RCMS_Test - Infrastructure de Monitoring Sécurisée pour DME

Structure du projet

```
RCMS_Test/
├── vm1_dme_simulator/     # Simulateur DME (SNMPv3)
├── vm2_data_collector/    # Collecteur de données SNMPv3
├── vm3_elasticsearch/     # Configuration Elasticsearch
├── vm4_logstash/          # Configuration Logstash
├── vm5_kibana/            # Configuration Kibana
├── hardening/             # Scripts de sécurisation
├── docs/                  # Documentation
└── docker-compose.yml     # Orchestration des conteneurs
```

Documentation

Consultez les documents suivants pour plus d'informations :

- Architecture - Vue d'ensemble de l'architecture
- Guide d'installation - Instructions d'installation et de configuration
- Rapport de sécurité - Analyse de sécurité et recommandations
- Guide SNMPv3 - Configuration et utilisation de SNMPv3

Environnement d'exécution

IMPORTANT : Les scripts Python de ce projet sont conçus pour fonctionner dans un environnement virtualisé (Docker). Cette approche est particulièrement importante pour les systèmes Ubuntu 24 et versions ultérieures qui imposent des restrictions sur l'installation directe des bibliothèques Python.

L'utilisation de conteneurs Docker garantit :

- Un environnement d'exécution isolé et cohérent
- L'installation correcte de toutes les dépendances Python nécessaires
- La compatibilité entre les différentes versions de bibliothèques
- Une sécurité renforcée grâce à l'isolation

Les scripts peuvent être exécutés directement sur des versions antérieures d'Ubuntu en installant les dépendances requises, mais l'approche conteneurisée reste recommandée pour garantir la portabilité et la sécurité.

Sécurité SNMPv3

Cette infrastructure utilise SNMPv3 avec authentification et chiffrement pour sécuriser les communications entre le simulateur DME et le collecteur de données. SNMPv3 offre :

- **Authentification** : Vérification de l'identité des agents et gestionnaires SNMP
- **Confidentialité** : Chiffrement des données pour empêcher l'écoute clandestine
- **Intégrité** : Protection contre la modification des données en transit

Les paramètres SNMPv3 sont configurables via des variables d'environnement dans le fichier docker-compose.yml.

Démarrage rapide

```
# Cloner le dépôt
git clone <url_du_depot> RCMS_Test
cd RCMS_Test

# Démarrer l'infrastructure
docker-compose up -d
```

Accédez à Kibana via http://localhost:5601 pour visualiser les données DME.