DEDICACE

Dans l'obscurité parfois incertaine de mon parcours académique, tu as toujours été la lumière qui guide mes pas. Jamais une hésitation, jamais un refus, seulement un phare constant éclairant mon chemin. Ce travail, Papa, est dédié à ton soutien inconditionnel.

REMERCIEMENTS

Nous rendons grâce à Dieu Tout-Puissant pour la force et la sagesse qu'il nous a accordées tout au long de ce parcours académique et pour l'achèvement de ce travail.

Ce mémoire n'aurait pu aboutir sans le soutien précieux de nombreuses personnes. Nous exprimons notre profonde gratitude envers tous ceux qui ont contribué, de près ou de loin, à sa réalisation.

Nos plus sincères remerciements vont à notre directeur de mémoire, KOYADONDRI Bob, pour son encadrement constant, ses conseils avisés et sa disponibilité. Son expertise a été déterminante pour la qualité de ce travail.

Nous remercions chaleureusement notre maître de stage, Monsieur MBOTE Depaul, pour son soutien pratique et moral, son encadrement et les opportunités offertes au sein de l'ACFPE. Son accompagnement a été essentiel.

Nous exprimons notre gratitude envers l'ensemble du corps professoral et administratif de l'Institut Supérieur de Technologie, et plus particulièrement envers le Directeur, Monsieur Jean M'BOLIGUIPA, Ph.D, le Directeur des Études, Monsieur Noé Landry Privace M'BOUANA, Ph.D, et le Chef du Département de Génie Informatique, Monsieur Innocent NGOUMAPE, pour leur soutien constant et leurs conseils éclairés.

Nous remercions également les collaborateurs de l'ACFPE pour leurs précieux conseils et leur aide.

Un immense merci à nos familles, amis et proches pour leur soutien indéfectible, leur patience, leur amour et leurs encouragements constants. Leur présence a été un véritable pilier.

Nous remercions nos camarades de promotion pour leur collaboration, leur solidarité et les moments de partage.

Enfin, nous remercions sincèrement le jury d'avoir accepté d'évaluer ce travail. Leurs remarques constructives contribueront à enrichir notre réflexion.

À tous, nous dédions ce mémoire en signe de respect et de profonde gratitude.

AVANT-PROPOS

L'Institut Supérieur de Technologie (IST), composante de l'Université de Bangui, assure depuis sa création en 1973 (sous le nom d'Institut Universitaire Technologique des Mines et Géologie - IUTMG) une formation technique et technologique professionnelle. Rebaptisé IST en 1992, l'institut a évolué, passant de trois à cinq départements, avec l'ajout notable du département de Génie Informatique en 2000, puis celui de Génie Pétrolier en 2020.

L'IST a pour mission d'offrir un enseignement supérieur technologique de qualité et de mener des activités de recherche contribuant au progrès des sciences technologiques. Les cinq départements sont :

Génie Civil,

Génie Industriel,

Génie Informatique,

Génie des Mines et Géologie,

Génie Pétrolier.

La formation, d'une durée de trois ans, aboutit à une Licence Professionnelle. Ce diplôme est conditionné par un stage pratique de trois mois au sein d'une institution ou d'un ministère, suivi de la rédaction et de la soutenance d'un mémoire. Ce stage permet aux étudiants de mettre en application les connaissances théoriques acquises durant leur cursus.

Dans le cadre de notre formation en Génie Informatique à l'IST, nous avons effectué un stage au sein de l'Agence Centrafricaine pour la Formation Professionnelles et l'Emploi (ACFPE). Ce stage a été l'occasion de mener un projet portant sur l'« Administration et le déploiement de Zabbix pour le monitoring réseau et de pfSense pour la gestion du trafic Internet ». Ce choix s'est imposé suite à une analyse des besoins de l'ACFPE, révélant des lacunes en matière de supervision et de gestion du trafic réseau, impactant la performance et la sécurité de leur infrastructure.

SOMMAIRE

In the digital age, effective management of IT networks has become a critical challenge for organizations, both public and private. This is particularly true for the Association Centrafricaine des Femmes Professionnelles de l'Éducation (ACFPE), which relies heavily on its IT infrastructure and internet access to carry out its mission. The exponential growth of data traffic, security threats, and the increasing dependency on online services make it essential to implement robust network supervision and traffic management solutions.

This thesis focuses on the administration and deployment of Zabbix, an open-source network monitoring solution, and pfSense, an open-source firewall and traffic monitoring and management platform, to enhance network performance and control internet consumption at ACFPE, leading to improved reliability, security, optimized bandwidth usage, and reduced operational costs.

The research examines the specific network supervision requirements of ACFPE and how Zabbix can be configured to monitor critical infrastructure, including servers, routers, and applications. Additionally, pfSense's capabilities in managing network traffic, security, and internet consumption are explored in-depth, focusing on firewall configurations, VPN setups, and bandwidth management. The integration of these two solutions offers a centralized view of the network, ensuring optimized management and seamless monitoring.

Through configuration analysis, performance testing in a simulated environment, and a real-life case study within ACFPE, this thesis demonstrates the efficiency of combining Zabbix and pfSense

to improve network performance, security, and resource management. The results highlight the benefits of this integrated approach, showing how it can enhance the overall functioning of the institution while ensuring the confidentiality and security of sensitive data."

En conclusion, l'abstract 1 est déjà très bon et la version révisée proposée apporte quelques améliorations mineures pour plus de concision et de cohérence.

INTRODUCTION

À l'ère de la digitalisation, la gestion efficace des réseaux est cruciale pour toute organisation. Performance, sécurité et disponibilité des infrastructures sont déterminantes pour la continuité des activités et la qualité des services. Face à la complexité croissante des réseaux, l'augmentation du trafic, les menaces et la dépendance aux services en ligne, des solutions de supervision et de gestion performantes sont indispensables.

La supervision réseau, autrefois limitée à l'état des équipements (ping, interfaces), intègre désormais la gestion des performances (CPU, mémoire, bande passante), la détection des anomalies (pics de trafic, erreurs), l'optimisation de la bande passante (QoS) et la sécurité (détection d'intrusion, logs). Elle permet de prévenir les pannes, d'optimiser les ressources, de garantir la qualité de service et de réagir efficacement aux incidents.

Parallèlement, la gestion du trafic Internet est un enjeu majeur. La maîtrise des coûts d'accès, l'optimisation de la bande passante et l'utilisation rationnelle des ressources (navigation, téléchargements, streaming) sont essentielles. Une mauvaise gestion peut entraîner ralentissements, dégradation des performances et coûts élevés.

Dans ce contexte, les outils open source Zabbix et pfSense offrent une alternative flexible, économique et performante. Zabbix, avec son architecture modulaire, collecte, analyse et visualise en temps réel les données de performance de l'infrastructure (serveurs, routeurs, commutateurs, applications, services). pfSense, plateforme de gestion de pare-feu et de routage basée sur FreeBSD, fournit des fonctionnalités avancées de contrôle du trafic (pare-feu, NAT, routage), de sécurité (VPN, IDS/IPS), de gestion de la bande passante (QoS, traffic shaping) et d'accès (authentification, portail captif), permettant un contrôle précis de la consommation et une protection efficace.

Pour l'ACFPE, dont les activités reposent sur les TIC (communication, formation en ligne, gestion administrative), l'infrastructure et l'accès Internet sont essentiels. Une solution de supervision et de gestion adaptée est donc primordiale pour optimiser le fonctionnement, maîtriser les coûts, garantir la sécurité et la confidentialité des données, et améliorer la qualité des services.

Ce mémoire étudie l'administration et le déploiement de Zabbix pour le monitoring réseau et de pfSense pour la gestion du trafic Internet à l'ACFPE, visant à améliorer la fiabilité, la sécurité et l'efficacité du réseau. La méthodologie s'appuie sur des analyses de configuration, des tests de performance en environnement simulé et une étude de cas concrète au sein de l'ACFPE. Il aborde les points suivants :

- Analyse des besoins spécifiques de l'ACFPE en supervision et gestion du trafic.
- Configuration et déploiement de Zabbix pour la supervision (métriques, alertes).
- Configuration avancée de pfSense pour la gestion du trafic, la sécurité, le contrôle d'accès, la QoS et l'optimisation de la consommation (règles de pare-feu, VPN, gestion de la bande passante).
- Intégration de Zabbix et pfSense pour une supervision centralisée et une gestion optimisée (intégration, automatisation).
- Évaluation des performances et propositions d'amélioration (tests de charge, analyses de performance, KPI).

PARTIE I

Présentation Générale

Chapitre 1 : Présentation de la structure d'accueil

1.1.Historique de l'ACFPE

L'Agence Centrafricaine pour la Formation Professionnelle et l'Emploi (ACFPE) a été créée par la Loi 99/008 du 19 mai 1999. Née des cendres des anciens organes dissous que sont l'Organisation Nationale Interprofessionnelle de Formation et de Perfectionnement (ONIFOP) et l'Office National de la Main d'œuvre (ONMO), l'ACFPE est un établissement à caractère économique et social qui jouit de la personnalité juridique et de l'autonomie financière.

L'ACFPE (Agence Centrafricaine pour la Formation Professionnelle et de l'Emploi) est un établissement public à caractère administratif, placé sous la tutelle du Ministère chargé de la Formation Professionnelle et de l'Emploi. Sa mission principale est de contribuer à l'adéquation entre l'offre et la demande d'emploi en République Centrafricaine, en développant la formation professionnelle, en promouvant l'emploi et en soutenant le développement de la libre entreprise.

Ses ressources proviennent essentiellement des entreprises du secteur privé et secteur parapublic notamment des subventions de l'État et d'organismes internationaux. Ces ressources sont constituées :

- Des cotisations patronales (2% de la masse salariale brute) ; elles représentent 95% de ses ressources ;
- Des subventions et des dons ;
- Des frais de visa des contrats de travail et d'établissement des cartes de travail ;
- Des produits d'amendes provenant d'infractions ;

- Des revenus générés par les fonds placés dans les établissements financiers.

1.2. Mission de l'ACFPE

L'Agence centrafricaine pour la Formation Professionnelle et l'Emploi a pour mission, dans le cadre des directives techniques qu' elle reçoit, d'exécuter toutes les opérations relatives à la promotion de I 'Emploi à la Formation Professionnelle et au développement de la libre entreprise génératrice L'emplois productifs sur toute L'etendue du territoire centrafricain.

A ce titre elle est chargée de :

- Recueillir et analyser toutes les Informations relatives à L'emploi aux métiers, au chômage et à la formation Professionnelle quelle diffuse aux décideurs, planificateurs, opérateurs économiques ou gestionnaire de programmes publics ou privés

- Recueillir, Centraliser et publier les offres et demande d'emploi

- Informer et orienter les demandeurs d'emploi et les personnes en activité en matière d'emploi, de carrière et sur les possibilités de promotion et de reconversion professionnelle

- Prospecter auprès des employeurs les besoins en placement, en formation professionnelle, en perfectionnement en vue de leur apporter l'aide et les conseils nécessaires au renforcement des capacités a générer emplois.

- Aider à I 'intégration au secteur moderne certaines entités économiques évoluant encore dans le secteur informel
- Mener pour son compte ou à la demande du Gouvernement des études prospectives et d'évaluation ainsi que des actions d 'Information et de sensibilisation du public en matière d'emploi et de formation professionnelle.
- Informer les Employeurs, les travailleurs et les Demandeurs d'emploi sur les offres de formation professionnelle disponibles sur le territoire national et contribuer à la diversification des filières et opportunités de formation et de perfectionnement.
- Concevoir, financer, exécuter et suivre des projets et programmes les à la formation professionnelle au perfectionnement et/ou au recyclage du personnel des entreprises ainsi qu'au développement des activités génératrices d'emplois et faciliter les moyens concourant à l'insertion des Jeunes en quête de premier emploi.
- Assurer directement certaines missions de formation professionnelle

- Proposer aux employeurs le placement des personnes avant le profil requis suite aux sélections des candidats
- Préparer et assurer le suivi des accords conclus avec les organismes de développement les collectivités locales, les établissements de formation et les Organisation Non Gouvernementales des actions visant à la promotion de l'emploi et la réduction de pauvreté
- Etablir les cartes de travail et viser les contrats de travail
- Etablir toutes actions administratives, juridiques et financière liée à sa mission.
- Agence Centrafricaine pour la Formation Professionnelle et de l'Emploi peut également être appelée à émettre son avis sur les questions qui lui sont soumise et mettre en oeuvre des dispositions spécifiques arrêtées par le gouvernement en faveur de I 'emploi et de la formation professionnelle.

Par ailleurs, l'ACFPE est placée sous la tutelle administrative du Ministère en charge de l'Emploi et de la formation professionnelle et sous tutelle également du Ministère Chargé du Contrôle général du secteur parapublic.

Ses publics cibles sont :

- Les demandeurs d'emploi ;
- Les promoteurs/porteurs de projets ;
- Les entreprises et offices publics ;
- Les ONG/associations ;
- Les centres et les organismes de formations professionnels et techniques.

Ses ressources perçues lui permettent ainsi de mettre à la disposition de sa clientèle :

- Des actions de formation ;
- Des travaux d'appui conseil aux entreprises ;
- L'intermédiation et le placement ;
- L'auto emploi.

1.3. Structure Organisationnelle

L'ACFPE est constituée de trois (03) grandes directions qui sont, elles, mêmes subdivisées en services. Les services sont chargés de la mise en œuvre des attributions de chaque direction. Ainsi, on retrouve les directions suivantes et les services qui leurs sont rattachés :

La Direction des Études, de la Planification et de l'Emploi (DEPE) Avec

pour services rattachés :

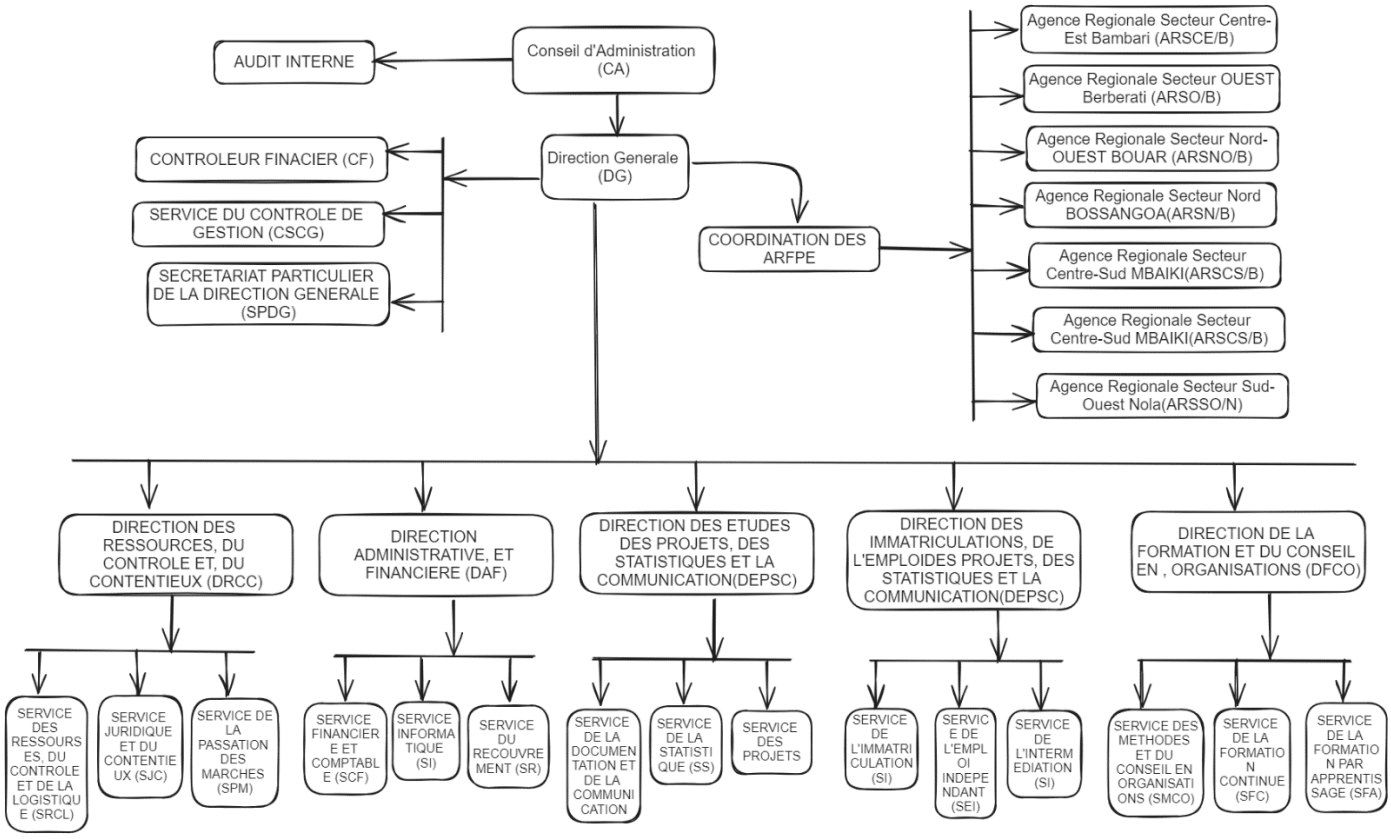
Le Service de l'Immatriculation et de l'Emploi (SIE)
Le Service des Statistiques et de la documentation (SSD)
Le Service des Études, de la Planification et des Projets (SEPP).
La Direction de la Formation et du Conseil en Organisations (DFCO) Le Service de la Formation Continue (SFC) Avec pour services rattachés :

Le Service de la Formation par Apprentissage (SFA)
Le Service des Méthodes et du Conseil en Organisations (SMCO)
Direction d'Appui
La Direction Administrative et Financière (DAF) Avec

pour services rattachés :

Le Service des Ressources, du Contrôle et du Contentieux (SRCC) :
Le Service du Recouvrement (SR)
Le Service Financier et Comptable (SFC)
Cellule Informatique]

1.4.Organigramme de l'ACFPE



Chapitre 2 : Analyse de l'existant

1. Étude de l'existant

L'Agence Centrafricaine pour la Formation Professionnelle et de l'Emploi (ACFPE), dans sa mission de développement des compétences et de promotion de l'emploi en République Centrafricaine, s'appuie sur un réseau informatique dont la gestion et le suivi nécessitent une optimisation continue pour assurer la continuité et la qualité de ses services.

Dans cette optique, une étude initiale est essentielle. Elle vise à recenser tous les équipements et services informatiques actuels de l'ACFPE et à identifier les défis existants.

Les bénéfices attendus incluent une meilleure disponibilité des services, une optimisation des coûts d'accès à Internet, une sécurité renforcée des données sensibles et une efficacité accrue dans les missions de formation et de promotion de l'emploi de l'ACFPE.

1.1. Architecture du réseau

L'ACFPE s'appuie sur une architecture réseau centralisée, où les différents bâtiments sont interconnectés via un réseau local (LAN) Ethernet. Le bureau de l'informaticien, véritable plaque tournante du système d'information, abrite les équipements névralgiques.

- **Cœur du réseau**: Le bureau de l'informaticien regroupe :
  - Un switch Sisco CBS 2500-24P-4G 24 ports de niveau 2 la distribution et la commutation des trames Ethernet au sein du LAN.
  - Un routeur WiFi (norme 802.11n ou supérieure) pour la connectivité sans fil, offrant un accès réseau mobile aux utilisateurs.
  - Une liaison VSAT (Very Small Aperture Terminal) pour l'accès à Internet, solution satellitaire permettant de s'affranchir des infrastructures terrestres.
- **Extension du réseau** : Chaque bâtiment est intégré au réseau principal par :
  - Un routeur WiFi (norme 802.11n) configuré en point d'accès, étendant la couverture sans fil aux différents locaux.
  - Un câblage structuré pour les connexions filaires, garantissant un débit suffisant pour les applications bureautiques.

Le réseau local de l'ACFPE est identifié par le nom de domaine ACFPE-RCA.org, soulignant l'identité de l'agence au sein du paysage numérique.

1. Matériel informatique

Les matériels informatiques de l'ACFPE comprend un ensemble d'équipements hétérogènes, allant des postes de travail aux serveurs, en passant par les périphériques d'impression.

1.1. Postes de travail :

- **Ordinateurs** portables : 73 ordinateurs portables sont déployés dans les bureaux, offrant une mobilité aux utilisateurs. Les modèles exacts ne sont pas spécifiés, mais il est probable qu'il s'agisse de machines bureautiques standard.
- **Ordinateurs fixes** : 35 ordinateurs fixes sont également présents dans les bureaux, constituant l'équipement principal pour les tâches sédentaires. Les spécifications techniques de ces machines ne sont pas détaillées.
- Salle informatique : La salle informatique est équipée de 40 ordinateurs fixes, dédiés à des usages spécifiques (formation).

1.2. Serveurs :

L'ACFPE dispose de trois serveurs HP ProLiant DL380 Gen10 , jouant des rôles distincts dans l'infrastructure :

- **Contrôleur de domaine** : Un serveur sous Windows Server 2019 avec licence assure le rôle de contrôleur de domaine, gérant l'authentification des utilisateurs et les accès aux ressources du réseau.

- **Serveur d'applications Sage** : Un serveur sous Windows Server 2019 avec liecence héberge l'application Sage, le logiciel de gestion utilisé par les services RH et comptabilité.
- **Serveur d'applications (Proxmox)** : Un serveur sous Proxmox, une plateforme de virtualisation open source, héberge d'autres applications utilisées localement.

1.3. Les Périphériques d'interconnexion et de sauvegarde

L'ACFPE dispose de 5 switches assurant l'interconnexion et le partage dans différents bureau, d'un Routeurs Fortigate FG-40F et de quatre Baie de de sauvegarde QNAP TS-453^{E} 8G.

1.4.Périphériques d'impression :

Le parc d'impression de l'ACFPE comprend :

- 7 photocopieurs Canon IR 2520, multifonctions (impression, copie, numérisation).
- 32 imprimantes multifonctions HP (modèles non spécifiés), des modèles bureautiques classiques.

Remarques importantes :

- **Système d'exploitation** : Tous les ordinateurs fonctionnent sous Windows 10, mais l'absence de licences soulève des questions de conformité et de sécurité.
- **Logiciel bureautique** : Le logiciel bureautique Microsoft Office 2013 est largement utilisé, mais l'absence de licences pose également des problèmes de conformité.

2. Logiciels

L'ACFPE utilise un ensemble de logiciels standards et d'applications métier pour la gestion de ses activités :

- **Logiciels bureautiques** : La suite Microsoft Office (versions 2013) est omniprésente, couvrant les besoins en traitement de texte, tableur, présentations, etc.
- **Logiciels de gestion** :
    - Sage : Solution de gestion intégrée pour les services des Ressources Humaines et de la Comptabilité, couvrant les fonctions administratives et financières.
    - Application d'immatriculation et de Recouvrement: Application métier dédiée au service d'immatriculation et de recouvrement, développée sur une technologie web ou client-serveur en [code geniter] .

3. Sécurité informatique

La sécurité informatique de l'ACFPE repose sur des mesures individuelles, sans approche globale :

- Protection individuelle : Chaque ordinateur est équipé d'un antivirus (Kaspersky), assurant une protection de base contre les logiciels malveillants.
- Absence de protection globale : L'agence ne dispose pas d'équipements de sécurité périmétriques (pare-feu, système de détection d'intrusion, etc.) ni de politique de reprise d'activité en cas d'incident, ce qui fragilise la sécurité du système d'information.

4. Compétences informatiques

- Équipe informatique : L'ACFPE s'appuie sur une équipe de deux informaticiens qualifiés, chargés de la maintenance du réseau et des équipements.
- Maîtrise des outils bureautiques : Les employés possèdent une maîtrise des outils bureautiques de la suite Microsoft Office, leur permettant d'être autonomes dans leurs tâches quotidiennes.

I. Critique de l'existant

L'analyse approfondie de l'infrastructure informatique de l'ACFPE, telle que décrite précédemment, met en lumière des vulnérabilités critiques et des axes d'amélioration majeurs qui justifient pleinement la mise en place d'une solution de monitoring réseau et de gestion du trafic avec Zabbix et pfSense.

1. Absence de monitoring

L'absence d'un système de monitoring proactif constitue une lacune majeure. L'équipe informatique, privée d'une visibilité en temps réel sur l'état du réseau et des serveurs, est contrainte de réagir aux incidents signalés par les utilisateurs. Cette approche réactive engendre plusieurs conséquences préjudiciables :

- **Détection tardive des pannes** : Les pannes ne sont détectées qu'une fois qu'elles ont un impact sur les utilisateurs, entraînant des interruptions de service et une perte de productivité. [Par exemple, une panne du serveur de fichiers (HP ProLiant DL380 Gen10) ne serait détectée que lorsque les utilisateurs ne peuvent plus accéder aux documents, perturbant ainsi les activités administratives et de formation.]
- **Difficulté à identifier les causes profondes des problèmes :** Sans données de monitoring, il est difficile de déterminer l'origine exacte des problèmes. L'équipe informatique doit alors mener des investigations chronophages, ce qui retarde la résolution des incidents. [Par exemple, un ralentissement du réseau pourrait être dû à une saturation de la liaison VSAT, à une surcharge du serveur d'applications Sage, à un problème avec le commutateur 24 ports ou à une utilisation excessive de la bande passante par certains utilisateurs. Sans monitoring, il est difficile de discriminer entre ces différentes causes.]

- **Impact sur la crédibilité de l'ACFPE** : Les interruptions de service répétées et les difficultés d'accès aux ressources informatiques peuvent nuire à la crédibilité de l'ACFPE auprès de ses partenaires et des bénéficiaires de ses services.

2. **Manque de visibilité sur la consommation internet et de la bande passante**

L'absence d'outil de suivi de la consommation de la bande passante rend la gestion des ressources Internet extrêmement difficile. Cette absence de visibilité a plusieurs implications :

- **Impossibilité d'identifier les goulets d'étranglement** : Sans données précises sur l'utilisation de la bande passante, il est impossible de déterminer si le réseau est réellement saturé ou si le problème vient d'ailleurs. [Par exemple, un utilisateur effectuant des téléchargements importants pourrait saturer la bande passante et impacter tous les autres utilisateurs, mais sans monitoring, il est difficile de l'identifier.]
- **Difficulté à optimiser les coûts :** L'ACFPE ne peut pas justifier une augmentation de la bande passante sans données concrètes sur son utilisation. Il est donc difficile d'optimiser les coûts d'accès à Internet et de justifier les dépenses auprès de la direction.
- **Impossibilité de mettre en place des politiques de QoS** : Sans suivi précis de la consommation par application, il est impossible de prioriser les trafics critiques, comme les applications de formation en ligne ou les communications avec les partenaires.

3. **Gestion limitée des flux réseaux et sécurité périmétrique insuffisante**

Le routeur WiFi, bien qu'offrant une connectivité sans fil, ne permet pas une gestion avancée des flux réseau. De plus, l'absence de pare-feu et de système de détection d'intrusion expose l'ACFPE à des risques de sécurité importants :

- **Vulnérabilités de sécurité** : L'absence de pare-feu rend le réseau vulnérable aux intrusions et aux attaques.
- **Manque de contrôle sur les flux** : Il n'est pas possible de mettre en place des politiques de QoS pour prioriser les applications critiques, ce qui peut impacter les performances des services importants.

4. **Absence d'alertes**

L'absence d'un système d'alertes en temps réel signifie que l'équipe informatique n'est informée des problèmes que lorsque les utilisateurs les signalent. Cela rallonge considérablement les temps de résolution des incidents et augmente leur impact sur les services.

L'analyse de l'existant met en lumière un besoin urgent d'optimisation de l'infrastructure réseau de l'ACFPE. Les lacunes actuelles en matière de monitoring, de gestion des trafics et de sécurité ont un impact direct sur la disponibilité et la performance des services, sur la maîtrise des coûts et sur la crédibilité de l'agence. La mise en place de Zabbix et pfSense apparaît donc comme une solution pertinente et nécessaire pour répondre à ces enjeux.

II. Problématique

La gestion actuelle du réseau informatique de l'ACFPE présente plusieurs limitations, notamment un manque de visibilité sur l'état du réseau, une gestion manuelle chronophage, l'absence de suivi précis de la consommation Internet et un manque d'alertes proactives. Ces limitations ont un impact négatif sur la disponibilité et la performance des services informatiques, sur la maîtrise des coûts d'accès à Internet et sur la sécurité du réseau. Par conséquent, la problématique centrale est la suivante :

Comment mettre en place une solution de monitoring et de gestion de l'Internet performante et centralisée afin d'améliorer la disponibilité des services, d'optimiser la gestion de la bande passante, de renforcer la sécurité du réseau et de contribuer à l'efficacité des missions de l'ACFPE ?

1. Objectifs

L'objectif de ce projet est de doter l'ACFPE d'une solution intégrée de monitoring réseau et de gestion d'internet, combinant Zabbix et pfSense, afin d'optimiser la visibilité, la sécurité et l'efficacité de son infrastructure informatique. Plus précisément, il s'agira de mettre en place une surveillance proactive et complète du réseau (couverture de 95% des équipements) avec Zabbix, incluant l'automatisation des alertes et de certaines tâches de maintenance. En parallèle, pfSense sera configuré pour collecter, analyser (par utilisateur et par application) et générer des rapports mensuels sur la consommation internet, offrant ainsi une gestion précise et Granulaire du trafic. Enfin, pfSense permettra de renforcer la sécurité du réseau grâce à la mise en place d'un portail captif performant .

2. Cout et Duree

Pour l'implémentation de ce projet, il est important d'élaborer un devis quantitatif prenant en compte l'ensemble du matériel indispensable, la main d'œuvre ainsi que la durée nécessaire correspondant.

1.1 Estimation du coût du projet

Catégorie	**Details**	**Coût estimé (FCFA)**
Infrastructure matérielle	Serveurs, Switch et routeurs	-
Infrastructure logicielle	Zabbix et pfsense Community Edition	-
Déploiement et Configuration	Main d'œuvre	5 000 000
Formation et documentation	Formation de l'équipe IT	2 000 000

Maintenance et Support	Contrat de maintenance	1 000 000/an
Total estimé		8 000 000

1.2 Estimation de la durée du projet

Phase	**Tache**	**Durée estimée**
Analyse et Préparation	Evaluation de l'infrastructure existante et Définitions des besoins	2 semaines
Installation et configuration	-Installation de Zabbix et pfsense sur le server - Configuration des agents sur périphériques terminaux - Mise en place des règles de gestion du trafic avec pfsense	2 semaines
Tests et ajustements	Tests de surveillance , vérifications des alertes et logs ajustement des paramètres	2 semaines
Formation	Formation de l'équipe IT	2 semaines
Déploiement finale	Mise en production, suivi des performance et corrections éventuelles	2 Semaine
Total estimé		10 Semaines

2 PARTIE

2

1 Etude Théorique

Chapitre 1 : Définition des concepts

I. La supervision informatique

1. Introduction à la supervision informatique

L'administration d'une infrastructure réseau est une tâche complexe et exigeante, nécessitant une surveillance constante, d'autant plus que le nombre d'équipements à gérer ne cesse d'augmenter. Le principal défi pour un administrateur est de prévenir et de gérer les pannes le plus rapidement possible afin d'éviter des interruptions de service prolongées, préjudiciables à l'activité de l'organisation. Un autre enjeu majeur est la gestion efficace du trafic internet, notamment pour optimiser la bande passante, contrôler les coûts et assurer la sécurité des accès. La supervision informatique intervient alors pour répondre à ces besoins cruciaux : elle permet d'anticiper les problèmes, de fournir des informations en temps réel sur l'état des équipements et de contrôler l'utilisation de la bande passante.

1.1.Définition et importance de la supervision

La supervision informatique, également appelée monitoring informatique, consiste à surveiller en temps réel les performances, la disponibilité et la sécurité d'un réseau informatique. Cette surveillance repose sur des outils capables de collecter, traiter, analyser et présenter des données relatives aux équipements réseau (routeurs, commutateurs, serveurs, pare-feu) et aux

services (applications, protocoles). On distingue principalement le monitoring de performance (CPU, mémoire, bande passante), de disponibilité (uptime des services) et de sécurité (détection d'intrusions, logs).

La supervision permet aux administrateurs réseau de surveiller le bon fonctionnement des systèmes d'information, en leur offrant une visibilité complète sur les différentes composantes matérielles et logicielles. L'administrateur peut ainsi visualiser et analyser les informations et données fournies, et vérifier le fonctionnement normal ou anormal du système informatique. L'objectif principal de la supervision est de donner à l'administrateur une vue d'ensemble de l'infrastructure informatique, afin de lui permettre de contrôler et de gérer plus facilement le réseau, surtout face à son évolution constante. Cela garantit la fiabilité et la continuité des différents services des entreprises et des administrations.

1.2. Objectifs du monitoring

Le monitoring informatique poursuit trois objectifs principaux :

- **Performance :** Surveiller et optimiser les performances des systèmes et des applications, en mesurant des indicateurs clés tels que le temps de réponse, la latence, le débit et l'utilisation des ressources (CPU, mémoire, disque).
- **Disponibilité :** Assurer la disponibilité des services et des applications, en détectant les pannes et les interruptions de service, et en mettant en place des mécanismes de redondance et de basculement.
- **Sécurité :** Protéger les systèmes et les données contre les menaces internes et externes, en surveillant les activités suspectes, en détectant les intrusions et en analysant les logs de sécurité.

1.3. Rôle de la supervision

Dans un monde de plus en plus dépendant des services numériques, la supervision réseau joue un rôle stratégique dans la gestion et la maintenance des infrastructures informatiques. Bien plus qu'une simple observation passive de l'état des systèmes, elle s'articule autour de trois axes majeurs : la prévention des problèmes, l'automatisation des remédiations et la mise à disposition d'une vision globale grâce aux rapports et tableaux de bord.

1.3.1. Prévention des problèmes

La supervision réseau repose sur une collecte et une analyse continue des données issues des systèmes, applications et équipements réseau. Cette démarche proactive permet d'identifier les

signaux faibles avant qu'ils ne se transforment en incidents critiques. Parmi les objectifs principaux de cette prévention, on peut citer :

- Détection des anomalies : Identifier les signes avant-coureurs de pannes, comme une surcharge progressive des CPU, une saturation de la mémoire ou un espace disque insuffisant.
- Surveillance du trafic réseau : Grâce à des protocoles comme NetFlow, sFlow ou IPFIX, il est possible de suivre en temps réel les flux de données pour identifier les goulots d'étranglement.
- Détecter les usages anormaux (pics de trafic, scans de ports).
- Prévenir les attaques par déni de service (DoS).
- Contrôler le respect des politiques d'utilisation du réseau.
- Minimisation des interruptions de service : En anticipant les risques, il devient possible de maintenir une haute disponibilité des services, essentielle pour les environnements critiques.

La prévention joue donc un rôle clé en permettant d'anticiper les problèmes avant qu'ils n'impactent le fonctionnement des infrastructures.

1.3.2. Automatisation des tâches de remédiation : Réduire les temps d'arrêt

Pour compléter cette démarche proactive, la supervision intègre des mécanismes d'automatisation afin de limiter les interruptions et de garantir la continuité des services. Quelques exemples d'actions automatisées :

- Redémarrage automatique des services critiques en cas d'arrêt inopiné.

- Gestion des surcharges : Réduction des processus ou arrêt contrôlé des systèmes pour prévenir une panne matérielle.

- Basculement automatique vers un serveur de secours en cas de défaillance du serveur principal.
- Sauvegardes préventives en cas de détection d'un risque imminent de perte de données.
- Actions sur les équipements réseau : Modification automatique des règles de pare-feu ou blocage des adresses IP suspectes.

Ces mécanismes permettent non seulement de réduire les temps d'arrêt, mais aussi d'augmenter la résilience et la robustesse des systèmes.

1.3.3. Raports et tableaux de bord : Une vue d'ensemble pour la prise de décision

En plus de prévenir et de réagir aux problèmes, la supervision fournit aux administrateurs des outils de pilotage efficaces grâce à des rapports et tableaux de bord personnalisés. Ceux-ci offrent une vision consolidée de :

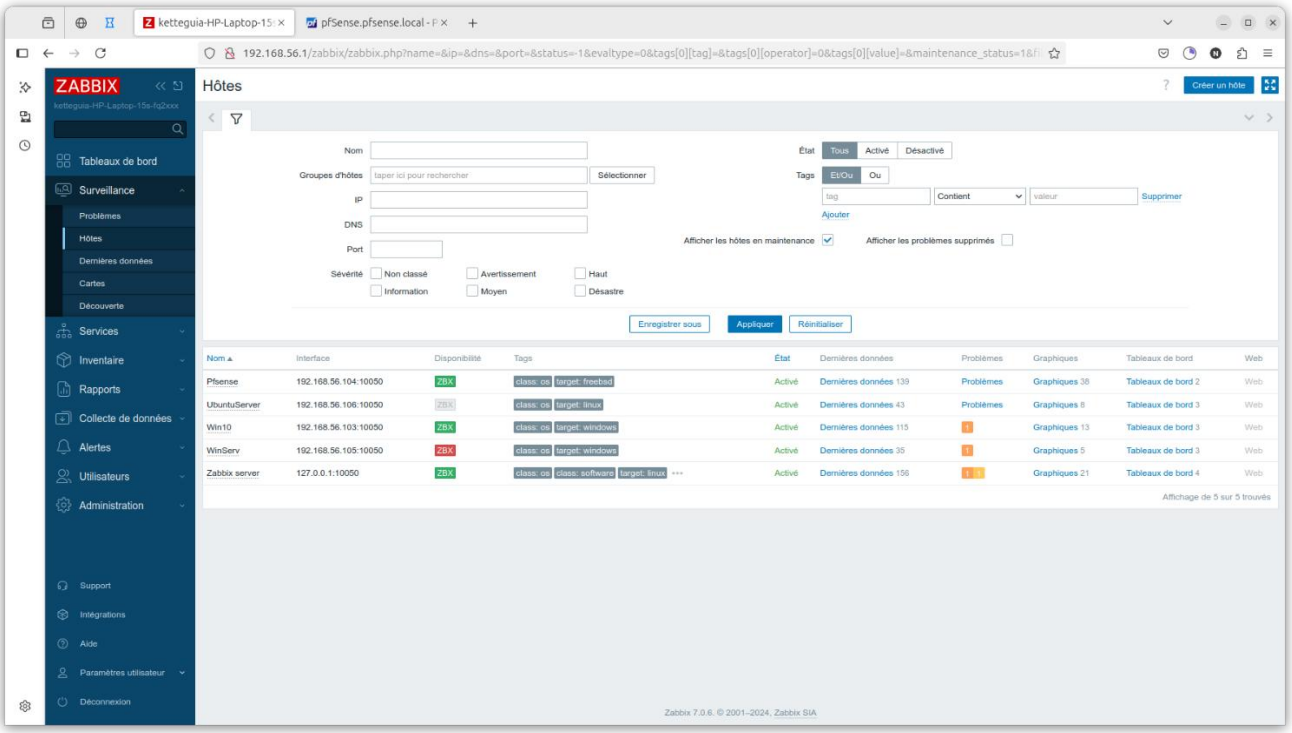
- L’état des ressources : Utilisation du CPU, mémoire, espace disque, etc.
- Les tendances d’utilisation : Analyse des périodes de forte sollicitation ou des anomalies dans le trafic réseau.
- Les alertes critiques : Mise en évidence des incidents nécessitant une intervention immédiate.
- Les données sur le trafic réseau : Identification des applications gourmandes en bande passante ou détection des activités suspectes.

Ces outils permettent aux administrateurs d’anticiper les besoins, d’optimiser les ressources disponibles et de renforcer la sécurité globale des infrastructures.

1.4. Notions clés : métriques, événements, alertes, tableaux de bord

Pour bien comprendre la supervision informatique, il est important de connaître les notions clés suivantes :

- **Métriques :** Ce sont les données brutes que l'on collecte sur le système ou l'application que l'on surveille. Il peut s'agir de valeurs numériques (par exemple, utilisation du CPU, latence, nombre de requêtes) ou d'indicateurs d'état (par exemple, "en ligne", "hors ligne").
- **Événements :** Ce sont des occurrences spécifiques qui se produisent dans le système, souvent liées à un changement d'état ou à une action. Par exemple, un serveur qui démarre, une base de données qui se connecte, une erreur qui se produit.
- **Alertes :** Ce sont des notifications qui sont déclenchées lorsqu'une métrique dépasse un certain seuil ou lorsqu'un événement spécifique se produit. Les alertes permettent d'être informé rapidement des problèmes et de prendre des mesures correctives.
- **Tableaux de bord :** Ce sont des interfaces graphiques qui permettent de visualiser les métriques et les événements de manière claire et concise. Les tableaux de bord sont personnalisables et peuvent être adaptés aux besoins spécifiques de chaque utilisateur.



Exemple d'un tableau de bord d'un outils de monitoring

2. Principes fondamentaux de la supervision

Le monitoring réseau repose sur un processus continu et structuré, une boucle itérative qui assure la disponibilité, la performance et la sécurité de l'infrastructure. Ce processus cyclique se déploie en cinq étapes clés, chacune contribuant à une vision globale et dynamique de l'état du réseau.

2.1. La collecte des données

La collecte de données constitue la pierre angulaire du monitoring. Elle vise à recueillir un ensemble riche et diversifié d'informations sur les équipements, services et protocole réseau, dressant ainsi un portrait précis de leur état et de leur comportement. Les données collectées se présentent sous différentes formes :

- **Métriques** : Les indicateurs quantifiables, le pouls du réseau : Ces indicateurs mesurables, tels que l'utilisation du CPU, de la mémoire ou de la bande passante, fournissent des données chiffrées sur l'activité des ressources. Ils permettent de quantifier l'utilisation des ressources et

de détecter les variations significatives.

- **Logs** : La mémoire du système, le journal de bord des événements : L'historique des événements et activités, consigné dans les logs, offre une trace précieuse des opérations passées. Ils permettent de reconstituer le déroulement des événements et d'identifier les causes potentielles des problèmes.
- **Événements** : Les signaux d'alerte, les changements d'état significatifs : Les changements d'état spécifiques ou les actions déclenchées, tels que le démarrage ou l'arrêt d'un service, constituent des événements importants à surveiller. Ils signalent des modifications dans l'état du système et peuvent indiquer des anomalies.
- **Tests actifs (ou Tests de performance synthétiques**) : Les simulations contrôlées, la mise à l'épreuve des services : Ces simulations, conçues pour évaluer les performances des services dans des conditions contrôlées, permettent d'anticiper les problèmes de performance en simulant des charges et des scénarios d'utilisation.

Pour collecter ces données, diverses méthodes sont employées, parmi lesquelles : SNMP, ICMP, les agents logiciels déployés sur les machines, les protocoles de flux NetFlow/sFlow et les API permettant une intégration avec d'autres systèmes.

2.2. Analyse et corrélation : Comprendre pour agir, transformer les données en information

Les données collectées ne sont que des chiffres bruts ; c'est l'analyse qui leur donne un sens. Cette étape cruciale vise à transformer ces données en information exploitable, permettant d'identifier les tendances, les anomalies et les problèmes potentiels. L'analyse s'articule autour de plusieurs axes :

- Comparaison avec des seuils prédéfinis : La surveillance des limites, le contrôle des paramètres vitaux. La comparaison des métriques avec des seuils prédéfinis permet de détecter les dépassements et de déclencher des alertes en cas d'anomalie.
- Analyse des tendances pour anticiper les besoins : L'analyse des tendances à long terme permet d'anticiper les besoins en ressources et de planifier les évolutions de l'infrastructure.
- Corrélation d'événements pour déterminer les causes racines des incidents : La corrélation d'événements provenant de différentes sources permet de reconstituer le fil des événements et d'identifier les causes racines des incidents.
- Utilisation de techniques avancées (IA, apprentissage automatique) pour détecter les anomalies complexes : L'utilisation de techniques avancées, telles que l'intelligence artificielle et l'apprentissage automatique, permet de détecter des anomalies complexes et subtiles qui pourraient échapper à une analyse manuelle.

2.3. Alertes et notifications : Informer pour réagir, la communication des anomalies

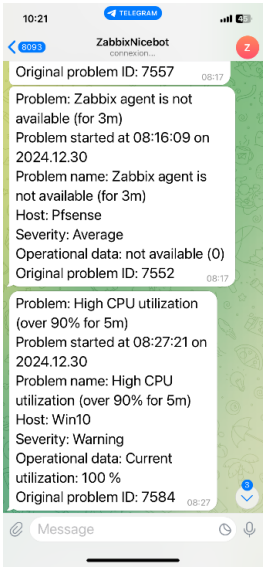
Lorsqu'une anomalie est détectée, le système de monitoring génère des alertes, classées selon leur criticité, afin de garantir une réponse appropriée :

- **Informationnel** : Ce niveau d'alerte fournit une simple notification d'un événement, sans nécessiter d'action immédiate.

- **Avertissement** : Ce niveau signale un problème potentiel qui nécessite une surveillance accrue.
- **Mineur(Moyen)** : Ce niveau indique un incident affectant les performances ou la disponibilité, mais sans interruption majeure.
- **Majeur(Haut)** : Ce niveau signale un incident important nécessitant une intervention rapide pour éviter une interruption de service.
- **Critique(Desastre)** : Ce niveau indique un incident majeur nécessitant une intervention immédiate pour rétablir le service.

Diagramme illustrant les niveaux de criticité des alertes, allant d'Informationnel (niveau le plus bas) à Critique (niveau le plus élevé), avec des exemples d'incidents pour chaque niveau.

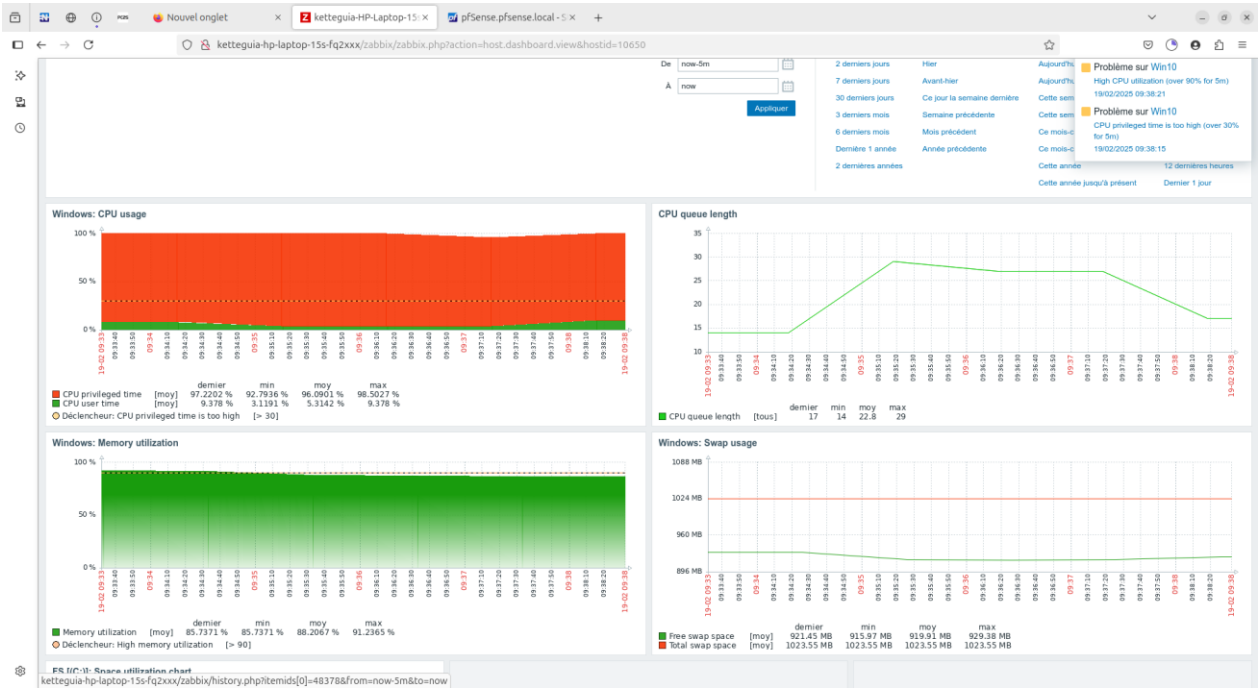
Ces alertes sont diffusées via divers canaux, tels que l'email, les SMS ou les notifications push, pour garantir une communication rapide et efficace aux équipes concernées.



[Image: Capture d'écran d'un smartphone affichant une alerte de supervision reçue par application de messagerie Telegram , indiquant le type d'alerte, l'équipement concerné et le niveau de criticité.]

2.4. Visualisation et reporting : Voir pour comprendre, transformer les données en connaissance

Les tableaux de bord et les graphiques offrent une vue d'ensemble claire et concise de l'état du réseau, transformant des données complexes en informations facilement compréhensibles. Les rapports, quant à eux, permettent d'identifier les tendances sur le long terme et d'évaluer l'efficacité des actions entreprises.



[Image: Exemple de tableau de bord de supervision affichant des graphiques de performance réseau (utilisation CPU, mémoire, trafic réseau, etc.) et des indicateurs clés (nombre d'alertes, disponibilité des services, etc.).]

2.5. Action et remédiation : Résoudre et prévenir, boucler la boucle du monitoring

Enfin, la dernière étape consiste à traiter les problèmes détectés. Cette étape cruciale boucle la boucle du monitoring et assure l'amélioration continue de l'infrastructure :

- **Interventions manuelles** : L'expertise humaine, l'action ciblée : Les interventions manuelles permettent aux administrateurs de prendre des actions correctives ciblées en fonction de la nature

de l'incident.

- **Automatisation** : L'automatisation des réponses aux alertes, par le biais de redémarrages automatiques, de basculements vers des systèmes de secours ou de sauvegardes, permet de minimiser les temps d'arrêt et de garantir la continuité de service.

[Capture d'écran d'un script d'automatisation (PowerShell, Bash, Python, etc.) illustrant un exemple de remédiation automatique, comme le redémarrage d'un service ou la libération d'espace disque.]

Cette étape s'accompagne d'une analyse approfondie post-incident pour identifier les causes profondes et mettre en place des mesures préventives afin d'éviter la réapparition d'incidents similaires à l'avenir.

3. La norme ISO 7498/4 et Fonctions de la supervision informatique

Le concept de supervision a été normalisé par l'**ISO (International Organisation for Standardisation)**. Voici les différentes fonctions qui ont été défini par l'**ISO 7498/4**[3] :

2.1. Gestion des performances (Performance Management)

Elle permet d'évaluer les performances des ressources (et la disponibilité) du réseau et de ses composants. Les performances du réseau sont évaluées à l'aide de quatre paramètres :

- Le temps de réponse.
- Le débit.
- Le taux d'erreur.
- La disponibilité (en termes de temps).

Le traitement des statiques se déroule en quatre étapes :

- La collecte.
- Le contrôle.
- La présentation des informations.
- L'archivage.

La gestion des performances comprend les procédures de collecte de données et de statistiques. Elle doit aboutir à l'établissement de tableaux de bord. Les informations recueillies doivent aussi permettre de planifier les évolutions du réseau.

[Image: Diagramme illustrant le cycle de la gestion des performances selon la norme ISO 7498/4 : Collecte, Contrôle, Présentation, Archivage, avec des flèches indiquant le flux cyclique.]

2.2. Gestion des configurations (Configuration Management)

La gestion des configurations représente l'inventaire des ressources nécessaire au fonctionnement du réseau, dont on peut identifier, paramétrer et contrôler ce qui suit :

- Le plan d'adressage et de routage IP du réseau, ou les objets de chaque couche sont concernés.
- Une éventuelle limitation du nombre de sessions applicatives simultanément établies.
- L'état du système : charge CPU ou mémoire, paramètres d'environnement (température dans le boitier ou la consommation électrique d'un appareil).

[Image: Exemple d'interface d'un outil de gestion de configuration, montrant un inventaire des équipements réseau et leurs configurations.]

2.3. Gestion de la comptabilité (Accounting Management)

Cette gestion a pour mission de relever les informations permettant d'évaluer le cout d'usage d'une ressource. Cette mesure tient compte de deux paramètres essentiels :

- Du temps d'utilisation.
- Du volume d'information échangé.

De plus, la gestion de la comptabilité autorise la mise en place de systèmes de facturation en fonction de l'utilisation pour chaque utilisateur.

[Image: Exemple de rapport de comptabilité montrant l'utilisation des ressources réseau par utilisateur ou par service (temps de connexion, volume de données transférées, etc.).]

2.4. Gestion des incidents (Fault Management)

Elle permet de nous informer des événements qui peuvent perturber le fonctionnement du réseau, on distingue deux types de défauts :

- Les défauts internes résultat d'une panne de l'élément actif lui-même.
- Les défauts externes indépendants des appareils eux-mêmes, mais liés à l'environnement propre du réseau.

Le traitement d'une panne est composé de quatre étapes :

- La signalisation du fonctionnement anormal d'un élément actif ou d'un lien inter-réseau.
- La localisation du défaut sur l'infrastructure.
- La réparation.
- La confirmation du retour à un comportement normal du réseau.

L'historisation des incidents peut aider le technicien ou l'ingénieur dans la compréhension de dysfonctionnement du réseau.[7]

[Image: Diagramme illustrant le processus de gestion des incidents : Signalisation, Localisation, Réparation, Confirmation, avec des flèches indiquant le flux des étapes.]

2.5. Gestion de la sécurité (Security Management)

La gestion de la sécurité contrôle l'accès aux ressources en fonction des politiques de droits d'utilisation établies. Elle veille à ce que les utilisateurs non autorisés ne puissent accéder à certaines ressources protégées. Elle permet aussi d'éviter toute perturbation du service et dégradation des performances. Elle a également pour rôle de mettre en application les politiques de sécurité.

[Image: Schéma illustrant les aspects de la gestion de la sécurité : Contrôle d'accès, Politiques de sécurité, Détection d'intrusion, Protection contre les menaces, avec des icônes représentant chaque aspect.]

2.6. Gestion des SLA

SLA (Service-Level Agreement) ou **accord de niveau de service**, est un contrat passé entre un fournisseur de service et ses clients internes ou externes. Les fournisseurs de services réseau sont à l'origine des SLA. Un service IT met au point un SLA afin que ses prestations puissent être mesurées, justifiées, voire comparées à celles de fournisseurs extérieurs. Les SLA mesurent les performances et la qualité du fournisseur de services de différentes manières. Ainsi, un SLA peut spécifier les éléments de mesure ou indicateurs suivants :

- Disponibilité des services.
- Nombre d'utilisateurs pouvant être pris en charge simultanément.
- Bancs d'essai de performances spécifiques à l'une desquelles sont mesurées périodiquement les performances réelles.
- Temps de réponse des applications.
- Calendrier des notifications préalables des modifications du réseau susceptibles d'affecter les utilisateurs.
- Délai de réponse du service d'assistance pour différentes catégories de problèmes.
- Statistiques d'utilisation mises à disposition.

[Image: Exemple de tableau de bord ou rapport illustrant le suivi des indicateurs clés d'un SLA (disponibilité, temps de réponse, etc.).]

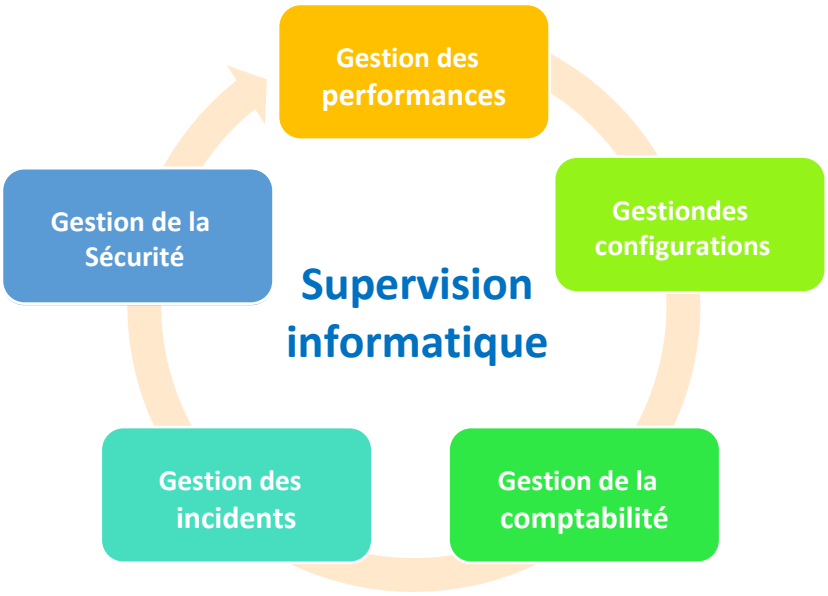


Schéma illustrant le cycle de monitoring définit par l'OSI

4. Méthodes de vérification

Il existe 2 méthodes de vérification pour une solution de supervision, soit active ou passive :

- **Méthode Active :** Dans cette méthode, c'est le serveur de supervision qui interroge à intervalles réguliers les composants à surveiller. Cette méthode est la plus utilisée et a l'avantage d'être fiable, les vérifications se font de manière régulière et en mode question-réponse.

[Image: Schéma illustrant la méthode de supervision active. Un serveur de supervision envoie des requêtes à des équipements réseau (serveur, routeur, switch) et reçoit des réponses. Les flèches indiquent le flux de requêtes et de réponses.]

- **Méthode Passive :** Cette méthode de vérification est l'exact inverse de la précédente. Ici, ce sont les composants surveillés qui envoient à intervalles réguliers (ou non) métriques et messages vers une instance centrale de supervision. Cette dernière peut être plus facilement tolérée par les responsables de la sécurité du système d'information étant donné qu'il s'agit

[Image: Schéma illustrant la méthode de supervision passive. Des équipements réseau (serveur, routeur, switch) envoient des métriques et messages à un serveur de supervision. Les flèches indiquent le flux d'informations des équipements vers le serveur.]

5. Protocoles de supervision

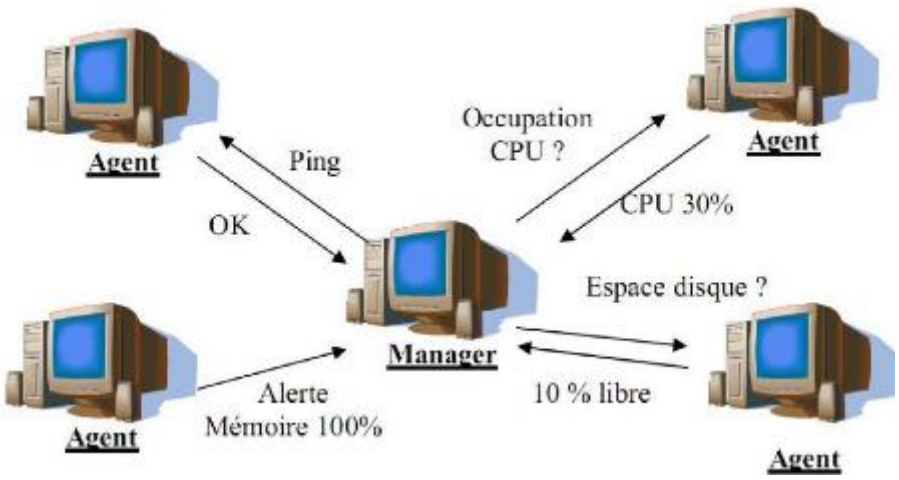
Les protocoles de monitoring sont **Les fondations de la surveillance réseau**. Ils sont essentiels pour la communication entre les outils de supervision et les éléments de l'infrastructure à surveiller. Ils définissent les règles et les formats d'échange des données, permettant ainsi la collecte d'informations cruciales sur l'état, les performances et la sécurité du réseau. Cette section détaille les protocoles les plus importants :

5.1. Protocole SNMP

Le **Simple Network Management Protocol (SNMP)** est un protocole de communication permettant aux administrateurs de surveiller et de gérer les équipements réseau en temps réel. Il est largement utilisé pour détecter les problèmes réseau et superviser les performances des équipements (routeurs, commutateurs, serveurs, imprimantes, etc.).

SNMP fonctionne sur la **couche application (couche 7 du modèle OSI)** et repose sur une **architecture client-serveur** :

- **Manager SNMP (client) / Station de supervision (NMS - Network Management System) :** Le Manager SNMP, souvent appelé Station de supervision ou NMS (Network Management System), joue le rôle de client dans l'architecture SNMP. Sa fonction principale est d'initier la communication au sein du réseau supervisé. En tant qu'initiateur, il envoie activement des requêtes vers les équipements du réseau, qu'on appelle Agents, afin de recueillir des informations cruciales sur leur état de fonctionnement et leurs performances. Ces requêtes sont conçues pour obtenir des détails spécifiques, allant du volume de trafic réseau transitant par un routeur à l'état opérationnel d'une interface réseau ou encore au niveau d'utilisation de la mémoire d'un serveur. En retour, le Manager SNMP reçoit les réponses des Agents, contenant les données sollicitées. Pour faciliter la gestion du réseau, le Manager SNMP est doté d'une interface utilisateur graphique. Cette interface offre aux administrateurs une vue d'ensemble en temps réel de l'infrastructure réseau, englobant routeurs, commutateurs, serveurs et autres équipements supervisés. Elle permet de visualiser les données collectées sous diverses formes, telles que des graphiques et des tableaux de bord, facilitant ainsi l'analyse et la compréhension de l'état du réseau. De plus, cette interface peut, dans une certaine mesure et avec prudence, permettre la configuration centralisée de certains paramètres des équipements. Un aspect essentiel du Manager SNMP est son système d'alerte intégré. Il est conçu pour détecter automatiquement les anomalies et les problèmes au sein du réseau. En cas de dysfonctionnement, de dépassement de seuil de performance ou de tout autre événement critique, le Manager SNMP a la capacité d'alerter l'administrateur réseau de diverses manières, notamment par SMS, e-mail ou notifications visuelles et sonores. Ce mécanisme d'alerte rapide est crucial pour permettre une intervention rapide et efficace, minimisant ainsi l'impact des incidents sur le réseau et ses utilisateurs. En résumé, le Manager SNMP est le véritable centre névralgique de la supervision SNMP, orchestrant la collecte d'informations, leur présentation à l'administrateur et le déclenchement d'alertes en cas de problèmes.



- **Agent SNMP (serveur) / Nœuds gérés :**

  L'Agent SNMP, désigné également comme Nœud géré, représente la composante serveur du modèle SNMP. Il s'agit d'un logiciel spécifique qui doit être installé sur chaque équipement du réseau que l'on souhaite intégrer au système de supervision. Une fois en place, l'Agent SNMP assume la responsabilité de la collecte continue d'informations sur l'équipement hôte. Cette collecte englobe un large éventail de données, allant de l'état général de l'équipement, incluant la détection d'éventuelles erreurs de fonctionnement, jusqu'à la surveillance des performances, telles que l'utilisation du processeur et de la mémoire, ainsi que le volume de trafic réseau. L'Agent SNMP est également capable de fournir des informations relatives à la configuration de l'équipement, comme les paramètres des interfaces réseau et les adresses IP. En réponse aux requêtes initiées par le Manager SNMP, l'Agent SNMP joue un rôle réactif. Lorsqu'il reçoit une question du Manager, il interroge sa propre base de données locale, appelée MIB (Management Information Base). La MIB sert de référentiel structuré pour toutes les informations que l'Agent est en mesure de fournir sur l'équipement. Après avoir consulté la MIB, l'Agent SNMP élabore une réponse au format SNMP et la transmet au Manager, incluant les données demandées. Au-delà de sa fonction de réponse aux requêtes, l'Agent SNMP possède une capacité proactive d'alerte. En effet, il peut envoyer de manière spontanée des notifications, appelées Traps, au Manager SNMP, sans y avoir été invité au préalable. Ces Traps sont déclenchées lorsqu'un événement jugé important survient sur l'équipement supervisé. Parmi ces événements, on peut citer les pannes d'interfaces réseau, les dépassements de seuils d'utilisation des ressources système, les problèmes de sécurité ou encore les redémarrages inattendus de l'équipement. En conclusion, l'Agent SNMP agit comme les capteurs et les transmetteurs d'informations pour le Manager au sein de chaque équipement réseau. Il assure une surveillance constante, répond aux interrogations du Manager et signale de manière proactive les incidents potentiels**.**

Figure II.3 : Implémentation IP typique

Les concepts clés de SNMP sont :

MIB (Management Information Base) :

La MIB, ou Management Information Base, constitue une base de données hiérarchique d'une importance capitale au sein du protocole SNMP. Elle se présente comme un inventaire exhaustif et structuré qui décrit l'ensemble des objets gérés par SNMP. Cette base de données, intrinsèquement liée à chaque équipement administrable, réside au cœur même de celui-ci. Elle recense de manière précise et détaillée toutes les informations pertinentes relatives à l'équipement réseau en question. Grâce à la MIB, il devient possible pour un administrateur de réseau de connaître avec exactitude l'ensemble des données et paramètres que possède un équipement, offrant ainsi une visibilité complète et essentielle pour optimiser la gestion de son fonctionnement.

La structure de la MIB repose sur un concept arborescent, rappelant l'organisation d'un arbre généalogique. Dans cette architecture, chaque chemin au sein de l'arbre permet d'accéder à une information spécifique, désignée sous le terme d'OID, ou Object Identifier. Chaque OID est représenté par une suite de nombres entiers, séparés par des points, suivant les recommandations établies par l'Union Internationale des Télécommunications. Chacun des nœuds qui composent cet arbre représente un objet géré distinct. Au sein de la MIB, il est pertinent de distinguer deux sections principales : une partie standard, qui se veut commune à l'ensemble des équipements réseau, et une partie privée, qui est spécifique à un équipement particulier, voire à un constructeur.

Afin d'illustrer concrètement le concept d'OID, prenons un exemple simple. Si l'on souhaite accéder, par le biais d'une requête SNMP, à un objet de gestion spécifique, son OID pourra être exprimé sous deux formes : une forme numérique, telle que 1.3.6.1.2.NumObjet, ou une forme textuelle, plus lisible, comme iso.org.dod.internet.mgmt.NomObjet. Chaque objet géré au sein de la MIB est donc rigoureusement identifié par un OID unique. Il est important de noter que les MIB standardisées sont définies et maintenues par des organismes de normalisation reconnus, tel que l'IETF (Internet Engineering Task Force). Cependant, les constructeurs d'équipements réseau ont également la possibilité de définir leurs propres MIB privées. Ces MIB privées sont conçues pour permettre la gestion des fonctionnalités qui sont spécifiques à leurs équipements et qui ne sont pas couvertes par les MIB standard.

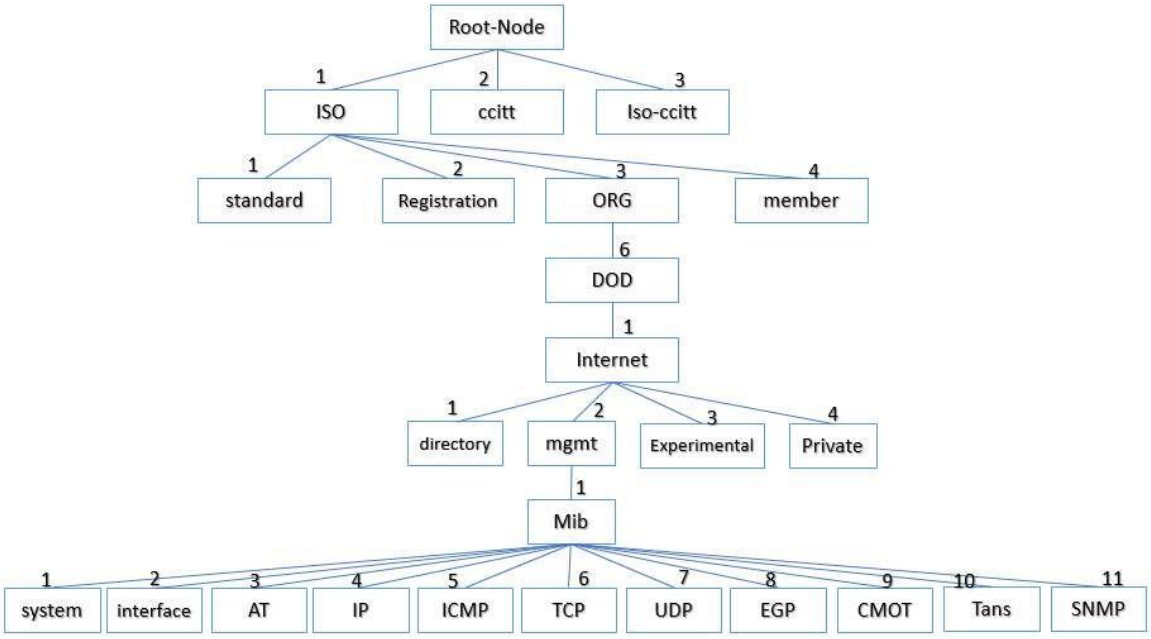
Pour mieux appréhender la richesse d'informations contenues dans la MIB, il est utile de citer quelques exemples de branches principales et d'objets gérés associés :

- La branche System est dédiée à la description du système de toutes les entités gérées. Elle englobe des objets tels que sysUpTime, qui indique la durée écoulée depuis le dernier démarrage de l'équipement.
- La branche Interfaces concerne les interfaces de données, qu'elles soient dynamiques ou statiques. Parmi les objets gérés dans cette branche, on retrouve ifNumber, qui fournit le nombre d'interfaces réseau présentes sur l'équipement.
- La branche At (adresse translation) contient la table de correspondance entre les adresses IP et les adresses MAC.
- La branche IP regroupe les statistiques relatives au protocole IP, l'adresse cache et la table de routage. Un exemple d'objet géré dans cette branche est ipInReceives, qui comptabilise

le nombre de datagrammes IP reçus.

- La branche Icmp est dédiée aux statistiques du protocole ICMP. On y trouve notamment l'objet icmpInEchos, qui enregistre le nombre de demandes d'écho ICMP reçues.
- La branche Tcp concerne les paramètres TCP, les statistiques et la table de connexion. L'objet tcpInSegs, qui indique le nombre de segments TCP reçus, en est un exemple.
- La branche Udp regroupe les statistiques UDP, avec par exemple l'objet udpInDatagrams, qui comptabilise le nombre de datagrammes UDP reçus.
- La branche Egp est dédiée aux statistiques relatives au protocole de routage EGP et à la table d'accessibilité.
- Enfin, la branche Snmp contient les statistiques propres au protocole SNMP lui-même.

Il est important de souligner qu'en complément du standard MIB, qui définit les informations d'administration réseau disponibles sur un équipement, il existe également un standard indépendant, nommé SMI (Structure of Management Information). Le SMI normalise les règles et les conventions à utiliser pour définir et identifier les variables au sein des MIB, assurant ainsi une cohérence et une interopérabilité entre les différentes MIB et les équipements SNMP.



- **Communauté :** SNMP définit la notion **communauté** qui représente l'association Agent/Manager, chaque communauté est identifiée par un **nom de communauté**, ce nom est envoyé avec le message SNMP qui fonctionne comme un mot de passe pour l'accès en lecture seule, ou en lecture et écriture (c'est le contrôle d'accès utilisée par SNMP) à la MIB. Le nom est transmis en claire donc ce mode d'authentification est faible. Les noms de communauté par défaut sont : **Public** pour lecture seule et **Private** pour lecture et écriture.

Versions de SNMP :

- **SNMPv1 :** La première version du protocole, cette version a un défaut majeur qui est le

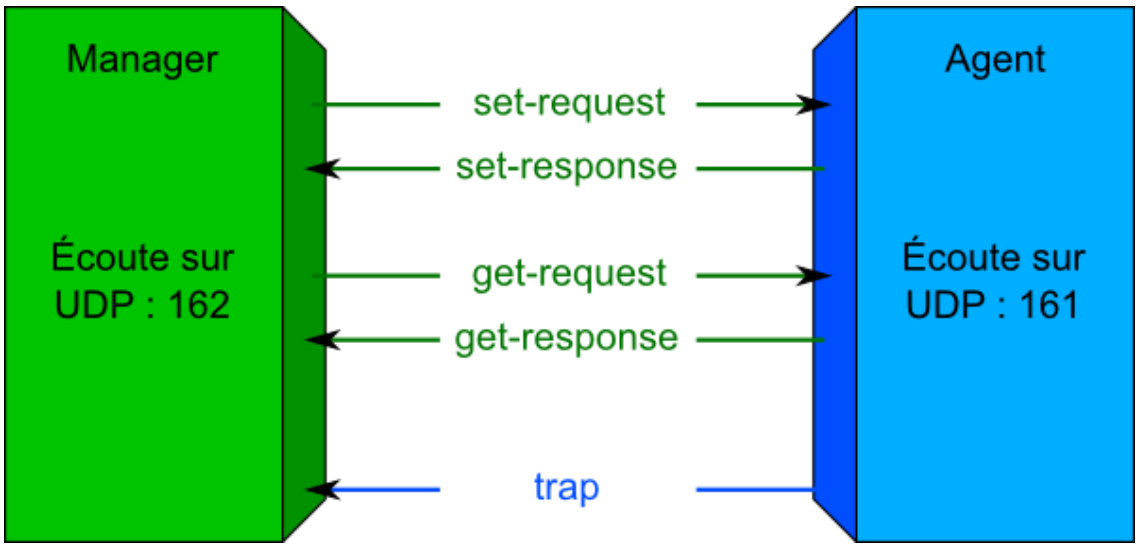
problème de sécurité car la seule vérification est basée sur une chaine de caractère appelée communauté. **SNMPsec :** le but de cette version est de sécuriser le protocole SNMP v1. Le format générique d'un message SNMP v1 est composé de : **Version** (numéro de version SNMP utilisée : 0 : SNMP v1, 2 : SNMP v2, 3 : SNMP v3), **Communauté** (nom de communauté de lecture seule (RO) ou lecture/écriture (RW) défini par l'administrateur), **Type PDU** (décrit le type de message - Tableau II-1: Type de Message pour chaque Type de PDU - GetRequest, GetNextRequest, SetRequest, GetReponse), **ID Request** (utilisé pour la vérification de l'association entre les réponses et les requêtes), **Statut Erreur** (pour signaler une erreur, zéro si pas d'erreur), **Indice Erreur** (spécifie la source d'erreur dans la requête - La position d'erreur), **OID** (Indicateur de chaque variable), **Valeur** (ce champ émis par le manager pour le but de la mise à jour de la MIB, la valeur dépend du type de PDU).

- **SNMPv2c :** Une version améliorée avec une meilleure gestion des erreurs et des types de données. Cette version est une mise à jour de SNMP v1 pour but d'amélioration des opérations du protocole. Les principales améliorations sont de définir des nouveaux objets, le principal changement est l'ajout de nouvelles méthodes **GetBulk** et **InformRequest**. **GetBulk :** cette requête permet au superviseur de récupérer les données de grande taille à la fois pour but de minimiser le nombre d'échange. **InformRequest :** cette requête confirme la réception d'un TRAP et grâce à celle-ci, la station de supervision peut envoyer une alarme à une autre station de supervision.
- **SNMPv3 :** La version la plus récente et la plus sécurisée, avec des mécanismes d'authentification et de chiffrement. SNMP v3 est La dernière version du protocole SNMP, cette version sert à améliorer la sécurité et la confidentialité des informations. Il est fortement recommandé d'utiliser SNMPv3 pour des raisons de sécurité.

Opérations SNMP : La simplicité de communication entre la station de supervision et les agents est illustrée par les messages SNMP, trois grands types d'opérations sont réalisables : **Get** pour la lecture, **Set** pour l'écriture, **Trap** pour les messages d'alertes. Le protocole SNMP prend en charge ces types de messages :

- **Message GetRequest :** Le manager demande la valeur d'un OID spécifique à l'agent. Ce message permet au manager d'interroger un agent pour récupérer une variable d'un objet de la MIB contenu sur l'équipement à gérer. L'attribut OID passé en paramètre.
- **Message GetNextRequest :** Le manager demande la valeur de l'OID suivant dans la MIB (utile pour parcourir les tables). Ce message est identique au message précédent, la différence étant que le message GetNextRequest demande la valeur de l'objet suivant dans l'arbre d'objets.
- **Message GetReponse :** En termes de réponse, ce message envoyé par l'agent au manager pour répondre aux messages GetRequest, GetNextRequest et SetRequest. Si l'information demandée n'est pas disponible les réponses sont **No such object, No access, No writable**.
- **Message SetRequest :** Le manager modifie la valeur d'un OID sur l'agent (utilisé pour la configuration, mais avec prudence). Le message SetRequest permet au superviseur de mettre à jour, ou modifier la valeur d'une variable par une valeur donnée en paramètre sur un agent SNMP.
- **Message TRAP (ou InformRequest en SNMPv2c et v3) :** L'agent envoie une notification asynchrone au manager en cas d'événement (par exemple, un changement d'état d'une interface, un dépassement de seuil). Les InformRequest garantissent la réception de la notification par le manager. Contrairement à tous les autres messages, les traps sont envoyées

par l'agent SNMP vers la station de supervision pour signaler un fonctionnement anormal, un changement d'état, un événement non attendu se produit. Il s'agit d'un mécanisme d'alarme, Il y a 7 types de messages TRAPS : **coldStart, WaemStart, LinkDown, LinkUp, AuthentificationFailure, egpNeighborLoss, entrepriseSpecific**.



5.2. ICMP (Internet Control Message Protocol) :

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.

[Image: Capture d'écran de la commande 'ping' en ligne de commande, montrant l'envoi de requêtes et la réception de réponses, ainsi que les statistiques (perte de paquets, temps de réponse).]

- **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.

[Image: Capture d'écran de la commande 'traceroute' (ou 'tracert') en ligne de commande, montrant la liste des routeurs traversés pour atteindre une destination, avec les temps de réponse pour chaque routeur.]

5.3. 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.
- **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 :

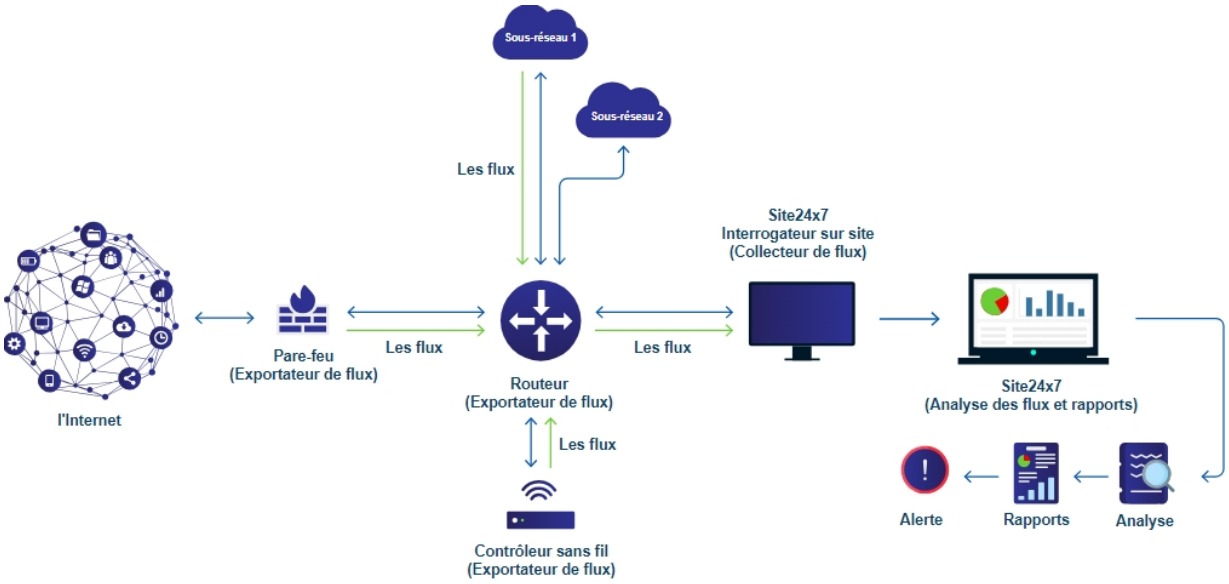
- Adresse IP source et destination.
- Ports source et destination.
- Protocole utilisé (TCP, UDP, etc.).
- Volume de trafic (octets, paquets).
- Durée du flux.
- Interfaces d'entrée et de sortie.
- **ToS (Type of Service) ou DSCP (Differentiated Services Code Point) :** Pour l'analyse de la qualité de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

[Image: Graphique (type "camembert" ou "histogramme") illustrant la répartition du trafic réseau par application ou par protocole, basé sur des données NetFlow/sFlow/IPFIX.]

s



5.4. 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.

Avantages :

- Collecte de métriques plus complexes, non disponibles via SNMP (par exemple, les performances d'une application, l'utilisation des ressources par un processus spécifique, les logs applicatifs).
- Surveillance de l'état des services et des processus.
- Exécution de scripts locaux pour collecter des données personnalisées ou effectuer des actions.
- Possibilité de collecter et de centraliser des logs.

Inconvénients :

- Nécessitent une installation et une maintenance sur chaque équipement à surveiller.
- Peuvent consommer des ressources système (CPU, mémoire), bien que les agents modernes soient optimisés pour minimiser cet impact.

[Image: Schéma illustrant le déploiement d'agents logiciels sur différents types d'équipements (serveurs, postes de travail, applications). Les agents communiquent avec un serveur de supervision centralisé.]

5.5. (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.

[Image: Diagramme illustrant l'utilisation d'APIs pour l'intégration entre un système de supervision et d'autres outils (gestion des incidents, CMDB, outils d'automatisation, etc.). Les flèches indiquent le flux de données via les APIs.]

5.6. Protocole IPMI

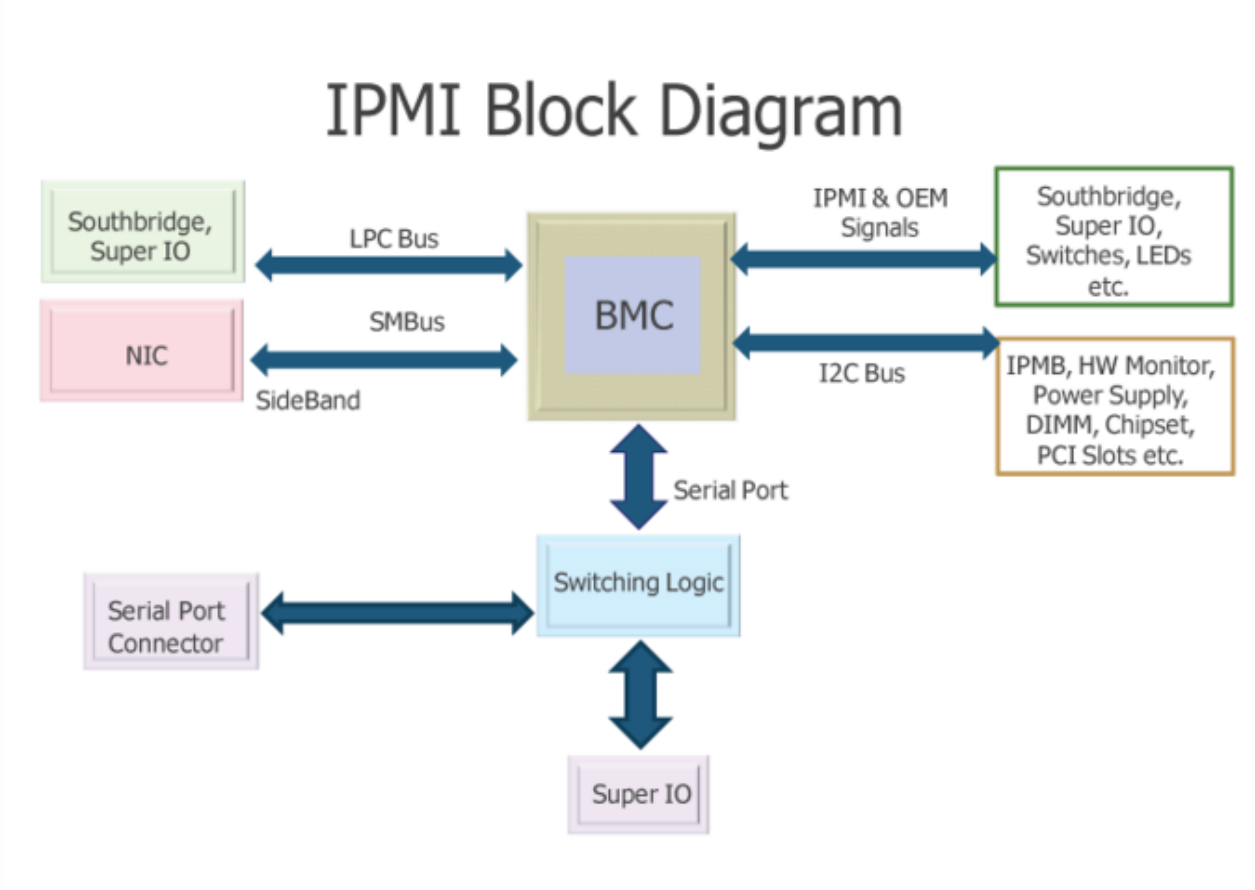
IPMI (Intelligent Platform Management Interface) est une interface ouverte standard, conçue pour la gestion et la maintenance des composants matériels, développée par **Intel, Cisco, Dell, HP**. IPMI offre la possibilité aux administrateurs de superviser l'état de fonctionnement des machines et serveur, la surveillance de températures, alimentation électrique, la tension, ventilateurs. L'IPMI permet d'éteindre, d'allumer ou de redémarrer un ordinateur à distance. L'IPMI permet de gérer le serveur lorsqu'il est éteint, il suffit que le serveur soit connecté au réseau électrique. Il support la journalisation et la documentation d'état, il permet d'accéder et collecter des données indépendamment de son système d'exploitation. IPMI est considéré comme un protocole d'interrogation, il peut fonctionner par l'interrogation ou par recevoir un TRAP, il utilise le port UDP 623.

Composants IPMI :

- **Contrôleur de gestion de la carte mère (BMC) :** Le cœur de l'architecture IPMI est le **BMC**, un microcontrôleur intégré à la carte mère d'un ordinateur ou d'un serveur. Le BMC offre des capacités de gestion à distance et des tâches de surveillance telles que les températures et les tensions, et permet de gérer le fonctionnement du CPU du serveur, au moyen de capteurs (capteurs de température, batterie et processeur), le BMC prend également en charge les fonctions d'alerte et de journalisation. Le **contrôleur de gestion de la carte mère (BMC)** et l'administrateur système communiquent via une connexion indépendante. BMC est alimenté par la tension de garde de la carte mère, c'est-à-dire qu'elle fonctionne toujours, quel que soit l'état du serveur. L'architecture IPMI est conçue de sorte que l'administrateur distant n'a pas un accès direct aux composants du système. Par exemple, pour obtenir des données à partir des capteurs, un administrateur distant envoie une commande à BMC, et BMC se tourne à son tour vers des capteurs.
- **Stockage indépendant de l'énergie :** Le **stockage indépendant de l'énergie** reste disponible même lorsque le processeur d'un serveur se bloque, par exemple via un réseau local ; Il a trois domaines : **Journal des événements système (SEL)**, **Enregistrement des données du capteur (SDR)**, **Unité remplaçable sur site (FRU)**.
- **Structure de commande IPMI :** IPMI envoie des messages en format demande-réponse. Les demandes sont des commandes. Les commandes lancent des actions et fixent des

valeurs. Les messages IPMI contiennent un ensemble de champs de base qui sont les mêmes pour toutes les commandes : **Network Fonction**, **Le champ d'identification demande/réponse**, **ID du demandeur**, **La pièce d'identité du répondeur**, **Commande**, **Données**.

- **Interface d'accès à distance :** Dans la version initiale d'IPMI, la console distante était connectée au BMC via l'interface série. La spécification IPMI v2.0 est basée sur l'utilisation d'une interface LAN. L'interface LAN est fournie via un port réseau BMC dédié avec sa propre adresse IP. Lorsqu'ils sont transmis sur le LAN, les messages IPMI passent par plusieurs étapes d'encapsulation : **paquets de session IPMI**, **RMCP (Remote Management Control Protocol)**, **datagrammes UDP**, **trames Ethernet**. L'interface série pour connecter la console distante au BMC n'est plus utilisée, mais elle est nécessaire pour implémenter deux fonctions : **Partage de port série** et **Série sur LAN (SoL)**.



5.7. Protocole WMI

WMI (Windows Management Instrumentation) est un protocole intégré au système d'exploitation Windows, ce protocole est considéré comme un protocole de supervision qui supporte la surveillance et la gestion des performances des systèmes Windows et permet de collecter des informations localement et à distance.

5.8. Protocole JMX

JMX est l'acronyme de **Java Management Extension**, c'est une technologie qui définit une architecture et une API pour permettre le monitoring des applications java en temps réel.

5.9. Autres protocoles et technologies de monitoring (mention rapide) :

- Syslog : Protocole standard pour la journalisation des événements.
- gRPC (**gRPC Remote Procedure Call**) : Un framework RPC (Remote Procedure Call) moderne et performant, de plus en plus utilisé pour le monitoring et la gestion.

6. Les différents types de monitoring

Le monitoring d'une infrastructure informatique ne se limite pas à une simple observation globale. Pour être efficace, il doit adopter une approche multicouche, en ciblant différents aspects et niveaux de l'infrastructure. Cette section décrit les principaux types de monitoring, chacun apportant une perspective unique et complémentaire.

6.1. Monitoring de l'infrastructure physique (Matériel)

Ce type de monitoring se concentre sur les éléments tangibles de l'infrastructure : les serveurs, les équipements réseau (routeurs, commutateurs, pare-feu), les onduleurs, les baies de stockage, etc. Véritable radiographie du matériel, il a pour mission de prévenir les défaillances et de garantir la disponibilité physique des équipements.

[Image: Photo d'une salle serveur typique, montrant des racks de serveurs, des équipements réseau, des câblages, etc. L'image peut mettre en évidence les différents types d'équipements physiques surveillés.]

Fonctionnement : Des agents logiciels, des sondes ou des capteurs intégrés aux équipements collectent en continu des données sur l'état du matériel. Ces données sont ensuite transmises à un système de supervision qui les analyse et génère des alertes en cas d'anomalie. Les protocoles SNMP et IPMI sont souvent utilisés pour la communication entre les équipements et le système de supervision.

Données surveillées :

- L'état de santé des équipements, tel un bulletin de notes : Allumé/éteint, alimentation électrique stable, ventilateurs en pleine forme...
- La température, véritable baromètre de l'activité : CPU, disques durs, carte mère... Chaque élément est sous surveillance pour éviter la surchauffe.
- L'utilisation des ressources, une gestion optimisée : CPU, mémoire, espace disque... Rien n'est laissé au hasard pour une performance maximale.
- Les disques durs, garants de la sécurité des données : État SMART, taux d'erreurs, espace libre... Une vigilance constante pour prévenir toute catastrophe.

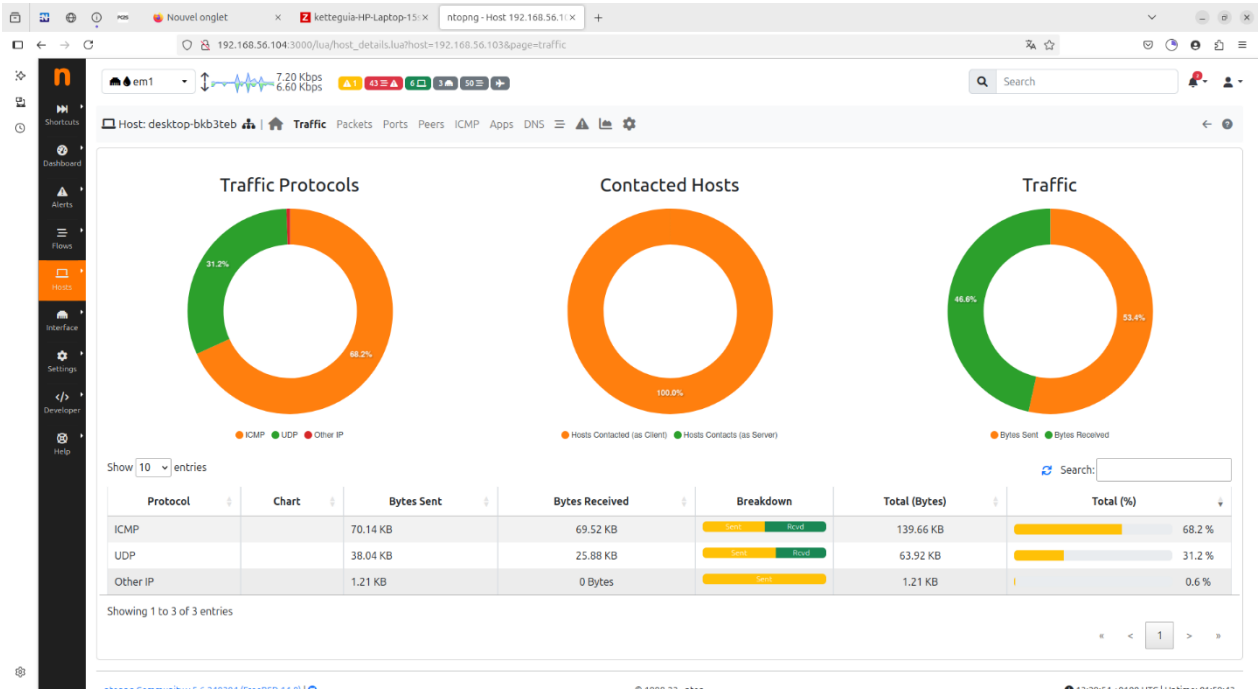
Objectifs :

- Anticiper les pannes matérielles, tel un médecin prévoyant les maux.
- Faciliter la maintenance préventive, pour une infrastructure toujours au meilleur de sa forme.
- Optimiser le cycle de vie du matériel, pour une gestion économique et durable.

6.2. Monitoring réseau : La circulation des données

Le monitoring réseau se concentre sur la danse des données, la connectivité et la performance du réseau. Il permet de comprendre les flux, de déceler les embouteillages et de résoudre les problèmes de connectivité.

[Image: Schéma simplifié d'un réseau informatique, montrant des routeurs, des commutateurs, des serveurs et des clients, avec des flèches indiquant le flux de données. L'image peut illustrer le concept de trafic réseau et de connectivité.]



Fonctionnement : Des équipements réseau (routeurs, commutateurs) collectent des données sur le trafic et les transmettent à un système de supervision. Des outils d'analyse de flux (NetFlow, sFlow, IPFIX) permettent de visualiser et d'analyser le trafic en détail. Des tests de connectivité (ping, traceroute) sont régulièrement effectués pour vérifier la disponibilité des liens.

Données surveillées :

- La bande passante, l'autoroute de l'information : Utilisation, taux d'utilisation des interfaces... Un œil sur le trafic pour éviter les ralentissements.
- La latence, le temps de réponse : Un indicateur clé de la réactivité du réseau.
- La perte de paquets, les données égarées : Un pourcentage à surveiller pour une transmission fiable.
- La gigue, les variations de latence : Un facteur de perturbation pour les applications sensibles.
- Les flux réseau, une analyse approfondie : NetFlow/sFlow pour identifier les sources, les destinations, les protocoles et la consommation de bande passante par application.

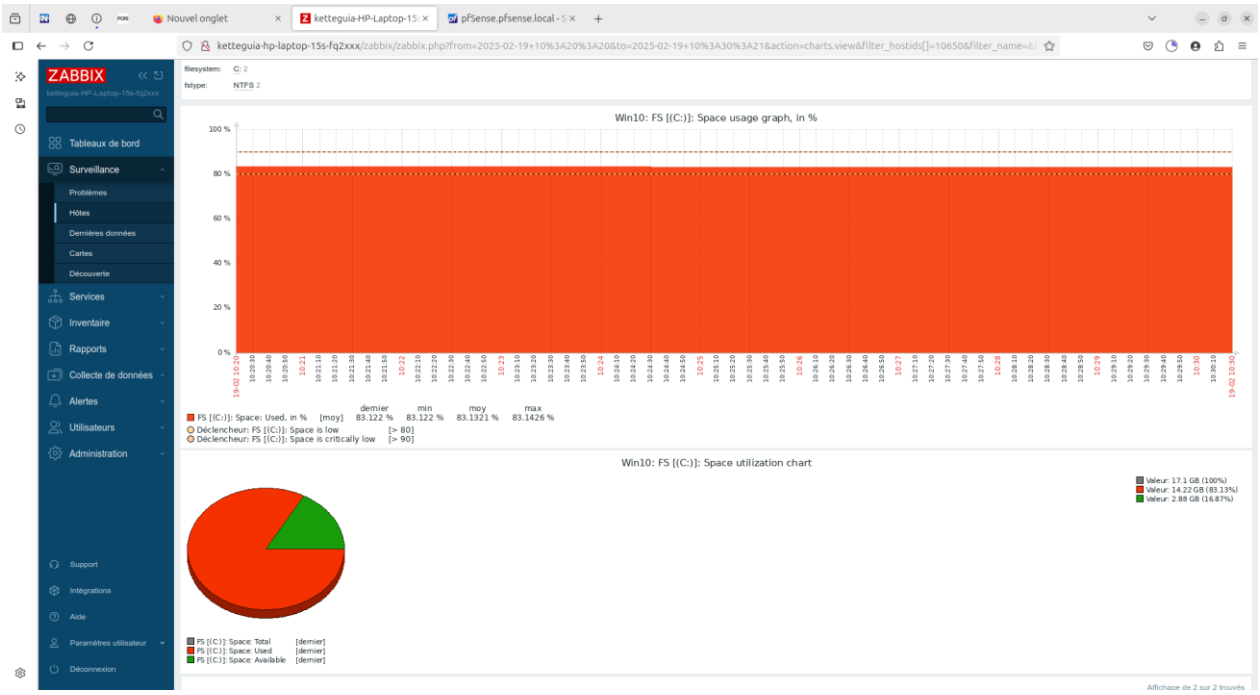
Objectifs :

- Garantir la connectivité et la disponibilité du réseau, tel un fil à la patte.
- Optimiser l'utilisation de la bande passante, pour une efficacité maximale.
- Détecter les attaques réseau (DoS, DDoS, etc.), telles des sentinelles veillant sur la sécurité.

Outils et protocoles : SNMP, ICMP, NetFlow/sFlow, IPFIX... Les outils indispensables pour une surveillance efficace.

6.3. Monitoring système

Le monitoring système se penche sur le fonctionnement des systèmes d'exploitation (OS) qui animent les serveurs et autres équipements. Il veille à l'utilisation optimale des ressources et au bon déroulement des services.



[Image: Capture d'écran d'un moniteur système (type "Task Manager" ou "System Monitor") affichant l'utilisation du CPU, de la mémoire, du disque et du réseau d'un serveur. L'image peut illustrer les types de données surveillées par le monitoring système.]

Fonctionnement : Des agents logiciels installés sur les serveurs collectent des données sur l'utilisation des ressources, les processus en cours d'exécution, l'état des services et les logs système. Ces données sont ensuite transmises à un système de supervision pour analyse et alerte.

Données surveillées :

- L'utilisation des ressources, une répartition équilibrée : CPU, mémoire, espace disque, swap... Chaque élément est scruté pour éviter les surcharges.
- Les processus, les acteurs en coulisse : Processus en cours d'exécution, utilisation des ressources par processus... Un suivi précis de l'activité.
- Les services, les garants de la disponibilité : État des services système (démarré, arrêté, en cours d'exécution)... Une vérification constante pour une continuité de service.

- Les logs système, la mémoire des événements : Logs d'événements du système d'exploitation... Une mine d'informations pour comprendre les incidents.

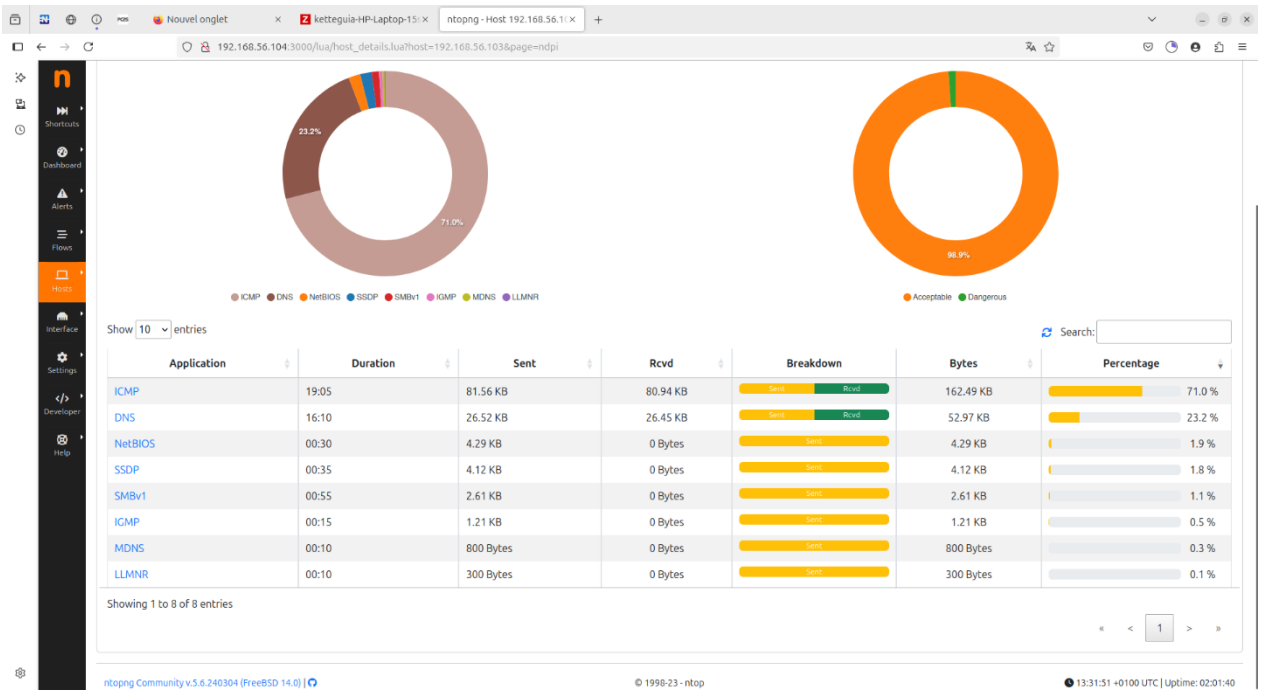
Objectifs :

- Garantir la stabilité et la performance des systèmes d'exploitation, tel un chef d'orchestre veillant à l'harmonie.
- Détecter les erreurs système et les problèmes de configuration, pour une résolution rapide.
- Assurer la sécurité des systèmes, tel un gardien protégeant les accès.

Outils et protocoles : Agents logiciels, SNMP, WMI, Syslog... Les instruments de choix pour une surveillance approfondie.

6.4. Monitoring applicatif et des services

Ce type de monitoring se concentre sur la performance et la disponibilité des applications et des services métiers. Son objectif principal est de garantir une expérience utilisateur optimale et la continuité des activités.



[Image: Schéma illustrant un parcours utilisateur typique à travers une application web (e-commerce, application métier, etc.). L'image peut mettre en évidence les différents points de contrôle du monitoring applicatif : temps de chargement des pages, temps de réponse des API, transactions, etc.]

Fonctionnement : Des agents logiciels, des API ou des scripts personnalisés surveillent les applications et les services. Des tests web (HTTP, HTTPS) sont régulièrement effectués pour vérifier la disponibilité et le temps de réponse des applications. Des outils de suivi des transactions permettent de contrôler le bon déroulement des processus métiers critiques.

Données surveillées :

- La disponibilité des applications, le nerf de la guerre : Temps de réponse, taux d'erreur, uptime... Chaque instant compte pour une expérience sans faille.
- Les performances des applications, un gage de satisfaction : Nombre de requêtes par seconde, temps de traitement des requêtes, utilisation des ressources par application... Une optimisation constante pour une fluidité maximale.
- Les transactions, le cœur de l'activité : Suivi des transactions critiques pour les applications métiers... Une surveillance rapprochée pour éviter toute interruption.
- L'expérience utilisateur, la priorité absolue : Temps de chargement des pages web, temps de réponse des API... Un utilisateur satisfait est un client fidèle.

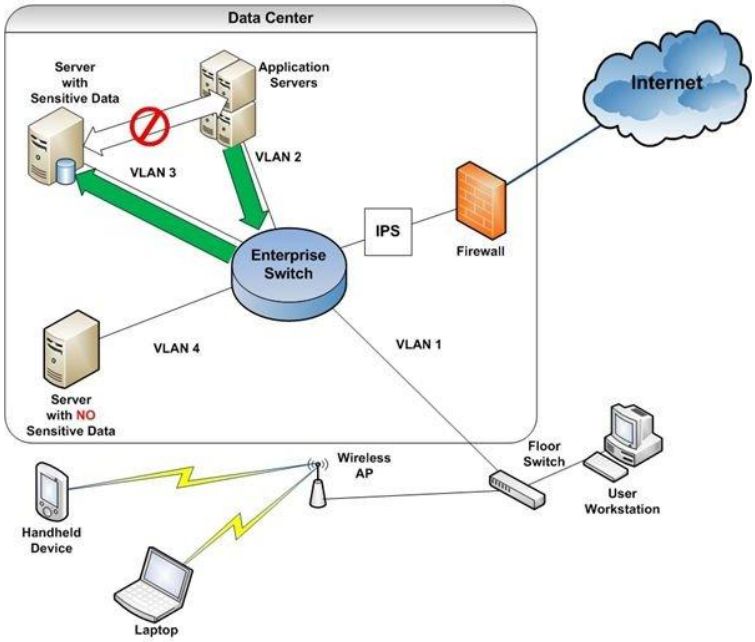
Objectifs :

- Assurer la disponibilité et la performance des applications, tel un maître d'œuvre veillant à la solidité de l'édifice.
- Optimiser l'expérience utilisateur, pour une navigation fluide et agréable.
- Identifier les problèmes applicatifs et les goulots d'étranglement, pour une résolution efficace.

Outils et protocoles : Agents logiciels, API, tests web (HTTP, HTTPS), scripts personnalisés... Les outils adaptés à chaque application.

6.5. Monitoring de sécurité : La protection du système d'information

Le monitoring de sécurité se concentre sur la détection des menaces et des vulnérabilités qui pourraient compromettre la sécurité du système d'information.



[Image: Schéma d'une architecture de sécurité typique, montrant un pare-feu, un système de détection d'intrusion (IDS), un système de gestion des informations et des événements de sécurité (SIEM), etc. L'image peut illustrer les différents composants de sécurité surveillés et le flux des logs de sécurité.]

Fonctionnement : Des outils de sécurité (pare-feu, systèmes de détection d'intrusion, SIEM) collectent des logs de sécurité, des événements et des informations sur les vulnérabilités. Ces données sont analysées pour détecter les intrusions, les attaques et les comportements suspects. Des analyses de vulnérabilités sont régulièrement effectuées pour identifier les faiblesses du système.

Données surveillées :

- Les logs de sécurité, les traces des événements : Logs de pare-feu, logs d'intrusion, logs d'authentification... Une analyse minutieuse pour déceler les anomalies.
- Les événements de sécurité, les signaux d'alerte : Tentatives d'intrusion, accès non autorisés, activités suspectes... Une réactivité indispensable pour contrer les menaces.
- Les vulnérabilités, les points faibles : Présence de failles de sécurité connues... Une identification précoce pour une protection renforcée.

Objectifs :

- Détecter les intrusions et les attaques, tel un chien de garde vigilant.
- Identifier les vulnérabilités du système, pour colmater les brèches.
- Réagir rapidement aux incidents de sécurité, pour minimiser les dégâts.

Outils et protocoles : Syslog, SNMP, NetFlow/sFlow, outils de détection d'intrusion (IDS/IPS), SIEM... L'arsenal complet pour une sécurité optimale.

Conclusion

Chapitre 2 : Présentation des Outils et Solutions de Supervision et choix de la Solution Retenue

1. Introduction

Le rôle de la supervision et son importance sont devenus primordiaux pour les entreprises de toutes tailles. La complexité croissante des infrastructures informatiques, la diversité des applications et la criticité des services exigent une gestion proactive et efficace. La supervision permet de garantir la disponibilité des services, d'optimiser la performance du réseau, de détecter les problèmes de sécurité et de réduire les coûts d'exploitation. Pour atteindre ces objectifs, les entreprises ont besoin d'outils de surveillance de réseau performants et complets.

Le marché des outils de supervision est vaste et se divise en deux catégories principales : les logiciels payants (commerciaux) et les logiciels gratuits (open source). Ces logiciels permettent de couvrir des périmètres entiers d'entreprises, allant de la surveillance des équipements (serveurs, routeurs, commutateurs) à la supervision des applications et des services. Ils offrent des fonctionnalités variées, telles que la surveillance en temps réel de l'état des machines critiques, la détection des anomalies, la génération d'alertes en cas de problème, l'analyse du trafic réseau et la fourniture de rapports détaillés.

Les logiciels de supervision peuvent être déployés de différentes manières, en fonction des besoins et des contraintes de l'entreprise. Ils peuvent être installés sur des serveurs dédiés, sur des machines virtuelles, dans le cloud ou même sur des équipements embarqués. Le choix du mode de déploiement dépend de facteurs tels que la taille de l'infrastructure, le budget disponible et les compétences techniques de l'équipe informatique.

Dans ce chapitre, nous allons explorer en détail les différents types de logiciels de supervision disponibles sur le marché, en mettant en évidence leurs avantages, leurs inconvénients et leurs fonctionnalités spécifiques. Nous allons également examiner les critères à prendre en compte pour choisir l'outil de supervision le plus adapté aux besoins de votre entreprise.

2. Les logiciels de supervision : un panorama des solutions actuelles

Les outils de supervision ont pour objectif principal de fournir une visibilité complète et en temps réel de l'état des infrastructures informatiques. Ils permettent de surveiller les équipements critiques (serveurs, commutateurs, routeurs), les services (applications, bases de données) et le trafic réseau,

afin de garantir la disponibilité, la performance et la sécurité des systèmes d'information. Le marché des logiciels de supervision est vaste, avec une variété de solutions répondant à différents besoins et budgets. On distingue principalement deux catégories : les solutions open source et les solutions commerciales.

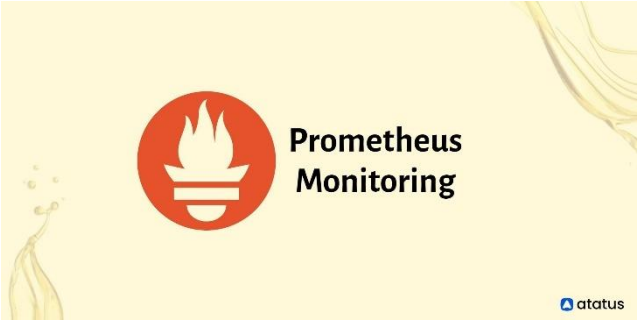
2.1.Solutions Open Source

Les outils open source offrent une grande flexibilité et bénéficient d'une large communauté d'utilisateurs et de développeurs. Leur nature ouverte permet une adaptation aux besoins spécifiques et une transparence du code source. Ils sont souvent gratuits, ce qui représente un atout majeur pour les petites et moyennes entreprises ou les organisations avec des budgets limités.

2.1.1. **Zabbix : la solution complète et évolutive**

Zabbix se distingue comme une solution de supervision open source puissante et extrêmement flexible, capable de surveiller une vaste gamme d'équipements et de services. Parmi ses principaux atouts, on note sa gratuité et son caractère open source, offrant une grande liberté d'utilisation et de modification. Il supporte une multitude de protocoles, tels que SNMP, ICMP et l'utilisation d'agents, ce qui le rend adaptable à divers environnements. De plus, Zabbix bénéficie d'une communauté active et d'une documentation exhaustive, facilitant son apprentissage et son utilisation. Ses fonctionnalités avancées de visualisation et de reporting permettent une analyse approfondie des données et une prise de décision éclairée. Enfin, son architecture évolutive le rend parfaitement adapté aux infrastructures de grande envergure. Cependant, la configuration initiale de Zabbix peut s'avérer complexe, nécessitant des compétences techniques pour son administration et sa maintenance. De plus, son interface utilisateur, bien que complète, peut sembler moins intuitive que celles de certaines solutions commerciales, en particulier pour les nouveaux utilisateurs.

2.1.2. **Prometheus**



Prometheus est un outil de supervision open source axé sur les métriques et l'observabilité, particulièrement adapté aux environnements dynamiques et conteneurisés. Il offre un modèle de données multidimensionnel et un langage de requête puissant (PromQL) pour analyser les données de performance. Prometheus est souvent utilisé en combinaison avec Grafana pour la visualisation des données. Ses points forts incluent sa capacité à collecter des métriques à partir de diverses sources, son architecture évolutive et sa popularité dans la communauté DevOps. Cependant, Prometheus peut être complexe à configurer et à gérer, et son interface de visualisation est limitée.

2.2. Solutions commerciales

Les outils commerciaux se distinguent par un support technique professionnel, des fonctionnalités avancées et une interface utilisateur généralement plus conviviale. Ces atouts facilitent leur déploiement et leur utilisation, en particulier pour les organisations qui ne disposent pas de ressources techniques importantes. Toutefois, leur principal inconvénient réside dans leur coût, qui peut être significatif, en particulier pour les grandes infrastructures.

2.2.1. **SolarWinds Network Performance Monitor (NPM)**

SOLARWINDS

SolarWinds NPM est une solution de supervision réseau complète, conçue pour répondre aux besoins des entreprises de toutes tailles. Son interface utilisateur intuitive facilite la navigation et la configuration, même pour les utilisateurs novices. Il offre une large gamme de fonctionnalités intégrées, couvrant la surveillance des performances, la gestion des erreurs et l'analyse du trafic, permettant une gestion centralisée du réseau. De plus, SolarWinds offre un support technique professionnel, assurant une assistance en cas de besoin. Cependant, le coût de SolarWinds NPM peut être élevé, en particulier pour les grandes infrastructures ou les organisations ayant des budgets limités. De plus, sa richesse fonctionnelle peut le rendre complexe à configurer pour les petites infrastructures ou les utilisateurs ayant des besoins plus simples.

2.2.2. **Datadog : la plateforme de monitoring cloud**

Datadog est une plateforme de monitoring cloud complète, conçue pour la surveillance des infrastructures, des applications et des logs. Sa facilité d'utilisation et de déploiement en font une solution attrayante pour les entreprises qui souhaitent une mise en œuvre rapide. L'intégration avec de nombreux services cloud permet une supervision centralisée des environnements hybrides ou multi-cloud. De plus, sa scalabilité et sa haute disponibilité garantissent une surveillance continue, même en cas de forte charge. Cependant, le coût de Datadog est basé sur l'utilisation, ce qui peut rendre la prévision budgétaire difficile. De plus, la dépendance à la connectivité Internet peut être un inconvénient en cas de coupure réseau. Enfin, les préoccupations potentielles concernant la sécurité des données, liées à leur stockage dans le cloud, doivent être prises en compte.

2.3. Solutions SaaS (Software as a Service)

Les outils SaaS, hébergés dans le cloud et accessibles via un navigateur web, offrent une grande flexibilité et ne nécessitent pas d'installation ni de maintenance sur site. Cette approche simplifie le déploiement et l'administration, et permet un accès distant aux données de supervision.

- **Datadog : la plateforme de monitoring cloud (mentionné précédemment)**
- **New Relic : la plateforme de monitoring axée sur les applications**

New Relic est une plateforme de monitoring axée sur les applications, offrant des outils pour analyser les performances et l'expérience utilisateur. Il permet de surveiller les temps de réponse, les erreurs et les transactions des applications, et de visualiser les données à l'aide de tableaux de bord et de graphiques. New Relic offre également des fonctionnalités de surveillance des infrastructures et des logs. Ses points forts incluent sa facilité d'utilisation, son intégration avec de nombreux langages et frameworks, et ses outils d'analyse des performances applicatives. Cependant, le coût de New Relic peut être élevé, en particulier pour les grandes applications ou les entreprises ayant des besoins complexes.

2.4.PfSense

PfSense, bien qu'étant avant tout un pare-feu et un routeur open source, joue un rôle crucial dans le monitoring du trafic réseau. Grâce à son support des protocoles NetFlow, sFlow et IPFIX, il permet de collecter des données précieuses sur les flux de trafic, offrant une visibilité granulaire sur l'utilisation de la bande passante, les applications utilisées et les utilisateurs les plus consommateurs. Ces données peuvent ensuite être exploitées par des outils de supervision tels que Zabbix pour une analyse approfondie et une optimisation du réseau. PfSense ne se substitue pas à une plateforme de supervision complète, mais il en est un complément précieux pour la surveillance du trafic. Son intégration avec des outils comme Zabbix permet de combiner la sécurité et la gestion du réseau avec une supervision centralisée et performante. Bien que pfSense offre des outils de monitoring basiques intégrés (comme les graphiques de trafic), sa force réside dans son interopérabilité avec des solutions dédiées.

3. Tableau Comparatif des Outils de Supervision

Caractéristique	Zabbix	Prometheus	SolarWinds NPM	Datadog	New Relic	PfSense
Type de solution	Open source	Open source	Commercial	Cloud (SaaS)	Cloud (SaaS)	Open source
Fonctionnalités principales	Supervision complète (réseau, systèmes, applications), alertes, tableaux de bord, rapports	Supervision de métriques, alertes, intégration avec Grafana	Supervision réseau complète, gestion des erreurs, analyse du trafic	Supervision cloud, applications, logs, intégration avec de nombreux services	Supervision applications, performances, expérience utilisateur	Pare-feu, routeur, monitoring du trafic réseau (NetFlow, sFlow, IPFIX)
Facilité d'utilisation	Moyen	Difficile	Facile	Facile	Facile	Moyen
Scalabilité	Très bonne	Très bonne	Très bonne	Très bonne	Très bonne	Bonne
Coût	Gratuit	Gratuit	Élevé	Variable (basé sur l'utilisation)	Élevé	Gratuit

Support	Communauté	Communauté	Commercial	Commercial	Commercial	Communauté
Adapté pour	Infrastructures de toutes tailles, besoins variés	Environnements dynamiques, applications conteneurisées	Supervision réseau complète, entreprises de toutes tailles	Supervision cloud, applications, environnements hybrides	Supervision applications, analyse des performances	Surveillance du trafic réseau, sécurité

4. Choix de solution retenue et Motivation

Le choix de Zabbix et pfSense pour l'ACFPE est une stratégie synergique, offrant une solution complète et intégrée pour une infrastructure IT performante, sécurisée et maîtrisée. Ensemble, ils démultiplient leurs avantages pour l'ACFPE, là où des outils isolés seraient limités.

4.1. Visibilité et Gestion Centralisée du Réseau de l'ACFPE : Clarté et Efficacité

- **Zabbix : Tableau de Bord Unifié.** Vue à 360° de l'infrastructure IT de l'ACFPE (serveurs, réseau, applications) sur une interface unique, simplifiant la gestion et l'aide à la décision rapide.
- **pfSense : Intégration des Données Trafic dans Zabbix.** Fusion des données d'infrastructure et trafic pfSense dans Zabbix, offrant une vision holistique pour un diagnostic précis et une compréhension globale du réseau de l'ACFPE.

4.2. Performance Optimisée et Bande Passante Maîtrisée pour l'ACFPE : Contrôle et Efficience

- **pfSense : Contrôleur Dynamique de la Bande Passante Internet.** QoS avancé pour prioriser le trafic pédagogique, éviter la congestion et garantir une expérience utilisateur fluide à l'ACFPE, même en forte charge.

- **Zabbix : Analyse Prédictive des Performances Système.** Surveillance continue des performances serveurs pour anticiper les goulots d'étranglement et optimiser l'allocation des ressources IT de l'ACFPE.

4.3. Sécurité Renforcée et Protection Proactive des Données de l'ACFPE : Bouclier et Surveillance

- **pfSense : Bouclier Périmétrique Avancé.** Pare-feu puissant et mis à jour pour bloquer les menaces externes, filtrer les accès et protéger le réseau et les données sensibles de l'ACFPE.
- **Zabbix : Détection des Anomalies et Surveillance de l'Intégrité.** Surveillance interne pour détecter comportements anormaux, pics de trafic suspects et incidents de sécurité, protégeant proactivement l'ACFPE.

4.4. Solution Durable, Économique et Adaptée à l'ACFPE : Stratégie à Long Terme

- **Open Source : Coût Maîtrisé, Flexibilité, Communauté.** Économies significatives pour l'ACFPE, adaptation précise aux besoins, support communautaire actif et évolution continue des solutions open source.
- **Évolutivité et Adaptabilité : Investissement Pérenne.** Architecture modulaire et flexibilité garantissant l'évolution de la solution avec l'ACFPE, assurant un investissement durable et adapté aux besoins futurs.

5. Conclusion

Le choix de Zabbix et pfSense pour l'ACFPE se justifie par une stratégie synergique visant à établir une infrastructure IT performante, sécurisée et parfaitement administrée. Cette combinaison dépasse la simple addition d'outils, offrant une solution intégrée où Zabbix assure une visibilité et une gestion centralisée de l'ensemble de l'infrastructure de l'ACFPE, tandis que pfSense garantit une gestion optimisée de la bande passante Internet et une sécurité périmétrique renforcée. Ensemble, ils permettent à l'ACFPE de bénéficier d'un tableau de bord unifié pour une prise de décision rapide, d'une performance réseau optimisée grâce à un contrôle dynamique de la bande passante et à une analyse prédictive des ressources, d'une sécurité multicouche protégeant proactivement les données, et d'une solution durable, économique et évolutive grâce à l'open source, représentant un investissement pérenne et adapté aux besoins spécifiques et futurs de l'ACFPE.

Chapitre III : Présentation des outils choisis

1 Introduction

Dans un environnement réseau moderne, une simple vue d'ensemble ne suffit plus. L'administration efficace exige une compréhension approfondie des outils et de leurs capacités. Ce chapitre vise à dépasser la superficialité des présentations générales pour explorer en profondeur les fonctionnalités clés de Zabbix et pfSense, deux piliers de la supervision et de la gestion réseau. Nous allons détailler leur architecture, leurs mécanismes internes, leurs options de configuration avancées et leur synergie, afin de fournir une base solide pour un déploiement et une administration réseau maîtrisés.

2 Zabbix

2.1 Définition

Zabbix n'est pas seulement un outil de supervision, mais une plateforme complète d'intelligence opérationnelle pour l'infrastructure informatique. Il excelle dans la collecte de données hétérogènes (métriques de performance, logs, événements), leur analyse en temps réel, la détection proactive d'anomalies, et la fourniture de visualisations riches et personnalisables. Son architecture distribuée et son moteur de règles puissant lui permettent de gérer des environnements complexes et de s'adapter à des besoins de supervision très spécifiques. Zabbix se distingue par sa capacité à automatiser des tâches complexes, à s'intégrer avec d'autres systèmes et à évoluer avec les besoins de l'infrastructure.

4.5.Architecture de Zabbix

Pour comprendre la puissance de Zabbix, il est essentiel d'examiner son architecture en détail :

- **Serveur Zabbix (Zabbix Server) :** Le cœur du système, écrit en C, gère la configuration, la collecte de données, le traitement des alertes, le stockage des données en base, et l'interface web (PHP). Il utilise des processus spécialisés (pollers, trappers, http pollers, vmware collectors, etc.) pour optimiser la collecte de données selon différents protocoles (Agent Zabbix, SNMP, JMX, IPMI, HTTP, etc.). Le serveur Zabbix peut être configuré en mode actif-passif pour la haute disponibilité.
- **Agents Zabbix (Zabbix Agent) :** Agents légers, écrits en C, installés sur les hôtes à superviser. Ils collectent des données de manière efficace et locale, minimisant l'impact sur les ressources de l'hôte. Les agents peuvent être passifs (répondent aux requêtes du serveur) ou actifs (envoient proactivement les données). Le choix du mode dépend des besoins de sécurité et de performance. L'agent Zabbix supporte de nombreux types de métriques (CPU, mémoire, disque, réseau, processus, logs, etc.) et peut être étendu via des UserParameters pour des métriques spécifiques à une application.
- **Proxies Zabbix (Zabbix Proxy) :** Proxies optionnels, écrits en C, agissant comme collecteurs de données intermédiaires. Ils réduisent la charge sur le serveur Zabbix central, améliorent la scalabilité, et permettent la supervision de réseaux distants, isolés ou avec une latence élevée. Les proxies stockent temporairement les données en cas de perte de connexion avec le serveur, assurant la continuité de la collecte. Ils peuvent également être utilisés pour centraliser la collecte de données SNMP dans un environnement distribué.
- **Interface Web Zabbix (Zabbix Frontend) :** Interface web PHP, offrant une console d'administration complète et conviviale. Elle permet de configurer tous les aspects de

Zabbix (hôtes, items, triggers, actions, templates, utilisateurs, permissions, etc.), de visualiser les données en temps réel et historiques (tableaux de bord, graphiques, cartes), de gérer les alertes, et de générer des rapports. L'interface web est personnalisable et extensible via des thèmes et des modules.

- **Base de données Zabbix (Database) :** Base de données relationnelle (MySQL, PostgreSQL, Oracle, SQLite) stockant la configuration, les données historiques, les événements, les logs et les informations utilisateurs. Le choix de la base de données dépend de la taille de l'infrastructure et des exigences de performance. Pour les grandes installations, une base de données robuste et performante comme PostgreSQL ou Oracle est recommandée.

Figure III.1 : Architecture Détaillée de Zabbix et Flux de Données.

III.2.3 Fonctionnalités Clés de Zabbix

Approfondissons certaines fonctionnalités clés de Zabbix :

- **Items (Éléments) :** Les items sont le fondement de la collecte de données dans Zabbix. Ils définissent *quoi* surveiller et *comment* le surveiller. Zabbix propose une variété de types d'items :
  - ✓ **Agent Zabbix Checks :** Collecte de données via l'agent Zabbix installé sur l'hôte cible. Peut être passif ou actif. Exemple : system.cpu.load[,avg1], vm.memory.size[pavailable], vfs.fs.size[/,pfree].
  - ✓ **SNMP Checks :** Collecte de données via le protocole SNMP (Simple Network Management Protocol). Permet de surveiller les équipements réseau (routeurs, commutateurs, imprimantes, etc.) compatibles SNMP. Exemple : ifInOctets[ifname], sysUptime. Nécessite la configuration SNMP sur l'équipement cible et la connaissance des MIB (Management Information Base).
  - ✓ **Simple Checks :** Vérifications simples sans agent, utilisant des protocoles standard comme ICMP (ping), TCP, HTTP, HTTPS, DNS, etc. Exemple : icmpping, net.tcp.port[<ip>,<port>], web.page.get[<url>].
  - ✓ **JMX Monitoring :** Surveillance des applications Java via JMX (Java Management Extensions). Permet de collecter des métriques spécifiques aux applications Java (utilisation du heap, nombre de threads, etc.).
  - ✓ **IPMI Checks :** Surveillance du matériel via IPMI (Intelligent Platform Management Interface). Permet de collecter des informations sur la température, la tension, la vitesse des ventilateurs, l'état de l'alimentation, etc.
  - ✓ **Calculated Items :** Items calculés à partir d'autres items, permettant de créer des métriques dérivées ou agrégées. Exemple : Calcul du taux d'utilisation CPU moyen sur un cluster de serveurs.
  - ✓ **Aggregate Items :** Items agrégés, permettant de collecter des statistiques agrégées sur plusieurs items (moyenne, minimum, maximum, somme, etc.). Exemple : Calcul de la charge CPU moyenne sur un groupe d'hôtes.
  - ✓ **External Checks :** Exécution de scripts externes (shell, Python, etc.) pour collecter des données personnalisées. Offre une grande flexibilité pour la supervision d'applications ou de systèmes non standard.
  - ✓ **HTTP Agent :** Collecte de données via des requêtes HTTP/HTTPS vers des APIs web. Permet de surveiller des services web, des APIs REST, etc.

- ✓ **Traps SNMP et Traps Zabbix :** Réception passive de traps SNMP et Zabbix envoyés par les équipements supervisés en cas d'événements. Permet une supervision réactive et temps réel basée sur les événements.

- **Triggers (Déclencheurs) :** Les triggers définissent les conditions d'alerte basées sur les données collectées par les items. Ils sont exprimés sous forme d'expressions logiques, utilisant des fonctions et des opérateurs pour analyser les valeurs des items sur différentes périodes. Exemples d'expressions de triggers :
  - ✓ ***{Host:system.cpu.load[,avg1].avg(5m)} > 80*** : Alerte si la charge CPU moyenne sur 5 minutes dépasse 80%.
  - ✓ *{Host:vfs.fs.size[/,pfree].last()}<10% :* Alerte si l'espace disque libre sur la partition racine est inférieur à 10%.
  - ✓ *{Host:icmpping.max(5m)}=0 :* Alerte si l'hôte est injoignable au ping pendant 5 minutes.
  - ✓ *{Host:net.tcp.port[<ip>,80].last()}=0* : Alerte si le port 80 (HTTP) n'est pas ouvert sur l'hôte.
  - ✓ *{Host:log[/var/log/apache2/error.log,"error",,,"skip*"]}.strlen()>0 : Alerte si le fichier de log Apache error.log contient des erreurs.
  - ✓ Les triggers peuvent avoir différents niveaux de gravité (Information, Warning, Average, High, Disaster) pour prioriser les alertes. Les états des triggers (OK, PROBLEM, UNKNOWN) reflètent l'état actuel du système.
- **Actions (Actions) :** Les actions définissent les réponses automatisées aux événements déclenchés par les triggers. Elles consistent en :
  - ✓ **Conditions (Conditions) :** Définissent quand l'action doit être exécutée (basée sur la gravité du trigger, l'hôte, le groupe d'hôtes, etc.).
  - ✓ **Opérations (Operations) :** Actions à exécuter en réponse à l'événement. Les opérations peuvent inclure :
    - ▪ **Notifications :** Envoi de notifications par email, SMS, Jabber, Slack, etc. Les notifications peuvent être personnalisées avec des macros pour inclure des informations dynamiques (nom de l'hôte, nom du trigger, valeur du item, etc.).
    - ▪ **Commandes à distance (Remote Commands) :** Exécution de commandes sur l'hôte supervisé (redémarrage d'un service, arrêt d'un processus, etc.). Nécessite une configuration de sécurité rigoureuse.
    - ▪ **Ajout/Suppression d'hôtes à des groupes :** Gestion dynamique des groupes d'hôtes en fonction des événements.
    - ▪ **Envoi de traps SNMP :** Envoi de traps SNMP vers un serveur de supervision externe.
    - ▪ **Intégration avec des systèmes externes (Webhooks) :** Envoi de notifications à des systèmes externes via des requêtes HTTP (systèmes de ticketing, outils d'automatisation, etc.).
    - ▪ Les actions peuvent être configurées pour être exécutées lors du déclenchement du trigger (passage à l'état PROBLEM), lors de la résolution du trigger (retour à l'état OK), ou lors de la mise à jour de la valeur du trigger. Des escalades d'actions peuvent être définies pour gérer les problèmes persistants (notifications répétées, actions plus drastiques après un certain temps).

- **Templates (Modèles) : La Simplification du Déploiement et de la Gestion** Les templates sont des ensembles préconfigurés d'items, de triggers, de graphes, d'applications et d'écrans. Ils permettent de :
    - ✓ **Standardiser la supervision :** Appliquer une configuration de supervision cohérente à plusieurs hôtes de même type (serveurs web, serveurs de bases de données, commutateurs, etc.).
    - ✓ **Accélérer le déploiement :** Déployer rapidement la supervision sur de nouveaux hôtes en appliquant un template existant.
    - ✓ **Faciliter la maintenance :** Modifier un template pour mettre à jour la configuration de supervision de tous les hôtes qui l'utilisent.
    - ✓ Zabbix propose de nombreux templates préconfigurés pour différents systèmes d'exploitation, services et équipements (Linux, Windows, Apache, MySQL, SNMP Generic, etc.). Des templates personnalisés peuvent être créés pour des besoins spécifiques. Les templates peuvent être liés entre eux (templates imbriqués) pour une organisation modulaire et réutilisable de la configuration.

3 pfSense

3.1 Définition

pfSense est bien plus qu'un simple pare-feu et routeur open source. Il s'agit d'une plateforme unifiée de gestion de réseau périmétrique, intégrant des fonctionnalités avancées de sécurité, de routage, de VPN, de gestion de la bande passante, et de portail captif. Basé sur FreeBSD, pfSense hérite de sa robustesse et de sa fiabilité, tout en offrant une interface web conviviale et une grande flexibilité de configuration. Sa nature open source et sa communauté active en font une solution évolutive et adaptable aux besoins changeants des réseaux modernes.

3.2 Architecture de pfSense :

L'architecture de pfSense repose sur les éléments clés suivants :

- **Noyau FreeBSD (FreeBSD Kernel) :** Le système d'exploitation sous-jacent, assurant la stabilité, la performance et la sécurité de pfSense. Le noyau FreeBSD est optimisé pour les tâches de réseau et de sécurité.
- **Pare-feu Packet Filter (PF) :** Le pare-feu stateful intégré à FreeBSD, au cœur de la sécurité de pfSense. PF est un pare-feu puissant et flexible, offrant un filtrage basé sur l'état des connexions, des règles personnalisables, du NAT, de la gestion des files d'attente, et de nombreuses options avancées. PF utilise une syntaxe de règles claire et expressive, permettant de définir des politiques de sécurité complexes.
- **Routeur (Routing) :** Fonctionnalités de routage basées sur le noyau FreeBSD, supportant le routage statique et dynamique (via des packages comme OSPF et FRR). pfSense permet de configurer des politiques de routage avancées (policy routing), le failover et le load balancing multi-WAN, les VLAN, le DHCP relay, et d'autres fonctionnalités de routage complexes.
- **Interface Web pfSense (pfSense WebGUI) :** Interface web PHP, offrant une console d'administration complète et intuitive. Elle permet de configurer tous les aspects de pfSense (pare-feu, routage, VPN, portail captif, services, packages, etc.), de surveiller l'état du

système, de consulter les logs, et d'effectuer des diagnostics réseau. L'interface web est conçue pour être accessible et conviviale, même pour les utilisateurs non experts.

- **Système de Packages pfSense (pfSense Packages) :** Système de gestion de packages basé sur pkg de FreeBSD, permettant d'étendre les fonctionnalités de pfSense en ajoutant des modules complémentaires. Les packages sont développés par la communauté pfSense et offrent une large gamme de fonctionnalités (VPN, IDS/IPS, proxy, serveurs, outils de monitoring, etc.). L'installation et la gestion des packages se font facilement via l'interface web.

Figure III.29 : Architecture Détaillée de pfSense et Flux de Trafic.

III.3.3 Fonctionnalités Clés de pfSense : Exploration Technique et Configuration

La distribution Pfsense met ainsi à la disposition de l'administrateur réseau une multitude d'outils open sources permettant d'optimiser ses taches à savoir :

- **Pare-feu Stateful (Stateful Firewall) : Inspection et Suivi des Connexions** Le pare-feu de pfSense est stateful, ce qui signifie qu'il suit l'état de chaque connexion réseau. Il ne se contente pas d'examiner chaque paquet individuellement, mais prend en compte le contexte de la connexion à laquelle il appartient. Cela permet :
  - ✓ **Sécurité accrue :** Le pare-feu stateful peut distinguer les connexions légitimes (établies) des nouvelles tentatives de connexion, et bloquer les connexions non sollicitées ou suspectes.
  - ✓ **Filtrage dynamique :** Les règles de pare-feu peuvent être définies de manière plus souple, car le pare-feu gère automatiquement le trafic de retour des connexions autorisées.
  - ✓ **Performance optimisée :** L'inspection stateful permet d'optimiser le traitement des paquets, car le pare-feu n'a pas besoin de ré-analyser chaque paquet d'une connexion établie.
  - ✓ pfSense utilise le pare-feu PF de FreeBSD, reconnu pour sa robustesse et ses performances. Les règles de pare-feu sont définies via l'interface web, avec de nombreuses options de personnalisation (interfaces, protocoles, ports, adresses sources/destinations, etc.). Les règles sont évaluées séquentiellement, de haut en bas. L'ordre des règles est donc crucial pour la sécurité.
- **NAT (Network Address Translation) : Masquage d'Adresses et Redirection de Ports** pfSense intègre des fonctionnalités de NAT (Network Address Translation) essentielles pour la gestion des adresses IP et la sécurité :
  - ✓ **NAT sortant (Outbound NAT) :** Masque les adresses IP privées du réseau local derrière l'adresse IP publique de l'interface WAN. Permet de partager une seule adresse IP publique entre plusieurs machines du réseau local. pfSense propose différents modes de NAT sortant (Automatique, Manuel, Hybride). Le mode automatique est le plus simple et le plus courant.
  - ✓ **NAT entrant (Port Forwarding) :** Redirige le trafic entrant sur un port public (interface WAN) vers une adresse IP et un port privés spécifiques du réseau local. Permet de rendre accessibles depuis Internet des services hébergés sur le réseau local (serveur web, serveur de messagerie, etc.). Le port forwarding doit être configuré avec précaution pour éviter d'ouvrir des failles de sécurité.

- ✓ **NAT 1:1 (1:1 NAT) :** Associe une adresse IP publique à une adresse IP privée de manière biunivoque. Permet de rendre un serveur du réseau local accessible depuis Internet avec sa propre adresse IP publique. Utilisé pour les serveurs nécessitant une adresse IP publique dédiée.
- ✓ **NAT de réflexion (NAT Reflection) :** Permet d'accéder aux services NATés depuis le réseau local en utilisant l'adresse IP publique du pare-feu. Facilite l'accès aux services internes depuis le réseau local et depuis Internet en utilisant le même nom de domaine ou adresse IP publique.

- **Portail Captif (Captive Portal) : Contrôle d'Accès et Authentification Utilisateurs** Le portail captif de pfSense permet de contrôler l'accès Internet des utilisateurs se connectant au réseau WiFi ou filaire. Il redirige les utilisateurs non authentifiés vers une page web (le portail captif) où ils doivent s'authentifier avant d'obtenir l'accès Internet. Le portail captif de pfSense offre de nombreuses options de configuration :
  - ✓ **Zones (Zones) :** Définition de zones de portail captif sur différentes interfaces réseau (WiFi, LAN, VLAN). Permet d'appliquer des politiques d'accès différentes selon la zone.
  - ✓ **Méthodes d'authentification (Authentication Methods) :** Support de différentes méthodes d'authentification :
    - **Local User Manager :** Authentification via une base de données d'utilisateurs locale à pfSense.
    - **Vouchers :** Authentification via des codes vouchers pré-générés. Utile pour les accès temporaires (visiteurs, événements).
    - **RADIUS Authentication :** Authentification via un serveur RADIUS externe (Active Directory, FreeRADIUS, etc.). Permet une gestion centralisée des utilisateurs et l'intégration avec des infrastructures d'authentification existantes.
    - **LDAP Authentication :** Authentification via un serveur LDAP externe (Active Directory, OpenLDAP, etc.). Similaire à RADIUS, mais utilisant le protocole LDAP.
  - ✓ **Page d'accueil personnalisable (Customizable Homepage) :** Personnalisation de la page du portail captif avec le logo de l'organisation, des informations d'accueil, des conditions d'utilisation, des liens utiles, etc. La page d'accueil peut être créée en HTML, CSS et JavaScript.
  - ✓ **Redirection après authentification (Redirection after Authentication) :** Redirection des utilisateurs vers une URL spécifique après l'authentification (page d'accueil de l'organisation, portail intranet, etc.).
  - ✓ **Journalisation (Logging) :** Enregistrement des informations de connexion au portail captif (utilisateurs, date/heure, adresses IP, etc.) pour le suivi et l'audit.
  - ✓ **No-charge addresses :** Définition d'adresses IP ou de noms de domaine exemptés de l'authentification du portail captif (accès à des services internes, mise à jour des antivirus, etc.).
  - ✓ **Pass-through MAC addresses :** Autorisation d'accès Internet permanent pour certaines adresses MAC (imprimantes, équipements IoT, etc.) sans authentification au portail captif.
- **Traffic Shaper (Gestionnaire de Bande Passante) : Optimisation du Trafic et QoS** Le Traffic Shaper de pfSense permet de contrôler et d'optimiser l'utilisation de la bande passante Internet, en garantissant une qualité de service (QoS) pour les applications

critiques et en limitant la consommation de bande passante par les applications non prioritaires. pfSense utilise des mécanismes de QoS basés sur des files d'attente (Queues) et des limiteurs (Limiters) :

- ✓ **Files d'attente (Queues) :** Définition de files d'attente avec différentes priorités pour différents types de trafic. pfSense supporte différents algorithmes de gestion des files d'attente (CBQ, HTB, HFSC, CoDel). L'algorithme HFSC (Hierarchical Fair Service Curve) est souvent recommandé pour sa flexibilité et sa performance.
- ✓ **Règles de pare-feu QoS (QoS Firewall Rules) :** Application des files d'attente aux règles de pare-feu pour classer le trafic et lui attribuer une priorité. Le trafic peut être classé en fonction de l'adresse IP source/destination, du port source/destination, du protocole, de l'utilisateur, de l'application, etc.
- ✓ **Limiteurs (Limiters) :** Définition de limiteurs de bande passante pour contrôler le débit maximal autorisé pour certaines connexions ou certains types de trafic. Les limiteurs peuvent être utilisés pour limiter le P2P, le streaming vidéo, ou d'autres applications consommatrices de bande passante.
- ✓ **Priorisation du trafic:** Configuration de règles de QoS spécifiques pour prioriser des trafics spécifiques garantissant une qualité optimale.

3.4 Avantages

Au-delà des avantages généraux déjà mentionnés, pfSense offre des bénéfices plus spécifiques et techniques :

- **Flexibilité et Personnalisation Extrêmes :** pfSense offre une flexibilité de configuration inégalée, permettant d'adapter le pare-feu et le routeur à des besoins très spécifiques. Presque tous les aspects de pfSense sont configurables via l'interface web ou la ligne de commande. Le système de packages permet d'étendre les fonctionnalités selon les besoins.
- **Sécurité Robuste et Mises à Jour Régulières :** Basé sur FreeBSD, pfSense bénéficie d'une sécurité intrinsèque et de mises à jour de sécurité régulières. La communauté pfSense est très active dans la détection et la correction des failles de sécurité. Les mises à jour de pfSense sont faciles à installer via l'interface web.
- **Performance Élevée et Scalabilité :** pfSense est conçu pour la performance et la scalabilité. Il peut gérer des débits élevés et un grand nombre de connexions simultanées. L'architecture distribuée (avec proxies Zabbix) permet de superviser des infrastructures de grande taille.
- **Communauté Active et Support Étendu :** La communauté pfSense est très large et active, offrant un support important via les forums, la documentation, les tutoriels, etc. Des services de support commercial sont également disponibles pour les entreprises. La documentation de pfSense est complète et régulièrement mise à jour.

Conclusion

En conclusion, l'association approfondie de Zabbix et pfSense représente une solution d'administration réseau holistique et puissante. Zabbix apporte une supervision détaillée et centralisée, tandis que pfSense assure une gestion d'Internet et une sécurité périmétrique avancées. Ce duo d'outils permet aux administrateurs réseau de maîtriser tous les aspects de leur

infrastructure, de la performance à la sécurité, en passant par la gestion de l'accès Internet, pour un réseau robuste, performant et sécurisé.

Implémentation de la Solution Retenue

Chapitre 1 : Mise en œuvre

1.1 Liste des besoins matériels et logiciels

1.2 Architecture de la solution retenue

1.3 Installation et configuration de Zabbix

1.4 Installation et configuration de pfSense

1.5 Intégration de pfSense avec Zabbix

1.6 Implémentation de la sécurité

Chapitre 2 : Présentation de la solution

2.1 Résultats obtenus

2.2 Analyse des performances

2.3 Retour d’expérience et recommandations

Conclusion