# Guide SNMP

2025

VINGUETAMA Saneilla

# SNMP

## Qu’est-ce que c’est ?

SNMP signifie Simple Network Management Protocol.
Ce protocole permet de surveiller les performances du réseau et de détecter les pannes afin de garantir la disponibilité des services. Il est donc utiliser pour “monitorer” et va de paire avec un serveur de supervision.

## L’utilisation exacte ?

est un standard majeur pour la gestion des équipements réseau, utilisé pour surveiller leur état, configurer leurs paramètres et recevoir des alertes en cas de dysfonctionnements. Ce protocole est essentiel pour assurer le bon fonctionnement des infrastructures réseau, en permettant une gestion centralisée et une supervision en temps réel des équipements tels que les routeurs, commutateurs, serveurs et imprimantes. Cette capacité, à collecter et à analyser les données en continu est cruciale pour garantir la disponibilité des services et réagir rapidement en cas de panne.

## Les différentes versions (V1, V2 et V3)

Les versions historiques comme SNMPv1 et SNMPv2 sont similaire  cependant elles présentent des faiblesses significatives en matière de sécurité, notamment l'absence de mécanismes robustes pour l'authentification des utilisateurs, la confidentialité des données et l'intégrité des messages. Ces limitations exposent les équipements à des risques sérieux de compromission, comme les attaques par interception, l'usurpation d'identité ou les modifications non autorisées des configurations réseau. SNMPv3 permet de renforcer la sécurité des échanges en intégrant des mécanismes avancés de protection des données. Il permet de réduire les risques de compromission, d'améliorer la résilience du réseau face aux cybermenaces et d'assurer une gestion sécurisée des infrastructures réseau.

# SNMP

## Les versions de SNMP en détail :

Les trois principales versions de SNMP (v1, v2, v3) se distinguent principalement par leurs niveaux de sécurité et leurs fonctionnalités :

- **SNMPv1 (RFC 1157)** : Version initiale, utilisant un système de sécurité simple basé sur des "communautés" (comme public ou private), sans chiffrement ni authentification forte, ce qui la rend vulnérable.
- **SNMPv2** : Introduit des améliorations en termes de performance et de types d'opérations, comme GETBULK (pour récupérer plusieurs variables en une seule requête). Malgré ces progrès, ses variantes (v2c, v2u, v2*) restent limitées en sécurité.
- **SNMPv3** : Le standard actuel, offrant une sécurité renforcée avec chiffrement DES (Data Encryption Standard, 64 bits) et authentification forte, pour une meilleure protection des données. Recommandé pour les infrastructures critiques.

Pour évaluer l'impact des différents niveaux de sécurité, voici un tableau comparatif entre les modes « auth no priv » (authentification sans chiffrement) et « auth priv » (authentification avec chiffrement) :

| Critère | Auth No Priv | Auth Priv |
|---|---|---|
| Authentification | Message authentifiés | Message authentifiés |
| Chiffrement | Données en clair | Données chiffrées |
| Complexité | Moins complexe (pas de gestion du chiffrement) | Plus complexe (chiffrement et gestion des clés) |
| Performance | Moins de surcharge | Moins performant (traitement du chiffrement) |
| Sécurité et configuration | Moyenne et simple | Elevée et complexe |

# SNMP en simple

## Fiche récapitulative

SNMP est un protocole permettant la supervision et la gestion des équipements réseau à distance. Il utilise des agents et des managers pour collecter et envoyer des informations de gestion.

### Composants :

- Agent SNMP : logiciel installé sur les équipements réseau, collecte les informations.
- Manager SNMP : outil de supervision qui interroge les agents pour obtenir des données ou configurer les équipements.

### Versions principales :

- SNMPv1 : version de base, peu sécurisée.
- SNMPv2c : performances améliorées mais même sécurité que v1.
- SNMPv3 : version sécurisée avec chiffrement, authentification et contrôle d'accès.

# SNMP

## Mise en place

### Exemple de configuration SNMPv3 (Routeur Cisco) :

snmp-server group MyGroup v3 priv
snmp-server user MyUser MyGroup v3 auth sha MyAuthPassword priv aes 128 MyPrivPassword

snmp-server view MyView iso included
snmp-server group MyGroup v3 priv read MyView write MyView

### Configuration SNMPv3 sur une VM Linux :

sudo apt-get update
sudo apt-get install snmpd snmp

**# Édition du fichier /etc/snmp/snmpd.conf**
createUser MyUser SHA MyAuthPassword AES MyPrivPassword
rouser MyUser authPriv

**# Redémarrer le service**
sudo systemctl restart snmpd

### Commande de test (via SNMPWALK) :

snmpwalk -v3 -u MyUser -l authPriv -a SHA -A MyAuthPassword -x AES -X MyPrivPassword localhost

Permet de tester la connectivité et les droits d'accès de l'utilisateur SNMPv3