CHAPITRE 2

État de le art

1. **Introduction**

Au sein de l’environnement sans cesse renouvelé des infrastructures informatiques, la supervision réseau est aujourd’hui un pilier indispensable pour garantir performance, fiabilité et sécurité. Confrontés à l’expansion et à la complexité croissantes des architectures, les outils de monitoring doivent évoluer pour fournir des données à la fois précises et en temps réel, tout en offrant simplicité d’usage, capacité de montée en charge et intégration fluide. Le chapitre « État de l’art » propose une étude approfondie des solutions de surveillance réseau les plus répandues, examinant leurs fonctionnalités, architectures et limites. En comparant ces outils selon leur ergonomie, leur évolutivité, leurs performances et leur coût, nous mettons en lumière les lacunes persistantes. Cette analyse révèle tant les atouts que les faiblesses de plateformes établies comme Nagios, Zabbix ou PRTG, et justifie la nécessité d’une solution plus moderne et adaptable. Comprendre l’état actuel du domaine est une étape essentielle pour concevoir un système à la fois innovant et en phase avec les besoins opérationnels du secteur.

1. **Aperçu sur SNMP**

Le protocole SNMP (Simple Network Management Protocol) est couramment employé pour administrer les équipements sur les réseaux IP. Il permet de superviser et de contrôler des matériels tels que routeurs, commutateurs, serveurs ou imprimantes. SNMP repose sur une architecture client-serveur : le gestionnaire SNMP (client) échange avec les agents SNMP (serveurs) installés sur les dispositifs. Cette communication donne aux administrateurs la possibilité de recueillir des indicateurs clés de performance, de configurer les équipements et de recevoir des notifications en cas d’événements réseau.

SNMP a connu plusieurs évolutions : SNMPv1 a vu le jour à la fin des années 1980, suivi de SNMPv2 au début des années 1990, puis de SNMPv3 à la fin des années 1990, cette dernière version apportant des renforcements significatifs en matière de sécurité et de gestion des données. Grâce à ces avancées successives, SNMP demeure un outil fiable et complet pour la gestion des infrastructures réseau.[1]

1. **Importance de la gestion réseau**

Une gestion efficace du réseau est essentielle au maintien de la santé et des performances des infrastructures numériques modernes. Face à la complexité croissante des réseaux et au nombre croissant d'appareils connectés, les entreprises sont confrontées à des défis majeurs pour garantir la fiabilité des communications et des transferts de données. Une gestion réseau efficace contribue à :

* **Surveillance des Performance** : Suivi Continue de réseau performance métrique permet d'identifier en temps opportun les goulots d'étranglement et les opportunités d'optimisation.
* **Gestion des pannes** : SNMP permet une détection rapide des défaillances, ce qui permet aux administrateurs de réagir rapidement pour minimiser les temps d’arrêt.
* **Gestion de la configuration** : Les changements de configuration automatisés peuvent être mis en œuvre à l’aide du SNMP, ce qui améliore l’efficacité opérationnelle et la cohérence entre les appareils.
* **Planification de la capacité**: En analysant les tendances d’utilisation, les organisations peuvent mieux planifier la croissance future et l’affectation des ressources.

L’utilisation efficace du SNMP contribue à l’efficacité organisationnelle globale, réduisant les coûts opérationnels et améliorant la prestation des services.

1. **Historique**

Depuis le début des années 1990, la surveillance du réseau est passée de simples scripts ping à des plateformes sophistiquées en temps réel alimentées par l’automatisation et les analyses.

* 1. **Origines de SNMP**

Le protocole SNMP (Simple Network Management Protocol) voit le jour à la fin des années 1980, alors que l’expansion rapide des réseaux informatiques rendait indispensable un outil de supervision unifié. À mesure que les organisations multipliaient les systèmes interconnectés, le besoin d’un standard pour surveiller et gérer ces infrastructures devint évident. C’est l’Internet Engineering Task Force (IETF) qui élabora SNMP pour répondre à cette exigence.

Conçu pour offrir une méthode simple et efficace de collecte d’informations sur les équipements réseau, SNMP permet aux administrateurs de suivre les performances, diagnostiquer les incidents et administrer les configurations. La première version, SNMPv1, fut formalisée en 1988 via la RFC 1157, jetant les bases d’une gestion de réseau amenée à évoluer au fil des décennies.

* 1. **Évolution des versions SNMP**

L’évolution du protocole SNMP (Simple Network Management Protocol) se décline en trois versions majeures : SNMPv1, SNMPv2 et SNMPv3, chacune apportant des améliorations et corrigeant les limites de la précédente.

Publiée en 1990, SNMPv1 a constitué le socle de la gestion réseau. Elle proposait des mécanismes de requête pour extraire des données et des pièges (« traps ») pour signaler les événements. Cependant, cette première version présentait d’importantes failles de sécurité, reposant uniquement sur des chaînes de communauté pour l’authentification, aisément interceptables.

Présenté au milieu des années 1990, SNMPv2 renforçait SNMPv1 en introduisant la récupération de données en masse et la possibilité de lancer des requêtes d’information fiables pour optimiser les échanges. Malgré des performances accrues et une interface plus conviviale, les lacunes en matière de sécurité restaient importantes, freinant son adoption généralisée. Déployé en 1998, SNMPv3 a comblé ces failles grâce à l’User-based Security Model (USM) robuste et au View-based Access Control Model (VACM). Ces améliorations ont offert une authentification solide, le chiffrement des messages et des contrôles d’accès granulaires, faisant de SNMPv3 la solution de référence pour une gestion réseau sécurisée dans les infrastructures modernes.

1. **Les normes actuel SNMP**

Cette section fournit un aperçu des normes actuel SNMP, y compris leur statut de conformité et de mise en œuvre dans l’ensemble du secteur.

* 1. **Aperçu des normes actuel (IETF RFC)**

Le Internet Ingénierie Tâche Forcer (IETF) a établi plusieurs clé Demande Documents de consultation publique (RFC) définissant les normes SNMP. Les plus importants sont :

* + - **RFC 1157** : définit SNMPv1, établissant le cadre de base et les opérations de gestion du réseau.
    - **RFC 1901-1908** : présente SNMPv2, détaillant les améliorations telles que les performances améliorées et les nouvelles capacités de gestion des données.
    - **RFC 2570-2576** : Spécifie SNMPv3, en se concentrant sur les améliorations de sécurité et l'introduction du modèle de sécurité basé sur l'utilisateur (USM) et de l'accès basé sur la vue Modèle de contrôle (VACM).

Ces RFC fournir des lignes directrices pour exécution SNMP à travers divers appareils et plateformes, garantissant l’interopérabilité et la cohérence des pratiques de gestion du réseau.

* 1. **État de la conformité et de la mise en œuvre dans l’industrie**

SNMPv3 est largement considéré comme la norme pour la gestion de réseau en raison de ses fonctionnalités de sécurité robustes. De nombreux réseaux gestion outils et prise en charge des appareils SNMPv3, réfléchissant un fort industrie changement vers sécurisé gestion pratiques. Conformité avec SNMP les normes varient selon l'organisation, les grandes entreprises et les fournisseurs de services adoptant généralement SNMPv3 pour la gestion des infrastructures critiques.

Bien que SNMPv1 et SNMPv2 soient toujours utilisés, notamment sur les systèmes existants, on observe une nette tendance à leur abandon progressif au profit de SNMPv3. De nombreuses organisations explorent également des protocoles et des stratégies de gestion alternatifs pour compléter SNMP, notamment dans les environnements où le cloud computing et les objets connectés sont prédominants.

1. **Architecture SNMP**

L’architecture Simple Network Management Protocol (SNMP) est conçue pour permettre une surveillance et une gestion efficaces des périphériques réseau. Il fonctionne sur un modèle client-serveur, composé de deux composants principaux : les gestionnaires SNMP et les agents SNMP. Cette architecture permet aux administrateurs réseau de recueillir des informations, de configurer les périphériques et de répondre efficacement aux événements sur divers éléments du réseau.

Le SNMP architecture comprend :

* **SNMP Directeur** : Centralisé logiciel que supervise le fonctionnement du réseau.
* **SNMP Agent** : Logiciel en cours d'exécution sur réseau appareils, collectionner et stockage des données de gestion.
* **Base d'informations de gestion (MIB)** : Base de données définissant la structure et les types de données disponibles pour la gestion.
  1. **Gestion Information Base (MIB)**

Le La base d'informations de gestion (MIB) est une composant crucial de SNMP Architecture. Il s'agit d'un référentiel structuré décrivant les objets gérés au sein d'un périphérique réseau. Les MIB sont organisées hiérarchiquement et utilisent des identifiants d'objet (OID) pour identifier chaque objet de manière unique.

Clé caractéristiques de Les MIB incluent :

* + - **Structure hiérarchique** : les objets sont organisés sous forme d'arborescence, facilitant ainsi la navigation et l'accès.
    - **Standard et Coutume Objets** : Contient standard objets défini par IETF comme Bien en tant qu'objets spécifiques au fournisseur qui fournissent des fonctionnalités supplémentaires.
    - **Types de données** : définit différents types de données pour les objets, tels qu'un entier, une chaîne ou une jauge, permettant une représentation précise des données.
  1. **SNMP agents**

SNMP agents sont logiciel applications installé sur réseau appareils que collecter et gérer l'information. Leurs principales responsabilités comprennent :

* + - **Données Collection** : Surveillance appareil paramètres comme processeur usage, mémoire, trafic réseau, etc. Ces données sont stockées dans la base de données MIB.
    - **Réponse aux demandes** : lorsqu'un gestionnaire SNMP envoie une demande, l'agent récupère les données pertinentes du MIB et répond en conséquence.
    - **Envoi de notifications** : les agents peuvent générer des messages non sollicités appelés interruptions pour alerter le gestionnaire SNMP des événements importants, tels que des pannes ou des dépassements de seuil.
  1. **SNMP gestionnaires et leur rôles**

Les gestionnaires SNMP, souvent intégrés aux systèmes de gestion de réseau (NMS), jouent un rôle essentiel dans la gestion des opérations réseau. Leurs principales fonctions incluent :

* + - **Information Récupération** : Envoi demandes à SNMP agents à collecter données depuis le MIB, permettant la surveillance en temps réel des périphériques réseau.
    - **Configuration Gestion** : Faciliter changements à appareil configurations en envoyant des commandes aux agents, garantissant ainsi des performances optimales de l'appareil.
    - **Surveillance des événements** : analyse continue des données des agents et réponse aux pièges pour résoudre les problèmes rapidement.
    - **Rapports et Analyse** : Agrégation données sur temps pour s'orienter analyse, rapports et planification des capacités, aidant les administrateurs à prendre des décisions éclairées
  1. **Communication Modèle (Protocole Données Unités)**

La communication dans SNMP est principalement réalisé en utilisant Unités de données de protocole (PDU). PDU sont le format pour messages échangés entre SNMP gestionnaires et agents. Le Les principaux types de PDU dans SNMP incluent :

* + - **GET** : Utilisé par le gestionnaire SNMP pour demander des informations à un agent. L'agent répond avec les données demandées.
    - **ENSEMBLE** : Permet le SNMP gestionnaire de modifier le valeurs de spécifique objets dans un MIB de l'agent. Utilisé pour les modifications de configuration.
    - **GETNEXT** : Facilite la récupération de l'objet suivant dans la hiérarchie MIB, permettant au gestionnaire de parcourir la structure MIB.
    - **PIÈGE** : Un non sollicité message envoyé par le agent à le directeur, alerte il à événements importants ou changements de statut.
    - **INFORMER** : Similaire à PIÈGE, mais nécessite reconnaissance depuis le gestionnaire, assurant une communication fiable.

Ces PDU activer robuste et efficace communication dans le SNMP cadre permettant une gestion efficace du réseau.[2]

* 1. **Flux de travail de SNMP opérations**

Le flux de travail des opérations SNMP implique plusieurs étapes clés, en particulier pour les opérations GET, SET et TRAP :

* **OBTENIR Opération :**

1. Le gestionnaire SNMP envoie une requête GET PDU à l'agent SNMP, spécifiant l'OID des données souhaitées.
2. Le agent processus le demande, récupère le données depuis le MIB, et renvoie une réponse PDU contenant les informations demandées.

* **Opération SET** :

1. Le gestionnaire SNMP envoie une requête SET PDU à l'agent, incluant l'OID et la nouvelle valeur à définir.
2. Le agent mises à jour le correspondant objet dans le MIB et répond avec confirmation indiquant le succès ou l'échec de l'opération.

* **PIÈGE Opération** :

1. Lorsqu'un événement important se produit (par exemple, une panne de périphérique ou un dépassement de seuil), l'agent SNMP génère un PDU TRAP.
2. Le agent envoie le PIÈGE à le SNMP directeur, lequel journaux le événement et peut déclencher des alertes ou des réponses automatisées.

Ce flux de travail structuré facilite une communication efficace entre les gestionnaires et les agents, permettant des réponses rapides aux conditions du réseau.

1. **Applications de SNMP**

Ce chapitre examine les applications de SNMP dans divers secteurs, mettant en valeur son rôle essentiel dans la gestion du réseau et la surveillance des performances.

* 1. **Utiliser cas dans divers industries**

Le protocole SNMP (Simple Network Management Protocol) est largement utilisé dans de nombreux secteurs en raison de son efficacité pour la surveillance et la gestion des réseaux. Parmi les principaux cas d'utilisation, on peut citer :

* **Télécommunications** : SNMP est essentiel à la surveillance de l'infrastructure réseau, notamment des routeurs, des commutateurs et des stations de base. Il permet aux fournisseurs de garantir la qualité de service, de gérer la bande passante et de réagir rapidement aux pannes ou aux problèmes de performances.
* **Technologies de l'information (TI)** : Dans les environnements informatiques, SNMP est utilisé pour gérer les serveurs, les postes de travail et les périphériques réseau. Il permet aux administrateurs de surveiller l'état du système, de suivre l'utilisation des ressources et d'appliquer des modifications de configuration à distance.
* **Internet des objets (IoT)** : Face à la prolifération des objets connectés, SNMP joue un rôle essentiel dans leur surveillance et leur gestion. Il permet une gestion centralisée de divers objets connectés, garantissant leur fonctionnement efficace et sécurisé.
  1. **Utilisé réseau surveillance outil**

Nombreux applications et outils effet de levier SNMP pour efficace réseau gestion.

Notable exemples inclure

Dans notre cas, nous utilisons Zabbix, une solution de surveillance réseau open source robuste qui fournit des informations détaillées sur les performances et la santé des infrastructures informatiques. Conçue pour surveiller divers composants, notamment les serveurs, les périphériques réseau, les applications et les ressources cloud, elle offre une grande polyvalence pour différents environnements. Voici les principales fonctionnalités de Zabbix [3].

* **Surveillance en temps réel** : Zabbix offre des fonctionnalités de surveillance en direct, permettant aux administrateurs de suivre les performances du réseau et l'état des appareils en temps réel, ce qui est crucial pour la détection immédiate des problèmes.
* **Méthodes de collecte des données** : il prend en charge plusieurs méthodes de collecte de données, notamment SNMP, IPMI, JMX et la surveillance basée sur des agents, offrant une flexibilité dans la manière dont les données sont collectées.
* **Tableaux de bord personnalisables** : les utilisateurs peuvent créer des tableaux de bord personnalisés adaptés à leurs besoins de surveillance spécifiques, affichant des indicateurs clés et des tendances pour une analyse rapide.
* **Alerte et Notifications** : Zabbix dispose d'un puissant système d'alerte qui peut informer les utilisateurs de problèmes potentiels par e-mail, SMS ou autres méthodes de communication, garantissant des réponses rapides aux événements critiques.
* **Évolutivité** : Il est conçu pour évoluer des petits réseaux aux grands environnements d'entreprise, capable de surveiller des milliers d'appareils sans compromettre les performances.
* **Données historiques et rapports** : Zabbix conserve les données historiques, permettant l'analyse des tendances et les rapports de performances, ce qui facilite la planification des capacités et la gestion des ressources.

1. **Progrès et innovations récents**

Cette section explore les derniers développements en matière de gestion de réseau qui améliorent et complètent les fonctionnalités SNMP traditionnelles .

* 1. **Nouveau Protocoles et Cadres complétant SNMP**

Les avancées récentes en matière de gestion de réseau ont introduit de nouveaux protocoles et infrastructures qui améliorent les capacités de SNMP. Des protocoles tels que NETCONF et RESTCONF offrent des moyens plus flexibles et plus efficaces de gérer les périphériques réseau, permettant la configuration et la surveillance via des services web modernes .

* 1. **Intégration avec moderne technologies**

L'intégration de SNMP aux technologies modernes, telles que le cloud computing et l'intelligence artificielle (IA), transforme la gestion des réseaux. Les solutions de surveillance cloud permettent une gestion centralisée des réseaux distribués, tandis que les algorithmes d'IA analysent les modèles de données pour prédire les problèmes réseau et optimiser les performances, améliorant ainsi la fiabilité globale des infrastructures réseau.

* 1. **Développement d’alternatives SNMP**

Face à l'évolution des besoins en gestion réseau, plusieurs alternatives au protocole SNMP sont développées. Les API RESTful, par exemple, offrent une approche plus simple et plus flexible de la gestion réseau, facilitant ainsi l'intégration aux applications et services web. Ces alternatives fournissent aux développeurs les outils nécessaires pour créer des systèmes de gestion réseau plus dynamiques et réactifs.