas
Configuração	60 segundos	Sim	Capturas de configuração mais frequentes, mais armazenamento
Verificações de Saúde	30 segundos	Sim	Mais responsivo a problemas de conectividade

Quando Ajustar Intervalos

Acurtar Intervalos (Mais Frequente):

- Solucionando problemas ativos
- Infraestrutura crítica de alto valor
- Monitoramento de SLA com requisitos rigorosos
- Testes e análises de capacidade

Alongar Intervalos (Menos Frequente):

- Reduzir tráfego de rede
- Reduzir uso de armazenamento do InfluxDB
- Ambientes de teste de baixa prioridade
- Links com largura de banda limitada

Etapa 1: Modificar Configuração

Os intervalos de coleta são configurados no código do aplicativo, não em runtime.exs. Para alterá-los, você precisará modificar o código-fonte e recompilar.

Exemplos de locais (podem variar por versão):

- Métricas de desempenho: `lib/ran_monitor/nokia/airscale/manager.ex`
- Alarmes: `lib/ran_monitor/nokia/airscale/manager.ex`
- Configuração: `lib/ran_monitor/nokia/airscale/manager.ex`

Nota: Entre em contato com o suporte da Omnitouch para assistência com alterações nos intervalos de coleta, pois isso requer modificações no código-fonte.

Etapa 2: Considerar Impacto

Antes de alterar os intervalos:

Impacto na Rede:

- Calcule: dispositivos × contadores × intervalo = consultas por segundo
- Intervalos mais curtos = mais tráfego de rede
- Certifique-se de que a rede pode suportar a carga aumentada

Impacto no Armazenamento:

- Calcule: pontos de dados por dia × período de reten��ão = armazenamento total
- Exemplo: intervalo de 10s = 8.640 medições/dia por contador
- Certifique-se de que o InfluxDB tenha espaço em disco suficiente

Desempenho do Sistema:

- Polling mais frequente = maior uso de CPU no Monitor RAN
- Monitore os recursos do sistema após as alterações

Etapa 3: Monitorar Após Mudanças

Após ajustar os intervalos:

1. **Observe os Logs do Aplicativo** para quaisquer erros
2. **Monitore os Recursos do Sistema:**
   - Uso de CPU no servidor do Monitor RAN
   - Utilização de largura de banda da rede
   - I/O de disco e crescimento de armazenamento do InfluxDB
3. **Verifique a Qualidade dos Dados:**
   - Verifique o InfluxDB para a frequência de medições esperada
   - Verifique se não há lacunas nos dados
4. **Ajuste se Necessário:**
   - Reverta se o sistema estiver sobrecarregado
   - Ajuste com base no desempenho observado

Gerenciando Configuração do Dispositivo

Como gerenciar com segurança as configurações das estações base através do Monitor RAN.

Fluxo de Trabalho de Configuração

Para procedimentos detalhados de gerenciamento de configuração, consulte o Guia da Interface Web - Gerenciamento de Configuração.

Referência Rápida:

1. **Baixar** a configuração atual (backup)
2. **Modificar** a configuração offline
3. **Carregar** nova configuração – obter ID do Plano
4. **Validar** configuração usando o ID do Plano
5. **Ativar** se a validação for bem-sucedida

6. **Verificar** se as mudanças tiveram efeito

Melhores Práticas

Sempre Baixe Primeiro:

- Mantenha um backup da configuração atual
- Permite reverter se necessário
- Documenta a configuração antes da mudança

Valide Antes de Ativar:

- Nunca ative sem validar
- A validação captura erros de sintaxe
- Prevê interrupções no serviço

Agende Mudanças Apropriadamente:

- Use janelas de manutenção quando possível
- Evite horários de pico
- Tenha um plano de reversão pronto

Documente Mudanças:

- Registre o que foi alterado e por quê
- Anote o ID do Plano para rastreamento
- Documente os resultados da verificação
- Atualize o sistema de gerenciamento de mudanças

Monitore Após Mudanças:

- Observe alarmes
- Verifique se as métricas se normalizam
- Verifique a estabilidade do dispositivo por 15-30 minutos
- Esteja preparado para reverter se ocorrerem problemas

Monitorando a Saúde do Sistema

Verificações de rotina para garantir que o Monitor RAN esteja operando corretamente.

Verificação de Saúde Diária

Realize essas verificações no início de cada turno:

1. Acesse o Painel da Interface Web

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

2. Revise o Status do Sistema

- Todos os dispositivos estão mostrando status verde (associado)?
- Algum dispositivo vermelho (falhado) requer investigação?
- A contagem de alarmes é razoável para a hora do dia?

3. Verifique o Resumo de Alarmes

- Algum alarme crítico ativo?
- A taxa de alarmes está aumentando ou diminuindo?
- Algum alarme repetido indicando problemas sistêmicos?

4. Verifique a Coleta de Dados

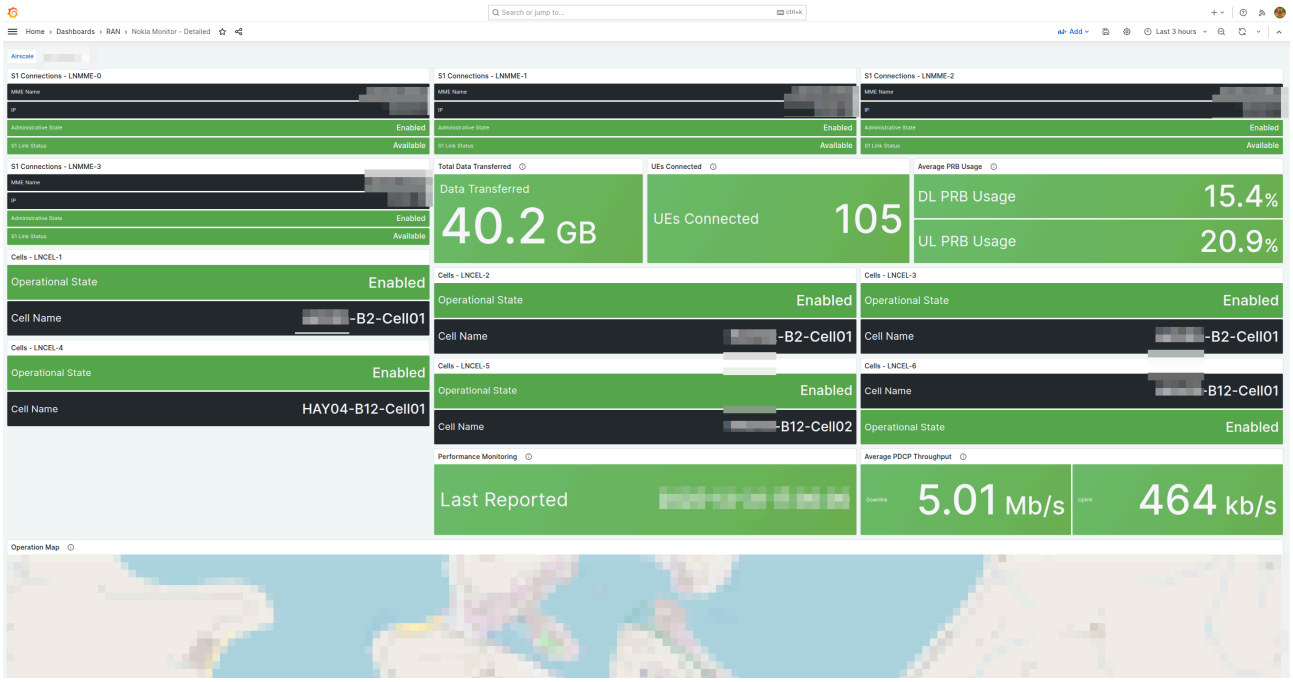
- Navegue até a página de Status do InfluxDB
- As contagens de medições estão aumentando?
- O timestamp da última atualização é recente?

5. Revise os Logs Recentes

- Navegue até a página de Logs do Aplicativo
- Filtre por nível "Erro"
- Algum erro recorrente?

Para procedimentos detalhados de verificação de saúde, consulte o Guia da Interface Web - Fluxos de Trabalho da Interface Web.

Exemplo: Painel de Monitoramento do Grafana



Painel de monitoramento abrangente mostrando o status das conexões S1 por LNMME, estado operacional, dados transferidos, UEs conectados, uso médio de PRB, métricas de monitoramento de desempenho e mapa de cobertura geográfica. Este painel fornece visibilidade instantânea sobre a saúde da rede e o status do dispositivo.

Revisão Semanal do Sistema

Verificação mais detalhada realizada semanalmente:

1. Revise Tendências de Alarmes

- Use o Grafana para analisar a taxa de alarmes na última semana
- Identifique tempestades de alarmes ou padrões
- Correlacione com manutenção ou mudanças

2. Verifique o Crescimento do Armazenamento

- Tendência de uso de disco do InfluxDB

- Tamanho do banco de dados MySQL
- Tamanhos dos arquivos de log do aplicativo

3. Revise a Conectividade do Dispositivo

- Algum dispositivo com desconexões frequentes?
- Problemas de tempo limite de sessão?
- Padrão de problemas de conectividade?

4. Utilização de Recursos do Sistema

- Uso de CPU no servidor do Monitor RAN
- Tendências de uso de memória
- Consumo de largura de banda da rede

5. Mudanças de Configuração

- Revise todas as mudanças de configuração feitas
- Verifique se as mudanças foram documentadas
- Correlacione com quaisquer problemas

Tempo Necessário: 30-45 minutos

Gerenciamento de Dados

Gerenciando Retenção de Dados

Consulte o Guia de Política de Retenção de Dados para detalhes completos.

Referência Rápida:

Verificar Retenção Atual:

- Navegue até a página de Retenção de Dados
- Verifique a configuração padrão global e por dispositivo

Ajustar Período de Retenção:

- Atualize as horas de retenção para um dispositivo específico
- Ou modifique o padrão global em `config/config.exs`

Limpar Dados Antigos:

- Limpeza manual: Clique no botão "Limpar Dados Antigos"
- A limpeza automática é executada a cada hora

Planejamento de Armazenamento:

- Monitore o uso de disco do InfluxDB semanalmente
- Ajuste a retenção com base no armazenamento disponível
- Equilibre o período de retenção com a capacidade de armazenamento

Exportando Dados

Exportar Configurações do Dispositivo:

1. Navegue até a página de detalhes do dispositivo
2. Clique em "Baixar Configuração"
3. Salve o arquivo XML em um local seguro
4. Rotule com o nome do dispositivo e a data

Exportar Métricas (via InfluxDB):

```
# Exportar dados para dispositivo específico
influx -database 'nokia-monitor' -execute '
  SELECT * FROM PerformanceMetrics
  WHERE basebandName='''Site-A-BS1'''
  AND time > now() - 7d
' -format csv > export.csv
```

Exportar via Grafana:

- Abra o painel
- Selecione o intervalo de tempo

- Clique em "Compartilhar" – "Exportar" – "CSV"

Backup e Recuperação

Backups Regulares

O que Fazer Backup:

1. Arquivos de Configuração

```
# Backup da configuração em tempo de execução
cp config/runtime.exs backups/runtime.exs.$(date +%Y%m%d)

# Backup de todo o diretório de configuração
tar -czf backups/config-$(date +%Y%m%d).tar.gz config/
```

2. Configurações do Dispositivo

- Baixe as configurações de todos os dispositivos via Interface Web
- Armazene em controle de versão ou local de backup
- Realize semanalmente ou antes/depois de mudanças

3. Banco de Dados MySQL

```
# Backup do banco de dados de estado da sessão
mysqldump -u ran_monitor_user -p ran_monitor >
backups/ran_monitor-$(date +%Y%m%d).sql
```

4. Dados do InfluxDB

```
# Backup do InfluxDB 1.x
influxd backup -portable -database nokia-monitor
/backups/influx-$(date +%Y%m%d)

# Backup do InfluxDB 2.x
influx backup /backups/influx-$(date +%Y%m%d)
```

5. Certificados SSL

```
cp priv/cert/* backups/certificates-$(date +%Y%m%d)/
```

Cronograma de Backup

Diário:

- Banco de dados MySQL (estado da sessão)
- Arquivos de configuração se alterados

Semanal:

- Dados do InfluxDB (ou por política de retenção)
- Configurações dos dispositivos de todas as estações base

Antes de Mudanças:

- Arquivos de configuração
- Configurações do dispositivo
- Snapshot do banco de dados

Processo de Recuperação

Recuperar de Erro de Configuração:

1. Pare o Monitor RAN

   ```
   systemctl stop ran_monitor
   ```

2. Restaure o arquivo de configuração

```
cp backups/runtime.exs.20251230 config/runtime.exs
```

3. Valide a configuração

```
elixir -c config/runtime.exs
```

4. Reinicie o Monitor RAN

```
systemctl start ran_monitor
```

5. Verifique se os dispositivos se reconectam

Recuperar de Perda de Banco de Dados:

1. Pare o Monitor RAN

```
systemctl stop ran_monitor
```

2. Restaure o banco de dados MySQL

```
mysql -u ran_monitor_user -p ran_monitor < backups/ran_monitor-
20251230.sql
```

3. Reinicie o Monitor RAN

```
systemctl start ran_monitor
```

4. Os dispositivos se registrarão automaticamente

5. A coleta de novas métricas começa

6. Os dados históricos permanecem no InfluxDB

Recuperar de Perda Completa do Sistema:

1. Reinstale o Monitor RAN em um novo servidor
2. Restaure os arquivos de configuração
3. Restaure o banco de dados MySQL
4. Restaure os dados do InfluxDB
5. Restaure os certificados SSL
6. Inicie o Monitor RAN
7. Verifique se todos os dispositivos se reconectam
8. Verifique se os dados históricos estão acessíveis

Manutenção do Sistema

Tarefas de Manutenção de Rotina

Mensal:

1. Revisar Logs

- Arquivar logs antigos do aplicativo
- Verificar erros ou avisos recorrentes
- Limpar arquivos de log para liberar espaço em disco

2. Atualizar Documentação

- Documentar quaisquer mudanças de configuração
- Atualizar diagramas de rede se a topologia mudar
- Revisar e atualizar procedimentos operacionais

3. Atualizações de Segurança

- Aplicar patches de segurança do SO
- Atualizar software de banco de dados se necessário
- Rotacionar senhas conforme a política de segurança

4. Revisão de Desempenho

- Analisar tendências de recursos do sistema
- Identificar qualquer degradação de desempenho
- Planejar atualizações de capacidade se necessário

Trimestral:

1. Teste de Recuperação de Desastre

- Testar o processo de restauração de backup
- Verificar se os procedimentos de recuperação funcionam
- Atualizar a documentação de recuperação de desastre

2. Auditoria de Segurança

- Revisar logs de acesso
- Verificar permissões de usuários
- Atualizar certificados SSL se estiverem prestes a expirar

3. Planejamento de Capacidade

- Revisar tendências de crescimento de armazenamento
- Prever necessidades futuras de capacidade
- Planejar atualizações de hardware se necessário

Anualmente:

1. Renovação de Certificado SSL

- Substituir certificados SSL prestes a expirar
- Testar novos certificados antes da expiração

2. Rotação de Senhas

- Atualizar todas as credenciais das estações base
- Atualizar senhas do banco de dados
- Atualizar tokens da API

3. Atualização do Sistema

- Planejar atualização da versão do Monitor RAN
- Testar em ambiente de staging
- Agendar atualização em produção

Janelas de Manutenção

Planejando uma Janela de Manutenção:

1. **Agendar Durante Tráfego Baixo:**
    - Noites ou fins de semana geralmente são melhores
    - Evitar horários de pico identificados no Grafana
2. **Notificar Stakeholders:**
    - Informar a equipe de operações
    - Atualizar a página de status
    - Definir expectativas para o tempo de inatividade
3. **Preparar Plano de Reversão:**
    - Fazer backup do estado atual
    - Documentar etapas de reversão
    - Ter a versão anterior pronta se estiver atualizando
4. **Executar Manutenção:**
    - Seguir procedimentos documentados
    - Monitorar o progresso de perto
    - Documentar quaisquer desvios
5. **Verificar Saúde do Sistema:**
    - Todos os dispositivos se reconectam
    - Métricas fluindo normalmente
    - Sem erros nos logs
    - Executar procedimentos de verificação de saúde

6. **Documentar Resultados:**
    - Registrar o que foi feito
    - Anotar quaisquer problemas encontrados
    - Atualizar procedimentos se necessário

Documentação Relacionada

- **Guia de Introdução** - Procedimentos de configuração inicial
- **Guia da Interface Web** - Guia do usuário do painel de controle
- **Guia de Configuração em Tempo de Execução** - Referência de configuração
- **Configuração do AirScale** - Configuração da estação base
- **Gerenciamento de Firmware** - Repositório de pacotes de software e atualizações
- **Guia de Integração do Grafana** - Análises e painéis
- **Guia de Gerenciamento de Alarmes** - Procedimentos de manuseio de alarmes
- **Guia de Política de Retenção de Dados** - Gerenciamento do ciclo de vida dos dados
- **Guia de Solução de Problemas** - Resolução de problemas
- **Guia de Operações** - Visão geral operacional completa

Referência de Contadores de Desempenho LTE da Nokia

Guia abrangente para medições de desempenho do Nokia AirScale/FlexiRadio

---

Índice

Visão Geral

As estações base LTE da Nokia (AirScale, FlexiRadio) relatam dados de desempenho usando um sistema de contadores estruturado. Cada contador mede um aspecto específico do desempenho da rede, desde a utilização de recursos até a qualidade do rádio.

O que são Contadores de Desempenho?

Contadores de desempenho são medições numéricas coletadas pela estação base em intervalos regulares. Eles fornecem visibilidade sobre:

- Quão ocupada está a rede (utilização de recursos)
- Quão bem ela está funcionando (taxa de transferência, qualidade)
- Quantos usuários estão conectados (carga)
- Se os serviços estão disponíveis (disponibilidade)
- Qualidade do sinal e condições de rádio

Grupos de Medição

Os contadores são organizados em grupos de medição, cada um cobrindo uma área funcional específica. O conjunto completo de contadores LTE da Nokia inclui os seguintes grupos de medição:

Medições de Desempenho Central (M8xxx)

Medição	Categoria	Contagem de Contadores	Foco Principal
M8000	Interface S1	33	Configuração inicial de contexto configuração/reset do S1, conte do UE
M8001	Desempenho da Célula	336	Atraso do PDCP, RACH, blocos d transporte, distribuição do MCS
M8004	Interface X2	4	Volume de dados X2, tráfego int eNB
M8005	Qualidade do Rádio	237	RSSI, SINR, condições de rádio, AMC
M8006	Portadora EPS	54	Configuração/modificação/libera da portadora
M8007	Portadora de Dados de Rádio	14	Estabelecimento e gerenciamer do DRB
M8008	Rejeição de Conexão RRC	14	Razões e estatísticas de rejeiçã conexão
M8009	Preparação de Transferência	8	Falhas na preparação de HO
M8010	Distribuição de CQI	27	Estatísticas do Indicador de Qualidade de Canal
M8011	Utilização de Recursos	55	Uso de PRB, alocação de recurs

Medição	Categoria	Contagem de Contadores	Foco Principal
M8012	Taxa de Transferência	121	Taxas de dados do PDCP, estatísticas de volume
M8013	Conexão de Sinalização	21	Tentativas/sucessos de configuração de conexão RRC
M8014	Transferência Inter-eNB	14	Procedimentos de transferência baseados em X2
M8015	Transferência Intra-eNB	13	Transferências internas de célul
M8016	Retorno de CS	18	Procedimentos de retorno de circuito
M8017	HO Inter-Sistema	10	Transferência para outras RATs (3G/2G)
M8018	Carga do eNB	8	Contagens de UE ativas, estatísticas de carga
M8019	NACC	4	Mudança de Célula Assistida pe Rede
M8020	Disponibilidade da Célula	7	Estado da célula e amostragem disponibilidade
M8021	Transferência Inter-Frequência	17	Procedimentos de transferência inter-frequência
M8022	Configuração X2	2	Estabelecimento da interface X

Medição	Categoria	Contagem de Contadores	Foco Principal
M8023	Volume de Dados	36	Volume de SDU do PDCP na interface aérea

Medições de Interface de Rede (M5xxx)

Medição	Categoria	Contagem de Contadores	Foco Principal
M5112	Entrada de Interface IP	112	Estatísticas de pacotes recebidos, métricas de interface
M5113	RX Ethernet	21	Estatísticas de pacotes Ethernet recebidos

Medições de Hardware (M4xxxx)

Medição	Categoria	Contagem de Contadores	Foco Principal
M40001	Hardware de Rádio	Variável	VSWR, saúde da antena, métricas de RF
M40002	Consumo de Energia	Variável	Uso de energia da estação base

---

Convenção de Nomenclatura de Contadores

Os contadores da Nokia seguem um formato de nomenclatura padrão:

```
M<medição><tipo>C<contador>
```

Exemplo: M8011C24

- **M** - Prefixo fixo indicando "Medição"
- **8011** - Grupo de medição (Recurso da Célula)
- **C** - Separador fixo indicando "Contador"
- **24** - Contador específico dentro do grupo (utilização média de PRB UL)

Tipos Lógicos

Cada contador tem um tipo lógico que determina como ele agrega dados:

- **Soma** - Contagem cumulativa de eventos
- **Média** - Valor médio durante o período de medição
- **Mínimo** - Valor mínimo observado
- **Máximo** - Valor máximo observado
- **Atual** - Valor amostrado atual
- **Denominador** - Usado para cálculos de razão

Categorias de Contadores

Por Área Funcional

Planejamento de Capacidade:

- M8011Cxx - Utilização de PRB
- M8018Cxx - Contagens de UE ativas

- M8012Cxx - Taxas de transferência

Monitoramento de Desempenho:

- M8001Cxx - Latência e atraso
- M8005Cxx - RSSI, SINR
- M8013Cxx - Taxas de sucesso de configuração

Rastreamento de Disponibilidade:

- M8020Cxx - Disponibilidade da célula
- M8049Cxx - Status da conexão

Solução de Problemas:

- M8005Cxx - Problemas de qualidade de rádio
- M8001Cxx - Problemas de fila
- M8013Cxx - Falhas de configuração

Contadores de Utilização de Recursos

M8011 - Medições de Recursos da Célula

Esses contadores rastreiam a utilização do Bloco de Recursos Físicos (PRB), que indica quão ocupados estão os recursos de rádio da célula.

Contador	Nome	Descrição	Unidade	Tipo	Escala
M8011C24	Utilização média de PRB UL por TTI	Uso médio de PRB uplink por Intervalo de Tempo de Transmissão	0.1%	Média	Dividir por 10 para porcentagem
M8011C37	Utilização média de PRB DL por TTI	Uso médio de PRB downlink por Intervalo de Tempo de Transmissão	0.1%	Média	Dividir por 10 para porcentagem

Entendendo a Utilização de PRB:

- **Blocos de Recursos Físicos (PRBs)** são as menores unidades de alocação de recursos de rádio em LTE
- **TTI (Intervalo de Tempo de Transmissão)** = 1 milissegundo em LTE
- Maior utilização = célula mais ocupada (mais tráfego)
- 100% de utilização indica que a célula está na capacidade máxima

Faixas de Valor:

- 0-1000 (representa 0.0% a 100.0%)
- Dividir o valor do contador por 10 para obter a porcentagem
- Exemplo: Valor do contador 453 = 45.3% de utilização de PRB

Uso no Planejamento de Capacidade:

- < 50% - Célula tem capacidade sobrando
- 50-70% - Célula normalmente carregada
- 70-85% - Pesadamente carregada, monitorar para congestionamento
- > 85% - Perto da capacidade, considerar adicionar setores/carriers

Exemplo de Consulta 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}))  //
Converter para porcentagem
```

Contadores de Taxa de Transferência

M8012 - Medições de Taxa de Transferência da Célula

Esses contadores medem a taxa de transferência da camada PDCP (Protocolo de Convergência de Dados de Pacote), indicando as taxas reais de transferência de dados do usuário.

Contador	Nome	Descrição	Unidade	Tipo	Gatilho Atualiza
M8012C23	Taxa de Transferência PDCP UL Média	Taxa média de transferência PDCP uplink	kbit/s	Média	Quando S PDCP recebido UE
M8012C26	Taxa de Transferência PDCP DL Média	Taxa média de transferência PDCP downlink	kbit/s	Média	Quando S PDCP transmiti para UE

Entendendo a Taxa de Transferência PDCP:

- A camada **PDCP** é onde os pacotes de dados do usuário são processados
- A taxa de transferência é medida em quilobits por segundo (kbit/s)
- Representa a taxa real de transferência de dados para o tráfego do usuário
- Atualizada a cada segundo

Cálculo da Taxa de Transferência:

- Medida como média durante um intervalo de amostragem de 1 segundo
- Considera todos os usuários ativos na célula
- Inclui tanto portadoras VoLTE quanto de dados

Referências de Desempenho:

Downlink (M8012C26):

- < 10 Mbps - Tráfego baixo / poucos usuários
- 10-50 Mbps - Tráfego moderado
- 50-100 Mbps - Tráfego alto / muitos usuários ativos
- > 100 Mbps - Tráfego de pico (depende da largura de banda da célula)

Uplink (M8012C23):

- < 5 Mbps - Tráfego baixo
- 5-20 Mbps - Tráfego moderado
- 20-40 Mbps - Tráfego alto
- > 40 Mbps - Tráfego de pico

Exemplo de Consulta Grafana:

```
from(bucket: "nokia-monitor")
  |> range(start: -1h)
  |> filter(fn: (r) => r["metricCounter"] == "M8012C26")
  |> filter(fn: (r) => r._field == "counterValue")
  |> map(fn: (r) => ({ r with _value: r._value / 1000.0}))  //
Converter para Mbps
```

Contadores de Atividade do UE

M8018 - Medições de Carga do eNB

Esses contadores rastreiam o número de dispositivos de Equipamento do Usuário (UE) ativos conectados à estação base.

Contador	Nome	Descrição	Unidade	Tipo	Intervalo de Atualização
M8018C1	Máximo de UE Ativas por eNB	Número máximo de UEs ativas por eNodeB	Inteiro	Máx	1 segundo

Entendendo a Atividade do UE:

- **UE Ativo** = Um dispositivo com pelo menos um Portadora de Sinalização de Rádio (SRB) e uma Portadora de Dados de Rádio (DRB)
- Valor máximo observado durante períodos de amostragem de 1 segundo
- Indica a carga máxima de usuários concorrentes

Níveis de Carga:

UEs Ativos	Nível de Carga	Recomendação
0-50	Baixo	Operação normal
50-100	Moderado	Monitorar capacidade
100-150	Alto	Avaliar adição de capacidade
> 150	Muito Alto	Expansão de capacidade necessária

Notas:

- A capacidade real depende da configuração de hardware da estação base
- O Nokia AirScale pode normalmente suportar de 150 a 250 UEs ativos concorrentes por célula
- Contagens altas de UE podem impactar a taxa de transferência por usuário

---

Contadores de Disponibilidade da Célula

M8020 - Medições de Disponibilidade da Célula

Esses contadores calculam a porcentagem de disponibilidade da célula amostrando o estado da célula em intervalos regulares.

Contador	Nome	Descrição	Unidade	Tipo
M8020C3	Amostras quando a célula está disponível	Contagem de amostras quando a célula estava disponível	Inteiro	Soma
M8020C4	Amostras quando a célula está planejada como indisponível	Contagem de amostras quando a célula estava em manutenção planejada	Inteiro	Soma
M8020C6	Denominador de disponibilidade da célula	Número total de amostras de verificação de disponibilidade	Inteiro	Denominador

Calculando a Disponibilidade da Célula:

```
Disponibilidade da Célula % = 100.0 × M8020C3 / (M8020C6 - M8020C4)
```

Explicação da Fórmula:

- **M8020C3** - Amostras quando a célula estava operando normalmente
- **M8020C6** - Total de amostras coletadas
- **M8020C4** - Amostras de inatividade planejada (excluídas do cálculo)

Metas de Disponibilidade:

Disponibilidade	Grau	Status
> 99.9%	Excelente	Atendendo SLA de nível de operador
99.0-99.9%	Bom	Operações normais
95.0-99.0%	Justo	Investigar problemas
< 95.0%	Ruim	Crítico - ação imediata necessária

Exemplo de Consulta 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,
      "Disponibilidade da Célula": 100.0 * r.M8020C3 / (r.M8020C6
- r.M8020C4)
    }))
```

Contadores de Qualidade de Rádio

M8005 - Medições de Qualidade de Rádio

Esses contadores medem o Indicador de Força de Sinal Recebido (RSSI) e a Relação Sinal/Ruído e Interferência (SINR), fornecendo informações sobre as condições de rádio.

Medições de RSSI

Contador	Nome	Descrição	Unidade	Tipo
M8005C0	RSSI para PUCCH Mínimo	RSSI mínimo no Canal de Controle de Uplink Físico	dBm	Mín
M8005C1	RSSI para PUCCH Máximo	RSSI máximo no Canal de Controle de Uplink Físico	dBm	Máx
M8005C2	RSSI para PUCCH Médio	RSSI médio no Canal de Controle de Uplink Físico	dBm	Média

Entendendo o RSSI:

- **RSSI** = Indicador de Força de Sinal Recebido (potência total recebida)
- **PUCCH** = Canal de Controle de Uplink Físico (transporta informações de controle)
- Medido em dBm (decibel-miliwatts)
- Atualizado quando os valores de RSSI relacionados ao UE são calculados

Interpretação dos Valores de RSSI:

Faixa de RSSI	Qualidade	Descrição
> -70 dBm	Excelente	Sinal muito forte
-70 a -85 dBm	Bom	Sinal forte, bom desempenho
-85 a -100 dBm	Justo	Sinal adequado
-100 a -110 dBm	Ruim	Sinal fraco, problemas potenciais
< -110 dBm	Muito Ruim	Sinal muito fraco, problemas prováveis

Casos de Uso:

- **Análise de cobertura** - RSSI baixo indica lacunas de cobertura
- **Solução de problemas de interferência** - Padrões de RSSI inesperados
- **Planejamento de RF** - Validar previsões de força de sinal

---

Contadores de Gerenciamento de Conexão

M8013 - Estabelecimento de Conexão de Sinalização

Esses contadores rastreiam tentativas e sucessos de configuração de conexão RRC (Controle de Recursos de Rádio), indicadores-chave de acessibilidade da rede.

Contador	Nome	Descrição	Unidade	Tipo
M8013C5	Conclusões de Estabelecimento de Conexão de Sinalização	Configurações de conexão RRC bem-sucedidas	Inteiro	Soma
M8013C17	Tentativas de Estabelecimento de Conexão de Sinalização MO-S	Tentativas de conexão - Sinalização Originada pelo Móvel	Inteiro	Soma
M8013C18	Tentativas de Estabelecimento de Conexão de Sinalização MT	Tentativas de conexão - Terminado pelo Móvel	Inteiro	Soma
M8013C19	Tentativas de Estabelecimento de Conexão de Sinalização MO-D	Tentativas de conexão - Dados Originados pelo Móvel	Inteiro	Soma
M8013C21	Tentativas de Estabelecimento de Conexão de Sinalização de Emergência	Tentativas de conexão de chamadas de emergência	Inteiro	Soma
M8013C31	Tentativas de Estabelecimento de Conexão de Sinalização de Alta Prioridade	Tentativas de conexão de alta prioridade	Inteiro	Soma
M8013C34	Tentativas de Estabelecimento de	Tentativas de conexão	Inteiro	Soma

Contador	Nome	Descrição	Unidade	Tipo
	Conexão de Sinalização Tolerantes a Atraso	tolerantes a atraso		
M8013C91	Tentativas de Estabelecimento de Conexão de Sinalização MO-V	Tentativas de conexão - Voz Originada pelo Móvel	Inteiro	Soma
M8013C93	Tentativas de Estabelecimento de Conexão de Sinalização MT-Access	Tentativas de conexão - Acesso MT	Inteiro	Soma

Calculando a Taxa de Sucesso de Configuração:

```
Taxa de Sucesso de Configuração % = 100.0 × M8013C5 / (M8013C17 + M8013C18 + M8013C19 + M8013C34 + M8013C31 + M8013C21 + M8013C93 + M8013C91)
```

Explicação da Fórmula:

- **M8013C5** - Conclusões bem-sucedidas (Configuração de Conexão RRC Completa recebida)
- **Soma dos contadores de tentativas** - Total de tentativas de conexão em todas as categorias

Tipos de Conexão:

- **MO-S (M8013C17)** - Sinalização Originada pelo Móvel (SMS, atualizações de localização)
- **MT (M8013C18)** - Terminado pelo Móvel (chamadas/dados recebidos)
- **MO-D (M8013C19)** - Dados Originados pelo Móvel (sessões de dados)
- **MO-V (M8013C91)** - Voz Originada pelo Móvel (chamadas VoLTE)

- **Emergência (M8013C21)** - Chamadas de emergência (911, 112)

Metas de Desempenho:

Taxa de Sucesso	Grau	Status
> 99%	Excelente	Operação normal
95-99%	Bom	Desempenho aceitável
90-95%	Justo	Investigação recomendada
< 90%	Ruim	Problema crítico - solucionar imediatamente

Causas Comuns de Falhas:

- Problemas de cobertura (sinal fraco)
- Congestionamento (célula na capacidade)
- Erros de configuração
- Problemas de hardware
- Interferência

Contadores de Latência e QoS

M8001 - Medições de Desempenho da Célula

Contador	Nome	Descrição	Unidade	Tipo
M8001C2	Atraso do SDU PDCP no DL DTCH Médio	Tempo médio de retenção do SDU PDCP downlink na eNB	ms	Média

Entendendo a Latência:

- **SDU PDCP** = Unidade de Dados de Serviço do Protocolo de Convergência de Dados de Pacote (pacote de dados do usuário)
- **Atraso** = Tempo que o pacote passa na estação base antes da transmissão
- **DL DTCH** = Canal de Tráfego Dedicado Downlink (canal de dados do usuário)
- Valores mais baixos = melhor capacidade de resposta

Metas de Latência:

Latência	Grau	Impacto na Aplicação
< 10 ms	Excelente	Ideal para VoLTE, jogos, chamadas de vídeo
10-20 ms	Bom	Aceitável para a maioria das aplicações
20-50 ms	Justo	Notável em aplicativos interativos
> 50 ms	Ruim	Impacta aplicações em tempo real

Causas de Alta Latência:

- Congestionamento de filas (muitos usuários)
- Problemas de configuração do agendador
- Condições de rádio ruins (muitas retransmissões)
- Atrasos na conexão de backhaul

Contadores da Interface S1

M8000 - Medições da Interface S1

Esses contadores rastreiam a interface S1 entre o eNodeB e o MME (Entidade de Gerenciamento de Mobilidade), incluindo configuração de contexto, gerenciamento de conexão S1 e procedimentos de sinalização.

Contador	Nome	Descrição	Unidade	Tipo
M8000C0	Solicitações de Configuração de Contexto Inicial	Número de tentativas de Configuração de Contexto Inicial	Inteiro	Soma
M8000C1	Conclusões de Configuração de Contexto Inicial	Configurações de Contexto Inicial bem-sucedidas	Inteiro	Soma
M8000C2	Falhas de Configuração - Rede de Rádio	Falhas devido a problemas na rede de rádio	Inteiro	Soma
M8000C3	Falhas de Configuração - Transporte	Falhas devido a problemas na camada de transporte	Inteiro	Soma
M8000C6	Solicitações de Configuração S1	Tentativas de estabelecimento da interface S1	Inteiro	Soma
M8000C7	Conclusões de Configuração S1	Configurações S1 bem-sucedidas	Inteiro	Soma
M8000C11	Solicitações de Paginação S1	Mensagens de paginação do MME	Inteiro	Soma
M8000C12	Configuração de S1 Lógica do UE	Conexões S1 associadas ao UE estabelecidas	Inteiro	Soma
M8000C29	Transporte NAS de uplink	Mensagens NAS enviadas para o MME	Inteiro	Soma

Contador	Nome	Descrição	Unidade	Tipo
M8000C30	Transporte NAS de downlink	Mensagens NAS recebidas do MME	Inteiro	Soma

Entendendo a Interface S1:

- A interface **S1** conecta o eNodeB ao EPC (Núcleo de Pacotes Evoluído)
- A **Configuração de Contexto Inicial** estabelece o contexto para uma nova conexão de UE
- A **Configuração S1** é o aperto de mão inicial entre o eNodeB e o MME
- Mensagens **NAS (Non-Access Stratum)** transportam sinalização de camada superior

Cálculo da Taxa de Sucesso de Configuração:

```
Taxa de Sucesso de Configuração S1 = 100 × M8000C7 / M8000C6
Taxa de Sucesso de Configuração de Contexto Inicial = 100 × M8000C1 / M8000C0
```

Metas de Desempenho:

- Taxa de Sucesso de Configuração S1: > 99%
- Taxa de Sucesso de Configuração de Contexto Inicial: > 95%

Contadores de Portadora EPS

M8006 - Medições de Portadora EPS

Esses contadores rastreiam o Estabelecimento, Modificação e Liberação da Portadora de Acesso de Rádio E-UTRAN (E-RAB).

Contadores Principais:

Contador	Nome	Descrição	Unidade	Tipo
M8006C0	Tentativas de Estabelecimento de Portadora EPS	Tentativas de estabelecimento da portadora	Inteiro	Soma
M8006C1	Conclusões de Estabelecimento de Portadora EPS	Estabelecimentos de portadora bem-sucedidos	Inteiro	Soma
M8006C2-C5	Falhas de Estabelecimento por Causa	Falhas categorizadas por razão	Inteiro	Soma

Entendendo as Portadoras EPS:

- **Portadora** = Canal lógico para dados do usuário entre o UE e a rede
- **Portadora Padrão** = Portadora sempre ativa para conectividade com a internet
- **Portadora Dedicada** = Portadoras adicionais para requisitos específicos de QoS (VoLTE, streaming de vídeo)

Casos de Uso:

- Monitorar taxas de sucesso de estabelecimento de portadoras
- Identificar razões para falhas de portadoras
- Rastrear alocação de portadoras QoS para serviços premium

Contadores de Transferência

M8009 - Medições de Preparação de Transferência

M8014 - Medições de Transferência Inter-eNB

M8015 - Medições de Transferência Intra-eNB

M8021 - Medições de Transferência Inter-Frequência

Esses grupos de medição rastreiam procedimentos de transferência - o processo de transferir uma conexão de UE de uma célula para outra sem interromper a chamada.

Tipos de Transferência:

Tipo	Descrição	Grupo de Medição
Intra-eNB	Transferência entre células na mesma estação base	M8015
Inter-eNB	Transferência entre diferentes estações base (X2)	M8014
Inter-Frequência	Transferência para uma frequência de portadora diferente	M8021
Inter-RAT	Transferência para uma tecnologia diferente (LTE→3G/2G)	M8017

Métricas Chave:

Grupo de Contadores	Foco	Contadores Críticos
M8009	Falhas de preparação de transferência	Tentativas de preparação, falhas por causa
M8014	HO baseado em X2	Tentativas de preparação, execuções, falhas
M8015	HO intra-célula	Tentativas de preparação, execuções, falhas
M8021	HO inter-frequência	Tentativas, sucessos, falhas

Fórmula da Taxa de Sucesso de Transferência:

```
Taxa de Sucesso de HO = 100 × (Execuções de HO) / (Tentativas de Preparação de HO)
```

Metas de Desempenho:

- Taxa de Sucesso de HO Intra-eNB: > 99%
- Taxa de Sucesso de HO Inter-eNB: > 98%
- Taxa de Sucesso de HO Inter-Frequência: > 95%

Causas Comuns de Falha de Transferência:

- Congestionamento da célula alvo (nenhum recurso disponível)
- Condições de rádio ruins na célula alvo
- Expiração do temporizador (UE não responde a tempo)
- Lacunas de medição impedindo a seleção adequada da célula

Medições de Qualidade do Canal

M8010 - Distribuição do CQI (Indicador de Qualidade de Canal)

Esses contadores rastreiam a distribuição de relatórios de CQI dos UEs, fornecendo informações sobre a qualidade do canal de rádio.

Entendendo o CQI:

- **CQI** = Indicador de Qualidade de Canal relatado pelo UE para o eNodeB
- **Faixa:** CQI 0 (pior) a CQI 15 (melhor)
- **Propósito:** Ajuda o agendador a selecionar o MCS (Esquema de Modulação e Codificação) apropriado
- **Frequência de Atualização:** A cada poucos milissegundos com base nas condições do canal

Mapeamento de CQI para Taxa de Dados:

Nível de CQI	Qualidade do Canal	Taxa Máxima Aproximada	Modulação
0-3	Muito Ruim	< 1 Mbps	QPSK
4-6	Ruim	1-5 Mbps	QPSK
7-9	Justo	5-15 Mbps	16-QAM
10-12	Bom	15-40 Mbps	64-QAM
13-15	Excelente	40-150 Mbps	64-QAM

Contadores M8010:

- M8010C0 - M8010C15: Contagem de relatórios de CQI em cada nível (0-15)

Análise de Desempenho:

```
CQI Médio = Σ(CQI_nível × M8010C[nível]) / Σ(M8010C[nível])
```

Interpretando a Distribuição de CQI:

- **CQI Alto (10-15):** Boa cobertura, alto potencial de taxa de transferência
- **CQI Médio (7-9):** Cobertura adequada, taxa de transfer��ncia moderada
- **CQI Baixo (0-6):** Problemas de cobertura, considerar otimização da célula

---

Contadores de Retorno de CS

M8016 - Medições de Retorno de CS

Esses contadores rastreiam procedimentos de Retorno de Circuito (CSFB), onde UEs LTE retornam a redes 2G/3G para chamadas de voz.

Entendendo o CSFB:

- **Propósito:** Lidar com chamadas de voz em redes sem VoLTE
- **Processo:** UE em LTE → Chamada de voz → Mover temporariamente para 2G/3G → Retornar ao LTE
- **Impacto:** Atraso na configuração da chamada, perda temporária de dados LTE

Contadores Chave:

Contador	Nome	Descrição
M8016C0	Tentativas de CSFB com Redirecionamento	CSFB usando método de redirecionamento
M8016C1	Tentativas de CSFB com Transferência	CSFB usando método de transferência

Métodos de CSFB:

1. **Redirecionamento:** UE desconecta do LTE, re-seleciona 2G/3G (mais rápido, mas interrupção breve do serviço)
2. **Transferência:** Transferência adequada do LTE para 2G/3G (mais lenta, mas sem interrupções)

Métricas de Desempenho:

- Taxa de Sucesso do CSFB = Transições bem-sucedidas / Tentativas totais de CSFB
- Meta: > 98%

Contadores de Volume de Dados

M8023 - Medições de Volume de Dados do SDU PDCP

Esses contadores rastreiam o volume total de dados do usuário transmitidos pela interface aérea.

Métricas Chave:

- Volume total de dados (uplink e downlink)
- Volume por QCI (Identificador de Classe de Qualidade de Serviço)
- Volume por tipo de portadora

Casos de Uso:

- Planejamento de capacidade da rede
- Estimativa de receita (rastreamento de uso de dados)
- Análise de consumo de dados por usuário
- Perfil de tráfego da classe QoS

Relação com M8012 (Taxa de Transferência):

- **M8012:** Taxa de dados instantânea (kbit/s)
- **M8023:** Volume de dados acumulado (bytes)

Contadores da Interface X2

M8004 - Medições de Volume de Dados X2

M8022 - Medições de Configuração X2

Esses contadores rastreiam a interface X2 entre eNodeBs, usada para transferências inter-eNB e balanceamento de carga.

M8004 - Volume de Dados X2:

- Mede dados encaminhados entre eNodeBs durante transferências
- Rastreia volume de tráfego X2 de entrada e saída

M8022 - Configuração X2:

- **M8022C0:** Tentativas de Configuração X2
- **M8022C1:** Sucessos de Configuração X2

Entendendo a Interface X2:

- **Propósito:** Comunicação direta entre eNodeBs vizinhos
- **Funções:** Coordenação de transferência, compartilhamento de carga, gerenciamento de interferência
- **Benefício:** Reduz a carga da rede central, transferências mais rápidas

Taxa de Sucesso de Configuração X2:

```
Taxa de Sucesso de Configuração X2 = 100 × M8022C1 / M8022C0
```

Meta: > 95%

Grupos de Medição Adicionais

M8007 - Medições de Portadora de Dados de Rádio (DRB)

Rastreia o estabelecimento, modificação e liberação de Portadoras de Dados de Rádio (DRBs) para transmissão de dados do usuário.

Áreas de Foco:

- Taxas de sucesso de estabelecimento de DRB
- Procedimentos de modificação de DRB
- Estatísticas de liberação de portadoras

M8008 - Medições de Rejeição de Conexão RRC

Rastreia solicitações de conexão RRC que são rejeitadas, categorizadas por causa de rejeição.

Razões Comuns para Rejeição:

- Congestionamento da rede (PRBs insuficientes)
- Limite máximo de UE atingido
- Redirecionamento de balanceamento de carga
- Restrições de mobilidade

M8019 - Mudança de Célula Assistida pela Rede (NACC)

Rastreia procedimentos NACC para otimizar a re-seleção de células de LTE para GSM.

Propósito: Fornece informações do sistema de células vizinhas GSM para UEs antes da re-seleção, acelerando a transição.

Medições de Interface de Rede

M5112 - Medições de Entrada de Interface IP

M5113 - Medições de RX Ethernet

Esses grupos de medição rastreiam estatísticas da interface de backhaul.

M5112 - Entrada de Interface IP (112 contadores):

- Contagens de pacotes de entrada
- Distribuição de tamanho de pacotes
- Estatísticas específicas de protocolo
- Utilização da interface

M5113 - RX Ethernet (21 contadores):

- Contagens de quadros Ethernet recebidos
- Distribuição de tamanho de quadros
- Estatísticas de erro (erros de CRC, erros de quadro)

Casos de Uso:

- Monitoramento de capacidade de backhaul
- Avaliação da saúde do link de transporte
- Solução de problemas de conectividade
- Planejamento de capacidade para atualizações de transporte

Contadores de Hardware e Unidade de Rádio

M40001 - Medições de Hardware de Rádio

Contador	Nome	Descrição	Unidade	Tipo	Escala
M40001C0	VSWR por ramo de antena	Relação de Ondas Estacionárias de Tensão	0.1	Média	Dividir por 10

Entendendo o VSWR:

- **VSWR** = Relação de Ondas Estacionárias de Tensão
- Mede a eficiência do sistema de antena
- Indica desajuste de impedância e potenciais problemas de cabo/antena
- Valores mais baixos = melhor

Interpretação do VSWR:

VSWR	Status	Ação
1.0-1.5	Excelente	Operação normal
1.5-2.0	Bom	Aceitável
2.0-3.0	Justo	Investigar
> 3.0	Ruim	Problema de cabo/antena - solucionar imediatamente

Causas Comuns de Alto VSWR:

- Cabos coaxiais danificados
- Conectores soltos

- Infiltração de água
- Danos à antena
- Desajuste de impedância

Exemplo de Consulta 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 - Medições de Consumo de Energia

Contador	Nome	Descrição	Unidade	Tipo	Escala
M40002C2	Consumo de Energia	Consumo de energia da estação base	100000 fator	Média	Dividir por 100000

Entendendo o Consumo de Energia:

- Mede o total de energia consumida pela estação base
- Útil para cálculos de OPEX e planejamento de capacidade
- Pode indicar problemas de hardware se inesperadamente alto/baixo

Exemplo de Consulta 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}))
```

Usando Contadores no Grafana

Construindo Painéis Eficazes

1. Painel de Utilização de Recursos

Combine M8011C24 e M8011C37 para mostrar a utilização de PRB uplink/downlink:

```
// Utilização de PRB Uplink
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": "Uplink PRB %"})

// Utilização de PRB Downlink
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": "Downlink PRB %"})
```

2. Painel de Taxa de Transferência

Mostre as taxas de transferência de dados:

```
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}))  //
Converter para Mbps
  |> pivot(rowKey: ["_time"], columnKey: ["metricCounter"],
valueColumn: "_value")
  |> map(fn: (r) => ({
      _time: r._time,
      "Uplink Mbps": r.M8012C23,
      "Downlink Mbps": r.M8012C26
    }))
```

3. Painel de Disponibilidade

Calcule e exiba a disponibilidade da célula:

```
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,
      "Disponibilidade %": 100.0 * r.M8020C3 / (r.M8020C6 -
r.M8020C4)
    }))
```

4. Painel de Taxa de Sucesso de Conexão

Rastreie o desempenho da configuração 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,
      "Taxa de Sucesso %": 100.0 * r.M8013C5 / (r.M8013C17 +
r.M8013C18 + r.M8013C19 + r.M8013C34 + r.M8013C31 + r.M8013C21 +
r.M8013C93 + r.M8013C91)
    }))
```

Melhores Práticas para Painéis

Use Tipos de Visualização Apropriados:

- Gráficos de séries temporais - Dados de tendência (taxa de transferência, utilização de PRB)
- Medidores - Valores atuais (porcentagem de disponibilidade)
- Painéis de estatísticas únicas - Valores máximos (máx. UEs ativos)
- Mapas de calor - Dados de distribuição (níveis de RSSI)

Defina Limiares Significativos:

- Verde: Operação normal
- Amarelo: Aviso (investigar)
- Vermelho: Crítico (ação imediata)

Configuração de Limiares de Exemplo:

- Utilização de PRB: Verde < 70%, Amarelo 70-85%, Vermelho > 85%
- Disponibilidade: Verde > 99%, Amarelo 95-99%, Vermelho < 95%
- Sucesso de configuração: Verde > 99%, Amarelo 95-99%, Vermelho < 95%

Agrupe Métricas Relacionadas:

- Crie painéis separados para capacidade, desempenho e qualidade

- Use variáveis de modelo para seleção de site/célula
- Inclua links de detalhamento para visualizações detalhadas

Documentação Relacionada

- Guia de Operações - Operações e fluxos de trabalho do RAN Monitor
- Guia de Integração do Grafana - Configurando painéis do Grafana
- Guia de Configuração em Tempo de Execução - Configurando o RAN Monitor
- Guia de Configuração do AirScale - Configuração da estação base
- Referência de Métricas - Estrutura de dados do InfluxDB

Tabela de Referência Rápida

Contadores Mais Comumente Usados

Contador	Nome	Caso de Uso	Unidade
M8011C24	Utilização média de PRB UL	Planejamento de capacidade	0.1%
M8011C37	Utilização média de PRB DL	Planejamento de capacidade	0.1%
M8012C23	Taxa de transferência PDCP UL	Monitoramento de desempenho	kbit/s
M8012C26	Taxa de transferência PDCP DL	Monitoramento de desempenho	kbit/s
M8018C1	Máximo de UEs Ativas	Monitoramento de carga	contagem
M8020C3	Amostras de célula disponível	Rastreamento de disponibilidade	contagem
M8020C6	Denominador de disponibilidade	Cálculo de disponibilidade	contagem
M8013C5	Conclusões de configuração	Rastreamento de taxa de sucesso	contagem
M8005C0	RSSI mínimo	Análise de cobertura	dBm
M8005C2	RSSI médio	Análise de cobertura	dBm
M8001C2	Atraso médio do PDCP	Monitoramento de latência	ms

Contador	Nome	Caso de Uso	Unidade
M40001C0	VSWR	Saúde do hardware	0.1 razão

Fontes:

- Medições de Desempenho do Nokia FlexiRadio LTE
- Especificações de Contadores de Desempenho da Nokia AirScale
- Padrões de Gerenciamento de Desempenho da 3GPP LTE

Apêndice: Listagem Completa de Contadores

Abaixo está a listagem de referência completa de todos os 1.186 contadores de desempenho LTE da Nokia extraídos da especificação KPI da Nokia.

```
================================================================================
REFERÊNCIA COMPLETA DE CONTADORES DE DESEMPENHO LTE DA NOKIA
================================================================================

--------------------------------------------------------------------------------
Grupo de Medição: M8000
--------------------------------------------------------------------------------
M8000C0         | Solicitações de Configuração de Contexto Inicial
inteiro
M8000C1         | Conclusões de Configuração de Contexto Inicial
Número inteiro
M8000C2         | Falhas de Configuração de Contexto Inicial devido a
Número inteiro
M8000C3         | Falhas de Configuração de Contexto Inicial devido a
Número inteiro
M8000C4         | Falhas de Configuração de Contexto Inicial devido a
Número inteiro
M8000C5         | Falhas de Configuração de Contexto Inicial devido a
Número inteiro
M8000C6         | Solicitações de configuração S1
Número inteiro
M8000C7         | Conclusões de configuração S1
Número inteiro
M8000C8         | Falha de configuração S1 devido à expiração do temp
Número inteiro
M8000C9         | Falha de configuração S1 devido à rejeição do MME
Número inteiro
M8000C11        | Solicitações de Paginação S1
Número inteiro
M8000C12        | Número de conexões lógicas S1 associadas ao UE
Número inteiro
M8000C13        | Reinicialização global S1 iniciada pelo eNB
Número inteiro
M8000C14        | Reinicialização global S1 iniciada pelo MME
Número inteiro
M8000C15        | Reinicialização parcial S1 iniciada pelo eNB
Número inteiro
M8000C16        | Reinicialização parcial S1 iniciada pelo MME
Número inteiro
M8000C23        | Tentativas de modificação de contexto do UE
Número inteiro
M8000C24        | Tentativas de modificação de contexto do UE devido
Número inteiro
```

```
M8000C25        | Falhas de modificação de contexto do UE
Número inteiro
M8000C29        | Número de Transporte NAS de uplink
Número inteiro
M8000C30        | Número de Transporte NAS de downlink
Número inteiro
M8000C31        | Tentativas de modificação de contexto do UE devido
Número inteiro
M8000C32        | Solicitações de Estabelecimento de E-RAB para IMS
Número inteiro
M8000C33        | Conclusões de Estabelecimento de E-RAB para IMS
Número inteiro
M8000C34        | Falhas de Estabelecimento de E-RAB para IMS
Número inteiro
M8000C35        | Número de Controle de Relatório de Localização
Número inteiro
M8000C36        | Número de mensagens de Relatório de Localização
Número inteiro
M8000C37        | Número de endereços IP X2 bem-sucedidos
Número inteiro
M8000C38        | Número de endereços IP X2 tentados
Número inteiro
M8000C39        | Número de WRITE-REPLACE
Número inteiro
M8000C40        | Número de WRITE-REPLACE
Número inteiro
M8000C41        | Número de mensagens de SOLICITAÇÃO DE KILL
Número inteiro
M8000C42        | Número de RESPOSTA DE KILL
Número inteiro

-----------------------------------------------------------------
Grupo de Medição: M8001
-----------------------------------------------------------------
M8001C0         | Atraso do SDU PDCP no DL DTCH Mínimo
M8001C1         | Atraso do SDU PDCP no DL DTCH Máximo
M8001C2         | Atraso do SDU PDCP no DL DTCH Médio
M8001C3         | Atraso do SDU PDCP no UL DTCH Mínimo
M8001C4         | Atraso do SDU PDCP no UL DTCH Máximo
M8001C5         | Atraso do SDU PDCP no UL DTCH Médio
M8001C6         | Tentativas de configuração RACH para tamanho pequer
Número inteiro
M8001C7         | Tentativas de configuração RACH para tamanho grande
Número inteiro
```

M8001C8 | Conclusões de configuração RACH
Número inteiro
M8001C9 | TBs transmitidos no PCH
Número inteiro
M8001C10 | TBs transmitidos no BCH
Número inteiro
M8001C11 | TBs transmitidos no DL-SCH
Número inteiro
M8001C12 | Retransmissões HARQ no DL-SCH
Número inteiro
M8001C13 | TBs UL-SCH corretos não duplicados com
Número inteiro
M8001C14 | TBs UL-SCH corretos com re-recepção
Número inteiro
M8001C15 | Recebimentos errôneos de TBs UL-SCH
Número inteiro
M8001C16 | Transmissões PUSCH usando MCS0
Número inteiro
M8001C17 | Transmissões PUSCH usando MCS1
Número inteiro
M8001C18 | Transmissões PUSCH usando MCS2
Número inteiro
M8001C19 | Transmissões PUSCH usando MCS3
Número inteiro
M8001C20 | Transmissões PUSCH usando MCS4
Número inteiro
M8001C21 | Transmissões PUSCH usando MCS5
Número inteiro
M8001C22 | Transmissões PUSCH usando MCS6
Número inteiro
M8001C23 | Transmissões PUSCH usando MCS7
Número inteiro
M8001C24 | Transmissões PUSCH usando MCS8
Número inteiro
M8001C25 | Transmissões PUSCH usando MCS9
Número inteiro
M8001C26 | Transmissões PUSCH usando MCS10
Número inteiro
M8001C27 | Transmissões PUSCH usando MCS11
Número inteiro
M8001C28 | Transmissões PUSCH usando MCS12
Número inteiro
M8001C29 | Transmissões PUSCH usando MCS13
Número inteiro

M8001C30 | Transmissões PUSCH usando MCS14
Número inteiro
M8001C31 | Transmissões PUSCH usando MCS15
Número inteiro
M8001C32 | Transmissões PUSCH usando MCS16
Número inteiro
M8001C33 | Transmissões PUSCH usando MCS17
Número inteiro
M8001C34 | Transmissões PUSCH usando MCS18
Número inteiro
M8001C35 | Transmissões PUSCH usando MCS19
Número inteiro
M8001C36 | Transmissões PUSCH usando MCS20
Número inteiro
M8001C37 | Transmissões PUSCH usando MCS21
Número inteiro
M8001C38 | Transmissões PUSCH usando MCS22
Número inteiro
M8001C39 | Transmissões PUSCH usando MCS23
Número inteiro
M8001C40 | Transmissões PUSCH usando MCS24
Número inteiro
M8001C41 | Transmissões PUSCH usando MCS25
Número inteiro
M8001C42 | Transmissões PUSCH usando MCS26
Número inteiro
M8001C43 | Transmissões PUSCH usando MCS27
Número inteiro
M8001C44 | Transmissões PUSCH usando MCS28
Número inteiro
M8001C45 | Transmissões PDSCH usando MCS0
Número inteiro
M8001C46 | Transmissões PDSCH usando MCS1
Número inteiro
M8001C47 | Transmissões PDSCH usando MCS2
Número inteiro
M8001C48 | Transmissões PDSCH usando MCS3
Número inteiro
M8001C49 | Transmissões PDSCH usando MCS4
Número inteiro
M8001C50 | Transmissões PDSCH usando MCS5
Número inteiro
M8001C51 | Transmissões PDSCH usando MCS6
Número inteiro

```
M8001C52        | Transmissões PDSCH usando MCS7
Número inteiro
M8001C53        | Transmissões PDSCH usando MCS8
Número inteiro
M8001C54        | Transmissões PDSCH usando MCS9
Número inteiro
M8001C55        | Transmissões PDSCH usando MCS10
Número inteiro
M8001C56        | Transmissões PDSCH usando MCS11
Número inteiro
M8001C57        | Transmissões PDSCH usando MCS12
Número inteiro
M8001C58        | Transmissões PDSCH usando MCS13
Número inteiro
M8001C59        | Transmissões PDSCH usando MCS14
Número inteiro
M8001C60        | Transmissões PDSCH usando MCS15
Número inteiro
M8001C61        | Transmissões PDSCH usando MCS16
Número inteiro
M8001C62        | Transmissões PDSCH usando MCS17
Número inteiro
M8001C63        | Transmissões PDSCH usando MCS18
Número inteiro
M8001C64        | Transmissões PDSCH usando MCS19
Número inteiro
M8001C65        | Transmissões PDSCH usando MCS20
Número inteiro
M8001C66        | Transmissões PDSCH usando MCS21
Número inteiro
M8001C67        | Transmissões PDSCH usando MCS22
Número inteiro
M8001C68        | Transmissões PDSCH usando MCS23
Número inteiro
M8001C69        | Transmissões PDSCH usando MCS24
Número inteiro
M8001C70        | Transmissões PDSCH usando MCS25
Número inteiro
M8001C71        | Transmissões PDSCH usando MCS26
Número inteiro
M8001C72        | Transmissões PDSCH usando MCS27
Número inteiro
M8001C73        | Transmissões PDSCH usando MCS28
Número inteiro
```

```
M8001C74        | Transmissões PUSCH usando MCS0
Número inteiro
M8001C75        | Transmissões PUSCH usando MCS1
Número inteiro
M8001C76        | Transmissões PUSCH usando MCS2
Número inteiro
M8001C77        | Transmissões PUSCH usando MCS3
Número inteiro
M8001C78        | Transmissões PUSCH usando MCS4
Número inteiro
M8001C79        | Transmissões PUSCH usando MCS5
Número inteiro
M8001C80        | Transmissões PUSCH usando MCS6
Número inteiro
M8001C81        | Transmissões PUSCH usando MCS7
Número inteiro
M8001C82        | Transmissões PUSCH usando MCS8
Número inteiro
M8001C83        | Transmissões PUSCH usando MCS9
Número inteiro
M8001C84        | Transmissões PUSCH usando MCS10
Número inteiro
M8001C85        | Transmissões PUSCH usando MCS11
Número inteiro
M8001C86        | Transmissões PUSCH usando MCS12
Número inteiro
M8001C87        | Transmissões PUSCH usando MCS13
Número inteiro
M8001C88        | Transmissões PUSCH usando MCS14
Número inteiro
M8001C89        | Transmissões PUSCH usando MCS15
Número inteiro
M8001C90        | Transmissões PUSCH usando MCS16
Número inteiro
M8001C91        | Transmissões PUSCH usando MCS17
Número inteiro
M8001C92        | Transmissões PUSCH usando MCS18
Número inteiro
M8001C93        | Transmissões PUSCH usando MCS19
Número inteiro
M8001C94        | Transmissões PUSCH usando MCS20
Número inteiro
M8001C95        | Transmissões PUSCH usando MCS21
Número inteiro
```

M8001C96 | Transmissões PUSCH usando MCS22
Número inteiro
M8001C97 | Transmissões PUSCH usando MCS23
Número inteiro
M8001C98 | Transmissões PUSCH usando MCS24
Número inteiro
M8001C99 | Transmissões PUSCH usando MCS25
Número inteiro
M8001C100 | Transmissões PUSCH usando MCS26
Número inteiro
M8001C101 | Transmissões PUSCH usando MCS27
Número inteiro
M8001C102 | Transmissões PUSCH usando MCS28
Número inteiro
M8001C103 | Transmissões PUSCH usando MCS29
Número inteiro
M8001C104 | Transmissões PUSCH usando MCS30
Número inteiro
M8001C105 | Transmissões PUSCH usando MCS31
Número inteiro
M8001C106 | Transmissões PUSCH usando MCS32
Número inteiro
M8001C107 | Transmissões PUSCH usando MCS33
Número inteiro
M8001C108 | Transmissões PUSCH usando MCS34
Número inteiro
M8001C109 | Transmissões PUSCH usando MCS35
Número inteiro
M8001C110 | Transmissões PUSCH usando MCS36
Número inteiro
M8001C111 | Transmissões PUSCH usando MCS37
Número inteiro
M8001C112 | Transmissões PUSCH usando MCS38
Número inteiro
M8001C113 | Transmissões PUSCH usando MCS39
Número inteiro
M8001C114 | Transmissões PUSCH usando MCS40
Número inteiro
M8001C115 | Transmissões PUSCH usando MCS41
Número inteiro
M8001C116 | Transmissões PUSCH usando MCS42
Número inteiro
M8001C117 | Transmissões PUSCH usando MCS43
Número inteiro

M8001C118 | Transmissões PUSCH usando MCS44
Número inteiro
M8001C119 | Transmissões PUSCH usando MCS45
Número inteiro
M8001C120 | Transmissões PUSCH usando MCS46
Número inteiro
M8001C121 | Transmissões PUSCH usando MCS47
Número inteiro
M8001C122 | Transmissões PUSCH usando MCS48
Número inteiro
M8001C123 | Transmissões PUSCH usando MCS49
Número inteiro
M8001C124 | Transmissões PUSCH usando MCS50
Número inteiro
M8001C125 | Transmissões PUSCH usando MCS51
Número inteiro
M8001C126 | Transmissões PUSCH usando MCS52
Número inteiro
M8001C127 | Transmissões PUSCH usando MCS53
Número inteiro
M8001C128 | Transmissões PUSCH usando MCS54
Número inteiro
M8001C129 | Transmissões PUSCH usando MCS55
Número inteiro
M8001C130 | Transmissões PUSCH usando MCS56
Número inteiro
M8001C131 | Transmissões PUSCH usando MCS57
Número inteiro
M8001C132 | Transmissões PUSCH usando MCS58
Número inteiro
M8001C133 | Transmissões PUSCH usando MCS59
Número inteiro
M8001C134 | Transmissões PUSCH usando MCS60
Número inteiro
M8001C135 | Transmissões PUSCH usando MCS61
Número inteiro
M8001C136 | Transmissões PUSCH usando MCS62
Número inteiro
M8001C137 | Transmissões PUSCH usando MCS63
Número inteiro
M8001C138 | Transmissões PUSCH usando MCS64
Número inteiro
M8001C139 | Transmissões PUSCH usando MCS65
Número inteiro

```
M8001C140       | Transmissões PUSCH usando MCS66
Número inteiro
M8001C141       | Transmissões PUSCH usando MCS67
Número inteiro
M8001C142       | Transmissões PUSCH usando MCS68
Número inteiro
M8001C143       | Transmissões PUSCH usando MCS69
Número inteiro
M8001C144       | Transmissões PUSCH usando MCS70
Número inteiro
M8001C145       | Transmissões PUSCH usando MCS71
Número inteiro
M8001C146       | Transmissões PUSCH usando MCS72
Número inteiro
M8001C147       | Transmissões PUSCH usando MCS73
Número inteiro
M8001C148       | Transmissões PUSCH usando MCS74
Número inteiro
M8001C149       | Transmissões PUSCH usando MCS75
Número inteiro
M8001C150       | Transmissões PUSCH usando MCS76
Número inteiro
M8001C151       | Transmissões PUSCH usando MCS77
Número inteiro
M8001C152       | Transmissões PUSCH usando MCS78
Número inteiro
M8001C153       | Transmissões PUSCH usando MCS79
Número inteiro
M8001C154       | Transmissões PUSCH usando MCS80
Número inteiro
M8001C155       | Transmissões PUSCH usando MCS81
Número inteiro
M8001C156       | Transmissões PUSCH usando MCS82
Número inteiro
M8001C157       | Transmissões PUSCH usando MCS83
Número inteiro
M8001C158       | Transmissões PUSCH usando MCS84
Número inteiro
M8001C159       | Transmissões PUSCH usando MCS85
Número inteiro
M8001C160       | Transmissões PUSCH usando MCS86
Número inteiro
M8001C161       | Transmissões PUSCH usando MCS87
Número inteiro
```

M8001C162 | Transmissões PUSCH usando MCS88
Número inteiro
M8001C163 | Transmissões PUSCH usando MCS89
Número inteiro
M8001C164 | Transmissões PUSCH usando MCS90
Número inteiro
M8001C165 | Transmissões PUSCH usando MCS91
Número inteiro
M8001C166 | Transmissões PUSCH usando MCS92
Número inteiro
M8001C167 | Transmissões PUSCH usando MCS93
Número inteiro
M8001C168 | Transmissões PUSCH usando MCS94
Número inteiro
M8001C169 | Transmissões PUSCH usando MCS95
Número inteiro
M8001C170 | Transmissões PUSCH usando MCS96
Número inteiro
M8001C171 | Transmissões PUSCH usando MCS97
Número inteiro
M8001C172 | Transmissões PUSCH usando MCS98
Número inteiro
M8001C173 | Transmissões PUSCH usando MCS99
Número inteiro
M8001C174 | Transmissões PUSCH usando MCS100
Número inteiro
M8001C175 | Transmissões PUSCH usando MCS101
Número inteiro
M8001C176 | Transmissões PUSCH usando MCS102
Número inteiro
M8001C177 | Transmissões PUSCH usando MCS103
Número inteiro
M8001C178 | Transmissões PUSCH usando MCS104
Número inteiro
M8001C179 | Transmissões PUSCH usando MCS105
Número inteiro
M8001C180 | Transmissões PUSCH usando MCS106
Número inteiro
M

Guia de Coleta de Dados PM

Visão Geral

A página de Coleta de Dados PM permite gerenciar quais contadores de Métricas de Desempenho (PM) são armazenados no InfluxDB. As estações base Nokia AirScale relatam mais de **22.000 contadores PM únicos**, mas armazenar todos eles não é prático nem necessário para a maioria dos casos de uso.

Este guia explica como selecionar quais contadores coletar com base em seus requisitos de monitoramento.

Início Rápido

Acessando a Página de Coleta de Dados PM

1. Navegue até o Painel de Controle: `https://localhost:9443`
2. Clique em **Filtros de Dados** no menu de navegação
3. Visualize e gerencie as configurações de coleta de contadores PM

Compreendendo a Interface

A página é dividida em duas seções principais:

Seção	Descrição
Dados PM Armazenados (Esquerda)	Contadores atualmente sendo coletados e armazenados no InfluxDB
Contadores Disponíveis (Direita)	Todos os 22.000+ contadores disponíveis para adicionar à sua coleção

---

Categorias de Contadores

Os contadores PM são categorizados pelo seu prefixo de código, que indica a tecnologia e a função:

Categoria	Prefixo de Código	Contagem	Descrição
LTE	M8xxx	~5.900	Contadores LTE L1/L2/L3 (ERAB, RRC, handover, etc.)
WCDMA	M5xxx	~885	Contadores 3G WCDMA (camada MAC, CQI, HSDPA)
5G-NR	M55xxx	~14.500	Contadores 5G NR (MIMO massivo, beamforming, etc.)
5G-Mobilidade	M51xxx	~500	Mobilidade e medições 5G
5G-Comum	M40xxx	~250	Contadores comuns/compartilhados 5G

Contadores Padrão

Na primeira inicialização, valores padrão sensatos são carregados de `priv/pm_counters.csv`. Esses padrões incluem contadores essenciais para:

- **Energia**: Monitoramento do consumo de energia
- **Volume de Dados**: Métricas de volume de tráfego
- **Disponibilidade**: Estatísticas de disponibilidade da célula
- **Acessibilidade**: Sucesso/falha da conexão RRC
- **PRB**: Utilização do Bloco de Recursos Físicos
- **Throughput**: Métricas de throughput UL/DL
- **RRC**: Estatísticas de conexão RRC
- **ERAB**: Contadores de configuração e liberação de E-RAB
- **PDCP**: Métricas da camada PDCP
- **Handover**: Estatísticas de handover entre células
- **Interferência**: Medições de interferência UL

Gerenciando Contadores

Adicionando Contadores

1. Use a **caixa de pesquisa** ou **filtro de categoria** na seção "Contadores Disponíveis"
2. Clique nas linhas para selecionar contadores (a caixa de seleção aparecerá marcada)
3. Use **Selecionar Todos** para selecionar todos os contadores visíveis
4. Clique em **Adicionar Selecionados** para movê-los para a coleção armazenada

Removendo Contadores

1. Na seção "Dados PM Armazenados", selecione os contadores a serem removidos

2. Clique em **Remover Selecionados** para parar de coletar esses contadores

Filtrando e Pesquisando

Ambas as seções suportam:

- **Pesquisa por texto**: Filtrar por ID do contador ou descrição
- **Filtro de categoria**: Mostrar apenas contadores de uma categoria específica (LTE, 5G-NR, etc.)

Resetando para Padrões

Clique em **Resetar para Padrões** para restaurar a lista original de contadores de `priv/pm_counters.csv`. Isso removerá quaisquer adições personalizadas.

Persistência

Mudanças na sua seleção de contadores PM são:

1. **Persistidas em disco** em `priv/pm_filters.etf`
2. **Sobrevivem a reinicializações da aplicação**
3. **Entram em vigor imediatamente** (sem reinicialização necessária)

O gravador em lote do InfluxDB é notificado sobre as mudanças e imediatamente começa/parar de coletar os contadores afetados.

Considerações de Armazenamento

Por Que Não Coletar Tudo?

Coletar todos os 22.000+ contadores resultaria em:

Cenário	Impacto
Armazenamento	~100-500 GB/mês por site (dependendo do intervalo de coleta)
Carga de Escrita	Pressão significativa de escrita no InfluxDB
Desempenho de Consulta	Consultas de dashboard mais lentas devido ao volume de dados
Custo	Custos mais altos de armazenamento e computação

Abordagem Recomendada

1. **Comece com os padrões**: Os contadores pré-configurados cobrem a maioria das necessidades comuns de monitoramento
2. **Adicione conforme necessário**: Ao construir novos dashboards, adicione contadores específicos que você precisa
3. **Revise periodicamente**: Remova contadores que não estão mais sendo usados

---

Referência de Contadores

Encontrando Descrições de Contadores

A seção "Contadores Disponíveis" mostra a descrição oficial da Nokia para cada contador. Use a função de pesquisa para encontrar contadores por:

- **ID do Contador** (ex: `M8012C23`)
- **Palavras-chave da Descrição** (ex: `throughput`, `handover`, `RSRP`)

Exemplos Comuns de Contadores

Contador	Categoria	Descrição
M8012C23	LTE	Throughput médio UL por célula
M8012C26	LTE	Throughput médio DL por célula
M8001C2	LTE	Atraso médio de PDCP SDU DL
M8011C24	LTE	Utilização de PRB UL
M8011C37	LTE	Utilização de PRB DL
M8013C17	LTE	Usuários Conectados RRC
M8020C3	LTE	Sucesso de Handover
M40001C0	5G	Consumo de Energia

Arquivos de Configuração

pm_counters.csv

Contadores padrão carregados na primeira inicialização:

```
# Formato: contador,categoria,descrição
M8012C23,Throughput,Throughput Médio de Uplink
M8012C26,Throughput,Throughput Médio de Downlink
M8001C2,Disponibilidade,Disponibilidade da Célula
...
```

Localização: `priv/pm_counters.csv`

pm_metrics.csv

Referência completa de todos os contadores disponíveis:

```
# Formato: PM_Code,Categoria,Descrição
M8000C6,LTE,S1_SETUP_ATT
M8000C7,LTE,S1_SETUP_SUCC
...
```

Localização: `priv/pm_metrics.csv`

Resolução de Problemas

Contadores Não Estão Sendo Coletados

1. Verifique se o contador está em "Dados PM Armazenados" (lado esquerdo)
2. Verifique se o eNodeB está enviando dados PM (veja a página de Status do InfluxDB)
3. Verifique se o ID do contador corresponde exatamente (sensível a maiúsculas e minúsculas)

Mudanças Não Entrando em Vigor

1. Mudanças de filtro são aplicadas imediatamente ao gravador em lote
2. **Novos dados só aparecem após o próximo envio de PM do eNodeB** (normalmente a cada 15 minutos)
3. Verifique os logs da aplicação para erros `[PmFilterStore]`
4. Verifique se o disco é gravável para o arquivo de persistência

Descrições de Contadores Ausentes

1. As descrições dos contadores vêm de `priv/pm_metrics.csv`
2. Certifique-se de que este arquivo está presente e formatado corretamente
3. Verifique se há problemas de codificação UTF-8

Documentação Relacionada

- Política de Retenção de Dados - Quanto tempo os dados PM são mantidos
- Integração com Grafana - Construindo dashboards com dados PM
- Consultas InfluxDB - Consultando dados PM

Pontos de Acesso

- **Coleta de Dados PM**: `https://localhost:9443/nokia/pm-filters`
- **Retenção de Dados**: `https://localhost:9443/nokia/retention`
- **Status do InfluxDB**: `https://localhost:9443/nokia/influx`

Guia de Configuração em Tempo de Execução do RAN Monitor

Entendendo config/runtime.exs

Tabela de Conteúdos

Visão Geral

O arquivo `config/runtime.exs` é o principal arquivo de configuração para o RAN Monitor. Ele é avaliado em tempo de execução (quando a aplicação é iniciada), permitindo que você configure todos os aspectos do comportamento do sistema.

O que é Configurado:

- Conexões de banco de dados (MySQL)
- Endpoints e portas do servidor web
- Detalhes da estação base Nokia
- Banco de dados de séries temporais InfluxDB

- Comportamento de logging
- Credenciais de segurança

Localização do Arquivo:

```
config/runtime.exs
```

Quem Deve Usar Este Guia

Importante: Toda a configuração do RAN Monitor é **realizada pela Omnitouch** como parte da implantação inicial e suporte contínuo. Este guia é fornecido para:

- **Usuários avançados** que desejam entender a configuração do sistema
- **Implantações autogerenciadas** onde os clientes mantêm sua própria configuração
- **Solução de problemas** e compreensão de como o sistema está configurado
- **Implantações personalizadas** com requisitos específicos

Se você é um cliente gerenciado pela Omnitouch, entre em contato com o suporte da Omnitouch para quaisquer alterações de configuração.

Para entender quais dados estão sendo coletados, consulte Referência de Contadores Nokia. Para criação de dashboards, veja Integração Grafana.

Configuração do Banco de Dados

Conexão 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
```

Propósito: Configura a conexão com o banco de dados MySQL usado para gerenciamento de estado de sessão e dados operacionais.

Parâmetros Explicados

username (String)

- Conta de usuário do banco de dados
- Valor atual: `"omnitouch"`
- **Uso:** Deve ter privilégios de CREATE, SELECT, INSERT, UPDATE, DELETE
- **Segurança:** Considere usar um usuário dedicado com privilégios mínimos necessários

password (String)

- Senha do banco de dados para autenticação
- Valor atual: `"omnitouch2024"`
- **Segurança:** Deve ser armazenada em variáveis de ambiente em produção
- **Recomendação:** Use senhas fortes e únicas

hostname (String)

- Endereço do servidor de banco de dados
- Valor atual: `"localhost"`

- **Opções:**
  - `"localhost"` - Banco de dados na mesma máquina
  - `"127.0.0.1"` - Conexão TCP para a máquina local
  - `"10.179.2.135"` - IP do servidor de banco de dados remoto
  - `"db.example.com"` - Nome do host do banco de dados remoto

database (String)

- Nome do banco de dados a ser usado
- Valor atual: `"ran_monitor"`
- **Nota:** O banco de dados deve existir antes de iniciar o RAN Monitor
- **Criação:** `CREATE DATABASE ran_monitor CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;`

stacktrace (Boolean)

- Incluir stacktraces nas mensagens de erro
- Valor atual: `true`
- **Desenvolvimento:** `true` - Ajuda na depuração
- **Produção:** `false` - Reduz o ruído nos logs

show_sensitive_data_on_connection_error (Boolean)

- Mostrar credenciais nas mensagens de erro de conexão
- Valor atual: `true`
- **Desenvolvimento:** `true` - Facilita a solução de problemas
- **Produção:** `false` - Impede a exposição de credenciais nos logs

pool_size (Integer)

- Número de conexões de banco de dados a serem mantidas
- Valor atual: `10`
- **Guia de Dimensionamento:**
  - 1-5 dispositivos: `pool_size: 5`
  - 6-20 dispositivos: `pool_size: 10`
  - 21-50 dispositivos: `pool_size: 15`
  - 50+ dispositivos: `pool_size: 20`

- **Fórmula:** Aproximadamente 2 conexões por estação base + 5 para a interface web

---

Endpoints Web

O RAN Monitor executa vários servidores web para diferentes propósitos.

Endpoint Principal SOAP/API

```
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
```

Propósito: Endpoint principal para comunicação com a estação base (interface SOAP para o protocolo Nokia NE3S).

ip (Tuple)

- Interface para vincular
- Valor atual: `{0, 0, 0, 0}` (todas as interfaces)
- **Opções:**
  - `{0, 0, 0, 0}` - Ouvir em todas as interfaces de rede
  - `{127, 0, 0, 1}` - Ouvir apenas no localhost
  - `{10, 179, 2, 135}` - Ouvir em um endereço IP específico

port (Integer)

- Número da porta TCP
- Valor atual: `8080`
- **Nota:** As estações base devem ser configuradas para enviar dados a esta porta

- **Firewall:** Certifique-se de que a porta esteja aberta para os IPs das estações base

check_origin (Boolean)

- Validar cabeçalhos de origem WebSocket/HTTP
- Valor atual: `false`
- **Explicação:** Definido como `false` para a API SOAP (não interface web voltada para o usuário)

secret_key_base (String)

- Chave de assinatura criptográfica para sessões
- Valor atual: string aleatória de 64 caracteres
- **Geração:** `mix phx.gen.secret`
- **Segurança:** Mantenha isso em segredo, nunca comite em repositórios públicos
- **Impacto:** Alterar isso invalida todas as sessões existentes

server (Boolean)

- Iniciar o endpoint quando a aplicação é iniciada
- Valor atual: `true`
- **Sempre:** Deve ser `true` em runtime.exs

Interface Web do Painel de Controle

```
# Obter a porta HTTPS da variável de ambiente, padrão para 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"
  ]
```

Propósito: Endpoint HTTPS para a interface web do painel de controle.

Variáveis de Ambiente:

- **CONTROL_PANEL_HTTPS_PORT** - Número da porta HTTPS (padrão: 9443)
  - Defina esta variável de ambiente para alterar a porta HTTPS em tempo de execução
  - Exemplo: `export CONTROL_PANEL_HTTPS_PORT=8443`

url (Lista de palavras-chave)

- Configuração da URL externa
- **host:** `"0.0.0.0"` - Aceitar conexões de qualquer host
- **port:** Usa a variável `https_port` (configurável via CONTROL_PANEL_HTTPS_PORT)
- **scheme:** `"https"` - Usar protocolo HTTPS

https (Lista de palavras-chave)

- Configuração do servidor HTTPS
- **ip:** `{0, 0, 0, 0}` - Vincular a todas as interfaces
- **port:** Usa a variável `https_port` (deve corresponder à porta da URL)
- **keyfile:** Caminho para a chave privada SSL

- **certfile:** Caminho para o certificado SSL

Arquivos de Certificado SSL:

- Devem ser certificados SSL/TLS válidos
- Certificados autoassinados funcionam para ambientes de laboratório
- A produção deve usar certificados assinados por CA
- Gere autoassinado:

```
openssl req -newkey rsa:2048 -nodes -keyout omnitouch.pem -x509
-days 365 -out omnitouch.crt
```

Endpoint 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
```

Propósito: Recebe dados de desempenho em tempo real das estações base Nokia AirScale.

port (Integer)

- Valor atual: `9076`
- **Nota:** Deve corresponder à porta configurada na estação base PMCADM (rTpmCollEntityPortNum)
- **Coordenação:** Esta porta deve corresponder ao que você configurou no Editor de Parâmetros WebLM da Nokia

---

Configuração do Logger

```
config :logger,
  level: :info

config :logger, :console,
  format: "$time $metadata[$level] $message\n",
  metadata: [:request_id]
```

Nível de Log

level (Atom)

- Controla a verbosidade do logging
- Valor atual: `:info`
- **Opções:**
  - `:debug` - Extremamente verboso, todos os detalhes
  - `:info` - Operações normais, recomendado para produção
  - `:warning` - Apenas avisos e erros
  - `:error` - Apenas erros

Quando Usar Cada Nível:

- **Desenvolvimento:** `:debug` - Veja todas as operações internas
- **Produção:** `:info` - Equilíbrio entre visibilidade e ruído
- **Solução de Problemas:** Defina temporariamente como `:debug`, depois reverta
- **Produção Silenciosa:** `:warning` - Apenas alertar sobre problemas

Formato do Console

format (String)

- Como as mensagens de log aparecem
- Valor atual: `"$time $metadata[$level] $message\n"`
- **Variáveis:**

    - `$time` - Timestamp
    - `$metadata` - Informações contextuais
    - `$level` - Nível de log (info, error, etc.)
    - `$message` - Mensagem de log real

metadata (Lista de átomos)

- Contexto adicional a incluir
- Valor atual: `[:request_id]`
- **request_id:** Rastreia solicitações HTTP individuais através do sistema

---

Integração Nokia

Esta seção configura como o RAN Monitor se comunica com as estações 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"
      }
    ]
  }
```

Configurações Gerais

mcc (String)

- Código do País Móvel
- Valor atual: `"505"`
- **Uso:** Identifica o país para redes 3GPP
- **Formato:** 3 dígitos
- **Referência:** ITU-T E.212

mnc (String)

- Código da Rede Móvel
- Valor atual: `"57"`

- **Uso:** Identifica o operador de rede específico
- **Formato:** 2 ou 3 dígitos

Configuração NE3S (Protocolo Nokia NE3S)

webhook_url (String)

- URL onde as estações base enviam notificações
- Valor atual: `"http://10.5.198.200:9076/webhook"`
- **Formato:** `http://<ran-monitor-ip>:<port>/webhook`
- **Endereço IP:** Deve ser o endereço IP onde o RAN Monitor está em execução
- **Porta:** Deve corresponder à porta de `RanMonitor.Web.Nokia.Airscale.Endpoint` (9076)
- **Caminho:** Sempre `/webhook`

private_key (String - Caminho do arquivo)

- Chave privada para autenticação do gerente
- Valor atual: `priv/external/nokia/ne.key.pem`
- **Formato:** Chave privada codificada em PEM
- **Segurança:** Mantenha este arquivo seguro, nunca compartilhe
- **Geração:** Fornecida pela Nokia ou gerada com OpenSSL

public_key (String - Caminho do arquivo)

- Certificado público para identidade do gerente
- Valor atual: `priv/external/nokia/ne.cert.der`
- **Formato:** Certificado codificado em DER
- **Uso:** Enviado para a estação base durante o registro
- **Par:** Deve corresponder à private_key

reregister_interval (Integer)

- Com que frequência re-registrar com as estações base (segundos)
- Valor atual: `30`

- **Explicação:** As sessões expiram, a re-registrar periódica mantém a conexão
- **Faixa:** 30-300 segundos
- **Recomendação:** 30 segundos para monitoramento confiável

Estações Base AirScale

airscales (Lista de mapas)

- Lista de estações base Nokia AirScale a serem monitoradas
- Valor atual: Uma estação base configurada

Cada entrada de estação base requer:

address (String)

- Endereço IP da estação base
- Valor atual: `"10.7.15.66"`
- **Formato:** Endereço IPv4 como string
- **Rede:** Deve ser acessível a partir do servidor RAN Monitor
- **Verificação:** `ping 10.7.15.66` deve ter sucesso

name (String)

- Nome amigável para identificação
- Valor atual: `"ONS-Lab-Airscale"`
- **Uso:** Aparece na interface Web, logs e tags do InfluxDB
- **Recomendação:** Use nomes descritivos (códigos de site, locais, etc.)
- **Exemplos:**
  - `"NYC-Site-A-BS1"`
  - `"LAX-Tower-Main"`
  - `"TestLab-Airscale-01"`

port (String)

- Porta da interface de gerenciamento na estação base
- Valor atual: `"8080"`

- **Padrão:** A Nokia AirScale normalmente usa 8080
- **Verificação:** Verifique a documentação da estação base
- **Nota:** O valor é uma string, não um inteiro

web_username (String)

- Nome de usuário para autenticação WebLM
- Valor atual: `"Nemuadmin"`
- **Uso:** Usado para chamadas de API para gerenciar a estação base
- **Privilégios:** Deve ter acesso de leitura/gravação à configuração
- **Nota:** Sensível a maiúsculas e minúsculas

web_password (String)

- Senha para autenticação WebLM
- Valor atual: `"nemuuser"`
- **Segurança:** Deve ser armazenada em variáveis de ambiente em produção
- **Rotação:** Alterar regularmente de acordo com a política de segurança

Adicionando Múltiplas Estações Base

Para monitorar várias estações base, adicione entradas adicionais à lista `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"
  }
]
```

Configuração do InfluxDB

```
config :ran_monitor, RanMonitor.InfluxDbConnection,
  auth: [
    username: "monitor",
    password: "sideunderTexasgalaxyview_61"
  ],
  database: "nokia-monitor",
  host: "10.179.2.135"
```

Propósito: Configura a conexão com o banco de dados de séries temporais InfluxDB para armazenar métricas, alarmes e dados de configuração.

Parâmetros Explicados

auth (Lista de palavras-chave)

- Credenciais de autenticação para o InfluxDB
- **username:** Conta de usuário do InfluxDB (`"monitor"`)
- **password:** Senha do InfluxDB (`"sideunderTexasgalaxyview_61"`)
- **Nota:** Para InfluxDB 2.x, isso pode ser um token de API em vez disso

database (String)

- Nome do bucket/banco de dados no InfluxDB
- Valor atual: `"nokia-monitor"`
- **InfluxDB 1.x:** Nome do banco de dados
- **InfluxDB 2.x:** Nome do bucket
- **Criação:** Deve ser criado antes de iniciar o 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)

- Endereço do servidor InfluxDB
- Valor atual: `"10.179.2.135"`
- **Formato:** Endereço IP ou nome do host
- **Porta:** A porta padrão do InfluxDB (8086) é assumida
- **Exemplos:**
  - `"localhost"` - Mesmo servidor que o RAN Monitor
  - `"10.179.2.135"` - Servidor InfluxDB remoto
  - `"influxdb.example.com"` - Nome do host

Notas de Conexão do InfluxDB

Acesso à Rede:

- O RAN Monitor deve ser capaz de alcançar o servidor InfluxDB na porta 8086
- Verifique: `curl http://10.179.2.135:8086/ping`

Políticas de Retenção:

- Definidas via página de Retenção de Dados da interface Web
- Padrão: 30 dias (720 horas)
- Pode ser personalizado por estação base

Desempenho de Escrita:

- O InfluxDB recebe gravações a cada intervalo de coleta (60s padrão)
- Cada estação base gera centenas de pontos de dados por intervalo
- Monitore o espaço em disco do InfluxDB regularmente

Melhores Práticas de Configuração

Segurança

1. Proteja Dados Sensíveis

```
# Em vez de senhas codificadas:
password: "omnitouch2024"

# Use variáveis de ambiente:
password: System.get_env("DB_PASSWORD") || "default_password"
```

2. Restringir Permissões de Arquivo

```
chmod 600 config/runtime.exs
chown ran_monitor:ran_monitor config/runtime.exs
```

3. Nunca Comite Segredos

- Use `.gitignore` para runtime.exs se contiver segredos
- Use variáveis de ambiente ou sistemas de gerenciamento de segredos
- Rotacione senhas regularmente

Desempenho

1. Dimensionamento do Pool de Banco de Dados

- Monitore o uso de conexões
- Aumente o pool_size se estiver vendo erros de tempo limite de conexão
- Cada dispositivo precisa de ~2 conexões durante a sondagem ativa

2. Intervalos de Coleta

- Equilibre entre granularidade de dados e carga do sistema
- Intervalos de 60 segundos funcionam bem para a maioria das implantações
- Intervalos mais curtos (15s) para solução de problemas

3. Otimização do InfluxDB

- Use políticas de retenção para gerenciar o uso de disco
- Monitore o desempenho de gravação do InfluxDB
- Considere um servidor InfluxDB separado para grandes implantações

Confiabilidade

1. Configuração de Rede

- Use endereços IP estáticos para todos os componentes
- Verifique rotas de rede entre o RAN Monitor e as estações base
- Teste a conectividade antes de adicionar dispositivos
- Configure regras de firewall adequadamente

2. Estratégia de Logging

- Desenvolvimento: `:debug` para solução de problemas detalhada
- Produção: `:info` para visibilidade operacional
- Sistemas críticos: Considere agregação de logs externa

3. Monitorando o RAN Monitor

- Monitore o monitor (meta-monitoramento)
- Fique atento a erros de conexão com o banco de dados
- Acompanhe as taxas de sucesso de gravação do InfluxDB
- Alerta sobre desconexões de estações base

Manutenção

1. Alterações de Configuração

- Sempre faça backup do runtime.exs antes de alterações
- Teste a configuração em desenvolvimento primeiro
- Documente alterações com comentários
- Reinicie o RAN Monitor após alterações de configuração

2. Adicionando Estações Base

```
# 1. Edite o runtime.exs
vim config/runtime.exs

# 2. Valide a sintaxe do Elixir
elixir -c config/runtime.exs

# 3. Reinicie a aplicação
systemctl restart ran_monitor
```

3. Considerações de Escalonamento

- Monitore o uso de recursos (CPU, memória, rede)
- Aumente o tamanho do pool de banco de dados à medida que o número de dispositivos cresce
- Considere uma instância separada do InfluxDB em 50+ dispositivos
- Monitore o espaço em disco tanto para MySQL quanto para InfluxDB

Exemplo: Configuração Completa

Aqui está um exemplo completo com várias estações base e melhores práticas aplicadas:

```
import Config

#
==========================================================================
# Configuração do Banco de Dados
#
==========================================================================

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,  # Produção: ocultar stacktraces
  show_sensitive_data_on_connection_error: false,  # Produção: oculta
credenciais
  pool_size: 15  # 6 estações base * 2 + 3 de sobrecarga

#
==========================================================================
# Endpoints 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

#
==============================================================================
# Configuração do Logger
#
==============================================================================

config :logger,
  level: :info  # Configuração de produção

config :logger, :console,
  format: "$time $metadata[$level] $message\n",
  metadata: [:request_id]

#
==============================================================================
# Configuração 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 - Torre Principal
      %{
        address: "10.7.15.66",
        name: "Site-A-Main-Tower",
        port: "8080",
        web_username: "admin",
        web_password: System.get_env("BS_SITE_A_PASSWORD") || "passwo
      },
```

```
    # Site A - Torre de Backup
    %{
      address: "10.7.15.67",
      name: "Site-A-Backup-Tower",
      port: "8080",
      web_username: "admin",
      web_password: System.get_env("BS_SITE_A_PASSWORD") || "passwo
    },

    # Site B - Interno
    %{
      address: "10.7.16.10",
      name: "Site-B-Indoor-DAS",
      port: "8080",
      web_username: "admin",
      web_password: System.get_env("BS_SITE_B_PASSWORD") || "passwo
    },

    # Site C - Telhado
    %{
      address: "192.168.100.50",
      name: "Site-C-Rooftop",
      port: "8080",
      web_username: "admin",
      web_password: System.get_env("BS_SITE_C_PASSWORD") || "passwo
    },

    # Laboratório - Equipamento de Teste
    %{
      address: "10.5.198.100",
      name: "Lab-Test-Airscale-01",
      port: "8080",
      web_username: "Nemuadmin",
      web_password: "nemuuser"
    },

    # Laboratório - Desenvolvimento
    %{
      address: "10.5.198.101",
      name: "Lab-Dev-Airscale-02",
      port: "8080",
      web_username: "Nemuadmin",
      web_password: "nemuuser"
```

```
      }
    ]
  }

#
# Configuração do 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"
```

Documentação Relacionada

- Guia de Operações - Operações do dia a dia
- Guia de Configuração AirScale - Configurando estações base
- Referência de Contadores Nokia - Definições de contadores de desempenho
- Integração Grafana - Construindo dashboards e alertas
- Endpoints da API - Referência da API REST
- Política de Retenção de Dados - Gerenciando o ciclo de vida dos dados

Coleta de Dados MDT com TCE

Entidade de Coleta de Traços (TCE)

O RAN Monitor inclui uma Entidade de Coleta de Traços integrada para capturar e analisar mensagens de protocolo LTE/5G. Isso permite uma solução de problemas detalhada, testes de drive e otimização de RF.

O que é TCE?

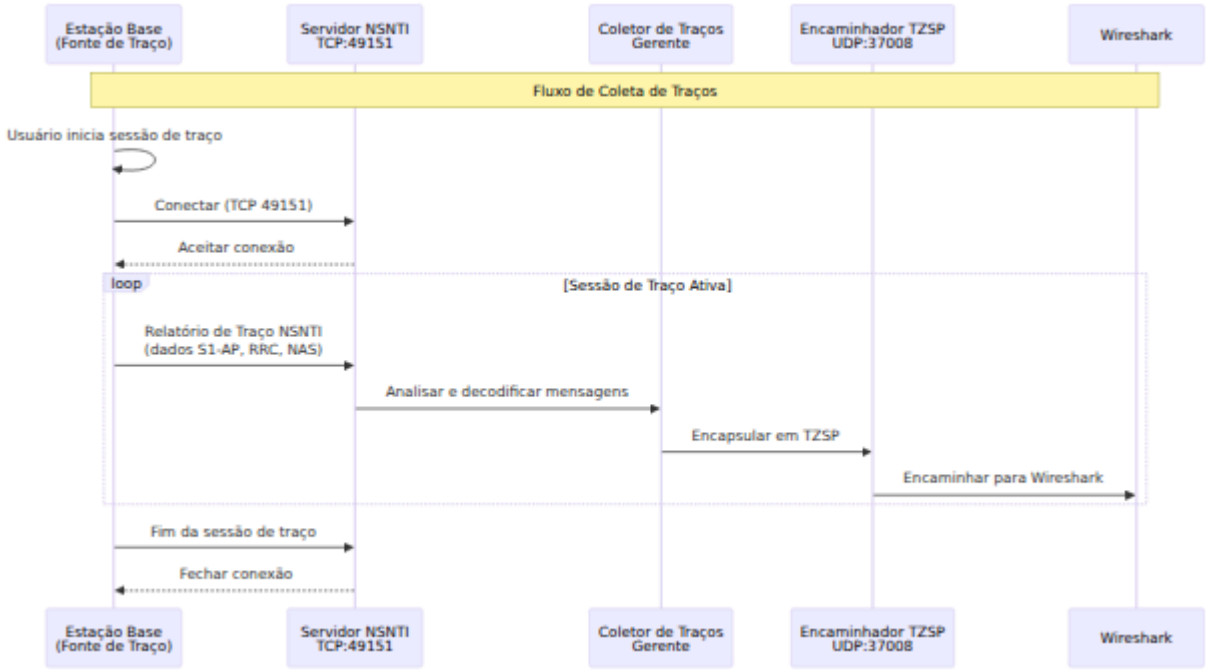
A Entidade de Coleta de Traços recebe dados de traço de estações base Nokia AirScale contendo:

- **Mensagens S1-AP** - Sinalização do plano de controle entre eNodeB e EPC
- **Mensagens RRC** - Sinalização de Controle de Recursos de Rádio
- **Mensagens NAS** - Sinalização do Estrato Não Acessível
- **Dados do Plano do Usuário** - Informações de throughput da camada PDCP

Componentes do TCE

Componente	Protocolo	Porta	Propósito
Servidor NSNTI	TCP	49151	Recebe mensagens de traço das estações base
Servidor TZSP	UDP	37008	Encaminha traços para o Wireshark para análise em tempo real
Decodificadores de Protocolo	ASN.1	-	Decodifica mensagens S1-AP e RRC

Como Funciona



A página de Coleta de Traços mostra conexões ativas, porta de escuta NSNTI (49151), configuração TZSP e estações base conectadas.

Configuração da Coleta de Traços

1. **Verifique se o TCE está em execução:**

```
ss -tlnp | grep 49151
# Deve mostrar: LISTEN 0.0.0.0:49151
```

2. **Configure o Traço da Estação Base:**

   - Defina o IP de destino do traço para o servidor RAN Monitor
   - Defina a porta de destino do traço para 49151
   - Ative as categorias de traço (S1-AP, RRC, NAS conforme necessário)
   - Inicie a sessão de traço

3. **Configure o Wireshark:**

Configuração Básica:

- Inicie a captura na interface que recebe pacotes TZSP
- Use o filtro de captura: `udp port 37008`

Configuração de Decodificação de Protocolo:

O RAN Monitor usa portas UDP específicas para identificar diferentes tipos de protocolo e canais RRC. Configure o recurso "Decode As" do Wireshark para decodificar corretamente esses protocolos:

Método 1: Usando a GUI do Wireshark

i. Vá para **Analisar → Decode As...**
ii. Clique no botão **+** para adicionar novas entradas
iii. Configure cada linha da seguinte forma:

Campo	Valor	Tipo	Atual	Decode As
udp.port	36412	Inteiro	(nenhum)	SCTP
sctp.port	36412	Inteiro	(nenhum)	S1AP
udp.port	37000	Inteiro	(nenhum)	TZSP
udp.port	37001	Inteiro	(nenhum)	LTE RRC (DL-CCCH)
udp.port	37002	Inteiro	(nenhum)	LTE RRC (DL-DCCH)
udp.port	37003	Inteiro	(nenhum)	LTE RRC (BCCH)
udp.port	37004	Inteiro	(nenhum)	LTE RRC (PCCH)
udp.port	37008	Inteiro	(nenhum)	TZSP
udp.port	37011	Inteiro	(nenhum)	LTE RRC (UL-CCCH)
udp.port	37012	Inteiro	(nenhum)	LTE RRC (UL-DCCH)
udp.port	38000	Inteiro	(nenhum)	MAC-LTE
udp.port	38001	Inteiro	(nenhum)	MAC-LTE (DL)
udp.port	38002	Inteiro	(nenhum)	MAC-LTE (BCH)
udp.port	38003	Inteiro	(nenhum)	MAC-LTE (PCH)
udp.port	38011	Inteiro	(nenhum)	MAC-LTE (UL)
udp.port	38012	Inteiro	(nenhum)	MAC-LTE (RACH)

Método 2: Usando o arquivo decode_as_entries

Crie ou edite `~/.config/wireshark/decode_as_entries` (Linux/Mac) ou `%APPDATA%\Wireshark\decode_as_entries` (Windows):

```
# Mapeamentos de Porta TZSP do 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
```

Guia de Referência de Portas:

Porta	Protocolo	Canal/Tipo	Descrição
36412	S1AP	-	Padrão de controle S1AP (eNodeB ↔ EPC)
37000	RRC	Genérico	Fallback para tipos de canal RRC desconhecidos
37001	RRC	DL-CCCH	Canal de Controle Comum de Downlink
37002	RRC	DL-DCCH	Canal de Controle Dedicado de Downlink
37003	RRC	BCCH-DL-SCH	Canal de Controle de Broadcast (Informação do Sistema)
37004	RRC	PCCH	Canal de Controle de Paging
37008	TZSP	-	Porta principal do ouvinte TZSP
37011	RRC	UL-CCCH	Canal de Controle Comum de Uplink (Solicitação de Conexão RRC)
37012	RRC	UL-DCCH	Canal de Controle Dedicado de Uplink (Relatórios de Medição)
38000	MAC-LTE	Genérico	Fallback para tipos de canal MAC desconhecidos
38001	MAC-LTE	Downlink	Canal Compartilhado de Downlink
38002	MAC-LTE	BCH	Canal de Broadcast
38003	MAC-LTE	PCH	Canal de Paging

Porta	Protocolo	Canal/Tipo	Descrição
38011	MAC-LTE	Uplink	Canal Compartilhado de Uplink
38012	MAC-LTE	RACH	Canal de Acesso Aleatório

Filtros de Exibição Úteis:

```
# Mostrar todos os pacotes TZSP
tzsp

# Mostrar protocolos específicos
s1ap || rrc || mac-lte

# Mostrar apenas mensagens RRC de uplink
udp.port == 37011 || udp.port == 37012

# Mostrar apenas mensagens RRC de downlink
udp.port == 37001 || udp.port == 37002

# Mostrar estabelecimento de conexão RRC
rrc.rrcConnectionRequest || rrc.rrcConnectionSetup

# Mostrar mensagens de handover
s1ap.HandoverRequired || s1ap.HandoverCommand
```

Casos de Uso

Teste de Drive:

- Capturar a experiência de RF do usuário final
- Analisar o desempenho de handover
- Medir a qualidade do sinal (RSRP, RSRQ, SINR)
- Identificar buracos de cobertura

Solução de Problemas:

- Depurar falhas na configuração de chamadas

- Analisar problemas de handover
- Investigar chamadas perdidas
- Revisar eventos de mobilidade

Otimização de RF:

- Validação do planejamento de PCI
- Otimização de relação de vizinhos
- Ajuste de parâmetros de handover
- Análise de cobertura e capacidade

Visão Geral

Minimização de Testes de Drive (MDT) permite coletar medições de rádio (RSRP, RSRQ, dados de cobertura) diretamente de UEs sem testes de drive tradicionais. Este guia mostra como capturar dados MDT de estações base Nokia AirScale usando a interface da Web do Omnitouch RAN Monitor e visualizá-los no Wireshark.

Arquitetura

A TCE (Entidade de Coleta de Traços) está integrada ao Omnitouch RAN Monitor e lida com a conversão de traços do protocolo Ne3s específico da Nokia em formatos padrão visualizáveis no Wireshark.

Pré-requisitos

Licenças Necessárias

O Nokia Airscale requer ativações de recursos, incluindo **Dados de Medição por Chamada** para coletar esses dados, e esses recursos devem estar habilitados e configurados.

Entre em contato com a ONS se precisar de ajuda com licenciamento ou tiver dúvidas sobre sua implantação específica.

Requisitos do Sistema

- Omnitouch RAN Monitor com TCE em execução
- Wireshark 3.0+ instalado em sua máquina
- Plugins Lua do TCE instalados no Wireshark
- Conectividade de rede com o AirScale

Configurando a Rastreabilidade MDT

O TCE embutido no RAN Monitor converte os dados Nokia recebidos em formatos visualizáveis padrão do Wireshark.

Passo 1: Configure a Entidade de Coleta de Traços

Use a interface da Web do RAN Monitor para configurar a estação base para enviar traços para o TCE:

1. Abra a interface da Web: `https://<ran-monitor-ip>:9443`
2. Navegue até a página **Estações Base**
3. Clique no dispositivo que você deseja rastrear
4. Vá para a seção **Gerenciamento de Configuração**
5. Baixe a configuração atual (backup)
6. Edite a configuração para adicionar/atualizar as configurações do TCE:
   - **IP da Entidade de Coleta de Traços**: `<Seu IP do RAN Monitor>`
   - **Porta da Entidade de Coleta de Traços**: `49151`
7. Faça o upload da configuração modificada
8. Valide a configuração (aguarde a validação ser concluída)
9. Ative a configuração

Para ajuda com parâmetros de configuração específicos ou versões de software AirScale, entre em contato com a ONS.

Passo 2: Configure o MDT no AirScale

Ative a rastreabilidade MDT em sua estação base. As opções de configuração incluem:

- **Tipo de Traço**: MDT Imediato (em tempo real) ou MDT Registrado (modo ocioso)
- **Escopo da Área**: Específico da Célula, Área de Rastreamento ou PLMN
- **Intervalo de Medição**: Com que frequência os UEs relatam (por exemplo, 5000ms)
- **Tipo de Medição**: RSRP, RSRQ ou ambos
- **Profundidade do Traço**: Mínima, Média ou Máxima

Entre em contato com a ONS para orientações sobre como configurar esses parâmetros para seu caso de uso específico.

Passo 3: Ative a Sessão de Traço

Uma vez configurada, ative a sessão de traço no AirScale. A estação base começará a enviar dados MDT para o TCE, que por sua vez os encaminhará para sua máquina de monitoramento.

Visualizando Dados MDT no Wireshark

Configurar Captura do Wireshark

1. Inicie o Wireshark em sua máquina
2. Capture na **interface de loopback** (`lo` no Linux, `lo0` no macOS, `Loopback` no Windows)
3. Defina o filtro de captura: `udp port 37008`
4. Inicie a captura

Exemplo de captura do Wireshark mostrando mensagens do plano de controle S1AP (InitialUEMessage, Attach request), mensagens LTE RRC (RRCConnectionReject, RRCConnectionReestablishment) e vários fluxos de sinalização capturados via TCE.

Filtrar por Medições MDT

Uma vez que os dados estão fluindo, use esses filtros de exibição:

```
# Mostrar todos os Relatórios de Medição RRC
lte-rrc.measurementReport

# Mostrar todas as mensagens RRC de uplink
udp.dstport >= 37011 && udp.dstport <= 37012

# Filtrar por RSRP fraco (< -100 dBm)
lte-rrc.rsrpResult < 40

# Filtrar por RSRQ fraco (< -12 dB)
lte-rrc.rsrqResult < 22
```

Compreendendo os Dados

As medições MDT aparecem como mensagens **Relatório de Medição RRC** contendo:

- **Medições da Célula Servidora**: RSRP e RSRQ para a célula conectada
- **Medições de Células Vizinhas**: RSRP e RSRQ para células próximas
- **IDs de Célula**: IDs de célula física para correlação

- **Localização GPS**: Se configurado e suportado pelo UE

Expanda a mensagem RRC no Wireshark para ver medições detalhadas:

```
Controle de Recursos de Rádio (RRC)
└─ UL-DCCH-Message
    └─ mensagem: measurementReport
        └─ MeasurementReport
            └─ measResults
                ├─ measResultServCell (RSRP/RSRQ da célula
servidora)
                └─ measResultNeighCells (medições de células
vizinhas)
```

Exportar para Análise

Para analisar dados offline:

1. **Arquivo → Exportar Dissecções de Pacotes → Como CSV**
2. Incluir campos: `lte-rrc.rsrpResult`, `lte-rrc.rsrqResult`, `lte-rrc.physCellId`
3. Processar no Excel, Python ou outras ferramentas

Casos de Uso Comuns

Análise de Cobertura: Procure áreas com RSRP/RSRQ fracos

```
lte-rrc.rsrpResult < 40 || lte-rrc.rsrqResult < 22
```

Análise de Handover: Veja quais células vizinhas os UEs estão relatando

```
lte-rrc.MeasResultListEUTRA
```

Detecção de Interferência: RSRP bom, mas RSRQ fraco indica interferência

```
lte-rrc.rsrpResult > 50 && lte-rrc.rsrqResult < 20
```

Solução de Problemas

Sem dados no Wireshark?

- Verifique se o TCE está em execução: `ps aux | grep beam`
- Verifique se o Wireshark está capturando loopback com o filtro `udp port 37008`
- Confirme se a sessão de traço está ativa no AirScale
- Verifique se o IP/porta do TCE estão configurados corretamente na estação base

Dados incompletos?

- Verifique se as licenças estão ativas (MDT + Medição por Chamada)
- Aumente a profundidade do traço para MÁXIMO
- Certifique-se de que os UEs suportam MDT (LTE Release 10+)

Para ajuda com configuração, problemas de licenciamento ou perguntas específicas sobre o AirScale, entre em contato com a ONS.

Lista de Verificação para Início Rápido

- [ ] Verifique se as licenças MDT e de medição por chamada estão ativas
- [ ] Configure o IP do TCE (IP do RAN Monitor) e a porta 49151 no AirScale
- [ ] Inicie o TCE no servidor RAN Monitor
- [ ] Ative a sessão de traço MDT na estação base
- [ ] Inicie a captura do Wireshark no loopback com o filtro `udp port 37008`
- [ ] Aplique o filtro de exibição: `lte-rrc.measurementReport`
- [ ] Analise as medições e exporte conforme necessário

Suporte

- **Serviços de Rede Omnitouch (ONS)**: Para configuração do AirScale, licenciamento e assistência na implantação

Guia de Solução de Problemas

Resolução de Problemas para RAN Monitor

Problemas comuns, procedimentos de diagnóstico e soluções

Índice

Visão Geral

Este guia ajuda você a diagnosticar e resolver problemas comuns com o RAN Monitor. Cada seção fornece sintomas, etapas de diagnóstico e soluções.

Abordagem de Solução de Problemas

1. Identifique o Sintoma

- O que não está funcionando como esperado?
- Quando o problema começou?

- O que mudou recentemente?

2. Reúna Informações

- Verifique os logs da aplicação
- Revise o status do dispositivo na Interface Web
- Verifique a conectividade do banco de dados
- Revise as alterações de configuração recentes

3. Diagnostique a Causa Raiz

- Use ferramentas de diagnóstico
- Revise mensagens de erro
- Teste componentes individuais
- Isolar o problema

4. Implemente a Solução

- Aplique a correção com base no diagnóstico
- Verifique se a solução resolve o problema
- Monitore para recorrência
- Documente as descobertas

Antes de Começar

Verifique o Básico:

- O RAN Monitor está em execução? (`ps aux | grep ran_monitor`)
- Os serviços necessários estão em execução? (MySQL, InfluxDB)
- A conectividade de rede está funcionando?
- Houve mudanças recentes?

Problemas de Conexão de Dispositivos

Problema: Dispositivo Não Registrado

Sintomas:

- O dispositivo mostra "Não Registrado" na Interface Web
- Status vermelho (falhou) na página de Estações Base
- Nenhuma métrica está sendo coletada do dispositivo
- Mensagens de erro nos logs da aplicação

Etapas de Diagnóstico:

1. Verifique a Conectividade da Rede

```
# Teste a conectividade básica
ping <device-ip>

# Teste a porta de gerenciamento
telnet <device-ip> 8080
```

Esperado: Ping e conexão telnet bem-sucedidos
Se Falhar: Problema de rede - verifique rotas, firewall, status do dispositivo

2. Verifique a Configuração

Na Interface Web → Estações Base → Clique no dispositivo → Revise a configuração:

- O endereço IP está correto?
- A porta está correta (normalmente 8080)?
- As credenciais estão configuradas?

Em `config/runtime.exs`:

```
%{
  address: "10.7.15.66",  # IP correto?
  name: "Site-A-BS1",
  port: "8080",           # Porta correta?
  web_username: "admin",  # Nome de usuário correto?
  web_password: "password" # Senha correta?
}
```

3. Verifique os Logs da Aplicação

Interface Web → Logs da Aplicação → Filtrar pelo nome do dispositivo

Procure por:

- `[error] Authentication failed` → Credenciais incorretas
- `[error] Connection refused` → Problema de porta/firewall
- `[error] Timeout` → Problema de conectividade de rede
- `[error] Certificate error` → Problema com chave/certificado do gerente

Soluções:

Problema de Rede:

1. Verifique se o dispositivo está ligado e operacional
2. Verifique as rotas de rede entre o RAN Monitor e o dispositivo
3. Verifique se o firewall permite:
   - RAN Monitor → Porta do dispositivo 8080
   - Dispositivo → RAN Monitor porta 9076 (webhooks)
4. Teste diretamente do servidor RAN Monitor

Credenciais Incorretas:

1. Verifique se as credenciais funcionam diretamente na interface WebLM do dispositivo
2. Atualize as credenciais em `config/runtime.exs`
3. Reinicie o RAN Monitor
4. Monitore os logs para registro bem-sucedido

Problema de Porta/Firewall:

1. Verifique a porta correta na configuração
2. Verifique as regras do firewall em ambos os lados
3. Teste a acessibilidade da porta: `telnet <device-ip> 8080`
4. Revise as configurações de segurança do lado do dispositivo

Problema com Chave/Certificado do Gerente:

1. Verifique se os arquivos existem:
   - `priv/external/nokia/ne.key.pem`
   - `priv/external/nokia/ne.cert.der`
2. Verifique as permissões dos arquivos (devem ser legíveis)
3. Verifique se os arquivos são credenciais válidas do gerente Nokia
4. Entre em contato com o suporte da Nokia se as chaves forem inválidas

---

Problema: Sessão Continua Expirando

Sintomas:

- O dispositivo desconecta e reconecta repetidamente
- Mensagens "Sessão expirada" nos logs
- Status intermitente vermelho/verde na Interface Web
- Lacunas na coleta de métricas

Etapas de Diagnóstico:

1. Verifique as Informações da Sessão

Interface Web → Estações Base → Clique no dispositivo → Ciclo de Vida da Sessão:

- Qual é o tempo de expiração da sessão?
- O keep-alive está funcionando?
- Com que frequência a sessão está expirando?

2. Verifique o Intervalo de Keep-Alive

Em `config/runtime.exs`:

```
nokia: %{
  ne3s: %{
    reregister_interval: 30  # Deve ser de 30 a 60 segundos
  }
}
```

3. Verifique a Estabilidade da Rede

- Existem problemas intermitentes de rede?
- Verifique se há perda de pacotes: `ping <device-ip> -c 100`
- Revise os logs da rede para interfaces flutuantes

4. Verifique a Sincronização do Relógio

```
# No servidor RAN Monitor
date

# No dispositivo (se acessível)
# Verifique se o horário está sincronizado
```

Soluções:

Intervalo de Keep-Alive Muito Longo:

1. Reduza `reregister_interval` para 30 segundos
2. Reinicie o RAN Monitor
3. Monitore a estabilidade da sessão

Instabilidade da Rede:

1. Trabalhe com a equipe de rede para diagnosticar
2. Verifique se há conectividade intermitente
3. Revise os logs de switches/roteadores
4. Considere caminhos de rede redundantes

Sincronização do Relógio:

1. Configure NTP em ambos RAN Monitor e dispositivos
2. Verifique se os relógios estão sincronizados
3. Verifique se há grandes diferenças de horário

Problema do Lado do Dispositivo:

1. Verifique os logs do dispositivo para erros
2. Verifique se a interface de gerenciamento do dispositivo está estável
3. Considere reiniciar o dispositivo se um problema de software for suspeito

---

Problema: Métricas Não Aparecendo

Sintomas:

- O dispositivo aparece como "Associado" (verde) na Interface Web
- Mas nenhuma métrica aparece no InfluxDB
- Nenhum dado nos dashboards do Grafana
- A página de Status do InfluxDB mostra contagens zero ou baixas

Etapas de Diagnóstico:

1. Verifique se o Dispositivo Está Associado

Interface Web → Estações Base:

- O status do dispositivo está verde?
- O timestamp do último contato é recente?
- A sessão está ativa?

2. Verifique a Conexão com o InfluxDB

Interface Web → Status do InfluxDB:

- O status da conexão está verde?
- O RAN Monitor pode escrever no InfluxDB?

Teste a conectividade:

```
# Do servidor RAN Monitor
curl http://<influxdb-host>:8086/ping
```

3. Verifique os Logs da Aplicação

Procure por:

- `[error] InfluxDB write failed` → Problema de conexão ou permissão
- `[error] Failed to collect metrics` → Problema de comunicação com o dispositivo
- `[info] Metrics collected: 0` → Dispositivo não retornando dados

4. Verifique o InfluxDB Diretamente

Consulta o InfluxDB para dados recentes:

```
# 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()'
```

Soluções:

Problema de Conexão com o InfluxDB:

1. Verifique se o InfluxDB está em execução
2. Verifique `config/runtime.exs` para:
   - Endereço do host
   - Porta (8086)

    - Nome do banco de dados/bucket
    - Credenciais/token da API
3. Teste a conectividade do servidor RAN Monitor
4. Verifique se o firewall permite a porta 8086
5. Reinicie o RAN Monitor após corrigir a configuração

Problema de Permissão do InfluxDB:

1. Verifique se as credenciais têm permissão de escrita no bucket/banco de dados
2. Verifique os logs do InfluxDB para erros de autenticação
3. Recrie o token da API com as permissões adequadas
4. Atualize `config/runtime.exs` com o novo token
5. Reinicie o RAN Monitor

Armazenamento do InfluxDB Cheio:

1. Verifique o espaço em disco: `df -h`
2. Revise as políticas de retenção
3. Limpe dados antigos ou expanda o armazenamento
4. Veja o Guia de Políticas de Retenção de Dados

Dispositivo Não Retornando Dados:

1. Verifique se o dispositivo está configurado para enviar métricas
2. Verifique se a URL do webhook está correta na configuração do dispositivo
3. Verifique os logs do dispositivo para erros
4. Verifique se o receptor de webhook do RAN Monitor está em execução (porta 9076)

Problemas de Coleta de Dados

Problema: Lacunas em Dados Históricos

Sintomas:

- Dashboards do Grafana mostram lacunas na série temporal
- Pontos de dados ausentes para certos períodos
- Consultas ao InfluxDB retornam resultados incompletos

Etapas de Diagnóstico:

1. Verifique o Tempo de Atividade da Aplicação

Houve interrupções de serviço durante o período da lacuna?

```
# Verifique os logs do sistema para reinicializações
journalctl -u ran_monitor --since "2025-12-29" --until "2025-12-
30"
```

2. Verifique o Histórico de Conectividade do Dispositivo

Interface Web → Estações Base → Dispositivo → Revise o histórico de "Último Contato"

- O dispositivo estava conectado durante o período da lacuna?
- Existem problemas de conectividade?

3. Verifique a Disponibilidade do InfluxDB

Houve interrupções no InfluxDB durante o período da lacuna?

- Verifique os logs do InfluxDB
- Revise o histórico de monitoramento/alertas

Soluções:

Inatividade do RAN Monitor:

- A lacuna de dados é normal durante uma interrupção de serviço
- Dados históricos não podem ser preenchidos retroativamente
- Documente o incidente e restaure o serviço

Desconexão do Dispositivo:

- Investigue por que o dispositivo se desconectou
- Corrija o problema de conectividade
- A lacuna de dados é normal durante a desconexão
- Dados futuros retomarão a coleta

Interrupção do InfluxDB:

- As métricas provavelmente foram coletadas, mas não armazenadas
- Verifique os logs do RAN Monitor para falhas de gravação
- Restaure o serviço do InfluxDB
- A lacuna de dados não pode ser recuperada

Prevenção:

- Implemente monitoramento para o tempo de atividade do RAN Monitor
- Configure alertas para desconexões prolongadas
- Monitore a saúde do InfluxDB
- Considere HA/redundância para sistemas críticos

Problemas na Interface Web

Problema: Não é Possível Acessar a Interface Web

Sintomas:

- O navegador não consegue se conectar a https://<ran-monitor-ip>:9443
- Timeout de conexão ou conexão recusada
- Erros de certificado SSL

Etapas de Diagnóstico:

1. Verifique se a Interface Web Está em Execução

Verifique os logs da aplicação:

```
[info] Running ControlPanelWeb.Endpoint with cowboy
```

Verifique o processo:

```
ps aux | grep control_panel
netstat -tulpn | grep 9443
```

2. Teste a Conectividade

De outra máquina:

```
telnet <ran-monitor-ip> 9443
```

Do próprio servidor RAN Monitor:

```
curl -k https://localhost:9443
```

3. Verifique o Firewall

```
# Verifique se a porta está aberta
sudo iptables -L -n | grep 9443

# Ou
sudo firewall-cmd --list-ports
```

Soluções:

Porta Não Aberta:

1. Adicione a regra do firewall:
   ```
   sudo firewall-cmd --add-port=9443/tcp --permanent
   sudo firewall-cmd --reload
   ```
2. Teste o acesso novamente

Interface Web Não Iniciada:

1. Verifique `config/runtime.exs` para a configuração do endpoint web
2. Verifique se os arquivos do certificado SSL existem
3. Verifique os logs da aplicação para erros de inicialização
4. Reinicie o RAN Monitor

Problemas com Certificado SSL:

1. Verifique se os arquivos do certificado existem e são legíveis:
   ```
   ls -l priv/cert/omnitouch.pem
   ls -l priv/cert/omnitouch.crt
   ```
2. Verifique a validade do certificado:
   ```
   openssl x509 -in priv/cert/omnitouch.crt -text -noout
   ```
3. Regenerate se expirado ou ausente
4. Reinicie o RAN Monitor

Porta Errada:

1. Verifique `config/runtime.exs` para a porta configurada
2. Use a porta correta no navegador
3. Ou defina a variável de ambiente `CONTROL_PANEL_HTTPS_PORT`

Problema: Interface Web Carrega, Mas Não Mostra Dados

Sintomas:

- A Interface Web é acessível
- As páginas carregam, mas mostram listas vazias ou contagens zero
- O dashboard não mostra dispositivos

Etapas de Diagnóstico:

1. Verifique a Configuração do Dispositivo

Há algo configurado em `config/runtime.exs`?

```
airscales: [
  # Deve haver pelo menos um dispositivo
]
```

2. Verifique a Conexão com o Banco de Dados

Os dispositivos estão armazenados no MySQL?

```
mysql -u ran_monitor_user -p ran_monitor -e "SELECT * FROM
airscales;"
```

3. Verifique os Logs da Aplicação

Procure por erros de conexão com o banco de dados ou falhas de consulta.

Soluções:

Nenhum Dispositivo Configurado:

1. Adicione dispositivos a `config/runtime.exs`
2. Reinicie o RAN Monitor
3. Os dispositivos devem aparecer na Interface Web

Problema de Conexão com o Banco de Dados:

1. Verifique se o MySQL está em execução
2. Verifique a configuração de conexão em `config/runtime.exs`
3. Teste a conexão com o banco de dados
4. Reinicie o RAN Monitor

Problemas de Banco de Dados

Problema: Erros de Conexão com o MySQL

Sintomas:

- Os logs da aplicação mostram erros de conexão com o banco de dados
- A Interface Web mostra erros ao carregar páginas
- Mensagens de "timeout de conexão com o banco de dados"

Etapas de Diagnóstico:

1. Verifique se o MySQL Está em Execução

```
systemctl status mysql
# ou
systemctl status mariadb
```

2. Teste a Conexão

Do servidor RAN Monitor:

```
mysql -h <mysql-host> -u <username> -p <database>
```

3. Verifique a Configuração

Em `config/runtime.exs`:

```
config :ran_monitor, RanMonitor.Repo,
  username: "ran_monitor_user",
  password: "password",
  hostname: "localhost",
  database: "ran_monitor",
  pool_size: 10
```

Soluções:

MySQL Não Está em Execução:

1. Inicie o serviço MySQL:
   ```
   systemctl start mysql
   ```
2. Verifique se inicia corretamente
3. O RAN Monitor reconectará automaticamente

Erro de Configuração de Conexão:

1. Verifique o hostname, nome de usuário, senha, nome do banco de dados
2. Teste a conexão manualmente
3. Atualize `config/runtime.exs` se estiver incorreto
4. Reinicie o RAN Monitor

Problema de Rede:

1. Verifique a conectividade de rede com o servidor MySQL
2. Verifique se o firewall permite a porta 3306
3. Verifique o endereço de ligação do MySQL (deve permitir conexões remotas, se necessário)

Muitas Conexões:

1. Verifique a configuração de max_connections do MySQL
2. Reduza pool_size na configuração, se necessário
3. Reinicie o RAN Monitor

Problemas de Desempenho

Problema: Alto Uso de CPU ou Memória

Sintomas:

- O RAN Monitor usa CPU ou RAM excessiva

- O sistema fica lento ou não responsivo
- Conexões com o banco de dados expirando
- Tempo de resposta degradado

Etapas de Diagnóstico:

1. Verifique o Uso de Recursos

```
# CPU e memória
top -p $(pgrep -f ran_monitor)

# Informações detalhadas do processo
ps aux | grep ran_monitor
```

2. Verifique o Número de Dispositivos Monitorados

Quantos dispositivos estão configurados?

- Mais dispositivos = mais recursos necessários
- Verifique se a contagem de dispositivos aumentou recentemente

3. Verifique os Intervalos de Coleta

Os intervalos de polling são muito frequentes?

- Mais frequente = maior uso de CPU/rede
- O padrão é 10 segundos para métricas

4. Verifique o Tamanho do Pool do Banco de Dados

Em `config/runtime.exs`:

```
pool_size: 10  # Pode precisar de ajuste
```

Soluções:

Demais Dispositivos para Recursos:

1. Monitore tendências de uso de recursos

2. Aumente os recursos do servidor (CPU/RAM)
3. Ou reduza o número de dispositivos monitorados
4. Considere escalar horizontalmente (múltiplas instâncias)

Pool do Banco de Dados Muito Grande:

1. Reduza pool_size na configuração
2. Regra geral: 2 conexões por dispositivo + 5 para a Interface Web
3. Reinicie o RAN Monitor
4. Monitore o uso de recursos

Vazamento de Memória:

1. Monitore o uso de memória ao longo do tempo
2. Se continuar aumentando, pode ser um vazamento de memória
3. Reinicie o RAN Monitor como uma correção temporária
4. Relate o problema com logs e métricas

Desempenho de Gravação do InfluxDB:

1. Verifique o uso de recursos do InfluxDB
2. Verifique se o InfluxDB não é um gargalo
3. Considere um servidor InfluxDB separado
4. Revise as políticas de retenção para reduzir o volume de dados

---

Problema: Resposta Lenta da Interface Web

Sintomas:

- A Interface Web leva muito tempo para carregar páginas
- O dashboard está lento
- Timeouts ao visualizar detalhes do dispositivo

Etapas de Diagnóstico:

1. Verifique os Recursos do Servidor

O servidor RAN Monitor está sobrecarregado?

```
top
free -h
df -h
```

2. Verifique o Desempenho do Banco de Dados

As consultas ao banco de dados estão lentas?

```
# Log de consultas lentas do MySQL
mysql -u root -p -e "SHOW VARIABLES LIKE 'slow_query_log%';"
```

3. Verifique a Latência da Rede

Há alta latência para o banco de dados ou clientes?

Soluções:

Problema de Recursos do Servidor:

1. Reduza a carga no servidor
2. Aumente os recursos do servidor
3. Mova bancos de dados para servidores separados

Desempenho do Banco de Dados:

1. Otimize a configuração do MySQL
2. Adicione índices, se necessário (as tabelas devem tê-los)
3. Aumente os recursos do servidor de banco de dados

Latência da Rede:

1. Investigue o caminho da rede
2. Considere mover componentes mais próximos
3. Use um banco de dados local, se possível

Problemas de Alarme

Problema: Alarmes Não Aparecendo

Sintomas:

- Falhas conhecidas não aparecem na página de Alarmes
- A contagem de alarmes é zero quando existem falhas
- Notificações de alarme atrasadas

Etapas de Diagnóstico:

1. Verifique se o Dispositivo Está Enviando Alarmes

Verifique na interface de gerenciamento do dispositivo se os alarmes estão configurados para serem enviados.

2. Verifique o Receptor de Webhook

O endpoint do webhook está em execução?

```
netstat -tulpn | grep 9076
```

Procure por:

```
tcp  0  0.0.0.0:9076  0.0.0.0:*  LISTEN
```

3. Verifique a Configuração do Webhook

Na configuração do dispositivo, verifique se a URL do webhook aponta para o RAN Monitor:

```
http://<ran-monitor-ip>:9076/webhook
```

4. Verifique os Logs da Aplicação

Procure por erros do receptor de webhook ou falhas de análise de alarme.

5. Verifique o InfluxDB

Os alarmes estão sendo gravados?

```
influx -database 'nokia-monitor' -execute '
  SELECT COUNT(*) FROM Alarms WHERE time > now() - 1h
'
```

Soluções:

Receptor de Webhook Não Está em Execução:

1. Verifique `config/runtime.exs` para a configuração do endpoint do webhook
2. Verifique se a porta 9076 está configurada
3. Reinicie o RAN Monitor
4. Verifique se a porta está ouvindo

Dispositivo Não Enviando:

1. Configure o dispositivo para enviar notificações de alarme
2. Verifique a URL do webhook na configuração do dispositivo
3. Teste a geração de alarmes no dispositivo

Firewall Bloqueando:

1. Verifique se o dispositivo pode alcançar a porta 9076 do RAN Monitor
2. Adicione a regra do firewall, se necessário
3. Teste a conectividade: `telnet <ran-monitor-ip> 9076` da rede do dispositivo

Falha de Gravação no InfluxDB:

1. Verifique a conexão com o InfluxDB
2. Verifique as permissões de gravação
3. Verifique a capacidade de armazenamento do InfluxDB

4. Revise os logs da aplicação para erros de gravação

Ferramentas de Diagnóstico

Logs da Aplicação

Acesse via Interface Web:

1. Navegue até a página de Logs da Aplicação
2. Filtre por nível de log
3. Pesquise por palavras-chave
4. Pause para revisar erros específicos

Acesse via Linha de Comando:

Se executando como serviço systemd:

```
journalctl -u ran_monitor -f
```

Se executando via mix:

- Os logs aparecem na saída do console

Níveis de Log:

- Emergência/Alerta/Critico - Problemas críticos do sistema
- Erro - Erros que precisam de atenção
- Aviso - Problemas potenciais
- Info - Mensagens operacionais normais
- Debug - Informações de diagnóstico detalhadas

Termos de Pesquisa Úteis:

- Nome do dispositivo (por exemplo, "Site-A-BS1")
- "error" ou "failed"

- "InfluxDB" ou "MySQL"
- "registration" ou "session"

Consultas ao InfluxDB

Consulta por métricas recentes:

```
influx -database 'nokia-monitor' -execute '
  SELECT * FROM PerformanceMetrics
  WHERE basebandName='''Site-A-BS1'''
  AND time > now() - 5m
  LIMIT 10
'
```

Contar métricas por dispositivo:

```
influx -database 'nokia-monitor' -execute '
  SELECT COUNT(*) FROM PerformanceMetrics
  GROUP BY basebandName
'
```

Consulta por alarmes:

```
influx -database 'nokia-monitor' -execute '
  SELECT * FROM Alarms
  WHERE time > now() - 1h
'
```

Consultas ao MySQL

Verifique os dispositivos configurados:

```
SELECT name, address, port, registration_status
FROM airscales;
```

Verifique erros no banco de dados:

```
mysql -u ran_monitor_user -p ran_monitor -e "SHOW PROCESSLIST;"
```

Diagnósticos de Rede

Teste a conectividade:

```
# Conectividade básica
ping <device-ip>

# Acessibilidade da porta
telnet <device-ip> 8080
nc -zv <device-ip> 8080

# Rastreio de rota
traceroute <device-ip>
```

Verifique o firewall:

```
# Liste as regras
sudo iptables -L -n -v

# Verifique uma porta específica
sudo iptables -L -n | grep 8080
```

Obtendo Ajuda

Antes de Contatar o Suporte

Reúna as seguintes informações:

1. Descrição do Problema

- O que não está funcionando?
- Quando começou?

- O que mudou recentemente?

2. Mensagens de Erro

- Copie as mensagens de erro exatas dos logs
- Inclua timestamps
- Anote a frequência dos erros

3. Informações do Sistema

- Versão do RAN Monitor
- Sistema operacional e versão
- Versões do banco de dados (MySQL, InfluxDB)
- Número de dispositivos monitorados

4. Resultados de Diagnóstico

- Resultados das etapas de diagnóstico acima
- Trechos de logs relevantes
- Configuração (sanitizar senhas)

5. Impacto

- Quantos dispositivos afetados?
- Isso está bloqueando operações?
- Qual é o impacto nos negócios?

Recursos de Documentação

- **Guia da Interface Web** - Referência do painel de controle
- **Guia de Operações Comuns** - Tarefas rotineiras
- **Guia de Configuração em Tempo de Execução** - Detalhes de configuração
- **Guia de Integração do Grafana** - Configuração de análises
- **Guia de Gerenciamento de Alarmes** - Manipulação de alarmes
- **Guia de Políticas de Retenção de Dados** - Gerenciamento de dados
- **Guia de Operações** - Visão geral completa

Recursos de Autoatendimento

Verifique os Logs Primeiro:

- Página de Logs da Aplicação na Interface Web
- Logs do sistema: `journalctl -u ran_monitor`
- Logs do banco de dados

Revise Alterações Recentes:

- Modificações em arquivos de configuração
- Adições/remoções de dispositivos
- Mudanças na rede
- Atualizações de software

Teste a Funcionalidade Básica:

- Você consegue acessar a Interface Web?
- Os dispositivos estão aparecendo como conectados?
- O InfluxDB está acessível?
- As métricas estão fluindo?

Escalonamento

Se você não conseguir resolver o problema:

1. Documente todas as etapas de diagnóstico realizadas
2. Reúna as informações listadas acima
3. Contate o suporte da Omnitouch com os detalhes
4. Esteja preparado para fornecer:
    - Arquivos de configuração (sanitizados)
    - Trechos de logs
    - Capturas de tela, se relevante
    - Etapas para reproduzir

Documentação Relacionada

- **Guia de Operações** - Visão geral operacional completa
- **Guia da Interface Web** - Guia do usuário do painel de controle
- **Guia de Operações Comuns** - Tarefas do dia a dia
- **Guia de Gerenciamento de Alarmes** - Procedimentos de manipulação de alarmes
- **Guia de Configuração em Tempo de Execução** - Referência de configuração
- **Guia de Integração do Grafana** - Análises e dashboards
- **Guia de Políticas de Retenção de Dados** - Gerenciamento do ciclo de vida dos dados

Guia da Interface Web

Painel de Controle do RAN Monitor - Referência da Interface do Usuário

Guia completo para o uso do painel de controle baseado na web do RAN Monitor

---

Índice

Documentação Relacionada

- **Guia de Gerenciamento de Firmware** - Documentação completa do repositório de firmware

---

Visão Geral

O RAN Monitor inclui um painel de controle baseado na web para monitoramento e gerenciamento operacional em tempo real. A Interface Web fornece visibilidade imediata sobre o status do dispositivo, alarmes, configuração e saúde do sistema.

Interface Web vs. Grafana

A Interface Web é Melhor Para:

- Verificações imediatas de status do dispositivo
- Monitoramento de alarmes em tempo real
- Gerenciamento de configuração
- Solução de problemas de sessão
- Administração do sistema

Grafana é Melhor Para:

- Análise de tendências históricas
- Painéis personalizados de KPI
- Planejamento de capacidade a longo prazo
- Identificação de padrões
- Relatórios executivos

Para painéis e análises do Grafana, consulte o Guia de Integração do Grafana.

Acessando a Interface Web

O painel de controle é acessado via HTTPS:

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

Porta Padrão: 9443 (configurável via variável de ambiente `CONTROL_PANEL_HTTPS_PORT`)

Certificados SSL:

- Certificados autoassinados funcionam para ambientes de laboratório
- A produção deve usar certificados assinados por CA
- Certificados configurados em `config/runtime.exs`

Para detalhes de configuração, consulte o Guia de Configuração em Tempo de Execução.

Atualização Automática: A maioria das páginas é atualizada automaticamente a cada 5 segundos para mostrar dados em tempo real.

Painel Principal

O painel fornece uma visão geral da sua infraestrutura RAN.

Seções Principais

Status do Sistema

- Indicadores de saúde geral
- Tempo de atividade e conectividade do sistema

Resumo do Dispositivo

- Contagem de dispositivos associados/falhados
- Visão geral do status de registro
- Instantâneo rápido da saúde do dispositivo

Alarmes Ativos

- Contagem atual de falhas por severidade
- Níveis de severidade codificados por cores (Crítico, Maior, Menor, Aviso)
- Links rápidos para detalhes do alarme

Atividade Recente

- Últimos eventos e mudanças
- Atualizações de configuração
- Mudanças de status da sessão

Recursos

- Atualizações automáticas a cada 5 segundos
- Indicadores de status codificados por cores (verde = saudável, vermelho = problemas)
- Navegação clicável para visualizações detalhadas
- Atualizações de métricas em tempo real

Página das Estações Base

Visualize todos os dispositivos gerenciados com seu status atual e informações da sessão.

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

A página de Status das BTS mostrando a lista de dispositivos com status de conexão, estado da sessão e botões de ação.

Resumo de Estatísticas

A barra superior mostra contagens agregadas de dispositivos:

Estatística	Descrição
Total de Sites	Número de estações base configuradas
Conectados	Sites com sessões ativas que enviaram dados de configuração e PM desde a última reinicialização
Pendentes	Sites que estão registrados, mas ainda não enviaram todos os tipos de dados
Desconectados	Sites que não estão registrados ou inacessíveis

Tabela de Dispositivos

Coluna	Descrição
Nome	Nome do site conforme configurado
Status	Status da conexão (veja abaixo)
Endereço	Endereço IP e porta do dispositivo
Sessão	Estado da sessão: "Ativa" (verde) ou "Nenhuma" (cinza)
Ações	Botões de ação do dispositivo

Estados de Status

Status	Ícone	Descrição
Conectado		Registrado, sessão ativa, tanto configuração quanto dados PM recebidos desde a última reinicialização
Aguardando Dados PM		Sessão ativa e configuração recebida, mas sem dados PM ainda (o ciclo PM do eNodeB é tipicamente a cada 15 minutos)
Sessão Ativa		Registrado com sessão ativa, aguardando envio inicial de dados
Registrando		Registro do NE3S em andamento
Desconectado		Não registrado ou inacessível

Botões de Ação

Cada linha de dispositivo possui botões de ação:

Botão	Descrição
Ping	Testar conectividade de rede com o dispositivo
Config	Visualizar a configuração atual do dispositivo
Config Ops	Acessar operações de gerenciamento de configuração (baixar, enviar, validar, ativar)
Forçar Nova Tentativa	Forçar tentativa de re-registro para dispositivos desconectados

Painel de Detalhes do Dispositivo

Clicando em uma linha de dispositivo, são exibidos detalhes adicionais:

Campo	Descrição
ID do Gerente	Identificador interno do gerente
ID da Sessão	Identificador da sessão atual
Tipo de Agente	Tipo de agente do dispositivo (por exemplo, COMA)
Fornecedor	Fornecedor do dispositivo (Nokia)

Filtragem e Pesquisa

- Filtrar por status de conexão
- Pesquisar por nome do dispositivo ou endereço IP
- Classificar por qualquer coluna

Visualização de Detalhes do Dispositivo

Clique em qualquer dispositivo da página das Estações Base para ver informações abrangentes.

Detalhes do Registro

- Identidade do gerente e status de autenticação
- Carimbo de data/hora do registro
- Credenciais de autenticação em uso
- Chaves e certificados do gerente

Ciclo de Vida da Sessão

- Hora de criação da sessão
- Hora de expiração da sessão
- Intervalo e status de keep-alive
- Último carimbo de data/hora de keep-alive
- Tempo restante até a expiração

Métricas Recentes

- Últimos instantâneos de dados de desempenho
- Valores de contadores e carimbos de data/hora
- Status da coleta de métricas
- Intervalos de coleta de dados

Alarmes Ativos

- Falhas atuais para este dispositivo específico
- Severidade e descrição do alarme
- Carimbos de data/hora dos alarmes
- Informações sobre a causa provável

Estado da Configuração

- Valores atuais dos parâmetros
- Mudanças recentes na configuração
- Carimbo de data/hora da configuração
- Histórico de mudanças de parâmetros

Página de Alarmes

Monitore todas as falhas em sua rede em uma visão centralizada.

Informações sobre Alarmes

Níveis de Severidade:

- **Crítico** (Vermelho) - Afetando o serviço, ação imediata necessária
- **Maior** (Laranja) - Degradação significativa, atenção urgente necessária
- **Menor** (Amarelo) - Não afetando o serviço, deve ser abordado
- **Aviso** (Azul) - Informativo, monitorar para tendências
- **Resolvido** (Verde) - Alarme anteriormente ativo foi resolvido

Detalhes do Alarme:

- Descrição do problema
- Causa provável
- Sistema afetado (DN - Nome Distinto)
- Carimbos de data/hora (quando o alarme ocorreu e foi atualizado pela última vez)

Recursos

Codificação por Cores:

- Identificação visual imediata da severidade
- Vermelho = Alarmes críticos
- Laranja = Alarmes maiores
- Amarelo = Alarmes menores
- Azul = Avisos
- Verde = Resolvido

Classificação e Filtragem:

- Classificar por severidade, dispositivo ou tempo
- Filtrar por tipo de alarme
- Pesquisar por problemas específicos

Links de Dispositivos:

- Clique no alarme para ver detalhes do dispositivo afetado
- Referenciar com métricas do dispositivo
- Navegar para a configuração do dispositivo

Para procedimentos detalhados de manuseio de alarmes, consulte o Guia de Gerenciamento de Alarmes.

Gerenciamento de Configuração

A Interface Web fornece ferramentas para gerenciar configurações de dispositivos de forma segura e eficiente.

Baixar Configuração

Objetivo: Recuperar e fazer backup da configuração atual

Passos:

1. Navegue até a página de detalhes do dispositivo
2. Clique em "Baixar Configuração"
3. A configuração é recuperada do dispositivo
4. Salve a configuração como um arquivo XML

Melhor Prática: Sempre baixe e salve a configuração antes de fazer alterações

Enviar Configuração (Provisionar)

Objetivo: Aplicar uma nova configuração a um dispositivo em uma única operação

A operação de provisionamento realiza o download, validação e ativação de forma atômica no dispositivo. Um fallback da configuração atual em execução é salvo automaticamente antes que a nova configuração seja aplicada.

Passos:

1. Clique em "Config Ops" no dispositivo alvo
2. Selecione um arquivo de configuração XML (arraste e solte ou clique para navegar)
3. Clique em "Enviar Configuração para o Dispositivo"
4. O dispositivo baixa, valida e ativa a configuração
5. Monitore a mensagem de resultado para sucesso ou erros

Como funciona:

- O dispositivo recebe o arquivo de configuração e cria um plano interno
- O plano é validado contra o esquema do dispositivo e o estado atual
- Se a validação passar, a configuração atual em execução é salva como fallback
- A nova configuração é ativada imediatamente
- Se a ativação falhar, o dispositivo pode reverter para o fallback

Avançado: Fluxo Manual em 3 Etapas

Para casos em que você precisa de mais controle (por exemplo, preparar uma configuração para revisão antes da ativação), a seção avançada no diálogo Config Ops fornece as etapas individuais:

1. **Preparar (Baixar)** - Envie a configuração para criar um plano no dispositivo sem ativar. Retorna um ID de Plano.
2. **Validar** - Valide um plano preparado pelo seu ID de Plano. Confirma que a configuração está sintaticamente e semanticamente correta.
3. **Ativar** - Aplique um plano validado pelo seu ID de Plano. Toma efeito imediatamente.

O ID do Plano da etapa de preparação é automaticamente preenchido nos campos de validação e ativação.

Fluxo de Trabalho de Configuração

Processo Recomendado:

1. Baixe a configuração atual (backup)

2. Modifique a configuração offline
3. Envie a nova configuração usando a operação de provisionamento
4. Verifique se as mudanças tiveram efeito
5. Monitore o dispositivo por estabilidade

Para detalhes de configuração da estação base, consulte o Guia de Configuração do AirScale.

Página de eNodeBs Não Configurados

Descubra e gerencie estações base que estão tentando se conectar e que ainda não estão configuradas no sistema.

Objetivo

A página de eNodeBs Não Configurados ajuda você a:

- Descobrir novas estações base na rede
- Identificar dispositivos tentando conexões não autorizadas
- Verificar identificadores de dispositivos antes de adicionar à configuração
- Rastrear tentativas de conexão de equipamentos desconhecidos

Informações Exibidas

ID do Agente

- Identificador do dispositivo detectado a partir das tentativas de conexão
- Use este ID ao adicionar o dispositivo à configuração

Última Vista

- Carimbo de data/hora da tentativa de conexão mais recente
- Ajuda a identificar dispositivos ativos vs. inativos

Ocorrências

- Número de vezes que o dispositivo tentou se conectar
- Tentativas frequentes podem indicar má configuração

Primeira Vista

- Quando o dispositivo foi detectado pela primeira vez
- Útil para rastrear novos equipamentos

Ações Disponíveis

Atualizar

- Recarregar a lista de dispositivos não configurados
- Atualiza carimbos de data/hora e contagens de ocorrências

Excluir

- Remover entradas individuais da lista
- Útil para limpar dispositivos antigos/desativados

Limpar Tudo

- Remover todos os registros de dispositivos não configurados
- Novo começo para a lista

Ajuda de Configuração

Quando dispositivos aparecem aqui, siga estas etapas:

1. **Anote o ID do Agente** da tabela
2. **Adicione a configuração do dispositivo** ao `config/runtime.exs`:

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

3. **Reinicie o RAN Monitor** para começar a monitorar o dispositivo

Para instruções detalhadas de configuração, consulte o Guia de Configuração em Tempo de Execução.

Casos de Uso

- **Descoberta de Rede:** Encontrar novas estações base adicionadas à rede
- **Segurança:** Identificar tentativas de conexão não autorizadas
- **Provisionamento:** Verificar identificadores de dispositivos antes da configuração
- **Desativação:** Rastrear tentativas de dispositivos que deveriam estar offline

---

Página de Logs da Aplicação

Painel de logs em tempo real para solução de problemas e monitoramento da atividade do sistema.

Níveis de Log

Filtrar por Nível de Log:

- **Emergência** - Falhas críticas do sistema
- **Alerta** - Ação imediata necessária
- **Crítico** - Condições críticas

- **Erro** - Condições de erro
- **Aviso** - Condições de aviso
- **Nota** - Normal, mas significativo
- **Info** - Mensagens informativas
- **Debug** - Informações detalhadas de depuração

Nota: Ao filtrar, o nível selecionado e todos os níveis de severidade superiores são exibidos.

Recursos

Pesquisar e Filtrar:

- Pesquisa de texto em todas as mensagens de log
- Streaming de logs em tempo real (últimas 500 mensagens)
- Filtrar por nível de log

Controles:

- **Pausar/Retomar** - Parar o streaming de logs ao vivo para revisar mensagens
- **Limpar** - Remover todos os logs da exibição
- **Nível do Sistema** - Alterar dinamicamente o nível de log em toda a aplicação

Codificação por Cores:

- Vermelho - Níveis de Emergência/Alerta/Critico
- Vermelho Claro - Nível de Erro
- Amarelo - Nível de Aviso
- Ciano - Nível de Nota
- Azul - Nível de Info
- Cinza - Nível de Debug

Casos de Uso

Solução de Problemas de Conexão:

- Filtrar por erros de dispositivos específicos
- Pesquisar por nomes de dispositivos ou endereços IP
- Revisar mensagens de falha de conexão

Monitorar Atividade do Sistema:

- Assistir logs de nível informativo para operações normais
- Rastrear eventos de registro de dispositivos
- Monitorar atividade de coleta de dados

Depurar Problemas:

- Definir temporariamente o nível de depuração
- Reproduzir o problema
- Revisar logs detalhados
- Reverter para o nível de info quando terminar

Investigar Falhas:

- Pesquisar mensagens de erro e rastreamentos de pilha
- Revisar carimbos de data/hora em torno do tempo de falha
- Correlacionar com eventos do dispositivo

Melhores Práticas

- **Use Pausa** ao revisar sequências de erro específicas
- **Defina o nível de log apropriado:**
  - Info para produção
  - Debug para solução de problemas
  - Aviso para produção silenciosa
- **Pesquise de forma eficaz** usando nomes de dispositivos ou palavras-chave de erro
- **Mudanças no nível de log persistem** até a reinicialização da aplicação

---

Página de Política de Retenção de Dados

Gerencie por quanto tempo os dados são armazenados no InfluxDB para cada estação base.

Exibição de Configurações Globais

Período de Retenção Padrão

- Política de retenção em todo o sistema em horas/dias
- Configurada em `config/config.exs`
- Padrão: 720 horas (30 dias)

Total de Registros

- Contagem de todos os pontos de dados em todos os dispositivos
- Atualizado na atualização da página

Status de Limpeza Automática

- Mostra execuções de limpeza a cada hora
- Status do trabalhador em segundo plano

Configurações por Dispositivo

Para cada estação base configurada:

Informações do Dispositivo:

- Nome do dispositivo
- Status de registro (Registrado/Não Registrado)
- Configuração atual do período de retenção

Contagens de Registros:

- **Métricas de Desempenho** - Número de pontos de dados PM armazenados
- **Configuração** - Número de instantâneos de configuração
- **Alarmes** - Número de registros de alarmes
- **Total** - Soma de todos os registros para este dispositivo

Ações:

- **Atualizar Período de Retenção** - Alterar horas de retenção (aplica-se apenas a este dispositivo)
- **Limpar Dados Antigos** - Acionar manualmente a limpeza com base no período de retenção
- **Limpar Todos os Dados** - Excluir todos os dados para este dispositivo (irreversível)

Como Funciona a Retenção

1. **Padrão Global** - Definido no arquivo de configuração, aplica-se a todos os dispositivos
2. **Substituição por Dispositivo** - Opcionalmente definir retenção personalizada para dispositivos específicos
3. **Limpeza Automática** - Executa a cada hora, exclui dados mais antigos que o período de retenção
4. **Limpeza Manual** - Use "Limpar Dados Antigos" para forçar limpeza imediata

Períodos de Retenção Comuns

- **720 horas (30 dias)** - Monitoramento operacional de curto prazo
- **2160 horas (90 dias)** - Retenção padrão para a maioria das implantações
- **4320 horas (180 dias)** - Retenção estendida para conformidade
- **8760 horas (365 dias)** - Análise histórica de longo prazo

Casos de Uso

- Reduzir o uso de armazenamento diminuindo o período de retenção

- Manter dados críticos de dispositivos por mais tempo que outros
- Limpar dados de teste antes da produção
- Gerenciar o uso de espaço em disco do InfluxDB

Aviso: Limpar todos os dados é permanente e não pode ser desfeito. Sempre verifique antes de executar.

Para informações detalhadas sobre a política de retenção, consulte o Guia de Política de Retenção de Dados.

Página de Status do InfluxDB

Monitore a saúde e o status do seu banco de dados de séries temporais InfluxDB.

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

A página de Status do InfluxDB mostrando status de conexão, medições, desempenho do gravador em lote e informações de armazenamento.

Status da Conexão

Campo	Descrição
Status da Conexão	Indicador verde quando conectado, vermelho quando desconectado
Banco de Dados	Nome do bucket do InfluxDB configurado
Versão do InfluxDB	Versão do banco de dados detectada (2.x)

Medições e Pontos de Dados

Contagens de pontos de dados em tempo real para cada tipo de medição:

Medição	Descrição
Métricas de Desempenho	Pontos de dados PM coletados dos dispositivos
Configuração	Instantâneos de configuração armazenados
Alarmes	Registros de alarmes no banco de dados
Total	Soma de todos os pontos de dados

Desempenho do Gravador em Lote

Estatísticas para o processo de gravador em lote do InfluxDB que lida com toda a ingestão de dados:

Métrica	Descrição
Tamanho da Fila	Pontos esperando para serem escritos. Codificado por cores: verde (< 1000), amarelo (< 10000), laranja (< 20000), vermelho (>= 20000)
Taxa de Filtragem	Percentual de pontos de dados duplicados bloqueados de serem escritos
PM Filtrados	Contagem de contadores PM filtrados (contadores não da dashboard que não estão na lista de dados PM armazenados)
Quedas de Fila	Pontos descartados devido ao transbordo da fila (deve ser 0 em operação normal)
Cache de Configuração	Número de hashes de configuração únicos armazenados em cache para detecção de delta
Cache de Alarmes	Número de alarmes ativos armazenados em cache para detecção de delta

Métricas adicionais:

Métrica	Descrição
Total Escrito	Pontos cumulativos escritos no InfluxDB desde a inicialização
Flushes	Número de operações de flush em lote
Filtrados	Total de pontos duplicados filtrados (não escritos)
Dados Escritos	Total de bytes escritos no InfluxDB
Taxa de Transferência	Taxa de transferência de escrita atual (KB/s ou MB/s)
Tempo de Atividade do Gravador	Tempo desde que o gravador em lote foi iniciado
Último Flush	Tempo desde o último flush bem-sucedido

Limpar Caches: Redefine os caches de detecção de delta. Use quando quiser forçar a reescrita de todos os dados (por exemplo, após alterações de esquema).

Informações de Armazenamento

Campo	Descrição
Políticas de Retenção	Configurações de retenção atuais (padrão: Indefinido)
Uso de Disco	Tamanho estimado do banco de dados com base nas contagens de registros
Atividade	Carimbo de data/hora da última atualização

Detalhes da Configuração

Campo	Descrição
Host	Nome do host do servidor InfluxDB
Porta	Porta do servidor InfluxDB (padrão: 8086)
Bucket	Nome do bucket do InfluxDB
Status	Insígnia de status da conexão
Medições	Número de tipos de medições (3: PerformanceMetrics, Configuration, Alarms)

Diagnósticos de Saúde

Indicadores de status para a saúde do sistema:

- **Conectividade do InfluxDB** - Banco de dados acessível e respondendo
- **Coleta de Dados** - Métricas de desempenho sendo coletadas dos dispositivos
- **Retenção de Dados** - Status atual da política de retenção
- **Última Sincronização** - Sincronização de dados mais recente

Atualização Automática

A página é atualizada automaticamente a cada 30 segundos.

Interpretando o Status

Condição	Significado
Conectado + Contagens de Dados Crescendo	Sistema operando normalmente
Conectado + Sem Dados	Verifique o registro do dispositivo e a configuração do contador PM
Desconectado	Verifique se o InfluxDB está em execução e a conectividade da rede
Tamanho da Fila Alto (amarelo/vermelho)	Problema de desempenho de escrita do InfluxDB ou latência de rede
Altas Quedas de Fila	Transbordo da fila - aumente o tamanho do lote ou reduza a taxa de coleta
Alta Taxa de Filtragem	Bom - indica detecção eficaz de duplicatas

Casos de Uso

- Verificar se o InfluxDB está recebendo dados
- Monitorar a saúde e a taxa de transferência do gravador em lote
- Solucionar problemas de desempenho de escrita
- Verificar a eficácia do cache de detecção de delta
- Confirmar que os dados estão sendo escritos

Página de Métricas do Sistema

Monitoramento de desempenho em tempo real para o gravador em lote do InfluxDB e recursos do sistema.

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

A página de Métricas do Sistema mostrando estatísticas do gravador em lote do InfluxDB e contagens de escrita por Airscale.

Gravador em Lote do InfluxDB

Estatísticas resumidas para o processo de gravador em lote:

Métrica	Descrição
Tamanho da Fila	Número de pontos de dados esperando para serem escritos no InfluxDB
Contagem de Flush	Número total de flushes em lote desde a inicialização
Total de Pontos Escritos	Pontos de dados cumulativos escritos no InfluxDB
Último Flush	Tempo desde a última operação de flush bem-sucedida

Estatísticas de Escrita do InfluxDB por Airscale

Desagregação por dispositivo dos dados escritos no InfluxDB:

Coluna	Descrição
Airscale	Nome do dispositivo
Métricas de Desempenho	Contagem de pontos de dados PM escritos
Configuração	Contagem de instantâneos de configuração escritos
Alarmes	Contagem de registros de alarmes escritos
Total de Registros	Soma de todos os pontos de dados para este dispositivo
Última Escrita	Carimbo de data/hora da escrita mais recente para este dispositivo

A linha de totais na parte inferior mostra contagens agregadas em todos os dispositivos.

Recursos do Sistema

Utilização de recursos da VM Erlang:

Métrica	Descrição
Memória Total	Memória total alocada para a VM Erlang
Memória do Processo	Memória usada pelos processos Erlang
Memória Binária	Memória usada para dados binários (XML, cargas JSON)
Memória de Átomo	Memória usada para átomos
Contagem de Processos	Número de processos Erlang ativos
Fila de Execução	Número de processos esperando por tempo de CPU (0 é saudável)

Atualização Automática

A página é atualizada automaticamente a cada 5 segundos.

Casos de Uso

- Monitorar a saúde e a taxa de transferência do gravador em lote
- Identificar dispositivos com alto volume de dados
- Solucionar problemas de desempenho de escrita
- Verificar se os dados estão fluindo de todos os dispositivos
- Monitorar o uso de recursos do sistema

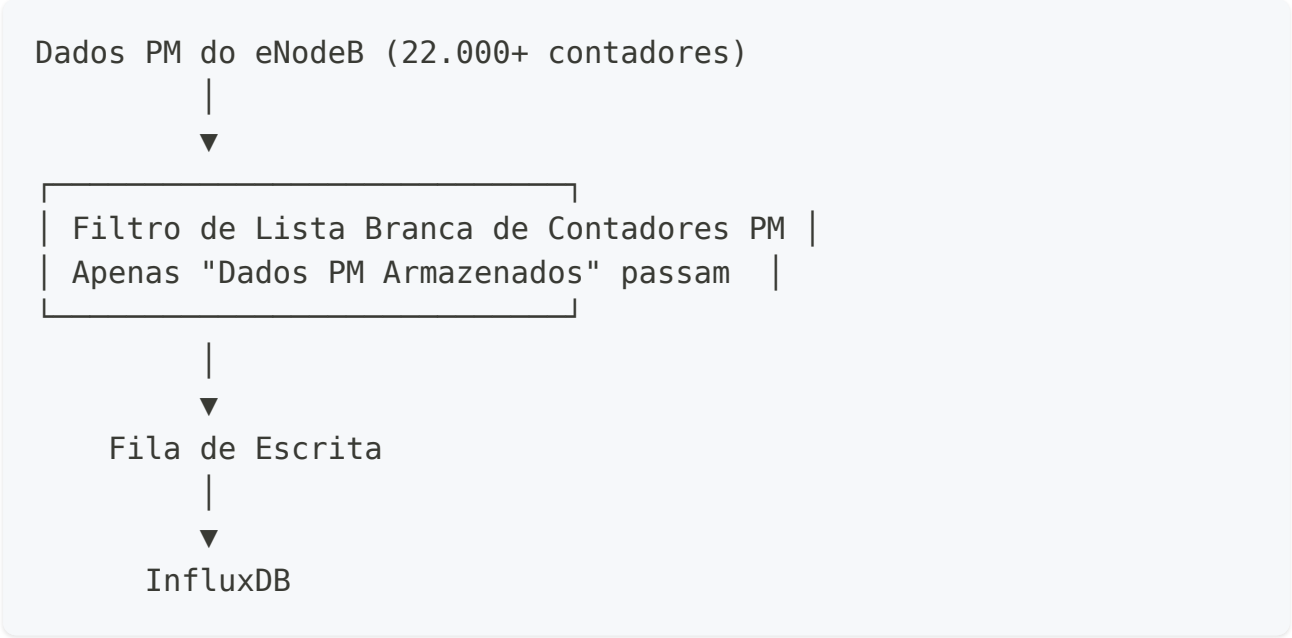
Página de Coleta de Dados PM

Controle quais contadores de Métricas de Desempenho (PM) são armazenados no InfluxDB. As estações base Nokia AirScale relatam mais de 22.000 contadores PM únicos, mas apenas um subconjunto é normalmente necessário para dashboards.

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

A página de Coleta de Dados PM mostrando contadores armazenados (esquerda) e contadores disponíveis (direita) com filtros de categoria.

Como Funciona a Filtragem PM



O gravador em lote filtra os dados PM recebidos contra a lista de "Dados PM Armazenados". Contadores que não estão nesta lista são descartados antes da fila, reduzindo o armazenamento e melhorando o desempenho das consultas.

Layout da Interface

Seção	Descrição
Dados PM Armazenados (Esquerda)	Contadores atualmente sendo coletados e escritos no InfluxDB
Contadores Disponíveis (Direita)	Todos os 22.000+ contadores disponíveis para adicionar
Chaves de Configuração (Inferior)	Parâmetros de configuração sendo rastreados (do `config_keys.csv`)

Painel de Dados PM Armazenados

Contadores nesta lista são escritos no InfluxDB quando recebidos dos dispositivos.

Filtros:

- **Pesquisar**: Filtrar por ID de contador ou descrição
- **Categoria**: Filtrar por tecnologia (LTE, 5G-NR, etc.)
- **Fonte**: Filtrar por Padrão (do CSV) ou Adicionado (adicionado pelo usuário)

Ações:

- **Remover Selecionados**: Parar de coletar contadores selecionados
- **Selecionar Todos**: Selecionar todos os contadores visíveis
- **Restaurar para Padrões**: Restaurar lista original do `pm_counters.csv`

Painel de Contadores Disponíveis

Navegue e adicione contadores do completo referencial PM da Nokia.

Filtros:

- **Pesquisar**: Encontrar contadores por ID ou palavras-chave de descrição
- **Categoria**: Filtrar por categoria de tecnologia

Ações:

- **Adicionar Selecionados**: Começar a coletar contadores selecionados
- **Selecionar Todos**: Selecionar todos os contadores visíveis (limitado a 200 exibidos)

Categorias de Contadores

Categoria	Prefixo de Código	Descrição
LTE	M8xxx	Contadores LTE L1/L2/L3
WCDMA	M5xxx	Contadores 3G WCDMA
5G-NR	M55xxx	Contadores 5G NR
5G-Mobilidade	M51xxx	Métricas de mobilidade 5G
5G-Comum	M40xxx	Contadores comuns 5G

Persistência

Mudanças são:

- **Persistidas em disco** em `priv/pm_filters.etf`
- **Sobrevivem a reinicializações da aplicação**
- **Entram em vigor imediatamente** (sem necessidade de reinicialização)

Estatísticas Relacionadas

A página de Status do InfluxDB mostra estatísticas de filtragem:

- **PM Filtrados**: Contagem de pontos PM descartados (não na lista branca)
- **Taxa de Filtragem**: Percentual de pontos de configuração/alarmes duplicados bloqueados

Para orientações detalhadas sobre seleção de contadores, consulte Guia de Coleta de Dados PM.

Página de Gerenciamento de Firmware

Gerencie pacotes de firmware Nokia AirScale para atualizações de software remotas.

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

Visão Geral

A página de Gerenciamento de Firmware fornece um repositório centralizado para pacotes de software de estações base. Carregue firmware no RAN Monitor e use as URLs HTTP geradas na opção "Servidor remoto" do WebEM para realizar atualizações de software.

Principais Recursos

Recurso	Descrição
Carregar	Armazenar pacotes de firmware .zip da Nokia AirScale
URLs de Download	Copiar URLs HTTP para configuração do servidor remoto do WebEM
Checksums MD5	Cálculo automático de checksum para verificação de integridade
Estatísticas de Armazenamento	Monitorar uso de disco do repositório

Fluxo de Trabalho Rápido

1. Carregue o pacote de firmware no RAN Monitor
2. Clique em **Copiar URL** para obter a URL de download

3. No Gerenciamento de Software do WebEM, selecione **Servidor remoto**
4. Cole a URL e clique em **Conectar e Atualizar**
5. Selecione o firmware e inicie a atualização

Para documentação completa, incluindo opções de configuração e solução de problemas, consulte o **Guia de Gerenciamento de Firmware**.

Página de Gerenciamento de Dados

Gerencie dados em cache, arquivos temporários e armazenamento persistente.

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

A página de Gerenciamento de Dados mostrando cache ETS, arquivos temporários e opções de limpeza de dados do InfluxDB.

Cache ETS (Em Memória)

Caches voláteis em memória que são limpos na reinicialização da aplicação:

Cache	Descrição
Cache de Configuração Nokia	Dados de configuração do dispositivo em cache
Cache de Alarmes Nokia	Registros de alarmes ativos em cache
Cache de Registro de Retenção	Contagens de registros de políticas de retenção em cache
Cache de Status do InfluxDB	Status de conexão do InfluxDB em cache

Limpar Todo o Cache ETS: Remove todas as entradas dos caches em memória. Os dados são regenerados na próxima solicitação.

Arquivos Temporários

Arquivos criados durante a extração e processamento de configuração:

- Extrações TAR de downloads de configuração do dispositivo
- Arquivos temporários criados durante o processamento

Limpar Arquivos Temporários: Remove arquivos temporários do diretório `/tmp`.

Dados do InfluxDB (Persistente)

Dados de séries temporais armazenados no InfluxDB para cada dispositivo:

- Métricas de desempenho (contadores PM)
- Instantâneos de configuração
- Registros de alarmes

Limpeza por Dispositivo: Clique em "Limpar Dados" ao lado de um dispositivo para remover todos os dados do InfluxDB para esse dispositivo.

Limpar Tudo: Remove todos os dados do InfluxDB para todos os dispositivos. Use com cautela.

Registro de Dispositivos

Mostra a contagem de dispositivos registrados. As configurações dos dispositivos são carregadas de `config/runtime.exs` na inicialização e armazenadas em ETS.

Casos de Uso

- Liberar memória limpando caches
- Limpar arquivos temporários após solução de problemas
- Remover dados de teste antes do uso em produção
- Limpar dados de dispositivos desativados

Fluxos de Trabalho da Interface Web

Fluxos de trabalho operacionais comuns usando a Interface Web.

Verificação de Saúde Diária

Objetivo: Verificar a saúde do sistema no início do turno

Passos:

1. Abra o painel principal
2. Verifique se todos os dispositivos mostram status verde
3. Verifique a contagem e severidade dos alarmes
4. Revise quaisquer dispositivos vermelhos/falhados
5. Investigue problemas conforme necessário
6. Documente quaisquer ações tomadas

Tempo: < 5 minutos

Investigação de Alarmes

Objetivo: Responder e resolver alarmes

Passos:

1. Abra a página de Alarmes
2. Classifique por severidade (Crítico primeiro)
3. Clique no alarme para detalhes completos
4. Navegue até o dispositivo afetado
5. Referencie com métricas recentes
6. Determine a ação necessária
7. Implemente a resolução
8. Verifique se o alarme é limpo

Para procedimentos detalhados de manuseio de alarmes, consulte o Guia de Gerenciamento de Alarmes.

Atualização de Configuração

Objetivo: Atualizar a configuração do dispositivo de forma segura

Passos:

1. Baixe a configuração atual (backup)
2. Modifique a configuração offline usando ferramentas apropriadas
3. Envie a nova configuração para o dispositivo
4. Anote o ID do Plano retornado
5. Valide a configuração usando o ID do Plano
6. Se a validação for bem-sucedida, ative a configuração
7. Verifique se as mudanças tiveram efeito
8. Monitore a estabilidade do dispositivo por 15-30 minutos
9. Documente a mudança no sistema de gerenciamento de mudanças

Notas de Segurança:

- Sempre valide antes de ativar
- Faça alterações durante janelas de manutenção, quando possível
- Tenha um plano de reversão pronto
- Monitore por comportamento inesperado

Adicionando uma Nova Estação Base

Objetivo: Adicionar uma nova estação base implantada ao monitoramento

Passos:

1. Verifique a página de eNodeBs Não Configurados para o dispositivo
2. Anote o ID do Agente e o endereço IP
3. Adicione o dispositivo ao `config/runtime.exs`
4. Reinicie a aplicação RAN Monitor
5. Verifique se o dispositivo aparece na página das Estações Base
6. Confirme se o registro é bem-sucedido (status verde)
7. Verifique se as métricas estão fluindo para o InfluxDB
8. Defina a política de retenção, se necessário
9. Adicione aos painéis do Grafana

Para operações detalhadas, consulte o Guia de Operações Comuns.

Solucionando Problemas de Conectividade do Dispositivo

Objetivo: Diagnosticar e corrigir problemas de conexão do dispositivo

Passos:

1. Verifique a página das Estações Base para o status do dispositivo
2. Se vermelho/falhado, clique no dispositivo para detalhes
3. Revise as informações da sessão e o último horário de contato
4. Verifique os Logs da Aplicação para mensagens de erro
5. Verifique a conectividade da rede (ping no dispositivo)
6. Confirme se as credenciais estão corretas

7. Verifique se o dispositivo é acessível na porta configurada
8. Revise logs do lado do dispositivo, se necessário
9. Reinicie a conexão ou o dispositivo conforme necessário
10. Verifique a recuperação

Para solução de problemas detalhada, consulte o Guia de Solução de Problemas.

Documentação Relacionada

- **Guia de Introdução** - Configuração inicial e implantação
- **Guia de Operações Comuns** - Tarefas operacionais do dia a dia
- **Guia de Gerenciamento de Alarmes** - Manuseio e escalonamento de alarmes
- **Guia de Configuração em Tempo de Execução** - Configuração do sistema
- **Guia de Integração do Grafana** - Análises e painéis
- **Guia de Política de Retenção de Dados** - Gerenciamento do ciclo de vida dos dados
- **Guia de Solução de Problemas** - Problemas comuns e soluções