Adrien Lefebvre
BTS SIO

Document de validation de compétences

AP-4 SUPERVIZ

18/11-16/12/2025 Groupe 5

2. Recherche et choix de la solution

Comparaison des logiciels de monitoring : LibreNMS vs Zabbix

Critères	LibreNMS	Zabbix
Type	Open-source	Open-source
Coût	Gratuit	Gratuit
Interface	Web, moderne et intuitive	Web, personnalisable
Découverte auto	Oui, auto-discovery intégré	Oui, avec configuration
SNMP	Support natif complet SNMPv1/v2c/v3	Support SNMP via templates
Configuration	Simple, rapide à déployer	Plus complexe, puissant
Alertes	Système d'alertes configurable par règles	Alertes avancées avec escalades
Cartographie	Weathermap et topologie réseau	Visualisation avancée
Base de données	MySQL/MariaDB	MySQL/PostgreSQL/Oracle

LibreNMS — Avantages :

- Gratuit et open-source avec découverte automatique des équipements.
- Support SNMP natif très complet, détection automatique du type d'équipement.
- Interface web moderne et intuitive, déploiement rapide.
- Grande communauté et documentation très fournie.

À l'issue de ce comparatif, la solution retenue est LibreNMS.

Recommandations de sécurité SNMP

1. Privilégier SNMPv3 : Utiliser SNMPv3 pour bénéficier de l'authentification, du chiffrement et de l'intégrité. Éviter SNMPv1/v2c qui ne chiffrent pas.

2. Protéger les identifiants : Ne jamais utiliser les communities « public » ou « private ». Créer des utilisateurs dédiés avec mots de passe forts.

3. Limiter les IP autorisées : Autoriser l'accès SNMP uniquement depuis le serveur de supervision (172.20.100.5). Mettre en place des ACL.

4. Lecture seule obligatoire : Configurer SNMP en read-only. Éviter le mode read-write. Créer des vues SNMP limitant les OID visibles.

5. Sécuriser le chemin réseau : Utiliser un VLAN de management pour les flux SNMP. Interdire SNMP depuis l'extérieur. Protéger les ports UDP 161 et 162 par pare-feu.

6. Désactiver si inutile : Désactiver SNMP sur les équipements non supervisés.

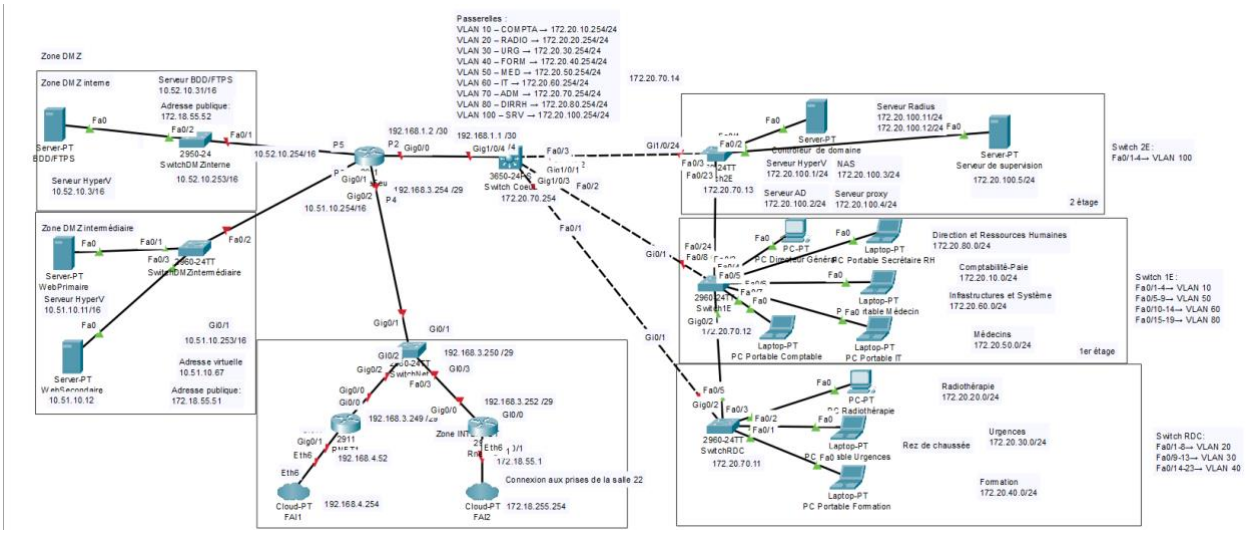
7. Journalisation : Activer les logs SNMP. Surveiller les tentatives d'accès non autorisées.

8. Politique de mots de passe : Utiliser des mots de passe complexes. Changer régulièrement les identifiants SNMP.

9. Documentation : Documenter les communautés, ACL et utilisateurs SNMPv3. Mettre à jour firmwares et agents SNMP régulièrement.

3. Actualisation du schéma réseau

Le schéma réseau a été mis à jour pour intégrer le serveur de supervision LibreNMS (172.20.100.5) dans le VLAN 100-SRV. Les flux SNMP (UDP 161) sont générés depuis le serveur LibreNMS vers l'ensemble des équipements supervisés. Le serveur proxy est en 172.20.100.4.



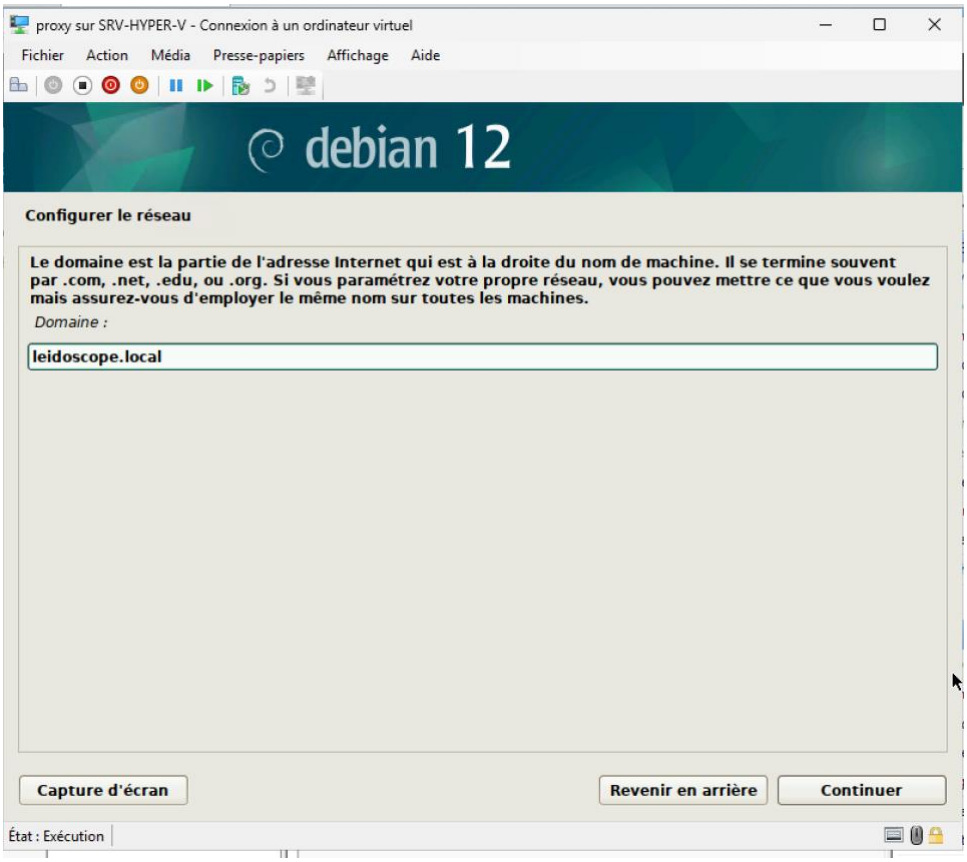
4. Installation de l'infrastructure de supervision

Création de la VM Debian 12

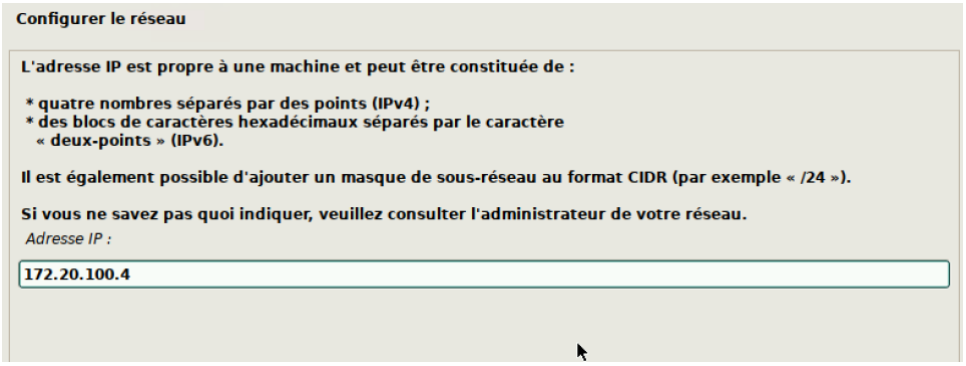
La machine virtuelle hébergeant LibreNMS est créée sur le serveur SRV-HYPER-V. Le système d'exploitation choisi est Debian 12. Lors de l'installation, seuls le serveur SSH et les utilitaires systèmes sont sélectionnés (pas d'interface graphique).

Configuration réseau de la VM :

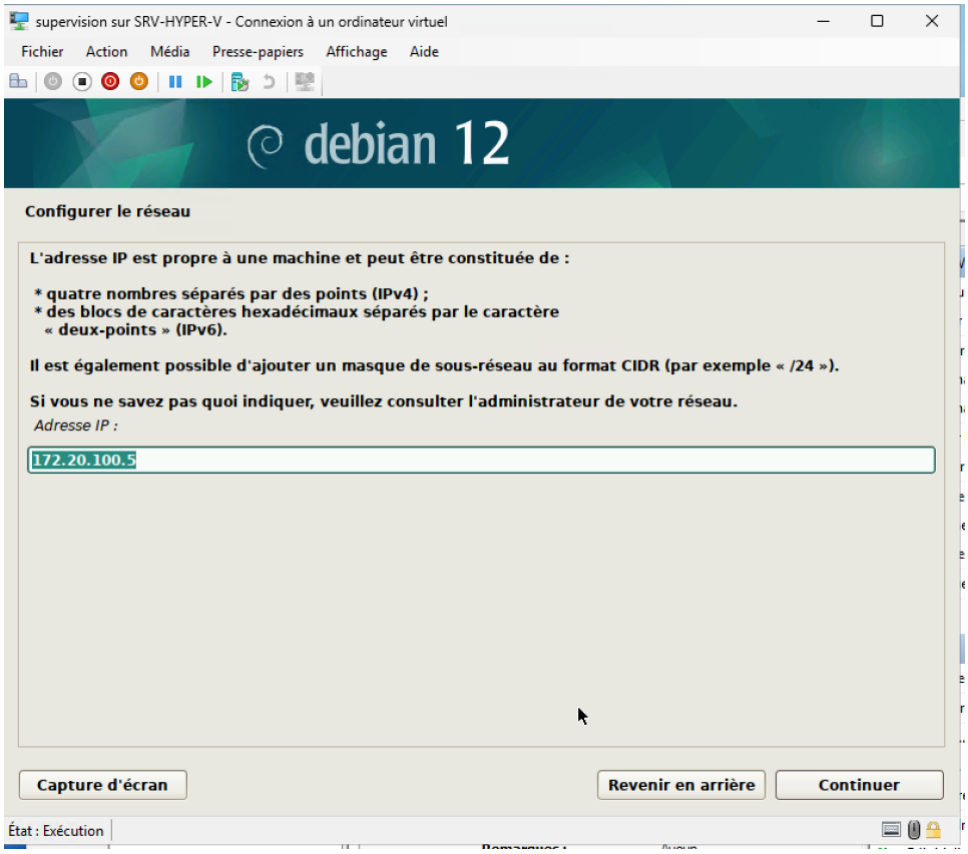
```
IP : 172.20.100.5 / Masque : 255.255.255.0 / Domaine : leidoscope.local
```



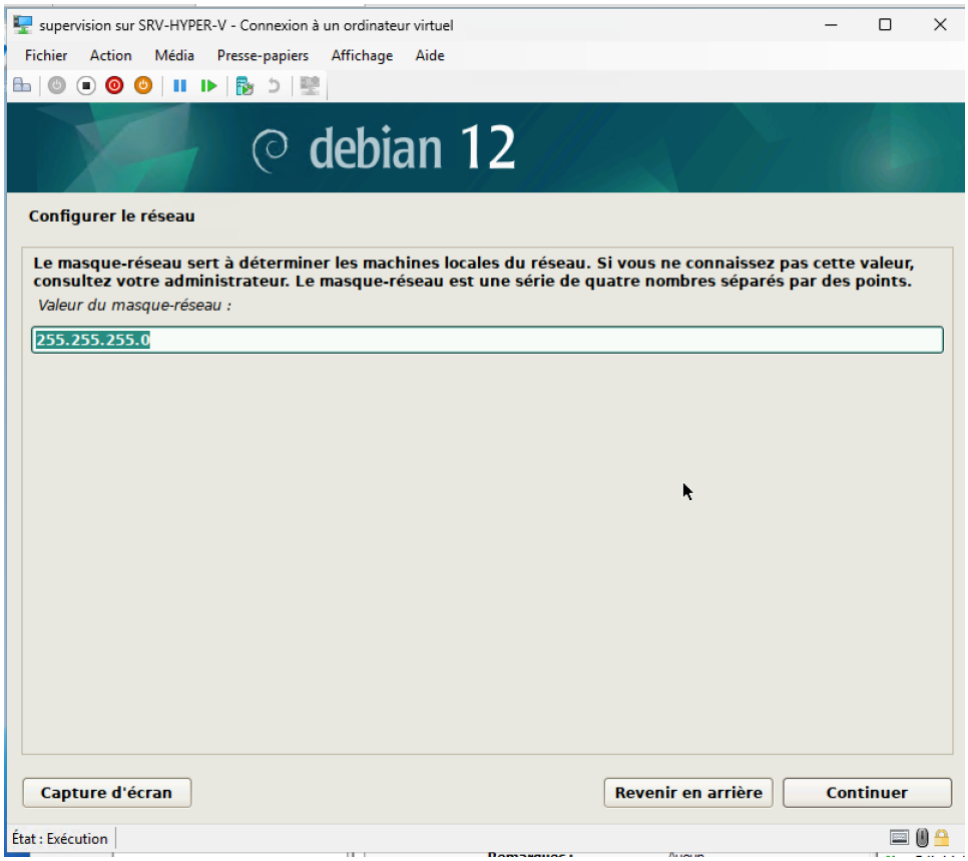
Attribution du domaine leidoscope.local lors de l'installation Debian 12.



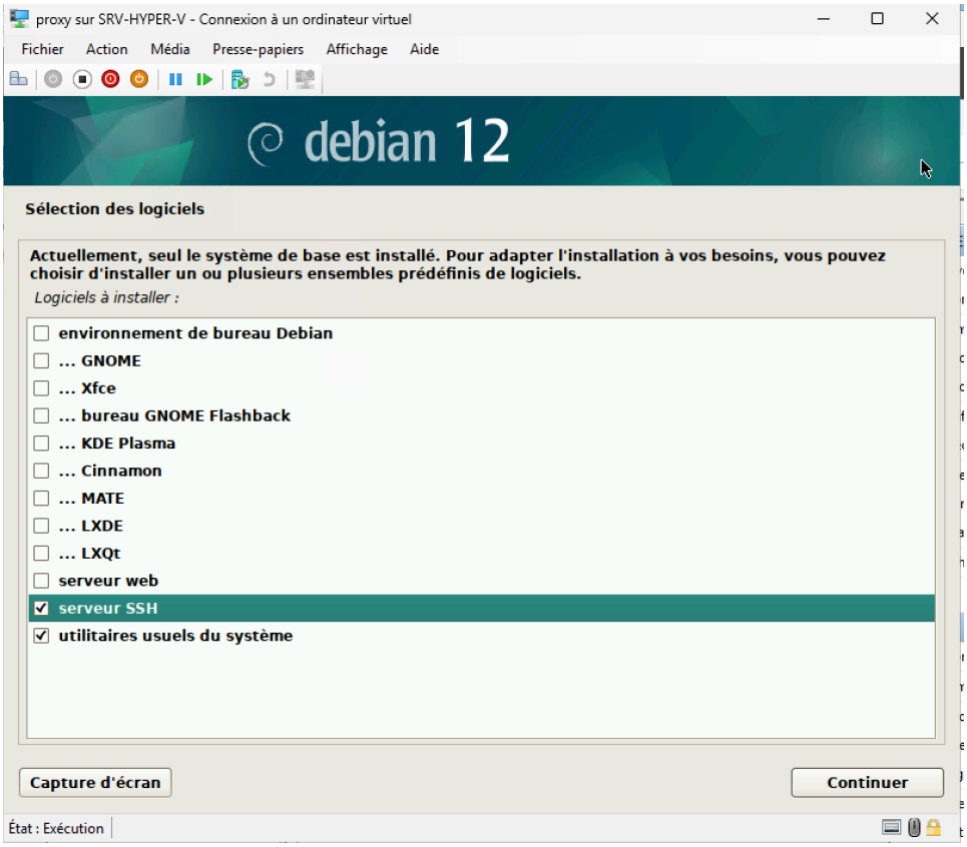
Configuration de l'adresse IP 172.20.100.4 (proxy) lors de l'installation.



Configuration de l'adresse IP 172.20.100.5 pour le serveur de supervision.



Configuration du masque de sous-réseau 255.255.255.0.



Sélection des logiciels : serveur SSH et utilitaires système uniquement (pas d'interface graphique).

Installation de LibreNMS

Installer les dépendances système :

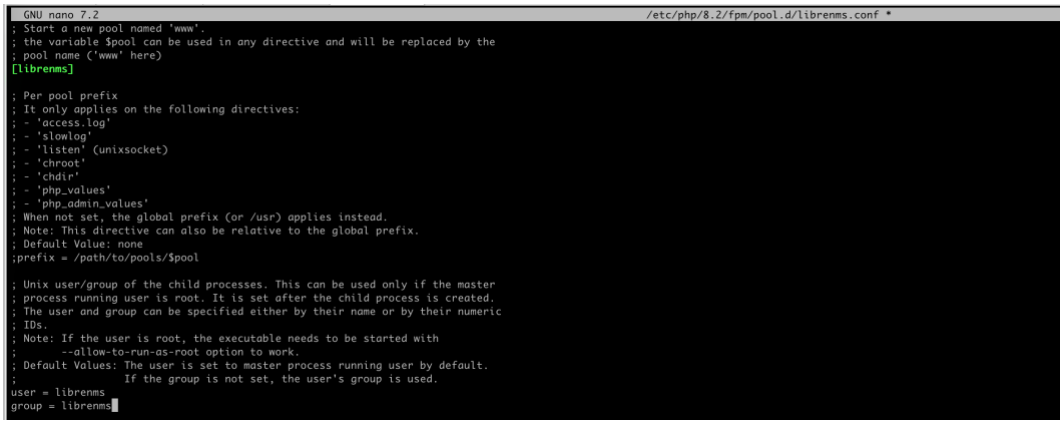
```
apt update && apt upgrade -y
apt install acl curl fping git graphviz imagemagick mariadb-server \
  mtr-tiny nginx-full nmap php-cli php-curl php-fpm php-gd php-gmp \
  php-json php-mbstring php-mysql php-snmp php-xml php-zip rrdtool \
  snmp snmpd whois python3-pymysql python3-dotenv python3-redis \
  python3-psutil unzip
```

Configurer PHP — éditer /etc/php/8.2/fpm/php.ini et /etc/php/8.2/cli/php.ini :

```
date.timezone = Europe/Paris
```

Créer le pool PHP-FPM dédié /etc/php/8.2/fpm/pool.d/librenms.conf :

```
[librenms]
user = librenms
group = librenms
listen = /run/php-fpm-librenms.sock
listen.owner = www-data
listen.group = www-data
```



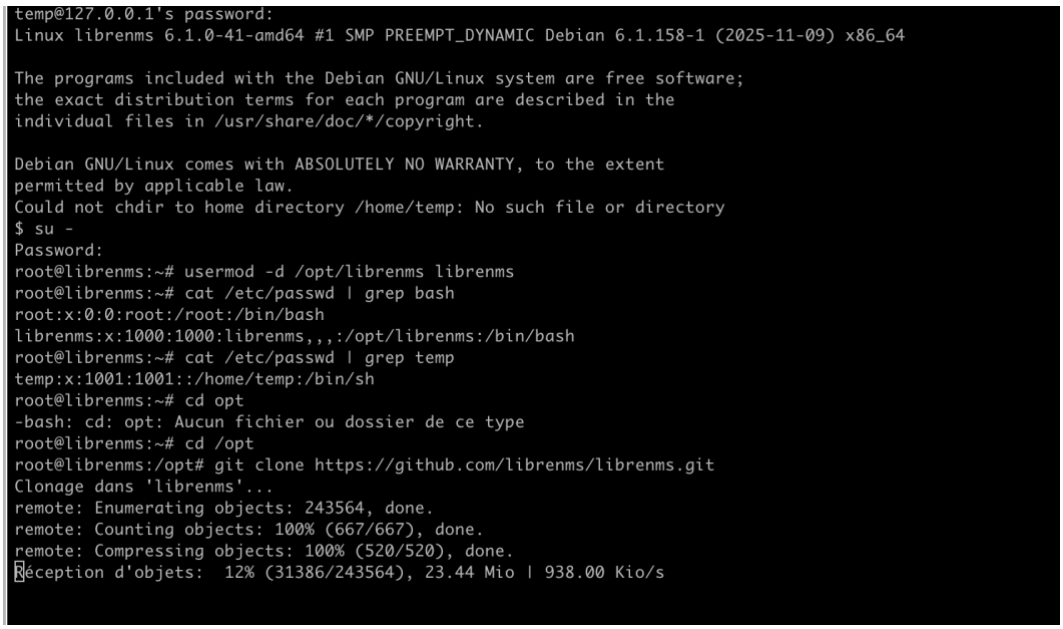
Contenu du fichier de configuration PHP-FPM pour LibreNMS.

Installer les packages Python :

```
pip3 install command_runner --break-system-packages
```

Créer l'utilisateur système LibreNMS et cloner le dépôt :

```
useradd librenms -d /opt/librenms -M -r -s "$(which bash)"
cd /opt
git clone https://github.com/librenms/librenms.git
```



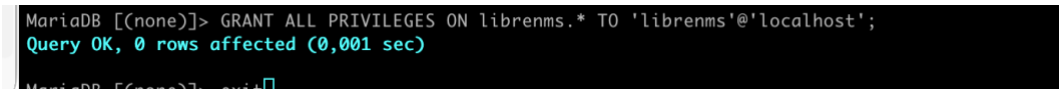
Clonage du dépôt LibreNMS depuis GitHub après connexion SSH au serveur.

Définir les permissions :

```
chown -R librenms:librenms /opt/librenms
chmod 771 /opt/librenms
setfacl -d -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache
/opt/librenms/storage
setfacl -R -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache
/opt/librenms/storage
```

Configurer MariaDB — créer la base de données :

```
mysql -uroot -p
CREATE DATABASE librenms CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'librenms'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON librenms.* TO 'librenms'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```



Attribution des droits complets à l'utilisateur librenms sur la base de données.

Configurer Nginx — créer le vhost /etc/nginx/conf.d/librenms.conf :

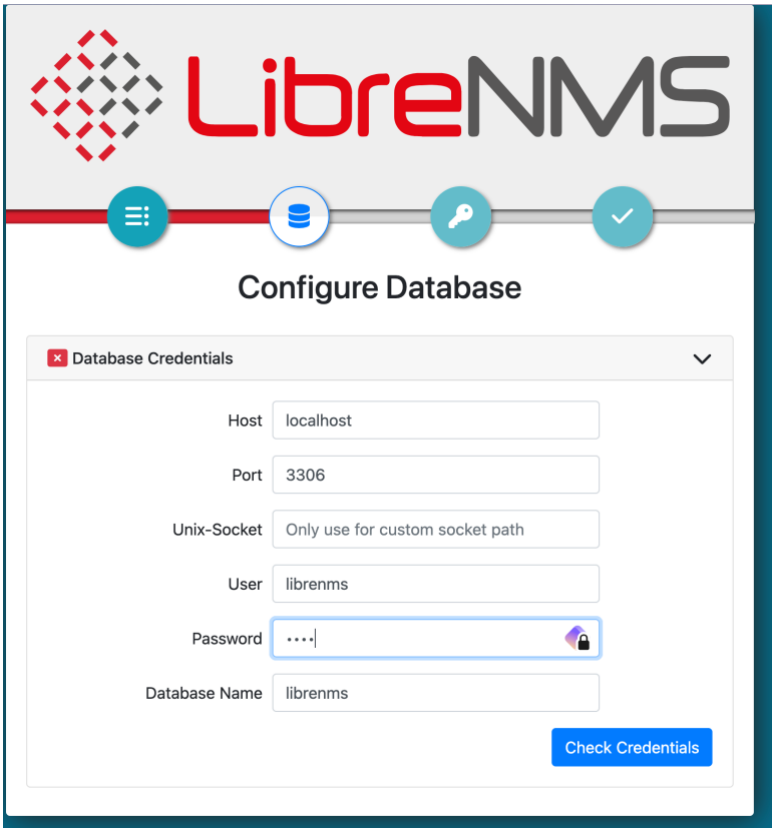
```
server {
    listen      80;
    server_name librenms.leidoscope.com 172.20.100.5;
    root        /opt/librenms/html;
    index       index.php;
    charset utf-8;
    gzip on;
    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }
    location ~ [^/]\.php(/|$) {
        fastcgi_pass unix:/run/php-fpm-librenms.sock;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        include fastcgi.conf;
    }
    location ~ /\.(?!well-known).* { deny all; }
}
```

Redémarrer les services :

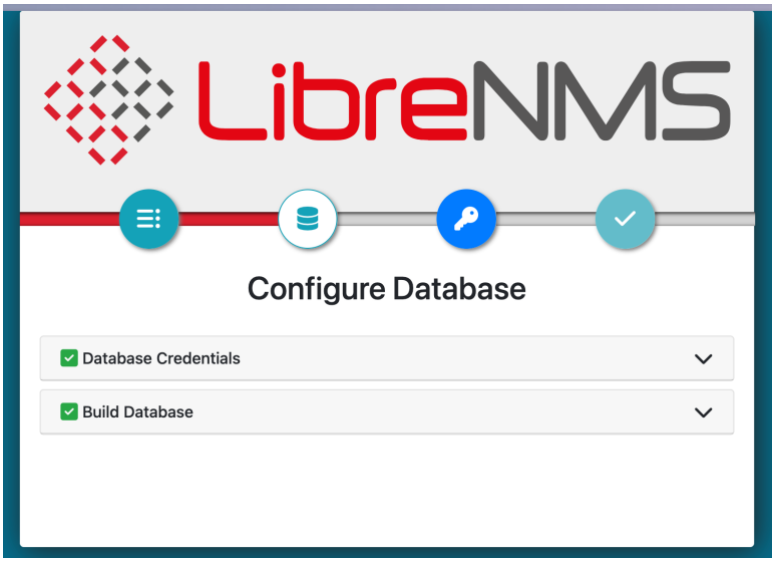
```
systemctl restart php8.2-fpm nginx mariadb
systemctl enable php8.2-fpm nginx mariadb
```

Configuration web de LibreNMS

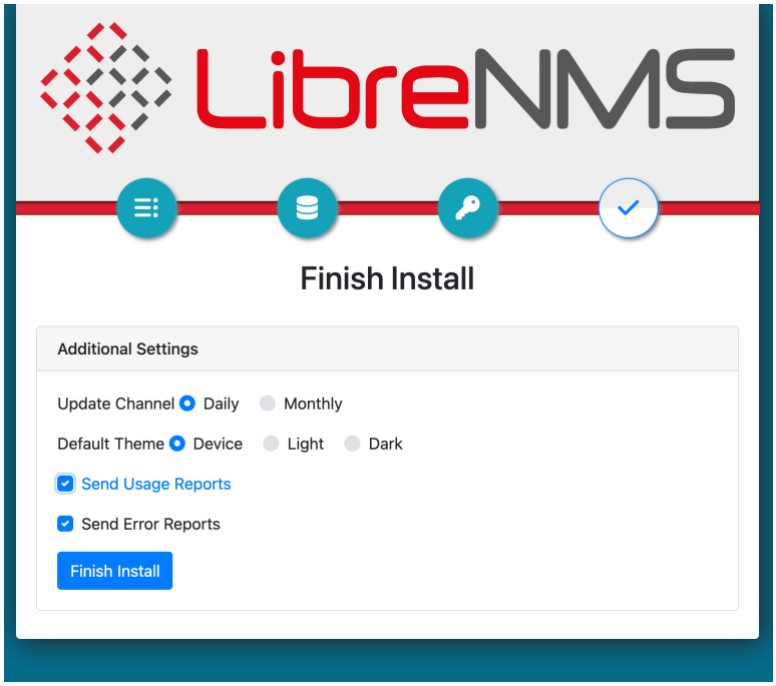
Accéder à l'interface web via http://172.20.100.5. L'assistant de configuration guide les étapes : vérification des prérequis, configuration de la base de données, création du compte admin, et finalisation.



Étape de configuration de la base de données dans l'assistant LibreNMS.



Validation des credentials et construction de la base de données — les deux étapes sont cochées.



Finalisation de l'installation — choix du canal de mise à jour et du thème.

Définir la base URL et configurer le cron :

```
/opt/librenms/lnms config:set base_url http://librenms.leidoscope.com
cp /opt/librenms/dist/librenms.cron /etc/cron.d/librenms
cp /opt/librenms/misc/librenms.logrotate /etc/logrotate.d/librenms
```

5. Mise en place de la surveillance des équipements

Pour les équipements réseau (Cisco — SNMPv2c)

La configuration SNMP est effectuée sur chaque switch et routeur Cisco. En parallèle, NTP est configuré pour garantir la synchronisation des horodatages.

```
! Configuration SNMP sur équipement Cisco
snmp-server community saveol-ro RO
snmp-server location Campus Carlo Acutis
snmp-server contact admin@saveol.fr

! Restriction d'accès au seul serveur LibreNMS
ip access-list standard ACL-SNMP
 permit 172.20.100.5
 deny   any
snmp-server community saveol-ro RO ACL-SNMP

! Configuration NTP
ntp server 172.20.100.5
```

Ajouter chaque équipement réseau dans LibreNMS via Devices > Add Device. Renseigner l'IP, sélectionner SNMP v2c, entrer la community. LibreNMS effectue l'auto-discovery et détecte automatiquement le modèle Cisco.

[Image: /home/claude/superviz/image.png] ([Errno 2] No such file or directory: '/home/claude/superviz/image.png')

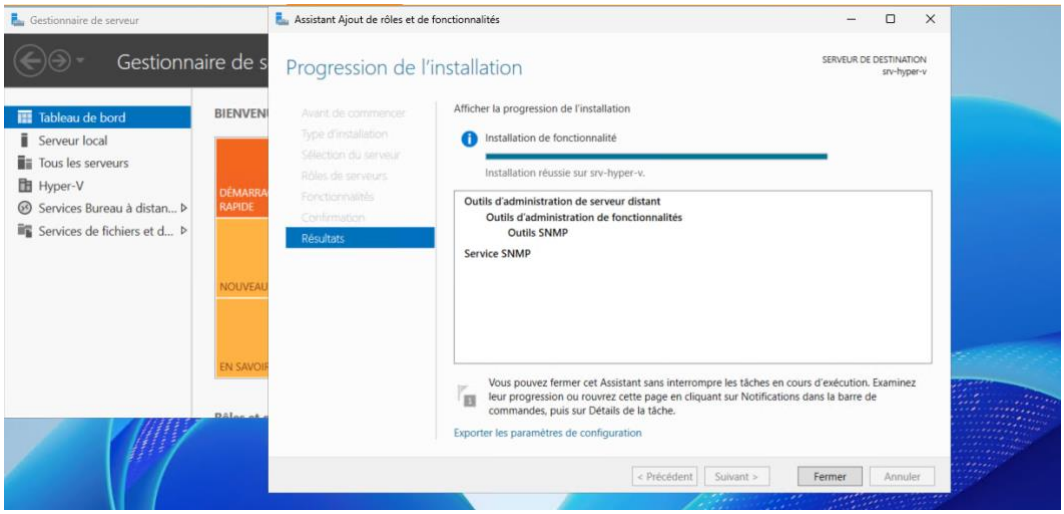
Vue LibreNMS des équipements réseau supervisés : switchs Catalyst 2960/2960X et routeurs Cisco 2911 détectés automatiquement via SNMP. Tous les équipements sont dans l'état "UP" (indicateur orange = avertissements mineurs).

Pour les serveurs Windows (SNMP)

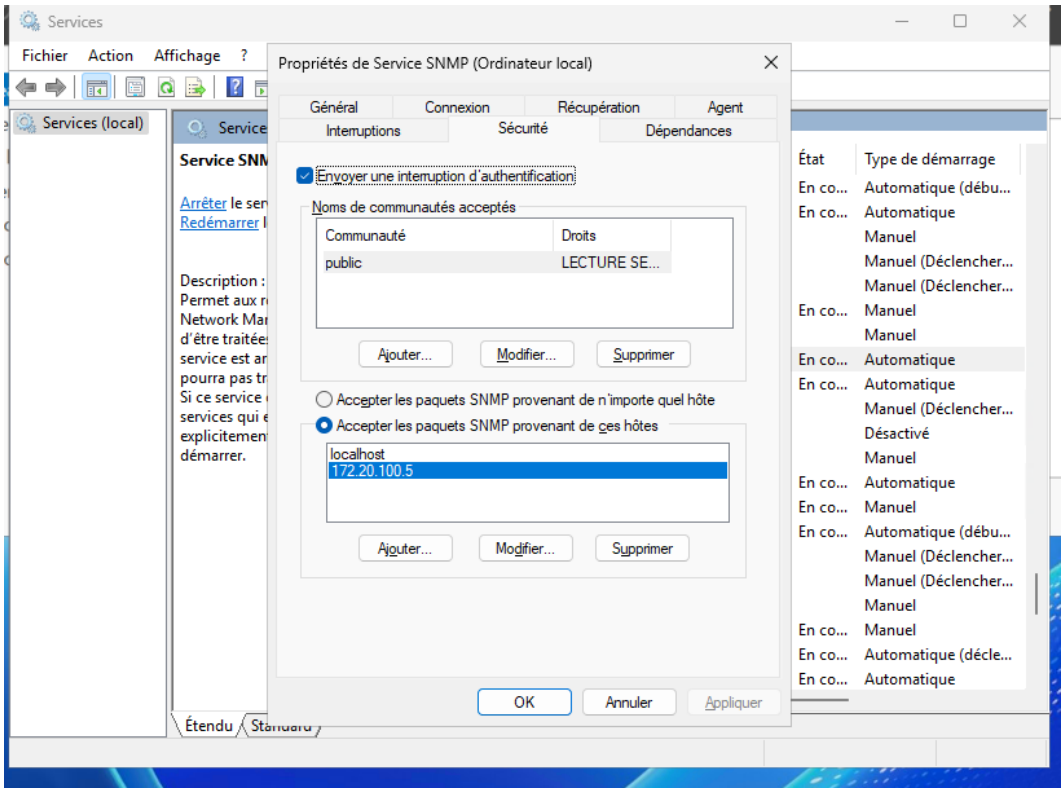
Activer le service SNMP sur chaque serveur Windows via les Fonctionnalités Windows. Configurer la community et autoriser les requêtes depuis 172.20.100.5 uniquement. Ouvrir les ports pare-feu nécessaires via PowerShell :

```
# Autoriser SNMP (UDP 161) entrant — LibreNMS
New-NetFirewallRule -Name "SNMP" -Protocol UDP -LocalPort 161 -Action Allow -Direction Inbound

# Autoriser SNMP-Trap (UDP 162) entrant
New-NetFirewallRule -Name "SNMP-Trap" -Protocol UDP -LocalPort 162 -Action Allow -Direction
Inbound
```

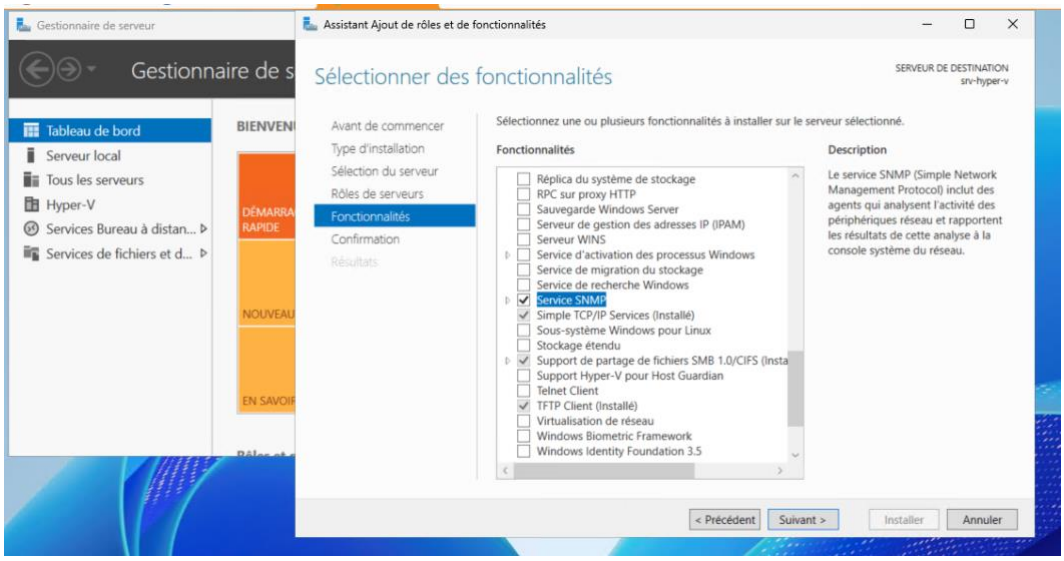


Création de la règle pare-feu Windows pour SNMP UDP 162 (SNMP-Trap) — DisplayName : LibreNMS.



Création de la règle pare-feu Windows pour SNMP UDP 161 — DisplayName : LibreNMS.

Ajouter ensuite le serveur Windows dans LibreNMS. LibreNMS détecte automatiquement l'OS (Microsoft Windows Server 2025) et les métriques associées.



Vue détaillée du serveur srv-hyper-v (172.20.100.1) dans LibreNMS : OS Windows Server 2025, métriques CPU, mémoire et réseau disponibles.

[Image: /home/claude/superviz/image (1).png] ([Errno 2] No such file or directory: '/home/claude/superviz/image (1).png')

Fiche complète du serveur 172.20.100.1 — informations matérielles, uptime, et graphiques de charge processeur en temps réel.

[Image: /home/claude/superviz/image (4).png] ([Errno 2] No such file or directory: '/home/claude/superviz/image (4).png')

Événements récents sur le serveur 172.20.100.1 : ajout du device, détection de l'IP et passage à l'état "Up".

6. Sécurisation des flux réseau

Les règles pare-feu ont été configurées pour n'autoriser que les flux SNMP légitimes entre le serveur LibreNMS (172.20.100.5) et les équipements supervisés.

Source	Destination	Proto	Port	Sens
172.20.100.5 (LibreNMS)	Équipements réseau	UDP	161	Sortant
Équipements réseau	172.20.100.5 (LibreNMS)	UDP	162	Entrant (traps)
172.20.100.5 (LibreNMS)	Serveurs Windows	UDP	161	Sortant
172.20.100.5 (LibreNMS)	Serveurs Linux	UDP	161	Sortant
Admins IT	172.20.100.5	TCP	80	Entrant (interface web)

7. Création de la vue d'ensemble de l'infrastructure

LibreNMS propose plusieurs vues pour visualiser l'état global de l'infrastructure. La page "Devices" liste l'ensemble des équipements supervisés avec leur état en temps réel. La vue "Weathermap" permet de créer une carte topologique de l'infrastructure.

[Image: /home/claude/superviz/image.png] ([Errno 2] No such file or directory: '/home/claude/superviz/image.png')

Vue globale des équipements supervisés dans LibreNMS : 9 équipements réseau Cisco (switchs et routeurs), triés par IP, avec métriques et état de connectivité.

8. Configuration des alertes et notifications

LibreNMS dispose d'un système d'alertes par règles. La configuration se fait dans Alerts > Alert Rules et Alerts > Alert Transports.

Configuration du transport mail

Dans Alerts > Alert Transports > Add Alert Transport, configurer :

```
Transport name : Alerte-Mail-Saveol
Transport type : Mail
Send to : technicien-reseau@saveol.fr ; technicien-systeme@saveol.fr
```

Création des règles d'alerte

Deux règles sont créées :

Règle 1 — Problèmes Réseau : déclenche une alerte et envoie un mail au technicien réseau lorsqu'un équipement d'interconnexion (switch, routeur) passe en état DOWN ou génère une alerte critique.

Règle 2 — Problèmes Système : déclenche une alerte et envoie un mail au technicien système lorsqu'un serveur (Linux ou Windows) présente un problème (CPU > seuil, disque > seuil, service arrêté).

```
# Exemple de règle LibreNMS (macros)
%macros.device_status = 0  -> équipement DOWN
%macros.pct_cpu > 90        -> CPU critique
%macros.storage_perc > 85   -> Disque critique
```

9. Phase de tests et validation du système

Test	Description	Résultat attendu	Résultat obtenu
T01	Découverte automatique d'un switch Cisco	Device ajouté avec bon modèle et OS	OK ✓
T02	Supervision CPU serveur Windows	Graphique CPU affiché en temps réel	OK ✓
T03	Supervision interfaces réseau switch	État des ports visible dans LibreNMS	OK ✓
T04	Déclenchement alerte DOWN (débranchement)	Alerte générée + mail envoyé	OK ✓
T05	Réception mail d'alerte	Mail reçu par le technicien concerné	OK ✓
T06	Vue globale des équipements	Tous les équipements visibles dans Devices	OK ✓
T07	Règle pare-feu SNMP Windows	Serveur Windows supervisé correctement	OK ✓
T08	Authentification SNMP v3 équipements	Échanges chiffrés et authentifiés	OK ✓

10. Production de la documentation projet

L'ensemble des documents produits dans le cadre de ce projet sont regroupés dans un dossier projet finalisé comprenant :

- Le présent document technique (installation, configuration, tests)
- Le schéma réseau actualisé intégrant le serveur LibreNMS
- Les recommandations de sécurité SNMP (ANSSI)
- Un guide utilisateur à destination de l'équipe IT pour l'utilisation quotidienne de LibreNMS
- Le rapport de tests