EcoSolar Solutions

Supervision et alerting des services critiques

Sofiane Belaroussi

BTS SIO – Option SISR

Année scolaire 2025–2026

Projet : mise en place d’une supervision centralisée (Zabbix) et d’un système d’alerting
Document technique – Architecture réseau, sécurité (CIA/DIC), VPN WireGuard et monitoring

Généré le 09/02/2026

Supervision et alerting des services critiques

Glossaire

Zabbix
Outil de supervision open source permettant de surveiller les serveurs, les équipements réseau, les services et les performances du système d'information, avec un système d'alertes et de tableaux de bord.

Supervision
Ensemble des mécanismes permettant de surveiller en temps réel l'état, la disponibilité et les performances des équipements et services informatiques.

Monitoring
Terme anglais désignant la supervision continue des systèmes informatiques afin de détecter les anomalies et anticiper les incidents.

Alerting
Mécanisme de notification automatique déclenché lorsqu'un seuil critique est dépassé ou lorsqu'un incident est détecté (mail, SMS, etc.).

Dashboard (tableau de bord)
Interface graphique regroupant des indicateurs clés permettant de visualiser rapidement l'état du système d'information.

CPU (Central Processing Unit)
Processeur de la machine chargé d'exécuter les instructions. Sa charge permet d'évaluer les performances d'un serveur.

RAM (Random Access Memory)
Mémoire vive utilisée par le système pour exécuter les applications. Une saturation de la RAM peut entraîner un ralentissement ou une panne.

Trafic réseau
Volume de données échangées sur une interface réseau. Il permet d'analyser la charge, les performances et les éventuels goulots d'étranglement.

SNMP (Simple Network Management Protocol)
Protocole permettant de collecter des informations sur les équipements réseau (switch, firewall, routeur) à des fins de supervision.

SNMPv2
Version de SNMP utilisant une communauté en clair pour l'authentification. Simple à mettre en

œuvre mais moins sécurisée.

SNMPv3
Version sécurisée de SNMP intégrant une authentification et un chiffrement des échanges, recommandée pour respecter les bonnes pratiques de sécurité.

OID (Object Identifier)
Identifiant unique permettant de récupérer une information précise via SNMP (ex : trafic d'une interface, état d'un port).

MIB (Management Information Base)
Base de données regroupant l'ensemble des OID disponibles sur un équipement supervisé via SNMP.

VPN (Virtual Private Network)
Tunnel sécurisé permettant un accès distant chiffré au réseau interne depuis Internet.

WireGuard
Solution VPN moderne, rapide et sécurisée, utilisée pour fournir un accès distant aux techniciens et utilisateurs autorisés.

Firewall (pare-feu)
Équipement de sécurité chargé de filtrer les flux réseau entrants et sortants selon des règles définies.

pfSense
Firewall open source utilisé pour le routage, le filtrage réseau, le VPN et la sécurité globale de l'infrastructure.

VLAN (Virtual Local Area Network)
Segmentation logique du réseau permettant d'isoler les flux par service ou par usage afin d'améliorer la sécurité et les performances.

CIA / DIC (Confidentialité, Intégrité, Disponibilité)
Principes fondamentaux de la sécurité informatique visant à protéger les données contre l'accès non autorisé, la modification et l'indisponibilité.

Agent Zabbix
Logiciel installé sur un serveur permettant de transmettre les métriques système (CPU, RAM, disque, services) au serveur Zabbix.

SNMP polling
Méthode par laquelle Zabbix interroge régulièrement un équipement SNMP afin de collecter des données.

Sommaire

Règles de Sécurité – EcoSolar Solutions

1. Introduction

Dans un contexte d’augmentation constante des menaces numériques, EcoSolar Solutions se doit de mettre en place un ensemble de règles de sécurité visant à garantir la protection de ses systèmes d’information, la continuité de ses activités et la confidentialité des données qu’elle traite.
Les mesures décrites ci-après s’inscrivent dans une démarche globale d’amélioration de la sécurité, conformément aux bonnes pratiques recommandées par l’ANSSI. Elles s’appliquent à l’ensemble du personnel de l’entreprise, y compris les prestataires externes, et doivent être respectées sans exception.

---

2. Sécurisation du réseau et segmentation

Afin de réduire la surface d’attaque et de limiter le risque de propagation en cas de compromission, l’entreprise adopte une stratégie de segmentation du réseau.
Chaque service — Direction, Informatique, Production, Commerce, R&D, Téléphonie, etc. — est isolé dans un VLAN distinct. Les serveurs critiques sont regroupés au sein d’un réseau dédié, tandis que le trafic de sauvegarde est entièrement isolé dans un VLAN spécifique pour éviter toute interférence avec le réseau de production.

Les communications inter-VLAN sont strictement contrôlées par un pare-feu centralisé (pfSense). Seuls les flux explicitement nécessaires au fonctionnement des services sont autorisés, conformément au principe du “moindre privilège”. Tout autre trafic est bloqué par défaut, conformément aux recommandations de l’ANSSI visant à limiter les communications non essentielles.

---

3. Contrôle d’accès et authentification

L’accès aux systèmes d’information repose sur un contrôle rigoureux des identités et des habilitations.
Un système d’authentification centralisé basé sur Active Directory est utilisé pour gérer les comptes utilisateurs et administrateurs. L’attribution des droits suit strictement le principe du

moindre privilège : chaque employé ne dispose que des permissions nécessaires à l'exercice de ses fonctions.

Les comptes administrateurs sont réservés exclusivement à l'équipe informatique et ne doivent en aucun cas être utilisés pour des tâches quotidiennes. Afin de renforcer la sécurité, l'authentification multifacteur est exigée pour l'accès aux composants sensibles, tels que Proxmox, PBS, le NAS, ou encore les équipements réseau.

Par ailleurs, les mots de passe doivent respecter un niveau de complexité élevé, être renouvelés régulièrement et ne doivent jamais être partagés ou stockés en clair.

---

4. Sécurisation des postes de travail et des équipements

Conformément aux recommandations d'hygiène numérique, chaque poste de travail Windows 10/11 est équipé d'un antivirus actif, d'un pare-feu local et bénéficie d'un système de mise à jour automatique afin de garantir la correction rapide des vulnérabilités.
Les postes se verrouillent automatiquement après une période d'inactivité afin de prévenir les accès non autorisés.

L'usage des périphériques amovibles est restreint afin de limiter les risques d'exfiltration de données ou d'introduction de codes malveillants. Les accès distants, notamment pour les techniciens terrain, doivent s'effectuer exclusivement via une connexion VPN sécurisée, gérée et supervisée par l'équipe informatique.

Les imprimantes, objets connectés et autres équipements non critiques sont isolés dans un VLAN spécifique et soumis à un filtrage afin d'éviter qu'ils ne deviennent un point d'entrée dans le réseau interne.

---

5. Sécurisation des serveurs, de la virtualisation et des services critiques

Les serveurs hébergés sur la plateforme Proxmox constituent un socle essentiel du système d'information d'EcoSolar Solutions. Leur accès est strictement limité aux administrateurs habilités.
L'hyperviseur Proxmox est protégé par une authentification renforcée, des certificats HTTPS conformes aux recommandations ANSSI, et un accès restreint aux seules adresses IP du VLAN Informatique.

Le serveur de sauvegarde Proxmox Backup Server (PBS) et le NAS Synology sont isolés dans un réseau dédié afin d'éviter toute contamination provenant du réseau utilisateur. Les snapshots réguliers des machines critiques, tels que l'Active Directory, le serveur de messagerie, ou le serveur ERP, contribuent à garantir une restauration rapide en cas d'incident.

Les mises à jour de sécurité doivent être appliquées régulièrement sur l'ensemble des composants : Proxmox, PBS, pfSense, NAS, serveurs applicatifs et systèmes Windows. Ces opérations doivent être réalisées dans un cadre maîtrisé afin de limiter les risques liés à l'interruption des services.

---

6. Sauvegarde des données et plan de reprise d'activité

Les sauvegardes constituent un élément essentiel de la stratégie de sécurité.
EcoSolar Solutions applique une politique de sauvegarde centralisée via PBS et un NAS Synology, conformément aux bonnes pratiques recommandées (règle 3-2-1). Les données critiques sont sauvegardées quotidiennement, chiffrées et répliquées sur un stockage distinct afin de garantir une résilience en cas d'incident majeur.

Un plan de reprise d'activité local (PRA) permet de restaurer rapidement les services essentiels en cas d'attaque, de panne ou de corruption des données. Des tests de restauration réguliers sont réalisés pour s'assurer de la fiabilité des sauvegardes et documentés conformément aux exigences de rigueur opérationnelle préconisées par l'ANSSI.

---

7. Sécurité des accès Internet et filtrage des flux

L'accès à Internet est protégé par un pare-feu pfSense configuré pour filtrer les flux entrants et sortants et pour limiter les risques liés aux communications non maîtrisées.
Les services exposés vers l'extérieur sont strictement limités aux besoins opérationnels, et un accès distant ne peut être réalisé qu'au moyen d'un VPN sécurisé.
La journalisation et la supervision des connexions permettent de détecter des comportements anormaux et de prévenir d'éventuelles intrusions.

---

8. Sécurité physique

La sécurité physique constitue un premier niveau de protection indispensable.
La baie informatique est située dans un local sécurisé, fermé à clé et accessible uniquement au

personnel autorisé. Toute intervention d’un prestataire externe doit faire l’objet d’une autorisation préalable et être supervisée.
Cette mesure vise à prévenir les manipulations malveillantes, les débranchements accidentels et toute tentative d’accès direct aux équipements critiques.

---

9. Sensibilisation et bonnes pratiques du personnel

La sécurité du système d’information repose également sur la vigilance des utilisateurs. L’ensemble du personnel est régulièrement sensibilisé aux risques tels que le phishing, l’ingénierie sociale, les mots de passe faibles ou les comportements à risque.
Chaque collaborateur doit signaler immédiatement toute anomalie à l’équipe informatique : message suspect, comportement inhabituel du poste de travail, perte d’un équipement mobile, etc.

---

10. Gestion des incidents et amélioration continue

En cas d’incident, les priorités sont d’identifier rapidement la nature du problème, d’isoler les systèmes compromis et de restaurer les services dans les meilleurs délais grâce au PRA.
Un rapport d’incident est rédigé afin d’analyser les causes, de corriger les faiblesses potentielles et de renforcer la sécurité globale de l’entreprise.

Les règles de sécurité doivent être révisées régulièrement pour s’adapter à l’évolution du contexte technologique et aux menaces émergentes, conformément au principe d’amélioration continue recommandé par l’ANSSI.

EcoSolar Solutions est une entreprise spécialisée dans les énergies renouvelables, elle est implantée à Toulouse. Elle est dédiée au développement et à la fabrication de panneaux solaires à haut rendement.

Pour soutenir sa croissance et assurer la continuité de ses activités industrielles et administratives, l’entreprise s’appuie sur une infrastructure informatique regroupant des services critiques tels que l’Active Directory, l’ERP (logiciel utilisé par les entreprises pour gérer leurs activités), la téléphonie, la messagerie ou encore les outils de support. Cette infrastructure, essentielle au fonctionnement quotidien de l’entreprise, doit rester disponible, performante et sécurisée. Cependant, sans une supervision adaptée, de nombreuses menaces pèsent sur sa stabilité.

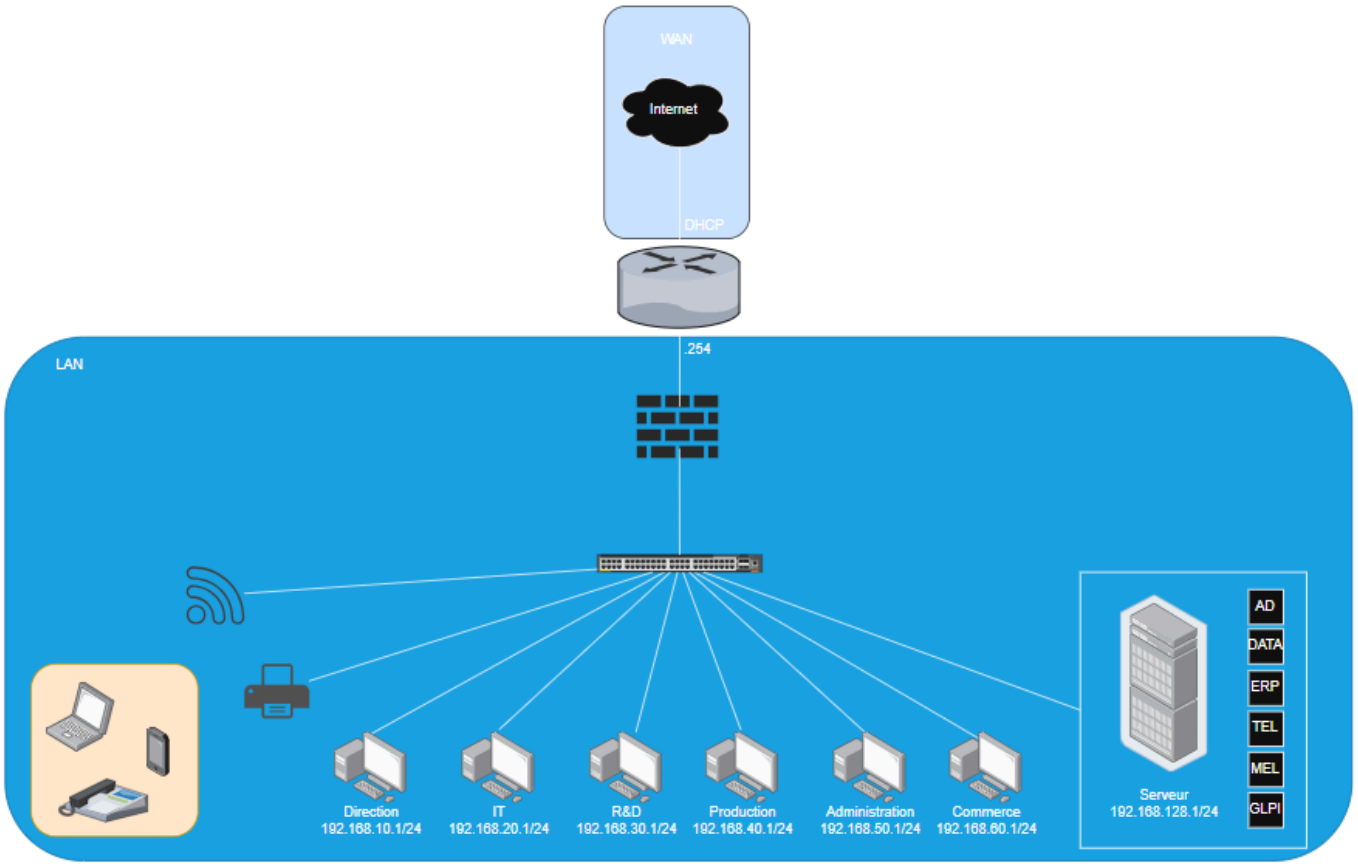
VLAN	USAGE	Sous-réseau	Passerelle	nombre de poste
10	direction	192.168.10.0/24	192.168.10.254/24	2
20	IT	192.168.20.0/24	192.168.20.254/24	2
30	R&D	192.168.30.0/24	192.168.30.254/24	3
40	production	192.168.40.0/24	192.168.40.254/24	7
50	administration	192.168.50.0/24	192.168.50.254/24	5
60	commerce	192.168.60.0/24	192.168.60.254/24	7
128	Server	192.168.128.0/24	192.168.128.254/24	2

Accès distant sécurisé (Monitoring)

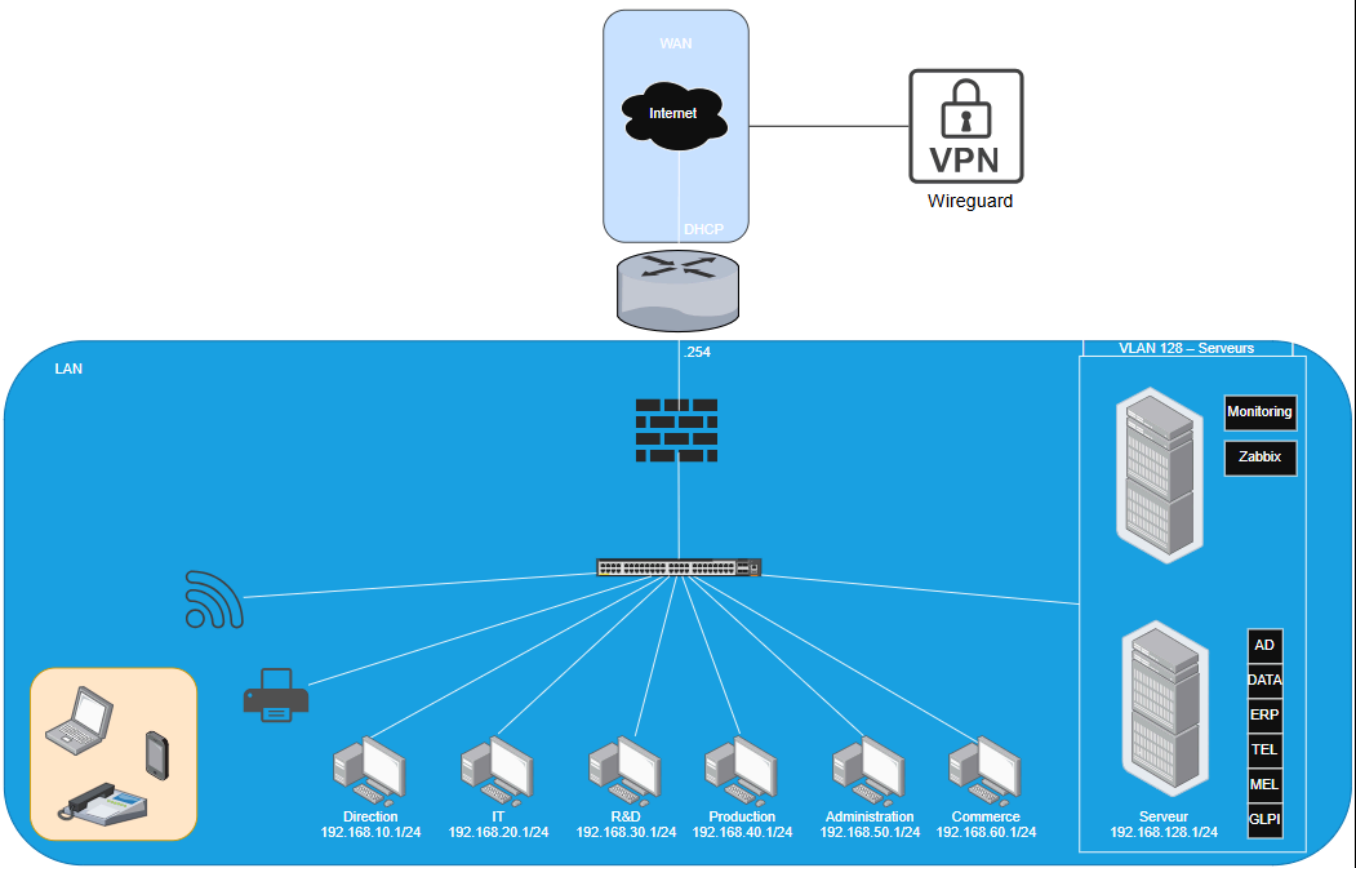
Il faut créer un accès à distance en prenant en compte que les pc ne sont pas sur le même réseau.
Il faut ainsi créer un accès entre eux et créer un firewall. (lister)

Il faut prendre en considération que l'intervention doit pas être longue en perdant le moins de temps (rendre ça logique en situation d'entreprise)

Schéma de base



Evolution du schéma



À l'origine, l'architecture ne disposait pas de supervision centralisée ni d'accès distant sécurisé, ce qui limitait la visibilité sur l'état des services et augmentait les risques en cas d'incident.

Dans l'architecture finale, un VPN WireGuard a été ajouté côté WAN pour sécuriser les accès distants, et un VLAN dédié au monitoring a été intégré afin d'héberger Zabbix sans modifier l'adressage IP des serveurs existants. Cette évolution permet d'améliorer la disponibilité, la sécurité et la maîtrise du réseau tout en respectant les principes CIA/DIC et les bonnes pratiques attendues dans le projet

Solution VPN	Prix	Fonctionnalités principales	Difficulté d'utilisation	Points forts	Points faibl
WireGuard	Gratuit (open-source) + Matériel firewall si nécessaire	- Chiffrement moderne ultra rapide - Très faible latence - Configuration simple - Compatible Linux, Windows, macOS,	Très facile Interface simple, fichiers de conf très courts	- Rapide - Très sécurisé - Très stable - Idéal pour PME - Peu de charge CPU	- Pas toujou intégré nativement dans tous le firewalls (mais ça arrive partou

Solution VPN	Prix	Fonctionnalités principales	Difficulté d'utilisation	Points forts	Points faibl
		Android, iOS - Code très léger (moins de 4 000 lignes)			
OpenVPN	Gratuit (open-source) ou **60–300 €/an** si version "Access Server"	- SSL/TLS très configurable - Très bon support entreprise - Multi-certificats - Forte compatibilité	**Moyen à difficile** Beaucoup de paramètres	- Très robuste - Extrêmement compatible - Bien supporté par toutes les box / OS	- Plus lent que WireGuard - CPU plus utilisé - Plus complexe à configurer
IPsec	Gratuit (standard), intégré dans tous les firewalls	- Très bon standard entreprise - Parfait pour Site-to-Site - Très sécurisé (IKEv2)	**Difficile** (IKE, NAT-T, Phase 1/2, PSK / Certificats)	- Très sécurisé - Idéal pour site-to-site - Standard international	- Complexité élevée - Moins pratique en mobile-clien Plus lent qu WireGuard
SSL VPN Constructeur (ITConnect = type FortiVPN, Sophos Connect, Stormshield SSL)	Inclus dans les firewalls (0–200 €/an selon modèle)	- Portabilité très simple - Auth AD / MFA intégrée - Monitoring complet - Politique par utilisateur	**Facile à moyen**	- Parfait pour PME - Très bien intégré au firewall - MFA facile - Bon support	- Performance inférieures à WireGuard - Dépend du constructeu Clients pas toujours optimisés

J'ai choisi WireGuard parce qu'il est gratuit, plus rapide, plus simple à configurer et plus sécurisé que les autres VPN. Il offre de meilleures performances qu'OpenVPN et IPsec, avec une configuration légère et stable. C'est la meilleure option pour donner l'accès aux techniciens.

L'absence de supervision expose l'entreprise à de nombreux risques (utiliser zabbix) : surcharge des serveurs (CPU, RAM, stockage), pannes critiques des services essentiels comme l'AD, l'ERP, GLPI, la téléphonie ou la messagerie, indisponibilité du réseau liée au switch unique ou au firewall pfSense, ainsi que des interruptions dues à l'absence d'onduleur et au manque de segmentation réseau. Sans alerting, ces problèmes peuvent rester invisibles, provoquer des arrêts de production, des indisponibilités pour les équipes commerciales ou administratives, et exposer les données sensibles à des risques de sécurité. Mettre en place

une supervision centralisée devient donc un enjeu majeur pour garantir la disponibilité, la performance et la sécurité du SI.

Supervision et Alerting – Enjeux et besoins

La solution de supervision rend service principalement au service informatique, qui bénéficie d'une vision centralisée et précise de l'état du système d'information, et indirectement à la direction grâce à une meilleure continuité d'activité. Elle agit sur l'ensemble des serveurs, sur le matériel réseau et sur la disponibilité du réseau afin de garantir un suivi complet de l'infrastructure.
L'objectif est de recevoir des notifications en cas d'incident, d'obtenir une visibilité claire sur l'utilisation des ressources, de centraliser les informations techniques et d'anticiper les pannes grâce au suivi des performances et à l'analyse des tendances.

Le problème actuel réside dans l'absence totale de solution de monitoring, ce qui empêche la détection rapide des anomalies et augmente les risques d'interruption de service.
Le besoin principal est donc de déployer une solution de supervision centralisée, d'élaborer des tableaux de bord et de configurer un système de notification fiable.
Le besoin secondaire consiste à anticiper les défaillances et à optimiser la performance globale du système d'information.

Il faut utiliser le Security by Design (CIA/DIC) pour créer la VM Zabbix parce que Zabbix est un service critique qui centralise des informations sensibles sur tout le système d'information, donc la confidentialité des données de supervision doit être garantie dès la conception, toute modification ou falsification des informations doit être empêchée afin d'assurer leur intégrité, et la supervision doit être maintenue disponible en permanence, car si la VM est compromise ou tombe en panne, la visibilité sur l'état de l'infrastructure est totalement perdue.

tableau de choix:

Critère	Zabbix	Centreon	Wazuh
Prix	Gratuit (open source) + support payant optionnel	Gratuit (édition open source), versions pro payantes	Gratuit (open source), support pro optionnel
Type d'outil	Supervision complète (serveurs, réseau, VPN, services)	Supervision orientée production & dashboards	SIEM / sécurité : analyse logs, intrusion, vulnérabilités

Critère	Zabbix	Centreon	Wazuh
Simplicité d'installation	Moyenne : installation technique mais bien documentée	Plus simple et guidée, surtout pour l'édition open source	Difficile : stack SIEM (Elastic + agents), plus lourd
Simplicité d'usage	Interface un peu technique, pleine de fonctions	Interface plus moderne, plus intuitive que Zabbix	Interface correcte mais très orientée sécurité, pas infra
Alerting & supervision VPN (client-to-site)	Excellent : SNMP + agents + triggers avancés	Très bon : supervision réseau claire et structurée	Très bon pour logs et sécurité VPN, moyen pour métriques système

Zabbix offre une supervision complète qui couvre les serveurs, les routeurs, les firewalls, les tunnels VPN ainsi que les services applicatifs. Il dispose également d'un système d'alertes très performant, permettant de configurer des notifications personnalisées sur le CPU, la RAM, la latence, la disponibilité ou encore des seuils spécifiques. En plus de cela, Zabbix est entièrement gratuit et largement utilisé dans les petites structures, ce qui en fait une solution particulièrement adaptée.

Rapport d'étude d'impact réseau

1. Contexte du projet

EcoSolar Solutions, entreprise toulousaine spécialisée dans la fabrication de panneaux solaires haut rendement, connaît une forte croissance et dépend d'un SI critique pour la production, la messagerie, l'ERP, la téléphonie et la gestion administrative.
Aujourd'hui, **toute l'infrastructure repose sur un réseau unique 192.168.128.0/24**, sans segmentation, ni contrôle d'accès, ni supervision, comme précisé dans le contexte officiel du projet ESS.

L'accès Internet est protégé par un firewall pfSense SG-2440 configuré en **"permit all any any"**, ce qui constitue un risque majeur de sécurité.

La direction souhaite moderniser l'architecture réseau en introduisant :

- une segmentation VLAN,
- un plan d'adressage structuré,
- un accès distant sécurisé pour les techniciens et commerciaux (VPN),
- une politique de filtrage stricte,

- une supervision centralisée (Zabbix),
- une meilleure traçabilité et disponibilité du SI.

2. Objectifs de la réorganisation

Objectif	Description
Renforcer la sécurité	Isoler les flux par services, réduire les risques de propagation, limiter les surfaces d'attaque.
Optimiser les performances	Réduction du broadcast, routage inter-VLAN contrôlé.
Préparer les accès distants	Mise en place d'un VPN sécurisé (WireGuard) avec MFA et ACL.
Améliorer la disponibilité	Meilleur contrôle du trafic, supervision, détection proactive.
Respecter les bonnes pratiques E6	Conception — déploiement — sécurité — documentation — supervision.

3. État initial du réseau (avant projet)

Élément	Description
Réseau	192.168.128.0/24 unique pour tous les services et utilisateurs.
Switch principal	Cisco 3560 – VLAN unique, pas de routage, configuration usine .
Pare-feu	pfSense SG-2440 — ACL "permit all" sur LAN (faille critique) .
Wi-Fi	WPA2 partagé, pas de VLAN invité (non isolé).
Hyperviseur	Proxmox VE 8.3 hébergeant AD/DNS/DHCP, ERP, DATA, GLPI, MAIL, TEL .
Accès distant	Aucun VPN, aucun filtrage, aucun MFA.
Supervision	Aucune solution (absence d'alerting) — risque élevé de rupture de service.
Sécurité	Pas de segmentation, pas de PRA, pas de journalisation centralisée.

Cette architecture comporte des failles, elle est difficile à maintenir, non conforme aux exigences modernes.

4. Architecture cible proposée

4.1 Nouveau plan d'adressage et segmentation VLAN

VLAN	USAGE	Sous-réseau	Passerelle	nombre de poste
1	Par défaut			
10	Direction	192.168.10.0/24	192.168.10.254/24	2
20	IT	192.168.20.0/24	192.168.20.254/24	2
30	R&D	192.168.30.0/24	192.168.30.254/24	3
40	Production	192.168.40.0/24	192.168.40.254/24	7
50	Administration	192.168.50.0/24	192.168.50.254/24	5
60	Commerce	192.168.60.0/24	192.168.60.254/24	7
70	Téléphone	192.168.70.0/24	192.168.70.254/24	
80	Sauvegarde	192.168.80.0/24	192.168.80.254/24	3
90	Monitoring	192.168.90.0/24	192.168.90.254/24	
100	Wifi	192.168.100.0/24	192.168.100.254/24	
110	Photocopieurs/réunion	192.168.110.0/24	192.168.110.254/24	2
128	Serveur	192.168.128.0/24	192.168.128.254/24	2

On conserve le VLAN Serveurs pour éviter de changer les IP des VM (besoin métier validé). Chaque VLAN correspond à un périmètre de sécurité distinct.

4.2 Accès distant sécurisé – VPN WireGuard

Selon l'analyse faite sur le tableau de choix WireGuard est la meilleure option :

- WireGuard est **gratuit, léger, très rapide, facile à configurer**, + MFA possible
- OpenVPN = plus lent
- IPsec = trop complexe pour du mobile-client

WireGuard est retenu comme solution VPN optimale pour EcoSolar Solutions.

Objectifs du VPN :

- Accès techniciens (IT)
- Accès commerciaux → accès restreint (ERP uniquement)
- MFA systématique
- ACL basées sur les VLAN

4.3 Règles de sécurité prévues (pfSense)

Filtrage inter-VLAN

Principe Zero Trust (CIA/DIC appliqué)

Exemples :

- VLAN Commerce → accès ERP uniquement
- VLAN Production → accès GLPI + ERP
- VLAN Direction → accès total
- VLAN Serveurs → inaccessible sauf IT + services essentiels

Journalisation & supervision

- Syslog activé vers Zabbix
- Alerting en cas de :
  - pics CPU, RAM, stockage
  - perte d'AD, ERP, GLPI, TEL, MAIL
  - coupure WAN
  - faille de tunnel VPN

MFA obligatoire

Par application mobile (TOTP).

4.4 Équipements concernés

- Cisco 3560 → reconfiguration VLAN + trunks 802.1Q
- pfSense SG-2440 → routage inter-VLAN + VPN + ACL
- Proxmox → maintien du VLAN Serveur
- Wi-Fi Cisco AP → futur VLAN Wi-Fi invité
- Zabbix → supervision globale

5. Impacts identifiés

Domaine	Impact	Détails / Actions
Adressage IP	organisation	Chaque poste doit migrer vers un VLAN dédié.
Switching	Reconfiguration totale	Création VLAN + affectation ports + trunk.

Domaine	Impact	Détails / Actions
Firewall	Durcissement	ACL strictes, fin du “permit any any”.
VPN	Nouveaux accès	Création comptes, MFA, politiques d’accès.
Supervision	Déploiement obligatoire	Ajout hôtes, alerting CPU/RAM/services.
Production	Risque temporaire	Intervention prévue hors horaires.
Sécurité	Isolation	Réduction des mouvements latéraux d’attaque.
Conformité E6	Amélioration majeure	Justification claire des choix techniques.

6. Bénéfices attendus

Domaine	Bénéfice concret
Sécurité	Isolation stricte, réduction du risque d’intrusion.
Performance	Réduction majeure du broadcast.
Disponibilité	Moins de collisions, supervision active.
Accès distant	VPN rapide, sécurisé, traçable.
Maintenance	Diagnostic simplifié par VLAN + supervision.
Scalabilité	Ajout futur de VLAN Wi-Fi invité, DMZ, PCA.

**7. Analyse des risques (incluant DIC, disponibilité, intégrité et confidentialité)

Risque	CIA/DIC impacté	Probabilité	Impact	Mesures préventives
Mauvaise config VLAN	Disponibilité	Moyenne	Forte	Double vérification + procédure écrite.
Erreur ACL	Confidentialité	Élevée	Très forte	Tests + règles minimales.
Échec VPN	Disponibilité	Faible	Forte	Redondance + test tunnel.
Perte supervision	Intégrité / dispo	Moyenne	Moyenne	Supervision locale + alertes mail.
Propag. attaque interne	Confidentialité	Élevée	Très forte	Segmentation + logs + MFA.
Coupure switch	Disponibilité	Moyenne	Forte	Plan PCA + matériel rechange.

8. Conclusion

La segmentation en VLAN, l'implémentation d'un accès distant sécurisé WireGuard et la mise en place d'un durcissement réseau offrent à EcoSolar Solutions :

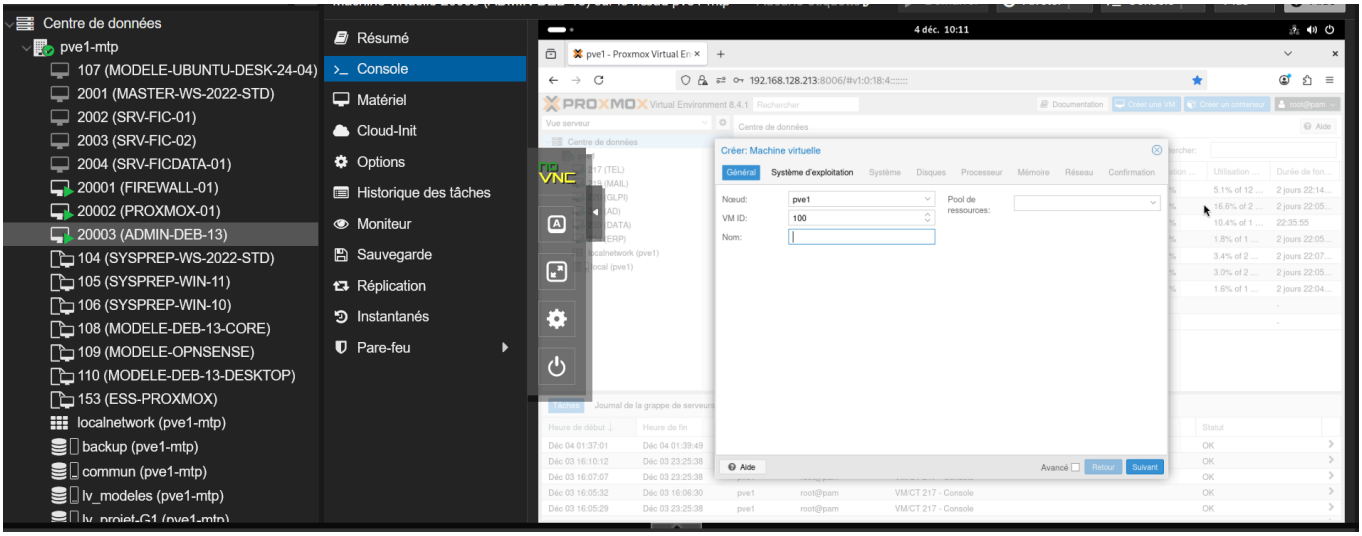
- une **sécurité renforcée**,
- une **réduction drastique des risques**,
- une **amélioration de la performance**,
- une **infrastructure alignée sur le référentiel E6**,
- une **base solide pour la supervision, le PRA et l'interconnexion future avec le datacenter de Marseille**.

Cette réorganisation transforme un réseau monolithique vulnérable en une architecture moderne, modulaire et sécurisée.

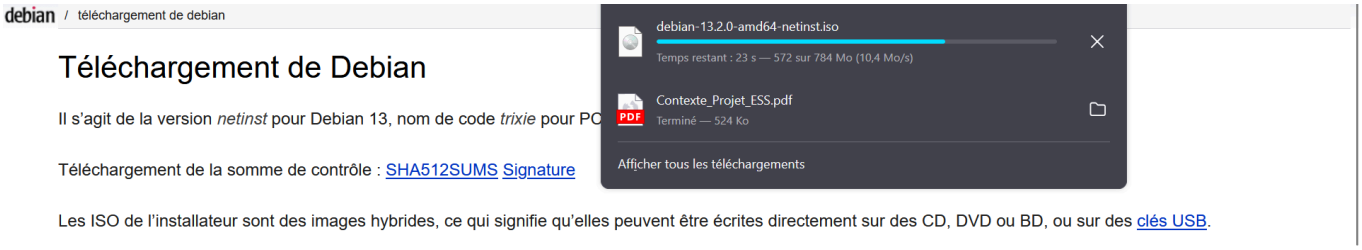
Machines	Volumes	Son (prévisionnel)	Father	G-Father
TEL	9.4	7* (10 %)	4*	12*
MAIL	5	7* (10 %)	4*	12*
GLPI	3,2	7* (10 %)	4*	12*
AD	17,8	7* (10 %)	4*	12*
DATA	17,1	7* (10 %)	4*	12*
ERP	2.8	7* (10 %)	4*	12*
Firewall/Switch	~2	7* (10 %)	4*	12*
Total	**~56Go**	**~40Go**	**~224Go**	**~672Go**
Grand Total :	**992Go**			

Mise en place serveur

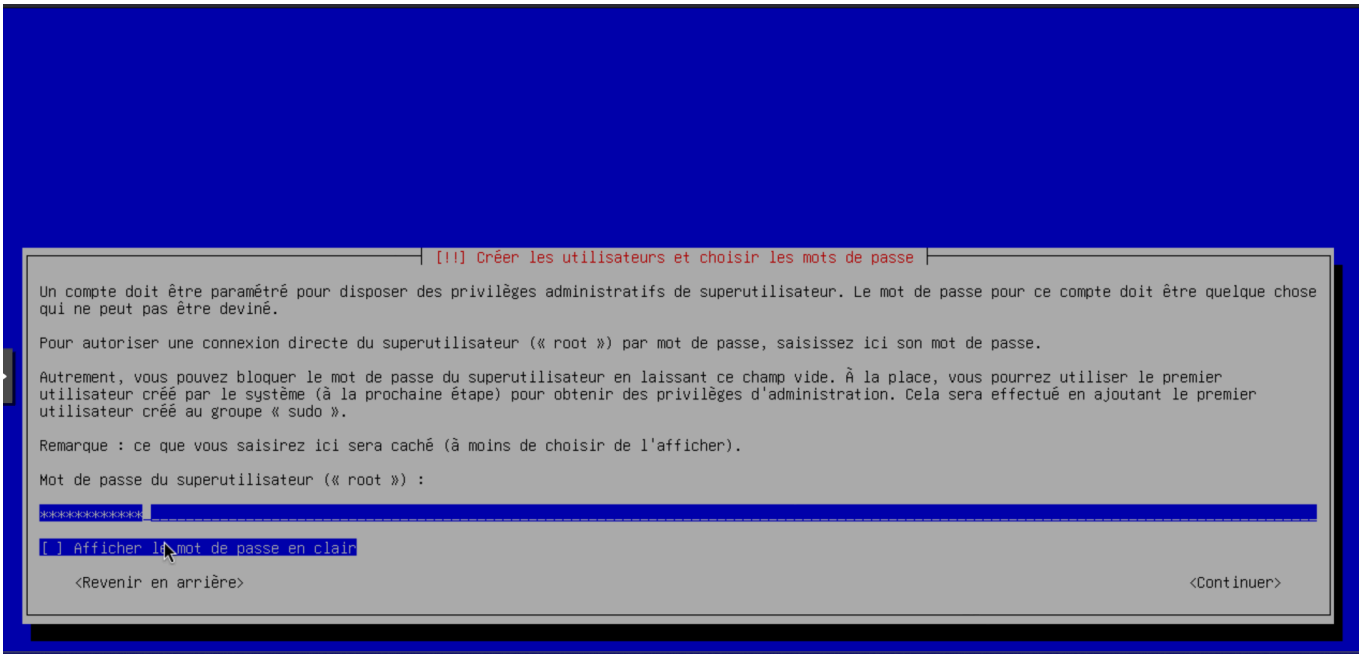
1/


Centre de données
pve1-mtp
107 (MODELE-UBUNTU-DESK-24-04)
2001 (MASTER-WS-2022-STD)
2002 (SRV-FIC-01)
2003 (SRV-FIC-02)
2004 (SRV-FICDATA-01)
20001 (FIREWALL-01)
20002 (PROXMOX-01)
20003 (ADMIN-DEB-13)
104 (SYSPREP-WS-2022-STD)
105 (SYSPREP-WIN-11)
106 (SYSPREP-WIN-10)
108 (MODELE-DEB-13-CORE)
109 (MODELE-OPNSENSE)
110 (MODELE-DEB-13-DESKTOP)
153 (ESS-PROXMOX)
localnetwork (pve1-mtp)
backup (pve1-mtp)
commun (pve1-mtp)
lv_modeles (pve1-mtp)
Résumé
Console
Matériel
Cloud-Init
Options
Historique des tâches
Moniteur
Sauvegarde
Réplication
Instantanés
Pare-feu
4 déc. 10:11
Créer: Machine virtuelle

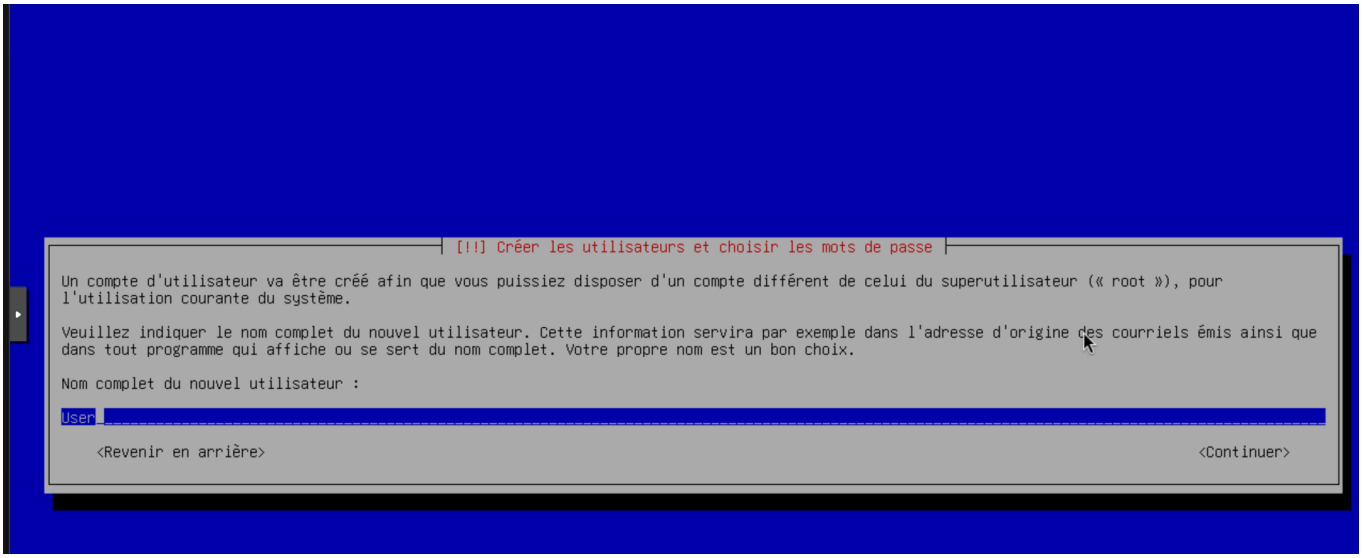
2/

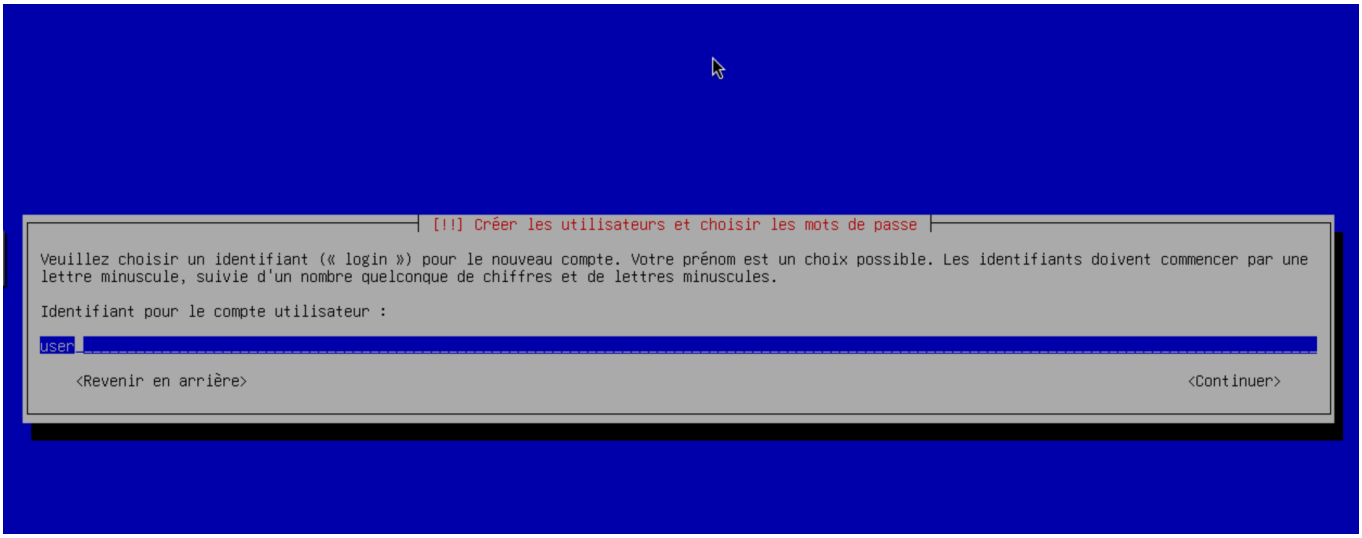

debian / téléchargement de debian
Téléchargement de Debian
Il s'agit de la version netinst pour Debian 13, nom de code trixie pour PC
Téléchargement de la somme de contrôle : SHA512SUMS Signature
Les ISO de l'installateur sont des images hybrides, ce qui signifie qu'elles peuvent être écrites directement sur des CD, DVD ou BD, ou sur des clés USB.
Autres installateurs
Les autres images et installateurs, tels que les systèmes autonomes, les installateurs pour des systèmes sans connexion réseau, les installateurs pour d'autres architectures ou les instances d'informatique dématérialisée, peuvent être trouvés sur la page Obtenir Debian.
Liens utiles
Manuel d'installation
debian-13.2.0-amd64-netinst.iso
Temps restant : 23 s — 572 sur 784 Mo (10,4 Mo/s)
Contexte_Projet_ESS.pdf
Terminé — 524 Ko
Afficher tous les téléchargements

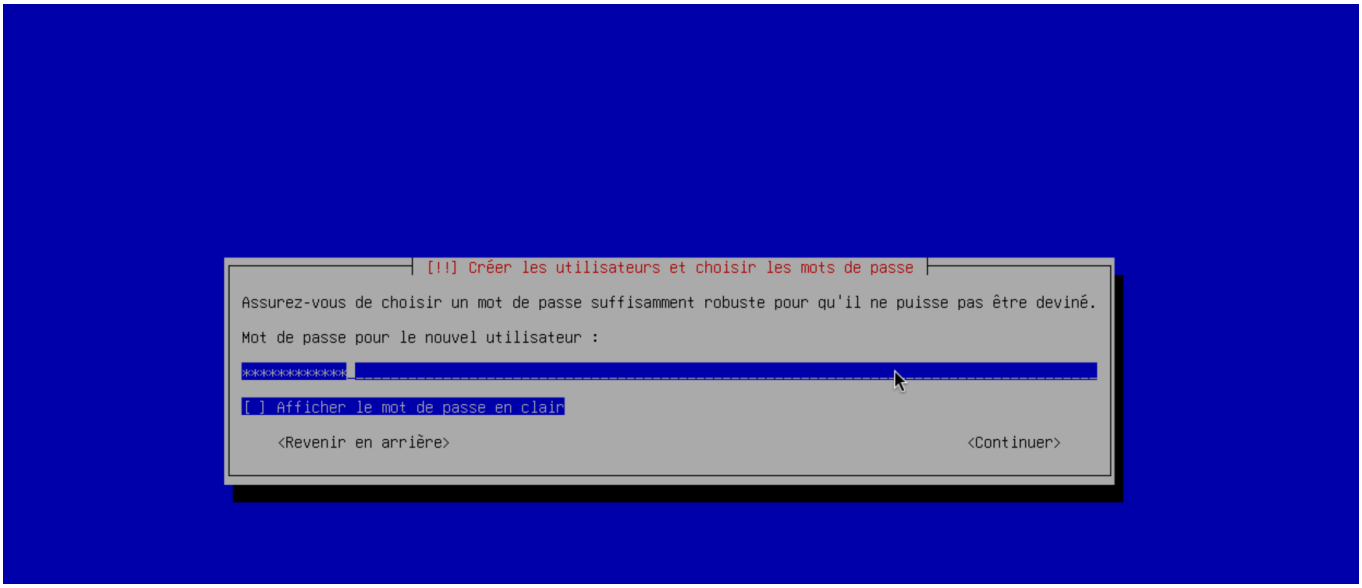
3/


[!!] Créer les utilisateurs et choisir les mots de passe
Un compte doit être paramétré pour disposer des privilèges administratifs de superutilisateur. Le mot de passe pour ce compte doit être quelque chose qui ne peut pas être deviné.
Pour autoriser une connexion directe du superutilisateur (« root ») par mot de passe, saisissez ici son mot de passe.
Autrement, vous pouvez bloquer le mot de passe du superutilisateur en laissant ce champ vide. À la place, vous pourrez utiliser le premier utilisateur créé par le système (à la prochaine étape) pour obtenir des privilèges d'administration. Cela sera effectué en ajoutant le premier utilisateur créé au groupe « sudo ».
Remarque : ce que vous saisirez ici sera caché (à moins de choisir de l'afficher).
Mot de passe du superutilisateur (« root ») :
[ ] Afficher le mot de passe en clair
<Revenir en arrière>
<Continuer>

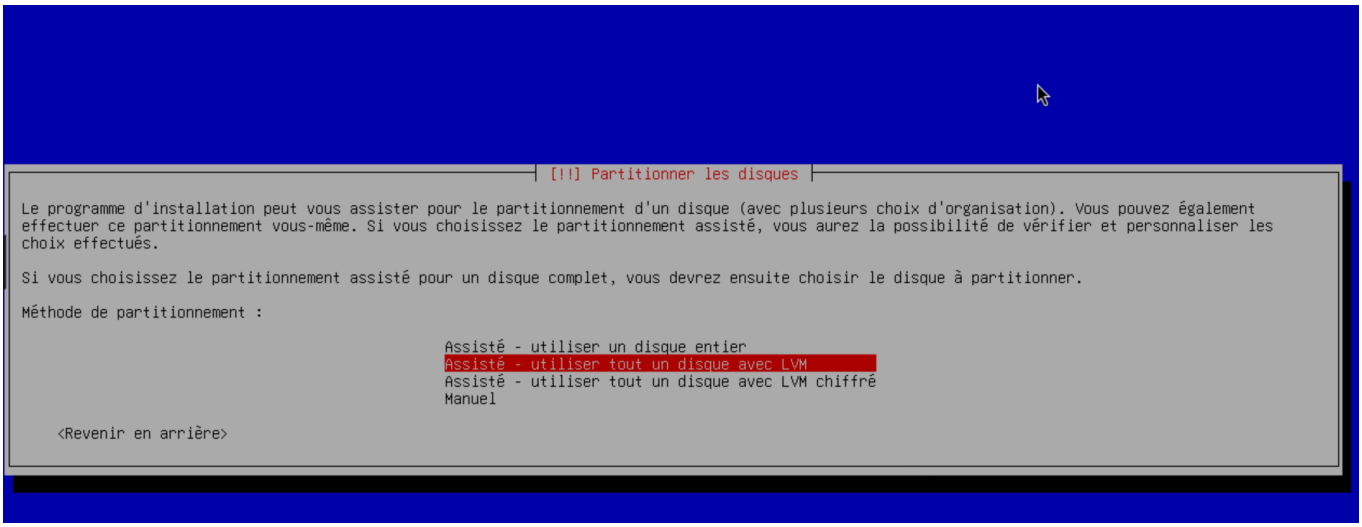
4/

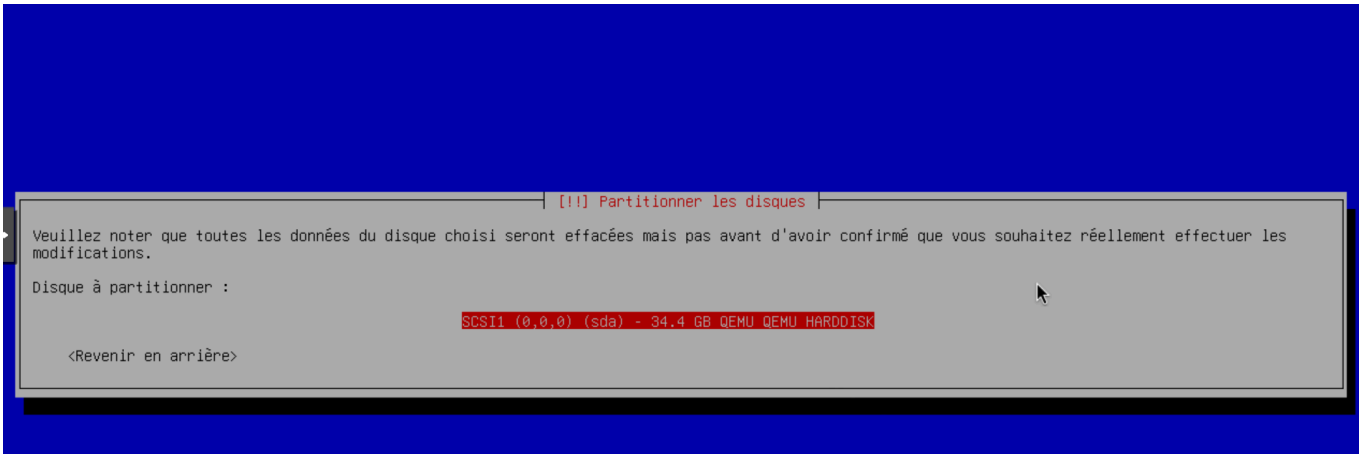


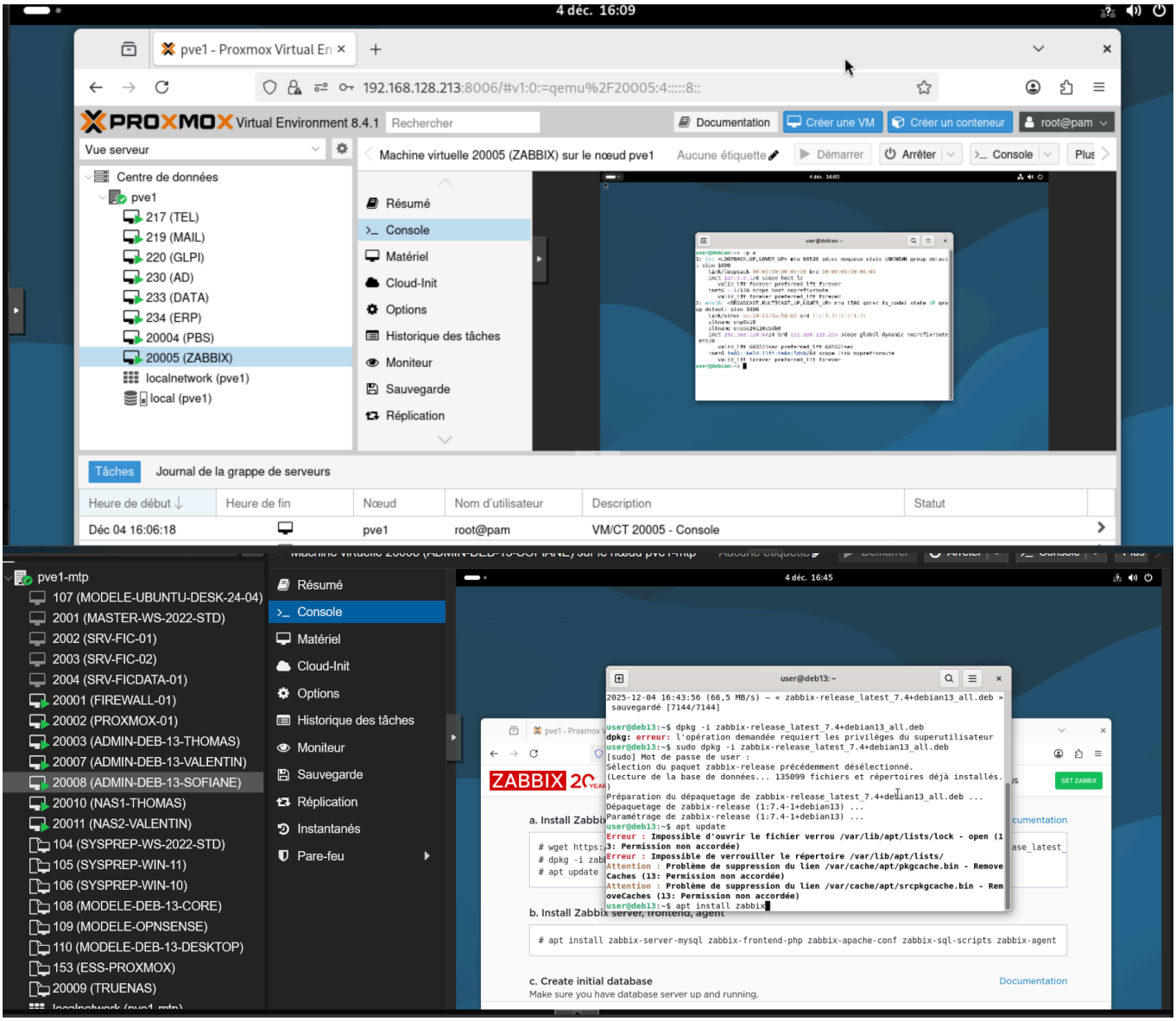


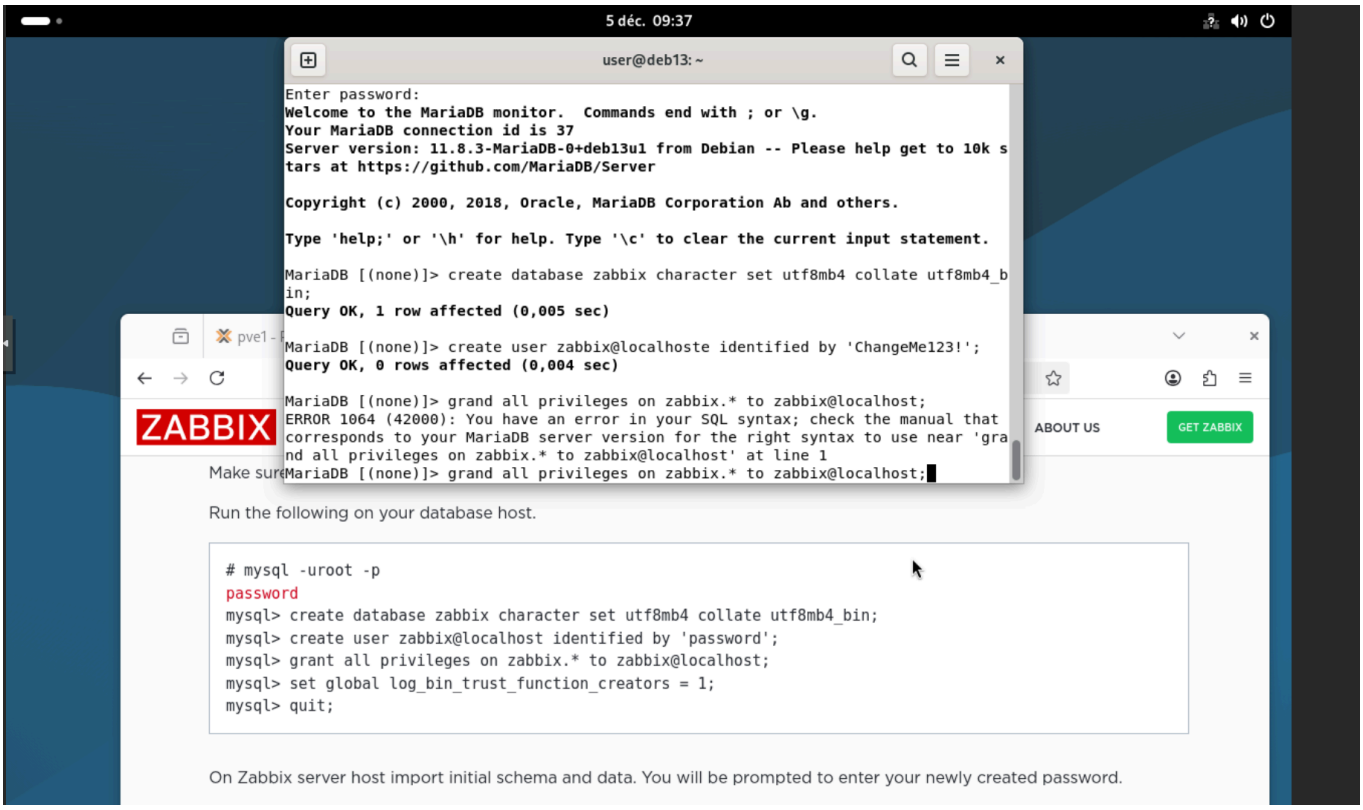


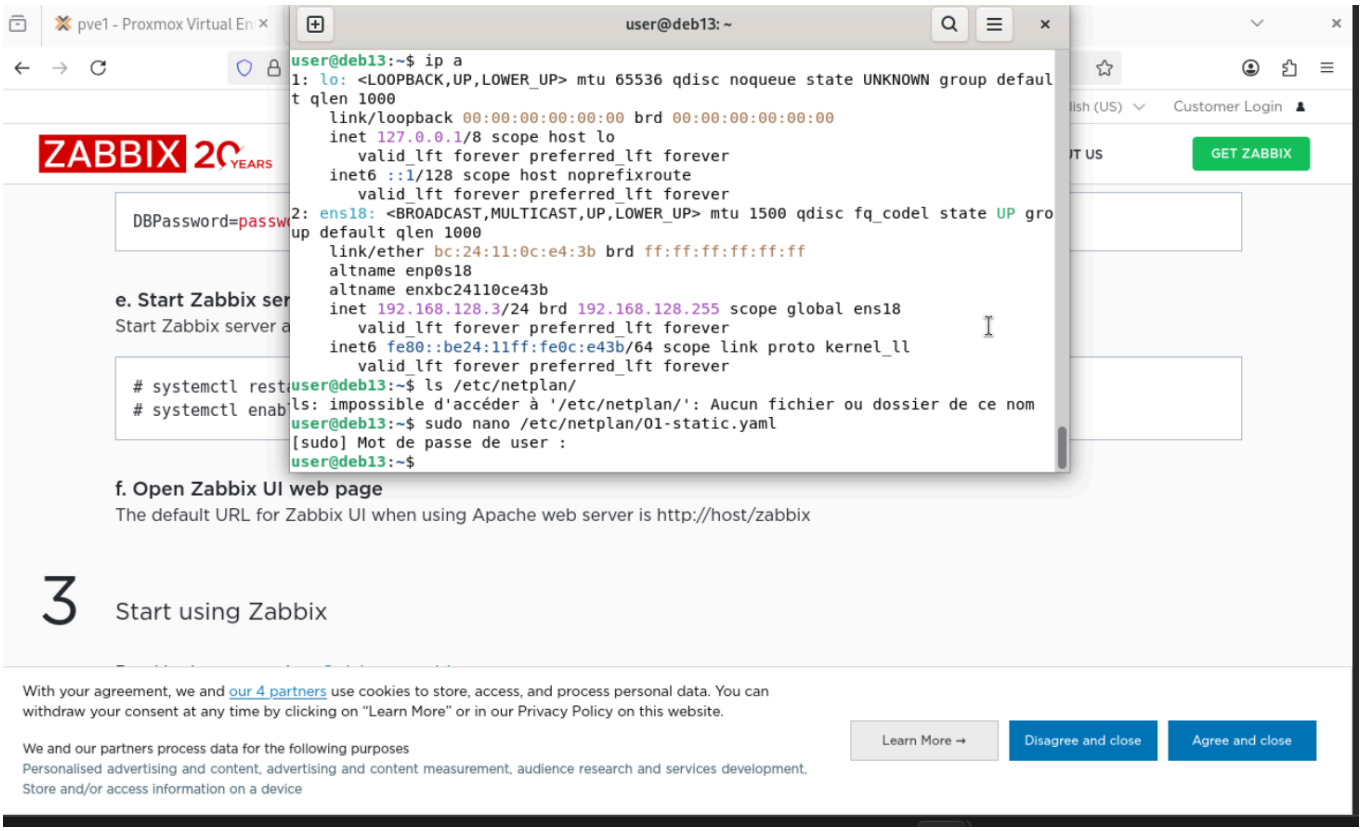
ChangeMe123!

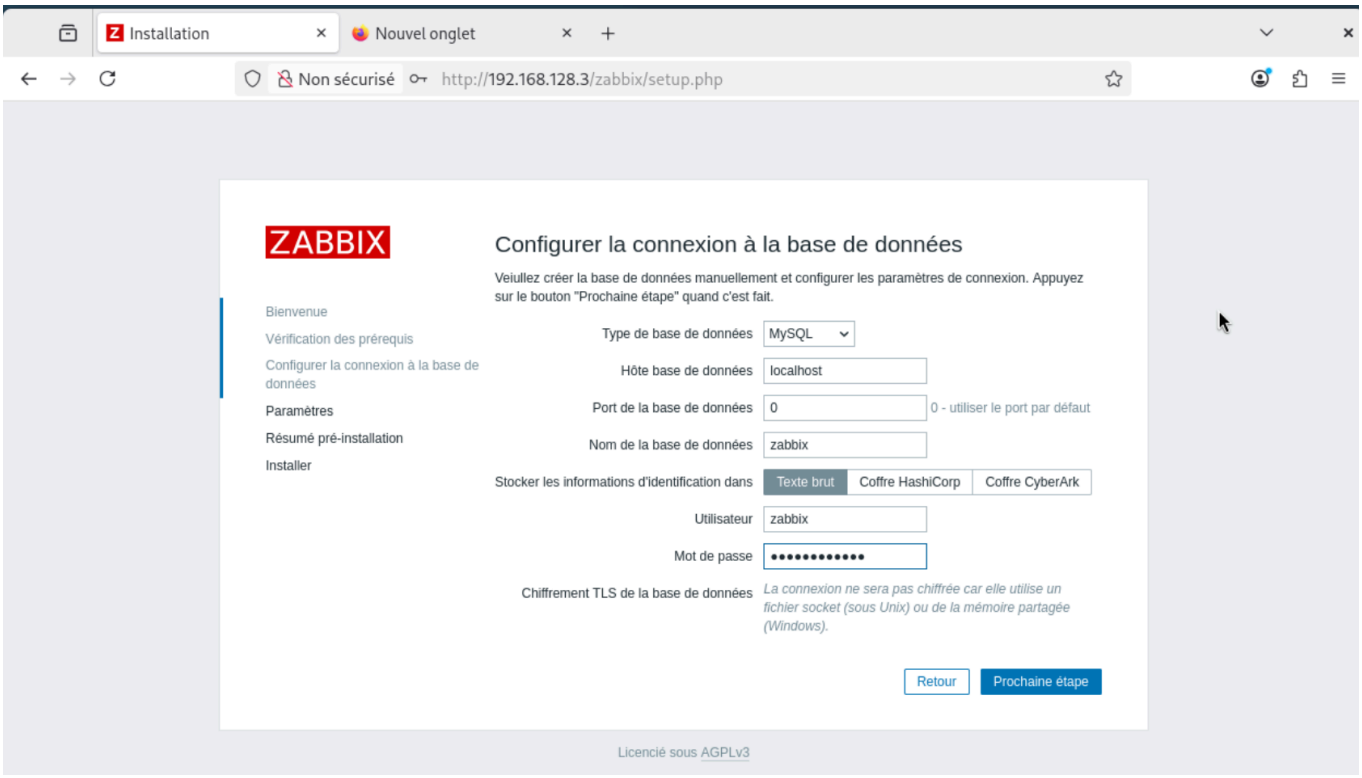

[!!] Partitionner les disques
Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.
Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.
Méthode de partitionnement :
Assisté - utiliser un disque entier
Assisté - utiliser tout un disque avec LVM
Assisté - utiliser tout un disque avec LVM chiffré
Manuel
<Revenir en arrière>


[!!] Partitionner les disques
Veuillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.
Disque à partitionner :
SCSI1 (0,0,0) (sda) - 34.4 GB QEMU QEMU HARDDISK
<Revenir en arrière>


4 déc. 16:09
pve1 - Proxmox Virtual En
192.168.128.213:8006/#v1:0:=qemu%2F20005:4::::8::
PROXMOX Virtual Environment 8.4.1
Rechercher
Documentation
Créer une VM
Créer un conteneur
root@pam
Vue serveur
Centre de données
pve1
217 (TEL)
219 (MAIL)
220 (GLPI)
230 (AD)
233 (DATA)
234 (ERP)
20004 (PBS)
20005 (ZABBIX)
localnetwork (pve1)
local (pve1)
Machine virtuelle 20005 (ZABBIX) sur le nœud pve1
Aucune étiquette
Démarrer
Arrêter
Console
Plus
Résumé
Console
Matériel
Cloud-Init
Options
Historique des tâches
Moniteur
Sauvegarde
Réplication
Tâches
Journal de la grappe de serveurs
Heure de début
Heure de fin
Nœud
Nom d'utilisateur
Description
Statut
Déc 04 16:06:18
pve1
root@pam
VM/CT 20005 - Console
pve1-mtp
107 (MODELE-UBUNTU-DESK-24-04)
2001 (MASTER-WS-2022-STD)
2002 (SRV-FIC-01)
2003 (SRV-FIC-02)
2004 (SRV-FICDATA-01)
20001 (FIREWALL-01)
20002 (PROXMOX-01)
20003 (ADMIN-DEB-13-THOMAS)
20007 (ADMIN-DEB-13-VALENTIN)
20008 (ADMIN-DEB-13-SOFIANE)
20010 (NAS1-THOMAS)
20011 (NAS2-VALENTIN)
104 (SYSPREP-WS-2022-STD)
105 (SYSPREP-WIN-11)
106 (SYSPREP-WIN-10)
108 (MODELE-DEB-13-CORE)
109 (MODELE-OPNSENSE)
110 (MODELE-DEB-13-DESKTOP)
153 (ESS-PROXMOX)
20009 (TRUENAS)
Résumé
Console
Matériel
Cloud-Init
Options
Historique des tâches
Moniteur
Sauvegarde
Réplication
Instantanés
Pare-feu
4 déc. 16:45
user@deb13: ~
2025-12-04 16:43:56 (66,5 MB/s) — « zabbix-release_latest_7.4+debian13_all.deb » sauvegardé [7144/7144]
user@deb13:~$ dpkg -i zabbix-release_latest_7.4+debian13_all.deb
dpkg: erreur: l'opération demandée requiert les privilèges du superutilisateur
user@deb13:~$ sudo dpkg -i zabbix-release_latest_7.4+debian13_all.deb
[sudo] Mot de passe de user :
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 135099 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_latest_7.4+debian13_all.deb ...
Dépaquetage de zabbix-release (1:7.4-1+debian13) ...
Paramétrage de zabbix-release (1:7.4-1+debian13) ...
user@deb13:~$ apt update
Erreur : Impossible d'ouvrir le fichier verrou /var/lib/apt/lists/lock - open (13: Permission non accordée)
Erreur : Impossible de verrouiller le répertoire /var/lib/apt/lists/
Attention : Problème de suppression du lien /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission non accordée)
Attention : Problème de suppression du lien /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission non accordée)
user@deb13:~$ apt install zabbix
ZABBIX
GET ZABBIX
a. Install Zabbix
b. Install Zabbix server, frontend, agent
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
c. Create initial database
Make sure you have database server up and running.
Documentation


5 déc. 09:37
user@deb13: ~
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 37
Server version: 11.8.3-MariaDB-0+deb13u1 from Debian -- Please help get to 10k s
tars at https://github.com/MariaDB/Server
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_b
in;
Query OK, 1 row affected (0,005 sec)
MariaDB [(none)]> create user zabbix@localhoste identified by 'ChangeMe123!';
Query OK, 0 rows affected (0,004 sec)
MariaDB [(none)]> grand all privileges on zabbix.* to zabbix@localhost;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MariaDB server version for the right syntax to use near 'gra
nd all privileges on zabbix.* to zabbix@localhost' at line 1
MariaDB [(none)]> grand all privileges on zabbix.* to zabbix@localhost;
ZABBIX
ABOUT US
GET ZABBIX
Run the following on your database host.
mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
On Zabbix server host import initial schema and data. You will be prompted to enter your newly created password.


pve1 - Proxmox Virtual En
user@deb13: ~
user@deb13:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
link/ether bc:24:11:0c:e4:3b brd ff:ff:ff:ff:ff:ff
altname enp0s18
altname enxbc24110ce43b
inet 192.168.128.3/24 brd 192.168.128.255 scope global ens18
valid_lft forever preferred_lft forever
inet6 fe80::be24:11ff:fe0c:e43b/64 scope link proto kernel_ll
valid_lft forever preferred_lft forever
user@deb13:~$ ls /etc/netplan/
ls: impossible d'accéder à '/etc/netplan/': Aucun fichier ou dossier de ce nom
user@deb13:~$ sudo nano /etc/netplan/01-static.yaml
[sudo] Mot de passe de user :
user@deb13:~$
ZABBIX 20 YEARS
Customer Login
GET ZABBIX
DBPassword=passw
e. Start Zabbix ser
Start Zabbix server a
systemctl rest
systemctl enab
f. Open Zabbix UI web page
The default URL for Zabbix UI when using Apache web server is http://host/zabbix
3
Start using Zabbix
With your agreement, we and our 4 partners use cookies to store, access, and process personal data. You can withdraw your consent at any time by clicking on "Learn More" or in our Privacy Policy on this website.
We and our partners process data for the following purposes
Personalised advertising and content, advertising and content measurement, audience research and services development.
Store and/or access information on a device
Learn More →
Disagree and close
Agree and close



Suite à cela la configuration de l'interface web est maintenant terminée. Ce processus crée le fichier de configuration `/usr/share/zabbix/conf/zabbix.conf.php`, que vous pouvez sauvegarder et utiliser à l'avenir. Cliquez sur **Finish** pour passer à l'écran de connexion. L'utilisateur par défaut est **Admin** et le mot de passe est **zabbix**.

Il faut maintenant configurer le logiciel d'agent qui enverra les données de surveillance au serveur Zabbix. Via ssh server_ip_address

Il faudra donc installer le package de configuration du dépôt :
wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb
sudo dpkg -i zabbix-release_5.0-1+focal_all.deb

Étape 6 - Installer et configurer l'agent Zabbix

Il faut maintenant configurer le logiciel d'agent qui enverra les données de surveillance au serveur Zabbix.

La connexion au deuxième serveur Ubuntu doit être établit :

```
ssh sammy@second_ubuntu_server_ip_address
```

Tout comme sur le serveur Zabbix, il faut exécuter les commandes suivantes pour installer le package de configuration du dépôt :

```
wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb
sudo dpkg -i zabbix-release_5.0-1+focal_all.deb
```

Ensuite, mettre à jour l'index des packages :

```
sudo apt update
```

Puis installer ensuite l'agent Zabbix :

```
sudo apt install zabbix-agent
```

Bien que Zabbix supporte le cryptage par certificat, la mise en place d'une autorité de certification dépasse le cadre de ce tutoriel. Mais il faut utiliser des clés pré-partagées (PSK) pour sécuriser la connexion entre le serveur et l'agent.

D'abord, générez une PSK :

```
sudo sh -c "openssl rand -hex 32 > /etc/zabbix/zabbix_agentd.psk"
```

Il faut montrer la clé en utilisant `le chat` pour pouvoir la copier quelque part :

```
cat /etc/zabbix/zabbix_agentd.psk
```

La clé ressemble à quelque chose comme ça :

```
Output75ad6cb5e17d244ac8c00c96a1b074d0550b8e7b15d0ab3cde60cd79af280fca
```

Elle servira à configurer l'hôte.

Maintenant, il faut modifier les paramètres de l'agent Zabbix pour établir sa connexion sécurisée au serveur Zabbix. Ouvrir le fichier de configuration de l'agent dans l'éditeur de texte :

```
sudo nano /etc/zabbix/zabbix_agentd.conf
```

Chaque paramètre de ce dossier est documenté par des commentaires informatifs tout au long du dossier, mais il faut modifier certains d'entre eux.

En commençant par modifier l'adresse IP du serveur Zabbix. Dans la section suivante :

/etc/zabbix/zabbix_agentd.conf

```
...
### Option: Server
#       List of comma delimited IP addresses, optionally in CIDR notation, or
DNS names of Zabbix servers and Zabbix proxies.
#       Incoming connections will be accepted only from the hosts listed here.
#       If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1',
'::ffff:127.0.0.1' are treated equally
#       and '::/0' will allow any IPv4 or IPv6 address.
#       '0.0.0.0/0' can be used to allow any IPv4 address.
#       Example:
Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=127.0.0.1
...
```

Je change la valeur par défaut pour l'IP du serveur Zabbix :

/etc/zabbix/zabbix_agentd.conf

```
...
Server=zabbix_server_ip_address
...
```

Par défaut, le serveur Zabbix se connecte à l'agent. Mais pour certains contrôles (par exemple, la surveillance des journaux), une connexion inverse est nécessaire. Pour un fonctionnement correct, Il faut spécifier l'adresse du serveur Zabbix et un nom d'hôte unique.

Trouver la section qui configure les contrôles actifs et modifiez les valeurs par défaut :

/etc/zabbix/zabbix_agentd.conf

```
...
##### Active checks related

### Option: ServerActive
#       List of comma delimited IP:port (or DNS name:port) pairs of Zabbix
servers and Zabbix proxies for active checks.
#       If port is not specified, default port is used.
#       IPv6 addresses must be enclosed in square brackets if port for that
host is specified.
#       If port is not specified, square brackets for IPv6 addresses are
optional.
#       If this parameter is not specified, active checks are disabled.
#       Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,
[12fc::1]
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=zabbix_server_ip_address

### Option: Hostname
#       Unique, case sensitive hostname.
#       Required for active checks and must match hostname as configured on
the server.
#       Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=Second Ubuntu Server
...
```

Ensuite, il est nécessaire de trouver la section qui configure la connexion sécurisée au serveur Zabbix et activer le support des clés pré-partagées. Puis trouver la section `TLSConnect`, qui ressemble à ceci :

/etc/zabbix/zabbix_agentd.conf

```
...
### Option: TLSConnect
#       How the agent should connect to server or proxy. Used for active
checks.
#       Only one value can be specified:
```

```
#               unencrypted - connect without encryption
#               psk         - connect using TLS and a pre-shared key
#               cert        - connect using TLS and a certificate
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for
'unencrypted' connection)
# Default:
# TLSConnect=unencrypted
...
```

Ajouter ensuite cette ligne pour configurer le support des clés pré-partagées :

/etc/zabbix/zabbix_agentd.conf

```
...
TLSConnect=psk
...
```

Ensuite, localiser la section `TLSAccept`, qui ressemble à ceci :

/etc/zabbix/zabbix_agentd.conf

```
...
### Option: TLSAccept
#       What incoming connections to accept.
#       Multiple values can be specified, separated by comma:
#               unencrypted - accept connections without encryption
#               psk         - accept connections secured with TLS and a pre-
shared key
#               cert        - accept connections secured with TLS and a
certificate
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for
'unencrypted' connection)
# Default:
# TLSAccept=unencrypted
...
```

Configurer les connexions entrantes pour prendre en charge les clés pré-partagées en ajoutant cette ligne :

/etc/zabbix/zabbix_agentd.conf

```
...
TLSAccept=psk
...
```

Ensuite, trouver la section `TLSPSKIdentity`, qui ressemble à ceci :

/etc/zabbix/zabbix_agentd.conf

```
...
### Option: TLSPSKIdentity
#       Unique, case sensitive string used to identify the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKIdentity=
...
```

je choisis un nom unique pour identifier votre clé pré-partagée en ajoutant cette ligne :

/etc/zabbix/zabbix_agentd.conf

```
...
TLSPSKIdentity=PSK 001
...
```

J'utilise l'id comme **identifiant PSK** lorsque qu'il faut ajouter mon hôte via l'interface web Zabbix.

Définir ensuite l'option qui pointe vers votre clé pré-partagée créée précédemment. Repérer l'option `TLSPSKFile` :

/etc/zabbix/zabbix_agentd.conf

```
...
### Option: TLSPSKFile
#       Full pathname of a file containing the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKFile=
...
```

Puis ajoute cette ligne pour pointer l'agent Zabbix vers votre fichier PSK que vous avez créé :

/etc/zabbix/zabbix_agentd.conf

```
...
TLSPSKFile=/etc/zabbix/zabbix_agentd.psk
...
```

Enregistrer et fermer le fichier. Il faut maintenant maintenant redémarrer l’agent Zabbix et le configurer pour qu’il démarre au moment du démarrage :

```
sudo systemctl restart zabbix-agent
sudo systemctl enable zabbix-agent
```

Pour faire bonne mesure, vérifier que l’agent Zabbix fonctionne correctement :

```
sudo systemctl status zabbix-agent
```

On voir le statut suivant, indiquant que l’agent est en cours d’exécution :

```
Output● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor
preset: enabled)
   Active: active (running) since Fri 2020-06-12 08:19:54 UTC; 25s ago
  ...
```

L’agent écoutera au port `10050` pour les connexions à partir du serveur. Configurez l’UFW pour permettre les connexions à ce port :

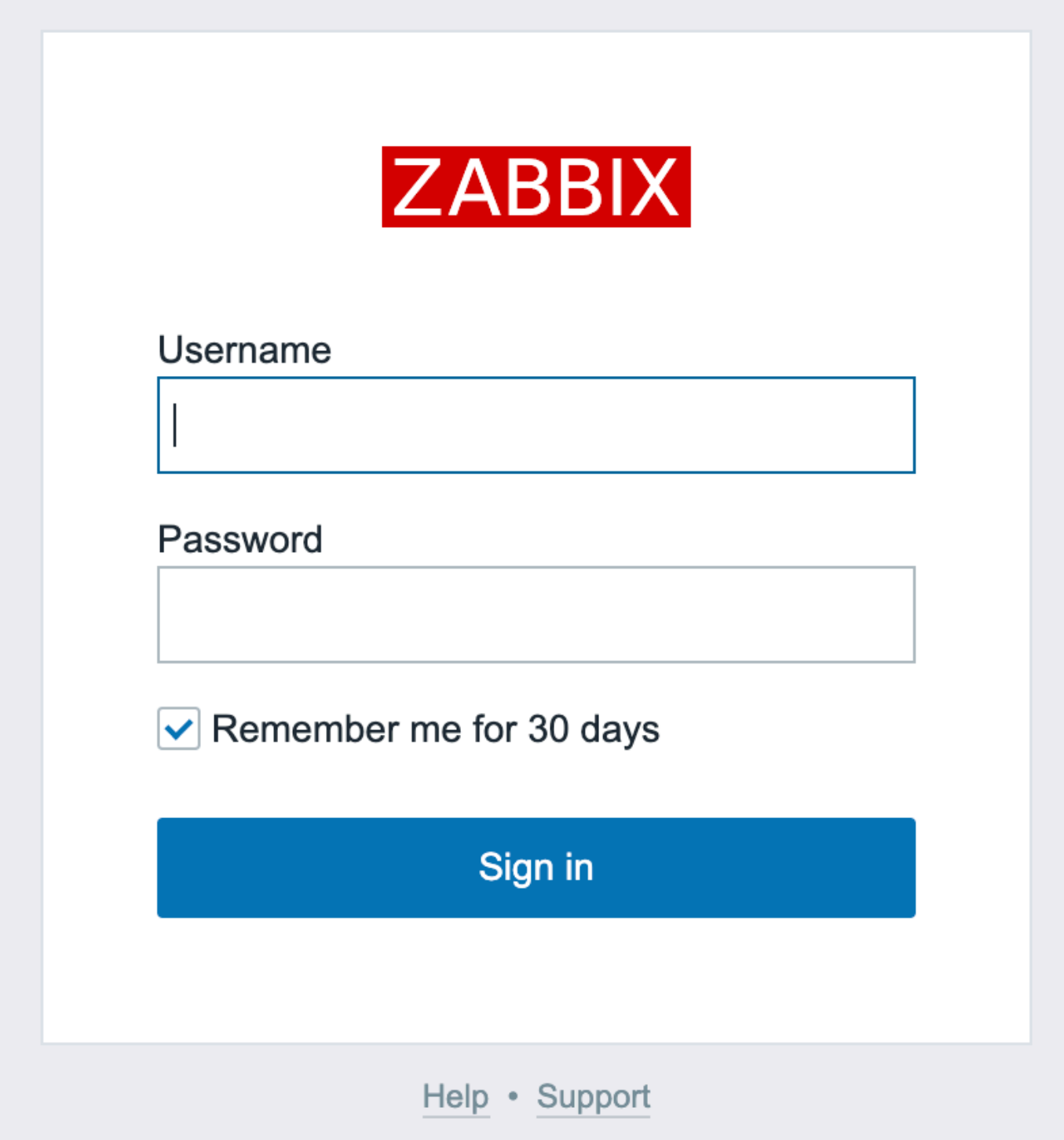
```
sudo ufw allow 10050/tcp
```

L'agent est maintenant prêt à envoyer des données au serveur Zabbix. Mais pour l’utiliser, il doit y accéder à partir de la console web du serveur. Dans l’étape suivante, il faut compléter la configuration.

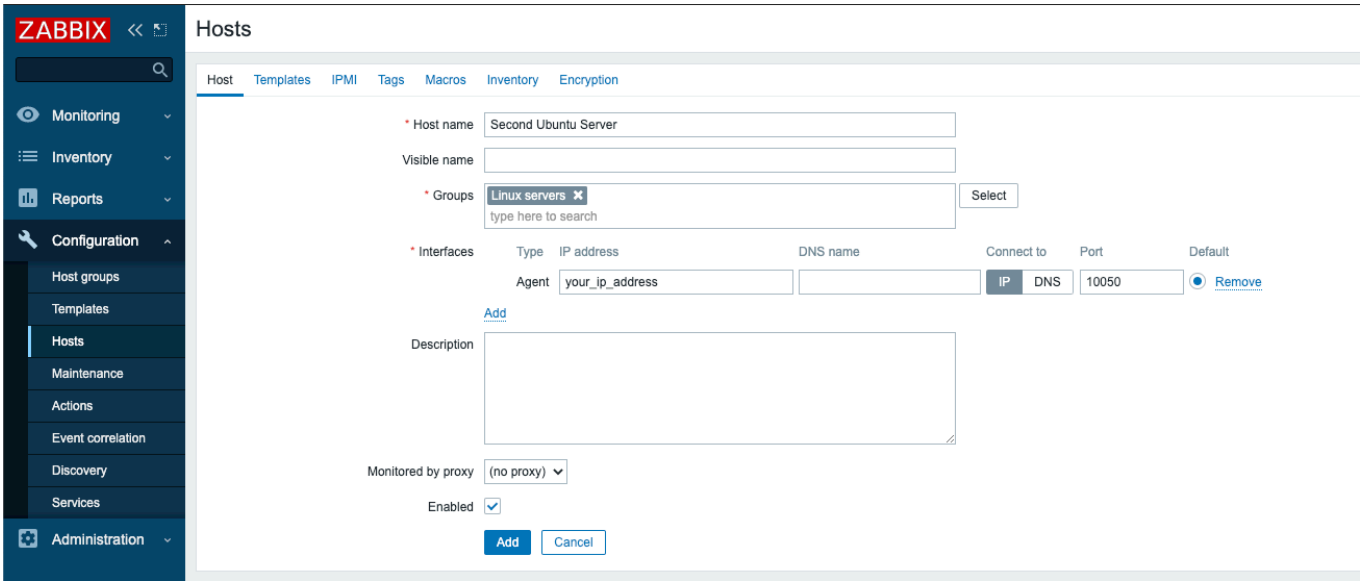
Étape 7 - Ajouter le nouvel hôte au serveur Zabbix]

L’installation d’un agent sur un serveur qu'il y a à surveiller ne représente que la moitié du processus. Chaque hôte que vous souhaitez surveiller doit être enregistré sur le serveur Zabbix, ce que vous pouvez faire via l’interface web.

Connectez-vous à l'interface web du serveur Zabbix en naviguant à l'adresse `http://==zabbix_server_name==` ou `https://==zabbix_server_name==` :

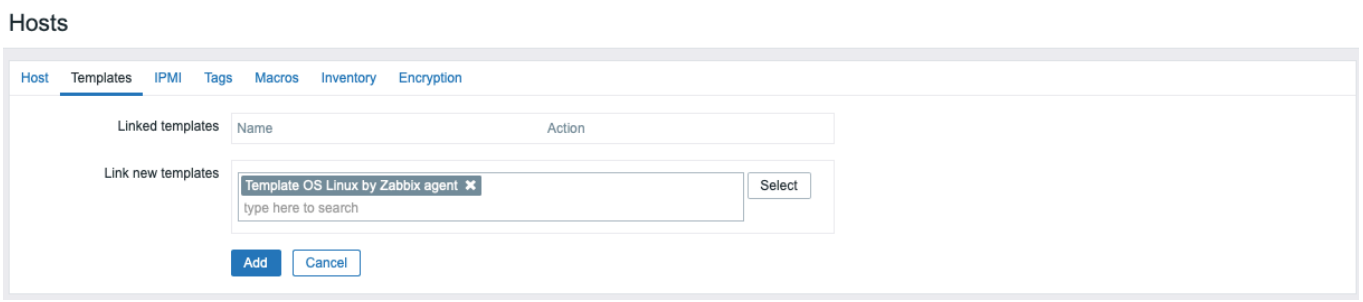


Lorsque la connexion est établit, cliquer sur **Configuration** et ensuite sur **Hosts** dans la barre de navigation de gauche. Puis cliquer sur le bouton **Create host** dans le coin supérieur droit de l'écran. Cela ouvrira la page de configuration de l'hôte.



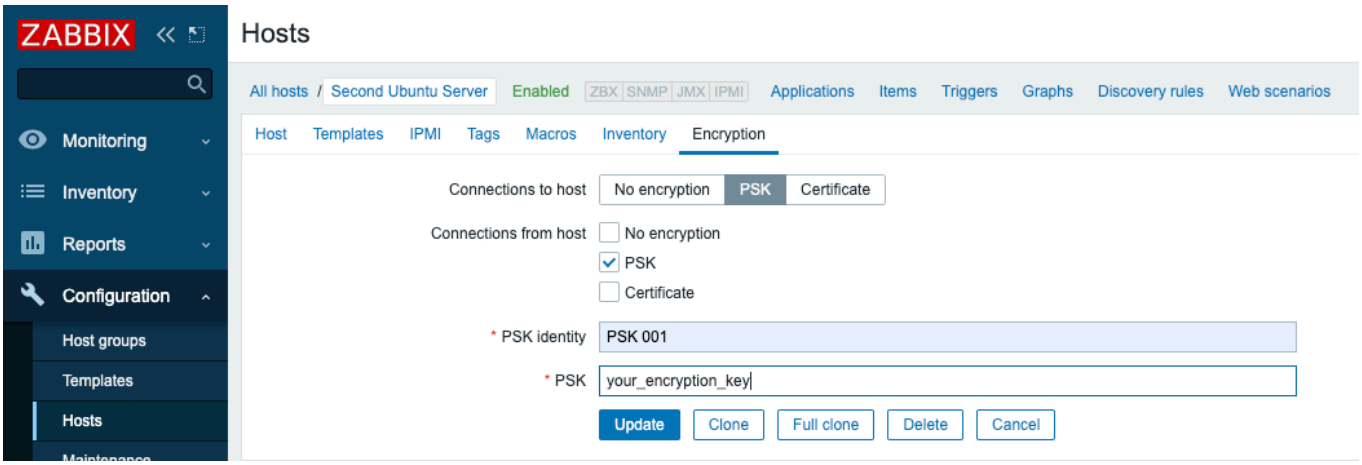
J'ajoute le **Host name** et l'**adresse IP** pour refléter le nom d'hôte et l'adresse IP de votre second serveur Ubuntu, puis ajoutez l'hôte à un groupe. Je vais sélectionner un groupe existant, par exemple **des serveurs Linux** ou créer votre propre groupe. L'hôte peut faire partie de plusieurs groupes. Pour ce faire, j'ajoute le nom d'un groupe existant ou nouveau dans le champ de saisie **Groups** et sélectionne la valeur souhaitée dans la liste proposée.

Avant d'ajouter le groupe, Il faut cliquer sur l'onglet **Templates**.



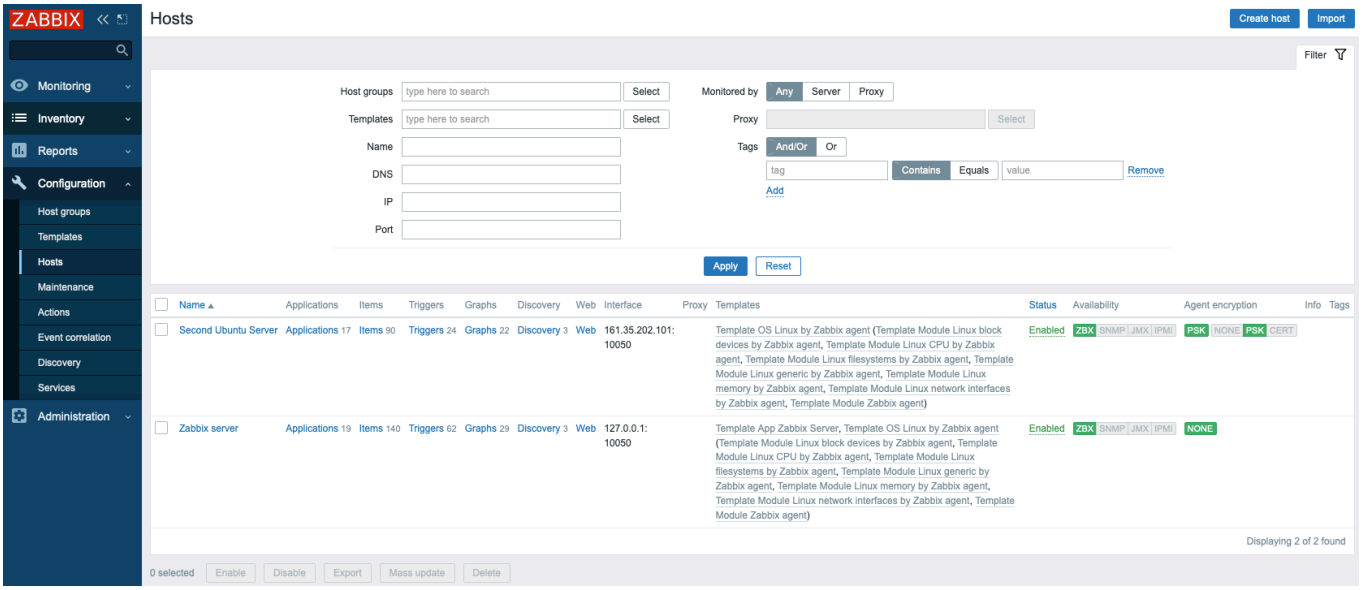
Tapez `Template OS Linux by Zabbix agent` dans le champ **Search**, puis sélectionnez-le dans la liste pour ajouter ce modèle à l'hôte.

Ensuite, Il faut naviguer jusqu'à l'onglet **Encryption**. Sélectionnez **PSK** pour les **connexions vers l'hôte** et les **connexions depuis l'hôte**. Définir ensuite l'**identité PSK** à `PSK 001`, qui est la valeur de la **TLSPSKIdentity** de l'agent Zabbix que vous avez configuré précédemment. Définir ensuite la valeur **PSK** à la clé que j'ai générée pour l'agent Zabbix. C'est celle qui est stockée dans le fichier `/etc/zabbix/zabbix_agentd.psk` sur la machine de l'agent.



Enfin, il faur cliquer sur le bouton **Add** au bas du formulaire pour créer l'hôte.

Il ya un nouvel hôte dans la liste. Il faut un peu attendre et recharger la page pour voir les étiquettes vertes indiquant que tout fonctionne bien et que la connexion est cryptée.



Le serveur Zabbix surveille maintenant le deuxième serveur Ubuntu.

Étape 8 - Configurer les notifications par courrier électronique

Zabbix supporte automatiquement plusieurs types de notifications : courriel, OTRS, Slack, Télégramme, SMS, etc. Il est possible de consulter la liste complète des intégrations sur le site de Zabbix.

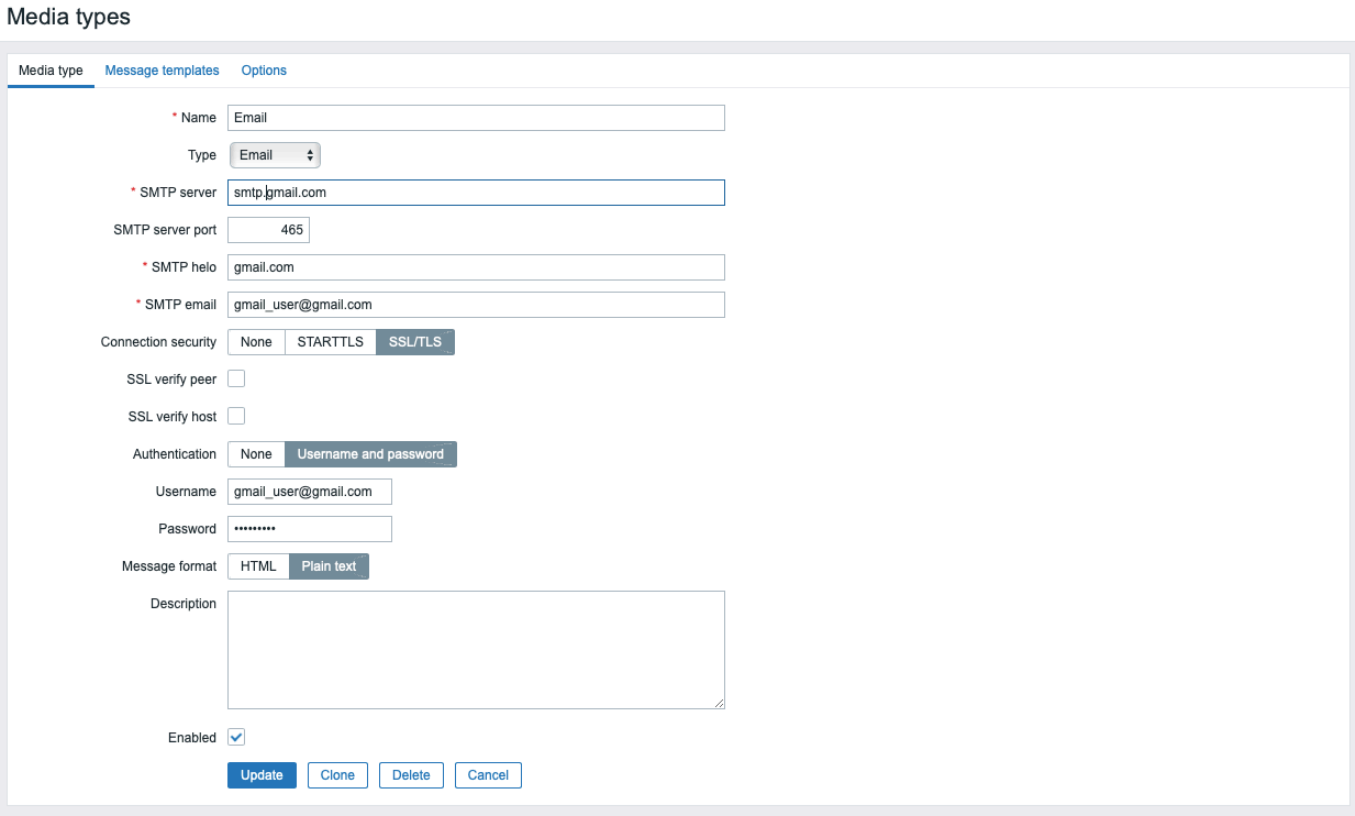
À titre d'exemple, ce tutoriel permet de configurer les notifications pour le type de support **courrier électronique**.

Il faut accéder au menu **Administration**, puis à **Media types** dans la barre de navigation de gauche. La liste de tous les types de médias est alors affichée. Deux options sont préconfigurées pour les courriels : la notification en texte clair et la notification en HTML. Il faut utiliser la notification en texte clair, puis sélectionner **Email**.

Il faut ajuster les options SMTP en fonction des paramètres fournis par le service de courrier électronique utilisé. Dans ce tutoriel, les capacités SMTP de Gmail sont utilisées pour configurer les notifications par e-mail. Pour obtenir plus d'informations sur cette configuration, il est possible de consulter la documentation relative à l'utilisation du serveur SMTP de Google.

Note : Si la vérification en deux étapes est activée sur Gmail, il est nécessaire de générer un mot de passe d'application pour Zabbix. Ce mot de passe n'est saisi qu'une seule fois lors de l'installation. Les instructions permettant de générer ce mot de passe sont disponibles dans le Centre d'aide Google.

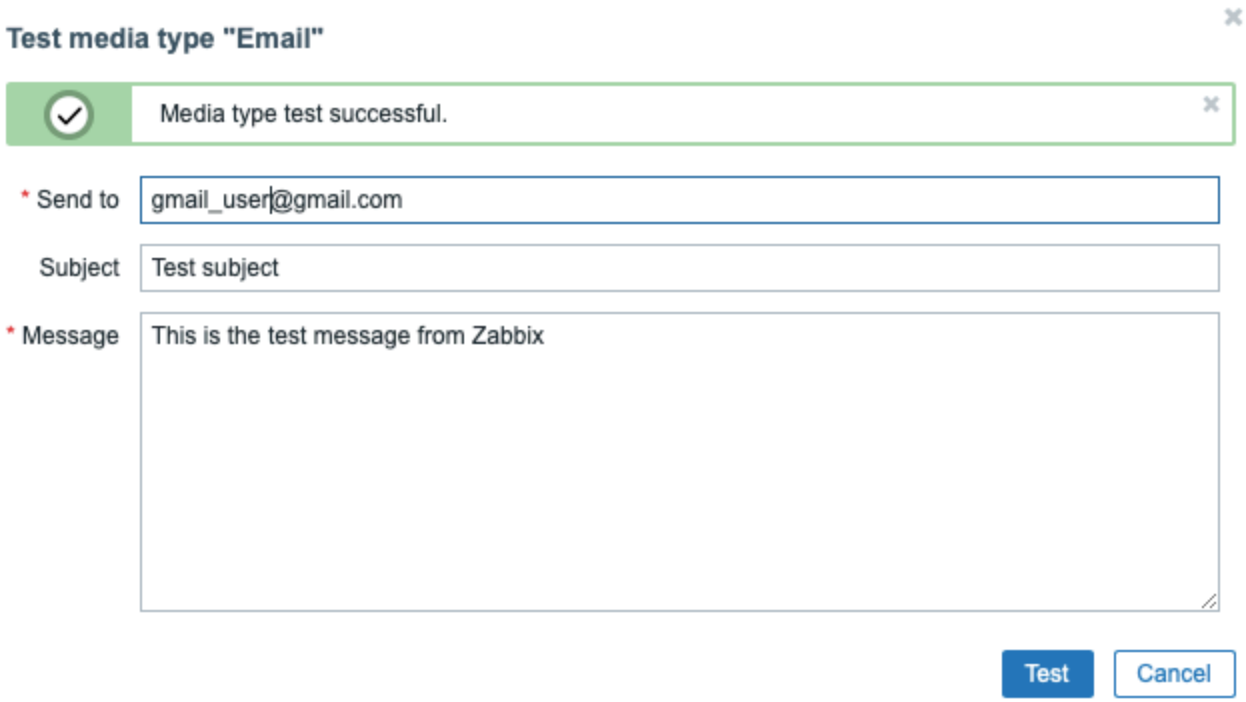
Par exemple, si Gmail est utilisé, il faut renseigner `smtp.gmail.com` dans le champ **Serveur SMTP**, `465` dans le champ **Port du serveur SMTP**, `gmail.com` dans le champ **SMTP helo**, et l'adresse de messagerie dans le champ **SMTP email**. Il faut ensuite sélectionner **SSL/TLS** pour la **sécurité de connexion** et **Username and password** pour l'**authentification**. L'adresse Gmail est alors définie comme **nom d'utilisateur**, et le mot de passe d'application généré depuis le compte Google est renseigné comme **mot de passe**.



Sous l'onglet **Message templates**, la liste des messages prédéfinis pour les différents types de notifications est affichée. Enfin, il faut cliquer sur le bouton **Update** en bas du formulaire afin de mettre à jour les paramètres du courrier électronique.

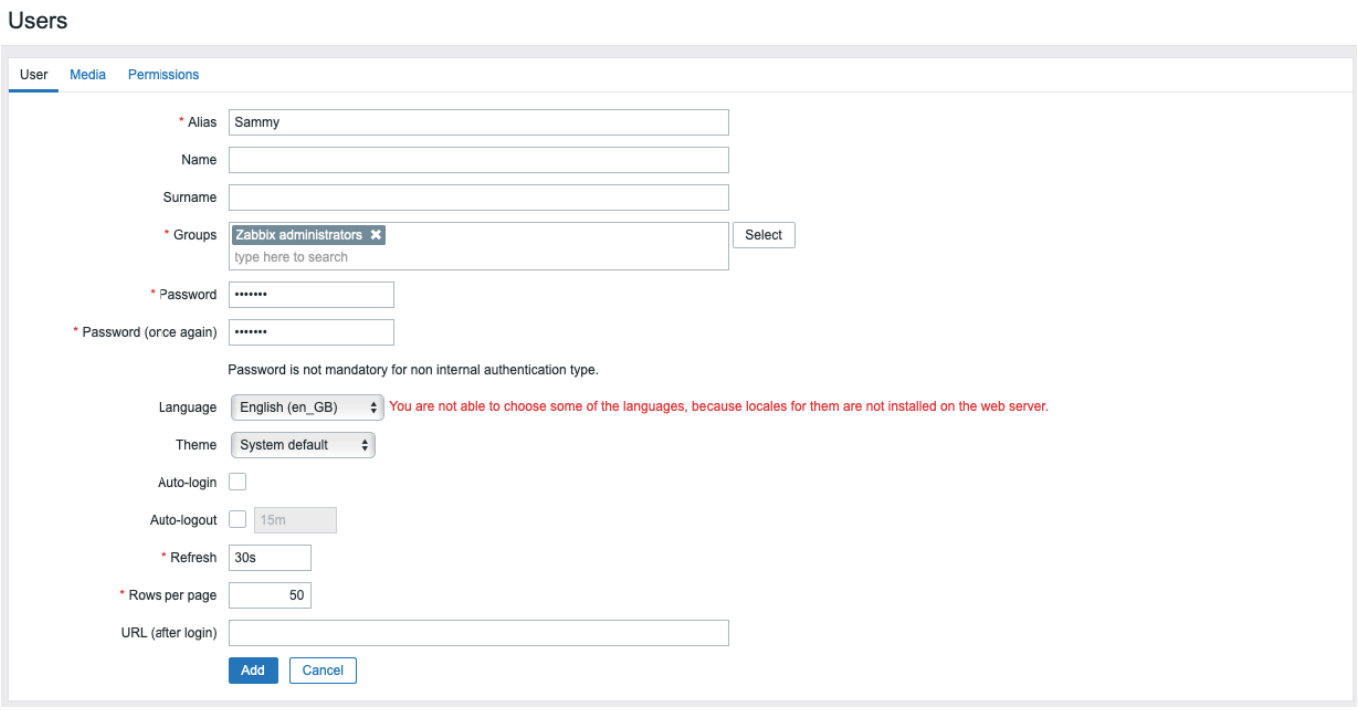
Il est ensuite possible de tester l'envoi des notifications. Pour cela, il faut cliquer sur le lien **Test** souligné dans la ligne correspondante.

Une fenêtre pop-up est alors affichée. Il faut saisir une adresse électronique dans le champ **Send to**, puis cliquer sur le bouton **Test**. Un message confirmant l'envoi réussi est affiché, et un message de test est reçu.



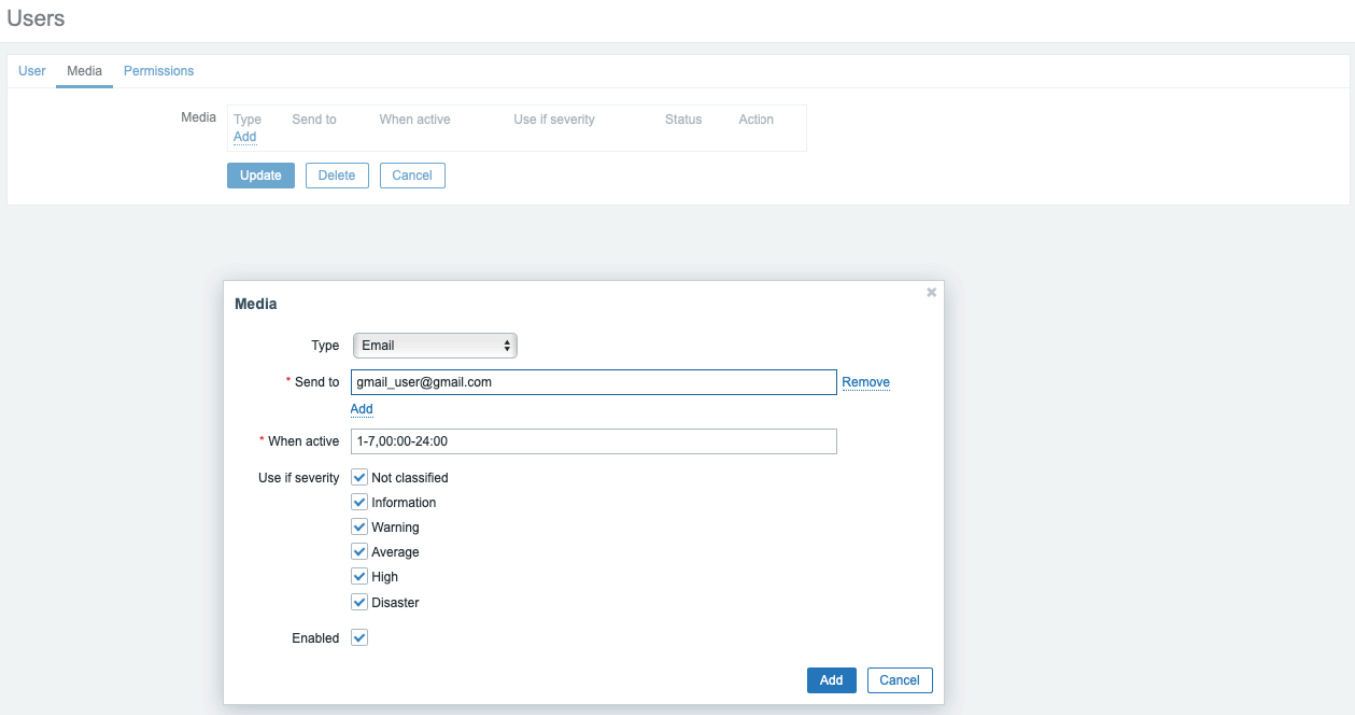
Il faut fermer la fenêtre pop-up en cliquant sur le bouton **Cancel**.

Il faut ensuite créer un nouvel utilisateur. Pour cela, il faut accéder au menu **Administration**, puis à **Users** dans la barre de navigation de gauche. La liste des utilisateurs est alors affichée. Il faut cliquer sur le bouton **Create user** situé dans le coin supérieur droit de l'écran. La page de configuration de l'utilisateur est alors ouverte.



Entrer le nouveau nom d'utilisateur est renseigné dans le champ **Alias** et un nouveau mot de passe est défini. L'utilisateur est ensuite ajouté au groupe administrateur. Pour cela, `Zabbix administrators` est saisi dans le champ **Groups**, puis sélectionné dans la liste proposée.

Une fois le groupe ajouté, l'onglet **Media** est ouvert, puis le lien **Add** souligné est sélectionné (et non le bouton **Add** situé en dessous). Une fenêtre pop-up est alors affichée.



L'option **Email** est sélectionnée dans le menu déroulant **Type**. L'adresse électronique est renseignée dans le champ **Send to**, tandis que les autres options sont laissées à leurs valeurs par défaut. Le bouton **Add**, situé en bas du formulaire, est ensuite sélectionné afin de valider la configuration.

L'onglet **Permissions** est ensuite ouvert. L'option **Zabbix Super Admin** est sélectionnée dans le menu déroulant **User type**.

Enfin, le bouton **Add**, situé en bas du formulaire, est sélectionné afin de créer l'utilisateur.

Note : L'utilisation du mot de passe par défaut n'est pas sécurisée. Afin de modifier le mot de passe de l'utilisateur intégré **Admin**, l'alias correspondant est sélectionné dans la liste des utilisateurs. L'option **Change password** est ensuite utilisée, un nouveau mot de passe est défini, puis les modifications sont validées via le bouton **Update**.

L'activation des notifications peut alors être réalisée. L'accès à l'onglet **Configuration**, puis à **Actions** dans la barre de navigation de gauche, permet d'afficher une action préconfigurée chargée de l'envoi des notifications à l'ensemble des administrateurs Zabbix. Les paramètres

peuvent être consultés ou modifiés si nécessaire ; dans le cadre de ce tutoriel, les paramètres par défaut sont conservés. L'action est activée en sélectionnant le lien **Disabled** affiché en rouge dans la colonne **Status**.

Le système est désormais prêt à recevoir des alertes. Une alerte de test est générée à l'étape suivante afin de vérifier le bon fonctionnement de la configuration de notification.

Étape 9 - Génération d'une alerte de test

Au cours de cette étape, une alerte de test est générée afin de vérifier que l'ensemble de la configuration est opérationnel. Par défaut, Zabbix surveille l'espace disque disponible sur le serveur et détecte automatiquement les supports de stockage, en ajoutant les contrôles associés. Cette phase de découverte étant exécutée toutes les heures, un délai peut être nécessaire avant le déclenchement de la notification.

Un fichier temporaire de taille suffisante est alors créé afin de provoquer une alerte liée à l'utilisation du système de fichiers de Zabbix. Pour cela, une connexion est établie sur le second serveur Ubuntu:

```
ssh sammy@second_ubuntu_server_ip_address
```

Ensuite, je détermine l'espace libre dont vous disposez sur le serveur. Je peux utiliser la commande `df` pour le savoir :

```
df -h
```

La commande `df` indiquera l'utilisation de l'espace disque de votre système de fichiers, et le `-h` rendra la sortie lisible à l'oeil humain. Vous verrez une sortie comme celle-ci :

```
OutputFilesystem      Size  Used Avail Use% Mounted on
/dev/vda1        78G  1.4G   77G    2% /
```

Dans ce cas, l'espace libre est de **77G**. Votre espace libre peut être différent.

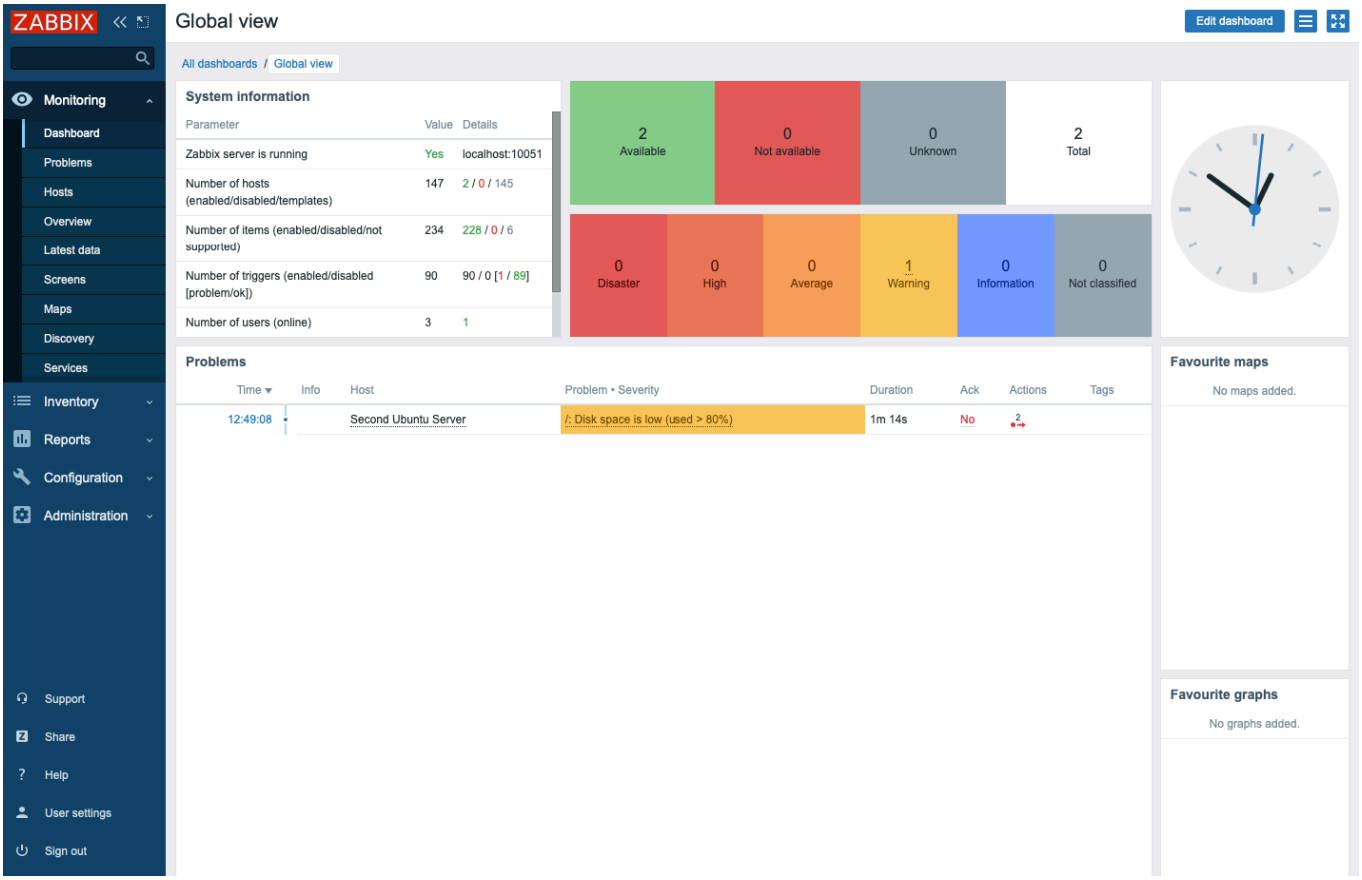
J'utilise la commande `fallocate`, qui permet de pré-allouer ou de désallouer de l'espace à un fichier, pour créer un fichier qui occupe plus de 80 % de l'espace disque disponible. Cela sera suffisant pour déclencher l'alerte :

```
fallocate -l 70G /tmp/temp.img
```

Après environ une heure, Zabbix déclenchera une alerte concernant la quantité d'espace disque disponible et exécutera l'action que j'ai configurée, en envoyant le message de notification. Je peux vérifier dans votre boîte de réception si le message provient du serveur Zabbix. Je verrai un message du type :

```
Problem started at 09:49:08 on 2020.06.12
Problem name: /: Disk space is low (used > 80%)
Host: Second Ubuntu Server
Severity: Warning
Operational data: Space used: 71.34 GB of 77.36 GB (92.23 %)
Original problem ID: 106
```

Je vais accéder accéder à l'onglet **monitoring** et ensuite au **Dashboard** pour voir la notification et ses détails.



Maintenant que les alertes fonctionnent, je supprime le fichier temporaire que j'ai créé afin de récupérer votre espace disque :

```
rm -f /tmp/temp.img
```

Au bout d’une minute, Zabbix enverra le message de récupération et l’alerte disparaîtra du tableau de bord principal.

Suivi du trafic réseau

Afin de mettre en place le suivi du trafic réseau dans le temps, Zabbix s’appuie sur le protocole SNMP et sur des templates dédiés permettant de collecter automatiquement les statistiques des interfaces réseau (débit entrant/sortant, erreurs, saturation).

Pour surveiller un périphérique réseau, nous devons configurer SNMPv3 à la fois sur le serveur et sur le périphérique surveillé.