Thème : Administration et déploiement de Zabbix pour le monitoring réseau et gestion d'Internet avec pfSense à l'ACFPE

Partie II : Étude Théorique

Chapitre 1 : Définition des concepts

1.1 Monitoring des réseaux (principes et importance)

1.2 Présentation de Zabbix (fonctionnalités principales, cas d'utilisation)

1.3 Présentation de pfSense

1.4 Avantages et inconvénients de Zabbix et pfSense

Chapitre 2 : Choix de la solution

2.1 Critères de choix (performances, coût, compatibilité, simplicité d'administration)

2.2 Comparaison avec d'autres solutions de monitoring et gestion Internet

2.3 Justification du choix de Zabbix et pfSense

Chapitre 3 : Généralités sur les outils choisis

3.1 Fonctionnalités de Zabbix et leur application à l'ACFPE

3.2 Fonctionnalités de pfSense et leur application à l'ACFPE

3.3 Architecture combinée Zabbix-pfSense pour une gestion complète

3.4 Cas d'utilisation de Zabbix et pfSense dans d'autres organisations

Partie III : Implémentation de la solution retenue

Chapitre 1 : Mise en œuvre

1.1 Liste des besoins matériels et logiciels

A Mme,

J'espère que vous allez bien.

Je me permets de vous écrire concernant ma soutenance de mémoire, prévue le 20 mars 2025, qui est une étape très importante pour la fin de mes études.

Malheureusement, des difficultés financières rendent sa préparation un peu plus compliquée que prévu.

C'est pourquoi je me tourne vers vous. Un petit coup de main de votre part, même modeste, me serait d'une grande aide, notamment pour les frais d'impression et de présentation.

Je comprends vos éventuelles contraintes et vous remercie par avance pour votre écoute et votre compréhension.

J'espère avoir bientôt de vos nouvelles.

Avec toute mon affection/Avec mes sentiments les plus respectueux,

Nicefort Gilchrist KETTEGUIA

Téléphone : 72134187

1.4. Protocoles de monitoring : Les fondations de la surveillance réseau

Les protocoles de monitoring sont essentiels à la surveillance réseau. Ils permettent la communication entre les outils de supervision et les éléments de l'infrastructure à surveiller, définissant les règles et les formats d'échange des données pour collecter des informations cruciales sur l'état, les performances et la sécurité du réseau. Cette section détaille les protocoles les plus importants, classés par catégorie pour une meilleure compréhension :

1.4.1. Protocoles de gestion et de configuration :

Ces protocoles permettent de configurer, de contrôler et de collecter des informations sur l'état des équipements réseau.

- **SNMP (Simple Network Management Protocol) : Le standard *de facto***

  SNMP, un protocole de la couche application (couche 7 du modèle OSI), est largement adopté pour la gestion et la surveillance des équipements réseau. Son architecture repose sur un modèle client-serveur :

  - *Manager (client) :* Le système de supervision qui initie les requêtes et reçoit les réponses des agents.
  - *Agent (serveur) :* Un logiciel installé sur chaque équipement à surveiller (routeurs, commutateurs, serveurs, imprimantes, etc.) qui collecte les informations et répond aux requêtes du manager.

  Les concepts clés de SNMP sont :

  - *MIB (Management Information Base) :* Une base de données hiérarchique qui décrit les objets gérés par SNMP. Chaque objet est identifié par un OID (Object Identifier). Les MIB standardisées sont définies par des organismes tels que l'IETF (Internet Engineering Task Force), mais les constructeurs peuvent également définir leurs propres MIB privées pour gérer les fonctionnalités spécifiques de leurs équipements.
  - *OID (Object Identifiers) :* Des identifiants numériques uniques qui permettent d'accéder à des informations spécifiques sur un équipement. Par exemple, l'OID .1.3.6.1.2.1.1.3.0 représente l'uptime système.

  Versions de SNMP :

  - *SNMPv1 :* La première version, avec des mécanismes de sécurité limités.
  - *SNMPv2c :* Une version améliorée avec une meilleure gestion des erreurs et des types de données, mais toujours avec des faiblesses de sécurité.
  - *SNMPv3 :* La version la plus récente et la plus sécurisée, avec des mécanismes d'authentification et de chiffrement robustes. *Les versions SNMPv1 et v2c présentent des faiblesses de sécurité importantes (absence d'authentification forte et de chiffrement) et leur utilisation est fortement déconseillée dans les environnements modernes. SNMPv3 est la version recommandée pour garantir la confidentialité et l'intégrité des données.*

  Opérations SNMP :

  - *GetRequest :* Le manager demande la valeur d'un OID spécifique à l'agent.
  - *GetNextRequest :* Le manager demande la valeur de l'OID suivant dans la MIB (utile pour parcourir les tables).
  - *SetRequest :* Le manager modifie la valeur d'un OID sur l'agent (utilisé pour la configuration, mais avec prudence).
  - *Trap (ou InformRequest en SNMPv2c et v3) :* Les *Traps* (ou *InformRequests* en SNMPv2c et v3) sont des notifications asynchrones envoyées par l'agent au manager en cas d'événement (par exemple, un changement d'état d'une interface, un dépassement de seuil). La différence principale est que les *InformRequests*

requièrent un accusé de réception du manager, garantissant ainsi la réception de la notification.

- **WMI (Windows Management Instrumentation) : La gestion des systèmes Windows**

  WMI est une technologie Microsoft permettant la gestion et la surveillance des systèmes Windows. Elle offre un accès unifié aux informations de configuration et d'état des systèmes, des applications et des périphériques. WMI utilise un modèle objet basé sur le CIM (Common Information Model) et permet d'effectuer des requêtes et des actions à distance.

- **API (Application Programming Interface) : L'intégration et l'automatisation**

  Les API (Interfaces de Programmation Applicative) permettent à différents systèmes de communiquer et d'échanger des données. Dans le contexte du monitoring, les API permettent :

  - *L'intégration avec d'autres outils :* Récupérer des données provenant d'autres systèmes de gestion, de sécurité ou de supervision.
  - *L'automatisation des tâches :* Automatiser la configuration des outils de monitoring, la création d'alertes, la génération de rapports, etc.
  - *Le développement d'intégrations personnalisées :* Créer des extensions ou des modules pour adapter les outils de monitoring à des besoins spécifiques.
  - *Types d'API couramment utilisés :*
    - *RESTful API :* Basées sur le protocole HTTP, elles sont largement utilisées pour l'intégration avec les services web et les applications cloud.
    - *gRPC (g Remote Procedure Call) :* Un framework RPC (Remote Procedure Call) moderne et performant, de plus en plus utilisé pour le monitoring et la gestion, offrant une communication inter-processus haute performance.

1.4.2. Protocoles de diagnostic :

Ces protocoles permettent de tester la connectivité et de diagnostiquer les problèmes réseau.

- **ICMP (Internet Control Message Protocol) : Tests de connectivité et diagnostic réseau**

  ICMP est un protocole de la couche réseau (couche 3 du modèle OSI) utilisé pour le diagnostic et le contrôle des erreurs réseau. Il est encapsulé dans les paquets IP. Les types de messages ICMP les plus couramment utilisés pour le monitoring sont :

  - *Echo Request et Echo Reply (utilisés par ping) :* Permettent de tester la connectivité entre deux équipements en mesurant le temps de réponse (latence) et la perte de paquets. Le ping est un outil de base pour vérifier si un hôte est accessible sur le réseau.

- *Traceroute (ou tracert sous Windows) :* Utilise des messages ICMP Time Exceeded pour tracer le chemin suivi par les paquets entre deux équipements, en affichant les routeurs intermédiaires. Cet outil est utile pour identifier les problèmes de routage.

1.4.3. Protocoles de flux : Analyse du trafic et visibilité des flux

Ces protocoles offrent une visibilité détaillée sur le trafic réseau, permettant d'analyser l'utilisation de la bande passante et d'identifier les applications et les utilisateurs qui consomment le plus de ressources.

- **NetFlow/sFlow/IPFIX : Analyse du trafic et visibilité des flux**

  Ces protocoles permettent de collecter des informations sur les flux de trafic réseau, offrant une visibilité détaillée sur l'utilisation de la bande passante, les types de trafic qui circulent sur le réseau et les applications qui les génèrent.

  - *NetFlow (Cisco) :* Protocole propriétaire de Cisco, mais largement implémenté par d'autres constructeurs.
  - *sFlow :* Protocole standardisé (RFC 3176) et multi-vendeurs, basé sur un *échantillonnage aléatoire* du trafic, ce qui le rend moins gourmand en ressources que NetFlow, qui capture *chaque flux*.
  - *IPFIX (Internet Protocol Flow Information Export) :* Standard IETF (RFC 7011) basé sur NetFlow v9, considéré comme le successeur de NetFlow.

  Ces protocoles collectent des données telles que :

  - Adresse IP source et destination.
  - Ports source et destination.
  - Protocole utilisé (TCP, UDP, etc.).
  - Volume de trafic (octets, paquets).
  - Durée du flux.
  - Interfaces d'entrée et de sortie.
  - ToS (Type of Service) ou DSCP (Differentiated Services Code Point) : Pour l'analyse de la qualité de service (QoS).

  Ces informations permettent de :

  - Identifier les applications et les utilisateurs qui consomment le plus de bande passante.
  - Détecter les anomalies de trafic (par exemple, les attaques DDoS).
  - Mettre en place des politiques de QoS (Quality of Service) pour prioriser le trafic critique.
  - Effectuer des analyses de sécurité et de forensics.

1.4.4. Agents logiciels : Une collecte de données granulaire et performante

Les agents logiciels sont des programmes installés directement sur les équipements à surveiller. Ils permettent une collecte de données plus précise et plus granulaire que les protocoles tels que SNMP ou ICMP. Exemples d'agents : Zabbix Agent, Nagios NRPE, collectd, Telegraf.

Avantages :

- Collecte de métriques plus complexes, non disponibles via SNMP (par exemple, les performances d'une application, l