Projet d'intégration Rapport

SECS 1026

Rédigé par : Groupe 3 – Incident Watchers
Type de cours : En classe

Enseignant : KALLA, Christian Gilles
Établissement : Collège Communautaire du Nouveau-Brunswick (CCNB)

Table de contenu

Résumé 3

Aperçu du projet 4

Portée 7

Questions non réglées 8

Approbations 8

3 janvier – 19 février 9

20 février – 1 mars 15

9 mars – 15 mars 18

16 mars – 22 mars 19

24 mars – 28 mars 22

31 mars – 4 avril 23

Conclusion 25

Terminologie 26

Bibliographie 28

Résumé

Dans le cadre du cour SECS1026 Projet d'intégration en cybersécurité, toute la classe de deuxième année ont été séparé en groupe pour ensuite collaborer et créé un infrastructure réseaux complexe. Notre équipe (groupe 3) allons entreprendre un projet basé sur la surveillance et la gestion des incidents de cette infrastructure. Nous avons entrepris cette partie pour en apprendre plus sur les outils, la terminologie, les innovations et plus qui ont rapport à notre sujet. Ce travail va nous permettre d'intégrer des logiciels tel que Zabbix, Wazuh, Grafana et Prometheus. De plus, nous ferons la gestion des alertes et la mise en place de réponses aux incidents. Tous ces éléments formeront un système de surveillance pour l'infrastructure.

Les systèmes de surveillance sont un élément essentiel pour les entreprises car ils aident à répondre adéquatement aux incidents de manière proactive et réactive. Selon une publication du NIST (National Institute of Standards and Technologie) la surveillance consiste à maintenir une sensibilisation permanente de la sécurité de l'information, des vulnérabilités et des menaces afin de soutenir les décisions de gestion des risques de l'organisation. Pour être à jour avec la cybersécurité, une entreprise doit : Maintenir la connaissance de la situation de tous les systèmes dans l'ensemble de l'organisation ; Maintenir une compréhension des menaces et des activités de menace; Évaluer tous les contrôles de sécurité ; Collecter, corréler et analyser les informations relatives à la sécurité ; Fournir une communication exploitable sur l'état de la sécurité à tous les niveaux de l'organisation ; Maintenir une gestion active des risques par les responsables de l'organisation. La gestion des incidents consiste à repérer et à analyse les dangers et les risques pour mettre en œuvre des mesures d'atténuation et de contrôle efficaces afin de réduire les perturbations des opérations causées par les incidents, de réduire l'impact négatif et d'éviter leur réapparition. Nous devrons donc, implémenter des logiciels capables d'identifier et de nous alerter des vulnérabilités et des menaces de notre système pour ensuite les analysés et les géré de façon proactive. Notre projet aidera à attendre ces points pour atteindre l'objectif globale de la classe et de notre groupe.

Aperçu du projet

But

La gestion efficace des logs, associée à la détection d'anomalies, joue un rôle crucial dans la surveillance globale des équipements réseau et des serveurs. Ceux-ci forment un système de surveillance complet qui permet aux administrateurs système de maintenir une visibilité optimale sur l'état et sur les performances de l'infrastructure. En centralisant notamment, les logs et en les analysant de manière intelligente, il devient donc, possible de repérer rapidement les comportements inhabituels ou les problèmes potentiels. Cette approche proactive est renforcée par la visualisation des données systèmes, qui elles offrent une représentation graphique claire et intuitive de l'information collectées. Les graphiques dynamiques vont permettent de visualiser l'état actuel du système mais également, d'observer les tendances de performances au fil du temps. Ainsi, la combinaison de ces différents aspects de la surveillance informatique permet une gestion plus réactive et préventive, assurant une meilleur disponibilité et performance des services pour l'infrastructure.

Résultat voulu

Voici les résultats que nous recherchons concernant l'analyse et la gestion des systèmes :

1. Collecte de données sur le système pour faciliter son analyse.
2. Amélioration de la résilience et de la réactivité face aux anomalies détectées dans le système.
3. Interface avec tous les appareils réseau de l'architecture et outils pour les gérer.
4. Interface affichant le serveur et les outils pour sa gestion.
5. Grafana fournira un support visuel graphique pour visualiser les données du système.
6. Approche proactive pour surveiller les performances du système et les ressources nécessaires au fonctionnement du serveur et des systèmes.

Ces éléments contribuent à une gestion efficace et une surveillance proactive des systèmes informatiques, permettant d'améliorer la résilience, d'anticiper les problèmes et d'optimiser les performances.

Objectif

Gestion des logs et sécurité

L'implémentation des logs permet de suivre les actions effectuées sur le système par les utilisateurs. Cette pratique est cruciale pour la sécurité et notamment, pour l'audit, car celle-ci permet de retracer les activités suspectes et d'investiguer sur les incidents potentiels.

Détection des anomalies

La mise en place d'un système de détection d'anomalies permet d'identifier rapidement les comportements inhabituels ou les problèmes potentiels. Cette approche proactive améliore la sécurité et la fiabilité du système en permettant une réponse rapide au potentiel menace.

Surveillance des équipements réseau et des serveurs

L'extension de ce système de surveillance aux équipements réseau et aux serveurs offre une bonne visibilité sur l'ensemble du système. Cela permet de détecter plus efficacement les problèmes de performance ou de sécurité à tous les niveaux de l'architecture informatique de l'organisation.

Visualisation des données avec Grafana

Grafana joue un rôle clé dans la visualisation des données de l'infrastructure. Ses capacités de création de tableaux de bord interactifs et personnalisables facilitent grandement la compréhension et l'analyse des données collectées.

Surveillance des performances du système

La visualisation des performances du système, incluant l'utilisation du CPU, du GPU et d'autres ressources, est essentielle pour maintenir des opérations optimales. En combinant l'aspect visuel de Grafana a la surveillance système de Prometheus, l'infrastructure peut mettre en place un système de surveillance robuste et complet, capable de détecter rapidement les problèmes, d'améliorer la sécurité et d'optimiser les performances de l'ensemble du système informatique.

Wazuh

But	Objectif	Résultat
Gérer les logs	Implémenter les logs pour être en mesure de voir les actions qui sont effectuer sur le système par les utilisateurs	Données sur ce qui se passe sur notre système facilitant une analyse de celui-ci
Détecter les anomalies dans le système	Détecter rapidement les anomalies lier au système pour offrir une réponse rapide et une sécurité plus fiable	Amélioration de la résilience et de la réactivité au niveau des anomalies détecter dans le système

Zabbix

But	Objectif	Résultat
Surveillance des équipements réseaux	Implémenter ce système pour obtenir une meilleure visualisation au niveau des équipement réseau	Interface avec tous les appareils réseaux comprise dans l'Architecture et outils pour gérer ces tout ça
Surveillance des serveurs	Implémenter ce système pour obtenir une meilleure visualisation au niveau du serveur	Interface montrant le serveur et des outils pour gérer celui-ci

Grafana

But	Objectif	Résultat
Visualisation des données du système	Grafana aidera le système, à pouvoir visualiser les données de l'infrastructure qui facilite la compréhension	Grafana fourni un support visuel graphique pour visualiser les données du système

Prometheus

But	Objectif	Résultat
Visualisation des performances du système	Visualiser les performances du système comme le CPU, GPU etc...	Approche proactive au niveau des performances systèmes et des ressources nécessaires pour le fonctionnement du Serveur et des systèmes.

Portée

- Les critères d'acceptations sont : notre équipe doit, avant la fin du semestre, finir l'installation et la configuration de Zabbix, Wazuh, Grafana et Prometheus. Nous devons aussi établir une gestion des incidents efficace qui convient à toutes les parties prenantes.

- Le projet est limité à l'utilisation de logiciels open sources gratuit, la date limite du projet, les compétences de tous les parties prenantes et externe, la puissance des équipements, etc.

- Notre équipe devra lire et apprendre sur les logiciels utilisé (Zabbix, Wazuh, Grafana et Prometheus) et acquérir les compétences nécessaires.

- Nous devrons documenter chaque modification de nos documents et inclure : le nom de la personne qui modifie, la date et la raison de modification

- Pour déterminer la réussite de notre projet nous ferons des tests de fonctionnement et de fiabilité. Le produit final devra être fonctionnelle et complet.

Questions non réglées

Nous attendons l'installation du serveur de l'équipe numéro 1 pour commencer à installer nos systèmes de gestions des incidents et de surveillance de système. En effet, il nous faut un serveur configurer pour commencer à intégrer les applications. Nous n'avons pas encore lu la documentation des systèmes que nous devons installer donc, pour l'instant, nous ne savons pas comment les installer et les configurer.

Approbations

Les parties prenantes interne, donc les membres du groupe sont : Antoine Gallant, Justin Maltais Thibault, Mikael Lacroix. Les parties prenantes externes sont : M. Christian Kalla et certains membres d'autre équipe qui contribuerons au projet global du cour. Par exemple, les membres du groupe 1 qui s'occupe d'installer les serveurs que nous allons utiliser pour installer nos logiciels de surveillance.

3 janvier – 19 février

Lecture des documentations

Comme première étape de notre projet d'intégration, nous devons comprendre les logiciels choisis pour comprendre leur installation et leur fonctionnement. Voici un résumé de chaque logiciel.

Wazuh :

Overview : Wazuh offre une surveillance et une protection robustes de la sécurité des actifs informatiques grâce à ses capacités de gestion des informations et des événements de sécurité (SIEM) et de détection et de réponse étendues (XDR). Les cas d'utilisation de Wazuh sont conçus pour protéger vos actifs numériques et améliorer la posture de cybersécurité.

Installation : L'installation de Wazuh se fait en 3 étapes. Le Wazuh indexer est un moteur de recherche et d'analyse en texte intégral hautement évolutif. Ce composant central indexe et stocke les alertes générées par le serveur Wazuh. Le serveur Wazuh analyse les données reçues des agents et les traite à l'aide de renseignements sur les menaces. Un seul serveur peut analyser les données de milliers d'agents et s'adapter lorsqu'il est configuré en grappe. Il est également utilisé pour gérer les agents, en les configurant à distance si nécessaire. Le tableau de bord Wazuh est l'interface utilisateur web pour la visualisation, l'analyse et la gestion des données. Il comprend des tableaux de bord pour la conformité réglementaire, les vulnérabilités, l'intégrité des fichiers, l'évaluation de la configuration, les événements de l'infrastructure en nuage, entre autres. Pour installer les 3, il est possible de le faire de 2 façons. Le premier est l'installation complète step by step de chaque composant à l'aide de la documentions fourni par Wazuh, cette façon exige une compréhension globale de Wazuh et du système d'exploitation choisi pour faire l'installation. La deuxième est la plus simple, Wazuh offre une installation complète et automatique de chaque composant de Wazuh qui convient aux plus petits systèmes informatiques.

(https://documentation.wazuh.com/current/installation-guide/index.html)

Fonctionnement : Wazuh inclut la surveillance en temps réel, l'analyse des logs, la détection des vulnérabilités, la gestion de la conformité, et des capacités de réponse active pour automatiser les actions en cas de détection de menaces.

Zabbix :

Overview : Zabbix est un logiciel qui surveille de nombreux paramètres d'un réseau ainsi que la santé et l'intégrité des serveurs, des machines virtuelles, des applications, des services, des bases de données, des sites web, du nuage et bien plus encore. Zabbix utilise un mécanisme de notification flexible qui permet aux utilisateurs de configurer des alertes par courriel pour pratiquement n'importe quel événement. Cela permet de réagir rapidement aux problèmes de serveur. Zabbix offre d'excellentes fonctions de reporting et de visualisation des données basées sur les données stockées. Zabbix est donc idéal pour la planification de la capacité. Zabbix est divisé en 6 composants principaux. Le 1e est le serveur, c'est le composant central de l'application auquel chaque agents vont reporter. Toutes les configurations, statistique et donnée d'opération sont stocker dans celui-ci. Le stockage en base de données est le 2e composant toutes les informations traitées par zabbix sont stocker dans celui-ci. Pour les entreprises à grande échelle, il est préférable d'avoir un serveur dédié à la base de données de Zabbix. Le 3e est l'interface web pour faciliter l'accès à Zabbix à partir de n'importe où et de n'importe quelle plate-forme, l'interface web est fournie. L'interface fait partie du serveur Zabbix et tourne généralement (mais pas nécessairement) sur la même machine physique que celle qui exécute le serveur. Le 4e est le proxy, il peut collecter des données de performance et de disponibilité pour le serveur Zabbix. Un proxy est une partie optionnelle du déploiement de Zabbix ; cependant, il peut être très bénéfique pour répartir la charge d'un seul serveur Zabbix. Le 5e est les agents, ils sont déployés sur des cibles de surveillance pour surveiller activement les ressources et les applications locales et transmettre les données recueillies au serveur Zabbix. Le 6e est le dataflow, c'est l'ensemble des données qui traverse, qui sont créé et qui sont enregistrer dans Zabbix

Installation : L'installation de Zabbix est faite entièrement à l'aide de la documentation fournie sur le site web officiel. La documentation comprend 3 méthodes différentes l'installation à partir de la source, ce qui veut dire l'installation directement des fichiers d'installation de zabbix. L'installation par packages qui est plus simple, mais ne permet pas la manipulation complète de

l'installation. L'installation par container, tout comme l'installation par package, la manipulation complète de l'installation n'est pas possible, cependant les dockers offrent des interfaces simples pour la manipulation des fichiers de configuration.

(https://www.zabbix.com/documentation/current/en/manual/installation)

Fonctionnement : Tout comme Wazuh, Zabbix offre des services de surveillance en temps réel, des services d'alertes et notifications et des services de visualisation de données. Cependant, Zabbix n'est pas un SIEM. Wazuh se concentre sur la sécurité des systèmes tandis que Zabbix se concentre sur la surveillance des systèmes.

Prometheus/grafana :

Overview : Prometheus est un système de monitoring et d'alerte open-source qui collecte et stocke les métriques de performance. Grafana est un outil de visualisation et d'analyse de données qui peut se connecter à diverses sources de données, dont Prometheus. Ensemble, ils forment une solution puissante pour la surveillance et la visualisation des mesures de systèmes et applicatives. Pour maitriser Prometheus nous devons comprendre le langage de queries (PromQL) créé pour la manipulation de cette application. Le langage est très similaire au langage Go créé par google.

Installation : La documentation de Prometheus offre 3 méthodes similaires à Zabbix. Le 1^{e} est un utilisant des fichiers binaires pré-compliés, la 2^{e} est à partir de la source et la 3^{e} est en utilisant un docker. La plus efficace est à partir des fichiers binaires, car il permet la manipulation complète et custom de l'installation. Pour ajouter Grafana, il faut suivre les étapes données par la documentation Grafana.

(https://grafana.com/docs/grafana/latest/setup-grafana/installation/debian/)

(https://prometheus.io/docs/prometheus/latest/installation/)

Fonctionnement : Prometheus collecte les métriques à partir de cibles configurées à intervalles réguliers. Il stocke toutes les données recueillies localement et exécute des règles sur ces données pour agréger et enregistrer de nouvelles séries temporelles ou générer des alertes. Grafana permet de créer des tableaux de bord personnalisés en utilisant les données collectées

par Prometheus. Il offre une interface utilisateur intuitive pour la création de graphiques, de tableaux et d'alertes basés sur ces métriques. L'utilisation combinée de Prometheus et Grafana permet de visualiser les métriques de système et applicatives en temps réel, créer des tableaux de bord personnalisés pour différents besoins de surveillance, configurer des alertes basées sur des seuils prédéfinis et analyser les tendances de performance sur le long terme. Cette solution est particulièrement appréciée pour sa flexibilité, permettant de consolider plusieurs sources de données dans une seule interface de visualisation.

Installation des logiciels sur des machines virtuels

Pour faire un test d'installation des logiciels, nous avons écrit quelques hypothèses avant de débuter :

1. Est-ce que nous pouvons installer tous les logiciels sur la même machine virtuelle et les faire fonctionner simultanément?

   Réponse : Oui, nous avons réussi à tout installé les logiciels simultanément. Ils fonctionnent bien ensemble, car ils ont des ports différents par défaut.

   Wazuh https://localhost:443

   Zabbix http://localhost/zabbix (port 80)

   Grafana http://localhost:3000/

   Prometheus http://localhost:9090/

2. Est-ce que l'installation "Quick Start" de Wazuh nous convient même si nous avons moins de contrôle sur l'installation globale des 3 composants principaux?

   Réponse : Oui, l'installation "Quick Start" de Wazuh nous convient, car nous installons seulement 1 serveur Wazuh. Si nous avions plusieurs serveurs principaux, nous aurions eu à installer manuellement l'indexer.

3. Est-ce que Zabbix et Wazuh vont interférer entre eux si on installe leurs agents sur la même machine client?

   Réponse : Non, nous n'avons eu aucun problème à installer les 2 agents sur la même machine. Wazuh se préoccupe de la santé et de la sécurité de la machine tandis que Zabbix surveille la machine.

4. Quel type d'installation devons-nous choisir pour chacun des logiciels?

   Réponse : Wazuh = "Quick Start", Zabbix= de la source et Prometheus= à partir des fichiers binaires précompilé.

Formation Prometheus (Antoine)

En attente de l'installation du serveur, j'ai décidé d'approfondir mes connaissances sur les logiciels que nous devons installer. J'ai donc suivi la formation LinkedIn Learning "Formation Prometheus Essential" de Opeyemi Onikute. Voici quelque point important que j'ai appris pendant cette formation :

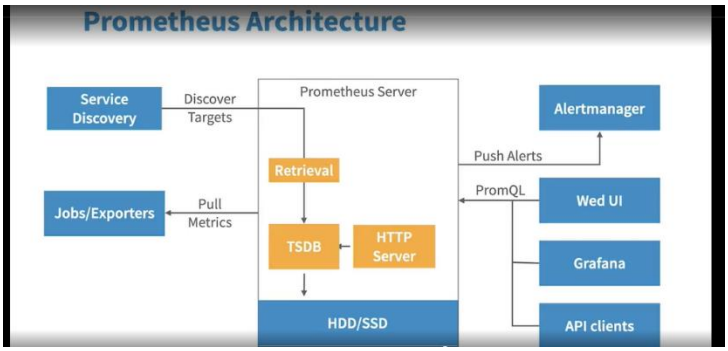
- Pour comprendre Prometheus, il faut comprendre ce qu'est le monitoring et observabilité. Le monitoring est la surveillance de tout ou certains aspects des systèmes et réseaux, dans le cas de Prometheus ce sont les performances des systèmes. Pour l'observabilité, les 3 piliers principaux sont les logs(journaux), les mesures de performance et la traçabilité.

- Vous ne devez pas utiliser Prometheus si vous voulez des mesures 100% exacts. Il faut noter que les données traitées ne sont pas entièrement précises.
- Quelques fonctions utiles pour PromQL (langage de queries créé pour Prometheus) : label_replace pour la manipulation des labels ; sum(), avg(), max (), min (), sum without(), avg_over_time() pour les calculs ; rate () et increase() pour les taux.
- Prometheus inclut une api, les end points sont : GET /api/v1/query et POST /api/v1/query. L'API à des réponses en JSON, peut faire des queries pour des mesures et peut écrire de nouvelles

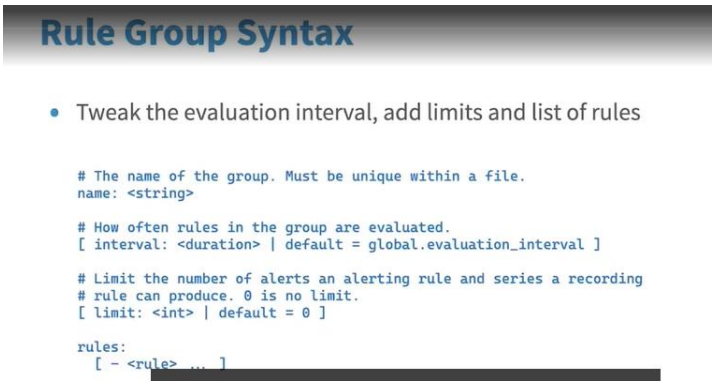
mesures. Les paramètre URL les plus important sont : query=<string>, time=<rfc3339 | unix_timestamp> et timeout=<duration>.

- Les meilleures pratiques pour utiliser Prometheus sont : commencez simplement, utilisez les fonctions PromQL, utilisez un filtrage approprié des labels, n'abusez pas des regex, pensez aux performances, surveillez Prometheus et utilisez PromLense pour améliorer vos requêtes. PromLense aide à créer, analysé et troubleshoot les queries.
- Les noms des mesures devraient seulement inclure des lettres et des underscores. Ils devraient avoir un préfixe qui décrit le service que correspond à la mesure et un suffixe qui décrit la mesure. EX : http_nomdelamesure_bytes.
- Une librairie Python peut être installée pour créer des scripts d'automatisation.
- Prometheus peut être lié à une base que donné tel que MySQL et MongoDB.
- On peut faire le service discovery avec Prometheus.

L'architecture de Prometheus

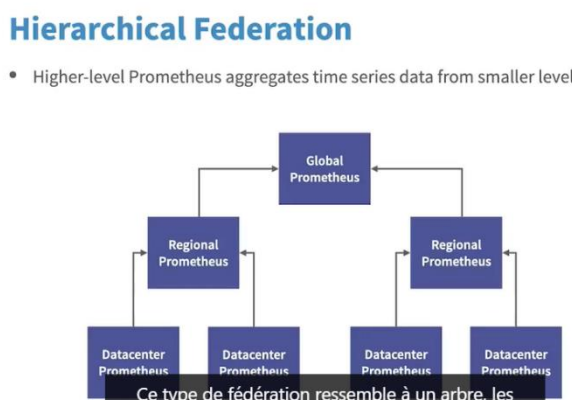


La syntaxe pour les groupes de règles



La syntaxe pour les règles d'alertes

La hiérarchie pour la fédération de Prometheus



20 février – 1 mars

Configuration des alertes de Wazuh à travers de courriel (règles d'alertes)

Pour créer des alertes courriel pour Wazuh il faut seulement un adresse électronique dédier aux alertes et suivre la documentation de Wazuh suivante : https://wazuh.com/blog/how-to-send-email-notifications-with-wazuh/. Nous avons créé le courriel à travers de google. Une fois le courriel créé, nous avons installé un serveur smtp pour être capable d'envoyer des courriels à travers de notre serveur. Ensuite, sur le fichier de configuration ossec de wazuh, nous avons ajouté les lignes suivantes pour configurer les alertes.

<ossec_config>

<global>

<email_notification>yes</email_notification> activation des notifications par couriel

<smtp_server>localhost</smtp_server> addresse du serveur smtp, dans notre cas localhost

<email_from> cyse2alerts@gmail.com </email_from> Le email qui envoi les notifications

<email_to> cyse2alerts@gmail.com </email_to> Le email qui reçois les notifications

<email_maxperhour>100</email_maxperhour> Le maximum de email par heure

</global>

<alerts>

<email_alert_level>9</email_alert_level> Le niveau minimum des alertes envoyer par wazuh

</alerts>

</ossec_config>

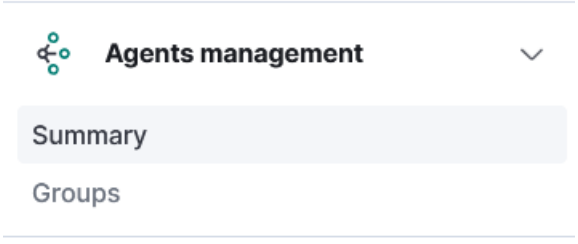
Installation des logiciels sur le serveur

Migration d'une machine virtuelle ayant comme application web Wazuh, Zabbix, Grafana ainsi que, Prometheus. Lors de la migration plusieurs problème fut rencontrer notamment en raison du manque de budget au niveau serveur. Par la suite, nous avons rencontré un problème au niveau de l'adresse ip avec le paramètre DHCP. Pour régler ce problème, nous avons suit la documentation de ubuntu server. Lorsque ce problème fut supprimé nous avons pu conclure l'installation et la configuration de notre machine virtuelle.

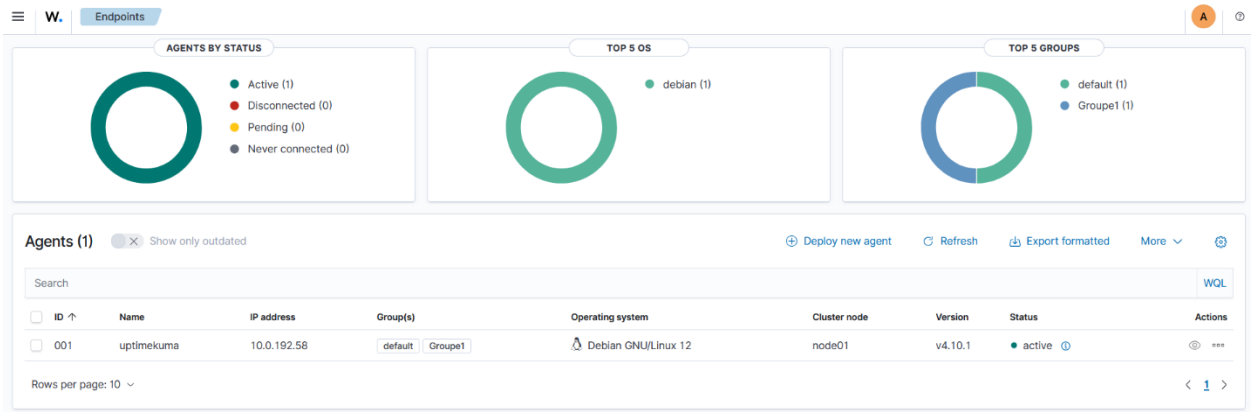
Installation d'agents wazuh et Zabbix

Wazuh:

Pour installer les agents Wazuh, il faut se rendre sur l'onglet "Agent management" et ensuite "Summary".



Ensuite clicker sur "Deploy new agents"



Ensuite, wazuh offre une interface avec des étapes simple pour installer les paquets nécessaires sur la machine voulue. Dans notre cas nous l'avons installé sur la machine Kuma et somme en train d'attendre pour l'accès aux autres machines.

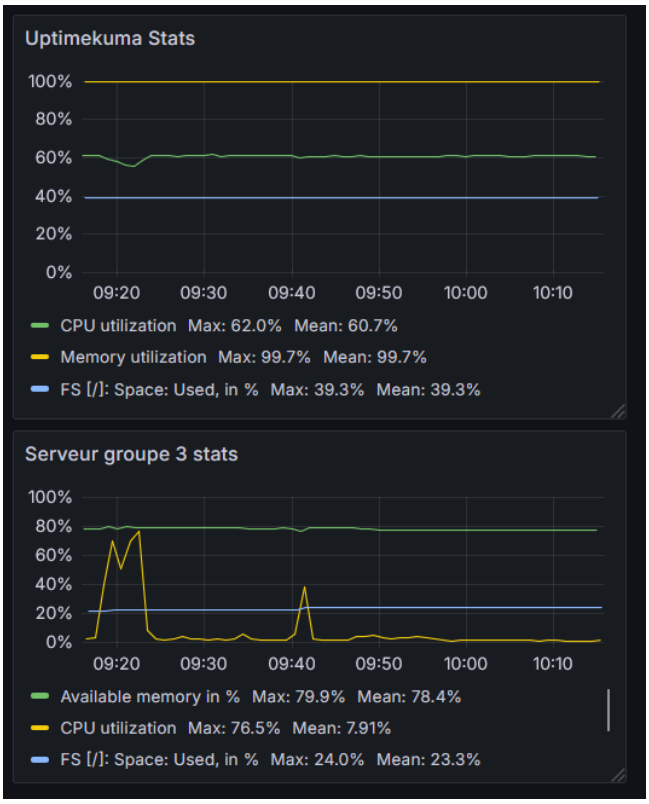
Zabbix :

Sur Zabbix, les agents sont nommés Hosts. Pour les installer, nous devons suivre les étapes données par la documentation Zabbix : https://www.zabbix.com/download_agents. Ensuite, aller sur Zabbix et aller dans la section Monitoring et ensuite Host.

Il faut ensuite clicker sur "Create Host" et remplir des informations nécessaires.

Affichage des données Zabbix avec grafana

Pour afficher les données de chaque agent Zabbix sur Grafana, nous avons installé un plugin pour créer une connexion entre les 2 logiciels. Une fois la connexion créée, il faut créer un Dashboard pour visualiser les données envoyer par Zabbix, nous avons donc créé un tableau par agent qui affiche les pourcentages d'utilisation du CPU, de la mémoire vive et de l'espace de stockage. Pour chaque ensemble de donnée, la légende affiche le % maximum et la moyenne d'utilisation.



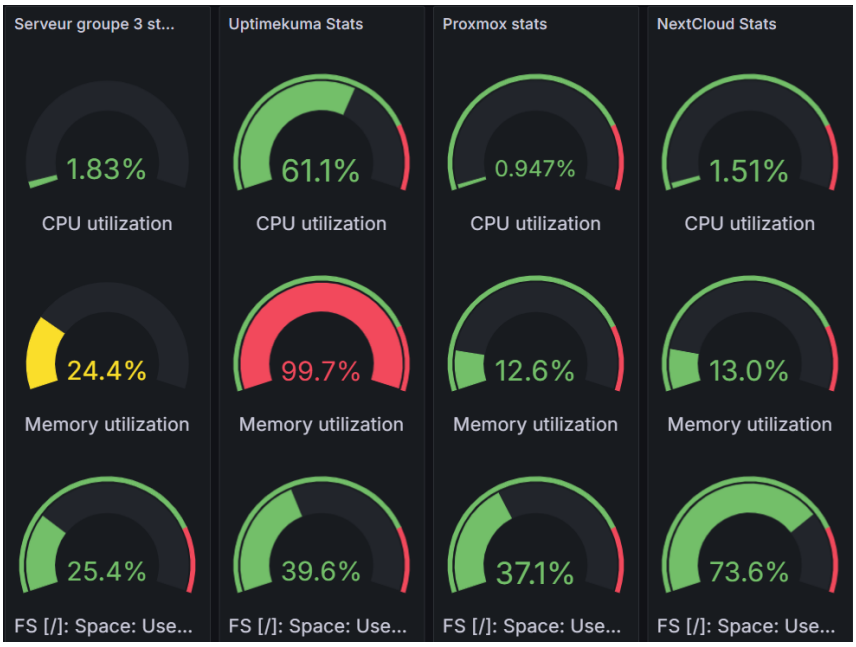
9 mars – 15 mars

Installation et configuration d'agents wazuh et Zabbix sur les machines virtuel

Lors de la semaine du 9 mars au 15 mars, nous avons installé de nouveaux agents notamment, sur le serveur Proxmox et sur la machine NextCloud. Lors de ces installations, nous avons rencontré des problèmes avec les bibliothèques de Zabbix mais, le une solution fut trouvée. Lors de l'installation des agents wazuh un autre problème est survenue, les machines n'avaient pas les paquets nessesaire installer. En vérifiant la documentation Wazuh, on peut voir que le paquet lsb-release doit impérativement être installer avant d'initialiser l'installation de l'agent wazuh. Le problème a donc également été résolu avec succès.

Création du dashboard grafana

Par la suite, nous avons continué de travailler sur Grafana en ajoutant les performances systèmes des nouvelles machines. Également, nous avons modifier le Dashboard afin que celui-ci, soit visuellement plus facile à comprendre.



16 mars – 22 mars

Implémentation des alertes Slack

Lors de la semaine du 16 mars au 22 mars, nous avons implémenter les alertes de notre serveur Wazuh vers une la boite de messagerie Slack afin, de pouvoir visualiser les anomalies. Cette messagerie nous donne ainsi, les alertes ainsi que leur détail en temps réel. Nous pouvons ainsi, savoir ce qui se passe sur nos machines qui ont l'agent wazuh installer. On peut voir que slack recevra donc les alertes de niveau 6 et plus.

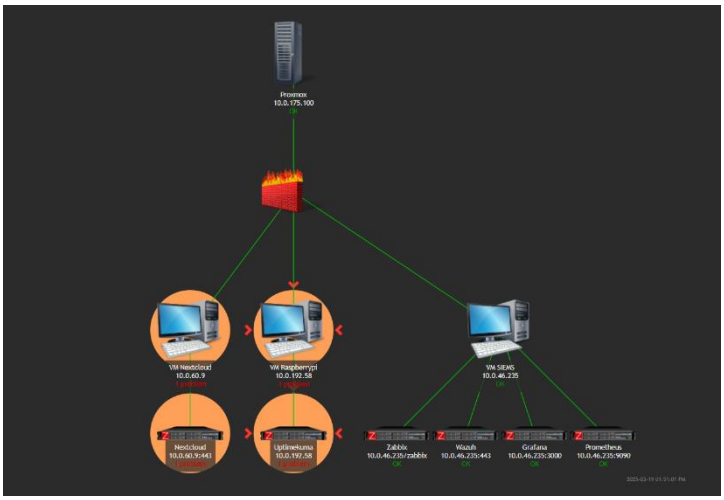
```
<integration>
  <name>slack</name>
  <hook_url>https://hooks.slack.com/services/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 </hook_ur>
  <alert_format>json</alert_format>
  <level>6</level>
</integration>
```

Début de la présentation

Également, nous avons commencé à travailler sur la présentation qui aura lieu le 4 avril prochain. Nous avons commencé à structurer celle-ci afin de pouvoir facilement inclure les éléments nécessaires lors de la finalisation de notre présentation.

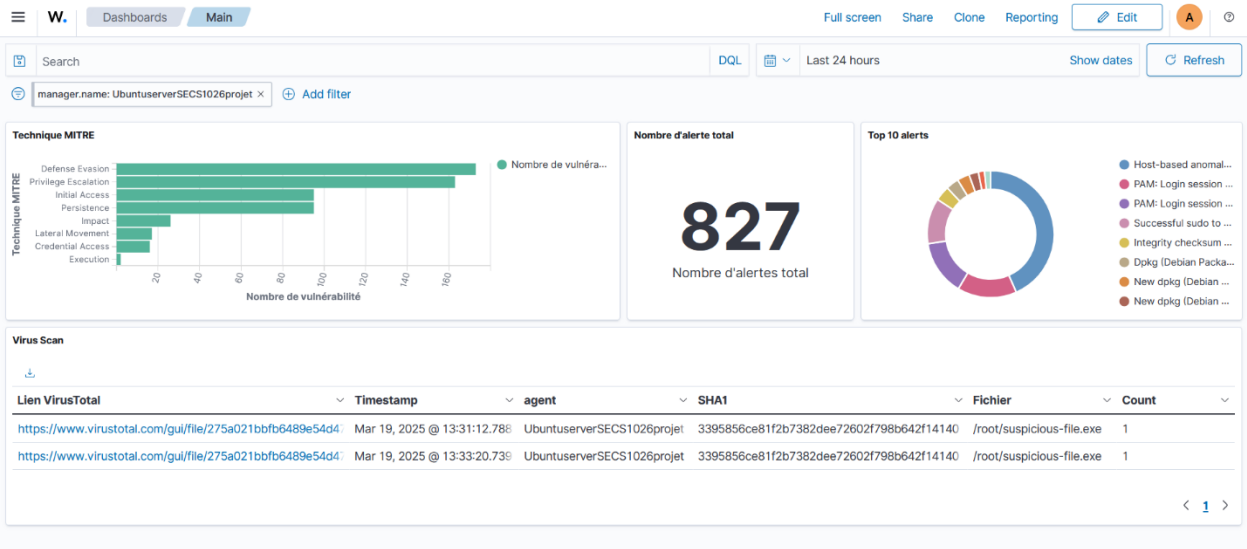
Création du mapping du réseau

Ensuite, nous avons créé un mapping du serveur Proxmox grâce à Zabbix. Le mapping inclue le serveur, le firewall, ainsi que les machines virtuelles présentement installer sur le serveur. Malheureusement pour l'instant, toutes les machines virtuelles qui doivent être installer sur le serveur ne le sont pas encore donc, nous devons attendre pour finaliser le mapping.



Création du visuel Wazuh

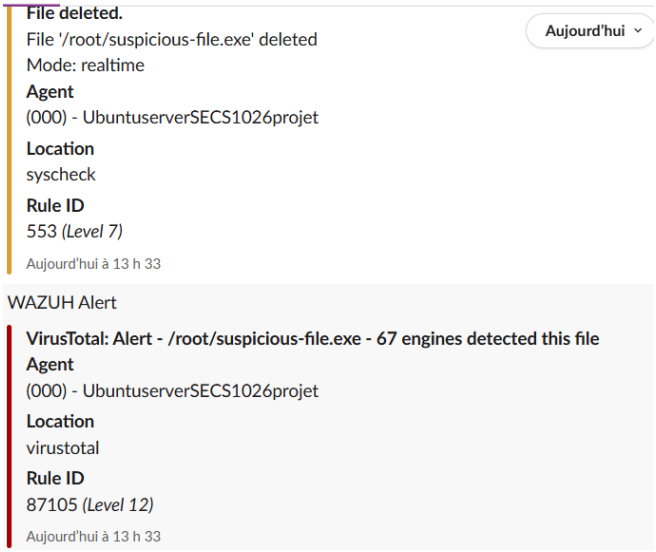
Malheureusement, le support Grafana ne prend pas en compte le logiciel de monitoring Wazuh. Heureusement, celui-ci peut également servir d'interface graphique. Nous avons ainsi, poursuivie avec cette option en créant des dashboard visuel pour voir les activités se déroulant sur notre serveur Wazuh. Le dashboard utilise les données collectées par les agents Wazuh dans les derniers 24 heures.



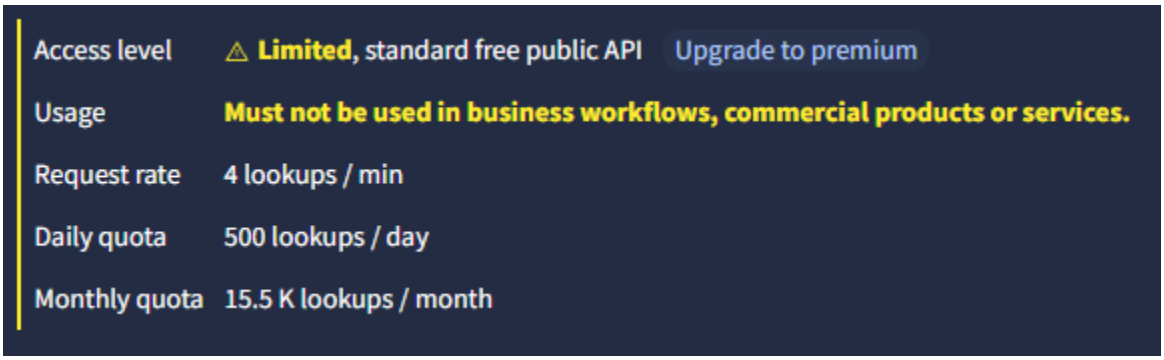
Implémentation de virustotal sur wazuh

Pour implémenter virus total sur Wazuh nous devons connecter l'API dans le fichier de configuration de wazuh. Par défaut, wazuh utilise l'api et génère des alertes virustotal sans autre configuration.

```
<integration>
  <name>virustotal</name>
  <api_key>                                                    </api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```



Cependant, l'api gratuit de virustotal a des limites. Nous avons donc du restreindre les scans de fichier a seulement les fichiers essentiels. Par exemple, les fichier /root et /bin serons scanner si un fichier est ajouté.



24 mars – 28 mars

Création du serveur SIEM

Lors de la semaine du 24 au 28 mars, le serveur proxmox crée par le groupe 1 à rencontrer des problèmes du côté de notre machine virtuelle Wazuh server. Christian nous a donc, demander de crée un autre server proxmox pour y installer notre machine Wazuh. Ce que nous avons réalisé avec une semaine avant la remise du projet.

Division de chaque logiciel dans des machines virtuelles différentes

Lors de la création première de notre machine virtuelle, nous avions mis tous nos logiciels sur la même VM. Ceci a notamment, affecter nos performances lorsque nous travaillons tous en même temps. Nous avons donc décider, de cloner les machines virtuelles et de désactiver les services un par un afin de seulement avoir un logiciel par VM. Nous avons alors cloné la machine virtuel 2 fois pour avoir Wazuh, Zabbix et Grafana/Prometheus. Ceci à grandement améliorer nos performances du système car les logiciels comme wazuh et grafana ont besoin d'énormément de RAM.

Le serveur a planté ?

Pour continuer dans la mal chance, le server Proxmox de base a arrêté de fonctionner. Nous étions donc en situation de remédiement. Notre équipe a donc, proposer son aide à l'équipe 1 afin de pouvoir rebâtir des serveurs pour pouvoir remettre les projets de tous le mondes a temp. Notre équipe comme mentionné plus haut a créé le serveur SIEM et backup mais, a également bâti le serveur pour le déploiement des applications de l'équipe 5.

Travail sur la Présentation

Nous avons également, travailler sur la présentation puisque nous devions la modifier en raison des problèmes survenu plus tôt dans la journée. Ainsi, la présentation était maintenant achevée a plus de 85%.

31 mars – 4 avril

Début de la dernière semaine

La dernière semaine de l'implémentation du projet était finalement arrivée mais, il restait encore beaucoup de travail à réaliser. Lors de cette dernière semaine, nous avons installé énormément d'agent tant du côté Wazuh que Zabbix. Ensuite après l'installation des agents Zabbix, Grafana a dû être mis à jour et afficher les nouvelle donner des nouvelles machines installer sur les différents serveurs.

Wazuh

Pour Wazuh, nous avons installé quelques agents en plus pour recueillir plus de données. Cependant, la plus grosse partie du travail étais de s'assurer du bon fonctionnement des alertes et des mesures de protection. Pour ce faire nous avons installé une machine linux server qui héberge un site web WordPress à l'aide de apache2. Pour commencer, nous avons tester plusieurs types d'attaque tel que brute force ssh, brute force sur la page web, man in the middle, installation de virus et autre. Une fois ce test fait nous avons vérifié si Wazuh agit correctement. Dans notre cas, les alertes de Wazuh fonctionnaient parfaitement

mais les mesures de protection non. Nous avons donc trouble shooter et ensuite ajouter des scripts pour les associer avec les alertes voulus. Firewall-drop a été associer avec tout type de brute force, si Wazuh détecte un brute force, il utilise le script pour bloquer l'adresse ip de l'attaquant à l'aide de UFW. remove-threat a été associer avec virus total pour effacer les fichiers malveillants.

Zabbix

Pour zabbix, nous avons installés ce qui restais en termes d'agent pour être en mesure de voir toutes les machines des serveurs sur zabbix. Nous avons bâti plusieurs maps pour visualiser les serveurs et les machines virtuelles que tout le monde à créer. Nous avons ajouté ce qui manquait pour la présentation du projet en termes de visualisation.

Grafana/Prometheus

Pour la partie Grafana/Prometheus, nous avons repenser à la manière dont nous avions bâti nos Dashboard et comment les améliorer. Il nous est donc, venu à l'idée de crée un support graphique pour chacun des serveurs puisque notre infrastructure en avait maintenant 3. Maintenant que nous avions une idée générale de ce que l'on voulait, il restait simplement à l'implémenter. Les nouveaux Dashboard Grafana nous donnent les statistiques lier à la performance notamment du CPU mais également, de la RAM et du stockage de chaque server et des machines virtuelles à l'intérieur.

Travail et finalisation de la Présentation

Lors que tous étaient fini, nous avons pris un peu de temp pour retravailler la présentation notamment, qui allaient parler de quoi. Ensuite, nous avons également améliorer le support visuel de celle-ci avec des images plus en rapport avec le sujet présenter. Nous avons également, effectuer quelque petit test de manipulation pour s'assurer que tous fonctionneraient lors de la présentation soit le 4 avril 2025.

Conclusion

Le projet d'intégration en cybersécurité réalisé par notre équipe (groupe 3) a permis de concevoir et de déployer un système de surveillance et de gestion des incidents pour une infrastructure réseau complexe. Ce projet, basé sur l'utilisation de logiciels open source tels que Wazuh, Zabbix, Grafana et Prometheus, a atteint ses objectifs en matière de collecte, d'analyse et de visualisation des données, tout en renforçant la sécurité globale du système. La collecte et l'analyse des données ont constitué une étape essentielle du projet. Les agents Wazuh et Zabbix ont été installés sur plusieurs machines virtuelles afin de surveiller la santé, la sécurité et les performances du système. Ces données ont été centralisées pour identifier les anomalies et les vulnérabilités. Cette approche a permis d'assurer une gestion proactive des incidents. La surveillance proactive a été mise en œuvre grâce à Zabbix, qui a permis une visualisation claire des équipements réseau et des serveurs via des cartes interactives. Prometheus a fourni des métriques sur les performances du système, tandis que Grafana a offert une interface graphique intuitive pour visualiser ces données. Ces outils ont contribué à améliorer la visibilité globale sur l'état de l'infrastructure.

La gestion des incidents a été optimisée grâce à Wazuh, qui a généré des alertes en temps réel via Slack et par courriel. Des scripts automatisés ont été développés pour répondre aux incidents critiques, comme le blocage d'adresses IP lors d'attaques brute force ou la suppression de fichiers malveillants. Ces mesures ont renforcé la réactivité face aux menaces. L'optimisation de l'infrastructure a également joué un rôle clé dans le succès du projet. La séparation des logiciels sur différentes machines virtuelles a permis d'améliorer les performances globales du système. Des tableaux de bord Grafana personnalisés ont été créés pour chaque serveur, offrant une vue détaillée sur les ressources utilisées telles que le CPU, la RAM et le stockage.

Malgré les défis rencontrés, notamment liés aux serveurs et aux limitations techniques, notre équipe a su collaborer efficacement pour surmonter ces obstacles. Le système mis en place est fonctionnel et robuste, prêt à être présenté comme un exemple concret d'intégration réussie en cybersécurité. Ce projet constitue une avancée importante dans notre compréhension des technologies modernes de surveillance et de gestion des incidents.

Terminologie

Zabbix : Un logiciel qui surveille de nombreux paramètres d'un réseau ainsi que la santé et l'intégrité des serveurs, des machines virtuelles, des applications, des services, des bases de données, des sites web, du nuage et bien plus encore.

Wazuh : Une plateforme de prévention, de détection et de réponse aux menaces qui est open source. Elle protège les charges de travail sur site, dans des environnements virtualisés, conteneurisés et en nuage. Wazuh est un outil de collecte, d'assosiation, d'indexation et d'analyse des données de sécurité qui aide les entreprises à détecter les intrusions, les menaces et les comportements suspects.

Grafana : Une plateforme d'observabilité open-source permettant de visualiser les métriques, les logs et les traces collectées à partir de vos applications. Il s'agit d'une solution cloud-native permettant d'assembler rapidement des tableaux de bord de données qui vous permettent d'inspecter et d'analyser des données.

Prometheus : Une solution de surveillance open-source qui permet de collecter et d'assembler des métriques sous forme de séries de données temporelles. Plus simplement, chaque élément d'un magasin Prometheus est un événement métrique accompagné de l'heure à laquelle il s'est produit.

NIST (National Institute of Standards and Technologie) : Une agence des États Unis qui favorise l'innovation en faisant avancer la science, les normes et la technologie des mesures. Les normes, les lignes directrices et les bonnes pratiques du cadre de cybersécurité du NIST sont établies pour aider les organisations à améliorer leur gestion des risques de cybersécurité.

Logs (Fichier de journalisation) : Des fichiers qui regroupent tous les événements enregistrés par un système informatique ou une application. On les emploie afin de surveiller les actions et les erreurs qui se produisent sur un système ou une application. Les journaux sont essentiels pour détecter les problèmes et assurer la maintenance des systèmes.

CPU (central processing unit) : CPU est un nom anglais utilisé pour appeler un processeur. Le CPU est un composant électrique qui exécute les instructions de la machine en utilisant des calculs complexes. On peut dire que c'est le cerveau d'un ordinateur

GPU (graphical processing unit) : GPU est le nom anglais pour unité de traitement graphique. Le GPU est un composant électrique dédié aux calculs de données graphiques, il travaille en parallèle avec le CPU pour fonctionner. On peut dire que le GPU est les yeux d'un ordinateur.

Audit : Une évaluation systématique et approfondie des systèmes d'information, des politiques et des pratiques de sécurité d'une organisation, visant à identifier les vulnérabilités et à recommander des améliorations pour renforcer la protection contre les cybermenaces

RAM: La RAM (ou mémoire vive) est la **mémoire à court terme d'un ordinateur**, où sont stockées les données actuellement utilisées par le processeur.

Bibliographie

AlexHost SRL. (2025, 12 février). *Zabbix : Qu'est-ce que c'est et comment l'utiliser & # 8902 ; ALexHost SRL*. ALexHost SRL. https://alexhost.com/fr/faq/zabbix-what-it-is-and-how-to-use-it/

Documentation Zabbix. (s. d.). https://www.zabbix.com/manuals

Grafana OSS and Enterprise | Grafana documentation. (s. d.). Grafana Labs. https://grafana.com/docs/grafana/latest/

Prometheus. (s. d.). *Overview | Prometheus*. https://prometheus.io/docs/introduction/overview/

Prometheus Essential Training Online Class | LinkedIn Learning, formerly Lynda.com. (2024, 12 avril). LinkedIn. https://www.linkedin.com/learning/prometheus-essential-training

Wazuh. (s. d.). *Wazuh documentation*. https://documentation.wazuh.com/current/index.html

Ubuntu Server documentation. (s. d.). *Ubuntu Server.* https://documentation.ubuntu.com/server/

VirusTotal. (s. d.). *VirusTotal.* https://www.virustotal.com/

How To Install lsb-release on Ubuntu 20.04. (2023, 13 juin). *Installati.one.* https://installati.one/install-lsb-release-ubuntu-20-04/