

# Rapport de stage

Infrastructures digital option système etréseaux

**TECHNICIEN SPÉCIALISÉ**

Stage en institut spécialisé de technologie appliquée  
el kelaa des sraghna



*Étude, conception et mise en place d'une solution SIEM  
: Wazuh*

En cadré par :

HAMMADCHI AMINE

SAADI HASNA

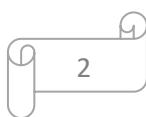
Réalisé par :

BELLAFRIKH ZAYNAB

2023/2024

## Table des matières

Fiche de stagiaire.....	5
DÉDICACE :.....	6
Remerciements .....	7
Résumé.....	8
Présentation du Stage .....	9
INTRODUCTION .....	10
Fiche Technique de l'ISTA :.....	11
Organigramme ISTA :.....	12
Les matériels utilisés .....	13
Les travaux effectués :.....	14
1) Scanner le réseau de direction .....	14
2) Formatage d'un serveur :.....	14
3) Formatage des PC :.....	15
4) Configuration des routeurs : .....	16
5) Configuration des switches : .....	18
6) Plan de réseau ISTA KELAA SRAGHNA.....	20
7) Test des ports de salle info 1 et 2 :.....	21
8) Sticker l'armoire de salle info 1 : .....	23
9) Sticker l'armoire de salle Info 2.....	23
10) Connecter l'appareil Bosch au réseau et Lancement de dernière version de MISE À JOUR : 23	
11) Exporter une machine virtuelle Ubuntu-server et l'importer dans ESXI8.....	24
État de l'art.....	26
Introduction :.....	27
I\ SIEM.....	28
1. Définition :.....	28
2. Avantages de l'utilisation d'un SIEM .....	28
3. Rôle des technologies SIEM.....	29
4. Fonctionnalités SIEM et cas d'utilisation.....	29
5. Architecture de SIEM :.....	30
6. Meilleurs pratiques pour la mise en place d'un SIEM.....	31
II\ Le choix de Wazuh comme solution SIEM.....	32
1. Définition .....	32
2. Fonctionnalité de Wazuh.....	32
3. Avantages de Wazuh .....	33



4.    Architecture de Wazuh.....	33
5.    Composants de Wazuh.....	34
Mise en place de Wazuh .....	35
I\ Installation de Wazuh.....	36
1.    Installer l'indexeur Wazuh.....	36
2.    Installer le serveur Wazuh.....	41
3.    Installation du tableau de bord Wazuh.....	44
II\ Déploiement d'un agent Wazuh .....	46
1.    Installation de Wazuh agent.....	46
2.    Intégration des agents à superviser .....	47
3.    Création de groupe agents .....	51
4.    Ajouter des agents Wazuh aux groupes.....	53
5.    Supprimer les agents Wazuh des groupes .....	55
6.    Détection de vulnérabilité.....	58
Conclusion .....	67

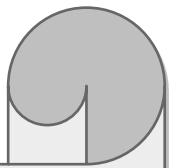
**Liste des figures :**

Figure 1	Topologie de réseau de direction
Figure 2/3	Screenshot d'accès à distant à un serveur
Figure 4	Topologie de réseau ISTA Kelaa Sraghna
Figure 5	Test des ports de salle Info 1
Figure 6	Test des ports de salle Info 2
Figure 7/8	Armoire de salle Info 1
Figure 9/10	Armoire de salle Info 2
Figure 11/12	Appareil Bosch

**Liste des Tableaux :**

Tableau 1	Les matériels utilisés
Tableau 2	Les équipements connecter au réseau de direction
Tableau 3	Les caractéristiques du Serveur DELL
Tableau 4	Les routeurs configurer
Tableau 5	Les switches configurer
Tableau 6	Marque des matériel réseaux utilisés dans ISTA KELAA DES SRAGHNA
Tableau 7	État de fonctionnement des ports et des câbles de salle Info 1
Tableau 8	État de fonctionnement des ports et des câbles de salle Info 2

## Fiche de stagiaire



- **NOM :** BELLAFRIKH
- **PRÉNOM :** ZAYNAB
- **DATE DE NAISSANCE :** 18/06/2002
- **NIVEAU :** 2<sup>ème</sup> Année Technicien Spécialisée en Infrastructure Digitale Option Système et Réseau

## DÉDICACE :

Nous dédions ce présent travail à :

◆ À notre Très chère Mère, pour sa compréhension, son amour et la tendresse qu'elle m'a toujours témoignée.

◆ À notre cher Père, pour tout le soutien qu'il m'a apporté, ses sacrifices et son affection.

◆ À mes chères Frères et sœurs.

◆ À nos chères Amies soutenus et encouragés

## **Remerciements**

Je tiens tout d'abord, à remercier tout particulièrement mes parents, **BELLAFRIKH MOHAMMED** et **NAJEM LAILA**, pour leur soutien indéfectible tout au long de mon cursus scolaire et universitaire. Leurs encouragements constants et leur confiance en moi m'ont permis de persévéérer dans mes études et de croire en mes capacités.

Je remercie mon maître de stage, Monsieur **HAMMADCHI AMINE**, pour son accueil chaleureux et son encadrement précieux tout au long de mon stage. Ses conseils avisés et sa disponibilité m'ont permis de beaucoup apprendre et de progresser dans mon domaine.

Nos sincères remerciements vont également à Mme Hasna Saadi, membre avisé du jury, pour le temps consacré et l'intérêt porté à l'évaluation de ce travail. Ses remarques éclairées et son analyse minutieuse ont permis d'enrichir et de consolider substantiellement la qualité de cette réalisation.

Je remercie également mes collègues, **EL ALAMY MOHAMMED** et **CHAIIJ ABDELFATTAH** pour leur collaboration et leur entraide au quotidien. J'ai beaucoup apprécié leur esprit d'équipe et leur bienveillance.

Je suis reconnaissant envers Institut Spécial de technologie appliquée **KELAA DES SRAGHNA** de m'avoir donné l'opportunité de faire un stage dans leur entreprise. Ce stage m'a permis de découvrir un nouveau métier et de mettre en pratique les connaissances acquises en formation.

Enfin, je profite de cette occasion pour exprimer mon remerciement à M. Le directeur de l'**ISTA EL KELAA DES SRAGHNA**, ainsi à tout le groupe administratif de l'institut pour leur bienveillance au bon déroulement de ma formation professionnelle au sein de l'établissement.

## Résumé

Ce rapport de stage présente une étude détaillée de l'implémentation et de l'utilisation de Wazuh, un système de gestion des informations et des événements de sécurité (SIEM) open-source. Il explore les fonctionnalités clés de Wazuh, notamment son intégration avec divers systèmes, la collecte et l'analyse des journaux, la détection d'anomalies et la génération d'alertes.

Le rapport met en lumière l'efficacité de Wazuh dans la surveillance en temps réel des activités suspectes au sein d'une infrastructure informatique. Cette capacité permet une identification rapide des menaces et une réponse immédiate aux incidents de sécurité, réduisant ainsi les risques potentiels et minimisant les dommages.

Au cours de ce stage, le déploiement de Wazuh a renforcé la supervision de la sécurité de l'infrastructure en centralisant la gestion des événements. L'installation de cette solution dans un serveur qui se trouve dans le même réseau ou se trouve les machines qui contiennent les données confidentielles qui doivent être sécurisé contre les attaques sophistiquées, sa facilité de mise en place et sa modularité en font une solution SIEM performante et économique pour l'établissement.

# wazuh.

## Chapitre 1 :

Présentation du Stage

## **INTRODUCTION**

Le stage est une étape importante dans la formation de chaque stagiaire, puisque c'est le seul moyen de mettre en œuvre l'ensemble des connaissances acquises pendant la formation, et de tirer profit de l'expérience de la vie professionnelle et de valoriser ses capacités et ses compétences. Dans ce cadre, j'ai passé un stage de fin de formation durant la période qui s'étend du 08/04/2024 au 05/05/2024 au sein de ISTA KELAA DES SRAGHNA.

J'essaierai dans ce rapport de donner une vue générale sur le déroulement du stage, le lieu du stage et les travaux réalisés.

## **Fiche Technique de l'ISTA :**

### **1) Identification**

- Dénomination : Institut Spécialisé de Technologie Appliquée El KELAA des SRAGHNA
- Date d'ouverture : 1988
- Directeur : CHAHIDI BADR
- Téléphone : 05 24 41 23 38

### **2) Consistance physique**

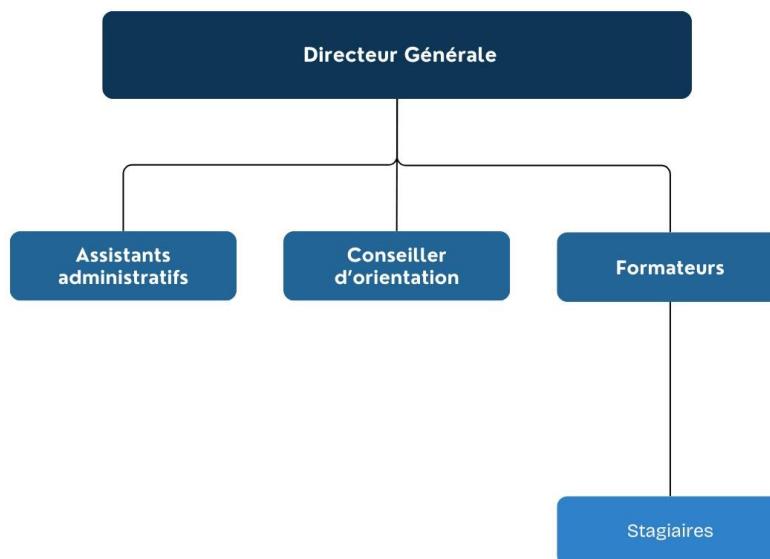
- Superficie : -Totale : 30 000 m<sup>2</sup> ; -couverture : 2150 m<sup>2</sup>
- Ateliers : 06
- Salles spécialisées : 02
- Salles de cours : 06
- Salle de séminaire : -
- Bloc administratif : 01
- Internat de capacité : -
- Magasin : 01
- Logements de fonction : 01
- Terrains de sport (nature et superficie) : Non aménagé
- Autres : -
- Les locaux vacants (Nbre et superficie) :

### **3) Ressources Humaines**

- Personnel Formateur : 26
- Personnel Administrateur : 07

**Organigramme ISTA :**

# **ORGANIGRAMME ISTA KELAA SRAGHNA**



## Les matériels utilisés

Routeur Cisco :	
Switch Cisco :	
Pare-feu Cisco :	
Serveur :	
PC bureau :	

Tableau 1

### Les travaux effectués :

#### 1) Scanner le réseau de direction :

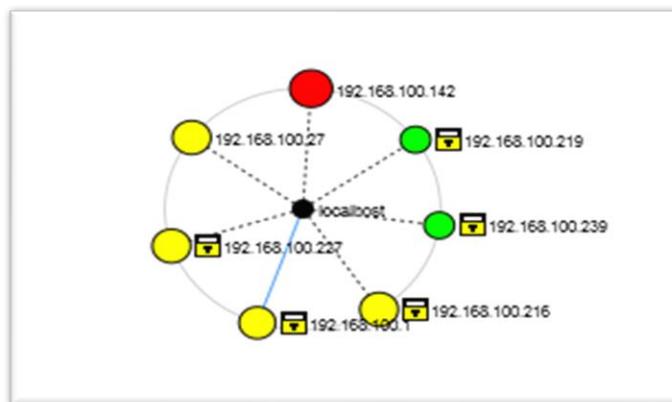


Figure 1

Équipement	Marque	@ IP	@ MAC
Routeur	Huawei Technologies	192.168.100.1	3C:15:FB:00:C8:D5
Imprimante	Kyocera Display	192.168.100.142	00:17:C8:D7:CC:F2
PC	Fujitsu Technology Solutions GmbH	192.168.100.219	00:19:99:5B:A0:77
Routeur	Netgear	192.168.100.239	C0:3F:0E:9D:FF:81
PC	Micro-Star Intl	192.168.100.227	00:D8:61:96:65:2E

Tableau 2

#### 2) Formatage d'un serveur :

Ses caractéristiques :

Nom du système d'exploitation	Microsoft Windows Server 2019 Standard Evaluation
Version	10.0.17763 Build 17763
Processeur	Intel(R) Xeon(R) CPU E5520 @ 2.27GHz, 2261 MHz, 4 cœurs(s), 8 processeurs(s) logique(s)
Mémoire physique (RAM) installée	24,0 Go
Mémoire physique totale	24,0 Go
HARD-DISK	272 Go

Tableau 3

✓ Accéder au serveur à distant Pour accéder à distant on utilise RDP :

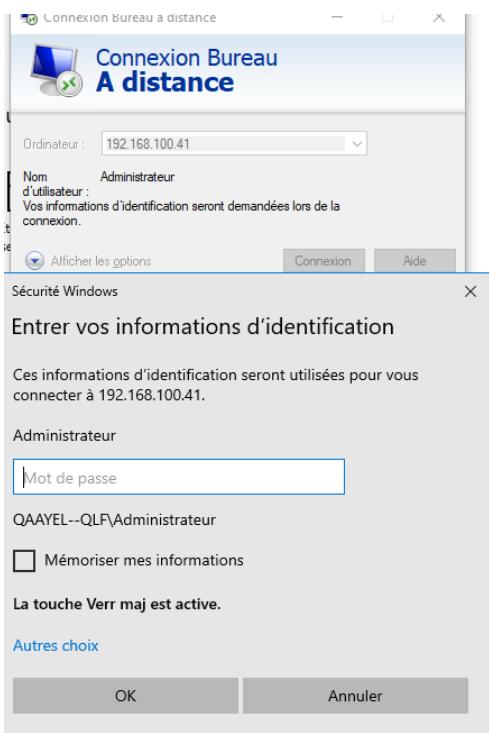


Figure 2

### 3) Formatage des PC :

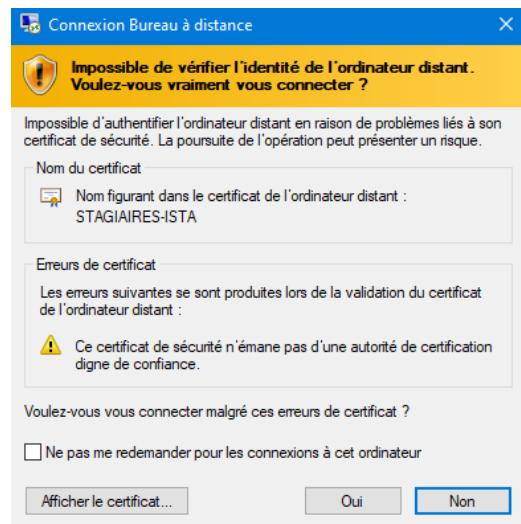


Figure 3

#### 4) Configuration des routeurs :

##### CONFIGURATION:

```
R1> ena
R1# conf t
R1 (config) # enable password cisco12
R1 (config) # enable secret cisco
R1 (config) # line console 0
R1 (config-line) # password cisco
R1 (config-line) # login
R1 (config-line) # exit
R1 (config) # line vty 0 15
R1 (config-line) # password cisco
SW (config-line) # login
R1 (config-line) # exit
R1 (config) # interface g0/0
R1 (config-if) # ip address 192.168.100.100 255.255.255.0
R1 (config-if) #no shutdown
R1 (config-if) #exit
R1 (config) # service password-encryption
R1 (config) # crypto key generate rsa
R1 (config) # ip ssh version 2
R1 (config) # line vty 0 4
R1 (config-line) # transport input ssh
R1 (config-line) # transport output ssh
R1 (config-line) # login local
R1 (config-line) # exit
R1 (config) # username ista password cisco
R1 (config) # end
R1 # wr
```

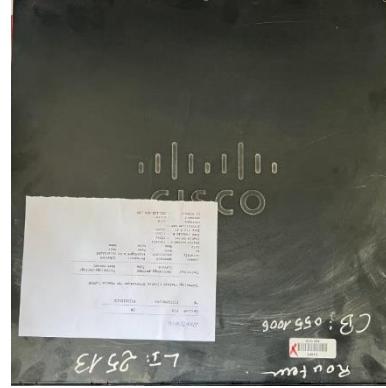
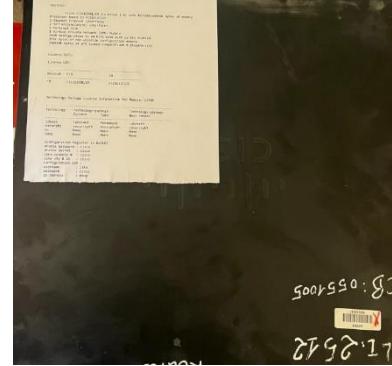
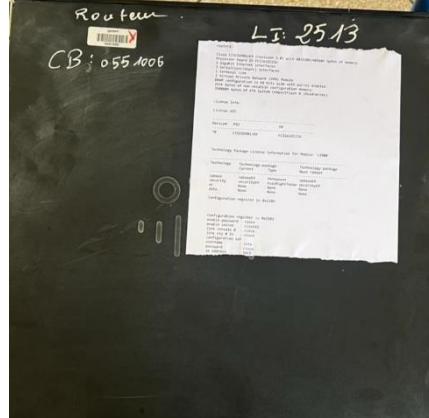
Configuration et fiche technique de routeur 1	 <p>A photograph of a Cisco router. A white configuration sheet is placed on top of the router. Below it, a technical card is visible. Handwritten text on the right side of the router includes "CB: 0551006", "L.I: 2513", and "Router".</p>
Configuration et fiche technique de routeur 2	 <p>A photograph of a Cisco router. A white configuration sheet is placed on top of the router. Handwritten text on the right side of the router includes "CB: 0551005" and "L.I: 2512".</p>
Configuration et fiche technique de routeur 1	 <p>A photograph of a Cisco router. A white configuration sheet is placed on top of the router. Handwritten text on the right side of the router includes "CB: 0551006", "L.I: 2513", and "Router".</p>

Tableau 4

## 5) Configuration des switches :

### CONFIGURATION :

```
SW > ena
SW # conf t
SW (config) # enable password cisco12
SW (config) # enable secret cisco
SW (config) # line console 0
SW (config-line) # password cisco
SW (config-line) # login
SW (config-line) # exit
SW (config) # line vty 0 15
SW (config-line) # password cisco
SW (config-line) # login
SW (config-line) # exit
SW (config) # vlan 10
SW (config-vlan) # exit
SW (config) # interface vlan10
SW (config-if) # ip address 192.168.100.42 255.255.255.0
SW (config-if) #exit
SW (config) # service password-encryption
SW (config) # crypto key generate rsa
SW (config) # ip ssh version 2
SW (config) # line vty 0 4
SW (config-line) # transport input ssh
SW (config-line) # transport output ssh
SW (config-line) # login local
SW (config-line) # exit
SW (config) # username ista password cisco
SW (config) # end
SW # wr
```

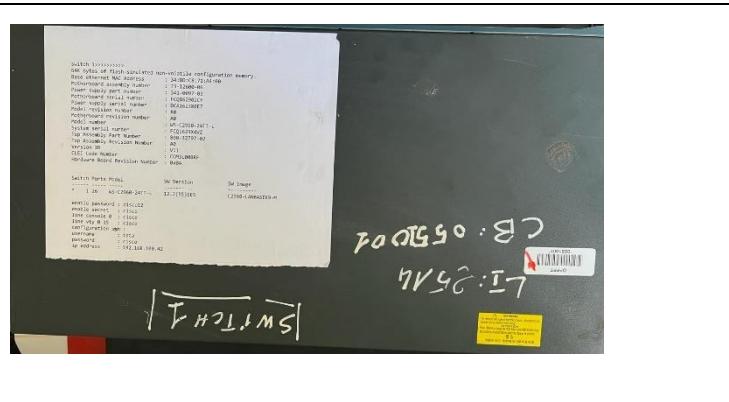
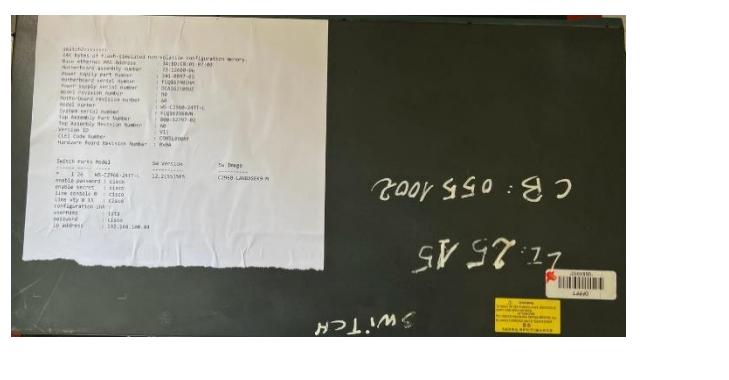
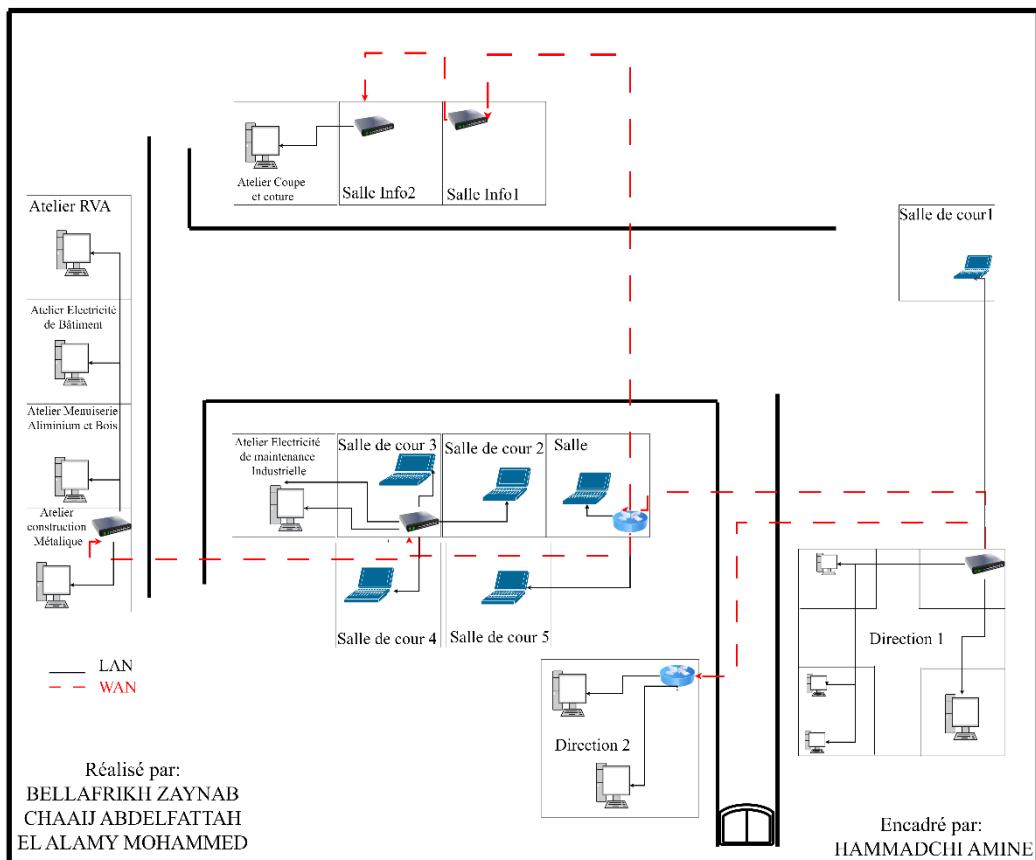
<p><b>Configuration et fiche technique de switch 1</b></p>	
<p><b>Configuration et fiche technique de switch 1</b></p>	
<p><b>Password des switches</b></p>	
<p><b>Routeurs et switches empilés</b></p>	

Tableau 5

**6) Plan de réseau ISTA KELAA SRAGHNA :**

## **PLAN RESEAU ISTA KELAA DES SRAGHNA**



**Figure 4**

Lieu du matériel	Marque du matériel
Direction 1	Switch Cisco / Routeur HUAWEI
Direction 2	Routeur
Salle	Routeur Netgear
Salle 3	Switch CONNECTION N&C
Salle Info 1	Switch Cisco
Salle Info 2	Switch Cisco
Atelier Construction Métallique	Switch D-Link

**Tableau 6**

## 7) Test des ports de salle info 1 et 2 :

Salle Info 1

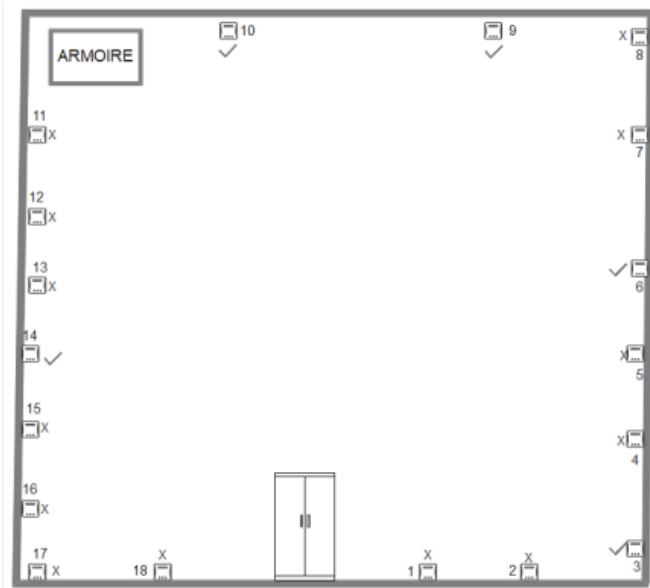


Figure 5

PORT	Pont brassage	Switch port	Fonctionne	Cable ne fonctionne pas
1	-	-	NON	-
2	-	-	-	-
3	4	4	OUI	-
4	5	5	OUI	-
5	-	-	-	-
6	7	7	OUI	-
7	8	6	NON	7
8	9	9	NON	8
9	10	10	OUI	-
10	11	11	OUI	-
11	12	12	NON	4-6-8
12	13	13	NON	4-5
13	14	14	NON	1-4-8
14	15	15	OUI	-
15	16	16	NON	5
16	-	-	-	-
17	18	18	NON	1-8
18	19	19	NON	1-7

Tableau 7

## Salle Info 2

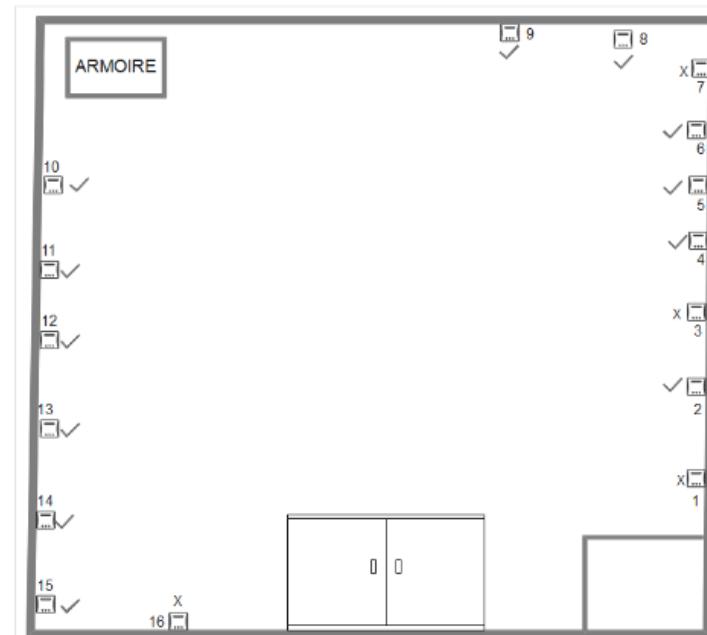


Figure 6

PORT	Pont brassage	Switch port	Fonctionne	Cable ne fonctionne pas
<b>1</b>	14	14	NON	<b>3-4</b>
<b>2</b>	13	13	OUI	-
<b>3</b>	12	12	NON	<b>2-4-8</b>
<b>4</b>	18	15	OUI	-
<b>5</b>	11	11	OUI	-
<b>6</b>	10	1	OUI	-
<b>7</b>	20	20	NON	<b>4</b>
<b>8</b>	17	17	OUI	-
<b>9</b>	9	9	OUI	-
<b>10</b>	8	8	OUI	-
<b>11</b>	7	7	OUI	-
<b>12</b>	6	6	OUI	-
<b>13</b>	5	2	OUI	-
<b>14</b>	4	5	OUI	-
<b>15</b>	3	3	OUI	-
<b>16</b>	2	4	NON	<b>4-7</b>

Tableau 8

**8) Sticker l'armoire de salle info 1 :**



Figure 7



Figure 8

**9) Sticker l'armoire de salle Info 2**



Figure 9



Figure 10

**10) Connecter l'appareil Bosch au réseau et Lancement de dernière version de MISE À JOUR :**



Figure 11

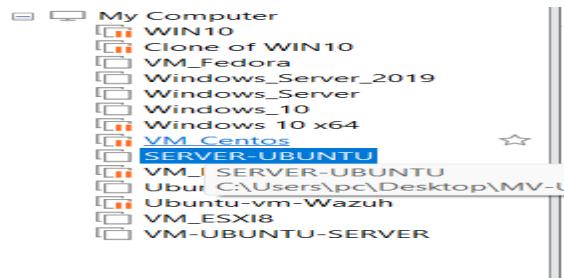


Figure 12

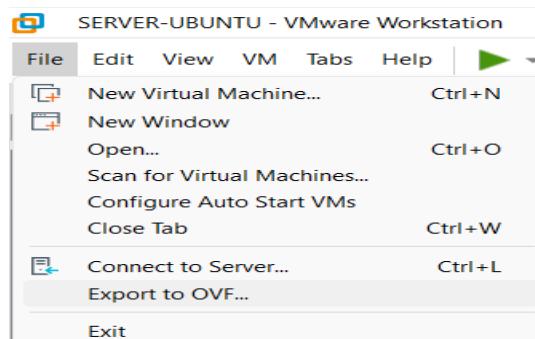
## 11) Exporter une machine virtuelle Ubuntu-server et l'importer dans ESXi8

### ✓ Exporter une machine virtuelle VMWARE WORKSTATION :

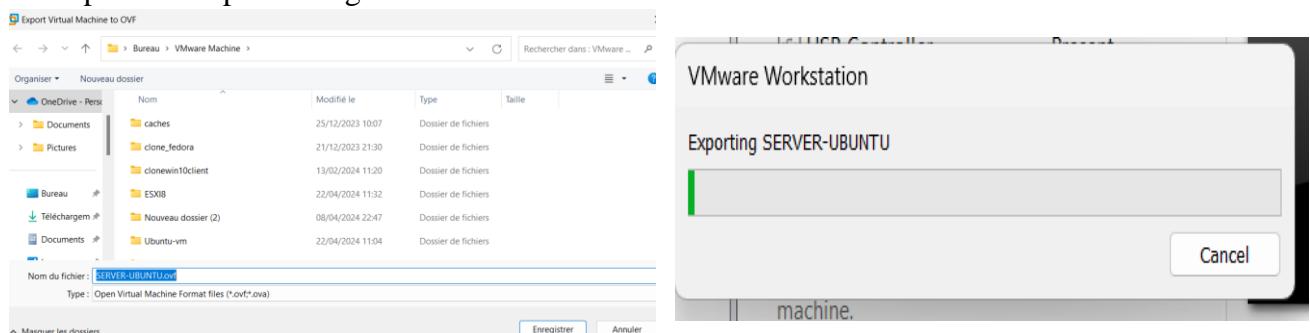
Sélectionnez la machine virtuelle que vous souhaitez exporter



Allez dans Fichier > Exporter to OVF Virtual Machine

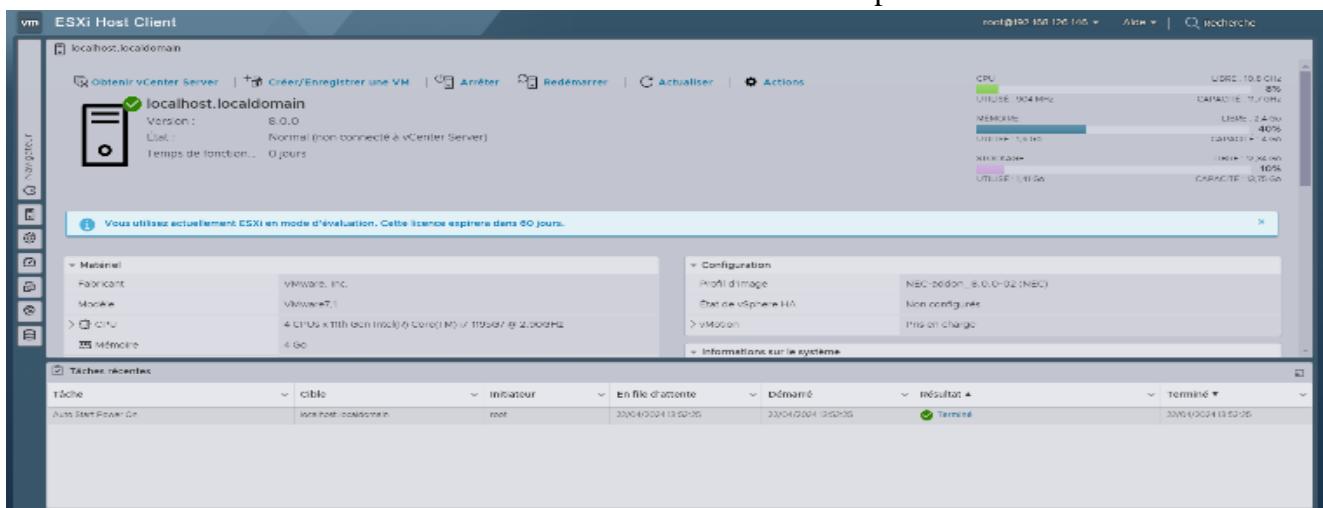


Sélectionnez OVF ou OVA comme format de fichier de destination et Spécifiez un emplacement pour enregistrer le fichier OVF/OVA > Terminer

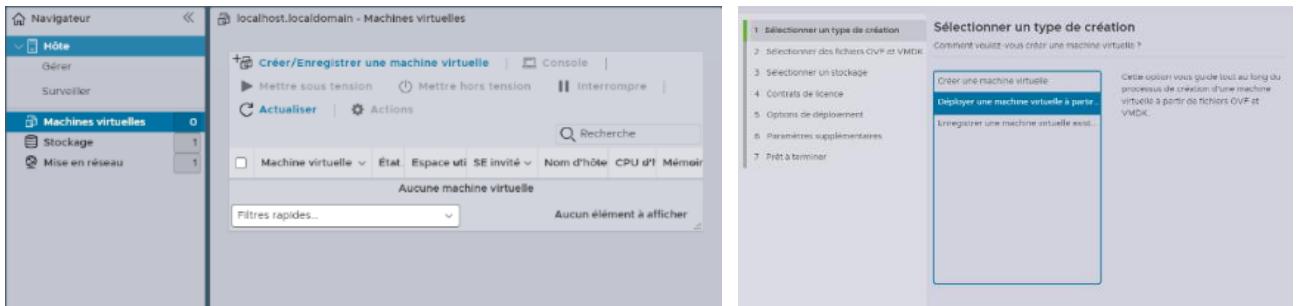


### ✓ Importer une machine virtuelle au format OVF/OVA dans ESXi 8 :

Connectez-vous à votre serveur ESXi 8 via l'interface Web ou vSphere Client



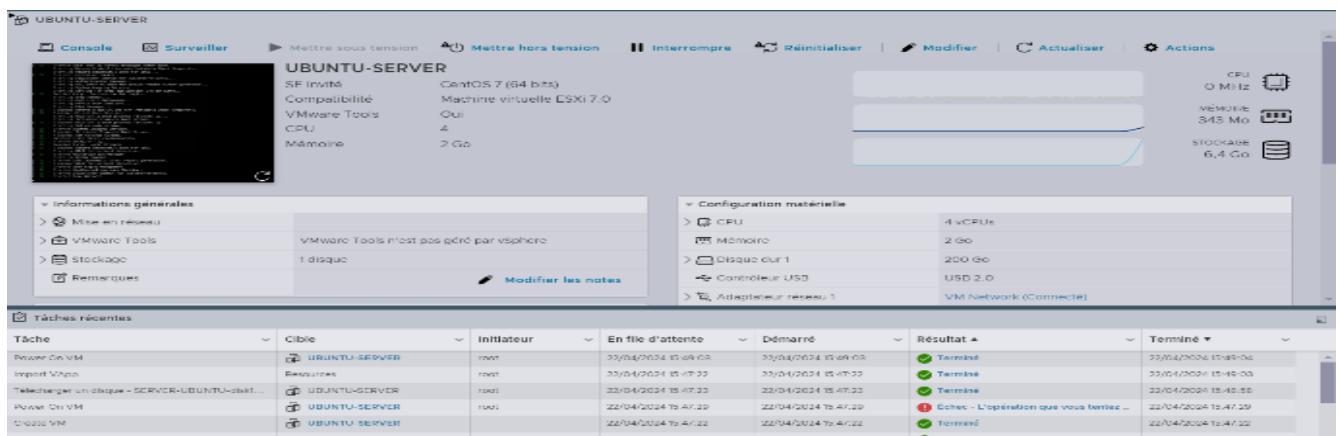
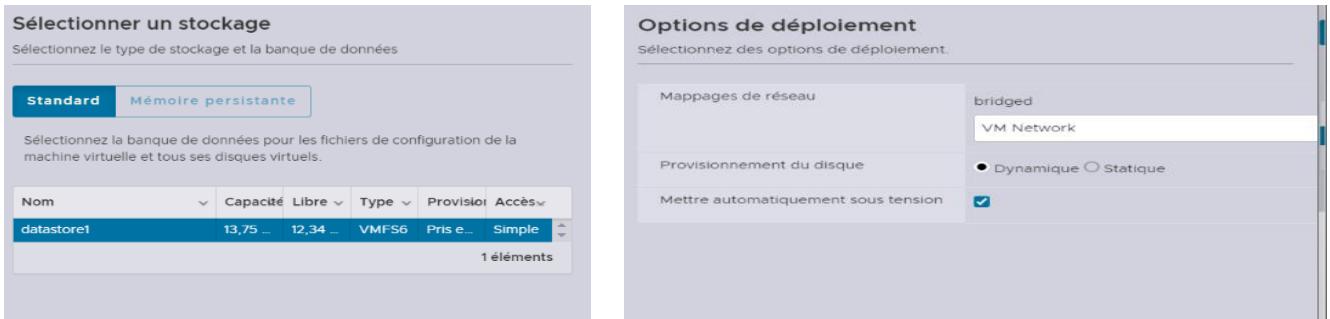
Allez dans Machines virtuelles > Créer/Enregidtrer une machine virtuelle > Déployer une machine virtuelle à partir d'un fichier



Sélectionnez le fichier OVF/OVA que vous avez exporté



Suivez les invites de l'assistant pour sélectionner un datastore, un nom de machine virtuelle et d'autres options de déploiement. Cliquez sur Terminer



# wazuh.

## Chapitre 2 :

État de l'art

## **Introduction :**

Dans le paysage numérique actuel, les organisations sont confrontées à un nombre croissant de menaces cybernétiques sophistiquées. La compromission de données, les attaques par ransomware et les intrusions dans les systèmes critiques ne sont que quelques exemples des périls auxquels les entreprises sont exposées. Pour faire face à ces menaces, il est crucial de mettre en place des solutions de sécurité robustes et efficaces.

Les systèmes de gestion des informations et des événements de sécurité (SIEM) jouent un rôle essentiel dans la protection des infrastructures informatiques. En centralisant la collecte et l'analyse des journaux provenant de divers systèmes et sources, les SIEM permettent aux organisations d'identifier les comportements suspects, de détecter les intrusions et de répondre rapidement aux incidents de sécurité.

## **IV SIEM**

ISTA kelaa des sraghna est confronté à une augmentation des incidents de sécurité informatique, tels que les intrusions, les malwares et les tentatives de phishing. Ces incidents peuvent entraîner des vols de données sensibles, des perturbations des cours et une atteinte à la réputation de l'établissement. Autant que stagiaire dans cet établissement, j'ai proposé La mise en place d'un système SIEM comme solution. Cette dernière peut aider l'établissement à mieux gérer ses risques de sécurité informatique.

### **1. Définition :**

SIEM signifie : systèmes de gestion des événements et des informations de sécurité. Par définition, les SIEM sont des systèmes centralisés qui offrent une visibilité totale sur l'activité de votre réseau et vous permettent ainsi de réagir aux menaces en temps réel. Les SIEM permettent de collecter, de lire et de catégoriser les données machine d'une grande diversité de sources, puis analysent celles-ci pour produire des informations qui vous permettront d'agir.

### **2. Avantages de l'utilisation d'un SIEM**

Les outils SIEM offrent de nombreux avantages qui peuvent contribuer à renforcer l'état de la sécurité globale d'une organisation, notamment :

- Vue centralisée des menaces potentielles
- Identification et réponse aux menaces en temps réel
- Veille des menaces avancée
- Audits et rapports sur la conformité réglementaire
- Plus grande transparence en termes de surveillance des utilisateurs, des applications et des appareils

### **3. Rôle des technologies SIEM**

Une solution SIEM est une composante importante de l'écosystème de cybersécurité d'une organisation. Une solution SIEM offre aux équipes chargées de la sécurité un emplacement central pour collecter, agréger et analyser de gros volumes de données à l'échelle de l'entreprise, ce qui permet de rationaliser efficacement les flux de travail en matière de sécurité. Elle offre également des fonctionnalités opérationnelles telles que des rapports de conformité, une solution de gestion des incidents et des tableaux de bord qui classent les menaces par ordre de priorité.

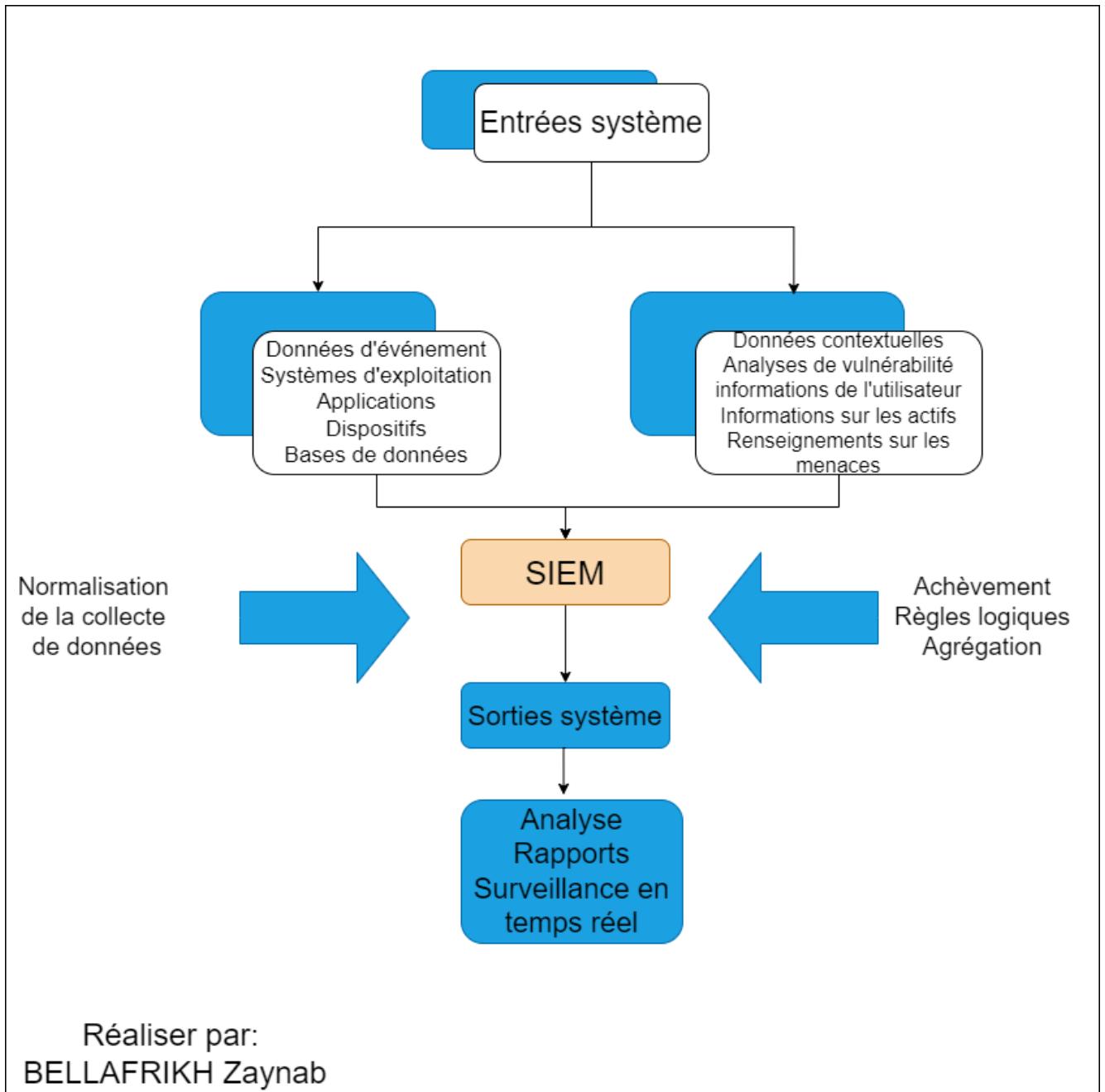
### **4. Fonctionnalités SIEM et cas d'utilisation**

Les systèmes SIEM varient en termes de capacités, mais offrent généralement les fonctions de base suivantes :

- Gestion des journaux : Les systèmes SIEM centralisent de grandes quantités de données qu'ils organisent avant de déterminer si celles-ci présentent des signes de menace, d'attaque ou de violation.
- Corrélation entre les événements : Les données sont ensuite triées pour identifier les relations et les schémas afin de détecter rapidement les menaces potentielles et d'y répondre.
- Surveillance et réponse aux incidents : Les technologies SIEM surveillent les incidents liés à la sécurité sur le réseau d'une organisation, et fournissent des alertes et des audits pour toutes les activités en lien avec ces incidents.

Les systèmes SIEM peuvent atténuer les cyberrisques grâce à une série de cas d'utilisation tels que la détection des activités suspectes des utilisateurs, la surveillance des comportements de ceux-ci, la limitation des tentatives d'accès et la génération de rapports de conformité.

## 5. Architecture de SIEM :



## 6. Meilleurs pratiques pour la mise en place d'un SIEM

La mise en place d'un système de gestion des informations et des événements de sécurité (SIEM) est essentielle pour renforcer la posture de cybersécurité des organisations. Voici quelques meilleures pratiques pour une mise en œuvre réussie du SIEM :

- **Clarifiez vos objectifs SIEM :** Avant de commencer, définissez clairement ce que vous souhaitez réaliser avec votre SIEM. Voulez-vous améliorer la visibilité, garantir la conformité réglementaire ou renforcer la détection des menaces ? Cette définition guidera tout le processus de mise en œuvre.
- **Pensez petit d'abord :** Lors de la phase de découverte, pilotez le système SIEM sur un petit sous-ensemble représentatif de la technologie et des politiques de votre organisation. Cela permettra de collecter des données cruciales pour guider les modifications nécessaires avant un déploiement à grande échelle.
- **Évaluation des besoins et objectifs de sécurité :** Comprenez les besoins spécifiques de votre entreprise en matière de sécurité. Quelles sont les menaces auxquelles vous êtes confronté ? Quels sont vos objectifs de sécurité ? Cette évaluation vous aidera à choisir la solution SIEM la mieux adaptée à votre contexte<sup>1</sup>.
- **Configuration des sources de données et des politiques de corrélation :** Assurez-vous que toutes les sources de données pertinentes (logs, événements, etc.) sont correctement configurées pour alimenter le SIEM. Définissez également des politiques de corrélation pour détecter les anomalies et les menaces.
- **Formation des équipes de sécurité :** Formez vos équipes de sécurité à l'utilisation et à la gestion du SIEM. Ils doivent comprendre comment interpréter les alertes, enquêter sur les incidents et prendre des mesures appropriées.
- **Testez et ajustez la solution :** Avant le déploiement complet, effectuez des tests approfondis pour vous assurer que le SIEM fonctionne correctement. Ajustez les paramètres si nécessaire pour optimiser les performances<sup>2</sup>.

## II\ Le choix de Wazuh comme solution SIEM

### 1. Définition

Wazuh est une plate-forme de sécurité SI tout-en-un, open source et puissante, conçue pour protéger les organisations contre les menaces cybernétiques

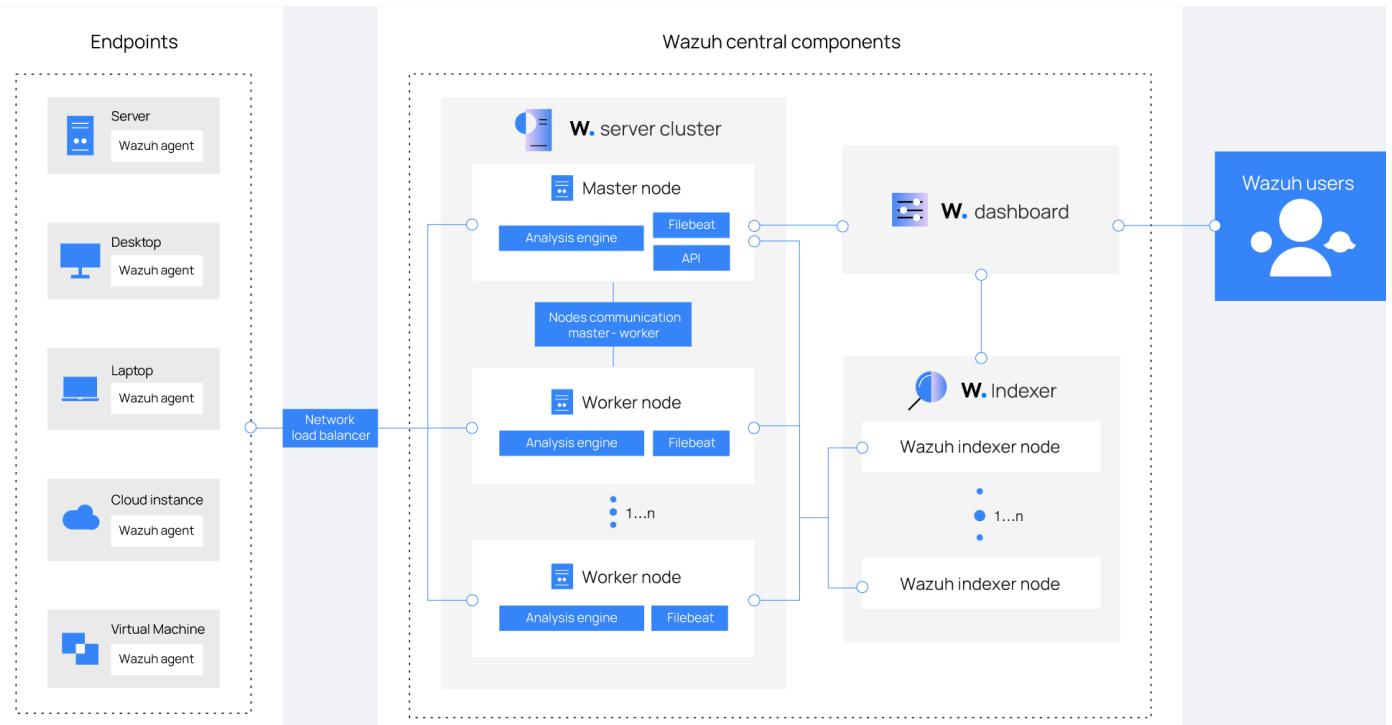
### 2. Fonctionnalité de Wazuh

- Détection d'Intrusions (IDS/IPS) : Wazuh surveille en temps réel les activités du système et les journaux de sécurité, repérant les comportements suspects qui pourraient indiquer une intrusion.
- Corrélation des Événements : La plateforme analyse et connecte les informations provenant de diverses sources pour identifier les attaques complexes, permettant une réponse plus efficace.
- Analyse des Logs : Wazuh excelle dans l'analyse approfondie des journaux, aidant les utilisateurs à comprendre les activités du système et à réagir rapidement en cas d'incident.
- Gestion de Vulnérabilités : En identifiant et évaluant les faiblesses potentielles du système, Wazuh aide à renforcer la sécurité en anticipant les vulnérabilités.
- Conformité et Rapports : La plate-forme génère des rapports détaillés pour aider les organisations à respecter les normes de sécurité, facilitant ainsi la démonstration de la conformité.
- Extensibilité et Intégrations : Wazuh peut être facilement étendu grâce à des modules complémentaires et s'intègre avec d'autres outils de sécurité, offrant une flexibilité d'utilisation.
- Architecture Évolutive : Que ce soit dans des environnements de petite ou grande envergure, sur site ou dans le cloud, Wazuh propose une architecture évolutive pour répondre aux besoins variés.
- Corrélation et Threat Intelligence : La plateforme utilise des mécanismes avancés de corrélation et s'appuie sur des informations sur les menaces pour améliorer la précision de la détection.

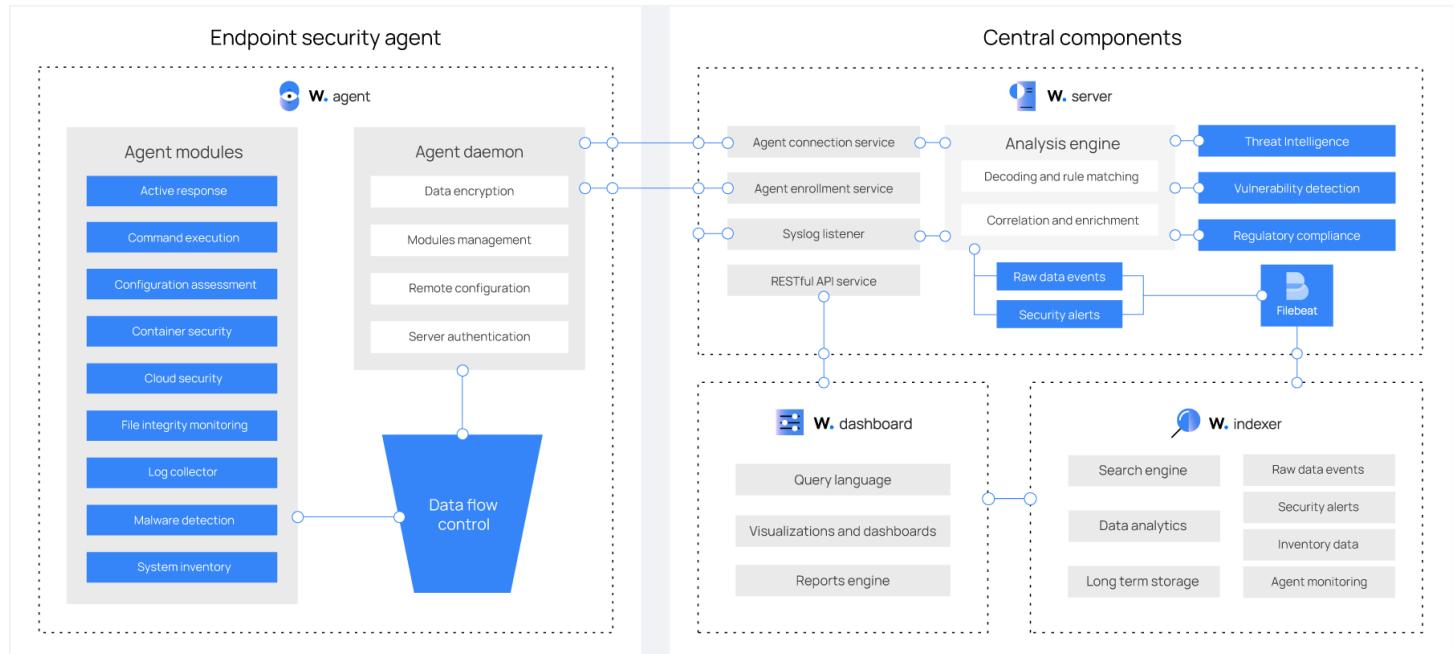
### 3. Avantages de Wazuh

- Open Source : Wazuh est gratuit, flexible et ne nécessite pas de licence. Il est pris en charge par une communauté active et est utilisé par des milliers d'utilisateurs d'entreprise.
- Protection des points de terminaison : Wazuh offre une protection pour les points de terminaison, qu'ils soient dans le cloud public, le cloud privé ou les centres de données sur site.
- Scalabilité : La solution est hautement évolutive et peut être déployée dans des environnements cloud gérés.
- Pas de verrouillage fournisseur : Wazuh ne vous lie pas à un fournisseur spécifique.
- Conformité réglementaire : Wazuh facilite la conformité avec les réglementations de sécurité

### 4. Architecture de Wazuh



## 5. Composants de Wazuh



# wazuh.

## Chapitre 3 :

Mise en place de Wazuh

## I\ Installation de Wazuh

### 1. Installer l'indexeur Wazuh

#### ➤ Création de certificats

Téléchargez le wazuh-certs-tool.sh script et le config.yml fichier de configuration. Cela crée les certificats qui chiffrent les communications entre les composants centraux Wazuh.

```
root@id-virtual-machine:/home/id# curl -s0 https://packages.wazuh.com/4.7/wazuh-certs-tool.sh
root@id-virtual-machine:/home/id# curl -s0 https://packages.wazuh.com/4.7/config.yml
root@id-virtual-machine:/home/id# 
```

Modifiez `./config.yml` et remplacez les valeurs IP par les adresses IP correspondants

```
root@id-virtual-machine:/home/id# ls
config.yml  Documents  Music      Public   Templates  wazuh-certs-tool.sh
Desktop      Downloads  Pictures   snap     Videos
root@id-virtual-machine:/home/id# nano config.yml 
```

```
GNU nano 6.2                                     config.yml                                     GNU nano 6.2                                     config.yml *
nodes:
# Wazuh indexer nodes
indexer:
- name: node-1
  ip: "<indexer-node-ip>" 
#- name: node-2
# ip: "<indexer-node-ip>" 
#- name: node-3
# ip: "<indexer-node-ip>" 

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
- name: wazuh-1
  ip: "<wazuh-manager-ip>" 
# node_type: master
#- name: wazuh-2
# ip: "<wazuh-manager-ip>" 
# node_type: worker
#- name: wazuh-3
# ip: "<wazuh-manager-ip>" 
# node_type: worker

# Wazuh dashboard nodes
dashboard:
- name: dashboard
  ip: "<dashboard-node-ip>" 

nodes:
# Wazuh indexer nodes
indexer:
- name: node-1
  ip: "127.0.0.1"
#- name: node-2
# ip: "<indexer-node-ip>" 
#- name: node-3
# ip: "<indexer-node-ip>" 

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
- name: wazuh-1
  ip: "127.0.0.1"
# node_type: master
#- name: wazuh-2
# ip: "<wazuh-manager-ip>" 
# node_type: worker
#- name: wazuh-3
# ip: "<wazuh-manager-ip>" 
# node_type: worker

# Wazuh dashboard nodes
dashboard:
- name: dashboard
  ip: "127.0.0.1" 
```

Exécutez `./wazuh-certs-tool.sh` pour créer les certificats

```
root@id-virtual-machine:/home/id# bash ./wazuh-certs-tool.sh -A
02/05/2024 10:09:25 INFO: Admin certificates created.
02/05/2024 10:09:25 INFO: Wazuh indexer certificates created.
02/05/2024 10:09:26 INFO: Wazuh server certificates created.
02/05/2024 10:09:26 INFO: Wazuh dashboard certificates created.
```

Comptez tous les fichiers nécessaires

```
root@id-virtual-machine:/home/id# tar -cvf ./wazuh-certificates.tar ./node-1-key.pem ./admin.pem ./root-ca.key ./root-ca.pem ./dashboard.pem ./node-1.pem ./wazuh-1-key.pem ./admin-key.pem ./wazuh-1.pem ./dashboard-key.pem
```

```
root@id-virtual-machine:/home/id# rm -rf ./wazuh-certificates
root@id-virtual-machine:/home/id# ls
config.yml  Documents  Music      Public    Templates  wazuh-certificates.tar
Desktop     Downloads  Pictures   snap       Videos    wazuh-certs-tool.sh
```

➤ Installation des nœuds

Installation des dépendances du package

```
root@id-virtual-machine:/home/id# apt-get install debconf adduser procps
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
adduser is already the newest version (3.118ubuntu5).
adduser set to manually installed.
debconf is already the newest version (1.5.79ubuntu1).
debconf set to manually installed.
procps is already the newest version (2:3.3.17-6ubuntu2.1).
procps set to manually installed.
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

## ➤ Ajout du référentiel Wazuh

Installer les package suivants s'ils sont manquants

```
root@id-virtual-machine:/home/id# apt-get install gnupg apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.2.27-3ubuntu2.1).
gnupg set to manually installed.
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 1,510 B of archives.
After this operation, 170 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 apt-transport-https all 2.4.12 [1,510 B]
Fetched 1,510 B in 1s (2,688 B/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 204546 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.4.12_all.deb ...
Unpacking apt-transport-https (2.4.12) ...
Setting up apt-transport-https (2.4.12) ...
```

Installer la clé GPG

```
root@id-virtual-machine:/home/id# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: keyring '/usr/share/keyrings/wazuh.gpg' created
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 96B3EE5F29111145: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" imported
gpg: Total number processed: 1
gpg:           imported: 1
```

Mettez à jour les informations sur les packages

```
id@id-virtual-machine:~$ sudo apt-get update
```

Installer le package de l'indexeur Wazuh

```
root@id-virtual-machine:/home/id# apt-get install wazuh-indexer
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  wazuh-indexer
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 683 MB of archives.
After this operation, 969 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-indexer amd64 4.7.4-1 [683 MB]
Fetched 683 MB in 1min 7s (10.2 MB/s)
Selecting previously unselected package wazuh-indexer.
(Reading database ... 204550 files and directories currently installed.)
Preparing to unpack .../wazuh-indexer_4.7.4-1_amd64.deb ...
Creating wazuh-indexer group... OK
Creating wazuh-indexer user... OK
Unpacking wazuh-indexer (4.7.4-1) ...
Setting up wazuh-indexer (4.7.4-1) ...
Created opensearch keystore in /etc/wazuh-indexer/opensearch.keystore
Processing triggers for libc-bin (2.35-0ubuntu3.7) ...
```

Modifiez le `/etc/wazuh-indexer/opensearch.yml` fichier de configuration

```
root@id-virtual-machine:/home/id# nano /etc/wazuh-indexer/opensearch.yml
GNU nano 6.2                               /etc/wazuh-indexer/opensearch.yml *
network.host: "127.0.0.1"
node.name: "node-1"
cluster.initial_master_nodes:
- "node-1"
#- "node-2"
#- "node-3"
cluster.name: "wazuh-cluster"
#discovery.seed_hosts:
# - "node-1-ip"
# - "node-2-ip"
# - "node-3-ip"
node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false

plugins.security.authcz.admin_dn:
- "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
- "CN=node-1,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-2,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-3,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
- "all_access"
- "security_rest_api_access"

plugins.security.system_indices.enabled: true
plugins.security.system_indices.indices: [".plugins-ml-model", ".plugins-ml-task", ".opendistro-alerting"]
### Option to allow Filebeat-oss 7.10.2 to work ###
compatibility.override_main_response_version: true
```

Exécutez les commandes suivantes en les remplaçant `<indexer-node-name>` par le nom du nœud d'indexation Wazuh que vous configurez comme défini dans `config.yml`. Celui-ci déploie les certificats SSL pour crypter les communications entre les composants centraux Wazuh

```
root@id-virtual-machine:/home/id# mkdir /etc/wazuh-indexer/certs
root@id-virtual-machine:/home/id# tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem
root@id-virtual-machine:/home/id# mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem /etc/wazuh-indexer/certs/indexer.pem
root@id-virtual-machine:/home/id# mv -n /etc/wazuh-indexer/certs/$NODE_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem
root@id-virtual-machine:/home/id# chmod 500 /etc/wazuh-indexer/certs
root@id-virtual-machine:/home/id# chmod 400 /etc/wazuh-indexer/certs/*
root@id-virtual-machine:/home/id# chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

```
root@id-virtual-machine:/home/id# NODE_NAME=node-1
```

## Démarrage du service

```
root@id-virtual-machine:/home/id# systemctl daemon-reload
root@id-virtual-machine:/home/id# systemctl start wazuh-indexer
root@id-virtual-machine:/home/id# systemctl enable wazuh-indexer
```

### ➤ Initialisation du cluster

```
root@id-virtual-machine:/home/id# /usr/share/wazuh-indexer/bin/indexer-security-init.sh
*****
** This tool will be deprecated in the next major release of OpenSearch **
** https://github.com/opensearch-project/security/issues/1755
*****
Security Admin v7
Will connect to 127.0.0.1:9200 ... done
Connected as "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
OpenSearch Version: 2.8.0
Contacting opensearch cluster 'opensearch' and wait for YELLOW clusterstate ...
Clustername: wazuh-cluster
Clusterstate: GREEN
Number of nodes: 1
Number of data nodes: 1
.opendistro_security index does not exists, attempt to create it ... done (0-all replicas)
Populate config from /etc/wazuh-indexer/opensearch-security/
Will update '/config' with /etc/wazuh-indexer/opensearch-security/config.yml
  SUCC: Configuration for 'config' created or updated
Will update '/roles' with /etc/wazuh-indexer/opensearch-security/roles.yml
  SUCC: Configuration for 'roles' created or updated
Will update '/rolesmapping' with /etc/wazuh-indexer/opensearch-security/roles_mapping.yml
  SUCC: Configuration for 'rolesmapping' created or updated
Will update '/internalusers' with /etc/wazuh-indexer/opensearch-security/internal_users.yml
  SUCC: Configuration for 'internalusers' created or updated
Will update '/actiongroups' with /etc/wazuh-indexer/opensearch-security/action_groups.yml
  SUCC: Configuration for 'actiongroups' created or updated
Will update '/tenants' with /etc/wazuh-indexer/opensearch-security/tenants.yml
  SUCC: Configuration for 'tenants' created or updated
Will update '/nodesdn' with /etc/wazuh-indexer/opensearch-security/nodes_dn.yml
  SUCC: Configuration for 'nodesdn' created or updated
Will update '/whitelist' with /etc/wazuh-indexer/opensearch-security/whitelist.yml
  SUCC: Configuration for 'whitelist' created or updated
Will update '/audit' with /etc/wazuh-indexer/opensearch-security/audit.yml
  SUCC: Configuration for 'audit' created or updated
Will update '/allowlist' with /etc/wazuh-indexer/opensearch-security/allowlist.yml
  SUCC: Configuration for 'allowlist' created or updated
SUCC: Expected 10 config types for node {"updated_config_types": ["allowlist", "tenants", "rolesmapping", "nodesdn", "audit", "roles", "whitelist", "internalusers", "actiongroups", "config"], "updated_config_size": 10, "message": null} is 10 ([{"allowlist", "tenants", "rolesmapping", "nodesdn", "audit", "roles", "whitelist", "internalusers", "actiongroups", "config"]]) due to: null
Done with success
```

## 2. Installer le serveur Wazuh

### ➤ Installation du gestionnaire Wazuh

Installer le package du gestionnaire Wazuh

```
root@id-virtual-machine:/home/id# apt-get -y install wazuh-manager
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  expect
The following NEW packages will be installed:
  wazuh-manager
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 172 MB of archives.
After this operation, 631 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-manager amd64 4.7.4-1 [172 MB]
Fetched 172 MB in 22s (7,801 kB/s)
Selecting previously unselected package wazuh-manager.
(Reading database ... 205676 files and directories currently installed.)
Preparing to unpack .../wazuh-manager_4.7.4-1_amd64.deb ...
Unpacking wazuh-manager (4.7.4-1) ...
Setting up wazuh-manager (4.7.4-1) ...
```

Activez et démarrez le service de gestion Wazuh

```
root@id-virtual-machine:/home/id# systemctl daemon-reload
root@id-virtual-machine:/home/id# systemctl start wazuh-manager
root@id-virtual-machine:/home/id# systemctl enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service → /lib/systemd/system/w
zuh-manager.service.
```

### ➤ Installation de Filebeat

Installer le package Filebeat

```
root@id-virtual-machine:/home/id# apt-get -y install filebeat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 22.1 MB of archives.
After this operation, 73.6 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 filebeat amd64 7.10.2 [22.1 MB]
Fetched 22.1 MB in 3s (8,253 kB/s)
Selecting previously unselected package filebeat.
(Reading database ... 227021 files and directories currently installed.)
Preparing to unpack .../filebeat_7.10.2_amd64.deb ...
Unpacking filebeat (7.10.2) ...
Setting up filebeat (7.10.2) ...
```

## ➤ Configuration de Filebeat

Téléchargez le fichier de configuration Filebeat préconfiguré

```
root@id-virtual-machine:/home/id# curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.7/tpl/wazuh/filebeat/filebeat.yml
```

Modifiez le `/etc/filebeat/filebeat.yml` fichier de configuration

```
root@id-virtual-machine:/home/id# nano /etc/filebeat/filebeat.yml
```

```
GNU nano 6.2                                     /etc/filebeat/filebeat.yml
# Wazuh - Filebeat configuration file
output.elasticsearch:
  hosts: ["127.0.0.1:9200"]
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificateAuthorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/filebeat.pem"
  ssl.key: "/etc/filebeat/certs/filebeat-key.pem"
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: false

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
  permissions: 0644

logging.metrics.enabled: false

seccomp:
  default_action: allow
  syscalls:
    - action: allow
      names:
        - rseq
```

Créez un magasin de clés Filebeat pour stocker en toute sécurité les informations d'authentification.

```
root@id-virtual-machine:/home/id# filebeat keystore create
Created filebeat keystore
```

Ajoutez le nom d'utilisateur et le mot de passe par défaut `admin : admin` au magasin de clés secrets

```
root@id-virtual-machine:/home/id# echo admin | filebeat keystore add username --stdin --force
Successfully updated the keystore
root@id-virtual-machine:/home/id# echo admin | filebeat keystore add password --stdin --force
Successfully updated the keystore
```

Téléchargez le modèle d'alertes pour l'indexeur Wazuh

```
root@id-virtual-machine:/home/id# curl -s /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v4.7.4/extensions/elasticsearch/7.x/wazuh-template.json
root@id-virtual-machine:/home/id# chmod go+r /etc/filebeat/wazuh-template.json
```

Installez le module Wazuh pour Filebeat

```
root@id-virtual-machine:/home/id# curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.3.tar.gz | tar -xvz -C /usr/share/filebeat/module
wazuh/
wazuh/archives/
wazuh/archives/ingest/
wazuh/archives/ingest/pipeline.json
wazuh/archives/config/
wazuh/archives/config/archives.yml
wazuh/archives/manifest.yml
wazuh/_meta/
wazuh/_meta/config.yml
wazuh/_meta/docs.asciidoc
wazuh/_meta/fields.yml
wazuh/alerts/
wazuh/alerts/ingest/
wazuh/alerts/ingest/pipeline.json
wazuh/alerts/config/
wazuh/alerts/config/alerts.yml
wazuh/alerts/manifest.yml
wazuh/module.yml
```

#### ➤ Déploiement de certificats

Remplacez <SERVER\_NODE\_NAME> par le nom de certificat de votre nœud de serveur Wazuh, le même que celui utilisé `config.yml` lors de la création des certificats. Ensuite, déplacez les certificats vers leur emplacement correspondant.

```
root@id-virtual-machine:/home/id# NODE_NAME=wazuh-1
```

```
root@id-virtual-machine:/home/id# mkdir /etc/filebeat/certs
root@id-virtual-machine:/home/id# tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./${NODE_NAME}.pem
root@id-virtual-machine:/home/id# mv -n /etc/filebeat/certs/${NODE_NAME}.pem /etc/filebeat/certs/filebeat.pem
root@id-virtual-machine:/home/id# mv -n /etc/filebeat/certs/${NODE_NAME}-key.pem /etc/filebeat/certs/filebeat-key.pem
root@id-virtual-machine:/home/id# chmod 500 /etc/filebeat/certs
root@id-virtual-machine:/home/id# chmod 400 /etc/filebeat/certs/*
root@id-virtual-machine:/home/id# chown -R root:root /etc/filebeat/certs
```

#### ➤ Démarrage du service Filebeat

```
root@id-virtual-machine:/home/id# systemctl daemon-reload
root@id-virtual-machine:/home/id# systemctl start filebeat
root@id-virtual-machine:/home/id# systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
```

### 3. Installation du tableau de bord Wazuh

- Installation des dépendances du package

```
root@id-virtual-machine:/home/id# apt-get install debhelper tar curl libcap2-bin #debhelper version 9 or later
```

- Installation du tableau de bord Wazuh

```
root@id-virtual-machine:/home/id# apt-get -y install wazuh-dashboard
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  wazuh-dashboard
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 179 MB of archives.
After this operation, 965 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-dashboard amd64 4.7.4-1 [179 MB]
Fetched 179 MB in 21s (8,624 kB/s)
Selecting previously unselected package wazuh-dashboard.
(Reading database ... 234281 files and directories currently installed.)
Preparing to unpack .../wazuh-dashboard_4.7.4-1_amd64.deb ...
Creating wazuh-dashboard group... OK
Creating wazuh-dashboard user... OK
Unpacking wazuh-dashboard (4.7.4-1) ...
Setting up wazuh-dashboard (4.7.4-1) ...
```

- Configuration du tableau de bord Wazuh

Modifiez le `/etc/wazuh-dashboard/opensearch_dashboards.yml` fichier de configuration

```
root@id-virtual-machine:/home/id# nano /etc/wazuh-dashboard/opensearch_dashboards.yml
```

```
GNU nano 6.2                                     /etc/wazuh-dashboard/opensearch_dashboards.yml
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://localhost:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersAllowlist: ["securitytenant", "Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wazuh
```

Remplacez <DASHBOARD\_NODE\_NAME> par le nom de nœud de votre tableau de bord Wazuh, le même que celui utilisé config.yml pour créer les certificats, et déplacez les certificats vers leur emplacement correspondant

```
root@id-virtual-machine:/home/id# NODE_NAME=dashboard
```

```
root@id-virtual-machine:/home/id# mkdir /etc/wazuh-dashboard/certs
root@id-virtual-machine:/home/id# tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./${NODE_NAME}.pem ./${NODE_NAME}-key.pem ./root-ca.pem
root@id-virtual-machine:/home/id# mv -n /etc/wazuh-dashboard/certs/${NODE_NAME}.pem /etc/wazuh-dashboard/certs/dashboard.pem
root@id-virtual-machine:/home/id# mv -n /etc/wazuh-dashboard/certs/${NODE_NAME}-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
root@id-virtual-machine:/home/id# chmod 500 /etc/wazuh-dashboard/certs
root@id-virtual-machine:/home/id# chmod 400 /etc/wazuh-dashboard/certs/*
root@id-virtual-machine:/home/id# chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

## Démarrage du service de tableau de bord Wazuh

```
root@id-virtual-machine:/home/id# systemctl daemon-reload
root@id-virtual-machine:/home/id# systemctl start wazuh-dashboard
root@id-virtual-machine:/home/id# systemctl enable wazuh-dashboard
```

L'interface d'accueil de Wazuh se présente comme suit :

The screenshot shows a browser window with the URL <https://10.0.0.10>. A red warning triangle icon is displayed at the top left. Below it, a message reads: "Votre connexion n'est pas privée. Des individus malveillants tentent peut-être de subtiliser vos informations personnelles sur le site 10.0.0.10 (mots de passe, messages ou numéros de carte de crédit, par exemple). En savoir plus". A note below says: "Pour bénéficier du niveau de sécurité le plus élevé de Chrome, activez la protection renforcée". At the bottom, there are two buttons: "Permettre l'accès" and "Revenir en toute sécurité".

WAZUH

Total agents	Active agents	Disconnected agents	Never connected agents
0	0	0	0

No agents were added to this manager. Add agent

**SECURITY INFORMATION MANAGEMENT**

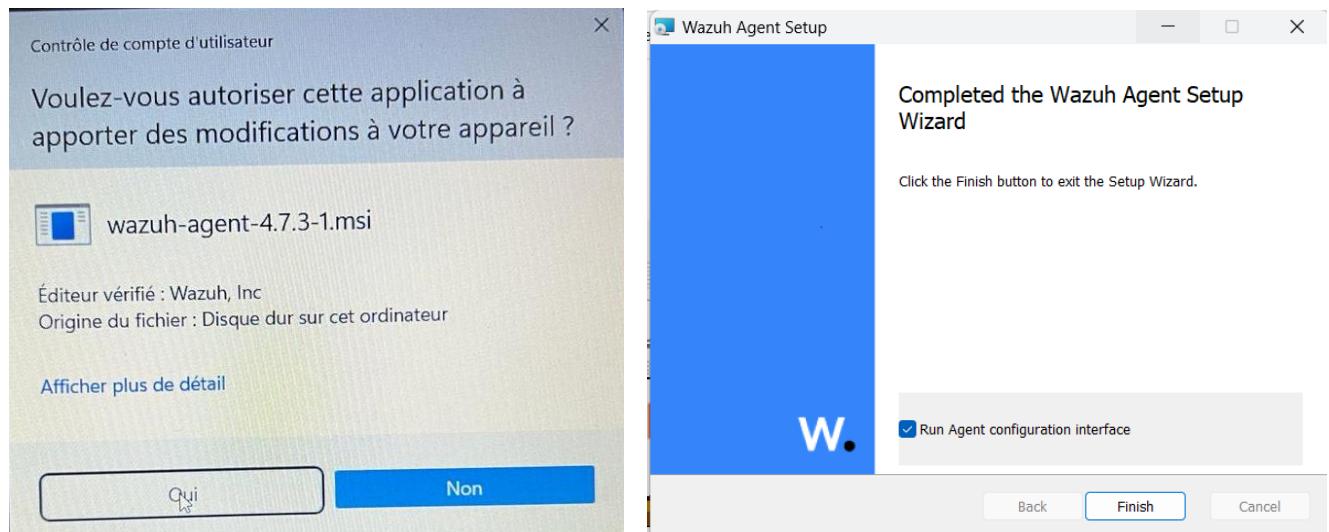
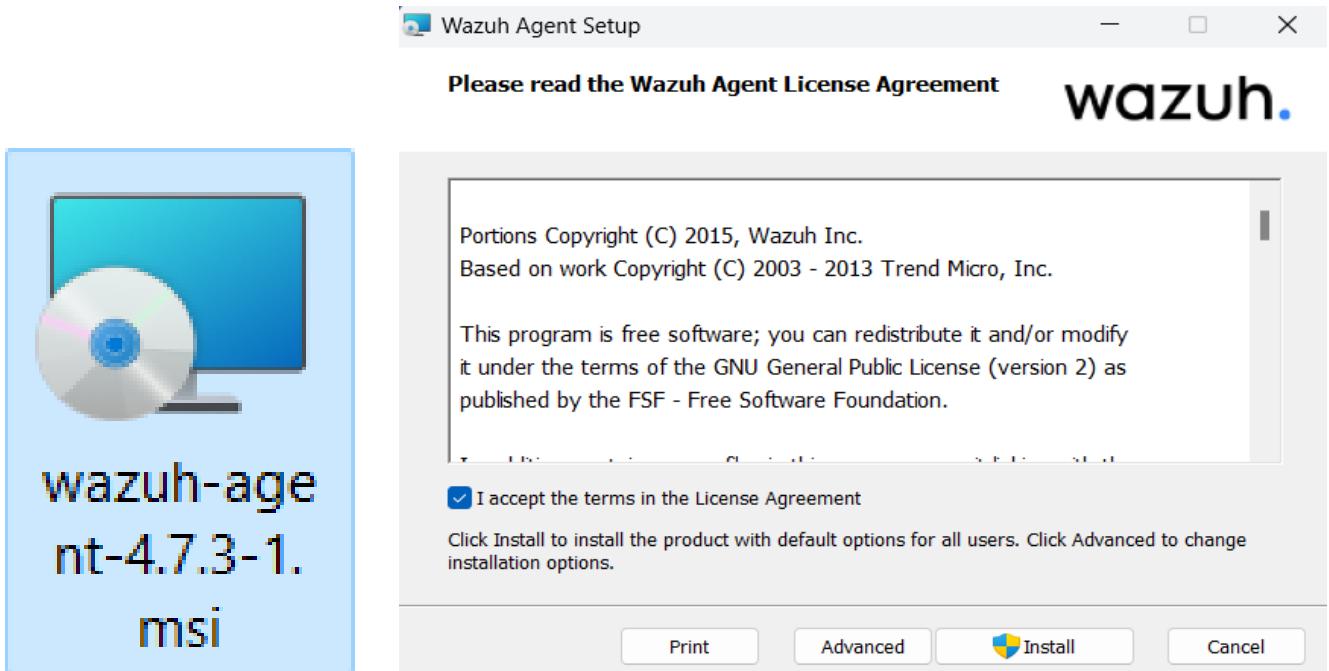
- Security events: Browse through your security alerts, identifying issues and
- Integrity monitoring: Alerts related to file changes, including permissions, content.

**AUDITING AND POLICY MONITORING**

- Policy monitoring: Verify that your systems are configured according to your
- System auditing: Audit users behavior, monitoring command

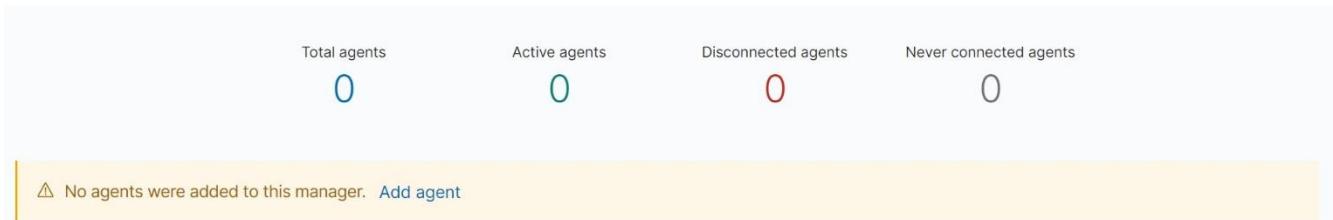
## II\ Déploiement d'un agent Wazuh

### 1. Installation de Wazuh agent



## 2. Intégration des agents à superviser

Pour initier la surveillance et la supervision de nos machines, il suffit d'ajouter la machine cliente en tant qu'agent.



- ✓ Déployer un nouvel agent graphiquement

### Déployer un nouvel agent

#### Sélectionnez le package à télécharger et à installer sur votre système :

<b>Linux</b>  <input type="radio"/> Régime amd64 <input type="radio"/> RPM aarch64 <input type="radio"/> DEBamd64 <input type="radio"/> DEB aarch64	<b>LES FENÊTRES</b>  <input checked="" type="radio"/> MSI 32/64 bits	<b>macOS</b>  <input type="radio"/> Intel <input type="radio"/> Silicium de pomme
--	--	---

ⓘ Pour des systèmes et architectures supplémentaires, veuillez consulter notre documentation [🔗](#).

#### Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address: [?](#)

10.0.0.19

#### Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: [?](#)

POSTE-1

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled. [🔗](#)

Select one or more existing groups: [?](#)

default [X](#)



Complétons les étapes, en exécutant notre script sur notre client Windows

**4 Run the following commands to download and install the agent:**

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile $env:tmp\wazuh-agent; msieexec.exe /i $env:tmp\wazuh-agent.msi /quiet WAZUH_MANAGER='10.0.0.19' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='POSTE-1' WAZUH_REGISTRATION_SERVER='10.0.0.19'
```

**① Requirements**

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

**5 Start the agent:**

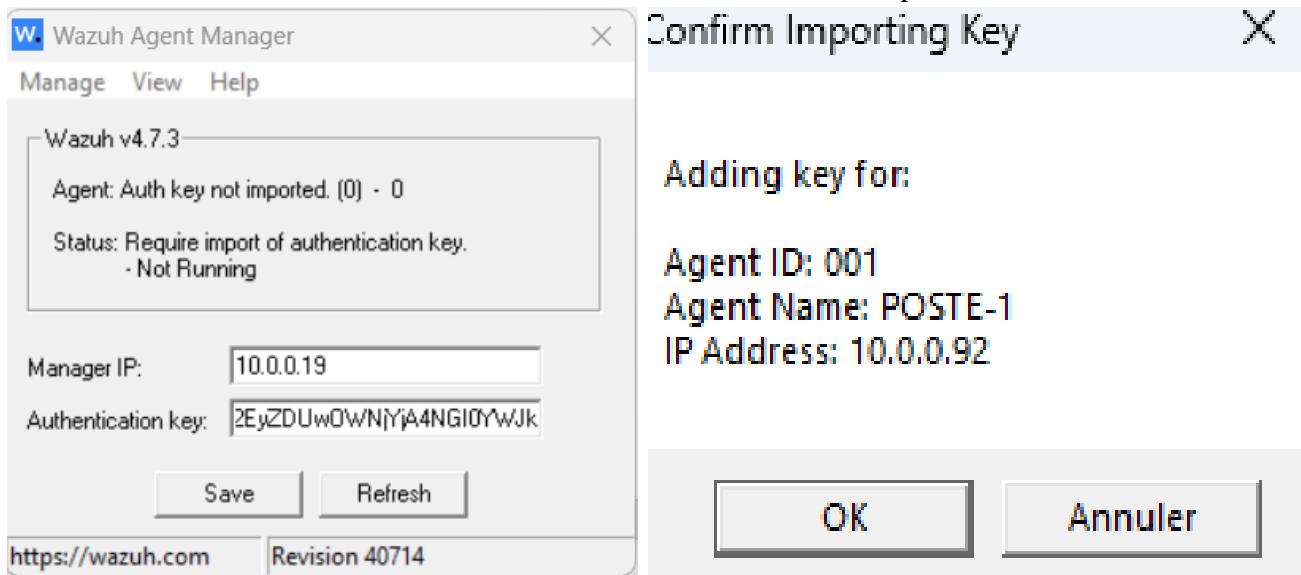
```
NET START WazuhSvc
```

**Close**

Pour démarer l'agent wazuh on va extraire un clé

```
*****
* Wazuh v4.7.4 Agent manager.          *
* The following options are available: *
*****  
(A)dd an agent (A).  
(E)xtract key for an agent (E).  
(L)ist already added agents (L).  
(R)emove an agent (R).  
(Q)uit.  
Choose your action: A,E,L,R or Q: E  
  
Available agents:  
ID: 001, Name: POSTE-1, IP: 10.0.0.92  
Provide the ID of the agent to extract the key (or '\q' to quit): 001  
  
Agent key information for '001' is:  
MDAxIFBU1RFLTEgMTAuMC4wLjkyIDM3MzFkZWI3NmJiZmY0OTM3Y2ZmNjkxNlM5MDMwMmVjZWY4Nzhj  
ZmQ2NjIwMWRiZjQ1NzgxMDc2ODI5MTdhOTQ=
```

Entrer l'add IP de serveur wazuh et le clé d'authentification et cliquer sur 'Save'



✓ Déployer un nouvel agent par commande

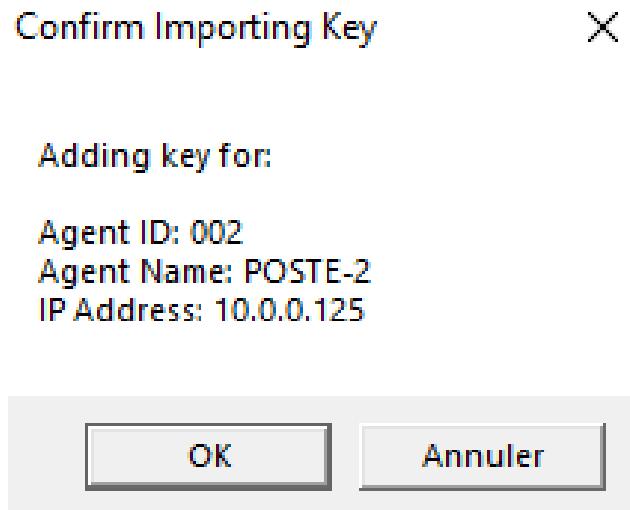
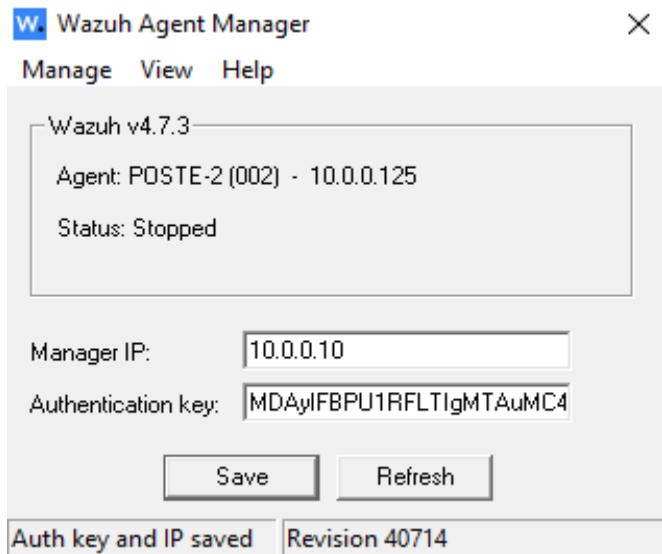
Exécuté 'manage\_agents' pour ajouter un agent Wazuh

```
root@id-virtual-machine:/# cd /var/ossec/bin/
root@id-virtual-machine:/var/ossec/bin# ls
agent_control      wazuh-agentlessd  wazuh-dbd          wazuh-monitord
agent_groups       wazuh-analysisd   wazuh-execd        wazuh-regex
agent_upgrade      wazuh-apid        wazuh-integratord  wazuh-remoted
clear_stats        wazuh-authd       wazuh-logcollector wazuh-reportd
cluster_control    wazuh-clusterd   wazuh-logtest      wazuh-syscheckd
manage_agents      wazuh-control     wazuh-logtest-legacy
rbac_control       wazuh-csyslogd   wazuh-maild
verify-agent-conf  wazuh-db         wazuh-modulesd
root@id-virtual-machine:/var/ossec/bin# ./manage_agents
*****
* Wazuh v4.7.4 Agent manager.
* The following options are available:
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: A
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
 * A name for the new agent: POSTE-2
 * The IP Address of the new agent: 10.0.0.125
Confirm adding it?(y/n): y
Agent added with ID 002.
```

Extrait la clé pour démarrer l'agent Wazuh

```
*****
* Wazuh v4.7.4 Agent manager.          *
* The following options are available: *
*****  
(A)dd an agent (A).  
(E)xtract key for an agent (E).  
(L)ist already added agents (L).  
(R)emove an agent (R).  
(Q)uit.  
Choose your action: A,E,L,R or Q: E  
  
Available agents:  
ID: 001, Name: POSTE-1, IP: 10.0.0.92  
ID: 002, Name: POSTE-2, IP: 10.0.0.125  
Provide the ID of the agent to extract the key (or '\q' to quit): 002  
  
Agent key information for '002' is:  
MDAyIFBPU1RFLTigMTAuMC4wLjEyNSBmZTk5NzQzNjhkNzA5Zjk1YmY1ZWVjNjU1NzNkYzc0NzZlZGYy  
MjUyYWQ1MmNmNkM2EyZDUwOWNjYjA4NGI0YWJk  
  
** Press ENTER to return to the main menu.
```

Entrer l'add IP de serveur wazuh et le clé d'authentification et cliquer sur 'Save'



### 3. Création de groupe agents

- Le tableau de bord Wazuh

Accédez à **Gestion > Groupes** et cliquez sur le bouton **Ajouter un nouveau groupe**

wazuh. ^ Modules

Modules

Gestion >

Agents

Outils

Sécurité

Paramètres

Annuaire de gestion

Administration

Règles

Décodeurs

Listes CDB

Groupes

Configuration

Statut et rapports

Statut

Grappe

Statistiques

Journaux

Rapports

Groupes ( 4 )

De là, vous pouvez lister et vérifier vos groupes, leurs agents et leurs fichiers.

Ajouter un nouveau groupe Rafraîchir Exporter formaté

Nom ↑	Agents	Somme de contrôle de configuration	Actions
défault	13	ab73af41699f13fd81903b5f23d8d00	🕒 🖊️ 🗑️

Présenter le nom du groupe

Windows

Enregistrer un nouveau groupe

## ➤ L'outil agent\_groups

Pour créer un compte, on exécute la commande suivante :

```
/var/ossec/bin/agent_groups -a -g <GROUP_ID> -q
```

Le paramètre `-a` ajoute un groupe ou un agent. Dans ce cas, un groupe.

Le paramètre `-g` définit un identifiant de groupe.

La variable `<GROUP_ID>` indique un nom de groupe unique à créer.

Le paramètre `-q` déclenche le mode silencieux ou sans confirmation.

```
root@id-virtual-machine:/home/id# /var/ossec/bin/agent_groups -a -g Linux -q
Group 'Linux' created.
root@id-virtual-machine:/home/id# █
```

Pour vous assurer que les groupes sont créés correctement, exécutez la commande suivante :

```
/var/ossec/bin/agent_groups -l
```

```
root@id-virtual-machine:/home/id# /var/ossec/bin/agent_groups -l
Groups (4):
  Linux (0)
  Windows (0)
  default (13)
  firewalls (0)
Unassigned agents: 0. █
```

## 4. Ajouter des agents Wazuh aux groupes

### ➤ Le tableau de bord Wazuh

Accédez à **Gestion > Groupes** et sélectionnez le groupe auquel vous souhaitez ajouter des agents.

Name	Agents	Configuration checksum	Actions
default	13	ab73af41699f13fd81903b5f23d8d00	
firewalls	0	ab73af41699f13fd81903b5f23d8d00	
Linux	0	ab73af41699f13fd81903b5f23d8d00	
Windows	0	ab73af41699f13fd81903b5f23d8d00	

Cliquez sur le bouton **Gérer les agents** dans le coin supérieur droit.

ID	Name	IP address	Operating system	Version	Status	Actions
No items found						

Sélectionner le ou les agents à ajouter, cliquer sur **Ajouter les éléments sélectionnés**, puis cliquez sur **Appliquer les modifications** pour enregistrer les modifications.

Available agents		Current agents in the group (0)	
<input type="text" value="Filter..."/>		<input type="text" value="Filter..."/>	
008 - VM-Ubuntu		001 - POSTE-1 002 - POSTE-2 003 - POSTE-3 004 - POSTE-4 005 - POSTE-5 006 - POSTE-6 007 - POSTE-7 009 - DESKTOP-QKE24AP 010 - Windows-10 012 - Win-10 013 - DESKTOP-EU4A3MA 014 - Agent-Wazuh	

## ➤ L'outil agent\_groups

Pour ajouter des agents à un groupe d'agents, on utilise la commande suivante :

```
/var/ossec/bin/agent_groups -a -i <AGENT_ID> -g <GROUP_ID> -q
```

Le paramètre **-a** ajoute un groupe ou un agent. Dans ce cas, un agent.

Le paramètre **-i** définit un ID d'agent.

La variable **<AGENT\_ID>** indique l'ID de l'agent à ajouter à un groupe.

Le paramètre **-g** définit un identifiant de groupe.

La variable **<GROUP\_ID>** indique un nom de groupe unique à créer.

Le paramètre **-q** déclenche le mode silencieux ou sans confirmation.

```
root@id-virtual-machine:/home/id# /var/ossec/bin/agent_groups -a -i 008 -g Linux
-q
Group 'Linux' added to agent '008'.
```

Affichez la liste des groupes avec le nombre d'agents affectés pour vous assurer que chaque groupe dispose du nombre correct d'agents :

```
root@id-virtual-machine:/home/id# /var/ossec/bin/agent_groups -l
Groups (4):
  Linux (1)
  Windows (12)
  default (13)
  firewalls (0)
Unassigned agents: 0.
```

## 5. Supprimer les agents Wazuh des groupes

- Le tableau de bord Wazuh

Accédez à **Gestion > Groupes** et sélectionnez le groupe dont vous souhaitez supprimer les agents.

The screenshot shows the Wazuh management interface. On the left, there's a sidebar with 'Modules', 'Management' (highlighted with a red box), 'Agents', 'Tools', 'Security', and 'Settings'. The main area has a 'Management directory' header. Under 'Management', there are links for 'Administration' (Rules, Decoders, CDB lists, Groups, Configuration), 'Status and reports' (Status, Cluster, Statistics, Logs, Reporting), and a 'Management' link pointing back to the sidebar. The 'Groups' link under 'Management' is also highlighted with a red box.

The screenshot shows the 'Groups' page with 4 entries. The columns are 'Name', 'Agents', 'Configuration checksum', and 'Actions'. The 'Actions' column contains icons for 'Edit' and 'Delete'. The groups listed are: default (13 agents, configuration checksum ab73af41699f13fdd81903b5f23d8d00), firewalls (0 agents, configuration checksum ab73af41699f13fdd81903b5f23d8d00), Linux (1 agent, configuration checksum ab73af41699f13fdd81903b5f23d8d00), and Windows (12 agents, configuration checksum ab73af41699f13fdd81903b5f23d8d00). There are buttons for 'Add new group', 'Refresh', and 'Export formatted' at the top right. A search bar and a 'WQL' button are at the bottom right. A note says 'From here you can list and check your groups, its agents and files.'

Cliquez sur le bouton **Supprimer** à droite de l'agent que vous souhaitez supprimer, puis cliquez sur Confirmer pour **confirmer** la suppression de l'agent.

The screenshot shows the Wazuh Management interface with the 'Agents' tab selected. A list of 12 agents is displayed in a table. The columns are: Id, Name, IP address, Operating system, Version, Status, and Actions. The 'Actions' column contains icons for each agent, including a delete icon. The agent 'DESKTOP-EU4A3MA' is highlighted with a red box around its delete icon.

Id	Name	IP address	Operating system	Version	Status	Actions
001	POSTE-1	10.0.0.92	Microsoft Windows 11 Enterprise 10.0.22631.3447	v4.7.3	● disconnected ⓘ	
002	POSTE-2	10.0.0.125	Microsoft Windows 10 Pro 10.0.19045.4291	v4.7.3	● disconnected ⓘ	
003	POSTE-3	10.0.0.28	Microsoft Windows 11 Enterprise 10.0.22631.3447	v4.7.4	● disconnected ⓘ	
004	POSTE-4	10.0.0.11	Microsoft Windows 11 Enterprise 10.0.22631.3296	v4.7.3	● disconnected ⓘ	
005	POSTE-5	10.0.0.71	Microsoft Windows 11 Enterprise 10.0.22631.3447	v4.7.3	● disconnected ⓘ	
006	POSTE-6	10.0.0.25	Microsoft Windows 10 Pro 10.0.19045.4291	v4.7.3	● disconnected ⓘ	
007	POSTE-7	10.0.0.18	Microsoft Windows 11 Enterprise 10.0.22621.3007	v4.7.3	● disconnected ⓘ	
009	DESKTOP-OKE24AP	10.0.0.28	Microsoft Windows 11 Enterprise 10.0.22631.3447	v4.7.4	● disconnected ⓘ	
010	Windows-10	10.0.0.20	Microsoft Windows 10 Pro 10.0.17134.1	v4.7.4	● disconnected ⓘ	
012	Win-10	192.168.1.114	Microsoft Windows 10 Pro 10.0.17134.1	v4.7.4	● disconnected ⓘ	
013	DESKTOP-EU4A3MA	192.168.0.112	Microsoft Windows 10 Pro 10.0.17134.1	v4.7.4	● disconnected ⓘ	

Remove DESKTOP-EU4A3MA agent from this group?

Cancel

Confirm

## ➤ L'outil agent\_groups

Pour supprimer des agents d'un groupe, exécutez la commande suivante :

```
/var/ossec/bin/agent_groups -r -i <AGENT_ID> -g <GROUP_ID> -q
```

<AGENT\_ID> avec l'ID de l'agent que vous souhaitez supprimer.

<GROUP\_ID> avec le nom du groupe dont vous souhaitez supprimer l'agent.

```
root@id-virtual-machine:/home/id# /var/ossec/bin/agent_groups -r -i 009 -g Windows -q
Agent '009' removed from Windows.
```

L'agent wazuh a été supprimé du groupe Windows

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	POSTE-1	10.0.0.92	default Windows	Microsoft Windows 11 Enterprise 10.0.22631.3447	node01	v4.7.3	● disconnected ⓘ	🔗 🔍
002	POSTE-2	10.0.0.125	default Windows	Microsoft Windows 10 Pro 10.0.19045.4291	node01	v4.7.3	● disconnected ⓘ	🔗 🔍
003	POSTE-3	10.0.0.28	default Windows	Microsoft Windows 11 Enterprise 10.0.22631.3447	node01	v4.7.4	● disconnected ⓘ	🔗 🔍
004	POSTE-4	10.0.0.11	default Windows	Microsoft Windows 11 Enterprise 10.0.22631.3296	node01	v4.7.3	● disconnected ⓘ	🔗 🔍
005	POSTE-5	10.0.0.71	default Windows	Microsoft Windows 11 Enterprise 10.0.22631.3447	node01	v4.7.3	● disconnected ⓘ	🔗 🔍
006	POSTE-6	10.0.0.25	default Windows	Microsoft Windows 10 Pro 10.0.19045.4291	node01	v4.7.3	● disconnected ⓘ	🔗 🔍
007	POSTE-7	10.0.0.18	default Windows	Microsoft Windows 11 Enterprise 10.0.22621.3007	node01	v4.7.3	● disconnected ⓘ	🔗 🔍
008	VM-Ubuntu	10.0.0.2	default Linux	Ubuntu 22.04.4 LTS	node01	v4.7.4	● disconnected ⓘ	🔗 🔍
009	DESKTOP-QKE24AP	10.0.0.28	default	Microsoft Windows 11 Enterprise 10.0.22631.3447	node01	v4.7.4	● disconnected ⓘ	🔗 🔍
010	Windows-10	10.0.0.20	default Windows	Microsoft Windows 10 Pro 10.0.17134.1	node01	v4.7.4	● disconnected ⓘ	🔗 🔍

## 6. Détection de vulnérabilité

Voici le tableau de bord du serveur Wazuh

The dashboard displays the following information:

- Total agents: 13
- Active agents: 0
- Disconnected agents: 13
- Pending agents: 0
- Never connected agents: 0

Modules available:

- SECURITY INFORMATION MANAGEMENT**:
  - Security events: Browse through your security alerts, identifying issues and threats in your environment.
  - Integrity monitoring: Alerts related to file changes, including permissions, content, ownership and attributes.
- AUDITING AND POLICY MONITORING**:
  - Policy monitoring: Verify that your systems are configured according to your security policies baseline.
  - System auditing: Audit users behavior, monitoring command execution and alerting on access to critical files.
  - OpenSCAP: Configuration assessment and automation of compliance monitoring using SCAP checks.
  - CIS-CAT: Configuration assessment using Center of Internet Security scanner and SCAP checks.
  - Security configuration assessment: Scan your assets as part of a configuration assessment audit.
- THREAT DETECTION AND RESPONSE**:
  - Vulnérabilités (highlighted with a red box)
- REGULATORY COMPLIANCE**: None listed.

Faites défiler vers le bas et accédez à « DÉTECTION ET RÉPONSE DES MENACES » > Les options « Vulnérabilités » sont disponibles.

DÉTECTION ET RÉPONSE AUX MENACES

- Vulnérabilités**: Découvrez quelles applications de votre environnement sont affectées par des vulnérabilités bien connues.
- VirusTotal**: Alertes résultant de l'analyse VirusTotal des fichiers suspects via une intégration avec leur API.
- ATTAQUE À ONGLET&CK**: Événements de sécurité issus de la base de connaissances des tactiques et techniques adverses basées sur des observations du monde réel.

Nous devons maintenant configurer le scanner de vulnérabilités.  
Édit : fichier « nano /var/ossec/etc/ossec.conf ».

```
root@id-virtual-machine:/var/ossec/bin# nano /var/ossec/etc/ossec.conf
```

Voici dans « ossec.conf » regardez « l'inventeur du système », cette configuration est déjà là, nous ajouterons ces configurations à l'agent Windows « ossec.conf » plus tard

```
GNU nano 6.2          /var/ossec/etc/ossec.conf
</wodle>

<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>

  <!-- Database synchronization settings -->
  <synchronization>
    <max_eps>10</max_eps>
  </synchronization>
</wodle>
```



Maintenant, faites défiler vers le bas et voyez que le « détecteur de vulnérabilité » n'est pas activé. De plus, la configuration de certaines vulnérabilités du système d'exploitation est définie sur non activée.

```
GNU nano 6.2          /var/ossec/etc/ossec.conf
<skip_nfs>yes</skip_nfs>
</sca>

<vulnerability-detector>
  <enabled>no</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>no</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>
```



Nous devons activer la configuration comme indiqué dans la figure suivante

```
GNU nano 6.2          /var/ossec/etc/ossec.conf *
</sca>

<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
```

```
<!-- Windows OS vulnerabilities -->
<provider name="msu">
  <enabled>yes</enabled>
  <update_interval>1h</update_interval>
</provider>

<!-- Aggregate vulnerabilities -->
<provider name="nvd">
  <enabled>yes</enabled>
  <update_interval>1h</update_interval>
</provider>

</vulnerability-detector>
```

Nous devons maintenant activer l'option « Aggregate Vulnerabilities ». Lorsque vous activez cette option, la base de données des vulnérabilités commence à se télécharger après le redémarrage du gestionnaire wazuh.

```
GNU nano 6.2                               /var/ossec/etc/ossec.conf *

<!-- Ubuntu OS vulnerabilities -->
<provider name="canonical">
  <enabled>yes</enabled>
  <os>trusty</os>
  <os>xenial</os>
  <os>bionic</os>
  <os>focal</os>
  <os>jammy</os>
  <update_interval>1h</update_interval>
</provider>

<!-- Debian OS vulnerabilities -->
<provider name="debian">
  <enabled>yes</enabled>
  <os>buster</os>
  <os>bullseye</os>
  <os>bookworm</os>
  <update_interval>1h</update_interval>
</provider>
```

Redémarrez maintenant le gestionnaire wazuh

Commande : `systemctl restart wazuh-manager`

```
root@id-virtual-machine:/var/ossec/bin# systemctl restart wazuh-manager
root@id-virtual-machine:/var/ossec/bin# 
```

Vérifiez maintenant les journaux du fichier « ossec.log ».

Commande : `cat /var/ossec/logs/ossec.log`

```
root@id-virtual-machine:/home/id# cat /var/ossec/logs/ossec.log
2024/05/14 20:17:48 sca: INFO: Starting Security Configuration Assessment scan.
2024/05/14 20:17:48 wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Ubuntu Trusty' database update.
2024/05/14 20:17:48 wazuh-modulesd:syscollector: INFO: Module started.
2024/05/14 20:17:48 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2024/05/14 20:17:48 sca: INFO: Starting evaluation of policy: '/var/ossec/rules/etc/sca/cis_ubuntu22-04.yml'
2024/05/14 20:17:49 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2024/05/14 20:17:55 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2024/05/14 20:17:55 wazuh-syscheckd: INFO: FIM sync module started.
2024/05/14 20:17:58 sca: INFO: Evaluation finished for policy '/var/ossec/rules/etc/sca/cis_ubuntu22-04.yml'
2024/05/14 20:17:58 sca: INFO: Security Configuration Assessment scan finished.
Duration: 10 seconds.
2024/05/14 20:18:10 wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'Ubuntu Trusty' feed finished successfully.
2024/05/14 20:18:10 wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Ubuntu Xenial' database update.
```

Nous devons maintenant modifier la configuration de l'agent Windows « ossec.conf » : fichier ouvert wazuh-agent.

Meilleur résultat

W. Manage Agent Application

Rechercher sur le Web

- 🔍 a - Afficher plus de résultats de recherche >
- 🔍 Amazon - Entreprise américaine >
- 🔍 ameli >
- 🔍 airbnb >
- 🔍 ants >
- 🔍 anime sama >
- 🔍 aliexpress >

Allez maintenant dans View > View Config

W. Wazuh Agent Manager X

Manage View Help

Wazuh Agent: Status: Running

Manager IP: 192.168.1.113

Authentication key: MDE0IEFnZW50LVdhenVoIGFt

Save Refresh

Restarted | Revision 40717

Ajoutez ici la ligne de configuration suivante.

J'ajoute ici une ligne supplémentaire : <hotfixes>oui</hotfixes>

ossec.conf - Bloc-notes

Fichier Edition Format Affichage ?

```
<max_eps>10</max_eps>
</synchronization>
</syscheck>

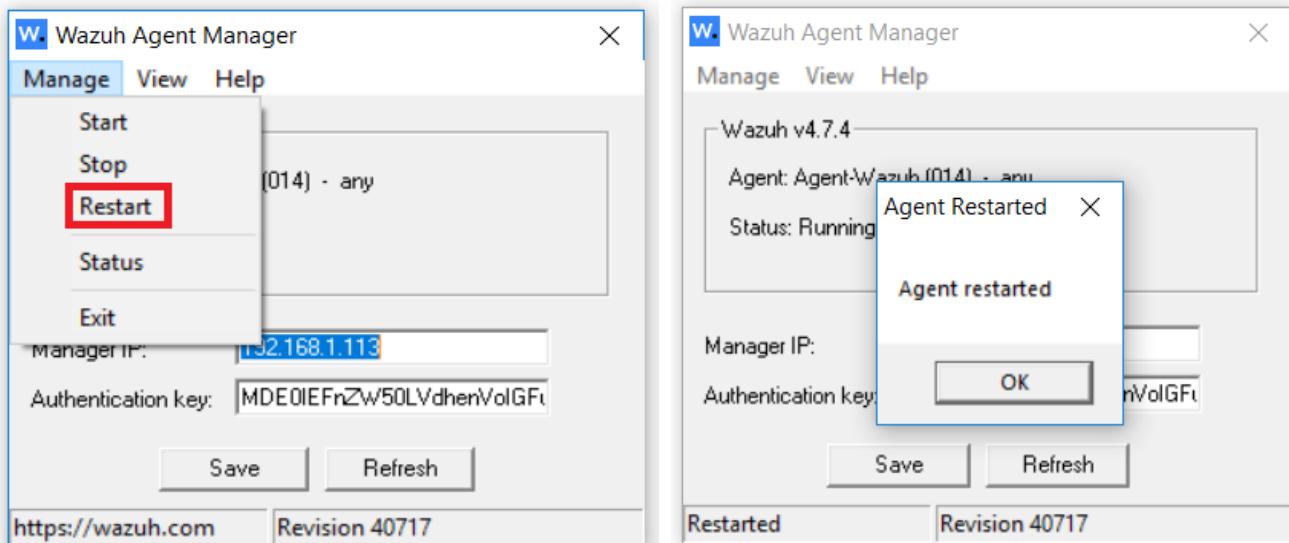
<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <hotfixes>yes</hotfixes>
  <ports all="no">yes</ports>
  <processes>yes</processes>

  <!-- Database synchronization settings -->
  <synchronization>
    <max_eps>10</max_eps>
  </synchronization>
</wodle>

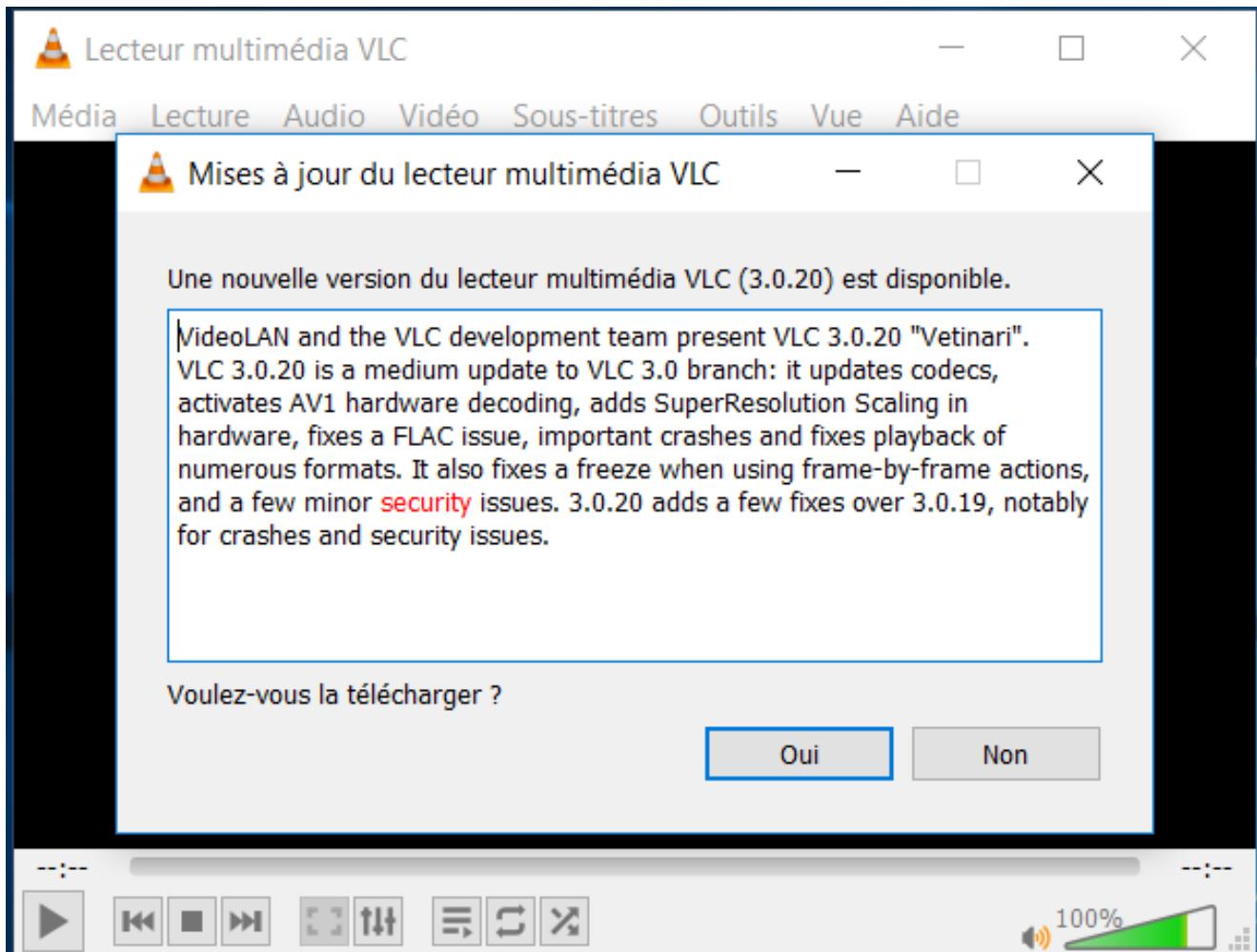
<!-- CIS policies evaluation -->
<wodle name="cis-cat">
  <disabled>yes</disabled>
  <timeout>1800</timeout>
  <interval>1d</interval>
  <scan-on-start>yes</scan-on-start>

  <java_path>\server\jre\bin\java.exe</java_path>
  <ciscat_path>C:\cis-cat</ciscat_path>
</wodle>
```

Après avoir ajouté la configuration, nous devons redémarrer wazuh agent.



Voici le lecteur multimédia VLC vulnérable installé sur ma machine Windows 10



Cliquez à nouveau sur « Vulnérabilités ».

**DÉTECTION ET RÉPONSE AUX MENACES**

**Vulnérabilités**

Découvrez quelles applications de votre environnement sont affectées par des vulnérabilités bien connues.

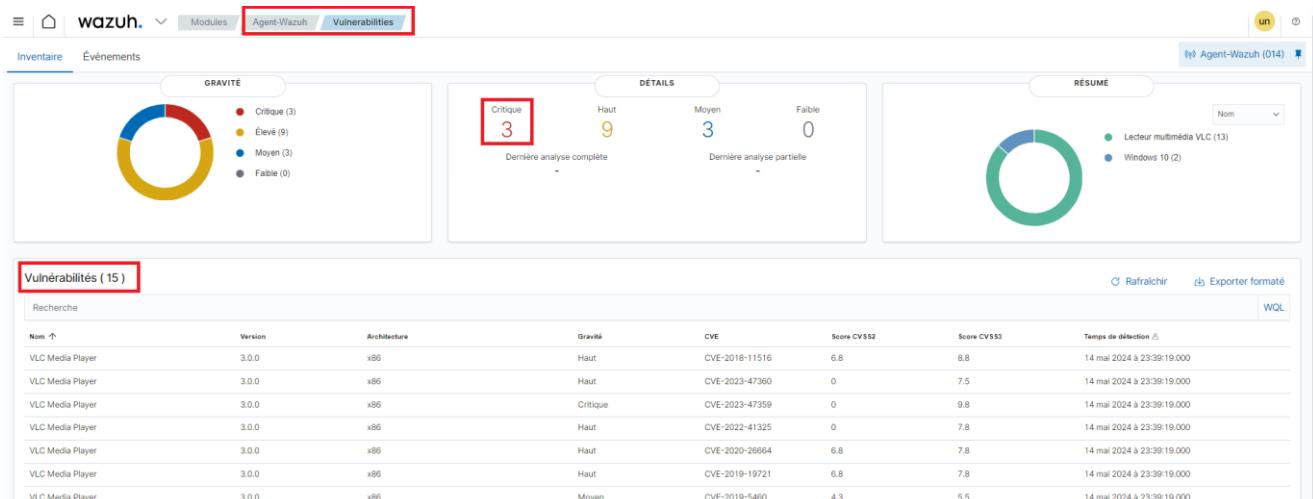
**VirusTotal**

Alertes résultant de l'analyse VirusTotal des fichiers suspects via une intégration avec leur API.

**ATTAQUE À ONGLET&CK**

Événements de sécurité issus de la base de connaissances des tactiques et techniques adverses basées sur des observations du monde réel

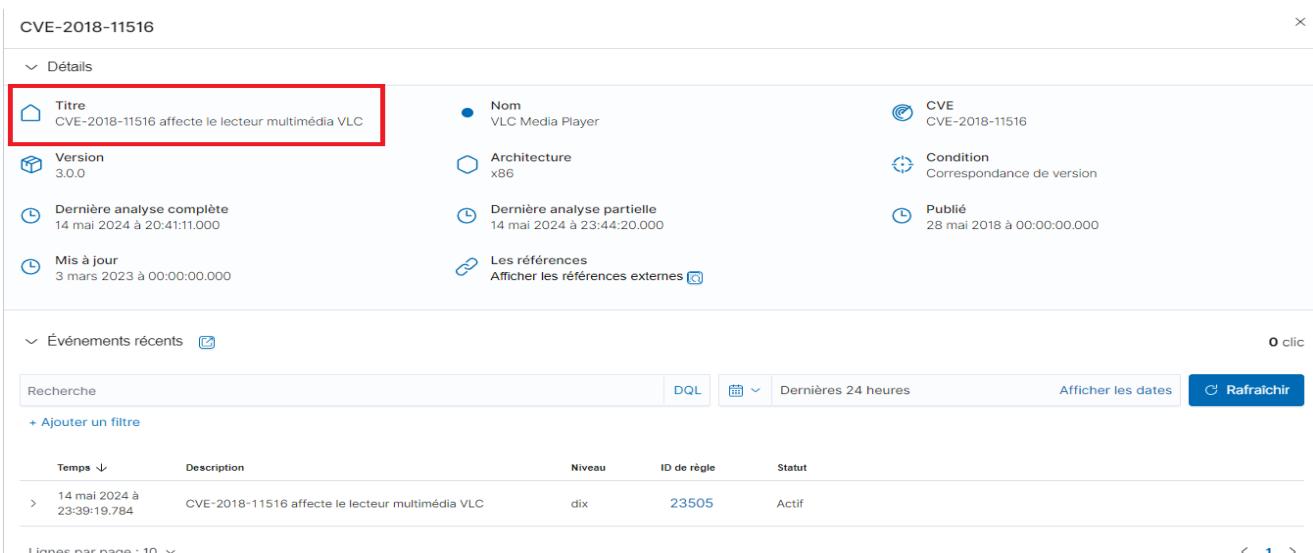
Cette vulnérabilité a été détectée !



The screenshot shows the Wazuh interface with the 'Vulnerabilities' tab selected. The main dashboard displays a donut chart for severity (Critique: 3, Élevé: 9, Moyen: 3, Fable: 0), a summary table for Agent-Wazuh (014) showing 13 VLC multimedia players and 2 Windows 10 hosts, and a detailed table of 15 vulnerabilities found in VLC Media Player. One specific vulnerability, CVE-2018-11516, is highlighted with a red box.

Nom	Version	Architecture	Gravité	CVE	Score CVSS2	Score CVSS3	Temps de détection
VLC Media Player	3.0.0	x86	Haut	CVE-2018-11516	6.8	8.8	14 mai 2024 à 23:39:19.000
VLC Media Player	3.0.0	x86	Haut	CVE-2023-47360	0	7.5	14 mai 2024 à 23:39:19.000
VLC Media Player	3.0.0	x86	Critique	CVE-2023-47359	0	9.8	14 mai 2024 à 23:39:19.000
VLC Media Player	3.0.0	x86	Haut	CVE-2022-41325	0	7.8	14 mai 2024 à 23:39:19.000
VLC Media Player	3.0.0	x86	Haut	CVE-2020-26664	6.8	7.8	14 mai 2024 à 23:39:19.000
VLC Media Player	3.0.0	x86	Haut	CVE-2019-19721	6.8	7.8	14 mai 2024 à 23:39:19.000
VLC Media Player	3.0.0	x86	Moyen	CVE-2019-5460	4.3	5.5	14 mai 2024 à 23:39:19.000

Voyons les détails de la vulnérabilité. Voici la vulnérabilité dans VLC Media Player



The screenshot shows the detailed view for CVE-2018-11516. It includes sections for 'Détails' (Title: CVE-2018-11516 affecte le lecteur multimédia VLC, Version: 3.0.0, Last full analysis: 14 mai 2024 20:41:11, Last partial analysis: 14 mai 2024 23:44:20, Last update: 3 mars 2023 00:00:00), 'Architecture' (x86), 'Condition' (Correspondance de version), and 'Publié' (28 mai 2018 00:00:00). Below this is a table of recent events and a footer with page navigation.

Temps	Description	Niveau	ID de règle	Statut
> 14 mai 2024 à 23:39:19.784	CVE-2018-11516 affecte le lecteur multimédia VLC	dix	23505	Actif

Nous avons 2 vulnérabilités majeures dans nos Windows 10.

The screenshot shows the Wazuh interface with the following details:

- Severity Distribution:** Critical (3), High (9), Medium (3), Low (0).
- Details:** Critical: 3, High: 9, Medium: 3, Low: 0. Last full scan: May 15, 2024 @ 17:01:02.000. Last partial scan: May 15, 2024 @ 17:26:34.000.
- Summary:** VLC media player (13), Windows 10 (2).
- Vulnerabilities (15):**

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
VLC media player	3.0.0	x86	High	CVE-2019-13602	6.8	7.8	May 14, 2024 @ 23:39:19.000
VLC media player	3.0.0	x86	Critical	CVE-2019-12874	7.5	9.8	May 14, 2024 @ 23:39:19.000
VLC media player	3.0.0	x86	Medium	CVE-2019-5439	4.3	6.5	May 14, 2024 @ 23:39:19.000
Windows 10	10.0.17134.1	x64	High	CVE-2018-8493	5	7.5	May 14, 2024 @ 20:41:11.000
Windows 10	10.0.17134.1	x64	High	CVE-2019-0841	7.2	7.8	May 14, 2024 @ 20:41:11.000

## Détails de la vulnérabilité de Windows 10.

The screenshot shows the Wazuh interface with the following details:

- Severity Distribution:** Critical (0), High (2), Medium (0), Low (0).
- Vulnerabilities (2):**

Name	Version	Architecture
Windows 10	10.0.17134.1	x64
Windows 10	10.0.17134.1	x64
- CVE-2018-8493 Details:**
  - Title:** CVE-2018-8493 affects Windows 10 (highlighted with a red box).
  - Version:** 10.0.17134.1
  - Last full scan:** May 14, 2024 @ 20:41:11.000
  - Updated:** Apr 1, 2024 @ 00:00:00.000
  - Name:** Windows 10
  - Architecture:** x64
  - Condition:** KB4462919 patch is not installed
  - Published:** Oct 10, 2018 @ 00:00:00.000
  - References:** View external references
- Recent events:**

Time	Description	Level	Rule ID	Status
May 14, 2024 @ 20:41:11.885	CVE-2018-8493 affects Windows 10	10	23505	Active

## Conclusion

En conclusion, l'intégration de Wazuh s'est avérée être un atout précieux pour la sécurité de l'établissement. La solution a permis d'accroître la visibilité, de détecter proactivement les menaces, d'accélérer la réponse aux incidents et de mieux répondre aux exigences de conformité. En poursuivant l'optimisation de la solution et en sensibilisant les utilisateurs, l'établissement peut maintenir une posture de sécurité robuste et se prémunir contre les menaces en constante évolution.