



DOCUMENT CHANGE RECORD

Version	Date	Auteur	Changement
V1	17/07/2023	Louis TRILLES	Création du document
V2	18/07/2023	Louis TRILLES	Modification du document

Table des matières

Introduction	4
I. Schéma de l'infrastructure.....	5
A. Explication de l'infrastructure (comparaison avec l'agriculture)	5
1. Docker.....	5
2. Grafana	5
II. Mise en place de la base MongoDB – SRV-MONGODB	6
III. Mise en place d'un système de backup journalier - SRV-MONGODB	8
IV. Mise en place de Grafana - SRV-DOCKER	9

Introduction

Nous vous présentons ce document technique qui servira de guide d'installation pour mettre en place l'infrastructure nécessaire à l'utilisation efficace de notre système de surveillance des cultures. Ce guide a été conçu pour vous accompagner pas à pas dans le processus d'installation, en fournissant des instructions détaillées et des recommandations claires pour garantir une configuration adéquate du système.

Ce guide vise à vous fournir les connaissances et les étapes nécessaires pour déployer l'infrastructure matérielle et logicielle requise. Il vous permettra de mettre en place les capteurs, de configurer les paramètres de communication et d'intégrer le système de surveillance des cultures à votre environnement agricole existant.

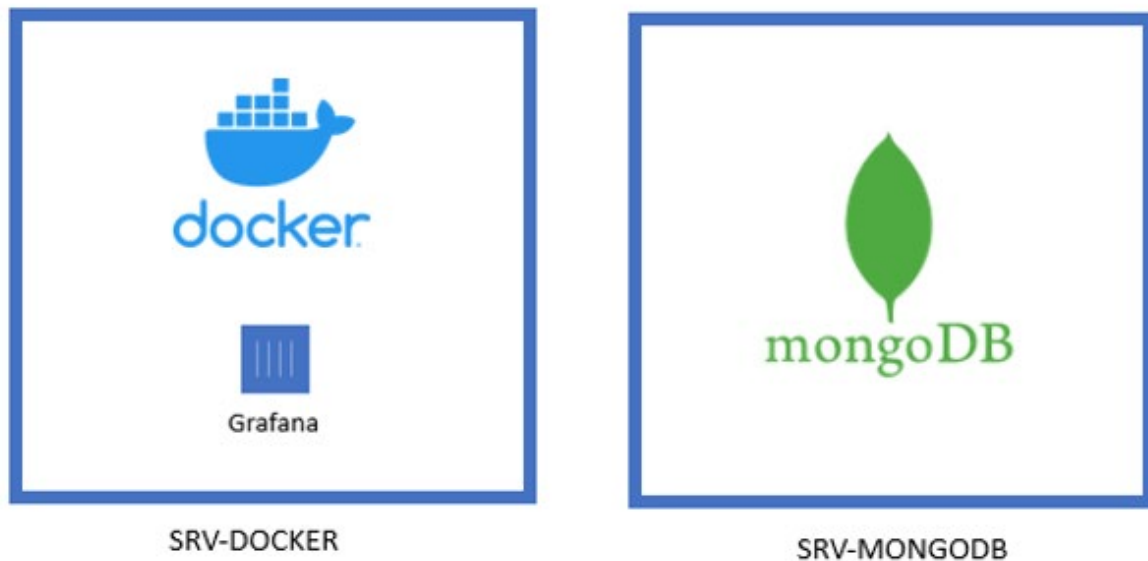
Nous avons pris soin de rendre ce guide accessible et facile à suivre, même pour les utilisateurs ayant une expérience technique limitée. Chaque étape d'installation est accompagnée d'explications claires, de captures d'écran et de schémas illustratifs pour vous guider tout au long du processus.

Il est important de souligner que la réussite de l'installation dépend de la précision et de l'attention portée à chaque étape. Nous vous encourageons à lire attentivement ce guide avant de commencer l'installation et à suivre les instructions étape par étape pour vous assurer d'obtenir un système de surveillance des cultures fonctionnel et performant.

Nous sommes convaincus que ce guide d'installation vous aidera à tirer pleinement parti de notre système de surveillance des cultures et à bénéficier de tous ses avantages pour optimiser vos rendements agricoles. En cas de questions supplémentaires ou de besoins d'assistance, notre équipe de support technique reste à votre disposition pour vous accompagner tout au long du processus d'installation.

Nous vous remercions de votre confiance et nous vous souhaitons une installation réussie de notre système de surveillance des cultures.

I. Schéma de l'infrastructure



A. Explication de l'infrastructure (comparaison avec l'agriculture)

1. Docker

Imaginez que vous avez un jardin et que vous souhaitez cultiver différents types de plantes, comme des tomates, des carottes et des herbes aromatiques. Chaque plante a des besoins spécifiques en termes d'eau, de lumière et de nutriments. Pour simplifier la gestion de ces différentes plantes, vous pourriez utiliser des conteneurs de jardinage.

Dans le contexte de l'informatique, Docker est comme un conteneur de jardinage pour les applications logicielles. Il permet de regrouper toutes les ressources nécessaires à l'exécution d'une application (code, bibliothèques, fichiers de configuration, etc.) dans un conteneur isolé et autonome.

En utilisant Docker, vous pouvez créer un conteneur pour chaque application logicielle dont vous avez besoin, tout comme vous créez un conteneur pour chaque plante de votre jardin. Chaque conteneur est indépendant des autres, ce qui signifie que vous pouvez les déployer, les mettre à jour ou les supprimer individuellement sans affecter les autres.

2. Grafana

Maintenant, imaginez que vous souhaitez avoir une vue d'ensemble de l'état de votre jardin. Vous voulez voir les mesures de température, d'humidité et de luminosité pour chaque plante, et les visualiser sous forme de graphiques et de tableaux faciles à comprendre. C'est là qu'intervient Grafana.

Grafana est comme un tableau de bord pour votre jardin. Il permet de collecter les données provenant de différents capteurs, de les regrouper et de les présenter de manière visuelle et intuitive. Vous pouvez voir l'évolution des températures, le niveau d'humidité du sol et d'autres métriques importantes pour évaluer la santé de vos plantes.

Dans le contexte de l'agriculture, Grafana pourrait être utilisé pour créer des tableaux de bord interactifs et personnalisés qui affichent les données collectées par les capteurs. Vous pourriez voir en temps réel les conditions météorologiques, les variations de température et d'humidité, et même les prévisions pour prendre des décisions éclairées sur l'arrosage, la protection contre les ravageurs, etc.

Grafana vous permet de visualiser et d'analyser les données agricoles de manière conviviale, ce qui facilite la compréhension de l'état de vos cultures et vous aide à prendre des décisions basées sur des informations précises et en temps réel.

II. Mise en place de la base MongoDB – SRV-MONGODB

Étape 1 : Mise à jour du système

Avant d'installer MongoDB, assurez-vous que votre système est à jour en exécutant les commandes suivantes :

```
sudo apt update  
sudo apt upgrade
```

Étape 2 : Ajout de la clé GPG de MongoDB

Ajoutez la clé GPG pour le référentiel MongoDB en exécutant la commande suivante :

```
wget -qO - https://www.mongodb.org/static/pgp/server-5.0.asc | sudo apt-key add -
```

Étape 3 : Ajout du référentiel MongoDB

Ajoutez le référentiel MongoDB à votre liste de sources en exécutant la commande suivante :

```
echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/debian bullseye/mongodb-org/5.0 main" | sudo tee /etc/apt/sources.list.d/mongodb-org-5.0.list
```

Étape 4 : Installation de MongoDB

Installez MongoDB en exécutant la commande suivante :

```
sudo apt update && sudo apt install mongodb-org
```

Étape 5 : Démarrage du service MongoDB

Démarrez le service MongoDB en exécutant la commande suivante :

```
sudo systemctl start mongod  
sudo systemctl enable mongod
```

Étape 6 : Vérification de l'état de MongoDB

Vérifiez que MongoDB est en cours d'exécution en utilisant la commande suivante :

```
sudo systemctl status mongod
```

III. Mise en place d'un système de backup journalier - SRV-MONGODB

Ce script Bash permettra de générer une sauvegarde automatique de votre base de données MongoDB toutes les 24 heures. Ce script automatisé vous permettra de sauvegarder vos données de manière régulière et fiable, assurant la protection de vos informations essentielles. En exécutant ce script, vous pourrez créer des sauvegardes périodiques de votre base de données, garantissant ainsi la disponibilité des données en cas de perte ou de problème technique.

```
#!/bin/bash

# Répertoire de destination pour les sauvegardes
backup_dir="/chemin/vers/le/repertoire/de/sauvegarde"

# Nom du fichier de sauvegarde (avec date et heure actuelles)
backup_file="$backup_dir/backup-$(date +%Y-%m-%d-%H-%M-%S).bson"

# Commande de sauvegarde MongoDB
mongo_dump_command="mongodump --archive=$backup_file --gzip"

# Réalisation de la sauvegarde
$mongo_dump_command

# Vérification de la réussite de la sauvegarde
if [ $? -eq 0 ]; then
    echo "Sauvegarde MongoDB réalisée avec succès : $backup_file"
else
    echo "Erreur lors de la sauvegarde MongoDB"
fi
```

Assurez-vous de personnaliser les variables **backup_dir** et **mongo_dump_command** en fonction de votre configuration.

Enregistrez le script dans un fichier, par exemple **mongodb_backup.sh**, puis rendez-le exécutable avec la commande suivante :

```
chmod +x mongodb_backup.sh
```

Ensuite, vous pouvez ajouter une tâche cron pour exécuter le script automatiquement toutes les 24 heures. Ouvrez votre fichier crontab avec la commande **crontab -e** et ajoutez la ligne suivante :

```
0 0 * * * /chemin/vers/le/fichier/mongodb_backup.sh
```

Ainsi, le script sera exécuté automatiquement toutes les 24 heures, générant une sauvegarde de la base de données MongoDB compressée au format BSON dans le répertoire de sauvegarde spécifié. Vous pouvez personnaliser davantage le script en ajoutant des fonctionnalités supplémentaires, comme la rotation des sauvegardes pour conserver uniquement les plus récentes.

Important

Assurez-vous de tester le script et de vérifier que les sauvegardes sont générées correctement avant de l'ajouter à une tâche cron en production.

IV. Mise en place de Grafana - SRV-DOCKER

Étape 1: Installation de Docker

1. Assurez-vous que votre système d'exploitation est pris en charge par Docker. Consultez la documentation officielle de Docker pour obtenir des informations spécifiques à votre système d'exploitation.
2. Suivez les instructions d'installation spécifiques à votre système d'exploitation pour installer Docker.
<https://docs.docker.com/engine/install/debian/>
3. Une fois l'installation terminée, ouvrez une nouvelle fenêtre de terminal pour vérifier que Docker est correctement installé en exécutant la commande suivante :

```
docker version
```

Cela devrait afficher les informations sur la version de Docker installée.

Étape 2: Installation de Docker Compose

Téléchargez le binaire Docker Compose en utilisant la commande suivante :

```
sudo curl -L "https://github.com/docker/compose/releases/latest/download/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
```

Donnez les permissions d'exécution au binaire Docker Compose :

```
sudo chmod +x /usr/local/bin/docker-compose
```

Vérifiez que Docker Compose est correctement installé en exécutant la commande suivante :

```
docker-compose version
```

Cela devrait afficher les informations sur la version de Docker Compose installée.

Maintenant, nous allons pouvoir lancer notre image Grafana dans un container :

Voici un exemple de fichier **docker-compose.yml** pour déployer Grafana en utilisant Docker Compose :

```
version: '3'

services:
  grafana:
    image: grafana/grafana
    container_name: grafana
    ports:
      - 3000:3000
    volumes:
      - grafana-data:/var/lib/grafana
    restart: always

volumes:
  grafana-data:
```

Ce fichier docker-compose.yml définit un service Grafana basé sur l'image officielle de Grafana provenant du référentiel Docker Hub. Les principales caractéristiques de ce fichier sont les suivantes :

- Le service Grafana est nommé "grafana".
- L'image Docker utilisée est "grafana/grafana", qui est l'image officielle de Grafana.
- Le port 3000 du conteneur Grafana est mappé sur le port 3000 de l'hôte (vous pouvez modifier le port de l'hôte si nécessaire).

- Un volume nommé "grafana-data" est utilisé pour persister les données de Grafana dans le répertoire "/var/lib/grafana" du conteneur.
- L'option "restart: always" assure que le conteneur Grafana sera redémarré automatiquement en cas de panne ou de redémarrage du système hôte.

Pour démarrer le service Grafana, placez ce fichier **docker-compose.yml** dans un répertoire de votre choix et exécutez la commande suivante dans ce répertoire :

```
docker-compose up -d
```

Cela démarrera le service Grafana en arrière-plan et vous pourrez y accéder en utilisant l'URL **http://localhost:3000** dans votre navigateur.

V. Recommandations sécurité

A. Sécurité des appareils

La sécurité des appareils est d'une importance capitale pour assurer le bon fonctionnement et la fiabilité du système de surveillance des cultures. Nous mettrons en œuvre des mesures strictes pour protéger physiquement les appareils sur le terrain. Cela inclut le choix de capteurs robustes et résistants aux intempéries, ainsi que leur installation dans des boîtiers résistants aux chocs, aux infiltrations d'eau et à la poussière. En outre, nous veillerons à ce que tous les appareils soient correctement fixés et installés dans des zones sécurisées pour minimiser les risques de vol ou de dommages non autorisés.

Pour garantir la sécurité des appareils sur le terrain, nous suivrons les meilleures pratiques de l'**ANSSI** en matière de protection physique des équipements informatiques (Référentiel général de sécurité, RG-1). Cela inclut l'utilisation de capteurs robustes et résistants aux intempéries, ainsi que leur installation dans des boîtiers sécurisés pour minimiser les risques de vol ou de dommages non autorisés.

B. Sécurité de l'infrastructure

La sécurité de l'infrastructure est essentielle pour garantir le bon fonctionnement continu du système de surveillance des cultures. Nous prendrons des mesures pour renforcer la sécurité de l'infrastructure informatique en utilisant des pare-feux, des systèmes de détection d'intrusion et des mécanismes de protection contre les attaques DDoS. De plus, nous mettrons en place des mécanismes de surveillance continue pour détecter toute activité suspecte ou non autorisée sur le réseau et réagir rapidement en cas de menace potentielle.

La régulation des canaux de transmission de données est essentielle pour garantir que les informations sensibles collectées par les capteurs sont transmises de manière sécurisée et fiable vers le système central de surveillance. Nous utiliserons des protocoles de communication sécurisés tels que HTTPS et SSL/TLS pour chiffrer les données pendant leur transmission. De plus, nous mettrons en place des mécanismes de vérification de l'authenticité des données pour empêcher toute altération ou interception des données en transit.

C. Sécurité des données personnelles (données agriculture)

La sécurité des données personnelles est une priorité absolue. Nous mettrons en place des mesures de sécurité robustes pour protéger les données personnelles collectées par le système de surveillance des cultures. Ces données seront stockées de manière sécurisée dans la base de données MongoDB, en utilisant des techniques de chiffrement avancées et en limitant l'accès aux seules personnes autorisées.

D. Politique des mots de passes

La sécurité des comptes utilisateurs est essentielle pour prévenir les accès non autorisés aux informations sensibles.

Pour renforcer la sécurité des comptes utilisateurs, nous mettrons en œuvre une politique de mots de passe conforme aux recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Conformément au Référentiel général de sécurité (RG-1.20), nous exigerons des mots de passe robustes comprenant une combinaison de lettres, de chiffres et de caractères spéciaux. De plus, nous imposerons des contraintes sur la longueur des mots de passe et nous mettrons en place une périodicité de changement régulier pour minimiser les risques de compromission de la sécurité des comptes. Cette politique de mots de passe renforcera la sécurité des comptes utilisateurs et préviendra les tentatives d'intrusion non autorisées.

E. Gestion des accès

La gestion des accès est cruciale pour assurer que seules les personnes autorisées peuvent accéder aux données du système de surveillance des cultures. Nous mettrons en place des rôles d'accès avec des niveaux de privilèges spécifiques pour différents utilisateurs, permettant ainsi de contrôler l'accès aux informations sensibles. Les comptes inactifs ou obsolètes seront désactivés pour limiter les risques de compromission de la sécurité.

F. Sécurisation des communications

La sécurisation des communications est essentielle pour protéger les échanges d'informations entre les utilisateurs et le système de surveillance des cultures. Nous utiliserons des protocoles de communication sécurisés tels que HTTPS pour chiffrer les données lors des communications entre l'application web et le serveur. Cela garantira la confidentialité et l'intégrité des données lors de leur transit.

Nous utiliserons des protocoles de communication sécurisés tels que HTTPS, conformément aux recommandations de l'**ANSSI** en matière de sécurisation des échanges de données (Référentiel général de sécurité, RG-1.01). Cela garantira que les informations sensibles transitant entre l'application web et le serveur sont protégées contre les interceptions et les altérations non autorisées.

G. Eviter les brèches de sécurité

Nous mettrons en œuvre des solutions de sécurité complètes pour éviter toute violation de sécurité potentielle des données du système de surveillance des cultures. Cela inclut des audits réguliers de sécurité, des tests de pénétration et des mises à jour régulières des logiciels pour combler les failles de sécurité connues. De plus, nous surveillerons en permanence les journaux d'activité pour détecter toute activité suspecte et réagir rapidement en cas de menace potentielle.

Ces mesures de sécurité contribueront à garantir que le système de surveillance des cultures est hautement sécurisé et protège les données personnelles et sensibles contre tout accès non autorisé ou atteinte à la confidentialité.