SNMP – OPNsense (Monitoring & Utilisation)

Auteur du document : Sadek Adel

1. Utilité de SNMP

SNMP (Simple Network Management Protocol) est utilisé pour :
- Lire des informations système (OS, uptime, contact, emplacement).
- Surveiller les interfaces réseau (noms, état, trafic RX/TX).
- Faire du monitoring centralisé avec LibreNMS, Observium, Zabbix, Nagios.
- Exporter des métriques à d'autres services (Grafana, Cacti, etc.).

⚠ Limite : SNMP montre des compteurs bruts, mais pas de détail par IP/port comme NetFlow.

2. Installation & Configuration

Sur Debian/Ubuntu (client SNMP)

```
apt update
apt install snmp snmp-mibs-downloader -y
```

➡ But :
- snmp = outils de base.
- snmp-mibs-downloader = installer les MIBs pour avoir les noms lisibles.

Sur OPNsense (agent SNMP)

- Activer Services > Net-SNMP > Général.
- Définir communauté 'public', emplacement, contact.
- Choisir IP d'écoute (ex: 192.168.0.254).
- Vérifier que le firewall autorise UDP/161.

3. Commandes principales

Commande	Description	Exemple

snmpget	Lire un seul objet	snmpget -v2c -c public 192.168.0.254 sysDescr.0
snmpwalk	Lire une branche entière	snmpwalk -v2c -c public 192.168.0.254 IF-MIB::ifTable
snmpbulkwalk	Walk optimisé	snmpbulkwalk -v2c -c public 192.168.0.254
snmpset	Modifier une valeur (RW)	snmpset -v2c -c private 192.168.0.254 sysName.0 s Firewall
snmptranslate	Traduire OID ↔ nom	snmptranslate -Td 1.3.6.1.2.1.2.2.1.2

4. OIDs utiles pour OPNsense

Système (SNMPv2-MIB)
- sysDescr.0 → description système (1.3.6.1.2.1.1.1.0)
- sysUpTime.0 → uptime (1.3.6.1.2.1.1.3.0)
- sysContact.0 → contact admin (1.3.6.1.2.1.1.4.0)
- sysName.0 → hostname (1.3.6.1.2.1.1.5.0)
- sysLocation.0 → localisation (1.3.6.1.2.1.1.6.0)

Interfaces (IF-MIB)
- ifDescr → nom interfaces (1.3.6.1.2.1.2.2.1.2)
- ifOperStatus → état UP/DOWN (1.3.6.1.2.1.2.2.1.8)
- ifInOctets → octets entrants (1.3.6.1.2.1.2.2.1.10)
- ifOutOctets → octets sortants (1.3.6.1.2.1.2.2.1.16)

5. Résultats obtenus sur OPNsense

Commande : snmpwalk -v2c -c public 192.168.0.254 IF-MIB::ifDescr

Résultats :
- vtnet0 → interface physique
- vtnet1 → interface physique
- vtnet2
- vtnet3
- lo0 → loopback
- enc0 → encapsulation (IPsec)
- pflog0 → interface de log firewall

- pfsync0 → réplication état (HA cluster)
- ovpns2 / ovpns3 → OpenVPN servers
- ovpnc1 → OpenVPN client
- tailscale0 → interface Tailscale

6. Tableau récapitulatif des commandes

Index	Commande	OID	Info affichée
1	snmpget sysDescr.0	1.3.6.1.2.1.1.1.0	Version système OPNsense
2	snmpget sysUpTime.0	1.3.6.1.2.1.1.3.0	Uptime firewall
3	snmpget sysContact.0	1.3.6.1.2.1.1.4.0	Contact admin
4	snmpget sysLocation.0	1.3.6.1.2.1.1.6.0	Localisation
5	snmpwalk ifDescr	1.3.6.1.2.1.2.2.1.2	Liste interfaces
6	snmpwalk ifOperStatus	1.3.6.1.2.1.2.2.1.8	État interfaces UP/DOWN
7	snmpwalk ifInOctets	1.3.6.1.2.1.2.2.1.10	Trafic entrant (octets)
8	snmpwalk ifOutOctets	1.3.6.1.2.1.2.2.1.16	Trafic sortant (octets)
9	snmpget tcpCurrEstab.0	1.3.6.1.2.1.6.9.0	Connexions TCP établies
10	snmpget udpInDatagrams.0	1.3.6.1.2.1.7.1.0	Paquets UDP reçus