



école supérieure de
génie informatique

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU SÉCURISÉE

Date : 30/10/2024

Résumé

Ce référentiel répertorie l'historique, les livrables ainsi que l'ensemble des configurations qui constituent le projet annuel du groupe deux de la classe des 4ème années ESGI.

Elie R. / Biram H. / Alexis B. / Michel P.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

CONTENTS

Présentation du projet et de son périmètre	7
Introduction.....	7
Présentation du MOA	7
PRESENTATION du MOE.....	7
Analyse de l'existant.....	8
Structure organisationnelle et infrastructure.....	8
Structure organisationnelle et infrastructure.....	8
Points critiques.....	9
Résumé.....	10
Inventaire initial des actifs SI.....	11
Analyse des besoins.....	11
Contexte	11
Réseau et infrastructures	11

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Sécurité et surveillance.....	11
Gestion des accès et des identités.....	11
Développement et hardening	12
Transfert de données	12
Besoins techniques spécifiques	12
Besoins organisationnels	12
Analyse de risque	14
Introduction	14
Identification des Risques	14
Évaluation des Risques.....	15
Mesures d'atténuation et priorités	16
Périmètre fonctionnel et technique	17
Introduction	17
Périmètre technique	19
Conclusion.....	20
Bests practices aux acces physiques	20
Introduction	20
Principes Généraux	21
Technologies de Contrôle d'Accès.....	21
Gestion des Visiteurs.....	21
Surveillance et Audits.....	22
CADRE JURidique.....	23
Réponse aux Incidents.....	23
Formation et Sensibilisation	23
Modèles et Documents	23
Modèles de formulaires	24
Organisation.....	27
Pilotage de projet	28
Communication projet.....	28
Présentation de l'équipe réalisatrice	28
Elie ROCAMORA	28
Biram HABIBOULAYE DANDARÉ	29
Alexis Brunel.....	29

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Michel Perez-Colombano	29
Schéma de la solution réseau et système.....	29
Vue physique	29
Vue logique.....	30
VLAN et adressage	30
Présentation des solutions techniques réseau et système	31
Solution de design d'infrastructure réseau	31
Solution d'infrastructure système	31
Solution de supervision	32
Solution de MicroSOC.....	32
Solution de virtualisation.....	33
Solution de sécurité réseau.....	33
Solution web.....	34
Solution d'analyse de vulnérabilité	34
Solution de SSO.....	35
Solution de transfert de secrets.....	35
Sécurisation et résilience de la solution :.....	36
1. Gestion des identités et accès sécurisés	36
2. Protection de l'infrastructure réseau	37
3. Supervision hardware	38
4. Protection des données sensibles.....	39
4. Résilience opérationnelle.....	39
5. Protection des données sensibles.....	40
6. Monitoring/SOC - Architecture unifiée	41
Plan de Continuité d'Activité (PCA) – TOURISK ASSURANCE.....	44
1. Objectif du PCA	44
2. Portée du PCA.....	45
3. Analyse d'Impact Métier (BIA)	45
4. SCÉNARIOS IDENTIFIÉS	46
4.1 – Petite Catastrophes naturelles et incidents locaux faible	46
4.2 – Défaillance IT.....	46
4.3 – Cybermenaces	46
5. Plans de réponse	46

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

5.1 – Incident Proxmox (infrastructure locale)	46
5.2 – Perte de connectivité	47
5.3 – Fuite ou vol de données.....	47
5.4 – Inaccessibilité locale	48
5.5 – Application web	48
6. Tests et maintenance	48
Plan de Reprise d'Activité (PRA) - Tourisk Assurance	50
1. Contexte et Objectifs Stratégiques	50
1.1 Périmètre du PRA.....	50
1.2 Architecture Hybride.....	50
2. Scénarios de Risque Étendus.....	50
2.1 Cyberattaque de Type Ransomware	50
2.2 Panne Électrique Prolongée (72h+)	51
2.3 Double Coupure Internet (Box 1 + 2)	51
3. Performances PBS : Tableaux de Référence.....	51
3.1 Temps de Restauration par Type de VM.....	52
3.2 Facteurs d'Optimisation.....	52
4. Procédures Opérationnelles Détaillées.....	52
4.1 Reconstruction Complète du Cluster	52
5. Annexes Techniques (Extraits)	53
Annexe A : Scripts d'Urgence	53
Annexe B : Métriques Zabbix pour Détection	53
Annexe C : Diagramme de Flux de Reprise	53
6. Validation et Amélioration Continue	54
6.1 Programme de Tests.....	54
6.2 Roadmap d'Amélioration.....	54
cahier de recette.....	56
Réalisation des tâches.....	56
Conclusion.....	57
Cahier D'exploitation	57
ZABBIX.....	58
Installation.....	58
GRAFANA	59

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

OPNSENSE	61
Tpot.....	63
PRIVATebin	65
Bastion Teleport	66
PROXMOX (PVE et PBS)	69
Scanner de vulnérabilité	70
SIEM et XDR	70
Annexes.....	82
PCA	82
Annexe 1	83
Court terme – Objectif : stopper la propagation	83
Annexe 2.....	85
Annexe 3.....	87
Annexe 4.....	88
PRA	89
5. Annexes Techniques (Extraits).....	89
Web	90
Annexe 1 : diagramme de sequence uml	90
Annexe 2 : diagramme de flux	91
Annexe plan des locaux physiques	92
ANNEXE : INSTALLATION ET CONFIGURATION DE opnsense	94
SOMMAIRE	94
MISE EN PLACE DU DHCP	100
Annexe Installation et utilisateur du Tpot.	115
INSTALLATION PRIVATEBIN ET D'UNE CA ET CA Intermédiaire.....	120
Annexe Installation de TELEPORT	122
Zabbix configuration.....	128
Ajout de client (Windows & Linux)	133
Windows.....	133
Sur linux.....	134
Configuration sur l'interface zabbix (Pour tous les OS)	136
Monitoring d'un service (apache2)	139
GRafana configuration	146

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Dashboard configuration	146
1- Data source	146

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

PRESENTATION DU PROJET ET DE SON PERIMETRE

INTRODUCTION

Le projet est réalisé dans le cadre de la formation des étudiants de 4ème année de l'ESGI.

Il a pour objectif de créer la maquette d'une infrastructure réseau sécurisée avec un faux client, dans le but de simuler un contexte professionnel qui sera détaillé dans la présentation du **MOA**.

Le projet a débuté le **30 octobre 2024** et devra être livré au plus tard, le **6 juillet 2024**.

Le groupe d'étudiants en charge du projet est composé de quatre personnes, chacune ayant des rôles prédefinis à l'avance. Ils feront partie de l'entreprise fictive qui devra réaliser le projet et qui sera détaillée dans la présentation du **MOE**.

PRESENTATION DU MOA

La société de cyber sécurité **FortifyOps** a été contacté par l'assurance internationale, **TouRisK** pour l'installation numérique et réseau de leur nouvelle filiale à Dubaï.

Ils doivent assurer la cohérence avec les exigences légales et réglementaires.

Cependant, l'évolution croissante du nombre de clients pousse à industrialiser et numériser les processus.

L'assurance implantée à **Toulouse**, vise à s'étendre aux Emirats Arabes Unis afin de s'adapter au marché et accueillir de nouveaux clients.

Pour cela, **TouRisK** a ouvert de nouveaux locaux récemment dans la ville de **Dubaï**.

Face aux défis numériques, le site principal à Toulouse était déjà équipé d'une petite infrastructure informatique qui devra être révisée.

Toutefois, le site secondaire à Dubaï n'est pas muni de matériel réseau et une infrastructure doit être construite pour répondre au besoin du client et communiquer avec le site principal.

Un pôle informatique est présent sur le site principal pour entretenir l'infrastructure réseau et assurer le support et la sécurité des utilisateurs.

PRESENTATION DU MOE

La start-up **FortifyOps**, spécialisée dans le consulting informatique a été contactée par **TouRisK** pour effectuer un audit sur leur infrastructure et proposer des solutions de sécurité.

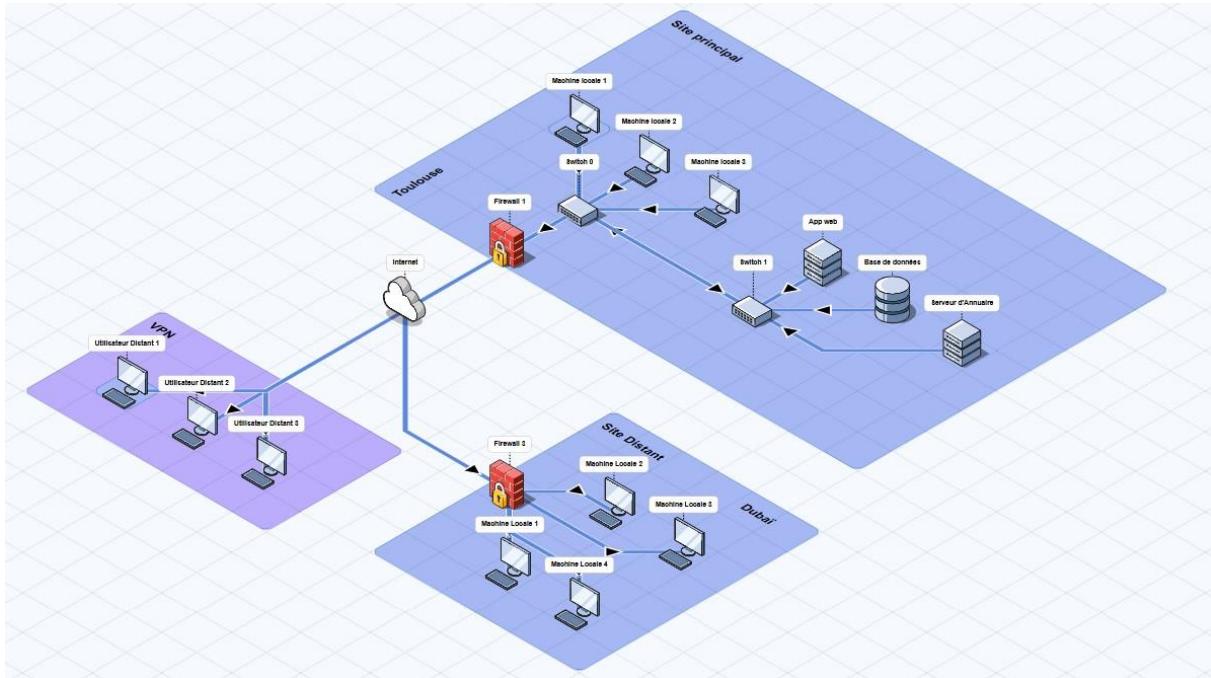
L'entreprise présente plusieurs services dont :

- Un pôle SI pour concevoir et mettre en place les infrastructures réseaux de nos clients.
- Une Red team pour mettre à l'épreuve la sécurité de nos clients.
- Un pôle développement web pour mettre en avant les projets de nos clients.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

ANALYSE DE L'EXISTANT

Schéma réseau actuel de la société TouRisK



On retrouve 2 sites, un site principal situé à Toulouse et un site distant récent créé à Dubaï.

Un accès VPN est mis en place depuis le site principal pour les utilisateurs en distanciel.

STRUCTURE ORGANISATIONNELLE ET INFRASTRUCTURE

L'entreprise **TouRisK** est une assurance internationale avec deux sites (Toulouse | siège et Dubaï | Nouveau local).

Elle permet de posséder un compte, de réaliser des transactions en ligne et de déposer de l'argent.

STRUCTURE ORGANISATIONNELLE ET INFRASTRUCTURE

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

SITE PRINCIPAL : TOULOUSE

Serveurs :

- Serveur d'annuaire : Gestion centralisée des identités et des accès, machines...
- Base de données : Stocke les informations critiques liées aux clients et aux transactions.
- Application Web : Permet l'accès utilisateur aux services proposés par l'entreprise.

Équipements réseau :

- Deux switches (Switch 0, Switch 1) pour la connectivité interne.
- Firewall de sortie protégeant les communications externes.

Machines de travail :

- Machines locales dédiées aux opérations courantes. Maintenance des utilisateurs et des développements et maintenance des outils internes.

SITE DISTANT : DUBAÏ

Machines de travail :

- Machines locales dédiées aux opérations courantes

Équipements réseau :

- Firewall de sortie garantissant la sécurité réseau.
- VPN pour interconnexion sécurisée entre les deux sites.

SITE PRINCIPAL : TOULOUSE

Machines de travail distantes :

- Trois machines distantes connectées via le VPN, suggérant des accès potentiels externes pour les développeurs ou activité métier.

POINTS CRITIQUES

FORCES DE L'INFRASTRUCTURE

Infrastructure distribuée :

- Les deux sites permettent une continuité géographique et opérationnelle.

Sécurité réseau initiale :

- Présence de firewalls sur chaque site pour limiter les risques d'intrusion.
- VPN entre les sites pour sécuriser les communications.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Centralisation des identités :

- Serveur d'annuaire pour gérer les autorisations, réduisant les risques d'erreurs dans la gestion des accès.

FAIBLESSES POTENTIELLES

Gestion des sauvegardes :

- Aucune mention des sauvegardes pour les serveurs, bases de données ou configurations critiques. Une panne pourrait entraîner des pertes significatives.

Absence de segmentation réseau :

- Les machines locales et distantes semblent partager un réseau sans indications claires de segmentation. Cela augmente le risque de propagation en cas de compromission.

Sécurité des machines de travail :

- Pas d'antivirus annoncé.
- Pas de centralisation des logs
- Pas de chiffrement des disques

Absence de supervision :

- Aucun système mentionné pour la surveillance proactive (SIEM, EDR, logs de sécurité, IDS/IPS).
- Pas de service de sécurité dédié à la surveillance d'alertes (SOC) et de réponse à incident (SOAR)

RISQUES LIÉS AU CONTEXTE DE L'ENTREPRISE

Conformité réglementaire :

- Étant une banque en ligne internationale, l'entreprise doit respecter diverses réglementations (GDPR, PCI DSS, etc.). Aucune mention d'un cadre de conformité en place.

Cyberattaques :

- Risques élevés de ransomware, phishing, ou attaques ciblées sur les systèmes critiques comme les bases de données.

Localisation géographique :

- Le nouveau site à Dubaï peut introduire des défis liés à la législation locale et aux infrastructures réseau.

RESUME

L'infrastructure en place montre un effort initial pour structurer et sécuriser les deux sites, mais elle présente des lacunes importantes en matière de sauvegarde, de surveillance et de sécurité. Ces

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

faiblesses augmentent les risques opérationnels et de sécurité, particulièrement dans un contexte bancaire critique. Différents besoins sont identifiés, se référer à l'analyse des besoins.

INVENTAIRE INITIAL DES ACTIFS SI

Voir annexe Inventaire des Actifs

ANALYSE DES BESOINS

CONTEXTE

L'entreprise, une banque en ligne internationale, évolue dans un environnement nécessitant une sécurisation accrue des systèmes d'information. Les nouvelles tâches identifiées indiquent une volonté de renforcer la sécurité, améliorer la gestion des infrastructures, et professionnaliser les processus internes.

RESEAU ET INFRASTRUCTURES

Serveurs web (Docker Swarm) :

- Gestion d'un cluster de serveurs pour une haute disponibilité.
- Ajout d'un WAF (Web Application Firewall) pour filtrer les requêtes malveillantes.

SECURITE ET SURVEILLANCE

Supervision :

- Centralisation des journaux et des métriques réseau via un SIEM.
- Surveillance des processus via un EDR (Endpoint Detection and Response).
- Automatisation de la réponse à incident via un SOAR.

Analyse des failles :

- Automatisation des scans de vulnérabilités.
- Formation d'une équipe interne pour auditer les applications et les systèmes (Purple Team).

Honeypots :

- Déploiement pour attirer et analyser les attaquants.
- Identification des techniques d'attaque utilisées.

GESTION DES ACCES ET DES IDENTITES

OpenLDAP :

- Centralisation de la gestion des utilisateurs pour simplifier l'administration.
- Synchronisation avec d'autres services (ex. VPN, applications internes).

SSO (Keycloak) :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Simplification de l'accès aux applications via une authentification unique.
- Intégration d'un MFA pour sécuriser les connexions.

DEVELOPPEMENT ET HARDENING

Développement d'applications web sécurisées :

- Implémentation des standards OWASP pour protéger contre les attaques courantes (ex. injection SQL, XSS).

Hardening du SI :

- Configuration renforcée des serveurs, postes de travail et équipements réseau.
- Chiffrement des disques avec Bitlocker.

TRANSFERT DE DONNEES

Transfert de secrets via Privatebin en local.

BESOINS TECHNIQUES SPECIFIQUES

INFRASTRUCTURE TECHNIQUE

Serveurs web et sécurité :

- Docker Swarm pour la gestion d'applications distribuées.
- WAF (ex. ModSecurity ou Bunkerweb) pour bloquer les requêtes malveillantes au niveau des serveurs web.

SECURITE RENFORCEE

Surveillance proactive :

- SIEM pour centraliser les alertes et corrélérer les événements (ex. Splunk, ELK Stack).
- EDR pour détecter et répondre aux incidents sur les postes de travail et serveurs.
- Zabbix pour supervision réseau.

Détection avancée :

- Analyse des tentatives d'intrusion via des honeypots déployés dans des segments spécifiques.

ACCES ET IDENTITES

- OpenLDAP et SSO intégrés pour une gestion simplifiée des droits.
- Sécurisation des mots de passe via des politiques fortes (rotation, MFA).

BESOINS ORGANISATIONNELS

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

FORMATION CONTINUE

- Formation sur les environnements Purple Team pour le personnel IT.
- Sensibilisation des utilisateurs finaux à la cybersécurité et aux pratiques sécurisées.

DOCUMENTATION ET GOUVERNANCE

- Documentation des configurations (serveurs, WAF, SIEM, EDR).
- Alignement sur des standards (ISO 27001, NIST).

PRIORITES CLES

Mise en place du SIEM et des honeypots :

- Centraliser la détection des menaces.
- Surveiller les comportements malveillants en temps réel.
- Déploiement de Docker Swarm avec un WAF :
- Garantir la résilience des services web.
- Filtrer les menaces au niveau applicatif.

Lancement d'un lab Purple :

- Former les équipes IT et sécurité via des simulations de scénarios réels.

Intégration OpenLDAP et SSO :

- Simplifier la gestion des utilisateurs.
- Améliorer l'expérience des utilisateurs avec un MFA.

Formalisation et tests du PRA :

- Identifier les priorités en cas de sinistre.
- Assurer une reprise rapide et coordonnée des activités.

Assurer la continuité :

- Mise en place d'un load balancer pour l'application web.

RECOMMANDATIONS IMMÉDIATES

Mettre en place des sauvegardes automatisées :

- Inclure la base de données, le serveur d'annuaire, et les configurations réseau.
- Répliquer les bases de données.
- Tester régulièrement les restaurations.

Renforcer la sécurité des terminaux :

- Installer des solutions EDR pour protéger les machines locales et distantes.
- Implémenter le chiffrement des disques et activer l'authentification multifactorielle (MFA).

Superviser et journaliser :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Déployer un SIEM pour la collecte et l'analyse des logs.
- Activer les journaux d'accès et de sécurité sur les serveurs et firewalls.

Segmenter le réseau :

- Isoler les machines critiques (serveurs, bases de données) des postes de travail.
- Mettre en œuvre des VLANs pour limiter les mouvements latéraux. (Administration, utilisateurs, dev ...)

Auditer la conformité :

- Évaluer l'alignement avec les normes applicables (ISO 27001, PCI DSS).
- Mettre en œuvre un cadre de gestion des risques basé sur NIST ou ISO.

ANALYSE DE RISQUE

INTRODUCTION

Cette analyse vise à identifier les principaux risques associés à l'existant et aux besoins exprimés, tout en proposant des axes prioritaires pour atténuer ces risques.

IDENTIFICATION DES RISQUES

RISQUES LIÉS À L'INFRASTRUCTURE

1. Pertes de données critiques
 - Faiblesse : Absence de stratégie claire de sauvegarde. Aucune mention de PRA pour les serveurs critiques (base de données, application Web).
 - Impact : Perte de données sensibles des clients, interruption de service et atteinte à la réputation.
 - Probabilité : Élevée en l'absence de mécanismes de test des restaurations.
2. Propagation latérale en cas de compromission
 - Faiblesse : Absence de segmentation réseau (VLANs) entre les postes de travail, serveurs et environnements critiques.
 - Impact : Facilitation de la propagation des menaces à travers l'infrastructure, compromettant l'intégralité du SI.
 - Probabilité : Moyenne à élevée.
3. Non-disponibilité des services
 - Faiblesse : Absence d'un mécanisme de haute disponibilité (HA) pour l'application Web et la base de données.
 - Impact : Rupture de services bancaires, non-respect des SLA (Service Level Agreement).
 - Probabilité : Moyenne.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

RISQUES LIÉS À LA SÉCURITÉ

4. Cyberattaques ciblées

- Faiblesse : Absence d'outils de détection proactive (SIEM, EDR, honeypots).
- Impact : Compromission des bases de données clients via ransomware, phishing ou DDoS.
- Probabilité : Élevée compte tenu du contexte bancaire.

5. Vol ou accès non autorisé aux données sensibles

- Faiblesse : Absence de chiffrement des disques et des bases de données.
- Impact : Exposition des données critiques en cas d'attaque ou vol physique.
- Probabilité : Moyenne à élevée.

6. Mauvaises pratiques d'accès utilisateur

- Faiblesse : Gestion décentralisée des identités sans SSO ni MFA pour sécuriser les connexions distantes.
- Impact : Exploitation des comptes par des acteurs malveillants, compromission des systèmes internes.
- Probabilité : Moyenne à élevée.

RISQUES LIÉS À LA CONFORMITÉ

7. Non-conformité réglementaire

- Faiblesse : Pas de cadre de conformité aligné sur GDPR, PCI DSS ou ISO 27001.
- Impact : Sanctions financières, perte de crédibilité auprès des régulateurs et des clients.
- Probabilité : Moyenne.

ÉVALUATION DES RISQUES

Catégorie	Risque	Impact	Probabilité	Priorité

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Infrastructure	Perte de données critiques	Très élevé	Élevée	Critique
	Propagation latérale	Élevé	Moyenne	Élevée
	Non-disponibilité des services	Élevé	Moyenne	Élevée
Sécurité	Cyberattaques ciblées	Très élevé	Élevée	Critique
	Vol de données sensibles	Élevé	Moyenne	Élevée
	Mauvaise gestion des accès	Élevé	Moyenne	Élevée
Conformité	Non-respect des régulations (GDPR, PCI DSS)	Élevé	Moyenne	Moyenne

MESURES D'ATTENUATION ET PRIORITES

INFRASTRUCTURE

Implémentation d'une stratégie de sauvegarde :

- Automatisation des sauvegardes quotidiennes des données critiques (base de données, annuaire, configurations).
- Rétention des sauvegardes hors site et tests réguliers de restauration.
- Impact attendu : Réduction des pertes de données et des interruptions critiques.

Mise en place de VLANs :

- Segmentation réseau pour isoler les postes utilisateurs, les serveurs d'applications, et les bases de données.
- Impact attendu : Limitation de la propagation des menaces.

Haute disponibilité (HA) :

- Déploiement de mécanismes comme le load balancer et la réplication des bases de données.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Impact attendu : Garantir la disponibilité continue des services en ligne.

SECURITE

Déploiement de solutions SIEM et EDR :

- SIEM pour la corrélation des événements de sécurité (ex. ELK Stack).
- EDR pour surveiller et protéger les postes de travail.
- Impact attendu : Détection proactive des incidents et réponse rapide.

Renforcement des accès :

- Implémentation d'un SSO (Keycloak) et d'un MFA pour toutes les connexions.
- Impact attendu : Réduction des risques d'accès non autorisés.

Chiffrement des données :

- Activation du chiffrement AES-256 pour les disques et les bases de données critiques.
- Impact attendu : Protection des données sensibles en cas de vol ou d'accès non autorisé.

Honeypots :

- Déploiement de leurres dans des segments spécifiques pour détecter les activités malveillantes.
- Impact attendu : Identification des techniques d'attaque.

CONFORMITE

Alignement sur les standards :

- Mise en place d'un cadre basé sur ISO 27001 et PCI DSS.
- Réalisation d'audits réguliers pour garantir le respect des réglementations.
- Impact attendu : Réduction des risques juridiques et amélioration de la confiance des clients.

PERIMETRE FONCTIONNEL ET TECHNIQUE

INTRODUCTION

CONTEXTE DU PROJET

La sécurité des systèmes d'information (SI) est un enjeu majeur pour la banque internationale TouRisK, notamment avec l'expansion de ses activités à Dubaï. Afin de garantir la protection de ses données sensibles et d'assurer la continuité de ses opérations, la banque a décidé de mettre en place un Security Operations Center (SOC) dédié. Ce centre aura pour mission de détecter, surveiller et répondre en

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

temps réel aux menaces, en utilisant des technologies avancées telles que le SIEM, les EDR, et les outils SOAR. FortifyOps a été mandaté pour concevoir et déployer cette infrastructure de sécurité.

OBJECTIFS DU DOCUMENT

Le but de ce document est de définir clairement le périmètre fonctionnel et technique du projet SOC pour TouRisk. Il permet de spécifier les fonctionnalités attendues, les outils et les technologies à utiliser, ainsi que les processus à mettre en place pour garantir une gestion efficace de la sécurité au sein de l'organisation.

FONCTIONNALITÉS PRINCIPALES

Le SOC devra remplir plusieurs fonctions essentielles pour être efficace :

- Surveillance continue : Surveillance 24/7 de l'ensemble des systèmes et des réseaux pour détecter toute anomalie ou activité suspecte.
 - Objectif : détection en temps réel des menaces
- Détection des incidents : Identification automatique des menaces à l'aide des outils de détection, notamment le SIEM, et analyse des événements suspects sur les endpoints.
 - Objectif : gestion des alertes
- Analyse des incidents : Identification, investigation et catégorisation des incidents de sécurité pour comprendre leur origine et leur impact potentiel.
 - Objectif : réduire les menaces
- Réponse et remédiation : Automatisation des réponses aux incidents via le SOAR, afin de limiter les délais de réponse et les erreurs humaines.
 - Objectif : répondre aux incidents
- Rapport et suivi : Génération de rapports réguliers sur les incidents traités, les alertes reçues, et les actions menées, afin d'assurer une traçabilité complète.
 - Objectif : Conformité et management

UTILISATEURS ET BESOINS

Les principaux utilisateurs du SOC seront :

- Les analystes SOC : Ils auront besoin d'une interface pour surveiller les alertes, analyser les incidents, et coordonner les réponses.
- Les responsables de la sécurité : Ils auront besoin de rapports sur l'efficacité du SOC, les incidents traités et la conformité aux normes de sécurité.
- Les administrateurs de systèmes : Ils devront configurer les outils de surveillance et de réponse, maintenir l'infrastructure, et gérer les accès.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

PROCESSUS ET FLUX DE TRAVAIL

Les principaux processus incluent :

- Collecte des logs et données de sécurité : Intégration des outils SIEM et EDR pour centraliser les données provenant des différents systèmes.
- Détection et évaluation des alertes : Lorsqu'une alerte est générée, l'analyste SOC doit évaluer sa criticité et déterminer si une action immédiate est nécessaire.
- Réponse aux incidents : Les actions peuvent inclure l'isolement d'un endpoint compromis, la mise en quarantaine de fichiers suspects ou la mise en œuvre de mesures de sécurité renforcées.
- Escalade : Les incidents critiques seront escaladés à un niveau supérieur pour une analyse approfondie et une action plus ciblée.

PERIMETRE TECHNIQUE

TECHNOLOGIES ET OUTILS UTILISÉS

Le SOC de TouRisK reposera sur plusieurs technologies spécifiques :

- SIEM (Security Information and Event Management) : Un outil comme ELK sera utilisé pour la collecte, l'analyse et la corrélation des logs afin de détecter les anomalies et les incidents de sécurité.
- EDR (Endpoint Detection and Response) : Une solution sera déployée pour surveiller les endpoints (ordinateurs, serveurs, etc.) et détecter les menaces en temps réel.
- SOAR (Security Orchestration, Automation, and Response) : Des outils seront utilisés pour automatiser les réponses aux incidents et orchestrer les actions de sécurité.
- Contrôles d'accès physiques : Le contrôle d'accès aux infrastructures sensibles sera assuré par des solutions matérielles et logicielles de gestion des accès physiques.

ARCHITECTURE TECHNIQUE

L'architecture du SOC comprendra :

- Infrastructure Interne : Le SOC sera déployé sur une infrastructure interne pour garantir la flexibilité, la gestion, la scalabilité et la résilience du système.
- Connectivité sécurisée : Une liaison sécurisée (VPN), tunnels IPSec, etc. entre les différents sites (y compris la filiale de Dubaï) et le centre d'opérations sera mise en place pour garantir la confidentialité et l'intégrité des données.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Stockage et traitement des données : Des serveurs sécurisés seront utilisés pour stocker les logs et les données critiques, avec des mécanismes de sauvegarde pour éviter toute perte de données.

CONCLUSION

RECAPITULATIF DU PERIMETRE

Le projet de mise en place du SOC pour TouRisK repose sur l'intégration de technologies de pointe pour garantir une détection et une réponse rapides aux menaces. Le périmètre fonctionnel et technique définit clairement les objectifs, les fonctionnalités, ainsi que les outils et l'architecture nécessaires pour répondre aux besoins de sécurité de l'entreprise.

PROCHAINES ETAPES

Finalisation du cahier des charges et validation par les parties prenantes.

Lancement du déploiement de l'infrastructure SOC selon les phases définies.

Mise en place d'un plan de maintenance et d'évolution pour le SOC, afin de garantir son efficacité sur le long terme.

BESTS PRACTICES AUX ACCES PHYSIQUES

INTRODUCTION

Dans le cadre de l'expansion internationale de TouRisK, et en particulier avec l'ouverture de la filiale de Dubaï, la sécurisation des infrastructures sensibles constitue une priorité stratégique. Ces infrastructures abritent des données critiques et des équipements essentiels, et leur protection contre

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

les menaces physiques est indispensable pour garantir la continuité des opérations et la confiance des clients.

Ce document présente les meilleures pratiques pour la gestion des accès physiques, permettant de prévenir les intrusions non autorisées, de minimiser les risques et d'assurer une résilience optimale.

PRINCIPES GENERAUX

- **Approche basée sur le risque** : Identifiez et classez les zones selon leur criticité (publiques, restreintes, hautement sécurisées). Allouez des ressources de sécurité en conséquence.
 - **Responsabilités définies** : Chaque acteur (employés, prestataires, sécurité) doit comprendre et assumer son rôle dans la gestion des accès physiques.
 - **Traçabilité des accès** : Maintenez des journaux d'accès rigoureux pour chaque entrée et sortie dans les zones sensibles, avec une conservation des données adaptée aux exigences légales.

TECHNOLOGIES DE CONTROLE D'ACCÈS

Systèmes de Badge :

- Utilisez des badges RFID ou NFC attribués individuellement, contenant des autorisations spécifiques pour chaque utilisateur.
 - Activez la désactivation immédiate des badges perdus ou volés.

Smartphone **comme** **support** **d'authentification**
Implémentation de solutions NFC/Bluetooth (ex : ARD Mobile ID) avec :

- Génération dynamique de certificats numériques
 - Verrouillage instantané via console d'administration
 - Combinaison avec authentification biométrique embarquée (Face ID/Touch ID)

Biométrie :

- Implémentez des solutions biométriques (empreintes digitales, reconnaissance faciale) pour les zones critiques, combinées avec un badge pour une double authentification.

Détection avancée en zones sensibles
Capteurs de pression au sol dans les bunkers pour :

- Détection de masse anormale
 - Prévention des accès groupés non autorisés
 - Intégration avec système d'alarme silencieuse

GESTION DES VISITEURS

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Procédures d'Accueil :

1. Tous les visiteurs doivent être préenregistrés par un employé hôte.
2. À leur arrivée, ils doivent fournir une pièce d'identité valide et recevoir un badge temporaire.

Supervision et Traçabilité :

Traçabilité numérique (Solution cloud) :

- Pré-enregistrement via portail web sécurisé
- QR code temporaire avec géolocalisation active
- Synchronisation automatique avec registre RGPD
- Purge automatique après 90 jours (conformément à la CNIL)

Zones Autorisées :

- Limitez les visiteurs aux zones publiques ou spécifiques selon leur besoin.
- Les zones hautement sécurisées ne doivent jamais être accessibles aux tiers sans validation exceptionnelle.

SURVEILLANCE ET AUDITS

Vidéosurveillance :

- Installez des caméras dans les points stratégiques, notamment les entrées/sorties et les zones sensibles.
- Configurez un système de détection automatique des comportements suspects.

Audits Périodiques :

Cycle de 24 mois avec :

- 4 mois d'évaluation des dispositifs de contrôle d'accès pour vérifier leur fonctionnalité et identifier les vulnérabilités (pentests physiques incluant lockpicking)
- 6 mois de remédiation priorisée
- Audit de vérification à 18 mois
- Rapport d'écart conforme ISO 27001
- Intégrer les résultats des audits dans un plan d'amélioration continue.

Tests techniques spécialisés :

- Évaluation trimestrielle des serrures électroniques
- Simulation d'intrusion physique avec scénarios réalistes

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

CADRE JURIDIQUE

Signalétique obligatoire (Panneaux visibles) avec :

- Mention CNIL pour vidéoprotection
- Interdiction de photographier (Art. 226-1 CP)
- Consignes de branchement d'équipements externes

Politique de sécurité matérielle :

- Connectique sécurisée avec port USB désactivés
- Système d'autorisation préalable pour périphériques externes
- Journalisation des connexions physiques

REPONSE AUX INCIDENTS

Détection Rapide :

- Configurez des alarmes pour détecter toute tentative d'effraction ou de manipulation des dispositifs de contrôle.

Procédures en Cas d'Incident :

1. **Signalement** : Informez immédiatement la direction de la sécurité.
2. **Investigation** : Collectez les journaux d'accès et enregistrements vidéo.
3. **Actions Correctives** : Renforcez les dispositifs défaillants et révisez les procédures si nécessaire.

FORMATION ET SENSIBILISATION

- **Formation Initiale** : Tous les employés doivent recevoir une formation sur les politiques d'accès physique dès leur intégration.
- **Formation Récurrente** : Organisez des sessions annuelles pour rappeler les bonnes pratiques et informer des mises à jour.
- **Simulations** : Effectuez des exercices pratiques pour évaluer la réaction des équipes face à des incidents simulés.

MODELES ET DOCUMENTS

Formulaire d'Autorisation d'Accès :

- Document requis pour valider tout accès exceptionnel aux zones restreintes ou hautement sécurisées.

Rapport d'Incident :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Modèle standardisé pour consigner les détails d'un incident, les mesures prises et les recommandations pour éviter sa répétition.

Conclusion

En appliquant ces bonnes pratiques, TouRisK renforce la sécurité de ses infrastructures sensibles tout en respectant les exigences opérationnelles et réglementaires. La combinaison de technologies modernes, de procédures rigoureuses et d'une culture de sécurité partagée garantit une protection optimale contre les menaces physiques.

MODELES DE FORMULAIRES

Dans le cadre de la gestion des accès physiques, l'utilisation de formulaires standardisés est essentielle pour garantir la traçabilité et l'efficacité des processus. Ces formulaires incluent les autorisations d'accès et les rapports d'incident, adaptés aux besoins de TouRisK. Voici les modèles proposés, accompagnés de schémas illustratifs pour faciliter leur utilisation.

FORMULAIRE D'AUTORISATION D'ACCÈS

Le formulaire d'autorisation d'accès est utilisé pour valider et documenter l'accès des employés, visiteurs ou prestataires aux zones restreintes ou hautement sécurisées. Ce formulaire doit être rempli avant toute demande d'accès et approuvé par les responsables habilités.

FORMULAIRE DE RAPPORT D'INCIDENT

Le formulaire de rapport d'incident est utilisé pour documenter tout incident lié aux accès physiques. Ce rapport sert à analyser les causes, évaluer les impacts et définir les mesures correctives nécessaires.

UTILISATION ET ARCHIVAGE DES FORMULAIRES

- Formulaire d'autorisation d'accès :**
 - Conservé pour une durée de 6 mois à 1 an, selon les politiques de l'entreprise.
 - Disponible en version papier et numérique pour faciliter les audits.
- Formulaire de rapport d'incident :**
 - Conservé pour une durée minimale de 3 ans, en conformité avec les exigences légales et les audits internes.
 - Intégré dans le système de gestion des incidents pour un suivi centralisé.

En standardisant ces formulaires et en les intégrant aux processus opérationnels, TouRisK améliore la traçabilité et la gestion des accès physiques, tout en renforçant sa capacité à réagir efficacement aux incidents.

MODELES DE FORMULAIRE

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Formulaire d'Autorisation d'Accès

Identité du Demandeur

Nom : _____

Prénom : _____

Fonction/Entreprise : _____

Contact (e-mail/téléphone) : _____

Détails de la Demande

Zone concernée : _____

Date(s) d'accès : _____

Durée estimée : _____

Motif de la demande : _____

Validation et Signature

Responsable autorisant : _____

Fonction : _____

Signature : _____

Date : _____

Commentaires (facultatifs)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Formulaire d'Autorisation d'Accès

Formulaire de Rapport d'Incident

Informations Générales

Date et heure de l'incident : _____

Lieu de l'incident : _____

Nom du rapporteur : _____

Fonction : _____

Description de l'Incident

Type d'incident :

Intrusion non autorisée

Alarme déclenchée

Dispositif défaillant

Autre (préciser) : _____

Description détaillée :

Données Collectées

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Formulaire d'Autorisation d'Accès

Témoins identifiés : _____

Enregistrements vidéo : [] Oui / [] Non

Actions Immédiates

Mesures prises :

Validation et Suivi

Rapport validé par : _____

Fonction : _____

Date et signature : _____

Commentaires (facultatifs)

ORGANISATION

Pour le bon déroulé du projet, des méthodes d'organisation efficaces ont dû être mises en place.

Le projet a débuté le **30 octobre 2024** et devra être livré au plus tard, le **6 juillet 2024** ce qui laisse un peu moins de **neuf mois** pour mettre en place la solution.

Cependant, les membres du groupe ont tous une activité à temps plein à côté du projet ce qui rend la tâche complexe pour organiser les tâches de chacun sur des heures précises.

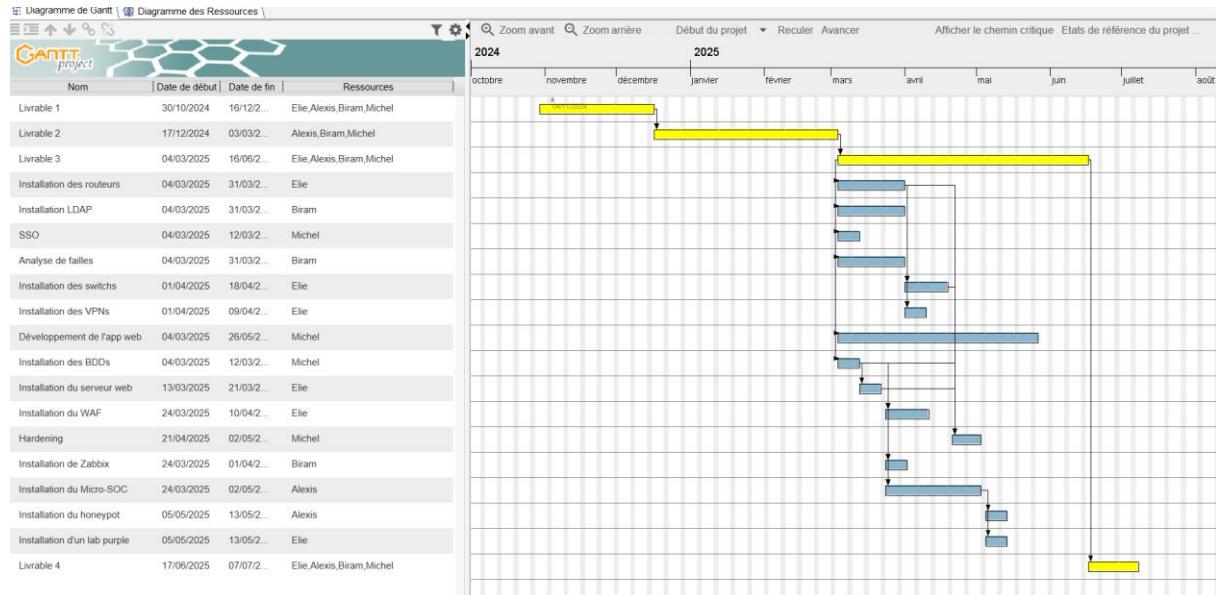
Le compromis trouvé a été de laisser chacun réaliser ses tâches de la semaine en étant souple vis à vis de la gestion du temps.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

La stratégie adoptée a été de donner une tâche à chaque membre de l'équipe en début de semaine, et faire un point le week-end suivant pour mettre l'ensemble de l'équipe au courant des avancés, et donner les nouvelles tâches pour la semaine suivante.

PILOTAGE DE PROJET

Voici le diagramme de Gantt détaillant les tâches du projet :



COMMUNICATION PROJET

Le système de communication au sein de l'équipe était un défi de taille pour faire avancer le projet car l'équipe est physiquement divisée sur le territoire national la majorité du temps.

Il fallait donc trouver une solution pour collaborer, le tout à distance.

L'équipe étant à l'aise avec **Discord**, nous avons choisi cette solution pour communiquer à la fois par écrit et par vive voix quand cela était nécessaire.

PRESENTATION DE L'EQUIPE REALISATRICE

ELIE ROCAMORA

Responsable du projet et chef d'équipe, il devra assurer la réalisation des tâches dans le temps imparti de la part des membres de l'équipe, la rédaction des documents du projet, la partie gestion du projet ainsi que de la bonne entente au sein de l'équipe.

En plus de ces tâches, il contribuera à des tâches techniques telles que :

- Configurer les équipements liés aux réseaux et à la haute disponibilité.
- L'installation du serveur web, de la répartition de charge et du WAF.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- La mise en place d'un laboratoire purple teaming.

BIRAM HABIBOULAYE DANDARÉ

Responsable de la partie supervision, annuaire et analyse de faille, il devra :

- Mettre en place le serveur Zabbix et l'alerting.
- Installer un annuaire LDAP et les agents Linux.
- Trouver une solution d'analyse des vulnérabilités.

ALEXIS BRUNEL

Responsable de la partie SIEM, il aura comme mission :

- L'installation de la suite ELK.
- La mise en place d'un outil d'alerting.
- La configuration des honeypots.

MICHEL PEREZ-COLOMBANO

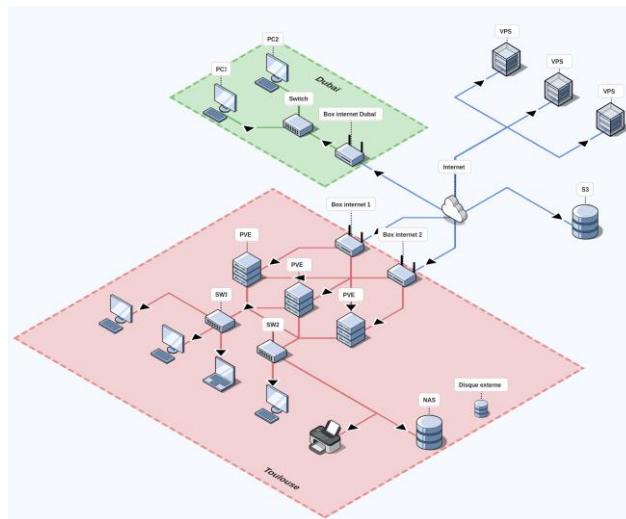
Responsable de la partie sécurisation et développement du site web, il devra :

- Développer le site web.
- Hardener des solutions systèmes et des services déployés sur le SI.
- Mettre en place d'un système de SSO.
- Rédition du PCA/PRA.

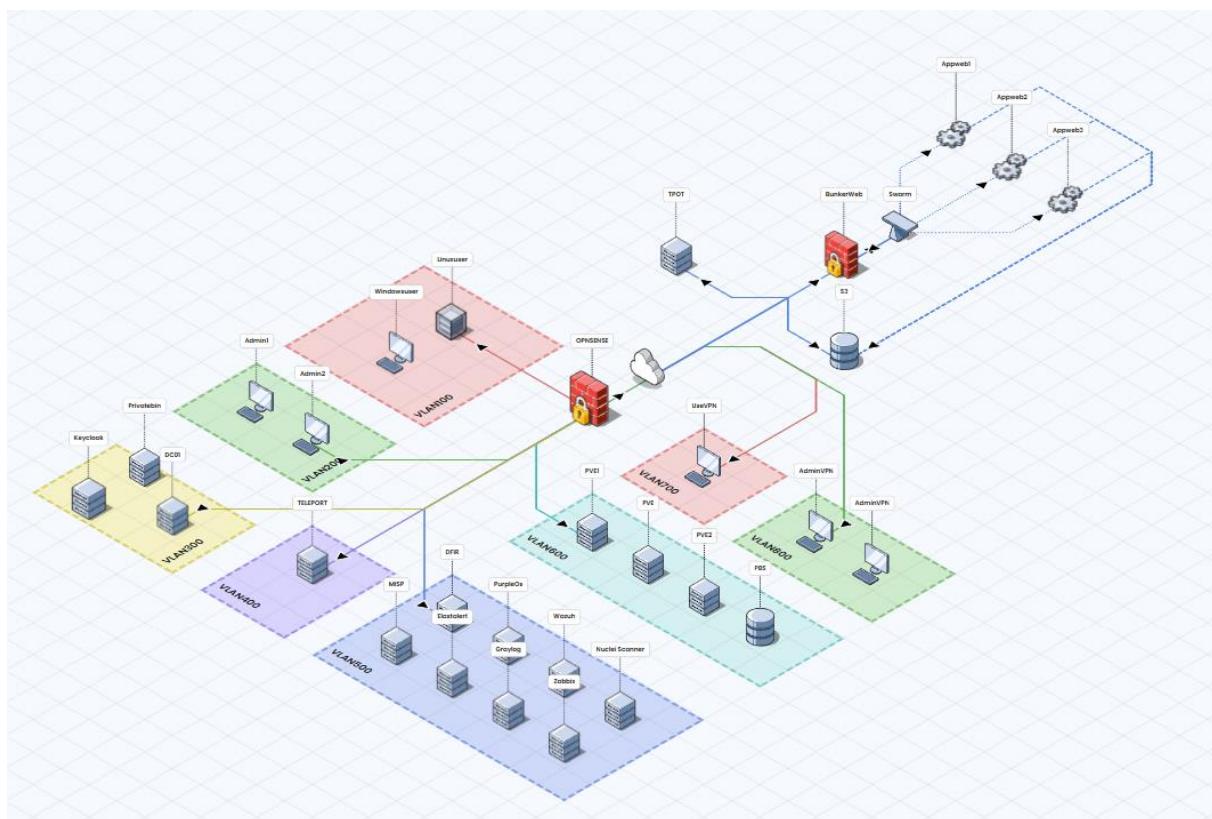
SCHEMA DE LA SOLUTION RESEAU ET SYSTEME

VUE PHYSIQUE

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



VUE LOGIQUE



VLAN ET ADRESSAGE

VLANs ID	Fonctions	IP (CIDR)
100	Utilisateurs	10.1.0.0/24
200	IT	10.2.0.0/24
300	Serveurs	10.3.0.0/24

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

400	Bastion	10.4.0.0/24
500	SOC	10.5.0.0/24
600	Proxmox	10.6.0.0/24
700	VPN utilisateurs	10.7.0.0/24
800	VPN administrateurs	10.8.0.0/24

PRESNTATION DES SOLUTIONS TECHNIQUES RESEAU ET SYSTEME

SOLUTION DE DESIGN D'INFRASTRUCTURE RESEAU

Afin de concevoir notre réseau de manière virtuelle, nous devions choisir une solution fiable, peu coûteuse et simple de prise en main.

Nous avions le choix entre Eve-NG et GNS3. Puisqu'aucun membre de l'équipe ne savait manipuler l'une de ces solutions, nous n'avions pas de préférence.

Cependant, nous avions à notre disposition des images GNS3 pour configurer des routeurs, des commutateurs etc.

C'est pourquoi nous avons choisi GNS3 comme logiciel pour réaliser le projet.



SOLUTION D'INFRASTRUCTURE SYSTEME

Le cahier des charges ayant fixé plusieurs besoins (serveur web, service de partage de fichiers, service de monitoring etc.), nous avions plusieurs services nécessitant un environnement Windows ou Linux.

C'est pourquoi nous avons décidé d'utiliser une solution hybride qui mélange des serveurs Windows et Linux selon les services.

Ce choix semblait évident d'un point de vue optimisation des ressources ainsi que de simplicité pour certains services.

Par exemple, le service d'annuaire est beaucoup plus complet et simple d'administration avec Active Directory dans un environnement Windows.

Cependant, un serveur Linux est beaucoup plus léger, sécurisé et efficient pour l'hébergement du serveur web.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

À noter que pour les serveurs Windows, nous avons utilisé Windows Server 2016 pour sa robustesse. Quant aux serveurs Linux, nous avons choisi Debian pour sa fiabilité ainsi que sa facilité d'administration.

À noter que les serveurs seront protégés par une solution de chiffrement tel que Bitlocker pour Windows et LUKS pour Linux.

SOLUTION DE SUPERVISION

Pour la supervision, nous avons choisi Zabbix qui est open source et populaire. De ce fait, nous savions que nous trouvons beaucoup de ressources et documentation en ligne. De plus, il est entièrement gratuit, ce qui lui apporte un argument supplémentaire contrairement à d'autres solutions comme SolarWinds.



SOLUTION DE MICROSOC

La mise en place d'un micro-soc en interne nécessitait l'installation d'une solution fiable, légère et utilisable par le pôle informatique de l'assurance puisqu'ils en seront les administrateurs principaux. Nous nous sommes donc penchés sur Wazuh, un EDR open source répondant à tous ces besoins. Un agent a été déployé sur tous les postes, tous les serveurs et tous les routeurs du projet. Nous aurions pu utiliser d'autres solutions telles qu'ESET Inspect qui coûte 2325€ hors taxe par an ce qui ne semblait pas raisonnable pour le projet et la taille de l'office.

En parallèle des EDR, nous installerons un SIEM Graylog pour pouvoir pousser le niveau d'analyse des investigations et centraliser les logs. Pour la partie alerting nous allons utiliser DFIR IRIS qui est open source et qui intègre parfaitement les alertes Graylog. Pour détecter les attaques et faire perdre du temps aux attaquants, nous avons décidé d'intégrer également un honeypot de type T-POT car celui-ci couvre un grand nombre de protocoles et apporte une interface simple pour gérer ses honeypots. La dernière solution que nous avons voulu mettre en œuvre dans le SOC est un lab de purple teaming afin qu'une équipe ait la capacité de tester le SOC, de générer des rapports et automatiser les process pour une amélioration continue. Nous avons choisi PurpleOps pour son interface intuitive et sa possibilité de personnaliser les rapports.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

wazuh.

The Open Source Security Platform

SOLUTION DE VIRTUALISATION

En plus de GNS3, il fallait un hyperviseur à des fins d'infrastructure résiliente grâce aux clusters, ainsi que d'économie de ressources matérielles pour les serveurs.

Un membre de l'équipe était déjà familiarisé avec Proxmox qui est une solution gratuite, complète et fiable.

Il répond à toutes les exigences d'infrastructures qui sont posées comme la haute disponibilité, la gestion des VLANs, un système de sauvegarde avec PBS, une simplicité de gestion et d'administration ainsi que d'automatisation puisqu'il fonctionne sur un serveur Linux.

Les autres solutions du marché qui ont été étudiées sont VmWare ESXI et Hyper V.

Cependant, elles ne sont pas gratuites et ne semblaient pas spécialement plus intéressantes en termes de fonctionnalité pour le projet par rapport à Proxmox.



SOLUTION DE SECURITE RESEAU

Le projet étant axé sur la mise en place d'un réseau sécurisé, il fallait installer des outils efficaces pour filtrer et protéger le trafic.

Pour cela, nous avons utilisé OPNsense qui est une solution open source de pare-feu.

Il supporte la mise en place d'IPS/IDS, de VPN dans divers protocoles, ainsi qu'une configuration fine des règles de pare-feu et des VLANs.

Pour les switchs nous utiliserons des produits Cisco pour leur modularité et leur sécurité.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



OPNsense®
Securing networks made easy

SOLUTION WEB

Pour le serveur web, nous avons utilisé trois machines virtuelles Debian situées en DMZ.

Le serveur web python est déployé à l'aide d'un cluster Docker Swarm ce qui permet une répartition automatique de la charge.

De plus, Docker apporte une flexibilité qui pourrait permettre une migration simplifiée pour les administrateurs à l'avenir.

La DMZ protège les utilisateurs car celle-ci est complètement isolée des autres réseaux.

Ce qui signifie que même en cas de compromission du serveur web, un acteur malveillant serait dans l'incapacité de pivoter sur les autres réseaux et d'accéder à d'autres ressources.

Pour le serveur web nous aurions pu déployer un serveur Apache ou Nginx sans passer par docker avec l'utilisation d'haproxy pour la répartition de charge.

Cependant, il s'agirait d'une solution plus coûteuse en ressources et moins modulable.

Le développeur de l'équipe étant à l'aise avec Python et Postgresql, nous travaillerons avec ces solutions pour le projet.

De plus, nous mettrons en place un WAF avec Bunkerweb, une solution open source clé en main et déployable avec Docker.



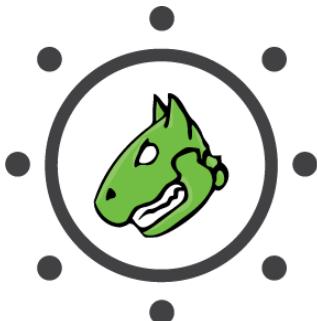
SOLUTION D'ANALYSE DE VULNERABILITÉ

Pour l'analyse de vulnérabilité nous avons trouvé des solutions de type scanner comme OpenVAS.

Ce type de solution permet de scanner certaines CVE les plus connues de manière automatisée ce qui couvre une bonne surface d'attaque.

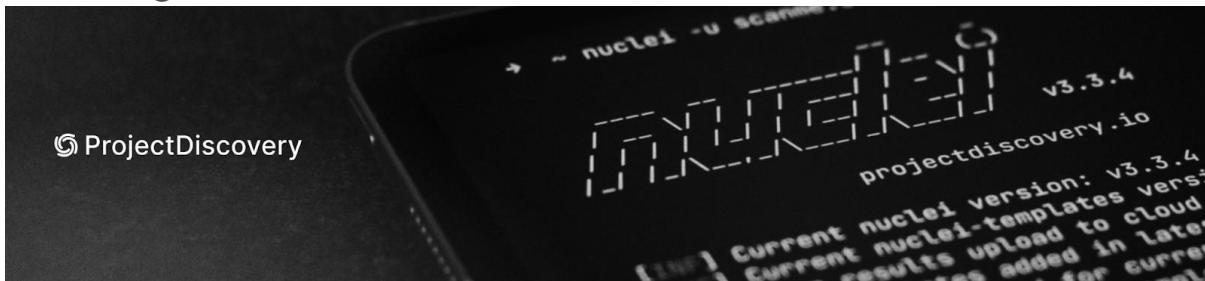
Cependant, nous voulions aller plus loin en utilisant une deuxième solution pour compléter la première avec Nuclei qui est un scanner qui se base sur des templates pour scanner un hôte et permet donc d'identifier un panel de vulnérabilité qui est bien plus large et varié.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



OpenVAS

Open Vulnerability Assessment Scanner



SOLUTION DE SSO

Afin de sécuriser et simplifier les accès à nos applications, nous avons mis en place Keycloak, qui est une solution open source et très réputée pour sa robustesse.

Ce type d'application permet un accès unique et sécurisé aux applications de l'infrastructure, ce qui améliore grandement le niveau de sécurité global du SI.



SOLUTION DE TRANSFERT DE SECRETS

Afin de communiquer des secrets entre les collaborateurs voire avec l'extérieur dans certains cas particulier, nous avons choisi de mettre en place PrivateBin qui propose une interface web pour créer des liens partageables avec des mots de passe et des informations sensibles. Une politique peut être définie pour l'expiration des liens et répond de manière sécurisée à une véritable problématique de partage de secret sur le réseau.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



SECURISATION ET RESILIENCE DE LA SOLUTION :

1. GESTION DES IDENTITES ET ACCES SECURISES

Keycloak (pour les applications web internes)

- Solution open-source de SSO (Single Sign-On) avec support natif d'OpenID Connect : Le **SSO** permet à un utilisateur de s'authentifier une seule fois pour accéder à plusieurs applications ou services de façon sécurisée sans avoir à ressaisir ses identifiants à chaque fois. Les mots de passe sont moins souvent saisis et donc moins exposés. **OpenID Connect** est un protocole d'authentification moderne basé sur OAuth 2.0 largement utilisé pour les applications web modernes.
- Centralisation des identités via intégration LDAP/Active Directory : L'outil peut fédérer plusieurs serveurs AD, synchroniser les utilisateurs et les groupes, et valider les mots de passe directement auprès de l'annuaire vu qu'ils seront stockés dans l'AD directement et non dans Keycloak, garantissant la centralisation de la gestion des identités.

Teleport (pour les connexions aux machines du réseau)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Bastion agit comme un proxy en se mettant entre l'utilisateur et la ressource pour sécuriser l'accès à la ressource. On va pouvoir centraliser l'accès aux ressources, gérer les utilisateurs/groupes, mettre en place des sécurités supplémentaires comme le SSO et la 2FA.
- Bastion moderne avec audit des sessions (enregistrement vidéo SSH/RDP) : Enregistrement vidéo SSH/RDP Teleport capture l'intégralité des sessions via un enregistrement vidéo interactif (format .session). Chaque action (commandes, déplacements souris RDP) est indexée et rejouable

2. PROTECTION DE L'INFRASTRUCTURE RESEAU

Pare-feu (Opsense) et DPI

Un pare feu couvrant les couches 3 à 7 est indispensable car il permet une protection contre les menaces très populaires ces derniers temps : ransomwares, exfiltration de données. **Couplé avec DPI, nous obtenons** une visibilité et un contrôle avancés sur tout le trafic applicatif du réseau, permettant une sécurité renforcée et une gestion optimisée des ressources réseau.

- Inspection approfondie L7 avec DPI (détection de malwares dans les flux SSL) : **C'est sur la couche 7 (couche applicative)** du modèle OSI que transitent les données des applications (web, messagerie, VoIP, etc.). C'est pourquoi il est impératif d'avoir un pare-feu qui fonctionne en L7, capable d'analyser le contenu du trafic jusqu'au niveau des applications, et pas seulement les adresses IP ou les ports utilisés.

DPI (*Deep Packet Inspection*, ou inspection approfondie des paquets) est une technologie qui permet d'analyser en profondeur non seulement l'en-tête, mais aussi le contenu des paquets de données qui circulent sur le réseau. Contrairement au filtrage traditionnel qui se limite à l'en-tête, le DPI va inspecter la charge utile (payload) pour identifier précisément l'application, le type de données, la présence de malwares ou de comportements suspects, même si le trafic est chiffré (SSL/TLS)

Ainsi, un pare-feu L7 avec DPI permet :

- **D'identifier et contrôler les applications utilisées sur le réseau, même si elles utilisent le même port (ex : distinguer YouTube de Google Drive sur le port 443).**
- **De détecter et bloquer des malwares, tentatives de phishing ou autres menaces cachées dans le trafic applicatif, y compris dans les flux chiffrés**
- **D'appliquer des politiques de sécurité très fines selon l'application, l'utilisateur, ou le contenu (ex : autoriser la messagerie mais bloquer le transfert de fichiers).**
- **De prioriser certains flux critiques (VoIP, visioconférence) pour garantir la qualité de service**

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

3. SUPERVISION HARDWARE

Supervision unifiée (AJOUTER SCHEMA RESILIENCE HARDWARE)

Corrélation logs/métriques via Prometheus/Loki

La supervision unifiée repose sur l'intégration de Prometheus (pour la collecte de métriques) et Loki (pour l'agrégation de logs), visualisés et corrélés dans Grafana.

- **Prometheus** collecte des métriques temps réel : CPU, mémoire, latence applicative, taux d'erreur, etc.
- **Loki** centralise les logs applicatifs, système et réseau, en les indexant par labels (namespace, pod, service, etc.) pour une recherche rapide et efficace
- **Grafana** permet de créer des dashboards combinant métriques et logs.
- En cas d'incident, l'opérateur repère un pic d'erreur dans les métriques Prometheus, puis bascule sur les logs Loki du même intervalle pour identifier la cause racine, ce qui accélère le diagnostic et la résolution

Alertes SMART prédictives sur le matériel

Les alertes SMART (Self-Monitoring, Analysis, and Reporting Technology) permettent d'anticiper les défaillances matérielles, notamment des disques durs et SSD.

- **Intégration avec Prometheus** : des exporters SMART collectent les données de santé des disques (température, erreurs de lecture, taux de réallocation de secteurs, etc.) et exposent ces métriques à Prometheus.
- **Alerting prédictif** : des règles d'alerte sont définies (par exemple, augmentation du taux d'erreurs ou dépassement de seuils critiques) pour déclencher des notifications avant qu'une panne ne survienne.
- Ces alertes sont visualisées dans Grafana et peuvent être transmises à des outils de gestion d'incidents (mail, Slack, ticketing).

Conformité RGPD/ISO 27001

La supervision unifiée, grâce à Prometheus, Loki et Grafana, permet de corrélérer efficacement logs et métriques pour une détection rapide des incidents, d'anticiper les pannes matérielles via des alertes SMART, et de piloter la conformité RGPD/ISO 27001 grâce à des dashboards adaptés et des capacités d'audit renforcées. Elle contribue à la conformité réglementaire en offrant une visibilité centralisée sur la sécurité et la disponibilité des systèmes :

- **RGPD** :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Les dashboards permettent de tracer les accès aux données personnelles, les incidents de sécurité, et de documenter les mesures de protection mises en œuvre (contrôles d'accès, chiffrement, etc.)
- Ils facilitent la tenue de registres d'activités et la génération de rapports pour les audits.
- ISO 27001 :
 - Les dashboards regroupent les indicateurs clés du SMSI (Système de Management de la Sécurité de l'Information) : taux d'incidents, conformité des sauvegardes, état des correctifs, etc
 - Ils assurent une documentation continue et une preuve d'auditabilité, essentielle pour démontrer la conformité lors des contrôles internes ou externes.

4. PROTECTION DES DONNEES SENSIBLES

1. RESILIENCE OPERATIONNELLE

Architecture redondante :

Basculement automatique (Fail-over) : Mise en place d'un système de basculement qui permet à un équipement secondaire de prendre automatiquement le relais en cas de défaillance du système primaire, garantissant ainsi la continuité des services sans intervention humaine.

Redondance active avec détection de pannes : Cette approche de redondance détecte les pannes et transfère automatiquement la charge du composant défaillant vers un composant fonctionnel. Cette méthode permet non seulement d'assurer la continuité du service, mais aussi d'identifier rapidement les équipements nécessitant une maintenance.

Infrastructure électrique sécurisée :

Alimentation électrique redondante : Déploiement de sources d'alimentation multiples et indépendantes pour tous les équipements critiques, éliminant ainsi le risque de point unique de défaillance électrique.

Groupes électrogènes de secours : Installation de générateurs capables de prendre le relais instantanément en cas de coupure du réseau électrique principal, assurant une autonomie suffisante pour maintenir les

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

opérations jusqu'au rétablissement de l'alimentation standard.

Onduleurs : Mise en place d'onduleurs et de batteries de secours qui fournissent une alimentation temporaire pendant la transition vers les générateurs, éliminant tout risque de micro-coupures pouvant affecter les équipements sensibles.

Redondance réseau multi-niveaux :

Équipements réseau dupliqués : Déploiement de routeurs, commutateurs et pare-feux en configuration redondante (N+1 ou N+N selon la criticité), permettant une disponibilité continue des services réseau malgré la défaillance d'un équipement.

Load-balancing actif/actif : Utilisation de répartiteurs de charge configurés en mode actif/actif pour distribuer le trafic entre plusieurs serveurs, optimisant ainsi les performances tout en offrant une redondance naturelle.

5. PROTECTION DES DONNEES SENSIBLES

Chiffrement

Le chiffrement AES-256-GCM avec rotation régulière des clés protège efficacement les données stockées contre tout accès non autorisé.

Données au repos : AES-256-GCM avec rotation hebdomadaire des clés

- AES-256-GCM (Advanced Encryption Standard, 256 bits, mode Galois/Counter Mode) est l'algorithme de référence pour le chiffrement des données stockées sur disque ou sauvegardées.
- Ce mode assure à la fois la confidentialité et l'intégrité des données grâce à l'authentification intégrée (GCM).

Données en transit : TLS 1.3 avec courbes elliptiques X25519

TLS 1.3/X25519 permet de sécuriser les échanges réseau.

- TLS 1.3 est la dernière version du protocole de sécurisation des échanges réseau, offrant des performances accrues et une sécurité renforcée par rapport à TLS 1.2
- Les échanges de clés utilisent la courbe elliptique X25519, garantissant une confidentialité persistante (Perfect Forward Secrecy) et une résistance aux attaques modernes

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- TLS 1.3 simplifie les suites cryptographiques, élimine les algorithmes faibles et chiffre l'intégralité des échanges dès le début de la connexion, réduisant fortement les risques d'interception ou de manipulation des données en transit

Partage sécurisé

Pour le partage ponctuel d'informations sensibles, PrivateBin garantit la confidentialité totale grâce au chiffrement côté client et à l'auto-destruction des messages, réduisant drastiquement les risques de fuite ou de compromission.

- PrivateBin est une solution open source de partage sécurisé où tout le chiffrement/déchiffrement se fait dans le navigateur de l'utilisateur, avant l'envoi sur le serveur
- Le serveur ne reçoit que des données chiffrées (AES-256-GCM), ce qui signifie qu'il n'a aucune connaissance du contenu partagé
- Auto-destruction :
 - L'option "burn after reading" permet de supprimer automatiquement le message après la première consultation, empêchant toute relecture ultérieure
- Fonctionnalités complémentaires :
 - Possibilité de protéger le partage par mot de passe, ajoutant une couche de sécurité supplémentaire
 - Aucun compte requis, pas de stockage de métadonnées ou d'IP utilisateur, ce qui limite la surface d'attaque et respecte la confidentialité
 - Solution adaptée au partage de mots de passe, d'informations sensibles ou de documents confidentiels sans risque d'exposition accidentelle.

6. MONITORING/SOC - ARCHITECTURE UNIFIEE

Wazuh : Collecte et détection avancée (Open-source)

Rôle : Agent XDR multi-plateforme pour la surveillance temps réel des endpoints.

- Détection des menaces et des intrusions : L'outil est capable de détecter en temps réel les comportements suspects, les attaques, les malwares, les rootkits ou les anomalies sur les serveurs, postes de travail, environnements cloud ou conteneurs

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Surveillance de l'intégrité : Il surveille les modifications de fichiers et de configurations critiques, permettant de détecter rapidement toute altération non autorisée ou potentiellement malveillante
- Collecte des logs : Wazuh collecte, centralise et corrèle les logs issus de multiples sources (systèmes, équipements réseau, cloud), offrant une visibilité complète sur l'activité de l'infrastructure
- Création de règles de détections
- Réponse aux incidents : Wazuh permet d'automatiser des actions de réponse (blocage d'IP, arrêt de processus, alertes) dès qu'une menace est détectée, réduisant ainsi le temps de réaction
- Conformité réglementaire : Il aide les organisations à répondre aux exigences de conformité (RGPD, ISO 27001, HIPAA...) grâce à ses capacités d'audit, de reporting et de surveillance continue

Règles de détection :

- Base de 10k+ règles préconfigurées (MITRE ATT&CK mappé)
- Syntaxe XML avec conditions complexes

Graylog : Centralisation et analyse avancée des logs

Rôle : Plateforme SIEM open source conçue pour la collecte, l'analyse et la corrélation de logs à grande échelle, optimisant la détection de menaces et la conformité.

1. Couverture des menaces alignée sur MITRE ATT&CK

Fonctionnalités clés :

- **Graylog Illuminate** : Bibliothèque de *content packs* préconfigurés pour des cas d'usage spécifiques (RGPD, NIST)
- **Threat Coverage Widget** : Visualisation des détections actives mappées sur la matrice MITRE ATT&CK, identifiant les lacunes de couverture
- **Détection contextuelle** : Alerte sur les menaces prioritaires en fonction du profil de risque de l'organisation (secteur d'activité, actifs critiques)

2. Gestion optimisée des données

Avantages :

- **Réduction de 60% des coûts de stockage via le *smart routing***
- **Conservation des logs bruts pour investigations forensiques, sans surcoût.**

3. Intégrations et automatisations

Écosystème technique :

- **Wazuh** : Envoi des alertes vers Graylog via Syslog/TLS pour corrélation avec les logs réseau
- **SocFortress** : Alimentation en IOC via API REST (mise à jour horaire des feeds de menaces)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- DFIR IRIS : Déclenchement automatique de playbooks depuis les alertes Graylog

4. Conformité et reporting

Fonctionnalités RGPD/ISO 27001 :

- Dashboard d'audit : Suivi en temps réel des indicateurs :
 - Nombre d'accès aux données personnelles
 - Délai moyen de suppression des logs
 - % de données chiffrées en transit/au repos
- Rapports générés par IA : Synthèse automatique des incidents pour les audits, avec preuves d'action

DFIR IRIS : Plateforme collaborative de gestion et réponse aux incidents

Rôle : DFIR IRIS (Incident Response Information Sharing) est une plateforme open source dédiée à la gestion, la documentation et la coordination des réponses aux incidents de sécurité. Elle permet aux analystes SOC, équipes de réponse à incident et investigateurs de centraliser, structurer et suivre l'ensemble du cycle de vie d'un incident, du signalement initial jusqu'à la résolution et au reporting

Fonctionnalités principales

- Gestion complète du cycle de vie des incidents
IRIS permet de gérer simultanément plusieurs incidents ou enquêtes, de suivre leur avancement, d'assigner des tâches aux membres de l'équipe, et de documenter chaque étape dans un format structuré et consultable. Chaque incident est traité comme un "case" avec sa propre timeline, ses preuves, ses IoC (indicateurs de compromission) et ses décisions stratégiques
- Collaboration en temps réel
Plusieurs analystes peuvent travailler sur le même incident, partager des notes, observations, hypothèses et décisions dans une interface collaborative. Cette approche accélère la prise de décision et améliore la coordination, même pour des équipes réparties ou en télétravail
- Gestion et préservation des preuves
DFIR IRIS centralise la collecte, la conservation et l'analyse des preuves numériques (fichiers, images disques, logs, captures réseau, etc.), tout en assurant la traçabilité et l'intégrité nécessaires pour des investigations internes ou des procédures légales
- Alerting intégré
IRIS reçoit automatiquement des alertes issues du SIEM (comme Graylog ou Wazuh) ou d'autres sources de confiance. Les analystes peuvent rapidement trier, annoter, corrélérer et transformer ces alertes en cas d'incident complets, facilitant ainsi la gestion des priorités et la réactivité

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- **Intégrations et automatisations**

La plateforme propose des modules d'intégration natifs avec des outils comme VirusTotal, MISP, IntelOwl, ou des webhooks personnalisés, permettant l'enrichissement automatique des IoC, la récupération d'informations contextuelles et l'automatisation de certaines tâches d'investigation

- **Reporting et conformité**

IRIS génère automatiquement des rapports détaillés et personnalisables pour chaque incident, facilitant la communication avec les parties prenantes et la documentation pour la conformité réglementaire (ISO 27001, RGPD, etc.)

Copilot (SocFortress) : Orchestration de la sécurité et Threat Intelligence centralisée

Rôle : Copilot est une plateforme de sécurité collaborative qui agit comme une “tour de contrôle” pour le SOC. L'outil s'interface nativement avec les outils Wazuh, Graylog, DFIR IRIS, et d'autres, pour offrir une visibilité et une coordination optimales sur l'ensemble du dispositif de cybersécurité.

Fonctionnalités principales

- **Centralisation des alertes et des incidents :** SocFortress agrège en temps réel les alertes provenant de multiples sources (SIEM, EDR, IDS, outils cloud...), les corrèle et les priorise selon la criticité, la nature de la menace et le contexte métier. Cela permet de réduire le bruit (faux positifs) et de concentrer les efforts sur les incidents réellement importants.
- **Threat Intelligence as a Service :** La plateforme intègre et met à jour automatiquement des flux d'indicateurs de compromission (IoC) issus de sources publiques et privées (MISP, AlienVault, OpenCTI, etc.). Ces IoC sont utilisés pour enrichir les alertes, accélérer la détection des menaces émergentes et automatiser la mise en quarantaine ou le blocage d'entités malveillantes.
- **Gestion collaborative des incidents :** La plateforme facilite la collaboration entre analystes SOC, RSSI et métiers : suivi des tâches, partage de notes, gestion des escalades, documentation centralisée des décisions et des actions entreprises.
- **Tableaux de bord conformité et reporting :** SocFortress propose des dashboards dédiés à la conformité (RGPD, ISO 27001...) : suivi des incidents, des accès, des mesures correctives, génération de rapports pour les audits internes ou externes.

PLAN DE CONTINUITÉ D'ACTIVITÉ (PCA) – TOURISK ASSURANCE

1. OBJECTIF DU PCA

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Garantir la continuité des services de Tourisk, minimiser l'impact sur les clients, les opérations et la conformité légale.

2. PORTEE DU PCA

Ce PCA couvre les services suivants :

- Souscription et gestion des contrats (santé, auto, habitation, voyage)
- Traitement des sinistres
- Support client
- Infrastructure IT (Proxmox, S3)
- Cybersécurité

3. ANALYSE D'IMPACT METIER (BIA)

Processus critique	Impact si indisponible	RTO (durée max arrêt toléré)	RPO (perte de données max tolérée)
Accès aux données clients	Très Élevé	2h	30 min
Traitement des sinistres	Élevé	4h	1h
Services en ligne (portail client)	Élevé	3h	1h
Communication	Moyen	6h	4h

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

interne/externe			
Paiement des indemnités	Moyen	1 jour	4h

Cette évaluation ne contient pas de réelle donnée concernant les pertes financières.

4. SCÉNARIOS IDENTIFIÉS

4.1 – PETITE CATASTROPHES NATURELLES ET INCIDENTS LOCAUX FAIBLE

- Inondation, incendie partielle des locaux
- Plan de relocalisation partielle ou télétravail immédiat

4.2 – DÉFAILLANCE IT

- Panne serveur Proxmox
- Coupure d'électricité
- Perte d'accès internet (une ligne uniquement)
Disque dur qui lâche
- Corruption ou perte de données

4.3 – CYBERMENACES

- Ransomware
- Fuite ou vol de données sensibles
- Compromission des identifiants de connexion

5. PLANS DE REPONSE

5.1 – INCIDENT PROXMOX (INFRASTRUCTURE LOCALE)

- **Supervision 24/7**

Utilisation d'un outil Zabbix pour vérifier les métriques des serveurs.

- **Backups réguliers des VM**

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

L'utilisation de Proxmox Backup serveur permet de réaliser des sauvegardes des VM(s) et de rapidement les restaurer. Une sauvegarde sur un bucket Amazon S3 dans le cloud et une sauvegarde hebdomadaire via un disque USB.

- **Continuité des services avec 3 Noeuds Proxmox permettant d'avoir de la haute disponibilité.**

Permet d'assurer une haute disponibilité sur les serveurs internes de l'entreprise.

5.2 – PERTE DE CONNECTIVITÉ

- **Redondance internet (fournisseur secondaire actif-passif)**

Permet en cas de panne internet d'un fournisseur de basculer automatiquement sur l'autre en ne rencontrant aucune coupure. Le choix d'actif passif est utilisé généralement moins de coup pour la société.

- **Onduleurs et groupe électrogène**

Permet en cas de coupure d'électricité de ne subir interruption l'onduleur et dans un second temps la prise du relais par le groupe électrogène permet d'avoir une durée d'approvisionnement en électricité plus longue. (Cette notion entre aussi dans le PRA)

- **Possibilité de télétravail activée immédiatement**

Télétravail pour les employés possibles.

5.3 – FUITE OU VOL DE DONNEES

- **Audit des accès via logs SIEM**

Permet aux équipes techniques de réaliser une investigation précise de l'événement afin de d'identifier les sources et réaliser des analyses Forensiques si nécessaire

- **Communication aux autorités (CNIL / RGPD)**
- **Plan de rotation des mots de passe**

Les employés ont pour recommandation de renouveler leur mot de passe tous les 3 mois pour les applications qu'ils utilisent. De plus, une rotation automatique des mots de passe administrateur. Pour de potentielles informations supplémentaires concernant les recommandations se référer au guide des mots de passe entreprise (Annexe 2 - PCA).

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

5.4 – INACCESSIBILITE LOCALE

- **Services cloud critiques accessibles à distance**

Le site internet accessible pour les clients est dans le cloud sur une instance EC2. Ce qui permet d'avoir un accès permanent en cas d'un événement rendant le site inaccessible pour les employés.

5.5 – APPLICATION WEB

- **Risques d'attaques DOS/DDOS**

Utilisation d'un Load Balancer sur 3 VPS pour assurer la disponibilité des applications et soutenir la charge.

- **Sauvegarde des bases**

Protection contre une potentielle corruption d'une base avec un sauvegarde régulière. Continuité d'activité pour les bases de données avec backup et restauration.

6. TESTS ET MAINTENANCE

- **Test PCA (simulation incident mineur) → Minimum 4 / an**

Ce test permet d'évaluer le niveau d'infrastructure du SI et sa capacité continué de fonctionner en cas d'incident mineur. Il ne faut pas le confondre avec un test dans le PRA. Un test avec une coupure d'une ligne d'un fournisseur et donc une coupure internet peuvent être des exemples d'incident mineur étant donné que l'entreprise possède plusieurs lien internet différents

- **Vérification des sauvegardes chaque semaine**

La vérification des sauvegardes permet de vérifier l'intégrité des sauvegardes pour une potentielle remise en service d'un backup.

- **Audit des plans d'accès / VPN chaque trimestre**

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Un audit de sécurité accès Black box et intrusion physique annuel permet de vérifier le bon fonctionnement des mesures d'accès physique.

- **Mise à jour du PCA tous les 6 mois ou après chaque incident**

Réévaluation du document pour mettre en place les nouvelles recommandations ou adapter le fonctionnement de la continuité d'activité en fonction des besoins

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

PLAN DE REPRISE D'ACTIVITE (PRA) - TOURISK ASSURANCE

1. CONTEXTE ET OBJECTIFS STRATEGIQUES

1.1 PERIMETRE DU PRA

Systèmes couverts	RTO	RPO	Priorité
Bases de données clients	1h	10 min	Critique
Portail web (Apache/Nginx)	45 min	5 min	Haute
Services d'authentification	30 min	0	Urgent

1.2 ARCHITECTURE HYBRIDE

[Cluster Proxmox HA (3 nœuds + 1 qdevice)]

- |
 - └ Stockage Ceph (3 réplicas) → 40 To utilisés / 100 To
 - └ PBS Local (VLAN 600) → RAID-Z2 + 500 snapshots
 - └ PBS Cloud (AWS S3) → Immutability + réplication cross-region

2. SCENARIOS DE RISQUE ÉTENDUS

2.1 CYBERATTAQUE DE TYPE RANSOMWARE

Détection :

- Alerte CrowdStrike Falcon sur comportement anormal (exfiltration de données)
- Zabbix : CPU à 100% sur VM "AD-Primary"

Procédure :

1. Isolement réseau via ACL sur switch Cisco (port shutdown)
2. Bascule vers AD de secours dans Azure

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Restauration depuis PBS Cloud en mode *air-gapped*

Air-grapped (la séparation des données de sauvegarde de tout réseau accessible au public, en créant un « mur d'air » entre les données et tout point d'accès susceptible d'être vulnérable aux pirates informatiques) :

```
3. proxmox-backup-client restore --repository cloud-  
pbs@tls:backup.tourisk.com --snapshot latest --verify --keyfile  
/mnt/usb/keyfile.key
```

Checklist :

- Vérifier l'absence de backdoors via
- Réinitialiser tous les tokens Kerberos

2.2 PANNE ÉLECTRIQUE PROLONGEE (72H+)

Déclenchement :

- Onduleurs (APC Smart-UPS 3000VA) → autonomie 2h
- Groupe électrogène diesel (200 kVA) → démarrage automatique

Procédure :

1. Arrêt contrôlé des VMs non critiques via script Ansible
2. Migration des VMs critiques vers AWS avec `proxmox-aws-migrate-tool`
3. Surveillance température data center via capteurs IoT LoRaWAN

2.3 DOUBLE COUPURE INTERNET (BOX 1 + 2)

Solution :

- Activation lien de secours 4G/5G (routeur MikroTik LTE)

Reconfiguration BGP via script Python :

```
from nornir import InitNornir

nr = InitNornir(config_file="config.yaml")
• nr.run(task=update_bgp, new_path="4G-backup")
```

KPI :

- Temps de basculement ≤ 8 minutes (SLA opérateur)

3. PERFORMANCES PBS : TABLEAUX DE REFERENCE

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

3.1 TEMPS DE RESTAURATION PAR TYPE DE VM

Taille VM	Stockage Source	Débit Réseau	Temps Restauration
50 Go (HDD)	PBS Local	1 Gbps	12 min
500 Go (SSD)	PBS Cloud	10 Gbps	25 min
2 To (NVMe)	RAID 10	25 Gbps	48 min

L'infrastructure complète de Tourisk pourrait prendre une demi-journée de restauration

3.2 FACTEURS D'OPTIMISATION

- **Compression LZ4** : Gain 35% sur temps de transfert
- **Déduplication** : Jusqu'à 60% d'espace sauvegardé
- **Parallel Restore** : Activer avec `--workers 8` (Proxmox 8.2+)

4. PROCEDURES OPERATIONNELLES DETAILLEES

4.1 RECONSTRUCTION COMPLETE DU CLUSTER

Étapes :

Désactivation manuelle du quorum :

```
1. pvecm expected 1 && systemctl stop pve-cluster
```

Téléchargement du dernier état Ceph depuis S3 :

```
2. aws s3 sync s3://tourisk-ceph-backup /ceph_backup --include "*$(date +%Y-%m-%d) *"
```

Redémarrage des services :

```
3. systemctl start ceph-mon@node1 && ceph orch apply -i spec.yml
```

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

5. ANNEXES TECHNIQUES (EXTRAITS)

ANNEXE A : SCRIPTS D'URGENCE

Bascule vers PBS Cloud :

```
#!/bin/bash

# Variables

PBS_REPO="cloud-pbs@tls:backup.tourisk.com"

VM_LIST="101 102 201"

for VMID in $VM_LIST; do

proxmox-backup-client restore --repository $PBS_REPO $VMID \
--output /var/lib/vz/images/$VMID \
--worker 4 --verbose

Done
```

ANNEXE B : METRIQUES ZABBIX POUR DETECTION

Métrique	Seuil Critique	Action Automatique
vfs.dev.read[dm-0]	> 90% IO delay	Migration VM vers autre nœud
net.if.total[eth0]	< 10 Mbps	Bascule vers eth1

ANNEXE C : DIAGRAMME DE FLUX DE REPRISE

[Incident] → [Détection Zabbix] → [Isolation] → [Restauration PBS]

| └→ [Test Intégrité] → [Monitoring 24h]

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

└─ [Post-Mortem] → [Mise à jour PCA/PRA]

6. VALIDATION ET AMELIORATION CONTINUE

6.1 PROGRAMME DE TESTS

Type de Test	Fréquence	Métrique Cible
Restauration complète cluster	Trimestriel	RTO ≤ 1h15
Cyberattaque simulée	Semestriel	Détection ≤ 15 min
Charge à 200%	Annuel	Latence API < 500 ms

6.2 ROADMAP D'AMELIORATION

- Intégration de Ceph Erasure Coding (économie 40% espace)

Erasure Coding est une méthode de codage de redondance : au lieu de simplement répliquer chaque donnée (comme dans le mode classique à 3 copies, qui triple l'espace nécessaire), Ceph divise chaque objet en plusieurs fragments de données (K), puis ajoute des fragments de parité (M) générés mathématiquement.

Plus le ratio K/M est élevé, plus l'économie d'espace est importante, mais la tolérance aux pannes peut diminuer si M est trop faible.

- Déploiement de Proxmox Backup Server en edge (5 sites)

Déployer Proxmox Backup Server (PBS) en edge sur 5 sites signifie installer et exploiter un serveur de sauvegarde Proxmox dédié dans chacun des sites distants (agences, filiales, points de présence, etc.), afin d'assurer la protection, la résilience et la souveraineté locale des données tout en permettant une synchronisation centralisée et une restauration rapide en cas d'incident.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Automatisation complète via Terraform + Ansible Tower

L'automatisation complète via Terraform + Ansible Tower combine deux outils clés du DevOps pour gérer le cycle de vie de l'infrastructure (provisionnement, configuration, déploiement) de manière centralisée, reproductible et sécurisée.

Documentation Associée :

- PCA Tourisk
- Politique de Sécurité des Données (Art. 12-15) **RGPD**
- Contrat SLA AWS S3 (n°AWS-TOURISK-789456)

(Le contrat SLA AWS S3 (Service Level Agreement, ou Accord de Niveau de Service) est le document officiel qui définit les engagements d'Amazon Web Services concernant la disponibilité et la fiabilité du service de stockage Amazon S3. Ce contrat précise les garanties minimales offertes aux clients, ainsi que les compensations prévues en cas de non-respect de ces engagements.)

Ce PRA inclut tous les éléments nécessaires pour faire face à des scénarios complexes tout en respectant vos contraintes RTO/RPO. Les annexes techniques et scripts opérationnels permettent une mise en œuvre rapide par les équipes IT.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

CAHIER DE RECETTE

REALISATION DES TACHES

Tâches	Avancement (/5)	Solutions et commentaires
Solution d'analyse de faille	5	Le scanner de vulnérabilité Nuclei est correctement mis en place et remonte des alertes sur Iris.
Solution face aux techniques d'audit	4	Des règles de détection sont mises en place sur le SIEM mais il faudrait davantage pour couvrir toute la surface d'attaque. PurpleTeam ok.
Solution de cryptographie	5	Le serveur web est sécurisé avec du HTTPS avec un certificat géré par une PKI.
Solution face aux méthodes d'intrusion physique	3	Un système de contrôle d'accès a été imaginé pour protéger l'entreprise et des plans ont été réalisés.
Solution d'accès aux services de l'entreprise (VPN/DMZ)	5	Le VPN d'entreprise est correctement implémenté et une DMZ est configurée avec un bastion pour la PMAD.
Solution de résilience de la solution système et réseau	5	La haute disponibilité est configurée avec Proxmox et des sauvegardes régulières des VMs sont programmées. Le protocole CARP est en place sur les routeurs pour assurer de la redondance.
Sécurisation des systèmes et des accès au réseau	5	La segmentation des réseaux a été mise en place avec des VLANs et une gestion fine des flux. Un WAF a été mis en place sur le serveur web.
Solution de gestion centralisée de l'authentification et des autorisations	5	Un contrôleur de domaine Active Directory a été mis en place pour l'authentification des utilisateurs.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

		Un serveur SSO Keycloak a également été configuré pour implémenter une authentification centralisée.
Solution de partage des secrets	5	La solution Privatebin a été configurée avec un certificat pour avoir le HTTPS.
Hardening des services clients et/ou collaborateurs basés sur Linux	3	Les configurations des serveurs Windows et Linux ont été durcies.
Solution de supervision	5	Zabbix est configuré pour envoyer des alertes par mail en cas de panne d'un équipement ou d'un service. Grafana est installé avec des dashboards pour surveiller l'activité du parc.
Solution SOC et outils SIEM	5	Un stack complète est configurée pour permettre l'ingestion des logs, l'envoie sur le SIEM, la détection des comportements suspects avec des règles elastalert, de la remédiation automatique avec l'EDR et une plateforme alerting fonctionnelle.

CONCLUSION

Les tâches ont toutes été globalement respectées bien que nous aurions pu travailler davantage sur les protections physiques. Nous ne l'avons pas fait par manque de moyen et de matériel.

La résilience de la solution système et réseau a été testée et s'est montrée efficace et fonctionnelle.

Le SOC a également été testé avec de l'injection de logs malveillant pour tester le bon fonctionnement des règles de détection, du SIEM et de la plateforme d'alerting.

CAHIER D'EXPLOITATION

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

ZABBIX

INSTALLATION

La documentation officielle de zabbix est très complète, il suffit de la suivre pour l'installer, selon vos besoins.

Vous trouverez le lien : <https://www.zabbix.com/download>

Pour ce tutoriel nous prendrons le pack classique complet :



1 Choisissez votre plateforme

VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES	SERVEUR WEB
7.2	Alma Linux	12 Bookworm (amd64, arm64)	Server, Frontend, Agent	MySQL	Apache
7.0 LTS	Amazon Linux	11 Bullseye (amd64)	Server, Frontend, Agent 2	PostgreSQL	Nginx
6.0 LTS	CentOS	-	-	-	-
5.0 LTS	Debian	11 Bullseye (amd64)	Proxy	-	-
7.4 (non-released)	OpenSUSE 15.2	-	-	-	-

L'installation sera faite sous debian 12 avec un serveur de base de données *mysql* et serveur web *apache*.

Suivez le tutoriel jusqu'à la partie **2.c**

c. Create initial database
Make sure you have database server up and running.

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;
```

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Et juste avant cette partie, vous devez installer un serveur de base de données.

Voici les commandes à exécuter :

```
sudo apt install mariadb-server mariadb-client -y  
sudo systemctl start mariadb  
sudo systemctl start zabbix-server
```

Pour vérifier que vos services tournent correctement vous pouvez vérifier à l'aides de ces commandes les status des services :

```
sudo systemctl status mariadb
```

```
sudo systemctl status zabbix-server
```

Dans la même partie du tutoriel, au niveau des commandes de la création de base de donnée, changez le mot "**password**" pour y placer le mot de passe de votre choix

```
# 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;
```

Vous pouvez ensuite continuer le tutoriel normalement.

En fin de tutoriel le zabbix sera accessible sur http://ip_de_votre_machine/zabbix

Vu que vous y accédez pour la première fois vous devez paramétrier l'interface, vous aurez juste à saisir le mot de passe de la base de données et valider tout le reste.

Et enfin les identifiants pour se connecter sont **Admin / zabbix**.

Le reste de la configuration sera disponible en annexe.

GRAFANA

Installation Debian/Ubuntu

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Pour juste une installation basique du grafana OSS, il suffit de se rendre sur la documentation du site officiel qui se trouve ici : <https://grafana.com/docs/grafana/latest/setup-grafana/installation/debian/>.

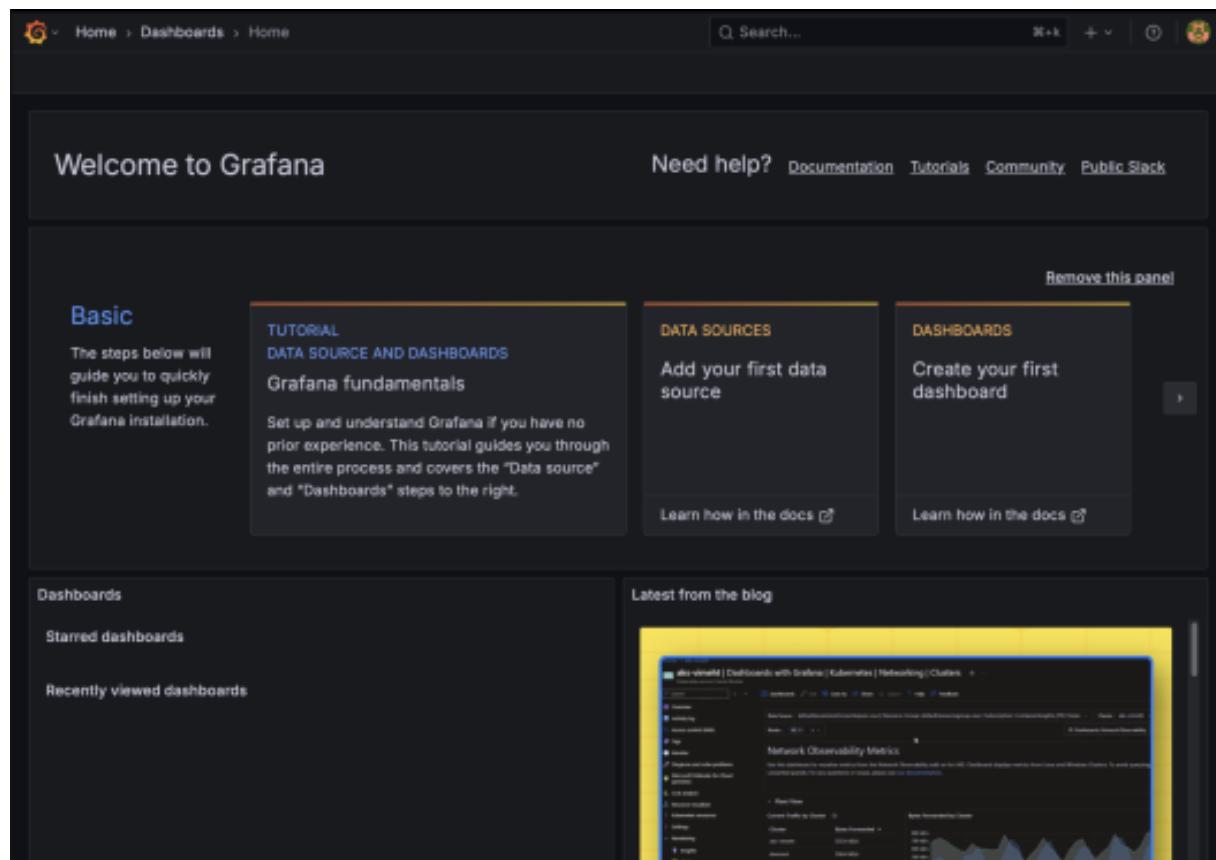
Il y'a une vidéo disponible sur la page aussi si besoin.

À la fin de l'installation ne pas oublier de lancer le serveur avec la commande :

- `systemctl start grafana-server`

Ensuite votre grafana sera accessible sur http://ip_de_votre_machine:3000

Les credentials par défaut sont **admin / admin**.



Le reste de la configuration sera exposé en annexe.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

OPNSENSE



Voici l'interface de OPNSENSE, on retrouve les différentes interfaces, correspondant aux différents Vlan(s). On retrouve plusieurs clients VPN, pour les utilisateurs et les administrateurs. On retrouve la configuration du Master avec les Virutal IP(s) en mode CARP pour de la reprise d'activité.

Le firewall permet d'avoir 6 réseaux différents + 2 VPN différents.

Dans les réseaux, on retrouve :

- Vlan utilisateur : 10.1.0.0/24 (tag100)
- Vlan IT : 10.2.0.0/24 (tag 200)
- Vlan Serveur : 10.3.0.0/24 (tag 300)
- Vlan Serveur : 10.4.0.0/24 (tag 400)
- Vlan SOC : 10.5.0.0/24 (tag 500)
- Vlan Proxmox: 10.6.0.0/24 (tag 600)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Vpn utilisateur : 10.7.0.0/24
- Vpn administrateur : 10.8.0.0/24

Au niveau reprise d'activité, on retrouve un second serveur OPENSENSE slave

The screenshot shows the 'System: High Availability: Status' page. On the left, a sidebar lists various system sections like System, Firewall, and Reporting. The main area displays a table of services with their descriptions and status icons. A search bar and a 'Synchronize and reconfigure all' button are at the bottom.

Service	Description	Status
configd	System Configuration Daemon	●
cron	Cron	●
dhcpgd	DHCPv4 Server	●
dhcpd6	DHCPv6 Server	●
login	Users and Groups	●
ntpd	Network Time Daemon	●
pf	Packet Filter	●

Sur cette capture on retrouve le Status de la haute disponibilité du Pare feu.

The screenshot shows the 'Dashboard' page with two tabs: 'Virtual IPs' and 'Interface'. The 'Virtual IPs' tab displays a table of CARP interfaces with their status (MASTER or BACKUP) and IP addresses. The 'Interface' tab shows interface statistics, traffic graphs, and system logs.

Interface	Status	IP Address
Utilisateur @ VHID 10	MASTER	10.1.0.254 (CARP IP)
IT @ VHID 20	BACKUP	10.2.0.254 (CARP IP)
Serveur @ VHID 30	BACKUP	10.3.0.254 (CARP IP)
Bastion @ VHID 40	BACKUP	10.4.0.254 (CARP IP)
SOC @ VHID 50	BACKUP	10.5.0.254 (CARP IP)

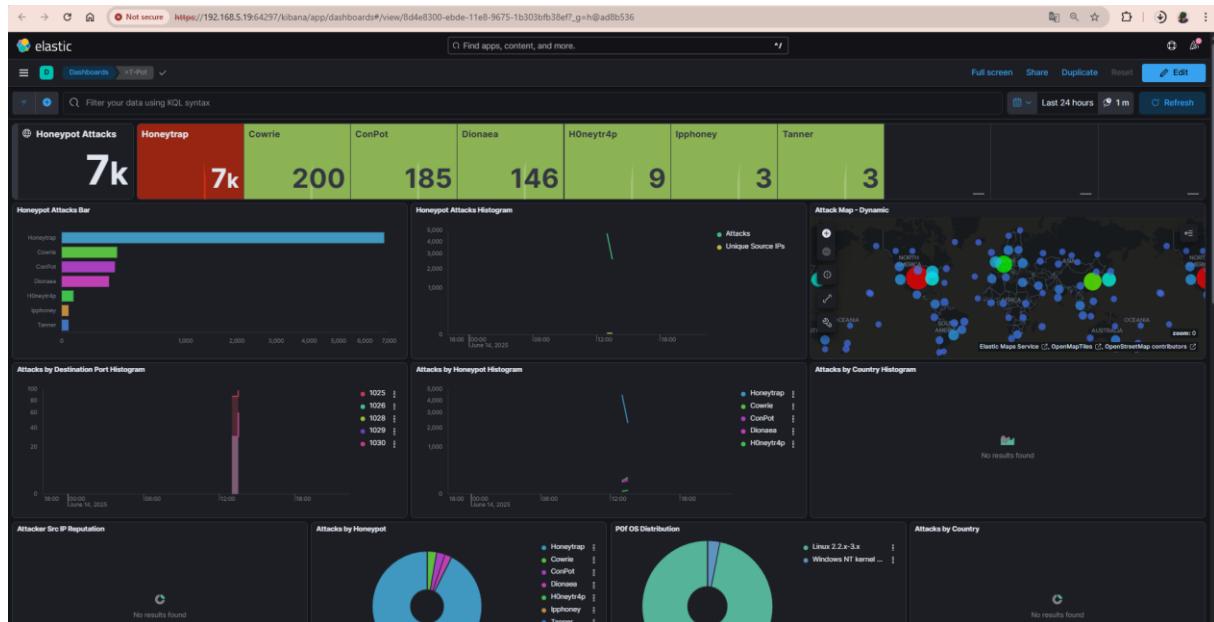
Puis on retrouve les Virtual ips configurer en mode Carp avec Master et backup

Pour l'installation et la configuration de OPENSENSE sur Proxmox, voir annexe Installation de OPENSENSE.

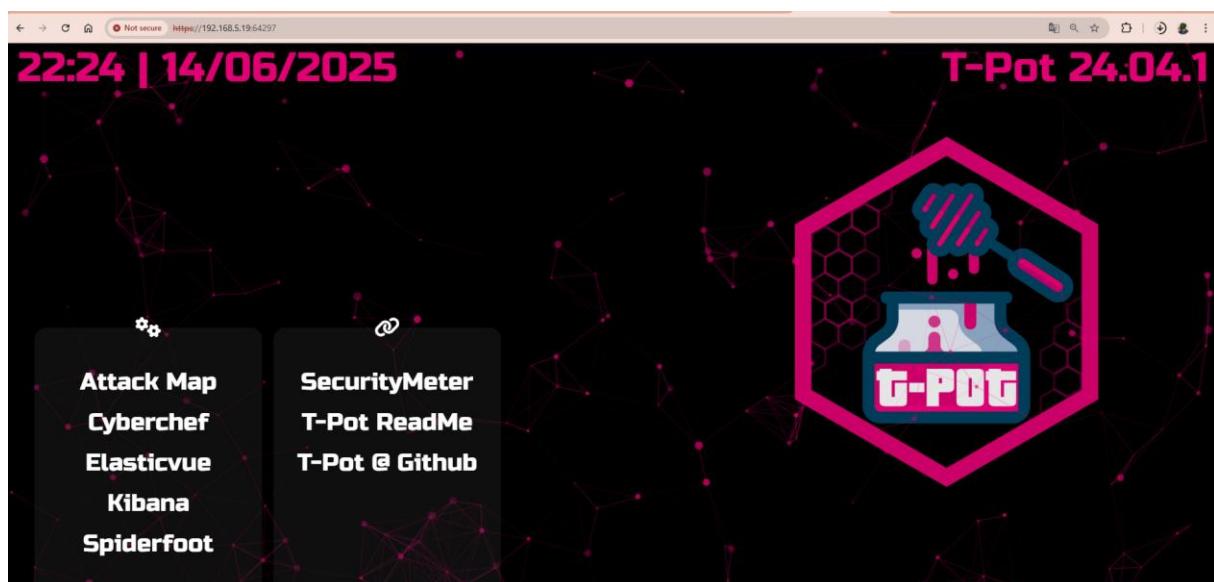
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

TPOT

Voici l'interface d'administration du TPOT, nous avons au milieu générée une attaque pour que l'on puisse afficher les logs et inspecter.

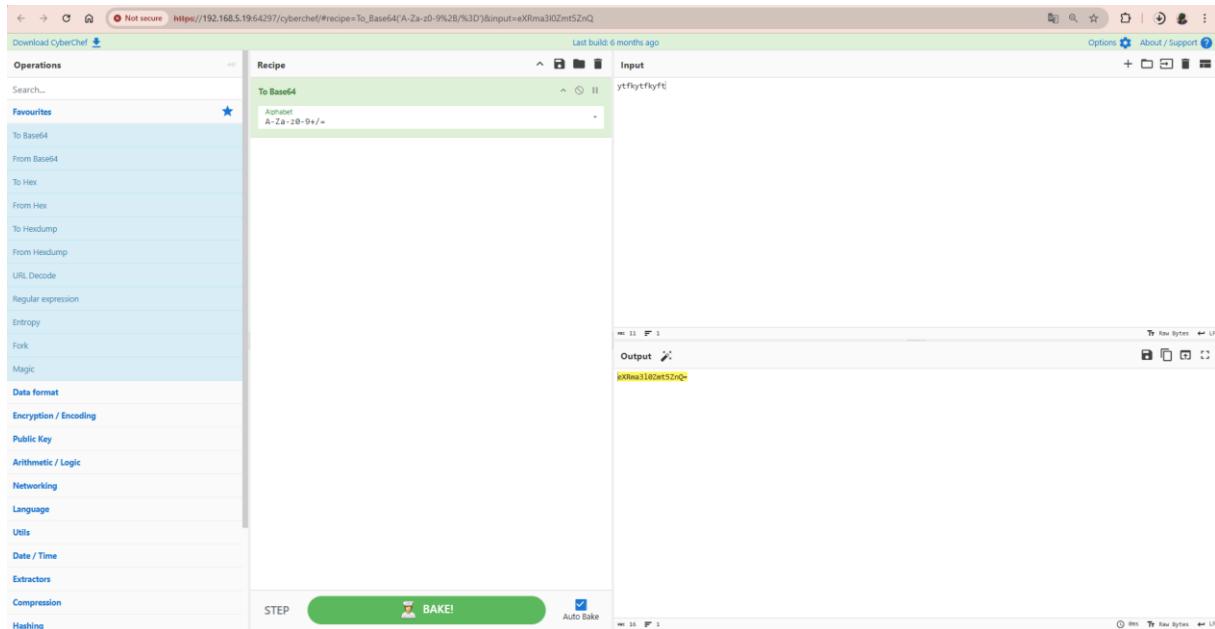


On retrouve différentes sections avec les tentatives, les essaies de login/mot de passe par l'attaquant.



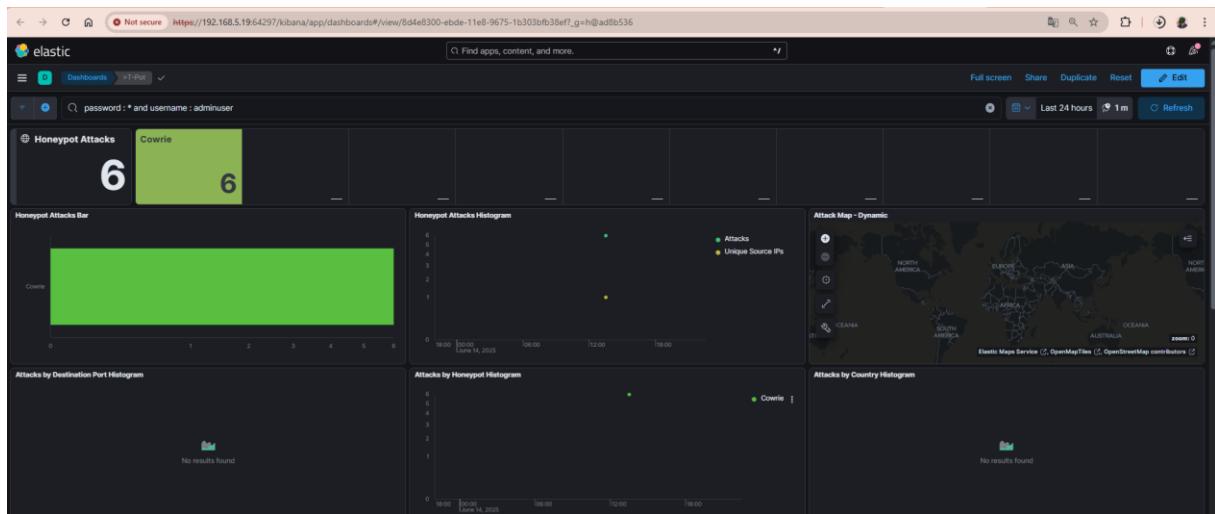
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

On retrouve différentes fonctionnalités comme l'Attack Map ou encore Cyberchef pour déchiffrer différents types d'encodage :



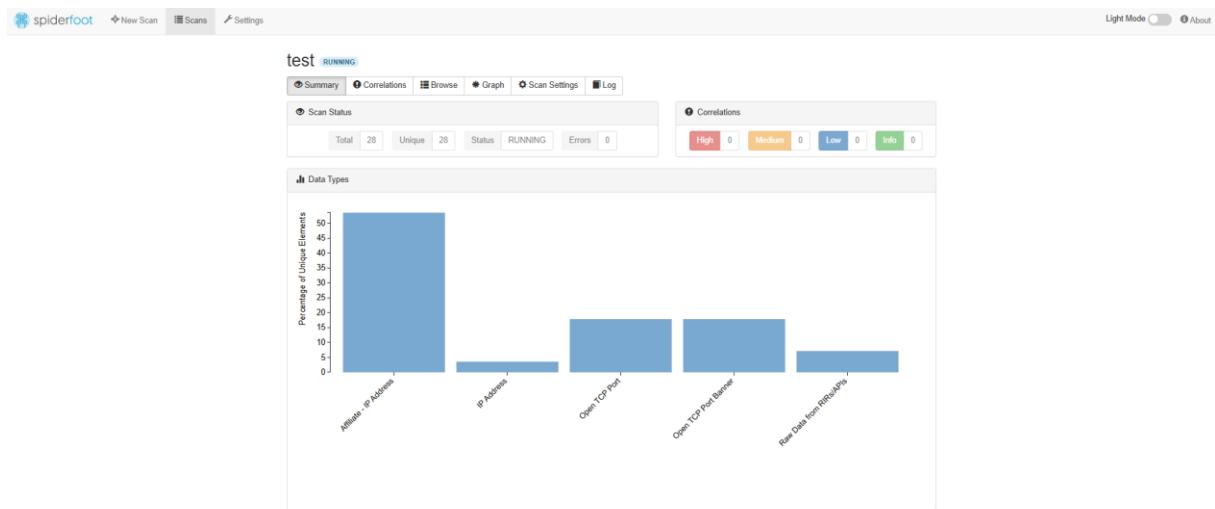
The screenshot shows the CyberChef interface. On the left, there's a sidebar with various tools like 'To Base64', 'From Base64', 'To Hex', etc. The main area has a 'Recipe' section titled 'To Base64' with an input field containing 'ytfktytktkyft'. Below it is an 'Output' section showing the result: 'eXRea3187ett5ZnQ'. At the bottom, there are buttons for 'BAKE!', 'Auto Bake', and file operations.

Voici un exemple, un utilisateur a essayé en SSH de se connecter sur le port 22 avec l'utilisateur admin user et différents mots de passe : (6 tentatives)



Une Instance spiderfoot qui permet d'analyser l'enprunte de nos machines pour générer de la correlation :

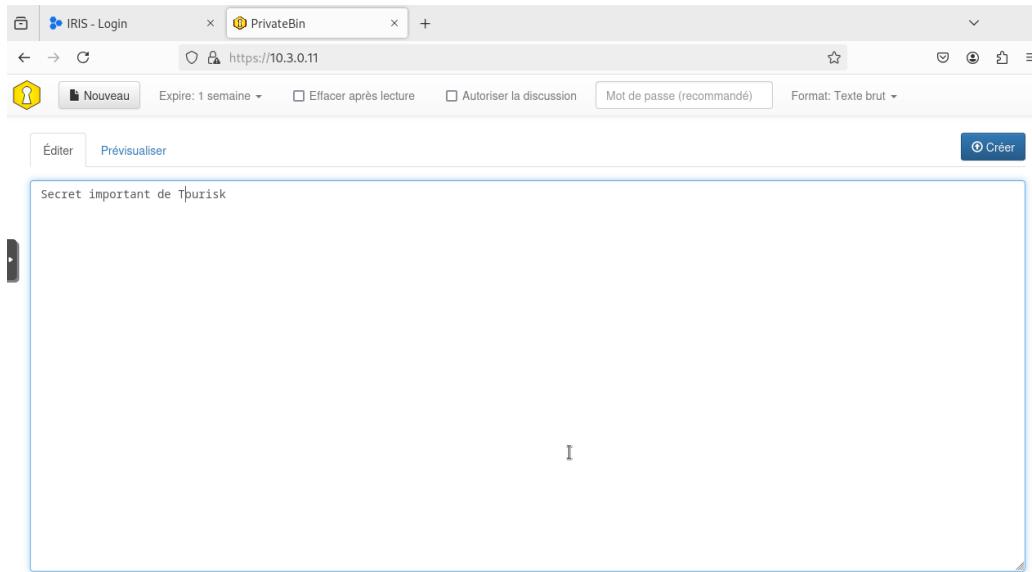
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Trace d'installation, de scan et affichage de résultat dans l'annexe Installation et utilisateur du Tpot.

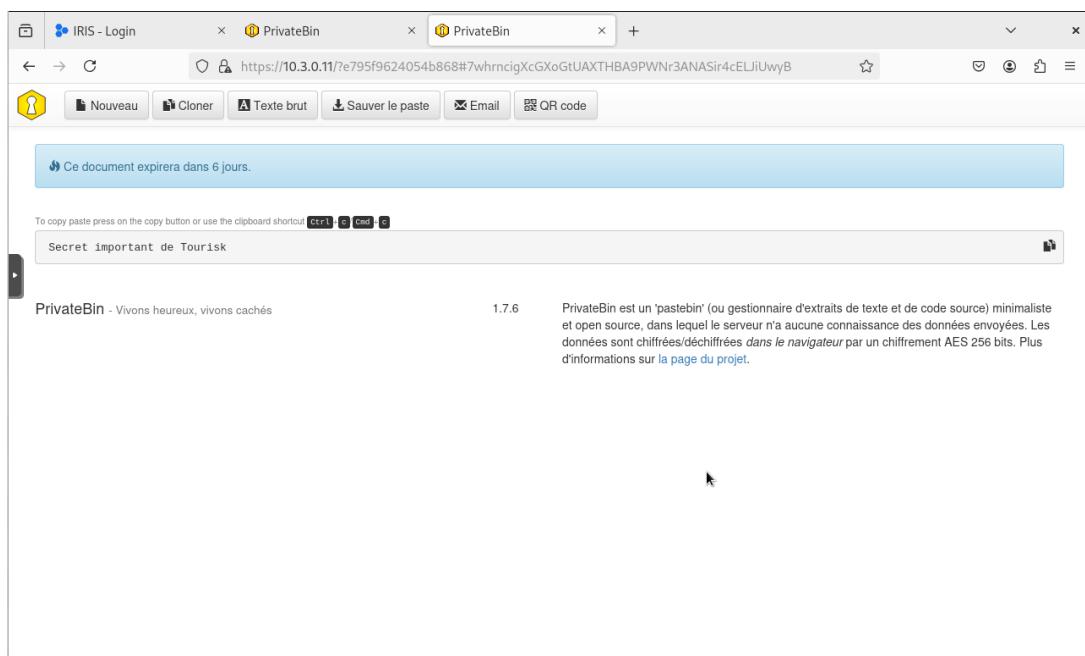
PRIVATEBIN

Il est possible d'échanger des informations au sein de l'entreprise avec cet outil. Il permet de faire un partage sécurisé de caractère.

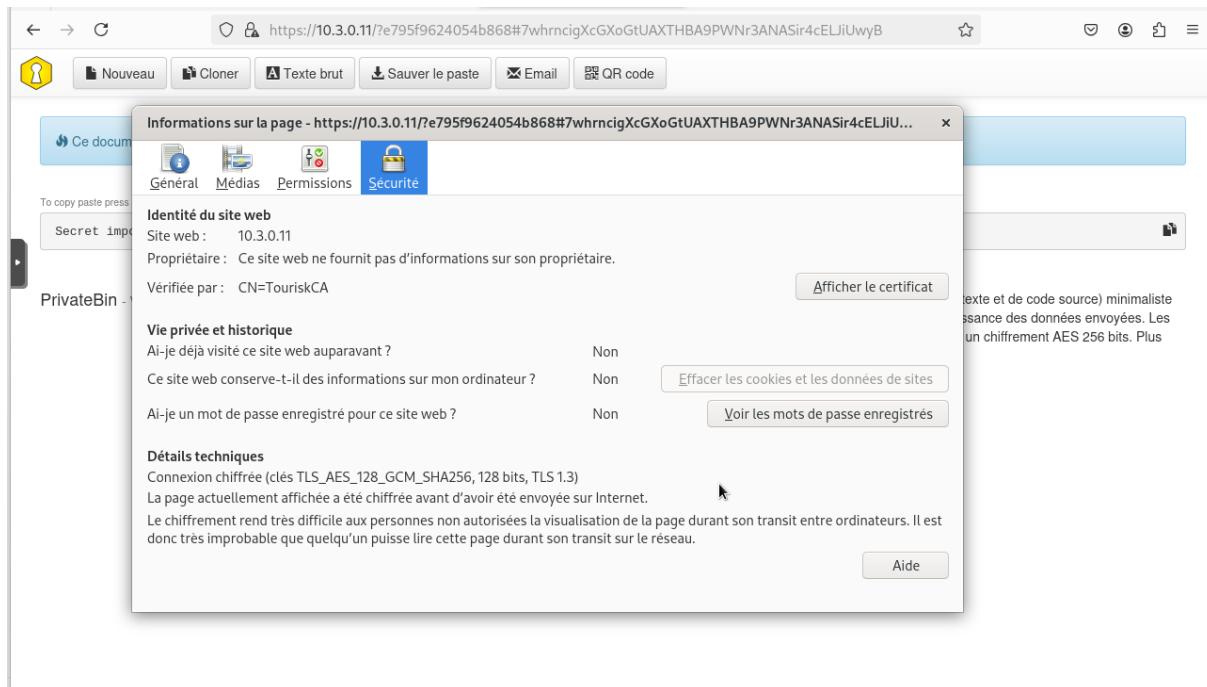


ON retrouve bien la donnés envoyés :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



L'application possède un certificat signé par notre CA **TouriskCA**.

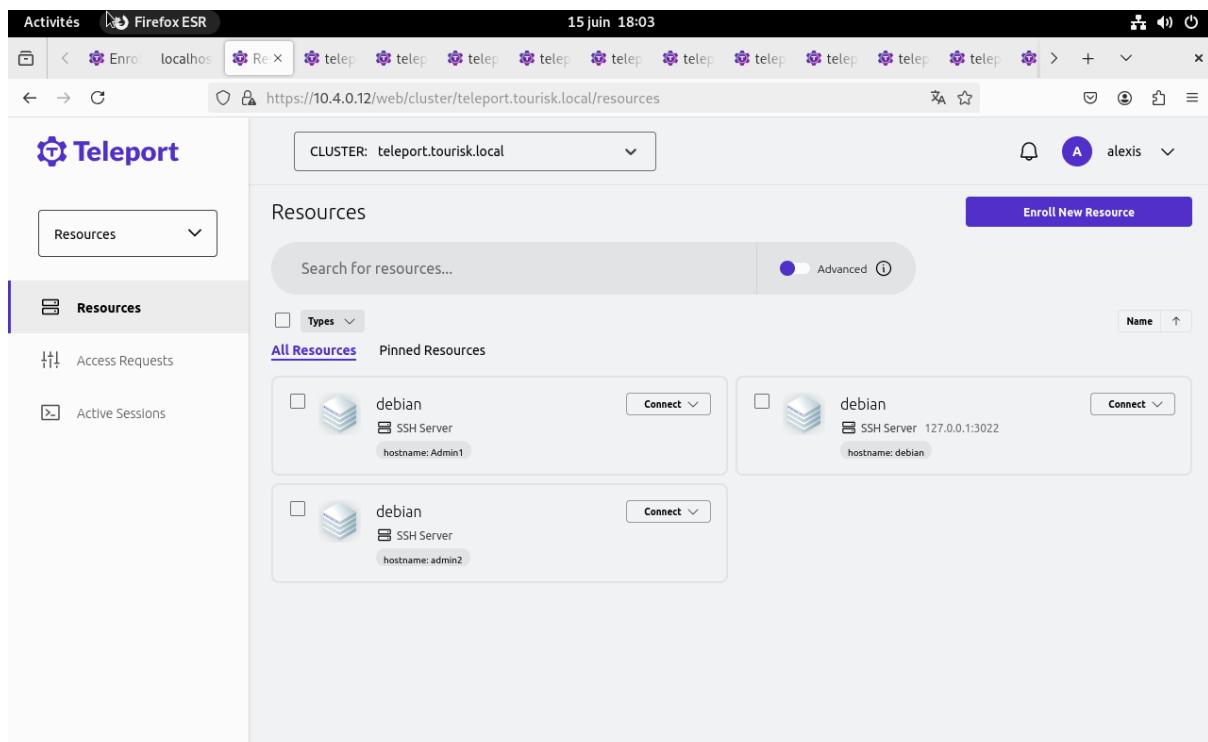


Vous trouverez l'installation de Privatebin, la création du certificat et signature par la CA dans l'annexe Configuration PrivateBin

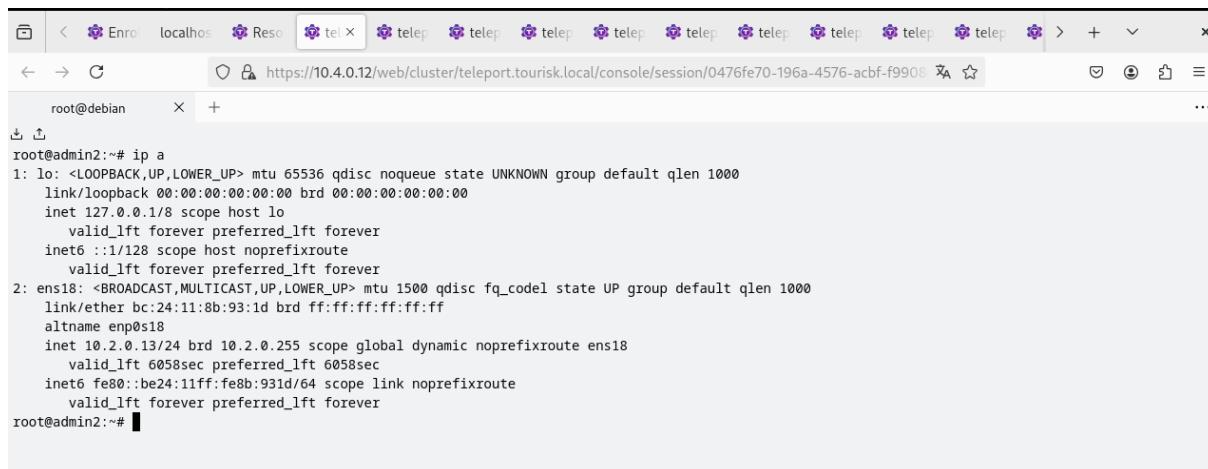
BASTION TELEPORT

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Le bastion TELEPORT permet après une authentification à 2 facteurs d'administrer les machines de l'entreprise.



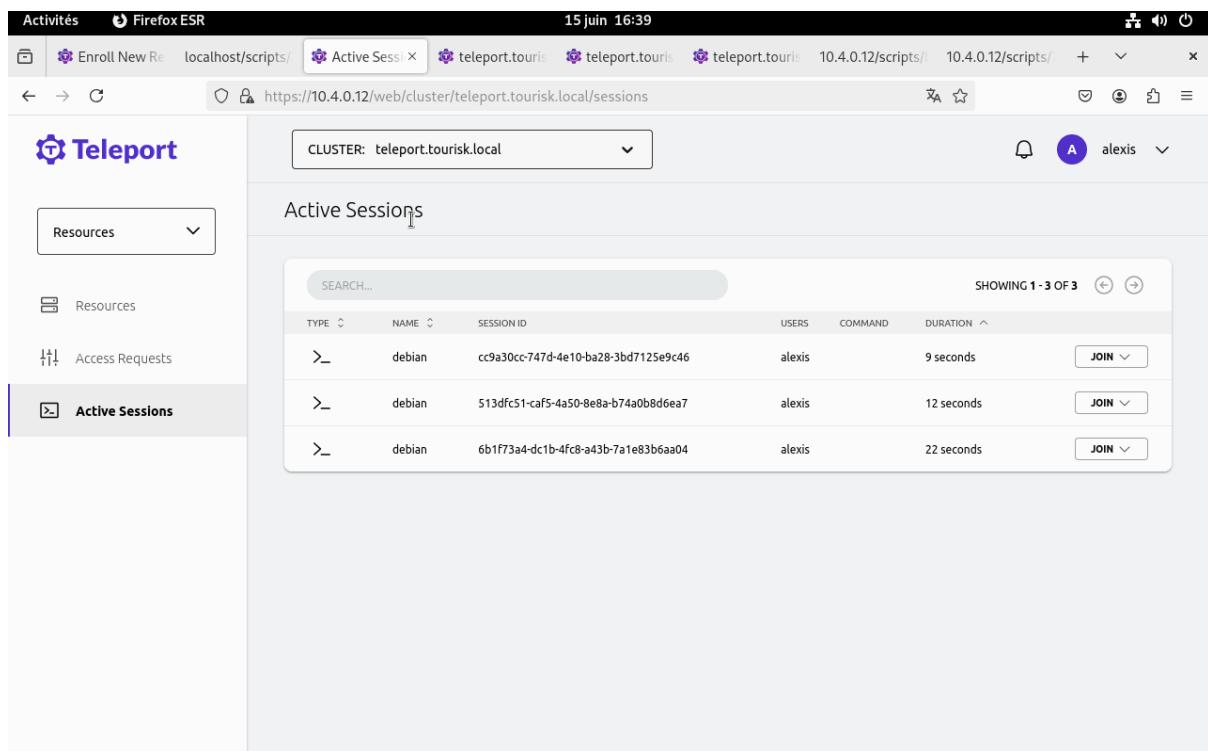
Dans cet exemple on retrouve 3 machines, l'administrateur 1, l'administrateur2 et la machine debian. Nous avons la possibilité d'ouvrir un shell sur les différentes machines, et d'afficher les sessions ouvertes :



```
root@admin2:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 group default qlen 1000
    link/ether bc:24:11:8b:93:1d brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.2.0.13/24 brd 10.2.0.255 scope global dynamic noprefixroute ens18
        valid_lft 6058sec preferred_lft 6058sec
        inet6 fe80::be24:11ff:fe8b:931d/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@admin2:~#
```

Et voici les différentes sessions actives

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



The screenshot shows a Firefox ESR browser window with the URL <https://10.4.0.12/web/cluster/teleport.tourisk.local/sessions>. The page title is "Active Sessions". The left sidebar has tabs for "Resources" (selected), "Access Requests", and "Active Sessions". The main content area displays a table of active sessions:

TYPE	NAME	SESSION ID	USERS	COMMAND	DURATION	JOIN
>_	debian	cc9a30cc-747d-4e10-ba28-3bd7125e9c46	alexis		9 seconds	JOIN ▾
>_	debian	513dfc51-caf5-4a50-8e8a-b74a0b8d6ea7	alexis		12 seconds	JOIN ▾
>_	debian	6b1f73a4-dc1b-4fc8-a43b-7a1e83b6aa04	alexis		22 seconds	JOIN ▾

Vous trouverez le guide d'installation et d'ajout des machines dans TELEPORT dans l'annexe Installation de TELEPORT.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

PROXMOX (PVE ET PBS)

Dans notre configuration, nous avons trois serveurs Proxmox Virtual Environment en cluster qui permettront la Haute Disponibilité avec CEPH notamment :

Ainsi, tous les serveurs du projet seront virtualisés sous forme de machines virtuelles réparties pour équilibrer les ressources sur les trois serveurs physiques.

Nous aurions les machines virtuelles suivantes dans le cluster de l'entreprise :

- Contrôleur de domaine Active Directory.
- Scanner de vulnérabilité Nuclei.
- Elastalert.
- Plateforme alerting DFIR Iris.
- Deux machines pour émuler des utilisateurs (GUI et CLI).
- Keycloak
- Bastion Teleport.
- Wazuh.
- Graylog.
- Serveur de supervision Zabbix.
- Serveur de monitoring Grafana.
- Plateforme de threat intelligence MISP.
- Honeypot T-Pot.

Dans la configuration actuelle, la perte d'un des trois serveurs physiques n'entraînera pas d'interruption de service des machines virtuelles. A noter que la haute disponibilité, n'exclue pas l'obligation de sauvegarder nos machines virtuelles pour pouvoir restaurer des données perdues ou endommagées.

Pour cela, nous avons décidé d'utiliser la solution **Proxmox Backup Server** qui est adapté à la sauvegarde des machines virtuelles d'un environnement Proxmox.

Nous en avons installé un sur le site principal à Toulouse ainsi qu'un deuxième dans le cloud S3 afin de profiter d'une sauvegarde externe (recommandé par l'ANSSI).

Les sauvegardes sont effectuées pour toutes les machines virtuelles sur les deux serveurs tous les jours à **01h** sur le premier serveur et à **04h** sur le deuxième.

La politique de rétention des sauvegardes qui a été choisie arbitrairement est la suivante :

- 7 sauvegardes journalières.
- 4 sauvegardes hebdomadaires.
- 12 sauvegardes mensuelles.
- 3 annuelles.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Toutes les documentations de Proxmox Virtual Environment et Proxmox Backup Server sont disponibles en annexe dont la restauration de sauvegarde pour le PCA/PRA.

SCANNER DE VULNERABILITÉ

Le scanner de vulnérabilité Nuclei a été mis en place sur une machine Debian.

Pour l'installer, il faut installer golang et exécuter la commande suivante :

```
go install -v github.com/projectdiscovery/nuclei/v3/cmd/nuclei@latest
```

Il se base sur des templates au format YAML pour effectuer des scans de vulnérabilité sur des hôtes.

Actuellement, il est configuré pour scanner le serveur web toutes les semaines avec une tâche crontab qui exécute le script bash suivant pour lancer le scan :

```
root@nuclei:~# cat nuclei.sh
#!/bin/bash

nuclei -u http://localhost/ -ts -severity medium,high,critical -o /root/output.txt
root@nuclei:~# []
```

Voici la tâche cron créée qui exécute le script tous les lundis à 2h00 du matin :

```
root@nuclei:~# cat /etc/fstab
# UNCONFIGURED FSTAB FOR BASE SYSTEM
0 2 * * 1 /bin/bash /root/nuclei.sh
root@nuclei:~# []
```

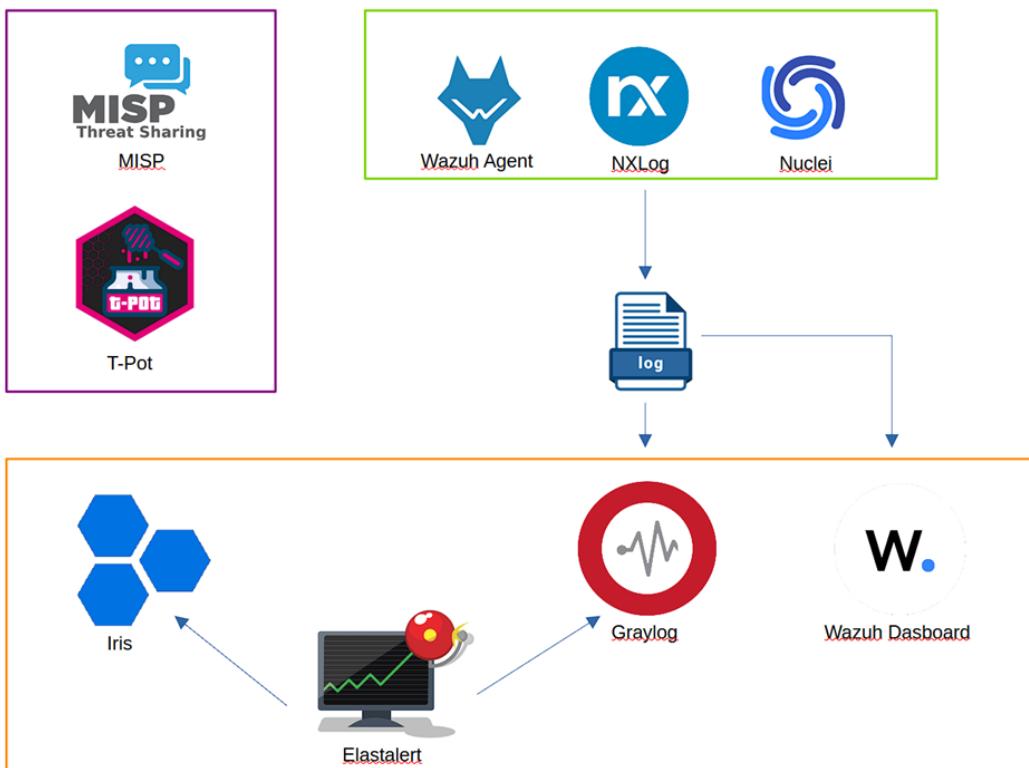
Un fichier de log est généré avec les résultats des scans qui est ensuite envoyé sur le SIEM Graylog grâce à un agent Filebeat installé sur la machine.

Cela permet de faire des règles de détection et ainsi être informé sur la plateforme d'alerting Iris lorsqu'une vulnérabilité est découverte.

SIEM ET XDR

Voici un schéma logique de la stack de détection et de réponse à incident :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



WAZUH AGENT

L'XDR Wazuh permet la collecte des logs sur les endpoints notamment, les postes utilisateurs mais aussi certains serveurs critiques comme le Domain Controller.

Sa plus-value par rapport au SIEM dans notre cas est la remédiation que permet l'EDR et aussi une collecte d'information plus importante qui permet une analyse plus approfondie par le SOC.

L'installation de l'agent se fait en deux lignes de commande Powershell à lancer en administrateur :

```
Administrator : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\Administrateur> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msieexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='10.5.0.26'
PS C:\Users\Administrateur> NET START WazuhSvc
```

NXLOG

Permet la collecte de logs sur le contrôleur de domaine pour les envoyer sur Graylog.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

L'agent se télécharge depuis le site officiel :

- <https://nxlog.co/downloads/nxlog-ce#nxlog-community-edition>

The NXLog Community Edition is a high-performance multi-platform log collection solution aimed at solving these tasks and doing it with a single tool. Your reports are as good as the data you gather. Make sure to collect your event data the right way!

- Superior OS support
- Windows log collection capabilities
- Compliance and security
- Open source

User Guide →
Reference Manual →

Available Downloads

Version: NXLog Community Edition

Platform: All, Red Hat, Debian, Docker, SUSE, Oracle

Select All

Windows

② Windows x86-64 nxlog-ce-3.2.2329.msi
 text/doc-cl.txt ChangeLog.txt
 text/doc-m-txt release_notes.txt
 text/doc-pdf nxlog-reference-manual.pdf

We open a new popup window when downloading multiple files.
Ensure to allow popups from your browser settings.

③ **Download** 1 files selected (remove)

Ensuite, il faut éditer le fichier de configuration comme suit :

```
1 # Récupérer les journaux Security de l'observateur d'événements
2 <Input in>
3   Module      im_msvisalog
4   <QueryXML>
5     <QueryList>
6       <Query Id='1'>
7         <Select Path='Security'>=</Select>
8       </Query>
9     </QueryList>
10    </QueryXML>
11  </Input>
12
13 # Déclarer le serveur Graylog (selon input)
14 <Extension gelf>
15   Module      xm_gelf
16 </Extension>
17
18 <Output graylog_udp>
19   Module      om_udp
20   Host        192.168.10.220
21   Port        12201
22   OutputType  GELF_UDP
23 </Output>
24
25 # Routage des flux in vers out
26 <Route 1>
27   Path        in => graylog_udp
28 </Route>
```

Désormais relancez le service NXLog pour appliquer la configuration :

```
1 Restart-Service nxlog
```

WAZUH DASHBOARD

Le dashboard Wazuh permet l'analyse des logs remontés par l'agent :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



L'installation se fait sur une Ubuntu server en exécutant la commande suivante :

```
$ curl -s0 https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

Des règles de détections peuvent être mises en place, voici un exemple pour détecter le brute force RDP sur Windows :

```
Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
-->
<rule id="100001" level="5">
  <if_sid>5716</if_sid>
  <srcip>1.1.1.1</srcip>
  <description>sshd: authentication failed from IP 1.1.1.1.</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>

</group>

<group name="rdp">
  <rule id="100100" level="10" frequency="3" timeframe="120">
    <if_matched_sid>60122</if_matched_sid>
    <description>RDP Attack Detected on Windows</description>
  </rule>
</group>
~
```

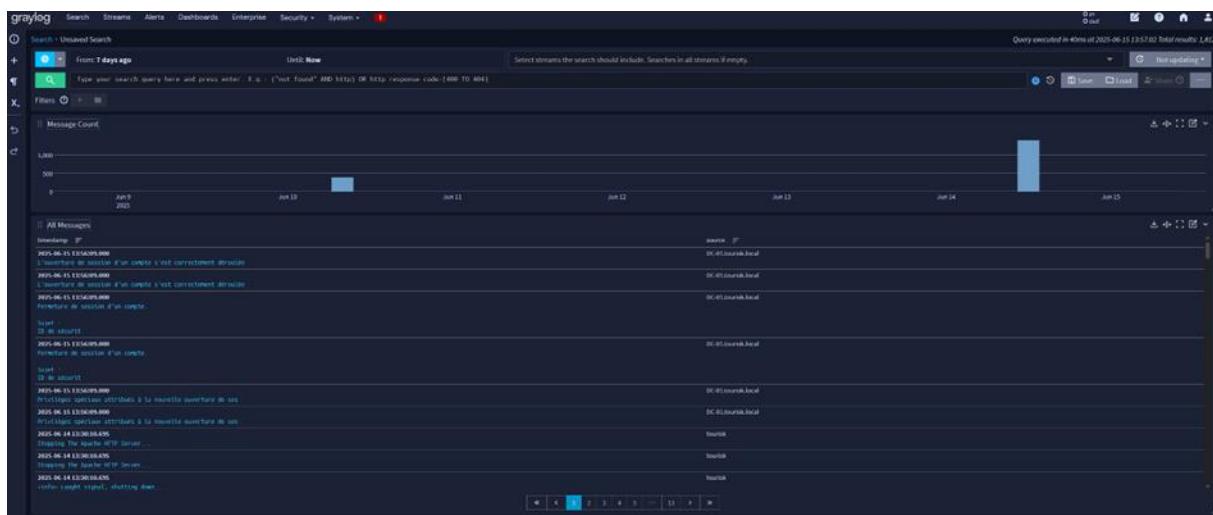
GRAYLOG

Le SIEM Graylog a pour objectif la centralisation des logs et leur analyse grâce à des queries et des agrégations qui sont utiles lors de réponse à incident.

L'installation sera fournie en annexe.

Voici l'interface principale de Graylog :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Les Inputs pour l'ingestion des logs sont configurés dans **System > Inputs** :

Les indexs sont configurés pour pouvoir choisir différents streams et filtrer les logs :

Title	Index Set	Archiving	Rules	Pipelines	Outputs	Throughput	Status	Actions
All events	Graylog Events					0 msg/s	Running	Edit Delete More
All system events	Graylog System Events					0 msg/s	Running	Edit Delete More
Default Stream	Default index set					0 msg/s	Running	Edit Delete More
linux_servers	linux_servers	On	On	On	On	0 msg/s	Running	Edit Delete More
windows_ad	windows_ad	On	On	On	On	0 msg/s	Running	Edit Delete More

ELASTALERT

Le service Elastalert joue les règles de détection sur la base Opensearch qui stocke les logs pour lever des alertes sur la plateforme Iris.

Pour l'installer il s'agit d'un conteneur docker, qu'on peut instancier à partir du fichier compose suivant :

```
services:  
  elastalert:  
    container_name: elastalert  
    image: ghcr.io/jertel/elastalert2/elastalert2:latest  
    volumes:  
      - ./rules:/opt/elastalert/rules  
      - ./config.yaml:/opt/elastalert/config.yaml  
    environment:  
      #- ELASTICSEARCH_USER=elastic  
      #- ELASTICSEARCH_PASSWORD=changeme  
      - SET_CONTAINER_TIMEZONE=true  
      - CONTAINER_TIMEZONE=Europe/Paris
```

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Voici l'arborescence mis en place pour son fonctionnement :

```
root@elastalert:~# tree .
.
|-- config.yaml
|-- docker-compose.yml
`-- rules
    |-- local_bruteforce.yml
    '-- win_auth.yml

2 directories, 4 files
```

- Les configurations générales comme les identifiants de connexion aux plateformes sont référencées dans le fichier config.yaml .
- Le dossier rules stocke les règles de détections.

Voici un exemple de règle elastalert pour détecter les attaques brute force sur l'AD :

```
root@elastalert:~# cat rules/local_bruteforce.yml
name: "local_brute_force"
index: "graylog_0"
is_enabled: true

type: frequency
query_key: TargetUserName
num_events: 5
filter:
  - query:
      query_string:
        query: "EventID:4625"

timeframe:
  minutes: 10

realert:
  minutes: 5

alert_subject_args:
  - "TargetUserName"
alert_subject: "Brute force attack on {}"

alert_text_args:
  - "TargetUserName"
alert_text: "Brute force attack on {}"

alert_text_type: alert_text_only
alert:
  - iris
```

DFIR IRIS

Iris est initialement une plateforme de réponse à incident qui sert aux équipes forensiques pour créer des timelines, gérer les cases, les évidences etc.

Cependant, la plateforme propose aussi un onglet pour gérer les alertes que l'on peut ensuite déplacer dans des cases pour investigation :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

MISP

La plateforme MISP est très utile pour la CTI et le management d'indicateurs de compromission.

Ces indicateurs peuvent être des IP, des hashs, des FQDN, des noms de fichier etc.

MISP permet l'ingestion de nouveaux indicateurs grâce des Feeds et les stocke dans des Events sous forme d'Attributes :

Pour l'exemple nous avons configuré le Feed de DuggyTuxy qui est open source.

MISP présente une API qui permet de récupérer des IOC.

Ainsi, il est possible de récupérer les IOCs sous forme de CSV, et les intégrer à Graylog pour effectuer de la détection dessus.

PURPLEOPS

L'outil PurpleOps permet de créer des scénarios à partir de la matrice MITRE et ainsi, lancer des attaques réalistes pour tester le SOC et créer des rapports purple team :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

TTP T1021.006 - WinRM Access with Evil-WinRM

Tactic Lateral Movement Status Complete

Restart	15/06/2025 22:08	18/06/2025 01:12	Go <input type="button"/>
Source(s)	Target(s)	Tools(s)	
An adversary may attempt to use Evil-WinRM with a valid account to interact with remote systems that have WinRM enabled			
evil-winrm -i Target -u Domain\Administrator -p P@ssw0rd1			
Attaque bloquée : connexion fermée instantanément			
Notes			
Wazuh detection : ok Elastalert detection : ok			
Actions			
Focus Prevent <input checked="" type="radio"/> Detect <input type="radio"/> N/A			
Control(s) <input type="checkbox"/> Tag(s) <input type="checkbox"/>			
Priority			
Prevented Yes <input checked="" type="radio"/> Partial <input type="radio"/> No <input type="radio"/> N/A			
Prevention Rating 5.0			
Detected Yes <input checked="" type="radio"/> No <input type="radio"/>			
Alerted High			
Alert Severity			
Detection Rating 3.0			
Upload Evidence Sélect. fichiers Aucun fichier choisi			
Notes			
UUID			
Upload Evidence Sélect. fichiers Aucun fichier choisi			

PurpleOps

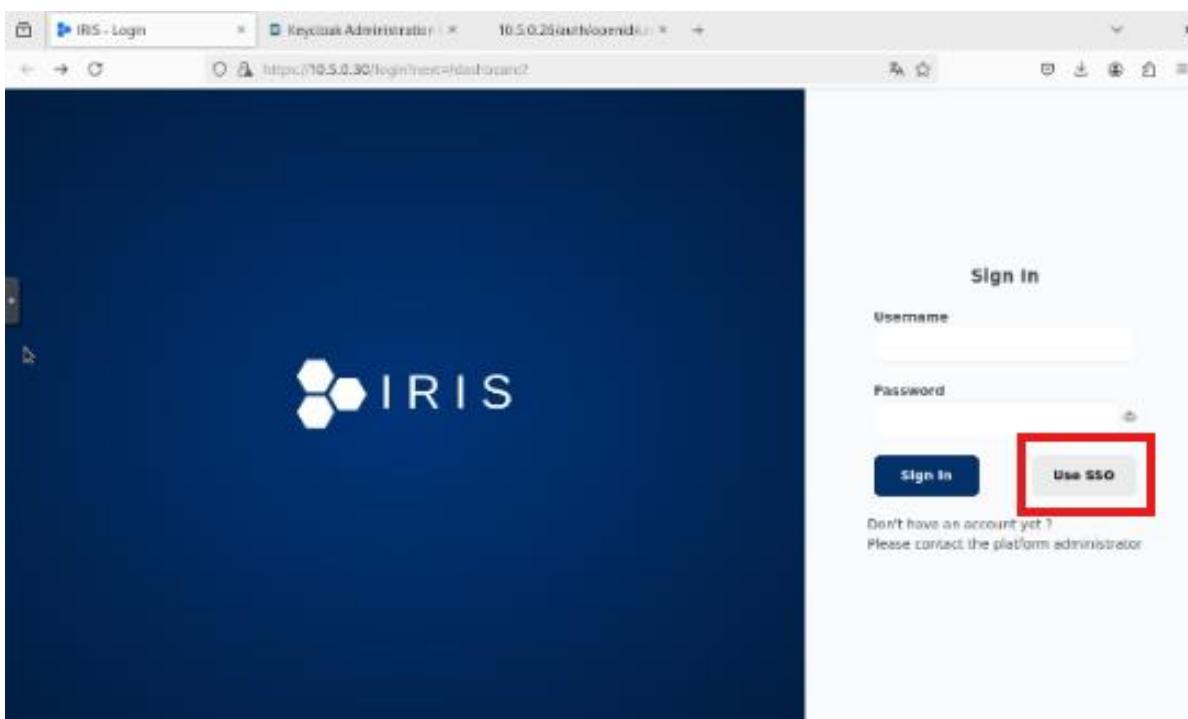
First Workshop New Import... Export... Statistics ATT&CK Navigator [1 selected]

Mitre ID	Name	Tactic	State	Tags	Actions
T1021.006	WinRM Access with Evil-WinRM	Lateral Movement	Complete		<input type="button"/>
T1547.012	Print Processors	Persistence	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	Registry dump of SAM, creds, and secrets	Credential Access	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	Registry parse with pskeyz	Credential Access	Complete	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	eventList SAM copy	Credential Access	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	PowerDump Hashes and Usernames from Registry	Credential Access	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	dump volume shadow copy hives with certutil	Credential Access	Complete	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	dump volume shadow copy hives with System.IO.File	Credential Access	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	WinPwn - Loot local Credentials - Dump SAM File for NTLM Hashes	Credential Access	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1003.002	Dumping of SAM, creds, and secrets/Bog Export	Credential Access	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1497.003	Delay execution with ping	Defense Evasion	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1053.005	PowerShell Cmdlet Scheduled Task	Execution	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1053.005	Task Scheduler via VBA	Execution	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	rsync remote file copy (push)	Command and Control	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	scp remote file copy (push)	Command and Control	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	afp remote file copy (pull)	Command and Control	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	curlfile download (urlcache)	Command and Control	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	Windows - BITSAdmin BITS Download	Command and Control	Complete	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	Windows - PowerShell Download	Command and Control	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	QSTAP Worming Activity	Command and Control	Pending	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	scutil writing a file to a UNC path	Command and Control	Complete	<input checked="" type="checkbox"/>	<input type="button"/>
T1105	Download a file with Windows Defender McmdRun.exe	Command and Control	Pending	<input checked="" type="checkbox"/>	<input type="button"/>

KEYCLOAK

Le Keycloak permet d'avoir une authentification OpenID connect sur différentes machines. Dans cette capture on retrouve l'a possibilité de se connecter en SSO sur DFIR iris, ce qui n'est pas natif dans une installation basique.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



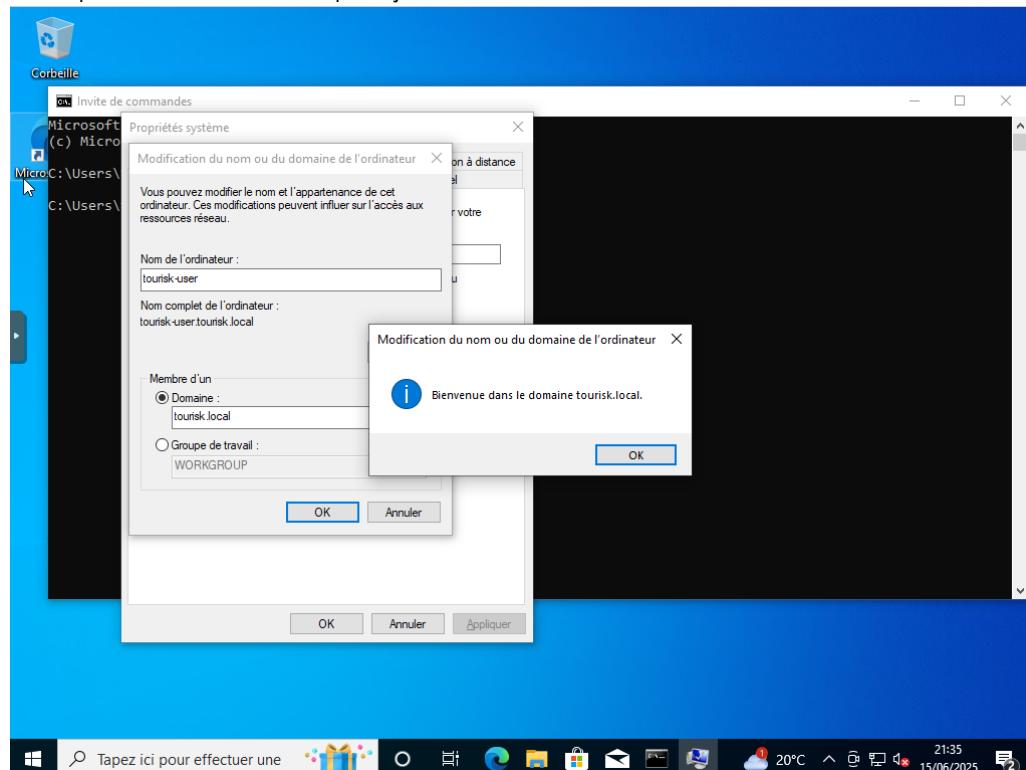
Pour retrouver l'installation de Keycloak, la configuration de Wazuh et D iris pour la mise en place d'une connexion via OPENID connect voir l'annexe Installation et configuration de Keycloak

WINDOWS SERVEUR - ACTIVE DIRECTORY ET UTILISATEUR

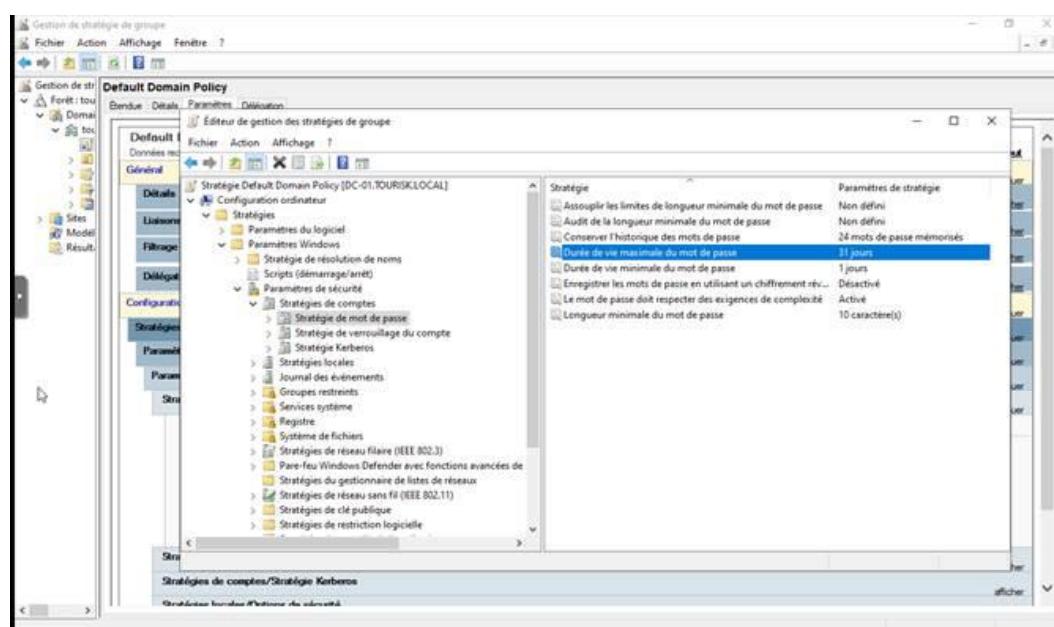
Nous avons monté un Windows Server – Active directory, nous avons ajouté des utilisateurs au domaine Tourisk.local.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Exemple d'un utilisateur qui rejoint le domaine :



Nous avons ensuite modifié des GPO(s) pour changer des paramètres importants liée à la sécurité. Exemple d'une GPO de durée de renouvellement des mots de passe



MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

APPLICATION WEB

Nous avons monté une application WEB qui permet à un utilisateur de souscrire à une assurance et d'avoir un Status de ses assurances.

🛡 Demande d'assurance – Étape 2

Type d'assurance


Auto


Santé


Habitation


Vie


Voyage


Responsabilité Civile

Durée souhaitée

La durée correspond à la période de validité souhaitée de votre contrat.

[← Précédent](#) [Suivant](#)

L'application utilise Fast API pour le backend et React JS pour le front END.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

FastAPI 0.1.0 OAS 3.1

/openapi.json

Authorize

auth

POST /auth/login Login

POST /auth/signup Signup

insurance

GET /insurance/insurance_requests List Insurance Requests

POST /insurance/insurance_requests Create Insurance Request

GET /insurance/insurance_requests/{request_id} Get Insurance Request

PATCH /insurance/insurance_requests/{request_id}/assign Assign Agent To Request

admin

POST /admin/agents Create Agent

DELETE /admin/agents/{agent_id} Delete Agent

GET /admin/users Get All Users

agent

PUT /agent/insurance/status Update Insurance Status

GET /agent/insurance Get Insurance Requests

DELETE /agent/insurance/{insurance_id} Delete Insurance Request

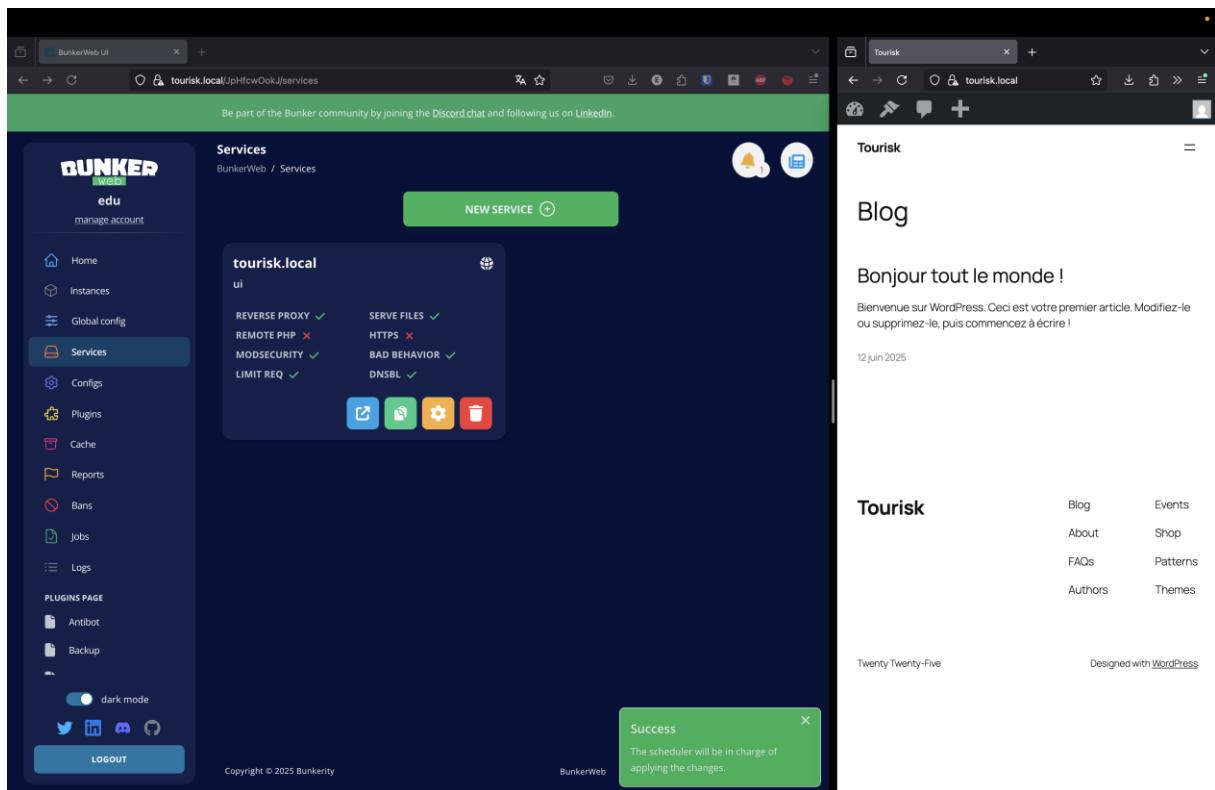
GET /agent/users Get Clients

GET /agent/users/{user_id} Get Client By Id

Vous trouverez toute les fonctionnalités et configuration de l'application WEB dans l'annexe APPLICATION WEB

L'application est sécurisée par un WAF bunkerweb

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



ANNEXES

PCA

- Procédure de confinement de l'incident et gestion de crise (Annexe 1 PCA)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Politique de gestion des mots de passe (Annexe 2 PCA)
- Procédure de restauration des Machines virtuelle (Annexe 3 PCA)
- Contacts critiques

ANNEXE 1

PROCEDURE DE CONFINEMENT DE L'INCIDENT ET GESTION DE CRISE

Objectif : Identifier, contenir, et limiter la propagation d'un incident de sécurité (ex. compromission de compte, ransomware, accès non autorisé), tout en préservant les éléments nécessaires à l'enquête.

1. DETECTION ET ALERTE INITIALE

Responsables : Utilisateur, SOC (si existant), ou Administrateur IT

- Identification d'un comportement anormal (ex. pic de trafic, comportement utilisateur inhabituel, fichier chiffré, connexion suspecte)
- Déclenchement d'une alerte via :
 - Système de détection (SIEM, IDS, antivirus)
 - Signalement par un utilisateur ou collaborateur
- Enregistrement de l'incident dans l'outil de ticketing ou registre d'incident (catégorie : Sécurité – Suspicion de compromission).

2. QUALIFICATION RAPIDE DE L'INCIDENT

Responsables : Équipe sécurité ou IT

- Vérification de l'origine de l'alerte
- Identification rapide de :
 - L'hôte ou le système concerné
 - L'utilisateur impliqué
 - L'heure estimée de la première activité suspecte

Décision : incident confirmé ou faux positif

3. PHASE DE CONFINEMENT IMMEDIAT

COURT TERME – OBJECTIF : STOPPER LA PROPAGATION

Actions immédiates : (Ne pas éteindre la machine)

Action	Détail

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Isolation réseau du poste compromis	Via Proxmox / VLAN / désactivation Wi-Fi
Révocation des identifiants compromis	Changement des mots de passe + MFA
Désactivation du compte utilisateur	Si soupçonné d'être compromis
Blocage des accès externes (VPN)	Pour tous les utilisateurs suspects
Sauvegarde de la mémoire et des logs	Dump mémoire RAM, logs d'accès, firewall

4. DELIMITATION DU PERIMETRE DE COMPROMISSION

Responsables : Équipe sécurité / Responsable PCA

- Analyse des logs (authentification, flux réseau, modifications système)
- Cartographie des équipements et comptes utilisateurs impactés
- Détection d'éventuelles escalades de priviléges ou mouvements latéraux

5. IDENTIFICATION DES ACTEURS

But : identifier les comptes/utilisateurs compromis malveillants ou non.

- Analyse des historiques d'activité :
 - Heures de connexion
 - Localisation géographique
 - Comportements anormaux (script, copie de données)
- Vérification auprès des utilisateurs :
 - Demander si les connexions ou actions leur appartiennent
 - Vérifier les accès VPN ou à distance récents

Exemple :

Un utilisateur connecté à 3h du matin depuis une IP en dehors du pays sans avoir prévenu → compte potentiellement compromis.

6. COMMUNICATION DE CRISE INTERNE

Responsables : RSSI / Responsable PCA / Direction

- Briefe les équipes concernées (IT, métier, juridique) en passant par le canal approprié.
- Communication à l'ensemble du personnel :
 - Nature de l'incident

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Mesures immédiates (ex. changement de mot de passe)

7. PRESERVATION DES PREUVES

Pour éventuelle action juridique ou analyse post-incident

- Conserver :
 - Images disques / VM
 - Logs réseau et système
 - Échanges internes liés à l'incident
- Ne pas redémarrer les systèmes concernés sans copie
- Documenter l'ensemble des actions effectuées avec horodatage

8. REMONTEE REGLEMENTAIRE (SI DONNEES PERSONNELLES TOUCHEES)

Responsable : DPO ou direction

- Évaluation de la nature des données touchées
- Si nécessaire :
 - Notification à la CNIL sous 72h (en France)
 - Notification aux personnes concernées

9. FIN DE PHASE DE CONFINEMENT

- Une fois les systèmes compromis isolés et les comptes sécurisés
- Passage à la phase de **remédiation** (reconstruction, restauration, nettoyage)
- Rapport initial d'incident produit pour revue

ANNEXE 2

1. POLITIQUE DE GESTION DES MOTS DE PASSE

TOURISK – Politique de gestion des mots de passe

Version : 1.0 | Date de mise à jour : 20/04/2025

1. OBJECTIF

Assurer la sécurité des systèmes, données et comptes utilisateurs par des pratiques robustes de gestion des mots de passe.

2. PORTEE

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Cette politique s'applique à tous les employés, partenaires, et prestataires ayant accès aux systèmes de Tourisk.

3. EXIGENCES MINIMALES POUR LES COMPTES UTILISATEURS

Élément	Valeur recommandée
Longueur minimale	12 caractères
Complexité	Majuscules, minuscules, chiffres, caractères spéciaux
MFA (authentification multifacteur)	Obligatoire pour VPN, email, SSO
Stockage	Interdit en clair – gestion via coffre-fort (ex: Bitwarden, KeePass)

4. MOTS DE PASSE ADMINISTRATEURS

- Changés à chaque départ de personnel IT
- Stockés dans un coffre sécurisé accessible uniquement aux responsables autorisés

4.1 EXIGENCES MINIMALES POUR LES COMPTES ADMINISTRATEURS

Élément	Valeur recommandée
Longueur minimale	18 caractères

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Complexité	Majuscules, minuscules, chiffres, caractères spéciaux
Rotation	Tous les 60 jours max
Historique	Ne pas réutiliser les 5 derniers
MFA (authentification multifacteur)	Obligatoire
Stockage	Interdit en clair – gestion via PAM

5. RESPONSABILITES

- **Utilisateurs** : protéger leurs mots de passe et signaler tout comportement suspect
- **IT** : appliquer la politique via AD / gestionnaire SSO / MFA

ANNEXE 3

PROCEDURE DE RESTAURATION VM (PROXMOX)

TOURISK – Procédure de restauration d'une machine virtuelle Proxmox

Version : 1.0 | Date de mise à jour : XX

1. OBJECTIF

Assurer une restauration rapide d'une VM critique en cas d'incident, depuis une sauvegarde locale ou distante.

2. PREREQUIS

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Accès à Proxmox (console ou web GUI)
- Sauvegardes à jour stockées localement ou sur S3
- Droits d'administration

3. ÉTAPES (RESTAURATION LOCALE)

1. Connexion à l'interface Proxmox

2. Sélection de la VM concernée

Aller dans Datacenter → Storage → Backup

3. **Choisir la sauvegarde à restaurer**

Vérifier la date et l'intégrité

Format **.vma.zst** recommandé

4. **Lancer la restauration**

Cliquer sur Restore

Choisir le node, l'ID (changer si besoin), et l'emplacement disque

VERIFICATION POST-RESTAURATION

Boot VM

Contrôle accès réseau / services

4. EN CAS DE RESTAURATION DEPUIS S3

- Télécharger l'image via l'outil CLI
- Charger manuellement sur le node local
- Appliquer les mêmes étapes

ANNEXE 4

1. CONTACTS CRITIQUES (HEBERGEURS, FOURNISSEURS, ETC.)

TOURISK – Liste des contacts critiques

Version : 1.0 | Date : Factice

Type de prestataire	Nom du fournisseur	Contact support	N° de contrat	Niveau de SLA	Remarques

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Hébergeur (local Proxmox)	[Nom]	[email / tél]	[ID contrat]	4h	Surveillance 24/7
Sauvegarde S3	[Nom S3 provider]	[email / tél]	[ID contrat]	99.9%	Chiffrement activé
Fournisseur Internet 1	[Nom FAI]	[email / tél]	[ID contrat]	1Gbit – SLA 4h	Lien principal
Fournisseur Internet 2	[Nom FAI secondaire]	[email / tél]	[ID contrat]	300 Mbit	Lien de secours
Fournisseur de VPN	[Nom]	[email / tél]	[ID contrat]	Ok	Lien de secours

PRA

5. ANNEXES TECHNIQUES (EXTRAITS)

ANNEXE A : SCRIPTS D'URGENCE

Bascule vers PBS Cloud :

```
#!/bin/bash

# Variables

PBS_REPO="cloud-pbs@tls:backup.tourisk.com"

VM_LIST="101 102 201"
```

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

```
for VMID in $VM_LIST; do  
  
    proxmox-backup-client restore --repository $PBS_REPO $VMID \  
    --output /var/lib/vz/images/$VMID \  
    --worker 4 --verbose  
  
Done
```

ANNEXE B : METRIQUES ZABBIX POUR DETECTION

Métrique	Seuil Critique	Action Automatique
vfs.dev.read[dm-0]	> 90% IO delay	Migration VM vers autre nœud
net.if.total[eth0]	< 10 Mbps	Bascule vers eth1

ANNEXE C : DIAGRAMME DE FLUX DE REPRISE

[Incident] → [Détection Zabbix] → [Isolation] → [Restauration PBS]



WEB

ANNEXE 1 : DIAGRAMME DE SEQUENCE UML

Acteurs principaux

- Client : Utilisateur final qui utilise l'application web pour accéder aux services d'assurance.
- Agent d'assurance : Employé de l'assurance qui valide les demandes et gère les contrats.

Objectifs

Client :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

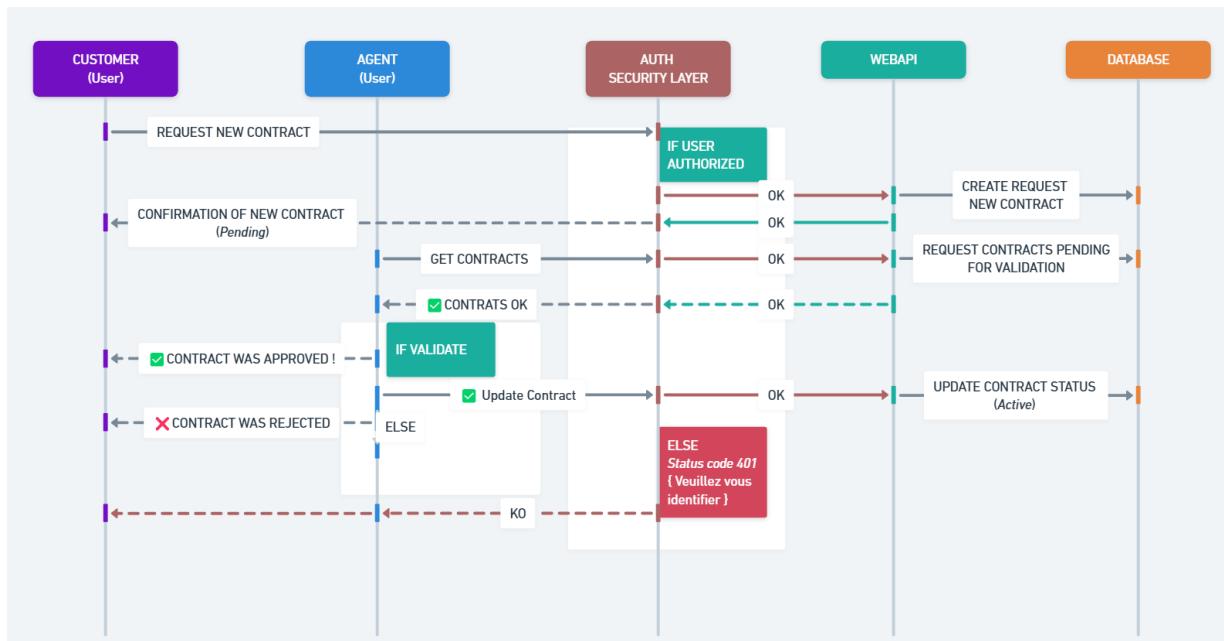
- Demander une offre d'assurance via un formulaire en ligne.
- Souscrire à une police d'assurance après validation.
- Gérer ses contrats (consulter, modifier, annuler).
- Déposer une réclamation en cas de sinistre.

Agent d'assurance :

- Valider ou refuser les demandes de souscription.
- Assister les clients lors des réclamations.
- Renouveler ou modifier les contrats existants.

Authentication/Authorization API Layer :

- Valider l'authentification du client ou de l'agent à chaque requête (via JWT).
- Contrôler les autorisations d'accès aux services (par exemple : seuls les agents peuvent valider des contrats).
- Assurer la sécurité de bout en bout dans les échanges (authentification, intégrité des données).



ANNEXE 2 : DIAGRAMME DE FLUX

Page de demande :

Client : Soumet une demande d'assurance en ligne et peut consulter le statut de cette demande.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Statut de la demande : Le client peut voir si sa demande est en attente, validée, ou refusée.

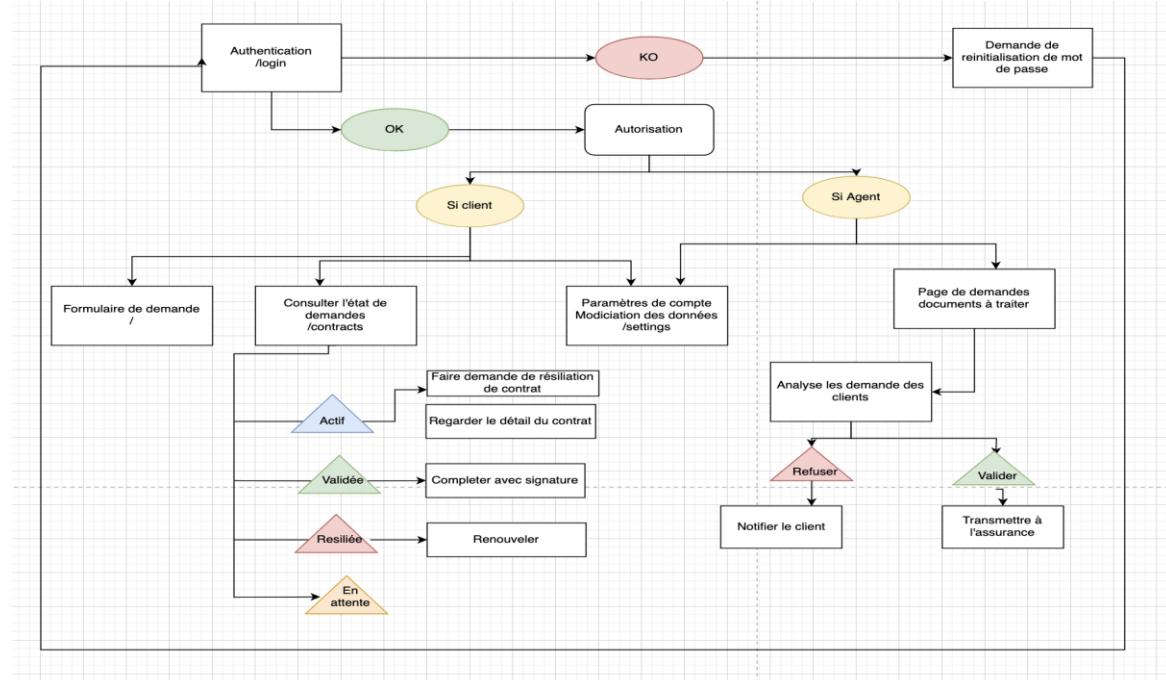
Dashboard de l'agent :

Agent : Consulte les demandes soumises par les clients via un tableau de bord.

Validation/Refus :

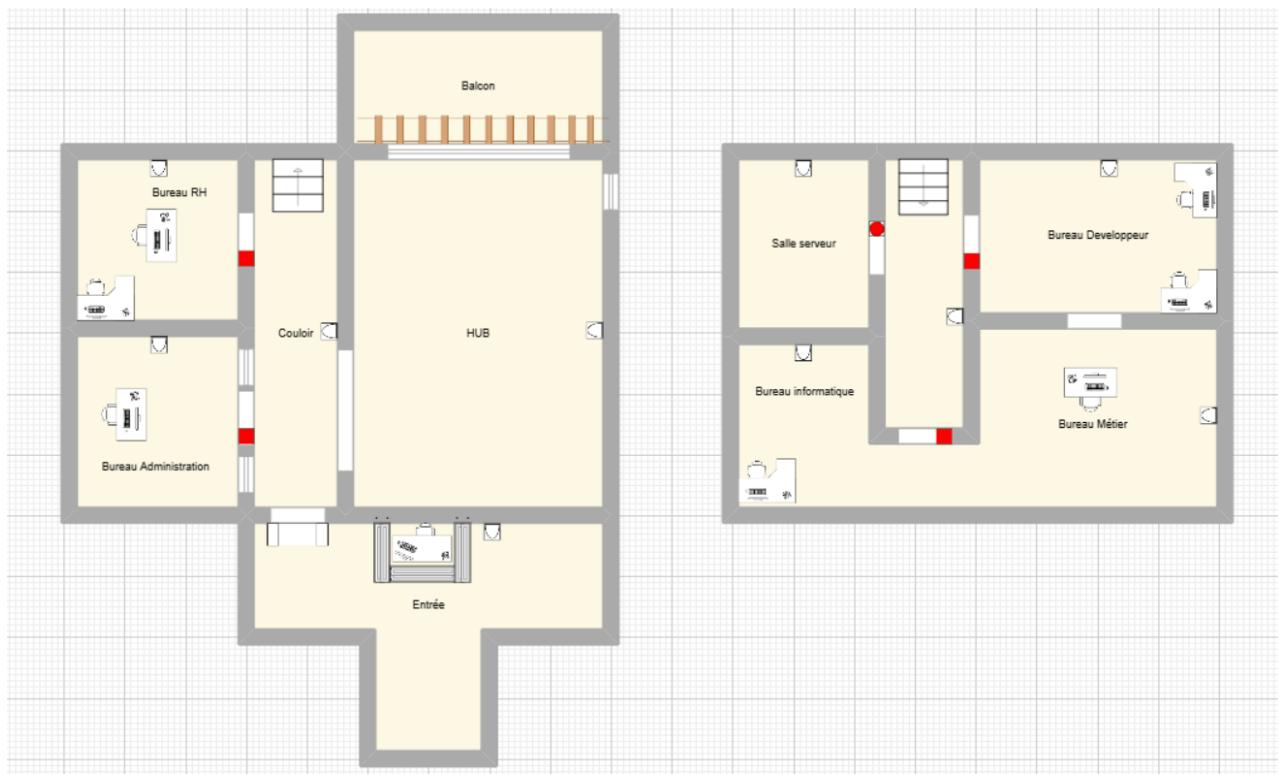
L'agent examine la demande et peut soit la valider, soit la refuser selon les critères définis.

Retour au client : Client : En fonction de la décision de l'agent (validation ou refus), le client est notifié du statut de sa demande (validée ou rejetée).



ANNEXE PLAN DES LOCAUX PHYSIQUES

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Légende

Portique de sécurité



Caméra



Vitre de sécurité



Accès biométrique



Contrôle de sécurité (badges)



ANNEXE : INVENTAIRE DES ACTIFS

LE SITE PRINCIPAL

- Serveurs :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Un serveur d'annuaire
 - Une base de données
 - Une application Web
- Equipement réseau :
 - Switch 0
 - Switch 1
 - Firewall de sortie

- Machine de travail :
 - Machine locale 1
 - Machine locale 2
 - Machine locale 3
 - Machine locale 4

LE SITE DISTANT

- Machine de travail :
 - Machine locale 1
 - Machine locale 2
 - Machine locale 3
 - Machine locale 4
- Equipement réseau :
 - Firewall de sortie

VPN

- Machine de travail distant :
 - Machine distante 1 (admin)
 - Machine distante 2 (admin)
 - Machine distante 3 (utilisateur)

ANNEXE : INSTALLATION ET CONFIGURATION DE OPENSENSE

SOMMAIRE

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Mise en place de la VM sur Proxmox
- Création et configuration des interfaces et des vlan(s)
- Mise en place du DHCP
- Haute disponibilité
- Mise en place des 2 VPN (admins-utilisateurs)
- Configuration des règles de firewall

MISE EN PLACE DE LA VM SUR PROXMOX

Récupération et installation de l'iso dans la banque d'iso disponible sur Promox :

Date	Name, Format	Format	Size
2023-12-11 11:50:25	iso	5.68 GB	
2024-04-29 14:21:44	iso	1.44 GB	
2025-04-07 21:47:36	iso	2.22 GB	
2024-04-04 14:09:49	iso	6.63 GB	
2023-11-10 22:44:42	iso	6.15 GB	
2025-05-20 21:56:14	iso	6.22 GB	
2024-03-01 10:13:03	iso	406.85 MB	
2023-11-11 11:22:44	iso	658.51 MB	
2023-12-04 16:22:34	iso	481.30 MB	
2024-04-26 16:42:03	iso	3.07 GB	
2024-04-28 19:03:55	iso	2.69 GB	
2023-11-01 09:47:55	iso	767.46 MB	
2025-05-30 12:27:01	iso	1.57 GB	
2024-01-15 20:25:43	iso	784.33 MB	
2024-01-28 14:10:37	iso	1.02 GB	
2024-02-20 19:12:34	iso	4.93 GB	
2024-03-31 22:03:15	iso	2.10 GB	
2023-11-10 22:59:04	iso	627.52 MB	
2025-05-28 22:06:33	iso	726.50 MB	
2025-05-09 13:31:58	iso	5.06 GB	

Création d'une machine virtuelle

Summary	Add	Remove	Edit	Disk Action	Revert
Console				Memory	4.09 GiB
Hardware				Processors	4 (1 sockets, 4 cores) [x86-64-v2-AES]
Cloud-Init				BIOS	Default (SeaBIOS)
Options				Display	Default
Task History				Machine	Default (i440fx)
Monitor				SCSI Controller	VirtIO SCSI single
Backup				CD/DVD Drive (ide2)	local:iso:OPNsense-25.1-dvd-amd64.iso,media=cdrom,size=2165500K
Replication				Hard Disk (scsi0)	local-lvm:vm-531-disk-0,iothread=1,size=30G
Snapshots				Network Device (net0)	virtio=BC:24:11:C5:1C:4F,bridge=vmbr500,firewall=1
Firewall				Network Device (net1)	virtio=BC:24:11:8B:0C:8C,bridge=bridge500,firewall=1
Permissions				Network Device (net2)	virtio=BC:24:11:59:6C:A2,bridge=vmbr501,firewall=1

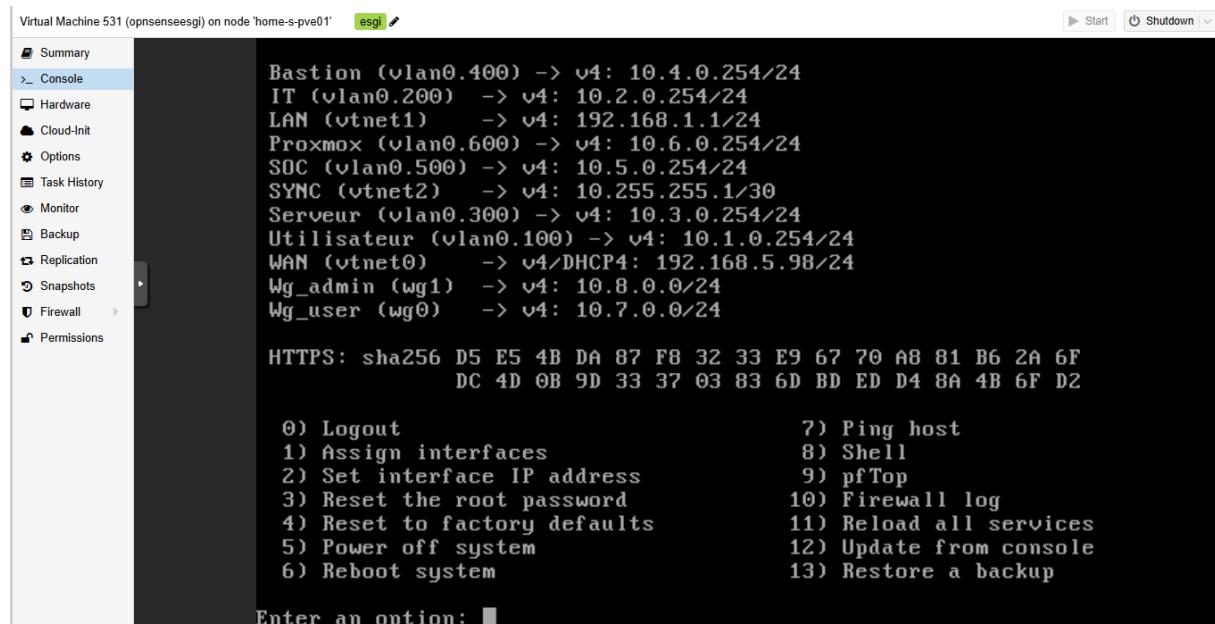
On retrouve 3 interfaces réseaux :

- L'interface vmbr501 qui sera utilisé pour la synchronisation entre les 2 OPNSENSE(s)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- L'interface vmbr500 qui représente la partie WAN (internet)
- L'interface bridge500 qui représente la partie LAN

Pour lancer l'installation il suffit de se connecter avec le compte installer et entrer le mot de passe OPNSENSE. À la suite de cela on peut assigner les interfaces WAN et LAN du firewall :



Il suffit d'assigner l'interface en sélectionnant la bonne et en cliquant sur 1. Puis dans un second temps mettre une IP statique avec le menu en cliquant sur 2. (Dans la capture on retrouve vtнет1 pour le LAN, vtнет0 pour le WAN et vtнет2 pour la synchro entre les 2 FW)

CREATION ET CONFIGURATION DES INTERFACES ET DES VLAN(S)

Dans un second temps nous allons installer sur PROXMOX openvswitch pour configurer un commutateur virtuel :

```
alexis@home-s-pve01:~$ sudo apt install openvswitch-switch  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  proxmox-kernel-6.2.16-19-pve proxmox-kernel-6.5.11-7-pve-signed  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libxdp1 openvswitch-common python3-netifaces python3-openvswitch  
  python3-sortedcontainers uuid-runtime  
Suggested packages:  
  openvswitch-doc python3-netaddr python-sortedcontainers-doc  
The following NEW packages will be installed:  
  libxdp1 openvswitch-common openvswitch-switch python3-netifaces  
  python3-openvswitch python3-sortedcontainers uuid-runtime  
0 upgraded, 7 newly installed, 0 to remove and 154 not upgraded.  
Need to get 4,686 kB of archives.
```

Dans un second temps je créer l'interface virtuelle OVS Bridge pour supporter les différents VLAN. Elle fonctionne comme un switch virtuel.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Edit: OVS Bridge

Name:	bridge500	Autostart:	<input checked="" type="checkbox"/>
IPv4/CIDR:		Bridge ports:	
Gateway (IPv4):		OVS options:	
IPv6/CIDR:		Comment:	VLAN
Gateway (IPv6):			

Advanced OK

Puis je vais créer les interfaces pour les VLANs :

Create: OVS IntPort

Name:	vlan100	OVS Bridge:	bridge500
IPv4/CIDR:		VLAN Tag:	100
Gateway (IPv4):		OVS options:	
IPv6/CIDR:		Comment:	Vlan_utilisateur
Gateway (IPv6):			

Advanced Create

Dans cet exemple je donne le tag 100 pour le vlan utilisateur et je l'associe au switch virtuel bridge500. Je vais faire la même chose pour les différents vlan :

vlan100	OVS IntPort	Yes	Yes	No	Vlan_utilisateur
vlan200	OVS IntPort	Yes	Yes	No	Vlan_IT
vlan300	OVS IntPort	Yes	Yes	No	Vlan_serveur
vlan400	OVS IntPort	Yes	Yes	No	Vlan_Bastion
vlan500	OVS IntPort	Yes	Yes	No	Vlan_SOC
vlan600	OVS IntPort	Yes	Yes	No	Vlan_Proxmox

Puis je me rends sur l'interface OPNSENSE et je peux aller créer des VLAN(s)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Edit Vlan

advanced mode full help

Device	vlan0.100
Parent	vtnet1 (bc:24:11:8b:0c:8c) [LAN]
VLAN tag	100
VLAN priority	Critical Applications (3)
Description	VLAN utilisateur

Cancel Save

Je nomme le premier vlan : vlan0.100 je l'associe à l'interface du LAN et je lui applique son tag. Je recommence pour les différents VLAN(s)

Interfaces, Devices, VLAN					
Device	Parent	Tag	PCP	Description	
vlan0.100 [Utilisateur]	vtnet1 (bc:24:11:8b:0c:8c) [LAN]	100	Best Effort (0, default)	VLAN utilisateur	
vlan0.200 [IT]	vtnet1 (bc:24:11:8b:0c:8c) [LAN]	200	Background (1, lowest)	Vlan IT	
vlan0.300 [Serveur]	vtnet1 (bc:24:11:8b:0c:8c) [LAN]	300	Critical Applications (3)	Vlan Serveur	
vlan0.400 [Bastion]	vtnet1 (bc:24:11:8b:0c:8c) [LAN]	400	Internetwork Control (6)	Vlan Bastion	
vlan0.500 [SOC]	vtnet1 (bc:24:11:8b:0c:8c) [LAN]	500	Excellent Effort (2)	Vlan SOC	
vlan0.600 [Proxmox]	vtnet1 (bc:24:11:8b:0c:8c) [LAN]	600	Best Effort (0, default)	Vlan proxom	

On retrouve les 7 VLAN(s) et on peut appliquer la configuration.

Puis je vais associer au chaque vlan a une interface et appliquer un nom à l'interface :

Interfaces: Assignments			
Interface	Identifier	Device	
[Bastion]	opt4	vlan0.400 Vlan Bastion (Parent: vtnet1, Tag: 400)	
[IT]	opt2	vlan0.200 Vlan IT (Parent: vtnet1, Tag: 200)	
[LAN]	lan	vtnet1 (bc:24:11:8b:0c:8c)	
[Proxmox]	opt7	vlan0.600 Vlan proxom (Parent: vtnet1, Tag: 600)	
[SOC]	opt5	vlan0.500 Vlan SOC (Parent: vtnet1, Tag: 500)	
[SYNC]	opt6	vtnet2 (bc:24:11:59:6ca2)	
[Serveur]	opt3	vlan0.300 Vlan Serveur (Parent: vtnet1, Tag: 300)	
[Utilisateur]	opt1	vlan0.100 VLAN utilisateur (Parent: vtnet1, Tag: 100)	
[WAN]	wan	vtnet0 (bc:24:11:c5:1c4f)	
[Wg_admin]	opt9	wg1 (WireGuard - Wg_admin)	
[Wg_user]	opt8	wg0 (WireGuard - WG_utilisateur)	

Puis je configure une adresse IP pour chaque interface (.254)

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Exemple pour l'interface Utilisateurs

The screenshot shows the configuration page for the 'Utilisateur' interface. It includes sections for generic configuration, static IPv4 configuration, and a note about dynamic gateway policy. The 'Dynamic gateway policy' note states: "This interface does not require an intermediate system to act as a gateway". The static IPv4 configuration section shows an IP address of 10.1.0.254 and a subnet mask of 24.

Setting	Value
Lock	<input type="checkbox"/> Prevent interface removal
Identifier	opt1
Device	vlan0.100
Description	Utilisateur
Generic configuration	
Block private networks	<input type="checkbox"/>
Block bogon networks	<input type="checkbox"/>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC address	[Empty]
Promiscuous mode	<input type="checkbox"/>
MTU	[Empty]
MSS	[Empty]
Dynamic gateway policy	<input type="checkbox"/> This interface does not require an intermediate system to act as a gateway
Static IPv4 configuration	
IPv4 address	10.1.0.254
IPv4 gateway rules	Disabled

Voici une capture pour l'adresse assigné sur chaque interface :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Lobby: Dashboard

Wireguard

Tunnels: 3 | Online: 1 | Offline: 2

- wg0 (WG_utilisateur)
User1 | 10.7.0.1/32
2025-06-14 18:33:40
↓ 190.72 MB | ↑ 612.39 MB
- wg1 (Wg_admin)
Wg_admin | 192.168.5.0/24, 10.8.0.1/32
2025-06-14 15:43:59
↓ 28.35 MB | ↑ 324.23 MB
- wg1 (Wg_admin)
Wg_admin1 | 10.8.0.2/32
Peer disconnected

CARP Status

- Utilisateur @ VHID 10
MASTER 10.1.0.254 (CARP IP)
- IT @ VHID 20
MASTER 10.2.0.254 (CARP IP)
- Serveur @ VHID 30
MASTER 10.3.0.254 (CARP IP)
- Bastion @ VHID 40
MASTER 10.4.0.254 (CARP IP)
- SOC @ VHID 50
MASTER 10.5.0.254 (CARP IP)
- Proxmox @ VHID 60
MASTER 10.6.0.254 (CARP IP)

Interfaces

- WAN
192.168.5.98/24
- LAN
192.168.1.1/24
- SYNC
10.255.255.1/30
- Utilisateur
10.1.0.254/24
- IT
10.2.0.254/24
- Serveur
10.3.0.254/24
- Bastion
10.4.0.254/24
- SOC
10.5.0.254/24
- Proxmox
10.6.0.254/24
- Wg_user
10.7.0.0/24
- Wg_admin
10.8.0.0/24

MISE EN PLACE DU DHCP

Ensuite, je viens appliquer du DHCP sur chaque interface

The screenshot shows a configuration page for a DHCP server. The 'Enable' checkbox is checked. Other options like 'Deny unknown clients' and 'Ignore Client UIDs' are unchecked. The 'Subnet' is set to 10.1.0.0 and the 'Subnet mask' is 255.255.255.0. The 'Available range' is specified as 10.1.0.1 - 10.1.0.254. The 'Range' fields show 'from' as 10.1.0.10 and 'to' as 10.1.0.240.

Pour les utilisateurs on retrouve 230 IP disponible en commençant de 10 à 230.

Pour l'IT je laisse que 100 IP de disponible

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Services: ISC DHCPv4: [IT]

<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable DHCP server on the IT Interface	
<input checked="" type="checkbox"/> Deny unknown clients	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Ignore Client UIDs	<input type="checkbox"/>	
Subnet	10.2.0.0	
Subnet mask	255.255.255.0	
Available range	10.2.0.1 - 10.2.0.254	
Range	from 10.2.0.10	to 10.2.0.110

Pour le VLAN serveur je laisse que 30

Services: ISC DHCPv4: [Serveur]

<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable DHCP server on the Serveur interface	
<input checked="" type="checkbox"/> Deny unknown clients	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Ignore Client UIDs	<input type="checkbox"/>	
Subnet	10.3.0.0	
Subnet mask	255.255.255.0	
Available range	10.3.0.1 - 10.3.0.254	
Range	from 10.3.0.10	to 10.3.0.40

Pour le VLAN Bastion je laisse 2 adresses :

Services: ISC DHCPv4: [Bastion]

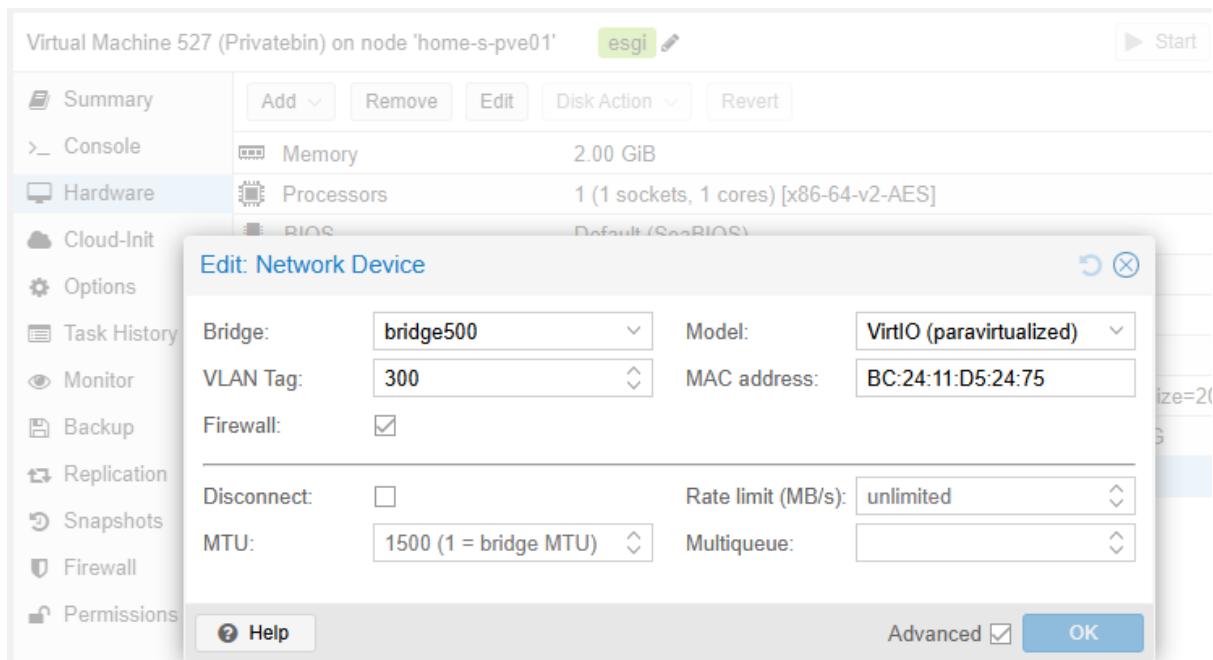
<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable DHCP server on the Bastion interface	
<input checked="" type="checkbox"/> Deny unknown clients	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Ignore Client UIDs	<input type="checkbox"/>	
Subnet	10.4.0.0	
Subnet mask	255.255.255.0	
Available range	10.4.0.1 - 10.4.0.254	
Range	from 10.4.0.10	to 10.4.0.12

Et je fais de même pour les autres Vlans (en changeant le nombre d'IP en fonction du nombre de machine présente)

Vérification du fonctionnement des VLANs

Voici la machine Privatebin, elle se situe dans le VLAN Serveur donc avec le tag 300

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Donc l'adresse que devra obtenir est 10.3.0.10 soit la première IP dans le réseau :

```
tourisk@tourisk:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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
                valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:d5:24:75 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.3.0.10/24 metric 100 brd 10.3.0.255 scope global dynamic ens18
        valid_lft 6921sec preferred_lft 6921sec
        inet6 fe80::be24:11ff:fed5:2475/64 scope link
            valid_lft forever preferred_lft forever
tourisk@tourisk:~$
```

Nous avons bien toute les interfaces avec chaque DHCP qui fonctionne pour chaque VLAN.

HAUTE DISPONIBILITÉ

Je crée une interface sur Proxmox :

VIRTUAL	LINUX DEVICE	TEG	TEG	TEG	LINKS
vmb501	Linux Bridge	Yes	Yes	No	Sync Opnsense

J'assigne l'interface :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Interfaces: Assignments

Interface	Identifier	Device	
[Bastion]	opt4	vlan0.400 Vlan Bastion (Parent: vtne1, Tag: 400)	
[IT]	opt2	vlan0.200 Vlan IT (Parent: vtne1, Tag: 200)	
[LAN]	lan	vtnet1 (bc:24:11:8b:0c:8c)	
[SOC]	opt5	vlan0.500 Vlan SOC (Parent: vtne1, Tag: 500)	
[Serveur]	opt3	vlan0.300 Vlan Serveur (Parent: vtne1, Tag: 300)	
[Utilisateur]	opt1	vlan0.100 VLAN utilisateur (Parent: vtne1, Tag: 100)	
[WAN]	wan	vtne0 (bc:24:11:c5:1c:4f)	

Save

+ Assign a new interface

Device: vtne2 (bc:24:11:59:6:ca2)

Description: SYNC

Add

Puis j'allume l'interface et je lui mets une adresse I

Interfaces: [SYNC]

Basic configuration

<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable interface
<input checked="" type="checkbox"/> Lock	<input type="checkbox"/> Prevent interface removal
<input checked="" type="checkbox"/> Identifier	opt6
<input checked="" type="checkbox"/> Device	vtne2
<input checked="" type="checkbox"/> Description	SYNC

Generic configuration

<input checked="" type="checkbox"/> Block private networks	<input type="checkbox"/>
<input checked="" type="checkbox"/> Block bogon networks	<input type="checkbox"/>
<input checked="" type="checkbox"/> IPv4 Configuration Type	Static IPv4
<input checked="" type="checkbox"/> IPv6 Configuration Type	None
<input checked="" type="checkbox"/> MAC address	<input type="text"/>
<input checked="" type="checkbox"/> Promiscuous mode	<input type="checkbox"/>
<input checked="" type="checkbox"/> MTU	<input type="text"/>
<input checked="" type="checkbox"/> MSS	<input type="text"/>
<input checked="" type="checkbox"/> Dynamic gateway policy	<input type="checkbox"/> This interface does not require an intermediate system to act as a gateway

Hardware settings

<input checked="" type="checkbox"/> Overwrite global settings	<input type="checkbox"/>
---	--------------------------

Static IPv4 configuration

<input checked="" type="checkbox"/> IPv4 address	<input type="text"/> 10.255.255.1	30
<input checked="" type="checkbox"/> IPv4 gateway rules	Disabled	

Save **Cancel**

Je choisi de mettre que 2 IP disponibles car il y a que 2 serveurs. Puis je fais la même chose sur le second coté.

Assignment de l'interface :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the 'Interfaces: Assignments' page in the OPNsense web interface. On the left, a sidebar lists various system sections like 'Lobby', 'Reporting', 'System', 'Interfaces', 'Assignments', 'Devices', 'Neighbors', 'Overview', 'Settings', 'Virtual IPs', 'Wireless', 'Diagnostics', 'Firewall', 'VPN', 'Services', 'Power', and 'Help'. The 'Interfaces' section is selected. The main panel displays a table of interface assignments:

Interface	Identifier	Device
[Bastion]	opt4	vlan0.400 Vlan Bastion (Parent: vtne1, Tag: 400)
[IT]	opt2	vlan0.200 Vlan IT (Parent: vtne1, Tag: 200)
[LAN]	lan	vtne1 (bc:24:11:5f:50:eb)
[SOC]	opt5	vlan0.500 Vlan SOC (Parent: vtne1, Tag: 500)
[Serveur]	opt3	vlan0.300 Vlan Serveur (Parent: vtne1, Tag: 300)
[Utilisateur]	opt1	vlan0.100 VLAN utilisateur (Parent: vtne1, Tag: 100)
[WAN]	wan	vtne0 (bc:24:11:27:46:b2)

Below the table, there's a 'Save' button and a 'Assign a new interface' section with a dropdown for 'Device' (set to 'vtne2') and a 'Description' field ('SYNC'). A red 'Add' button is also present.

Mise en place de l'adresse IP :

The screenshot shows the configuration page for interface [WAN]. The interface is named 'wan' and is assigned to the device 'vtne0'. The configuration includes:

- Basic configuration:** Includes fields for 'Enable' (checked), 'Lock' (unchecked), 'Identifier' (opt6), 'Device' (vtne2), and 'Description' (SYNC).
- Generic configuration:** Includes fields for 'Block private networks' (unchecked), 'Block bogon networks' (unchecked), 'IPv4 Configuration Type' (Static IPv4), 'IPv6 Configuration Type' (None), 'MAC address' (empty), 'Promiscuous mode' (unchecked), 'MTU' (empty), 'MSS' (empty), and 'Dynamic gateway policy' (unchecked).
- Hardware settings:** Includes a 'Overwrite global settings' checkbox (unchecked).
- Static IPv4 configuration:** Includes fields for 'IPv4 address' (10.255.255.2) and 'IPv4 gateway rules' (Disabled).

Enfin je peux créer des IP virtuel avec des interfaces en mode CARP

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Interfaces: Virtual IPs: Settings

Address	VHID	Interface	Type	Description	Commands
10.1.0.254/24	10 (freq. 1/0)	Utilisateur	CARP	CARP for VLAN 100	
10.2.0.254/24	20 (freq. 1/0)	IT	CARP	Carp for VLAN 200	
10.3.0.254/24	30 (freq. 1/0)	Serveur	CARP	Carp for VLAN 300	
10.4.0.254/24	40 (freq. 1/0)	Bastion	CARP	Carp for VLAN 400	
10.5.0.254/24	50 (freq. 1/0)	SOC	CARP	Carp for vlan 500	
10.6.0.254/24	60 (freq. 1/0)	Proxmox	CARP	Carp for Vlan 600	

Showing 1 to 6 of 6 entries

Edit Virtual IP

advanced mode full help

Mode: CARP

Interface: Proxmox

Network / Address: 10.6.0.254/24

Gateway:

Peer (IPv4): 224.0.0.18

Peer (IPv6): ff02::12

Deny service binding:

Password:

VHID Group: 60 Select an unassigned VHID

advbase: 1

advskew: 0

Description: Carp for Vlan 600

Cancel Save

Voici toutes les Virtual IP configurées (sur les 2 serveurs)

Interfaces: Virtual IPs: Settings

Address	VHID	Interface	Type	Description	Commands
10.1.0.254/24	10 (freq. 1/0)	Utilisateur	CARP	CARP for VLAN 100	
10.2.0.254/24	20 (freq. 1/0)	IT	CARP	Carp for VLAN 200	
10.3.0.254/24	30 (freq. 1/0)	Serveur	CARP	Carp for VLAN 300	
10.4.0.254/24	40 (freq. 1/0)	Bastion	CARP	Carp for VLAN 400	
10.5.0.254/24	50 (freq. 1/0)	SOC	CARP	Carp for vlan 500	

Showing 1 to 5 of 5 entries

apply

Puis je vais dans l'onglet haute disponibilité pour configurer le second serveur :

OPNsense® <

Lobby Reporting System Access Configuration Firmware Gateways High Availability Settings Status Routes Settings Snapshots Trust Wizard Log Files Diagnostics Interfaces Firewall VPN Services Power Help

System: High Availability: Settings

General Settings

Disable preempt:

Disconnect dialup interfaces:

Synchronize all states via: SYNC

Sync compatibility: OPNsense 24.7 or above

Synchronize Peer IP: 10.255.255.2

Configuration Synchronization Settings (XMLRPC Sync) Perform synchronization

Synchronize Config: 10.255.255.2

Verify peer:

Remote System Username: root

Remote System Password:

Services to synchronize (XMLRPC Sync)

Services: Aliases, Auth Servers, Backup - Google Drive, Capt ▾

Clear All Select All

Apply

Sur le second serveur :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the OPNsense web interface under the 'System' menu, specifically the 'High Availability' settings. The page title is 'System: High Availability: Settings'. It contains several configuration sections:

- General Settings:**
 - Disable preempt: checked
 - Disconnect dialup interfaces: checked
 - Synchronize all states via: SYNC
 - Sync compatibility: OPNsense 24.7 or above
 - Synchronize Peer IP: 10.255.255.1
- Configuration Synchronization Settings (XMLRPC Sync):** Includes fields for Synchronize Config, Verify peer (unchecked), Remote System Username, and Remote System Password.
- Services to synchronize (XMLRPC Sync):** Services listed: Nothing selected. Buttons: Clear All, Select All.

At the bottom is a red 'Apply' button.

Dans l'onglet Status, je retrouve les informations du serveur secondaire

The screenshot shows the OPNsense web interface under the 'System' menu, specifically the 'Status' section of the 'High Availability' settings. The page title is 'System: High Availability: Status'. It displays two tables:

Backup firewall versions		Base	Kernel
Firmware	25.1	25.1	25.1

Service	Description	Status
configd	System Configuration Daemon	Green
cron	Cron	Green
dhcpcd	DHCPv4 Server	Green
dhcpd6	DHCPv6 Server	Green
login	Users and Groups	Green
ntpdate	Network Time Daemon	Green
pf	Packet Filter	Green

At the bottom right, it says 'Showing 1 to 7 of 12 entries'.

Sur le Dashboard je me rajoute un widget avec le Status des Virtual IP(s) en mode CARP :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the OpenSense UI Dashboard. On the left, a sidebar lists navigation options like Lobby, Dashboard, License, Password, Logout, Reporting, System, Interfaces, Firewall, VPN, Services, Power, and Help. The main area is divided into three sections: 'System Information' (Name: OPNsense.localdomain, Versions: OPNsense 25.1-amd64, OpenSSL 3.0.15), 'CARP Status' (listing various nodes like Utilisateur @ VHID 10, IT @ VHID 20, etc., all in Master mode), and 'Interfaces' (listing WAN, LAN, SYNC, Utilisateur, IT, Server, Bastion, SOC, Proxmox, and several Virtual IP (VIP) entries). A central dashboard displays CPU usage (QEMU Virtual CPU version 2.5+ (4 cores, 4 threads)) and memory/disk usage.

Sur le serveur slave on retrouve les Virtual IP en mode backup

This screenshot shows two windows of the OpenSense UI. The left window displays the 'CARP Status' section, which lists the same nodes as the main dashboard but with a red border around the 'Virtual IP' entries. The right window shows the 'Status | Virtual IPs | Interfaces' page, specifically the 'Virtual IPs: Status' section. It lists several VIP entries, each with a red border, and shows their assigned VHDs and addresses. A red box highlights the table of virtual IP assignments.

Interface	VHD	Address	Status
Utilisateur	10 (freq. 1/100)	19.1.0.254	► BACKUP
IT	20 (freq. 1/100)	19.2.0.254	► BACKUP
Server	30 (freq. 1/100)	19.3.0.254	► BACKUP
Bastion	40 (freq. 1/100)	19.4.0.254	► BACKUP
SOC	50 (freq. 1/100)	19.5.0.254	► BACKUP
Proxmox	40 (freq. 1/100)	19.6.0.254	► BACKUP

MISE EN PLACE DES 2 VPN (ADMINS-UTILISATEURS)

Création d'une instance Wireguard pour les utilisateurs :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the OPNsense web interface for managing a WireGuard VPN. On the left, a sidebar lists various network components like Reporting, System, Interfaces, Firewall, IPsec, OpenVPN, and WireGuard. The main panel is titled 'VPN: WireGuard' and contains three tabs: 'Instances', 'Peers', and 'Peer generator'. The 'Instances' tab is selected, displaying a list of instances with their status (Enabled or Disabled). A specific instance, 'WG_utilisateur', is highlighted. A modal window titled 'Edit instance' is open, showing detailed configuration options: Name (WG_utilisateur), Instance (0), Public key (a long hex string), Private key (another long hex string), Listen port (51821), Tunnel address (10.7.0.0/24), Depend on (CARP), Peers (User1), and Disable routes. Buttons for 'Cancel' and 'Save' are at the bottom right of the modal.

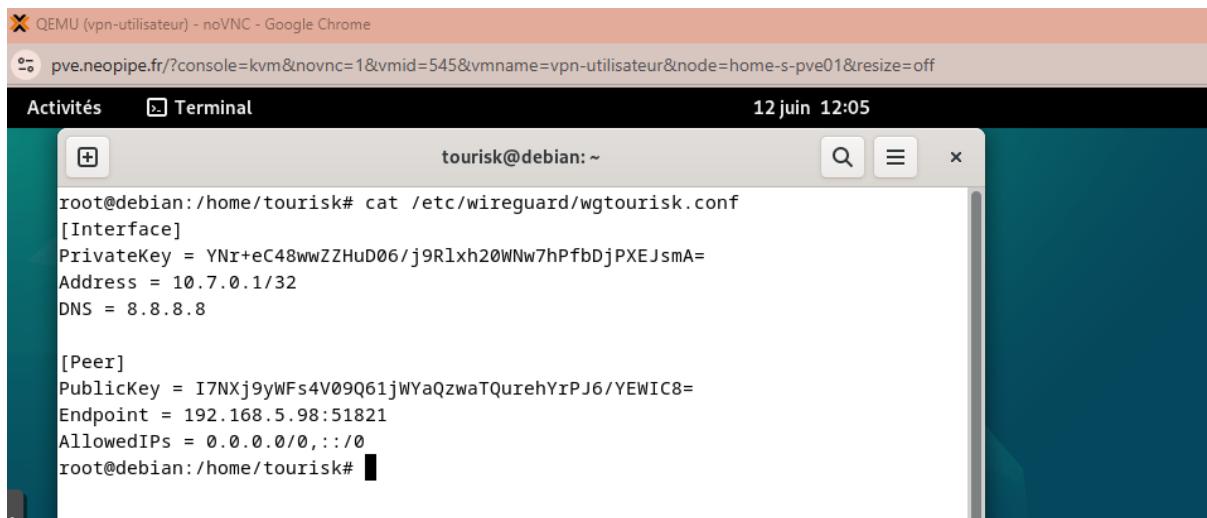
On retrouve une paire de clé, le port en écoute, le nom et l'adresse du tunnel.

Dans un second temps je vais ajouter un Peer avec l'onglet Peer Generator :

The screenshot shows the 'Peer generator' tab of the OPNsense WireGuard configuration. It allows generating a peer configuration for an existing instance. The 'Peer generator' tab is selected. The configuration fields include: Instance (WG_utilisateur), Endpoint (192.168.5.98:51821), Name (User1), Public key (a long hex string), Private key (a long hex string), Address (10.7.0.1/32), Pre-shared key (a placeholder field), Allowed IPs (0.0.0.0/0::/0), Keepalive interval (8.8.8.8), DNS Servers (8.8.8.8), and Config (a text area containing the generated configuration). Below the fields is a QR code. At the bottom, there are buttons for 'Store and generate next' and 'Enable WireGuard'.

Ont choisi le nom d'utilisateur du client, son adresse ip puis on set la machine publique et le port associé au Firewall.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



The screenshot shows a terminal window titled "Terminal" running on a Debian system. The window title is "tourisk@debian: ~". The terminal displays the output of the command "cat /etc/wireguard/wgtourisk.conf". The configuration file contains the following sections:

```
root@debian:/home/tourisk# cat /etc/wireguard/wgtourisk.conf
[Interface]
PrivateKey = YNr+eC48wwZZHuD06/j9Rlxh20WNw7hPfbDjPXEJsmA=
Address = 10.7.0.1/32
DNS = 8.8.8.8

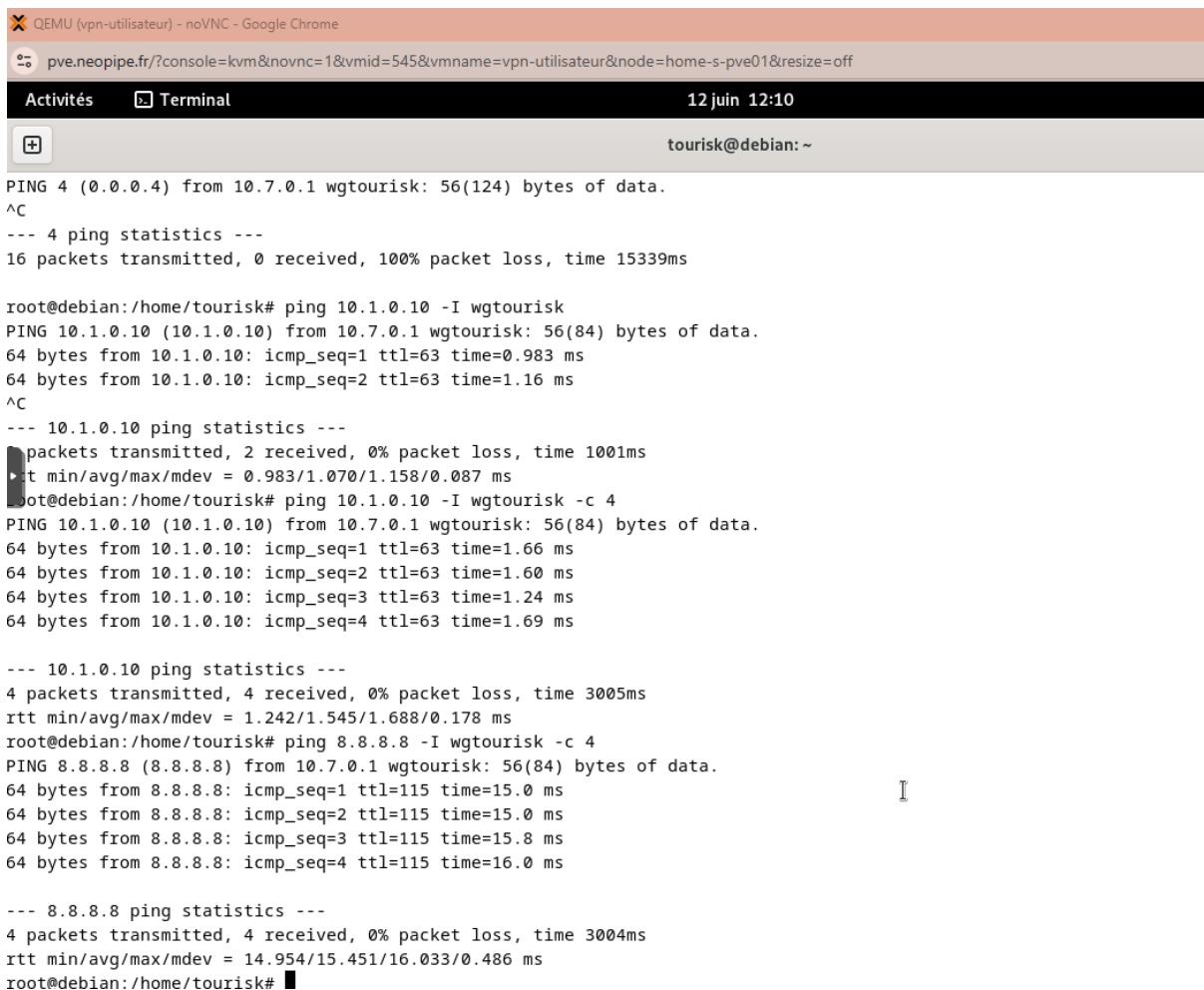
[Peer]
PublicKey = I7NXj9yWFs4V09Q61jWYaQzwaTQurehYrPJ6/YEWIC8=
Endpoint = 192.168.5.98:51821
AllowedIPs = 0.0.0.0/0,::/0
root@debian:/home/tourisk#
```

Je lance la configuration avec la commande

Sudo wg-quick up wgtourisk

Puis je teste la connexion vers internet et un autre réseau :

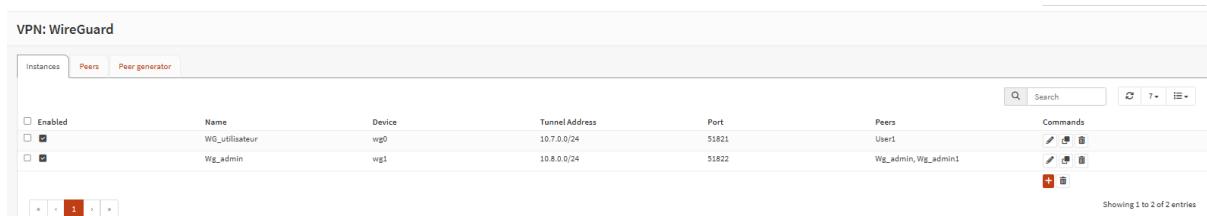
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



The screenshot shows a terminal window titled "QEMU (vpn-utilisateur) - noVNC - Google Chrome" with the URL "pve.neopipe.fr/?console=kvm&novnc=1&vmid=545&vmname=vpn-utilisateur&node=home-s-pve01&resize=off". The terminal window has tabs for "Activités" and "Terminal". The date and time at the top right are "12 juin 12:10". The user is "tourisk@debian: ~". The terminal output shows several ping commands:

```
PING 4 (0.0.0.4) from 10.7.0.1 wgtourisk: 56(124) bytes of data.  
^C  
--- 4 ping statistics ---  
16 packets transmitted, 0 received, 100% packet loss, time 15339ms  
  
root@debian:/home/tourisk# ping 10.1.0.10 -I wgtourisk  
PING 10.1.0.10 (10.1.0.10) from 10.7.0.1 wgtourisk: 56(84) bytes of data.  
64 bytes from 10.1.0.10: icmp_seq=1 ttl=63 time=0.983 ms  
64 bytes from 10.1.0.10: icmp_seq=2 ttl=63 time=1.16 ms  
^C  
--- 10.1.0.10 ping statistics ---  
packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 0.983/1.070/1.158/0.087 ms  
root@debian:/home/tourisk# ping 10.1.0.10 -I wgtourisk -c 4  
PING 10.1.0.10 (10.1.0.10) from 10.7.0.1 wgtourisk: 56(84) bytes of data.  
64 bytes from 10.1.0.10: icmp_seq=1 ttl=63 time=1.66 ms  
64 bytes from 10.1.0.10: icmp_seq=2 ttl=63 time=1.60 ms  
64 bytes from 10.1.0.10: icmp_seq=3 ttl=63 time=1.24 ms  
64 bytes from 10.1.0.10: icmp_seq=4 ttl=63 time=1.69 ms  
  
--- 10.1.0.10 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 1.242/1.545/1.688/0.178 ms  
root@debian:/home/tourisk# ping 8.8.8.8 -I wgtourisk -c 4  
PING 8.8.8.8 (8.8.8.8) from 10.7.0.1 wgtourisk: 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=15.0 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=15.0 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=15.8 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=16.0 ms  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 14.954/15.451/16.033/0.486 ms  
root@debian:/home/tourisk#
```

Je vais la même chose pour le VPN admin mais je crée un Peer qui se nomme wg_admin



The screenshot shows a "VPN: WireGuard" interface. At the top, there are tabs for "Instances", "Peers", and "Peer generator". The "Instances" tab is selected. Below the tabs is a search bar and some filter options. A table lists two instances:

Enabled	Name	Device	Tunnel Address	Port	Peers	Commands
<input type="checkbox"/>	WG_utilisateur	wg0	10.7.0.0/24	51821	User1	
<input type="checkbox"/>	Wg_admin	wg1	10.8.0.0/24	51822	Wg_admin, Wg_admin1	

At the bottom left, there are navigation buttons for pages 1 and 2. A message at the bottom right says "Showing 1 to 2 of 2 entries".

On retrouve la seconde instance Wireguard

Puis, je vais ensuite créer le Peer :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Edit peer

full help 

Enabled	<input checked="" type="checkbox"/>
Name	Wg_admin
Public key	7plaBb2rAcQot7xA+v1nFGu782j37CZQKv4F0oqY...
Pre-shared key	
Allowed IPs	10.8.0.1/32    
Endpoint address	
Endpoint port	
Instances	Wg_admin 
Keepalive interval	

Je teste la connexion de la même manière et cela fonctionne. Dans cette partie je ne montre pas les règles firewall mise en place sur les différentes interfaces. Elles sont dans l'étape suivante du guide d'installation.

CONFIGURATION DES REGLES DE FIREWALL

Les utilisateurs ont besoin d'accéder uniquement au vlan serveur pour pouvoir interagir avec le Keycloak et Privatebin. Ils ont évidemment besoin d'accéder à internet.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Firewall: Rules: Utilisateur

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Action
<input type="checkbox"/>	IPv4 TCP	Utilisateur net	*	*	80 (HTTP)	*	*	Automatically generated rules	
<input type="checkbox"/>	IPv4 TCP	Utilisateur net	*	*	443 (HTTPS)	*	*	Autoriser le https	
<input type="checkbox"/>	IPv4 TCP/UDP	Utilisateur net	*	*	53 (DNS)	*	*	Autoriser le DNS	
<input type="checkbox"/>	IPv4 *	*	*	Serveur net	*	*	*	Autoriser le VLAN Serveur	
<input type="checkbox"/>	IPv4 *	Utilisateur net	*	10.5.0.26	*	*	*	Autoriser le Wazuh	
	pass	(disabled)							
	pass (disabled)								
	Active/Inactive Schedule								
	Alias (click to view/edit)								
Utilisateur rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.									

```
home-s-pve01 - Proxmox Console - Google Chrome
pve.neopeipe.fr/?console=tcc&xtermjs=1&vmid=535&vmname=utilisateur&node=home-s-pve01&cmd=
root@utilisateur:~# wget google.com
--2025-06-14 09:21:42-- http://google.com/
Resolving google.com (google.com) ... 172.217.20.174, 2a00:1450:4007:80c::200e
Connecting to google.com (google.com)|172.217.20.174|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com [following]
--2025-06-14 09:21:42-- https://www.google.com/
Resolving www.google.com (www.google.com) ... 172.217.20.196, 2a00:1450:4007:810::2004
Connecting to www.google.com (www.google.com)|172.217.20.196|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.2'

index.html.2 [=>] 17.17K --.-KB/s in 0.01s
2025-06-14 09:21:42 (1.24 MB/s) - 'index.html.2' saved [17585]

root@utilisateur:~# ping -c 1 10.5.0.26
PING 10.5.0.26 (10.5.0.26) 56(84) bytes of data.
64 bytes from 10.5.0.26: icmp_seq=1 ttl=63 time=0.704 ms

--- 10.5.0.26 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.704/0.704/0.704/0.000 ms
root@utilisateur:~# ping -c 1 10.3.0.10
PING 10.3.0.10 (10.3.0.10) 56(84) bytes of data.
64 bytes from 10.3.0.10: icmp_seq=1 ttl=63 time=0.817 ms

--- 10.3.0.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.817/0.817/0.817/0.000 ms

```

On retrouve une tentative d'accès à internet en HTTPS + résolution DNS et 2 ping valide vers le Wazuh et le le Privatebin

Les administrateurs ont besoin d'accéder à tous les services sur tous les vlan :

Firewall: Rules: IT

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Action
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	*	Automatically generated rules	
	pass	(disabled)		block		block (disabled)		reject	
	pass (disabled)		block		block (disabled)		reject (disabled)		
	Active/Inactive Schedule (click to view/edit)								
	Alias (click to view/edit)								
IT rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.									

Les serveurs ont besoin d'accéder à internet et de pouvoir communiquer avec le wazuh pour l'agent aussi.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Firewall: Rules: Serveur

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 TCP	Serveur net	*	*	80 (HTTP)	*	*	Autoriser le http
IPv4 TCP	Serveur net	*	*	443 (HTTPS)	*	*	Autoriser le https
IPv4 TCP/UDP	Serveur net	*	*	53 (DNS)	*	*	Autoriser le DNS
IPv4 *	Serveur net	*	10.5.0.26	*	*	*	Autoriser le Wazuh

```

pass (disabled) X QEMU (Privatebin) - noVNC - Google Chrome
https://pve.neopipe.fr/?console=kvm&novnc=1&vmid=527&vmname=Privatebin&node=home-s-pve01&resize=off&cmd=
Active/Inactive
Alias (click to view/edit)
Server rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

tourisk@tourisk:~$ wget google.com
--2025-06-14 09:25:29 Resolving google.com (www.google.com) ... 172.217.20.174, 2a00:1450:4007:800::2000
--2025-06-14 09:25:29 Connecting to www.google.com (www.google.com)|172.217.20.174|:80... connected.
--2025-06-14 09:25:29 HTTP request sent, awaiting response... 301 Moved Permanently
--2025-06-14 09:25:29 Location: http://www.google.com/ [following]
--2025-06-14 09:25:29 Resolving www.google.com (www.google.com) ... 172.217.20.196, 2a00:1450:4007:8100::2004
--2025-06-14 09:25:29 Connecting to www.google.com (www.google.com)|172.217.20.196|:80... connected.
--2025-06-14 09:25:29 HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html
[ <> ] 16.87K --.-KB/s in 0.003s

2025-06-14 09:25:29 (5.92 MB/s) - "index.html" saved [17275]

tourisk@tourisk:~$ ping -c 1 10.5.0.26
PING 10.5.0.26 (10.5.0.26) 56(84) bytes of data.
64 bytes from 10.5.0.26: icmp_seq=1 ttl=63 time=1.30 ms
--> 10.5.0.26 ping statistics ---
packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.295/1.295/1.295/0.000 ms
tourisk@tourisk: ~

```

Le bastion doit pouvoir communiquer avec tous les serveurs :

Firewall: Rules: Bastion

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 *	*	*	*	*	*	*	Automatically generated rules
pass (disabled)	X block (disabled)	reject (disabled)	log (disabled)	in	out		first match last match

Le Wire guard utilisateur doit pouvoir communiquer avec internet et les serveurs :

Firewall: Rules: Wg_user

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 TCP	Wg_user net	*	*	80 (HTTP)	*	*	Autoriser le http
IPv4 TCP/UDP	Wg_user net	*	*	53 (DNS)	*	*	Autoriser le DNS
IPv4 TCP	Wg_user net	*	*	443 (HTTPS)	*	*	Autoriser le https
IPv4 *	Wg_user net	*	Serveur net	*	*	*	Autoriser le VLAN serveur

```

pass (disabled) X block (disabled)
reject (disabled)
log (disabled)
In
out
first match
last match

Wg_user rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

tourisk@tourisk:~$ wget google.com
--2025-06-14 09:25:29 Resolving google.com (www.google.com) ... 172.217.20.174, 2a00:1450:4007:800::2000
--2025-06-14 09:25:29 Connecting to www.google.com (www.google.com)|172.217.20.174|:80... connected.
--2025-06-14 09:25:29 HTTP request sent, awaiting response... 301 Moved Permanently
--2025-06-14 09:25:29 Location: http://www.google.com/ [following]
--2025-06-14 09:25:29 Resolving www.google.com (www.google.com) ... 172.217.20.196, 2a00:1450:4007:8100::2004
--2025-06-14 09:25:29 Connecting to www.google.com (www.google.com)|172.217.20.196|:80... connected.
--2025-06-14 09:25:29 HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html
[ <> ] 16.87K --.-KB/s in 0.003s

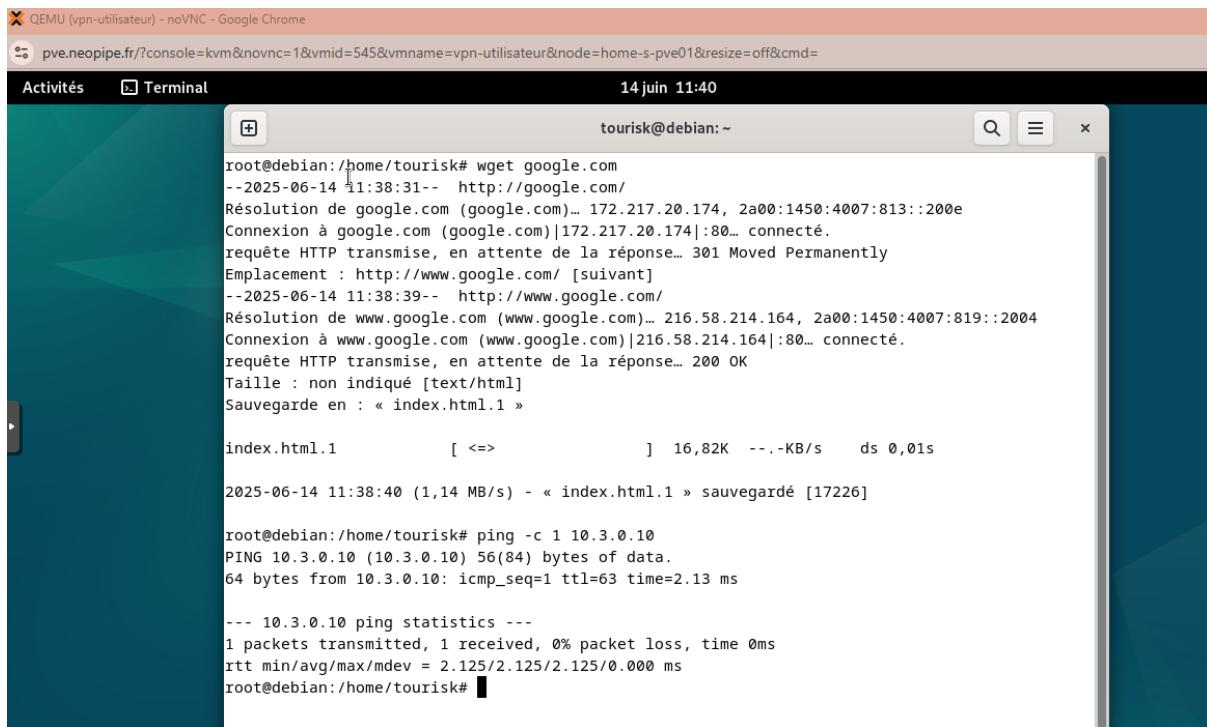
2025-06-14 09:25:29 (5.92 MB/s) - "index.html" saved [17275]

tourisk@tourisk:~$ ping -c 1 10.5.0.26
PING 10.5.0.26 (10.5.0.26) 56(84) bytes of data.
64 bytes from 10.5.0.26: icmp_seq=1 ttl=63 time=1.30 ms
--> 10.5.0.26 ping statistics ---
packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.295/1.295/1.295/0.000 ms
tourisk@tourisk: ~

```

Voici la démonstration des communications :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



```
tourisk@debian:~/home/tourisk# wget google.com
--2025-06-14 11:38:31--  http://google.com/
Résolution de google.com (google.com)... 172.217.20.174, 2a00:1450:4007:813::200e
Connexion à google.com (google.com)|172.217.20.174|:80... connecté.
requête HTTP transmise, en attente de la réponse... 301 Moved Permanently
Emplacement : http://www.google.com/ [suivant]
--2025-06-14 11:38:39--  http://www.google.com/
Résolution de www.google.com (www.google.com)... 216.58.214.164, 2a00:1450:4007:819::2004
Connexion à www.google.com (www.google.com)|216.58.214.164|:80... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : non indiqué [text/html]
Sauvegarde en : « index.html.1 »

index.html.1          [ <= ]           16,82K  --.-KB/s   ds 0,01s

2025-06-14 11:38:40 (1,14 MB/s) - « index.html.1 » sauvegardé [17226]

root@debian:~/home/tourisk# ping -c 1 10.3.0.10
PING 10.3.0.10 (10.3.0.10) 56(84) bytes of data.
64 bytes from 10.3.0.10: icmp_seq=1 ttl=63 time=2.13 ms

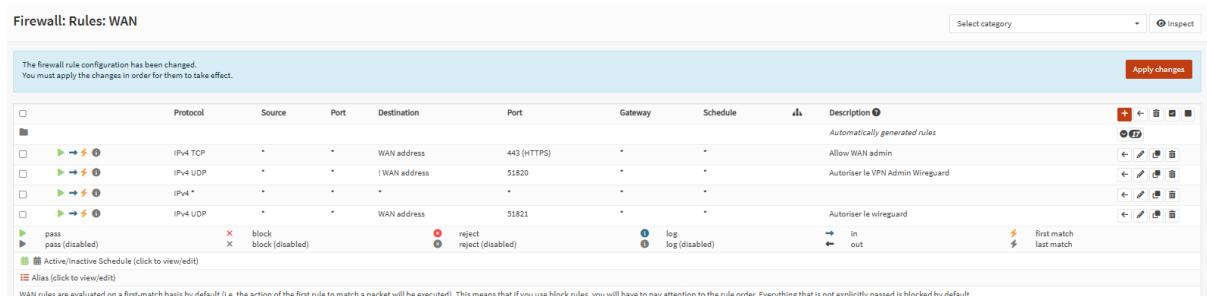
--- 10.3.0.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.125/2.125/2.125/0.000 ms
root@debian:~/home/tourisk#
```

Le Wire Guard administrateur doit pouvoir accéder à tous :



Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 *	Wg_admin net	*	*	*	*	*	Automatically generated rules
pass	block	*	*	*	*	*	reject
pass (disabled)	block (disabled)	*	*	*	*	*	reject (disabled)

Coté WAN j'ai mis en place 3 règles, une pour l'administration depuis le WAN de l'interface opnsense. Puis une autorisation pour les 2 VPN(s)



Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	*	Allow WAN admin
IPv4 UDP	*	*	!WAN address	51820	*	*	Autoriser le VPN Admin Wireguard
IPv4 *	*	*	*	*	*	*	Autoriser le wireguard
pass	block	*	*	*	*	*	reject
pass (disabled)	block (disabled)	*	*	*	*	*	reject (disabled)

Dans cette capture on retrouve un Pass All pour vérifier le bon fonctionnement du VPN. Mais il n'est pas utile.

Voici le Status des 2 VPN(s) :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the OPNsense web interface under the 'VPN' section, specifically the 'WireGuard' tab. The left sidebar includes links for Lobby, Reporting, System, Interfaces, Firewall, and VPN (IPsec, OpenVPN, WireGuard, Instances, Peers, Peer generator, Status, Log File). The main content area is titled 'VPN: WireGuard: Status' and displays a table of current connections. The table has columns for Device, Status, Public key, Name, Port / Endpoint, Handshake, Send, and Received. There are two entries:

Device	Status	Public key	Name	Port / Endpoint	Handshake	Send	Received
vg0	up	... (long hex string)	Wg_utilisateur	51821	2025-06-14 18:33:40	584.02 MB	181.88 MB
vg0	up	... (long hex string)	User1	192.168.5.12:40517			
vg1	up	pan+e=0B... (long hex string)	Wg_admin	51822			
vg1	up	tpLabB24Q... (long hex string)	Wg_admin	192.168.5.14:56687	2025-06-14 15:43:59	309.21 MB	27.04 MB
vg1	up	VQGDYEM2N4gw... (long hex string)	Wg_admin1	(none)		0	0

At the bottom right, it says 'Showing 1 to 5 of 5 entries'.

ANNEXE INSTALLATION ET UTILISATEUR DU TPOT.

INSTALLATION DU TPOT

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Installation d'une machine virtuelle Debian 12 :

The screenshot shows the Proxmox VE interface for managing a virtual machine named 'tpot'. The left sidebar lists various management options like Summary, Console, Hardware, Cloud-Init, Options, Task History, Monitor, Backup, Replication, Snapshots, Firewall, and Permissions. The main panel displays hardware specifications: Memory (16.00 GiB), Processors (6 cores), BIOS (Default SeaBIOS), Display (Default), Machine (Default i440fx), SCSI Controller (VirtIO SCSI single), CD/DVD Drive (ide2) with ISO path local:/iso/debian-12.2.0-amd64-netinst.iso, Hard Disk (scsi0) with LVM path local:lvm:vm-550-disk-0, and Network Device (net0) with virtio settings. A green status bar at the top right indicates 'esgi'.

Il faut configurer un disque de 100Go minimum et plus de 15 go de RAM.

Dans un second temps il faut créer un utilisateur, l'ajouter dans le groupe sudoers puis télécharger le GitHub de TPOT.

git clone <https://github.com/telekom-security/tpotce>

Puis lancer l'installation :

```
tourisk@debian:~$ ls
Bureau  Documents  Images  Modèles  Musique  Public  Téléchargements  tpotce  Vidéos
tourisk@debian:~$ cd tpotce/
tourisk@debian:~/tpotce$ ./install.sh -type=user
[Progress Bar]
### This script will now install T-Pot and all of its dependencies.
### Install? (y/n)
```

Dans l'installation on spécifie h pour choisir le mode ruche et installé ELK, Kibana et l'outil Spiderfoot.

Une fois l'installation terminé nous devons reboot la machine puis accèder au serveur :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

```
✓miniprint Pulled
✓suricata Pulled
✓tpoinit Pulled
✓logstash Pulled
✓heralding Pulled
✓map_data Pulled
✓honeypot Pulled
✓proxy Pulled
✓adbhoneyp Pulled
✓honeymtrap Pulled
✓wordpot Pulled
✓eusposter Pulled
✓tanner_api Pulled
✓elasticscanner Pulled
✓phish Pulled
✓dionaea Pulled
✓ciscosasa Pulled
✓map_redis Pulled
✓fatt Pulled
✓medgot Pulled
✓redissharding Pulled
✓proxy Pulled
✓elastictcpot Pulled
✓sentrypeer Pulled
✓kibana Pulled
✓honeyptrp Pulled
✓mailoney Pulled

13.5s
34.5s
39.2s
59.6s
9.6s
42.3s
37.3s
22.5s
42.2s
59.5s
28.1s
35.6s
25.2s
59.1s
13.1s
49.6s
32.7s
39.2s
27.2s
10.5s
37.0s
17.5s
26.4s
35.9s
82.7s
7.8s
43.6s

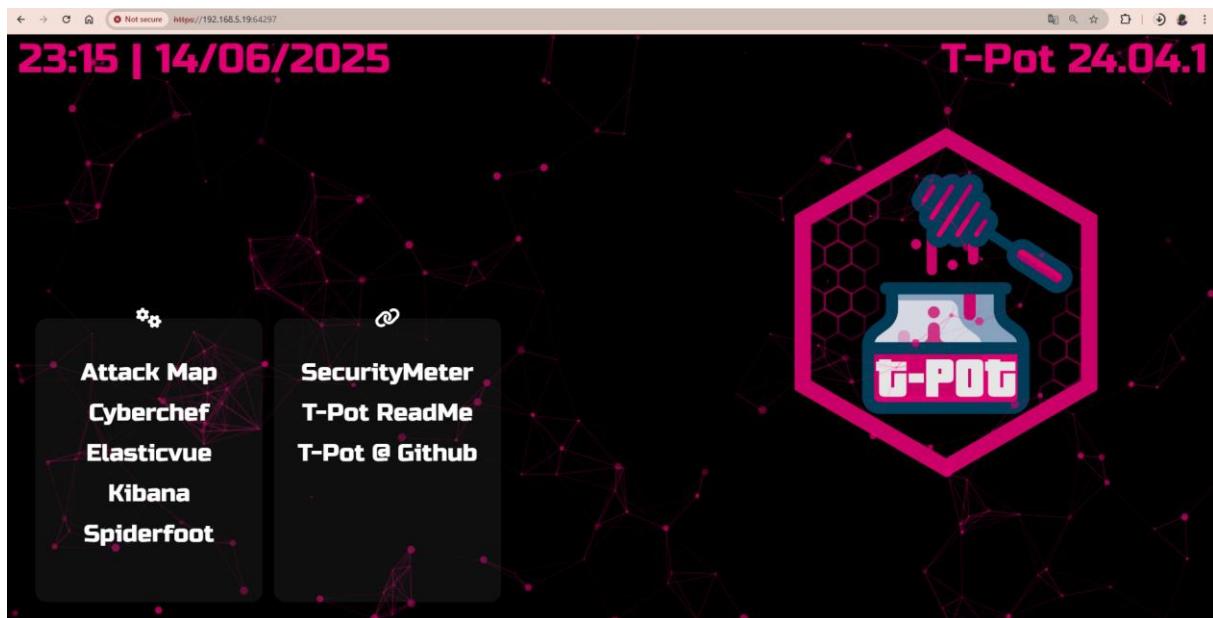
## Please review for possible honeypot port conflicts.
## While SSH is taken care of, other services such as
## SMTP, HTTP, etc. might prevent T-Pot from starting.

Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale           Adresse distante      Etat      Utilisatr  Inode      PID/Program name
tcp     0      0 0.0.0.0:64295              0.0.0.0:*          LISTEN    0          42548   14311/sshd: /usr/sb
tcp6    0      0 ::ffff:64295                ::*:             LISTEN    0          42550   14311:sshd: /usr/sb
udp    0      0 0.0.0.0:68                  0.0.0.0:*          0          13085   430/dhcclient

## Done. Please reboot and re-connect via SSH on tcp/64295.

adminuser@tnt01:~/tptools$
```

Page de démarrage du serveur :

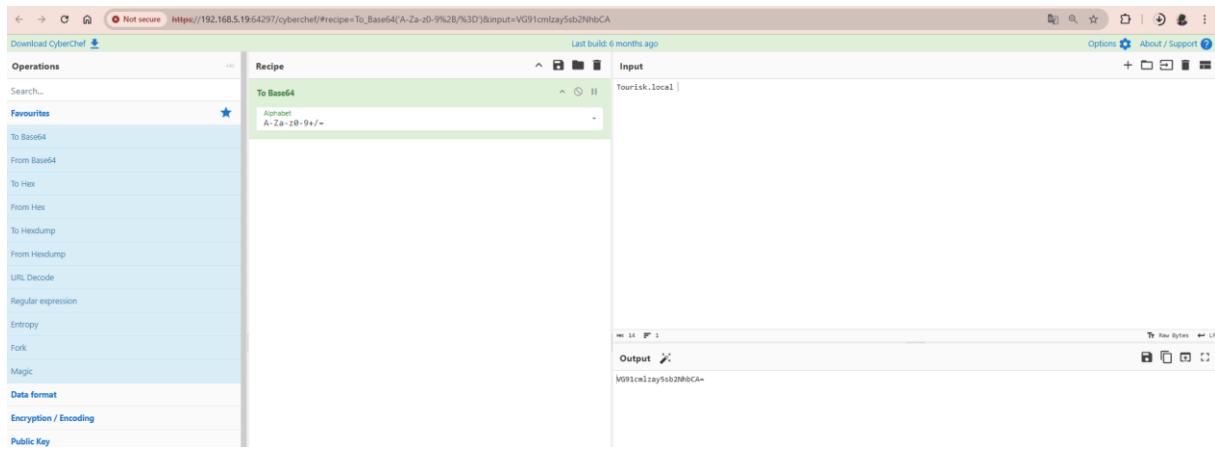


On retrouve différentes fonctionnalités, comme l'attaque map, cyberchef Elasticcvue, Kibana et Spiderfoot.

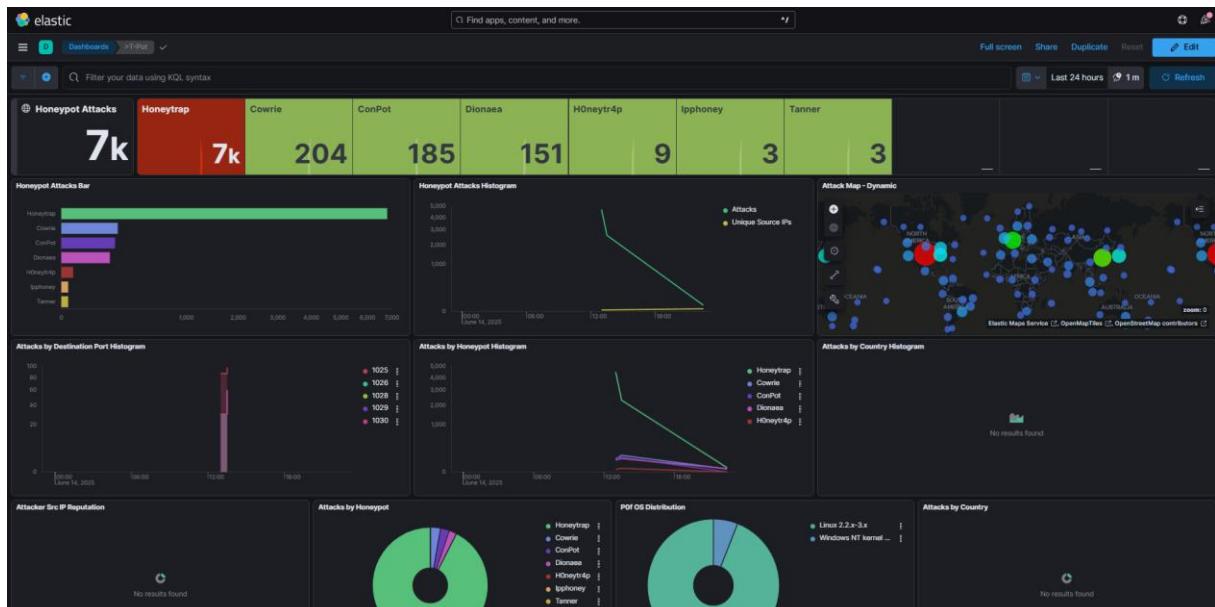
L'interface Attack map permet de voir un aperçu de la localisation des différentes attaques.

On retrouve Cyberchef, une application web pour chiffrer et déchiffrer du texte :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

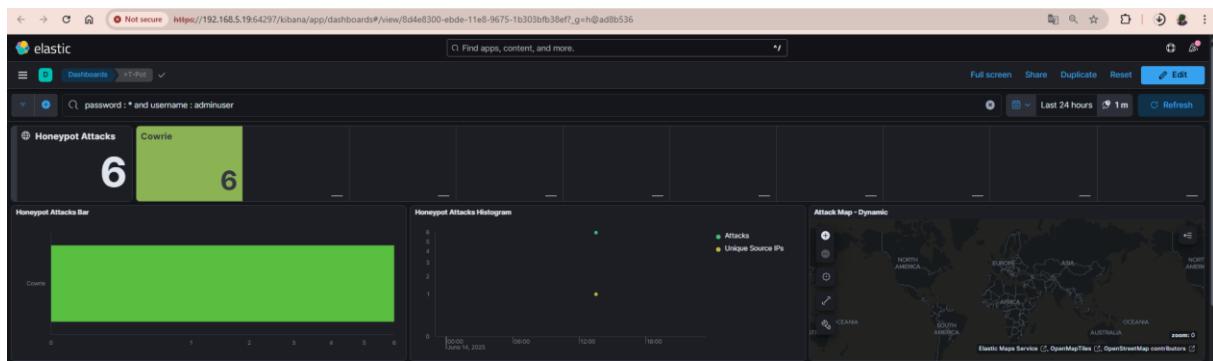


Puis Kibana qui représente le Dashboard pour la recherche :



Exemple d'un filtre possible :

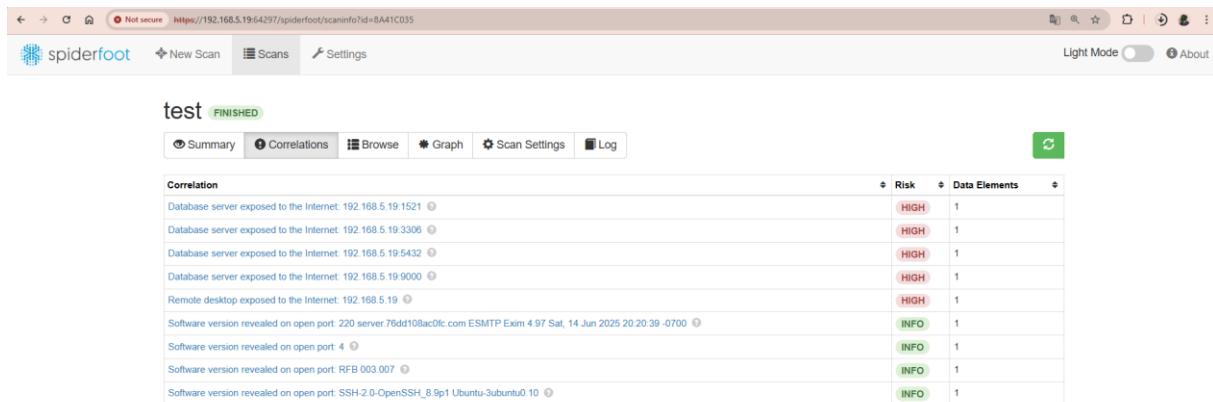
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



On peut retrouver les tentatives de l'utilisateurs et mot de passe.

Sur la dernière interface, on retrouve un outil d'analyse type scanner couplé à de l'OSINT pour avoir des petits scans de Threat Intelligence.

Exemple d'un scan lancé sur le TPOT lui-même :



On retrouve différentes sections avec les bases de données exposées, les ports ouverts etc...

Exemple d'un second scan sur notre OPNSENSE :

Démarrage du scan :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the 'New Scan' configuration page of the SpiderFoot tool. It includes fields for 'Scan Name' (opnsense), 'Scan Target' (192.168.5.19), and a detailed help box explaining target types like Domain Name, IPv4 Address, IPv6 Address, Hostname, Subnet, and Bitcoin Address. Below this are tabs for 'By Use Case' (All, Footprint, Investigate, Passive) and 'By Required Data' (Get anything and everything about the target, Understand what information this target exposes to the Internet). A note states that all modules will be enabled for the 'All' option. The 'Footprint' option is selected. At the bottom is a red 'Run Scan Now' button.

Synthèse du scan :

The screenshot shows the 'Scaninfo' page for the 'opnsense' scan, which is marked as 'FINISHED'. It features a summary table with columns for Type, Unique Data Elements, Total Data Elements, and Last Data Element. The data is as follows:

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - IP Address	15	15	2025-06-14 20:55:57
IP Address	1	1	2025-06-14 20:55:54
Raw Data from RIAs/APIs	2	2	2025-06-14 20:55:57

INSTALLATION PRIVATEBIN ET D'UNE CA ET CA INTERMEDIAIRE

INSTALLATION DE PRIVATEBIN

Je récupère le GitHub de Privatebin :

```
git clone https://github.com/PrivateBin/PrivateBin.git /var/www/privatebin
```

Puis je lance apache2.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Systemctl start apache2

Dans un second temps je vais créer CA et signé le certificat du serveur :

```
tourisk@tourisk:~/TouriskCA$ openssl genrsa -out TouriskCA.key 4096
tourisk@tourisk:~/TouriskCA$ openssl req -x509 -new -nodes -key TouriskCA.key -sha256 -days 3650 -out TouriskCA.pem -subj "/CN=TouriskCA"
tourisk@tourisk:~/TouriskCA$ ls
TouriskCA.key  TouriskCA.pem
tourisk@tourisk:~/TouriskCA$ openssl genrsa -out privatebin.key 2048
tourisk@tourisk:~/TouriskCA$ openssl req -new -key privatebin.key -out privatebin.csr -subj "/CN=Touriskprivatebin"
tourisk@tourisk:~/TouriskCA$ openssl x509 -req -in privatebin.csr -CA TouriskCA.pem -CAkey TouriskCA.key -CAcreateserial -out privatebin.crt -days 825 -sha256
Certificate request self-signature ok
subject=CN = Touriskprivatebin
tourisk@tourisk:~/TouriskCA$ |
```

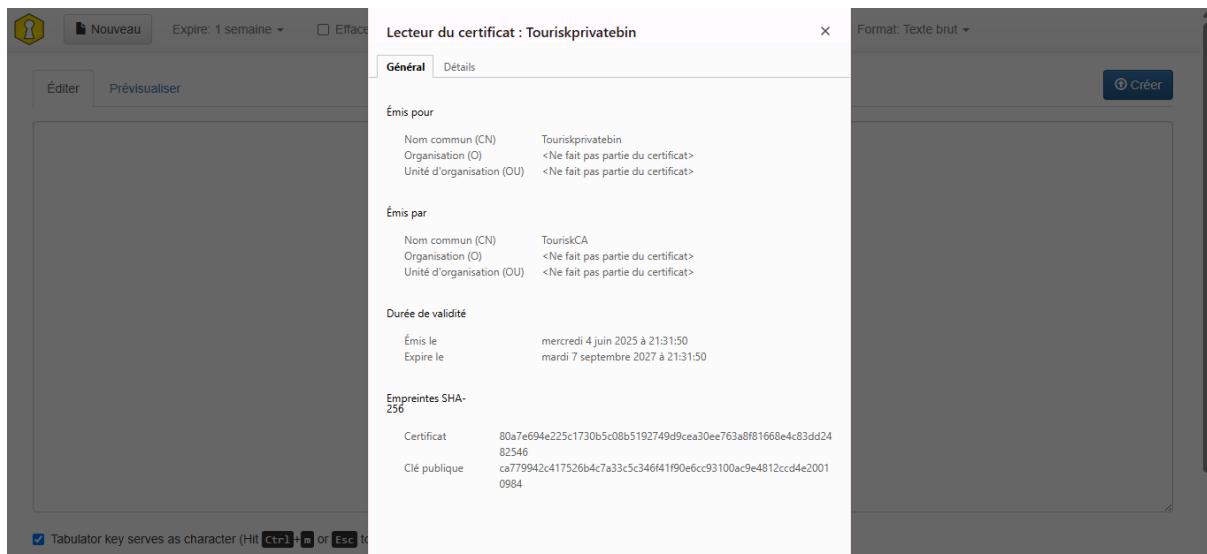
Puis j'active le module SSL pour apache :

```
tourisk@tourisk:~/TouriskCA$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
```

Je configure un Virtual host pour qu'il récupére mes certificats

Puis je lance relance apache2 :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



On retrouve le certificat signé par l'autorité de certification TouriskCA.

Puis on peut utiliser Privatebin pour transférer des identifiants :

The screenshot shows a Privatebin paste page. At the top, there are buttons for "Nouveau", "Cloner", "Email", and "QR code". Below that, there is a button "Copier le lien" and a "Supprimer les données du poste" button. A green message bar says: "✓ Votre poste est disponible à l'adresse <https://192.168.5.92/?b6d3090eed19d594#FNsXjGu7oMdV8898RT4NkDT81Qxb531DMDIH84C118Jb> (Appuyez sur **ctrl + c** pour copier)". Below this, there is a note: "To copy paste press on the copy button or use the clipboard shortcut **ctrl + c** **cmd + c**". The main area contains the identifier "Identifiant factice". At the bottom, there is information about PrivateBin: "PrivateBin - Vivons heureux, vivons cachés" and "1.7.6". A note says: "PrivateBin est un 'pastebin' (ou gestionnaire d'extraits de texte et de code source) minimalist et open source, dans lequel le serveur n'a aucune connaissance des données envoyées. Les données sont chiffrées/déchiffrées dans le navigateur par un chiffrement AES 256 bits. Plus d'informations sur la page du projet."

Puis récupération des données :

The screenshot shows a Privatebin paste page. At the top, there are buttons for "Nouveau", "Cloner", "Texte brut", "Sauver le poste", "Email", and "QR code". Below that, there is a note: "Ce document expirera dans 6 jours." A note at the bottom says: "To copy paste press on the copy button or use the clipboard shortcut **ctrl + c** **cmd + c**". The main area contains the identifier "Identifiant factice". At the bottom, there is information about PrivateBin: "PrivateBin - Vivons heureux, vivons cachés" and "1.7.6". A note says: "PrivateBin est un 'pastebin' (ou gestionnaire d'extraits de texte et de code source) minimalist et open source, dans lequel le serveur n'a aucune connaissance des données envoyées. Les données sont chiffrées/déchiffrées dans le navigateur par un chiffrement AES 256 bits. Plus d'informations sur la page du projet."

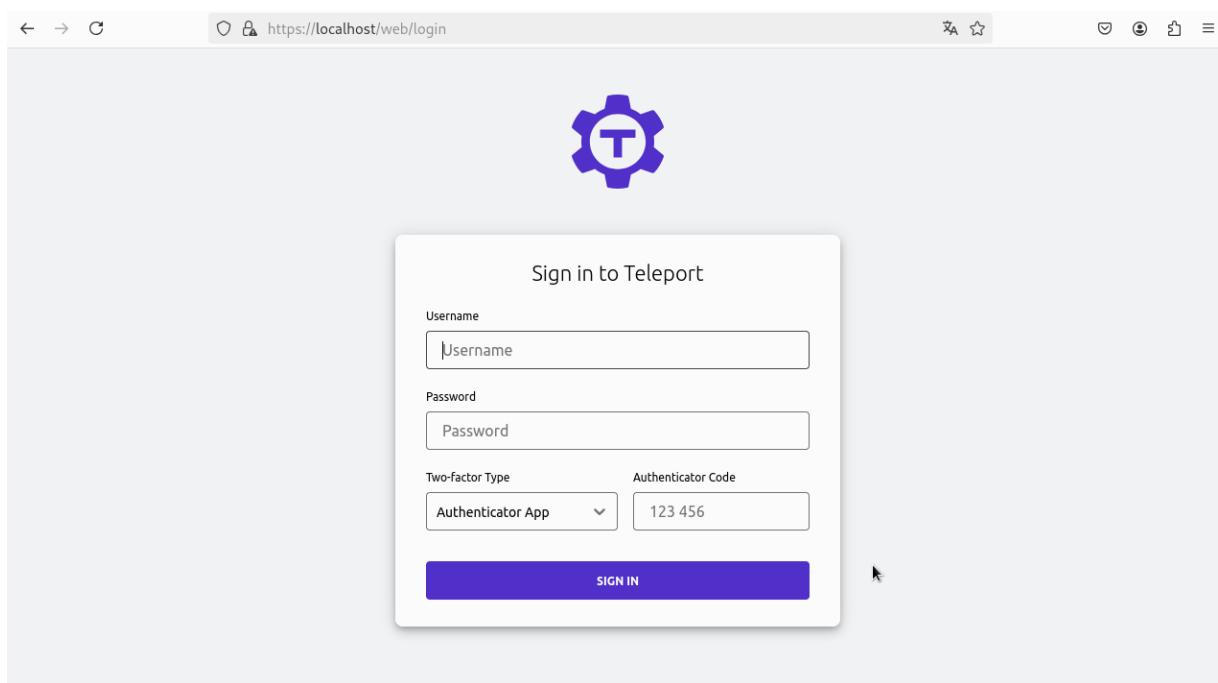
ANNEXE INSTALLATION DE TELEPORT

Récupération de l'instance TELEPORT :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

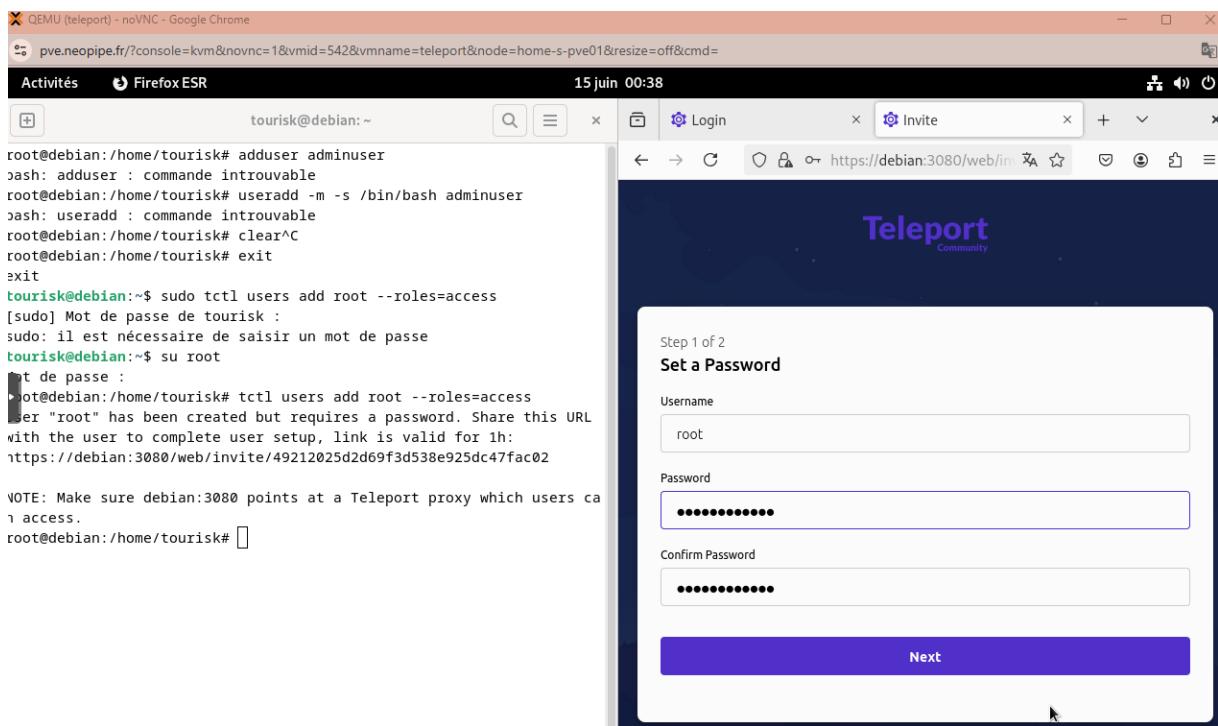
```
root@debian:/home/tourisk# curl https://goteleport.com/static/install.sh | bash
-s 14.1.1
  % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
          Dload  Upload   Total   Spent   Left  Speed
100  3318  100  3318    0      0  17203      0 --::--- --::--- --::--- 17191
Downloading https://cdn.teleport.dev/install-v16.1.8.sh
+ curl -fL -o /tmp/teleport-LwSBBopcSE/install-v16.1.8.sh https://cdn.teleport.d
ev/install-v16.1.8.sh
  % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
          Dload  Upload   Total   Spent   Left  Speed
100 11963  100 11963    0      0  21812      0 --::--- --::--- --::--- 21830
+ set +x
Downloading https://cdn.teleport.dev/install-v16.1.8.sh.sha256
+ curl -fL -o /tmp/teleport-LwSBBopcSE/install-v16.1.8.sh.sha256 https://cdn.tel
eport.dev/install-v16.1.8.sh.sha256
```

Une fois installé, je peux directement aller me connecter sur l'interface :



Pour créer un utilisateur administrateur il faut entrée la commande :

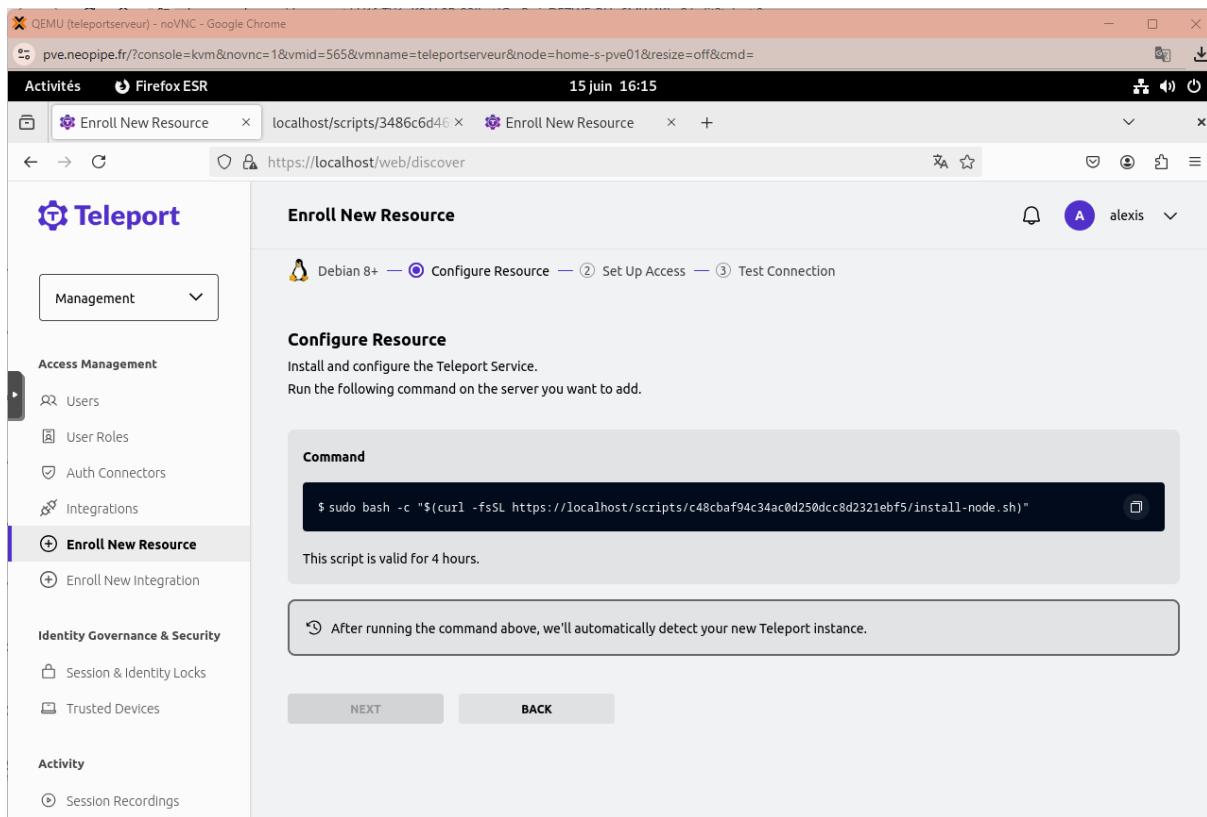
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Le rôle Access permet d'ajouter l'utilisateur en lecture et editor en écriture.

Une fois sur la plateforme d'administration je peux commencer à ajouter des nouvelles ressources

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Sur la machine je vais lancer la commande :

```
tourisk@debian:~$ su root
Mot de passe :
root@debian:/home/tourisk# nano install.sh
root@debian:/home/tourisk# nano /etc/hosts
root@debian:/home/tourisk# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      debian
10.4.0.12      teleport.tourisk.local
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@debian:/home/tourisk# chmod +x install.sh
```

(Dans cette capture le script est dans install.sh), pour utiliser la commande donnée par TELEPORT il faut rajouter un k pour passer au-dessus du certificat auto-signé

Voici ce qu'il manque :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Curl :

```
root@debian:/home/tourisk# apt install curl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  curl
0 mis à jour, 1 nouvellement installés, 0 à enlever et 4 non mis à jour.
Il est nécessaire de prendre 315 ko dans les archives.
Après cette opération, 501 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 curl amd64 7.88.1-10+deb12u12 [
315 ko réceptionnés en 0s (1 838 ko/s)
Sélection du paquet curl précédemment désélectionné.
(Lecture de la base de données... 186050 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../curl_7.88.1-10+deb12u12_amd64.deb ...
Dépaquetage de curl (7.88.1-10+deb12u12) ...
Paramétrage de curl (7.88.1-10+deb12u12) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Et exporter les bons Path :
```

```
root@debian:/home/tourisk# export PATH=$PATH:/usr/local/sbin:/usr/sbin:/sbin
root@debian:/home/tourisk# echo 'export PATH=$PATH:/usr/local/sbin:/usr/sbin:/sbin' >> /root/.ba
```

Au cas où, il préférable de supprimer TELEPORT
et les confs

```
root@debian:/home/tourisk# pkill -f teleport
root@debian:/home/tourisk# rm -rf /var/lib/teleport
root@debian:/home/tourisk# rm -f /etc/teleport.yaml
root@debian:/home/tourisk# rm -f /usr/local/bin/teleport /usr/local/bin/tctl /usr/local/bin/tsh
root@debian:/home/tourisk# apt autoremove teleport
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants seront ENLEVÉS :
  teleport
0 mis à jour, 0 nouvellement installés, 1 à enlever et 4 non mis à jour.
Après cette opération, 552 Mo d'espace disque seront libérés.
Souhaitez-vous continuer ? [O/n] 0
(Lecture de la base de données... 186067 fichiers et répertoires déjà installés.)
Suppression de teleport (14.1.1) ...
dpkg: avertissement: lors de la suppression de teleport, le répertoire « /usr/local » n'était pas
  donc il n'a pas été supprimé
root@debian:/home/tourisk# apt purge teleport
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
E: Impossible de trouver le paquet teleport
root@debian:/home/tourisk#
```

Puis je lance l'installation : ./install.sh

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

```
(Lecture de la base de données... 186057 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../teleport_14.1.1_amd64.deb ...
Dépaquetage de teleport (14.1.1) ...
Paramétrage de teleport (14.1.1) ...
2025-06-15 16:29:51 CEST [teleport-installer] Found: Teleport v14.1.1 git:api/v14.1.1-0-gfb6429e go1.21.3
2025-06-15 16:29:51 CEST [teleport-installer] Writing Teleport node service config to /etc/teleport.yaml

A Teleport configuration file has been created at "/etc/teleport.yaml".
To start Teleport with this configuration file, run:

teleport start --config="/etc/teleport.yaml"

Happy Teleporting!
2025-06-15 16:29:51 CEST [teleport-installer] Host is using systemd
2025-06-15 16:29:51 CEST [teleport-installer] Starting Teleport via systemd. It will automatically be started whenever the system reboots.

Teleport has been started.

View its status with 'sudo systemctl status teleport.service'
View Teleport logs using 'sudo journalctl -u teleport.service'
To stop Teleport, run 'sudo systemctl stop teleport.service'
To start Teleport again if you stop it, run 'sudo systemctl start teleport.service'

You can see this node connected in the Teleport web UI or 'tsh ls' with the name 'debian'
Find more details on how to use Teleport here: https://goteleport.com/docs/user-manual/
```

Je peux maintenant démarrer l'agent TELEPORT. Sans oublier de mettre **-insecure** pour passer au-dessus du certificat auto-signé

```
root@debian:/home/tourisk# teleport start --config="/etc/teleport.yaml" --insecure
2025-06-15T16:35:31+02:00 INFO Starting Teleport v14.1.1 with a config file located at "/etc/teleport.yaml" common/teleport.go:58
8
2025-06-15T16:35:32+02:00 INFO [PROC:1] Joining the cluster with a secure token. pid:6943.1 service/connect.go:460
2025-06-15T16:35:32+02:00 INFO [PROC:1] Joining the cluster with a secure token. pid:6943.1 service/connect.go:460
2025-06-15T16:35:32+02:00 INFO [AUTH] Attempting registration via proxy server. auth/register.go:279
WARNING: You are using insecure connection to Teleport proxy https://teleport.tourisk.local:443
2025-06-15T16:35:32+02:00 INFO [AUTH] Successfully registered via proxy server. auth/register.go:286
2025-06-15T16:35:32+02:00 INFO [AUTH] Attempting registration via proxy server. auth/register.go:279
WARNING: You are using insecure connection to Teleport proxy https://teleport.tourisk.local:443
2025-06-15T16:35:32+02:00 INFO [PROC:1] Instance has obtained credentials to connect to the cluster. pid:6943.1 service/connect.go:518
2025-06-15T16:35:32+02:00 INFO [AUTH] Successfully registered via proxy server. auth/register.go:286
2025-06-15T16:35:32+02:00 INFO [PROC:1] Node has obtained credentials to connect to the cluster. pid:6943.1 service/connect.go:518
2025-06-15T16:35:32+02:00 INFO [PROC:1] The process successfully wrote the credentials and state of Instance to the disk. pid:6943.1 service/connect.go:560
2025-06-15T16:35:32+02:00 INFO [PROC:1] Instance: features loaded from auth server: Kubernetes:true App:true DB:true Desktop:true Assist:t
rue DeviceTrust:<> AccessRequests:<> pid:6943.1 service/connect.go:92
2025-06-15T16:35:32+02:00 INFO [UPLOAD:1] starting upload completer service pid:6943.1 service/service.go:2858
2025-06-15T16:35:32+02:00 INFO [UPLOAD:1] Creating directory /var/lib/teleport/log. pid:6943.1 service/service.go:2874
2025-06-15T16:35:32+02:00 INFO [UPLOAD:1] Creating directory /var/lib/teleport/log/upload. pid:6943.1 service/service.go:2874
2025-06-15T16:35:32+02:00 INFO [UPLOAD:1] Creating directory /var/lib/teleport/log/upload/streaming. pid:6943.1 service/service.go:2874
2025-06-15T16:35:32+02:00 INFO [UPLOAD:1] Creating directory /var/lib/teleport/log/upload/streaming/default. pid:6943.1 service/service.go:2874
2025-06-15T16:35:32+02:00 INFO [UPLOAD:1] Creating directory /var/lib/teleport/log. pid:6943.1 service/service.go:2874
```

Puis maintenant j'ai la possibilité de choisir les utilisateurs pour se connecter, j'ajoute root dans mon cas. Et je peux accéder à la machine depuis l'interface TELEPORT.

Voici les 3 ressources accessibles :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Pour y accéder, je clique sur "connect", sélectionne l'utilisateur et cela m'ouvre une nouvelle page avec un Shell.

Voici un shell ouvert sur Admin1 depuis le Bastion Teleport.

ZABBIX CONFIGURATION

GMAIL CONFIGURATION

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Sur zabbix il est possible de rajouter un compte gmail nous permettant d'activer de recevoir des alertes sur certains trigger custom.

Rendez vous sur votre page d'administration de zabbix

The screenshot shows the Zabbix Global view dashboard. On the left, a sidebar lists navigation options: Tableaux de bord, Surveillance, Services, Inventaire, Rapports, Collecte de données, Alertes, Utilisateurs, Administration, Support, Intégrations, Aide, Paramètres utilisateur, and Déconnexion. The main content area includes:

- Top hosts by CPU utilization:** Shows Zabbix server with 2.44% utilization over 1m avg, 5m avg, 15m avg, and 153 processes.
- Information système:** Displays various system parameters like Zabbix version (7.2.6), frontend version (7.2.6), and host count (1).
- Disponibilité de l'hôte:** Host status distribution: Disponible (1), Non dis... (0), Mixte (0), Inconnu (0).
- Problèmes par sévérité:** Problem severity distribution: Désastre (0), Haut (0), Moyen (0), Avertisse... (0), Information (0), Non classé (0).
- Current problems:** A section stating "Aucune donnée disponible".
- Carte géographique:** A map showing locations like Marupe.

Sur la barre de navigation à gauche, allez dans la partie Alertes. Ensuite sélectionnez Types de média

The screenshot shows the Zabbix Alertes menu. The navigation items are: Alertes, Actions, Types de média, Scripts, and Utilisateurs. The 'Types de média' item is highlighted, indicating it is selected.

Vous verrez tous les types de médias possibles, mais nous allons juste s'intéresser à la partie email. Ils sont tous désactivé par défaut, il faudra cliquer sur le bouton désactivé pour l'activer.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows a list of media types in a Zabbix-like interface. The top bar has a green header with a checkmark icon and the text "Type de média activé". Below the header, there are filters for "Nom" (Name), "État" (Status), and buttons for "Appliquer" (Apply) and "Réinitialiser" (Reset). The main table lists four media types:

Nom	Type	État	Utilisé dans les actions	Détails
Brevis.one	Webhook	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	
Discord	Webhook	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	
Email	Courriel	Activé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	serveur SMTP: "mail.example.com", courriel: "zabbix@..."
Email (HTML)	Courriel	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	serveur SMTP: "mail.example.com", courriel: "zabbix@..."

Ensuite cliquer sur le bouton Email en lui même.

The screenshot shows the configuration page for the "Email" media type. It features three tabs: "Email" (selected), "Courriel" (Email in French), and "Activé" (Active). The "Email" tab is currently active, indicated by a blue background and white text.

On atterrit sur la page de configuration

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Type de média

Type de média Modèles de messages 5 Options

* Nom	Email (HTML)
Type	Courriel
Fournisseur de messagerie	Generic SMTP
* serveur SMTP	mail.example.com
Port du serveur SMTP	25
* Courriel	zabbix@example.com
SMTP helo	example.com
Sécurité de la connexion	Aucun STARTTLS SSL/TLS
Authentification	Aucun Nom d'utilisateur et mot de passe
Format du message	HTML Texte brut
Description	
Activé	<input type="checkbox"/>

[Actualiser](#) [Clone](#) [Supprimer](#) [Annuler](#)

Il faudra bien changer le 'Fournisseur de messagerie' pour n'afficher que les paramètres pour un compte gmail, comme ceci.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Type de média Modèles de messages 5 Options

* Nom

Type

Fournisseur de messagerie

* Courriel

* Mot de passe

Format du message

Description

Activé

Modifiez la partie 'Courriel' en mettant votre gmail et au niveau du mot de passe, il faudra créer un mot de passe tiers sur votre compte google, vous avez un tutoriel ici (<https://wiki.bibisan.com/books/tools/page/gmail-app-passwords>).

Enregistrez les modifications. Vous pourrez tester avec le bouton test qui sera tout à droite sur la ligne de votre template



MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Saisissez une adresse mail destinataire accessible et envoyez votre message à l'aide du boutton test en bas à droite.

The screenshot shows a modal dialog titled "Tester le type de média \"Email\"". It contains three input fields: "Envoyer à" (Recipient) with placeholder "Entrer l'adresse e-mail", "Sujet" (Subject) with placeholder "Titre du message", and "Message" (Message) containing the text "Ceci est un message de test de Zabbix". At the bottom right of the dialog are two buttons: "Test" (in blue) and "Annuler" (Cancel).

Vérifiez dans la boite mail saisie et vous verrez le mail de zabbix.

AJOUT DE CLIENT (WINDOWS & LINUX)

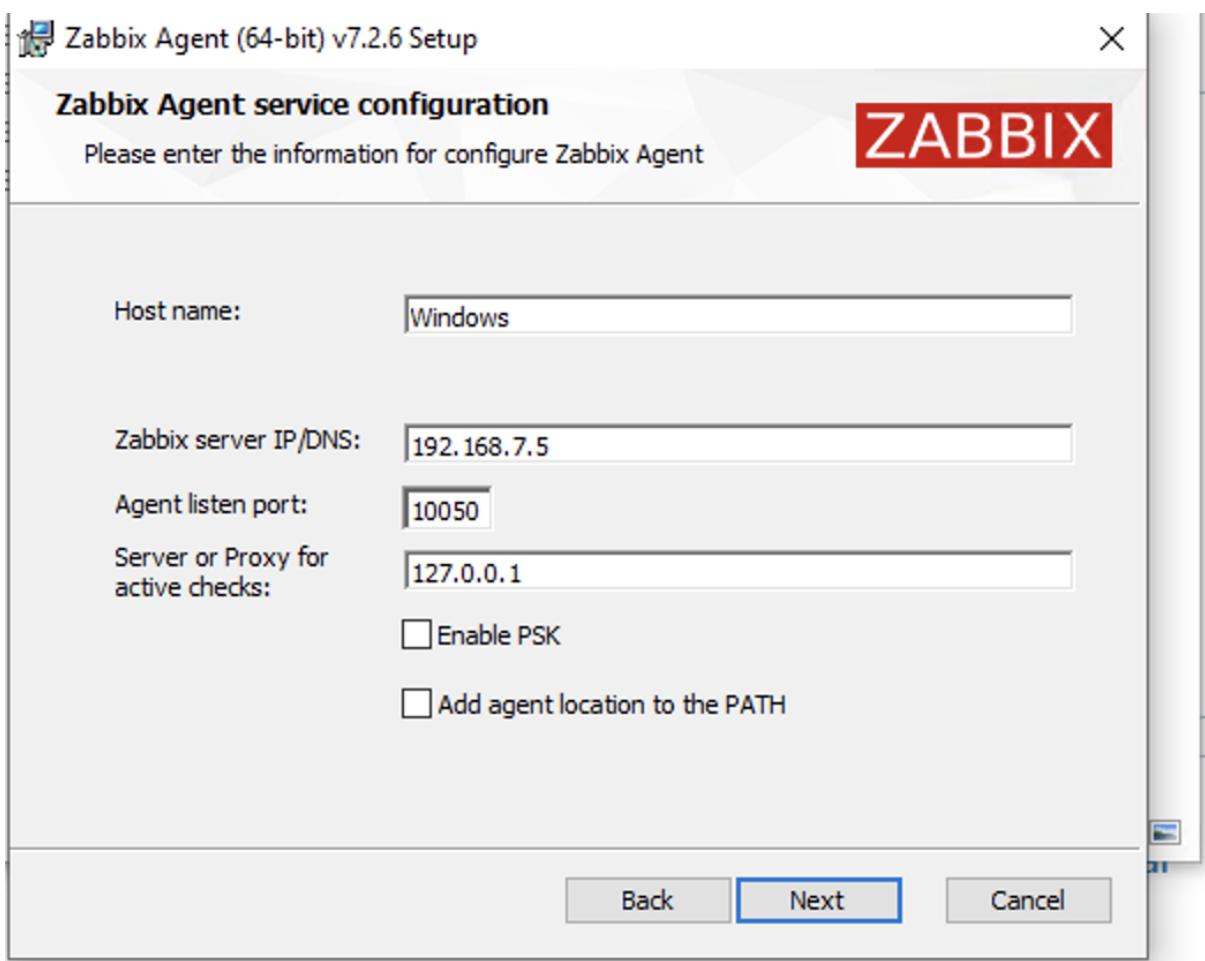
WINDOWS

L'ajout de client windows est très simple, il suffit de ce rendre sur le site officiel de zabbix sur la partie ajout d'agent, disponible [ici](#).

Ça vous fera télélécharger un exécutable, qu'il faudra installer comme tout autre application.

À un moment vous aurez cette étape.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Host name : C'est le nom qui sera afficher sur la console zabbix.

Zabbix server IP/DNS: C'est l'adresse ip du serveur zabbix

Agent listen port: Laissez le par défaut

Server or Proxy for active checks : Mettez également l'ip du serveur zabbix à la place du localhost.

Continuer ensuite l'installation normalement.

SUR LINUX

Lancer la commande : sudo apt install zabbix-agent.

Le paquet zabbix sera ensuite installé.

Editez le fichier /etc/zabbix/zabbix_agentd.conf

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Rechercher la ligne avec Server=127.0.0.1 et changez la par l'ip du serveur zabbix.

```
# Mandatory. yes, if StartAgents is
# Default:
# Server=

Server=127.0.0.1

### Option: ListenPort
#           Agent will listen on this po
#
```

Ensute cherchez la ligne ServerActive = 127.0.0.1et changez également l'adresse ip contre celle du serveur zabbix.

```
# Default.
# ServerActive=

ServerActive=127.0.0.1

### Option: Hostname
#           List of comma delimit
```

Cherchez ensuite la ligne Hostname` , qui sera commenté, elle se trouve juste en dessous de ServerActive. Décommenter la ligne et mettez le hostname de votre choix.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

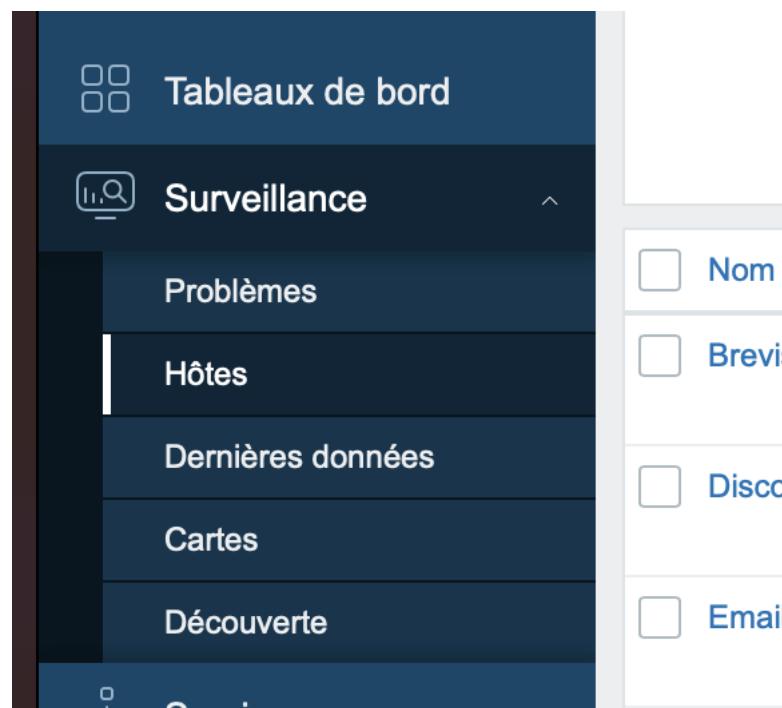
```
ServerActive=192.168.7.5
```

```
### Option: Hostname
#      List of comma delimited unique, case sensitive
#      Required for active checks and must match host
#      Value is acquired from HostnameItem if undefined
#
# Mandatory: no
# Default:
Hostname=webServer
```

CONFIGURATION SUR L'INTERFACE ZABBIX (POUR TOUS LES OS)

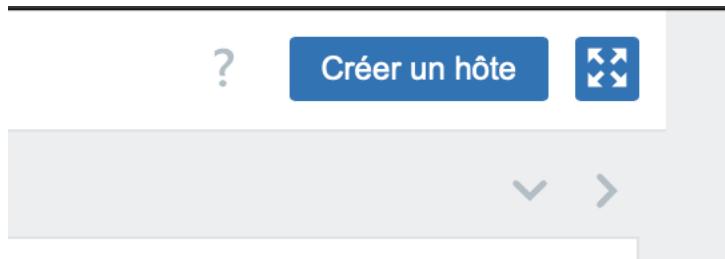
Que vous ayez rajouté une machine windows ou linux, vous devrez la rajouter sur la console zabbix.

Allez sur la page d'accueil zabbix. Dans le menu à gauche cliquer sur l'onglet Surveillance ensuite aller dans Hôtes.



MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Tout en haut à droite vous avez le bouton Crée un hôte, cliquez dessus.



Au niveau du Nom de l'hôte vous devez mettre exactement le même nom que vous avez renseigner sur la machine, que ce soit windows ou linux.

Sur la partie Modèle et Groupe d'hôtes, vous avez les propositions zabbix par défaut selon la machine rajouté, choisissez celle qui vous semble la plus adapté selon vos besoins.

A screenshot of the "Nouvel hôte" (New Host) creation form in Zabbix. The "Hôte" tab is active. The form includes fields for "Nom de l'hôte" (Host Name) set to "webServer", "Nom visible" (Visible Name) also set to "webServer", "Modèles" (Models) showing "Linux by Zabbix agent" with a search input and a "Sélectionner" (Select) button, and "Groupes d'hôtes" (Host Groups) showing "Linux servers" with a search input and a "Sélectionner" (Select) button. Below these, the "Interfaces" (Interfaces) section shows "Aucune interface n'est définie." (No interface is defined) and an "Ajouter" (Add) button. A large empty text area for "Description" (Description) is at the bottom.

Au niveau des interfaces, cliquez sur Ajouter puis Agent.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Interfaces Aucune interface n'est définie.

Ajouter

Description	Agent
	SNMP
	JMX
	IPMI

Surveillé par Serveur Proxy Groupe de proxy

Renseigner uniquement l'adresse ip de votre hôte, et laissez tout le reste par défaut. Cliquer sur le bouton ajouter en bas droite.

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	192.168.7.3			IP	10050	<input checked="" type="radio"/> Supprimer

Ajouter

Description

Surveillé par Serveur Proxy Groupe de proxy

Activé

Ajouter Annuler

Attendez que votre machine passe au vert (ça peut prendre plusieurs minutes souvent), et votre agent sera prêt.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Nom ▲	Interface	Disponibilité	Tags
webServer	192.168.7.3:10050	ZBX	classeur
Windows	192.168.7.8:10050	ZBX	classeur
Zabbix server	127.0.0.1:10050	ZBX	classeur

MONITORING D'UN SERVICE (APACHE2)

Dans ce tutoriel nous allons choisir un template basique qui permet de moniterer un serveur web.

Nous prenons le cas où l'agent zabbix est déjà rajouté.

Allez sur la liste de vos hôtes zabbix, et cliquer sur celui ou votre serveur apache tourne, dans mon cas c'est la machine webServer.

<input type="checkbox"/> Nom ▲	Éléments	Déclencheurs	Graphiques	Dé
<input type="checkbox"/> webServer	Éléments 100	Déclencheurs 31	Graphiques 18	Dé
<input type="checkbox"/> Windows	Éléments 111	Déclencheurs 77	Graphiques 12	Dé
<input type="checkbox"/> Zabbix server	Éléments 141	Déclencheurs 78	Graphiques 14	Dé

Cliquez ensuite sur l'hôte pour afficher les paramètres. Sur les modèles rechercher et rajouter le modèle Apache by HTTP. Sauvegardez ensuite.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte: webServer

Nom visible: webServer

Modèles:

Nom	Actions
Apache by HTTP	Supprimer lien Supprimer lien et nettoyer
Linux by Zabbix agent	Supprimer lien Supprimer lien et nettoyer

taper ici pour rechercher Sélectionner

* Groupes d'hôtes:

taper ici pour rechercher	Sélectionner
Linux servers X	Sélectionner

Interfaces:

Type	adresse IP	Nom DNS	Connexion à	Port	
Agent	192.168.7.3		IP	DNS	10050

Ajouter

Description:

Ensuite allez sur la partie Déclencheurs

Hôte

Éléments

Déclencheurs

Graphiques

Découverte

Web

SCRIPTS

Detect operating system

Ping

Traceroute

Nom ▲

webServer

Windows

Zabbix server 127.0.0.1:10050 ZBX

Avertisse

Moyen

Disponibilité

ZBX

ZBX

Rajoutez un filtre Apache et appliquer le, et là on va se concentrer sur le déclencheur Apache service is down.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows a configuration interface for a network host named 'Apache'. The top section includes search fields for 'Groupes d'hôtes' and 'Hôtes' (set to 'webServer'), and various filter options like 'Nom', 'Sévérité' (Non classé, Avertissement, Haut, Information, Moyen, Désastre), 'État' (Tous, Normal, Inconnu, Activé, Désactivé), and 'Valeur' (Tous, Ok, Problème). Buttons for 'Ajouter', 'Hérité', 'Découvert', and 'Avec dépendances' are also present. A red circle highlights the 'Nom' field and the 'Appliquer' button.

The main table lists operational data for the Apache host:

Sévérité	Valeur	Nom	Données opérationnelles	Expression
Avertissement	OK	Apache by HTTP: Apache: Failed to fetch status page		<code>nodata(/webServer/apache.get_status,30m)=1</code>
Information	OK	Apache by HTTP: Apache: Service has been restarted		<code>last(/webServer/apache.uptime)<10m</code>
Moyen	OK	Apache by HTTP: Apache: Service is down		<code>last(/webServer/net.tcp.service[http,"\${APACHE.STATUS.HOST}","\${APACHE.STATUS.PORT}"])=0</code>
Avertissement	OK	Apache by HTTP: Apache: Service response time is too high		<code>min(/webServer/net.tcp.service.perf[http,"\${APACHE.STATUS.HOST}","\${APACHE.STATUS.PORT}"],5m)>\${APACHE.RESPONSE_TIME.MAX.WARN}</code>
Information	OK	Apache by HTTP: Apache: Version has changed		<code>last(/webServer/apache.version,#1)<>last(/webServer/apache.version,#2) and length(last(/webServer/apache.version))>0</code>

At the bottom, there are buttons for 'Activer', 'Désactiver', 'Copier', 'Modification collective', and 'Supprimer'. A red circle highlights the entry for 'Apache by HTTP: Apache: Service is down'.

Changer le niveau d'alertes et passer le, en catégorie désastre et enregistrez.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Déclencheur Tags 1 Dépendances

Déclencheurs parents Apache by HTTP

* Nom Apache: Service is down

Nom de l'événement Apache: Service is down

Données opérationnelles

Sévérité Non classé Information Avertissement Moyen Haut Désastre

* Expression last(/webServer/net.tcp.service[http,"\${APACHE.STATUS.HOST}","\${APACHE.STATUS.PORT}"])=0

Ajouter

Constructeur d'expression

Génération d'événement OK Expression Expression de récupération Aucun

Mode de génération des événements PROBLÈME Seul Multiple

Un événement OK ferme Tous les problèmes Tous les problèmes si les valeurs de tag correspondent

Autoriser la fermeture manuelle

Nom de l'entrée de menu ? URL du déclencheur

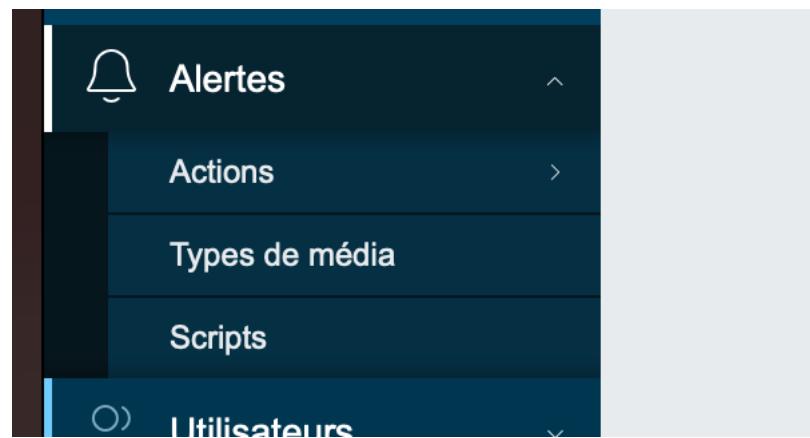
URL de l'entrée de menu

Description

Actualiser Clone Supprimer Annuler

The screenshot shows a configuration page for a trigger named "Apache: Service is down". It includes fields for event name, operational data, severity (set to Disaster), and an expression using the Constructeur d'expression tool. The expression is set to generate events on OK status changes. The mode is set to PROBLÈME (Problem) with a single entry. The "Autoriser la fermeture manuelle" (Allow manual closure) option is checked. Buttons at the bottom include Actualiser (Update), Clone, Supprimer (Delete), and Annuler (Cancel).

Ensuite sur le menu de gauche, allez dans la partie Alertes.



Allez sur la partie, Actions et Actions de déclencheur.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the Zabbix configuration interface. On the left, there's a sidebar with icons and labels: 'Alertes' (with a bell icon), 'Actions' (with a gear icon), 'Types de média' (with a document icon), 'Scripts' (with a script icon), 'Utilisateurs' (with a user icon), and 'Administration' (with a gear icon). The 'Actions' section is currently active. To its right, a large panel displays a list of trigger-based actions under the heading 'Actions de déclencheur'. The listed actions are: 'Actions des services', 'Actions de découverte', 'Actions d'enregistrement automatique', and 'Actions internes'. Below this list, there are two more sections: 'Actions de déclencheur' and 'Actions internes'.

Vous verrez l'action Report problems to zabbix administrators qui est présent, mais désactivé par défaut, activez le.

This screenshot shows the 'Actions' configuration screen in Zabbix. It lists various triggers and their associated actions. One trigger, 'Report problems to Zabbix administrators', is highlighted with a red circle. Its status is 'Désactivé' (Disabled), which is also highlighted with a red circle. At the top, there are 'Appliquer' (Apply) and 'Réinitialiser' (Reset) buttons. At the bottom, there are buttons for selecting, activating, disabling, and deleting actions.

Toujours sur l'onglet Alertes, allez cette fois dans Types de média

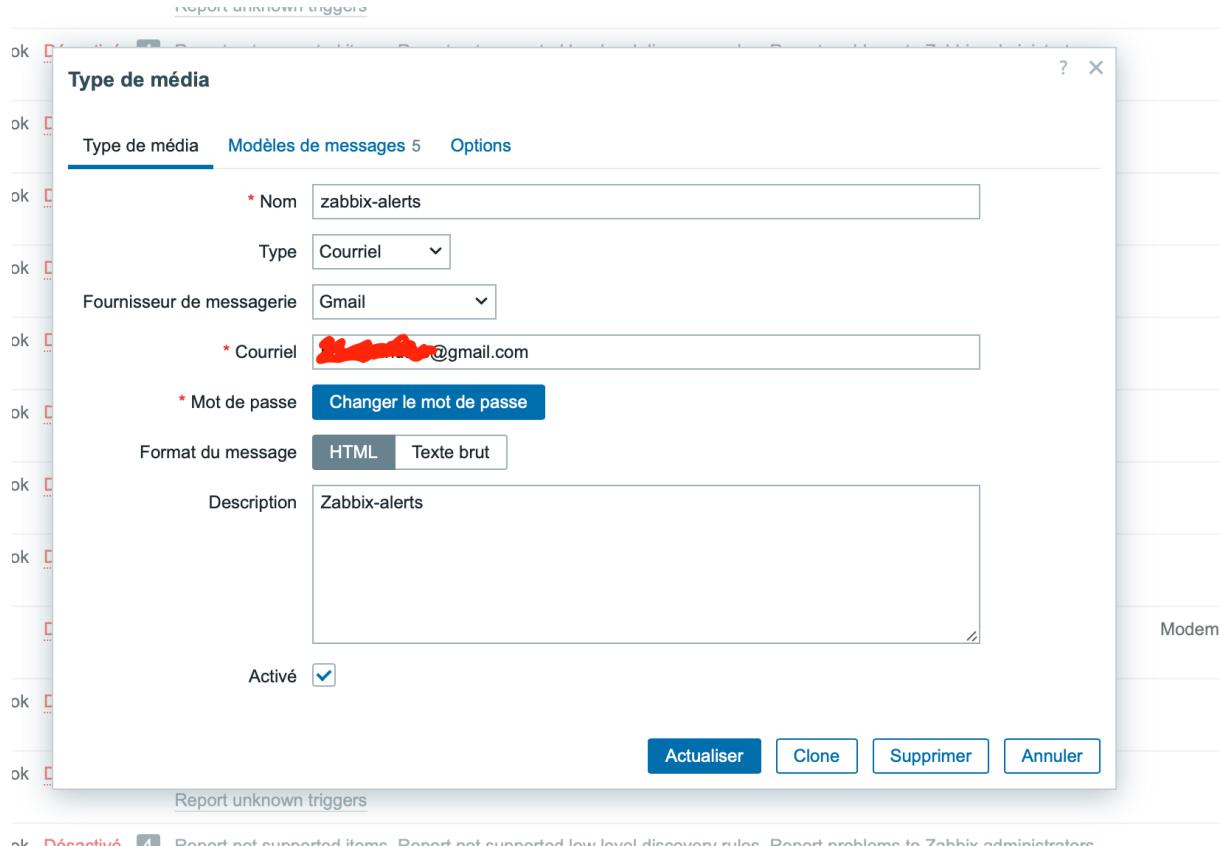
Vous verrez le média Email, cliquez sur le bouton désactiver, ce qui va l'activer directement.

This screenshot shows the 'Types de média' configuration screen in Zabbix. It lists different media types: 'Email', 'Email (HTML)', 'Discord', 'Brevis.one', and others. The 'Email' entry is circled in red. Its status is 'Activé' (Active), which is highlighted in green. At the top, there are 'Appliquer' (Apply) and 'Réinitialiser' (Reset) buttons. At the bottom, there are buttons for viewing actions, selecting all, selecting all available, and performing a search.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Changez le fournisseur de messagerie pour Gmail, ensuite saisissez votre adresse gmail, et pour le mot de passe il sera différent de celui de votre compte, vous devez créer un mot de passe tiers en suivant le tutoriel [ici](#).

Vous pouvez renommer le média, s'appelant par défaut Email, pour ma part j'ai mis zabbix-alerts.



Allez ensuite dans l'onglet Utilisateurs, puis sur l'administrateur.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the Zabbix web interface. On the left, a dark sidebar lists various modules: Inventaire, Rapports, Collecte de données, Alertes, Utilisateurs, Groupes d'utilisateurs, Rôles utilisateur, Utilisateurs (selected), Tokens API, Authentification, and Administration. The 'Utilisateurs' section is expanded, showing sub-options: Média, Permissions, and a list of users. The main content area on the right displays a table of users:

<input type="checkbox"/>	Nom d'utilisateur ▲	Prénom
<input type="checkbox"/>	Admin	Zabbix
<input type="checkbox"/>	guest	

Below the table, there are buttons: '0 sélectionné' (0 selected) and 'Provisionner maintenant' (Provision now).

Ensuite sur la section Média, ajouter un nouveau média, avec comme source Type le média gmail que vous aurez paramétré. Activer le média et choisissez comme niveau de严重性 Haut et Désastre, si vous souhaitez recevoir les autres niveaux, activez-les.

Utilisateurs

The screenshot shows the 'Utilisateurs' configuration screen. At the top, there are tabs: Utilisateur, Média 1, and Permissions. The Média tab is selected, showing a table with one row for 'zabbix-alerts'. The table columns are: Média, Type, Envoyer à, Lorsque actif, Utiliser si严重性, État, and Actions. The 'Actions' column contains buttons for 'Edition' (Edit) and 'Supprimer' (Delete). Below the table are buttons for 'Actualiser' (Update), 'Supprimer' (Delete), and 'Annuler' (Cancel).

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

GRAFANA CONFIGURATION

DASHBOARD CONFIGURATION

Dans ce tutoriel nous allons aborder les sujets suivants :

- Ajout d'une source de données sur Grafana (Zabbix)
- Création de premier Dashboard
- Ajout de machine

1- DATA SOURCE

Grafana a besoin d'une source de données pour les exploiter. Les plus connues étant Prometheus, Mysql, Graphite, etc...

Nous allons utiliser nous zabbix.

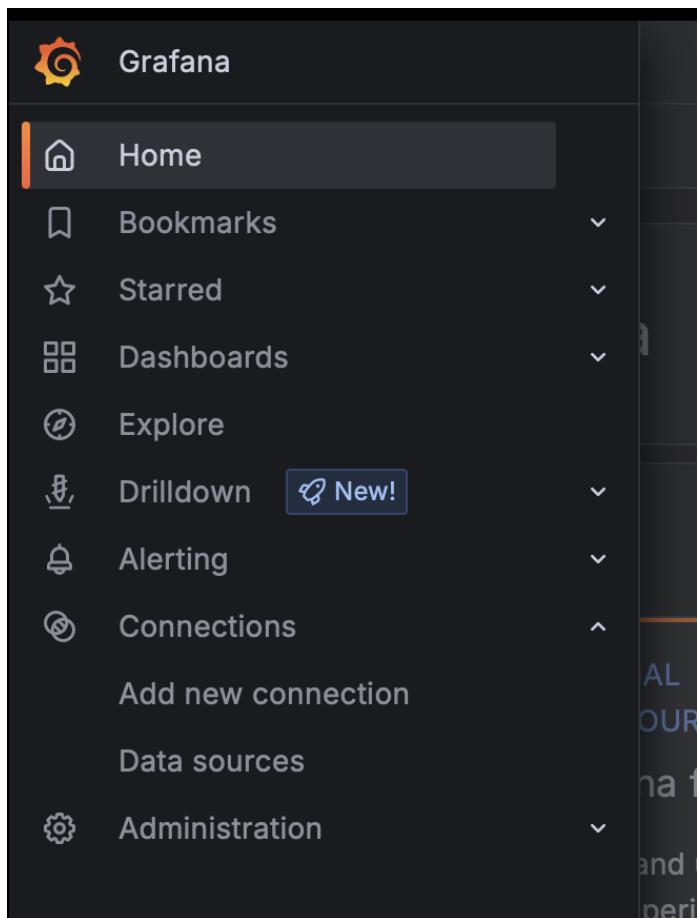
Le plugin Zabbix n'est pas inclus par défaut il faut l'installer manuellement avec la commande:

- `sudo grafana-cli plugins install alexanderzobnin-zabbix-app`

Et redémarrer ensuite le serveur avec : `sudo systemctl restart grafana-server`

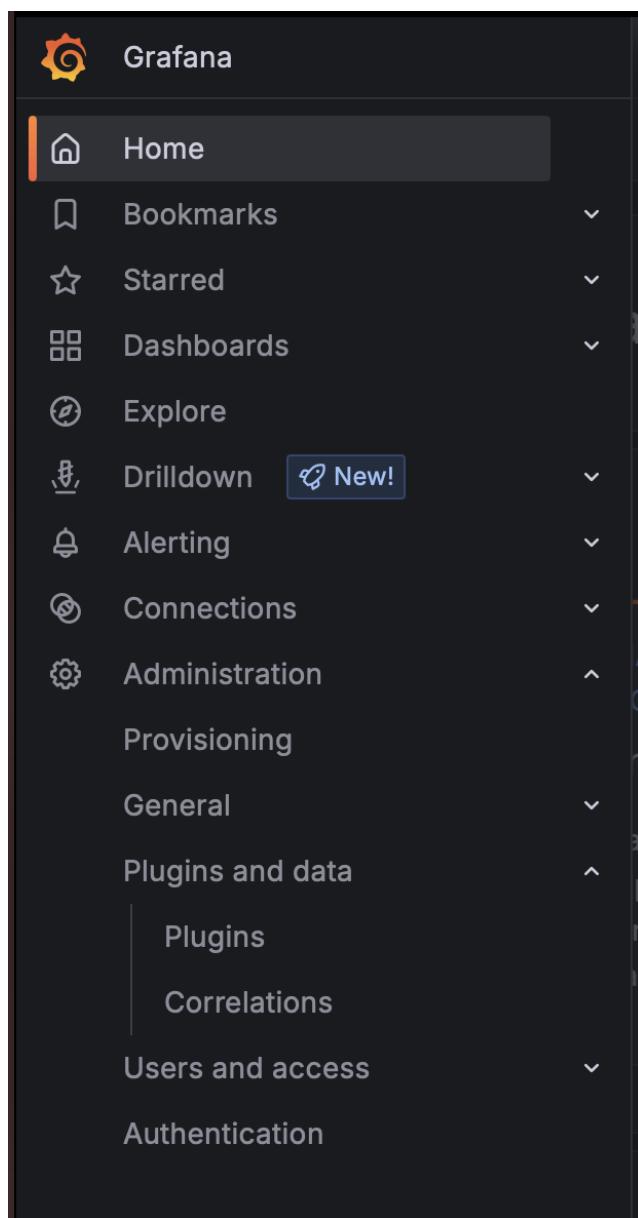
Normalement les data sources se trouvent sur la barre latérale de gauche dans la partie connections

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Mais notre zabbix étant un plugin, nous allons nous rendre sur l'onglet Administration ensuite Plugins and data (ou "Apps" selon la version) pour l'activer

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Rechercher Zabbix

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Plugins

Extend the Grafana experience with panel plugins and apps. To find more data sources go to [Connections](#).

The screenshot shows the Grafana plugin store interface. A search bar at the top has 'za' typed into it. Below the search bar are filters for 'Type' (set to 'All') and 'State' (with 'All' selected). There are also tabs for 'Installed' and 'New Updates'. Three plugin cards are displayed:

- Mapgl** by Vadim Pyatakov: A card with a green circular icon showing numbers 7, 9, and 11. It has a 'Signed' button.
- Organisations** by timomyl: A card with a tree icon. It has a 'Signed' button.
- Zabbix** by Alexander Zobnin: A card with a red 'Z' icon. It has a 'Signed' button and an 'Installed' button.

Et cliquer sur Enable, si ce n'est pas déjà le cas

The screenshot shows the details page for the 'Zabbix' plugin in the Grafana store. At the top, there's a 'Zabbix' logo and the text 'Zabbix plugin for Grafana'. Below that are navigation links: 'Overview' (which is underlined), 'Version history', 'Changelog', and 'Screenshots'. On the right side, there are 'Uninstall' and 'Disable' buttons. The main content area contains the text 'Zabbix plugin for Grafana'.

Maintenant retournez sur les data sources et vous pourrez rechercher et rajouter Zabbix.

Dès que vous cliquez sur Zabbix vous aurez cette page

- **Name** nommez votre source de données
- **Url**, c'est l'api de Zabbix, mettez http://localhost/zabbix/api_jsonrpc.php en remplaçant uniquement localhost par l'adresse IP de votre Zabbix s'il est sur un serveur différent.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

The screenshot shows the Grafana Settings page for a Zabbix data source. At the top, there are two tabs: "Settings" (which is selected) and "Dashboards". Below the tabs, there is a search bar with the name "Zabbix" and a "Default" toggle switch which is turned on (indicated by a blue circle with a checkmark). A note below the search bar states: "Before you can use the Zabbix data source, you must configure it below or in the config file. For detailed instructions, see the documentation." It also mentions that "Fields marked with * are required". The main section is titled "Connection" and contains a field for "URL *" with the value "http://192.168.7.5/zabbix/api_jsonrpc.php".

- **Auth type** choisissez User and password
- Et en dessous mettez les identifiants zabbix (Admin/zabbix) par défaut

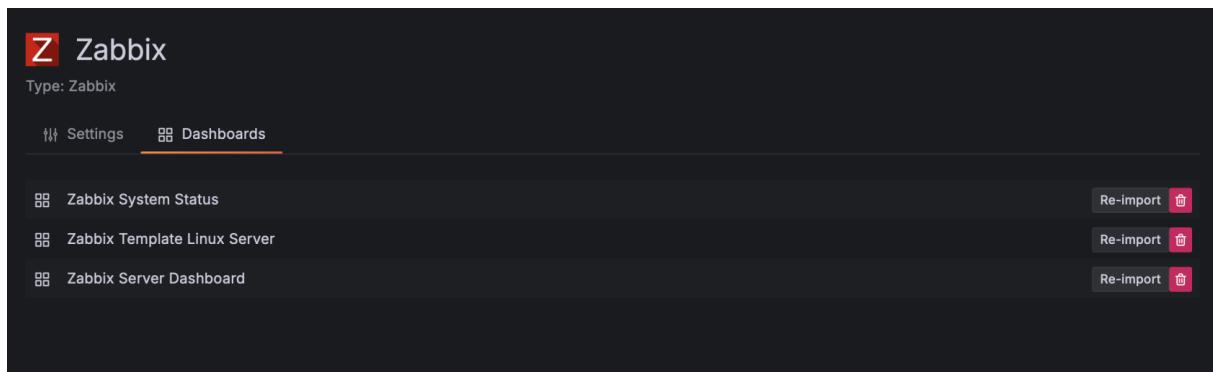
The screenshot shows the "Zabbix Connection" configuration page. It has three fields: "Auth type" set to "User and password", "Username" set to "Admin", and "Password" represented by five dots ("....."). Below this section, there is a heading "Additional settings".

Vous pouvez ensuite commencer à paramétrer vos Dashboard.

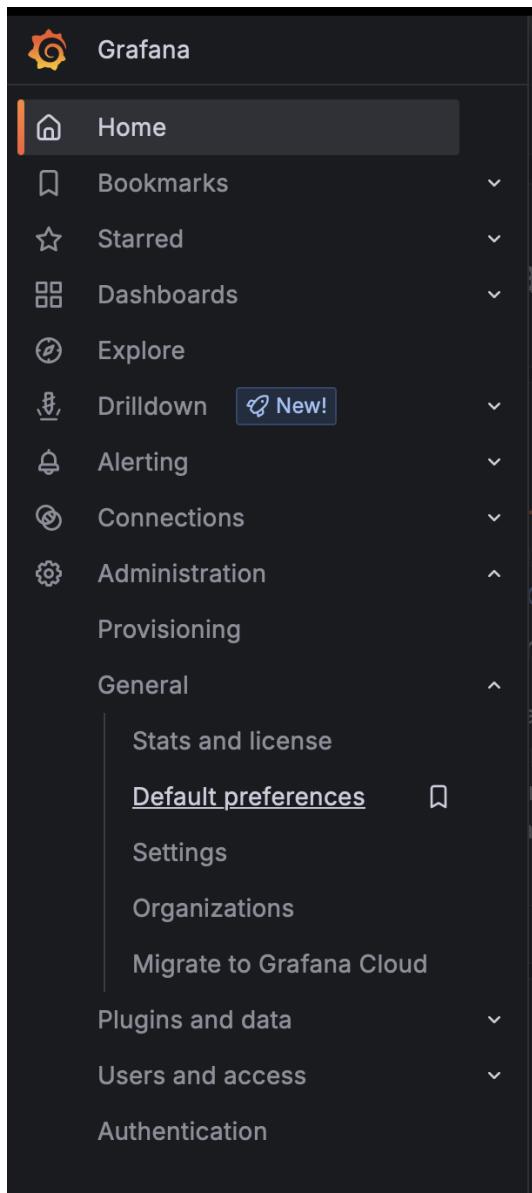
The screenshot shows a confirmation message: "✓ Zabbix API version: 7.2.6" followed by the text "Next, you can start to visualize data by [building a dashboard](#), or by querying data in the Explore view."

Sur la même page allez tout en haut, et cliquer sur Dashboards, vous verrez des Dashboards par défaut, que vous pourrez importer.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Maintenant sur le menu de gauche, allez dans Administration puis General puis Default préférences



MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Choisissez un Dashboard par défaut et sauvegardez.

Organization profile

Organization name

Update organization name

Preferences

Interface theme

Enjoying the experimental themes? Tell us what you'd like to see [here](#).

Default

Home Dashboard

- Dashboards/Zabbix Server Dashboard
- Dashboards/Zabbix Server Dashboard
- Dashboards/Zabbix System Status
- Dashboards/Zabbix Template Linux Server

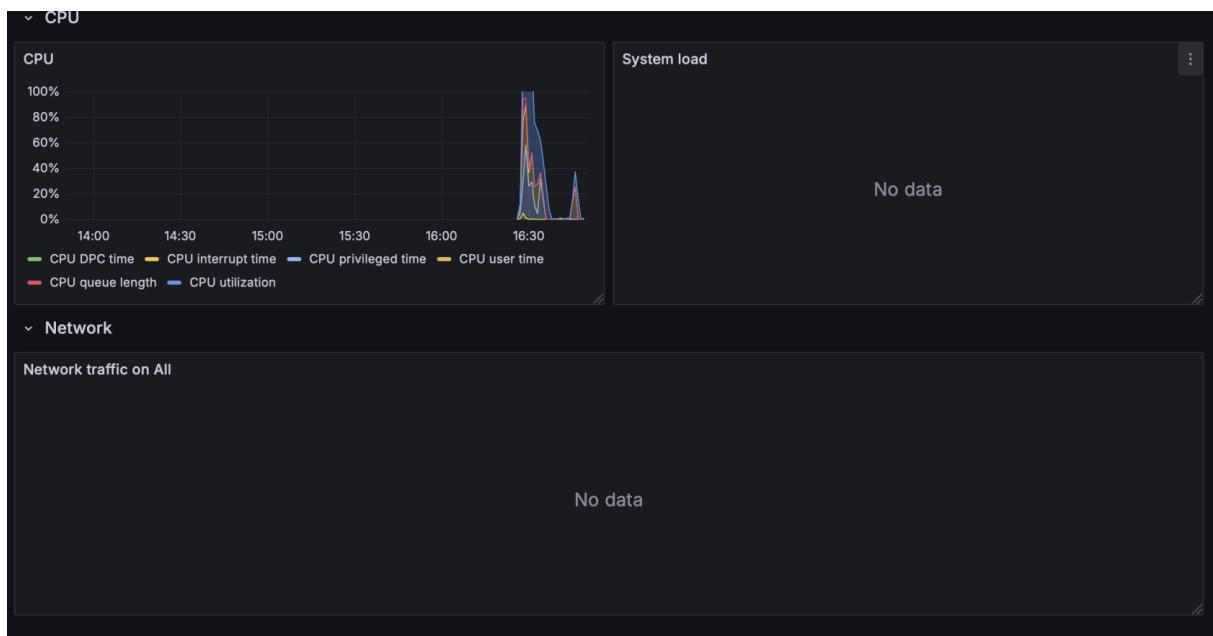
Language [Preview](#)

Default

Save

Vous aurez ensuite vos différents Dashboard sur Dashboard et vous pourrez voir les données concernant les machines présentes sur Zabbix.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



ANNEXE INSTALLATION ET CONFIGURATION DE KEYCLOACK

Installation et Configuration du SSO avec Keycloak sur DFIR-IRIS et Wazuh

1. Présentation de Keycloak

Keycloak est une solution open source de gestion des identités et des accès (IAM) permettant la fédération d'utilisateurs, l'authentification unique (SSO), la gestion centralisée des comptes et des permissions, ainsi que l'intégration avec de nombreuses applications via OpenID Connect (OIDC) ou SAML.

2. Installation de Keycloak

2.1. Prérequis

- Java 17+
- Accès root ou administrateur.

2.2. Installation manuelle (Linux)

1.Télécharger et extraire Keycloak :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

```
curl -L -O https://github.com/keycloak/keycloak/releases/download/23.0.1/keycloak-23.0.1.tar.gz
```

```
tar xvzf keycloak-23.0.1.tar.gz
```

```
cd keycloak-23.0.1
```

2.Démarrer Keycloak en mode développement :

```
bin/kc.sh start-dev
```

3.Créer l'utilisateur administrateur :

```
Export KEYCLOAK_ADMIN=admin
```

```
Export KEYCLOAK_ADMIN_PASSWORD=admin
```

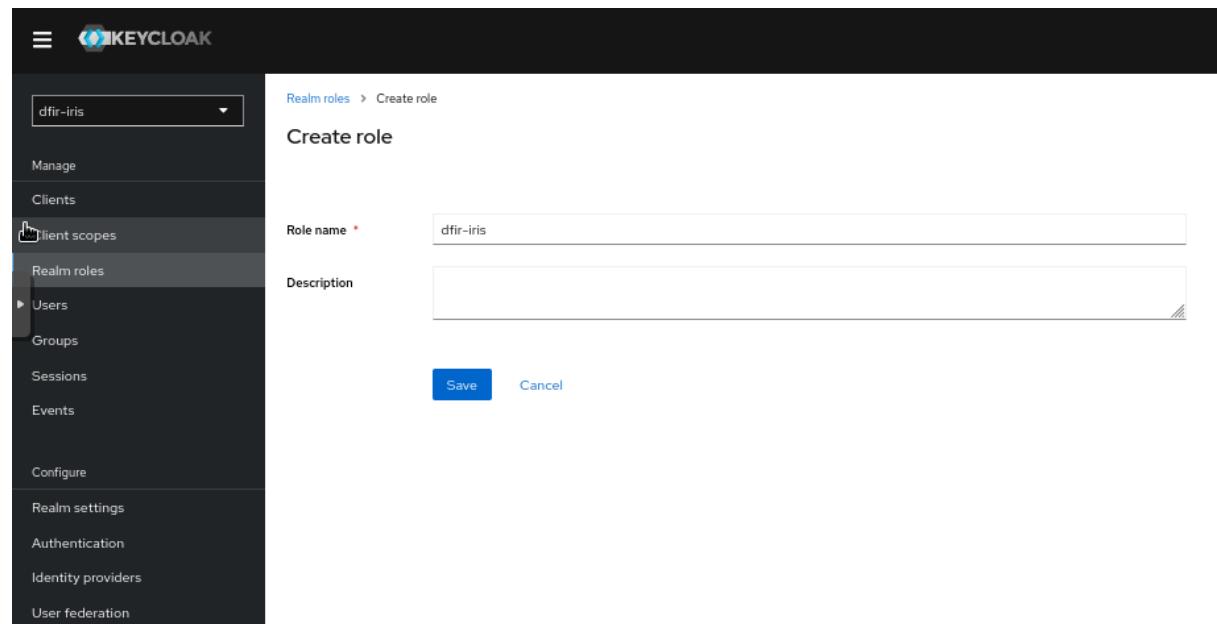
```
bin/kc.sh start-dev
```

3. Configuration Initiale de Keycloak

- Se connecter à la console d'administration.
- Créer un nouveau **realm** pour chaque application à intégrer (ex : dfir-iris, wazuh).
- Créer des utilisateurs, groupes et rôles selon les besoins

4. Intégration SSO Keycloak dans DFIR-IRIS

4.1. Crédit et Configuration du Client DFIR-IRIS

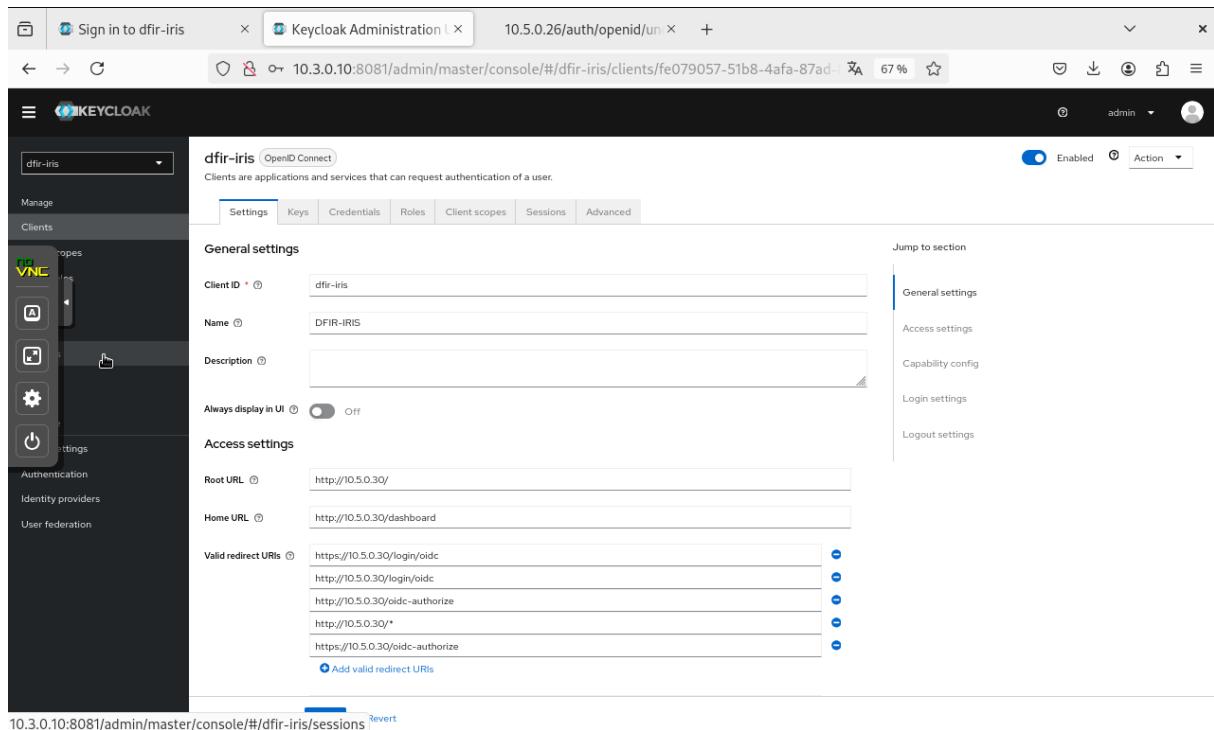


The screenshot shows the Keycloak administration interface. The left sidebar is dark-themed and lists various management sections: Manage, Clients, Realm roles (which is currently selected and highlighted in blue), Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area has a white background and displays a 'Create role' form. At the top of the form, it says 'Realm roles > Create role'. The 'Role name *' field contains the value 'dfir-iris'. Below it is a 'Description' field which is currently empty. At the bottom of the form are two buttons: a blue 'Save' button and a grey 'Cancel' button.

- Dans le realm dédié, créer un client nommé dfir-iris de type OpenID Connect.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Définir les URLs de redirection valides (Valid Redirect URIs) pour permettre l'authentification et le retour vers DFIR-IRIS après connexion (par exemple : <http://10.5.0.30/login/oidc>, [http://10.5.0.30/oidc-authorize](http://10.5.0.30/oidc- authorize), etc.).

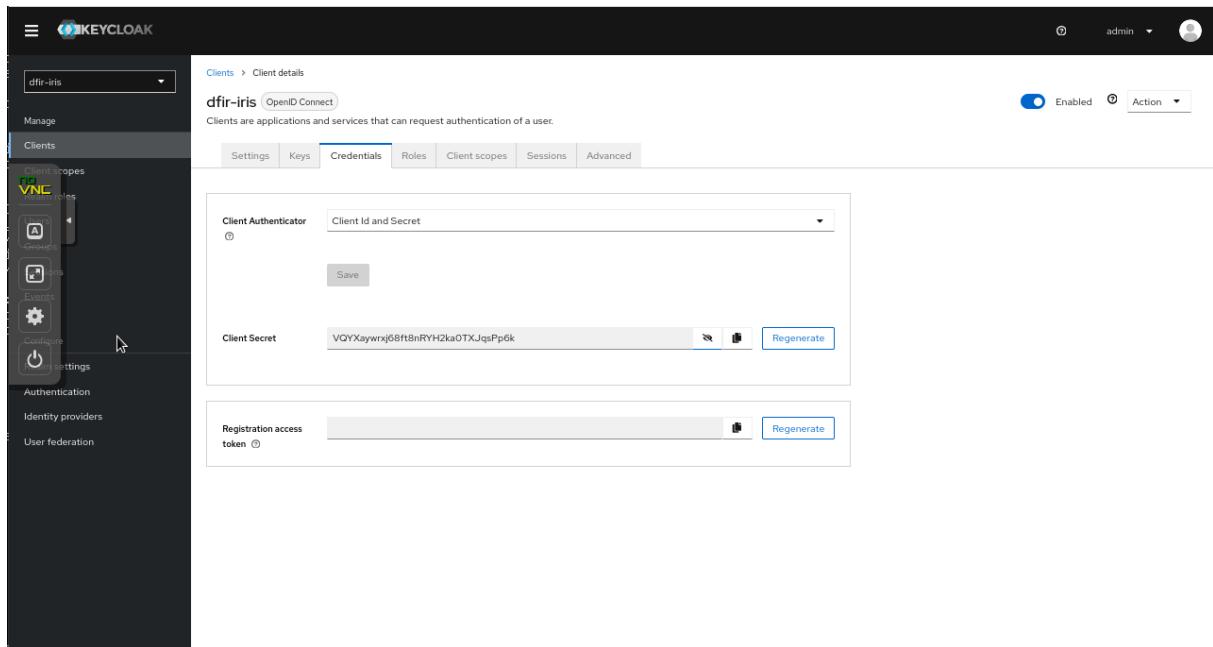


The screenshot shows the Keycloak Administration interface for managing clients. A client named "dfir-iris" is selected. In the "General settings" tab, the "Valid redirect URIs" field contains the following entries:

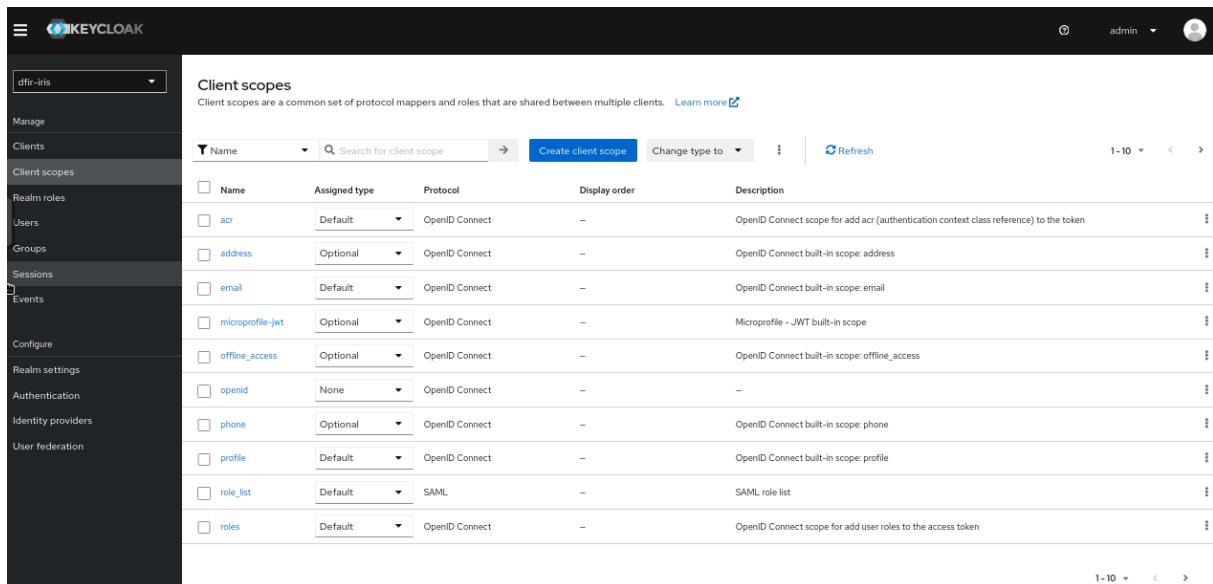
- https://10.5.0.30/login/oidc
- http://10.5.0.30/login/oidc
- http://10.5.0.30/oidc-authorize
- http://10.5.0.30/*
- https://10.5.0.30/oidc-authorize

- Générer et sécuriser le secret client, utilisé pour l'échange de tokens entre DFIR-IRIS et Keycloak.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



- Configurer les rôles et scopes nécessaires selon les besoins de la plateforme



Name	Assigned type	Protocol	Display order	Description
acr	Default	OpenID Connect	–	OpenID Connect scope for add acr (authentication context class reference) to the token
address	Optional	OpenID Connect	–	OpenID Connect built-in scope: address
email	Default	OpenID Connect	–	OpenID Connect built-in scope: email
microprofile-jwt	Optional	OpenID Connect	–	Microprofile - JWT built-in scope
offline_access	Optional	OpenID Connect	–	OpenID Connect built-in scope: offline_access
openid	None	OpenID Connect	–	–
phone	Optional	OpenID Connect	–	OpenID Connect built-in scope: phone
profile	Default	OpenID Connect	–	OpenID Connect built-in scope: profile
role_list	Default	SAML	–	SAML role list
roles	Default	OpenID Connect	–	OpenID Connect scope for add user roles to the access token

4.2. Configuration de DFIR-IRIS pour OIDC

- Modifier le fichier d'environnement de DFIR-IRIS pour activer l'authentification OIDC.
- Ajouter les URLs de redirection valides dans la configuration du client Keycloak pour couvrir tous les cas d'usage (login, logout, wildcards, etc.).

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

```
GNU nano 7.2
CELERY_BROKER=amqp://rabbitmq

# -- AUTH
#IRIS_AUTHENTICATION_TYPE=local
IRIS_AUTHENTICATION_TYPE=oidc

# Config OIDC
OIDC_ISSUER_URL=http://10.3.0.10:8080/realmms/dfir-iris
OIDC_CLIENT_ID=dfir-iris
OIDC_CLIENT_SECRET=VQYXaywrxj68ft8nRYH2ka0TXJqsPp6k

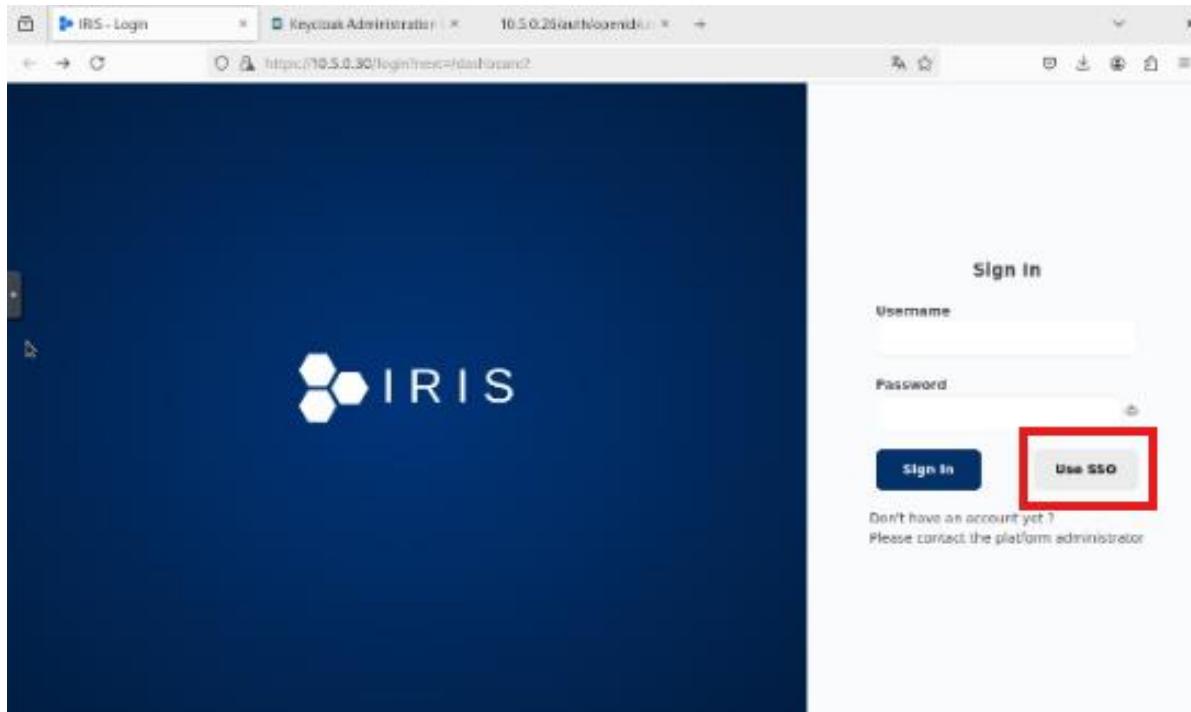
# Forcer l'HTTP
IRIS_FORCE_HTTP=true
IRIS_SECURE_COOKIES=true
OIDC_FORCE_HTTPS=true

# Endpoints spécifiques si nécessaire
OIDC_AUTH_ENDPOINT=https://10.3.0.10:8080/realmms/dfir-iris/protocol/openid-connect/auth
OIDC_TOKEN_ENDPOINT=https://10.3.0.10:8080/realmms/dfir-iris/protocol/openid-connect/token
OIDC_END_SESSION_ENDPOINT=https://10.3.0.10:8080/realmms/dfir-iris/protocol/openid-connect/logout

# Config SSL
REQUESTS_CA_BUNDLE=""[]
PYTHONHTTPSVERIFY=0
SSL_VERIFY=false
```

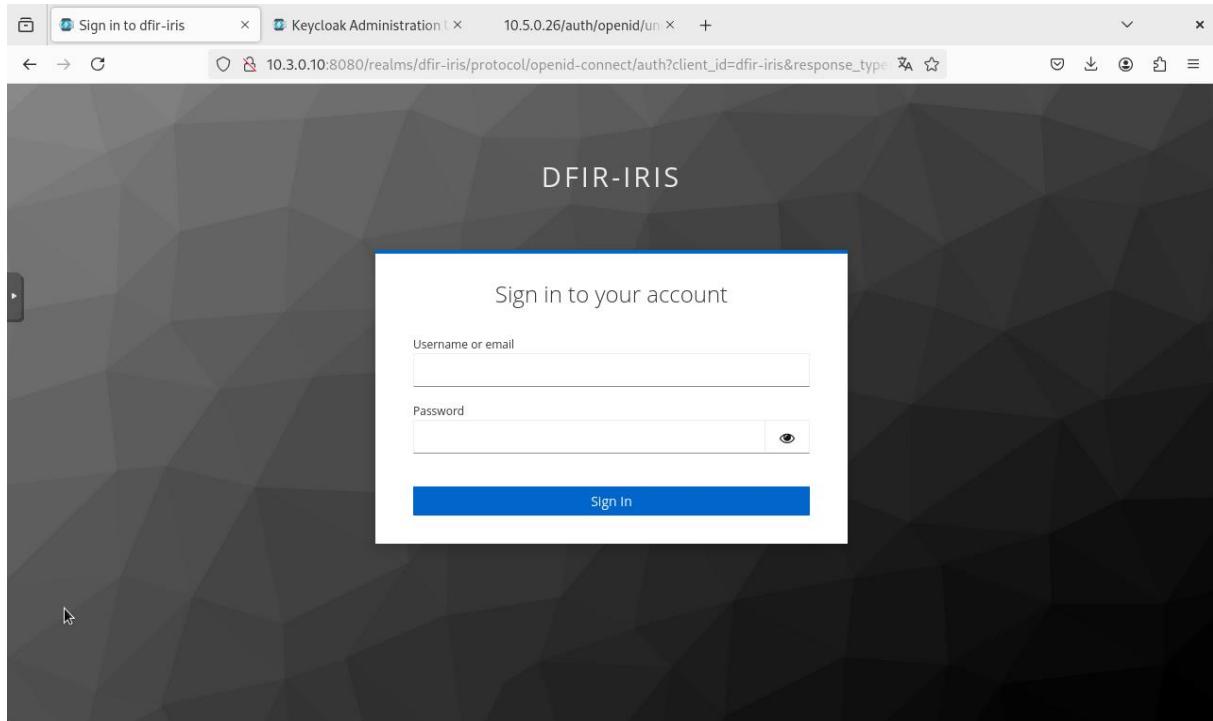
4.3. Validation

- Accéder à la page de connexion DFIR-IRIS, sélectionner “Use SSO”.



Vérifier la redirection vers Keycloak, l’authentification, puis le retour sécurisé sur DFIR-IRIS avec ouverture de session.

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



5. Intégration SSO Keycloak dans Wazuh

5.1. Création et Configuration du Client dans Keycloak

- Utiliser le même realm que DFIR-IRIS dans Keycloak pour centraliser les utilisateurs et métadonnées nécessaires à l'intégration.
- Créer un client de OpenID Connect:
 - Créer un client OIDC, définir les Valid redirect URIs

5.2. Mapping des Rôles et Utilisateurs

- Créer les rôles nécessaires dans le realm Keycloak et les assigner aux utilisateurs ou groupes concernés.
- Ajouter les utilisateurs dans les groupes et effectuer le mapping des rôles dans la configuration du client Keycloak

5.3. Configuration de Wazuh

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Modifier le fichier de configuration de l'indexeur Wazuh (config.yml) pour activer l'authentification via SAML ou OpenID Connect.
- Configurer l'URL du provider, les clés de rôles, et les paramètres de sécurité (SSL, vérification d'hôte, etc.).
- Recharger la configuration et redémarrer les services Wazuh concernés

5.4. Validation

- Vérifier l'apparition du bouton “Login with SSO” sur le dashboard Wazuh.
- Tester le flux d'authentification : redirection vers Keycloak, connexion, puis retour sécurisé sur Wazuh avec session ouverte.
- Vérifier le mapping des rôles et l'accès aux fonctionnalités selon les droits attribués dans Keycloak

ANNEXE INSTALLATION D'UN WINDOWS SERVEUR ACTIVE DIRECTORY

Installation d'un windows server 2025 en français :

<https://www.microsoft.com/fr-fr/evalcenter/download-windows-server-2025>

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Veuillez sélectionner votre téléchargement de Windows Server 2025

Anglais (États-Unis)	Téléchargement ISO Édition 64 bits >	Téléchargement VHD Édition 64 bits >	Essayer Windows Server sur Azure Découvrir plus d'informations >
Chinois (simplifié)	Téléchargement ISO Édition 64 bits >		
Français	Téléchargement ISO Édition 64 bits >		

Importer l'iso dans Proxmox. Il est possible de passer par une installation via une ISO locale.

Storage 'local' on node 'home-s-pve01'

Summary	Upload	Download from URL	Remove
Backups			
ISO Images			
CT Templates			
Permissions			
17763.3650.221105-1748.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_fr-fr.iso			
LinuxMint_2022.iso			
OPNsense-25.1-dvd-amd64.iso			
Qubes-R4.2.1-x86_64.iso			
Win10_22H2_French_x64.iso			
Windows_server_2025.iso			
debian-11.6.0-amd64-netinst.iso			
debian-12.2.0-amd64-netinst.iso			
kali-linux-2023.1-installer-netinst-amd64.iso			
linuxmint-21.3-cinnamon-64bit.iso			
Imde-6-cinnamon-64bit.iso			
pfSense-CE-2.6.0-RELEASE-amd64.iso			
systemrescue-9.06-amd64.iso			
ubuntu-18.04.6-live-server-amd64.iso			
ubuntu-22.04.2-desktop-amd64.iso			
ubuntu-22.04.4-live-server-amd64.iso			
virtio-win.iso			

Télécharger les drivers virtuels sur ce lien :

<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso>

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Task viewer: File virtio/win2025.iso - Download

Output Status

Stop Download

```
--2025-05-26 22:06:07-- https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/virtio-win-0.1.271-1/virtio-win-0.1.271.iso
Reusing existing connection to fedorapeople.org:443.
HTTP request sent, awaiting response... 200 OK
Length: 726501376 (693M) [application/octet-stream]
Saving to: '/var/lib/vz/template/iso/virtio-win2025.iso.tmp_dwnl.2955378'

OK ..... 4% 17.8M 37s
32768K ..... 9% 27.2M 29s
65536K ..... 13% 27.3M 26s
98304K ..... 18% 27.2M 23s
131072K ..... 23% 27.2M 22s
163840K ..... 27% 28.9M 20s
196608K ..... 32% 27.1M 18s
229376K ..... 36% 28.9M 17s
262144K ..... 41% 27.1M 16s
294912K ..... 46% 28.9M 14s
327680K ..... 50% 27.1M 13s
360448K ..... 55% 28.9M 12s
393216K ..... 60% 25.6M 10s
425984K ..... 64% 27.3M 9s
458752K ..... 69% 29.1M 8s
491520K ..... 73% 25.6M 7s
524288K ..... 78% 27.3M 6s
557056K ..... 83% 27.3M 4s
592832K ..... 87% 27.3M 3s
```

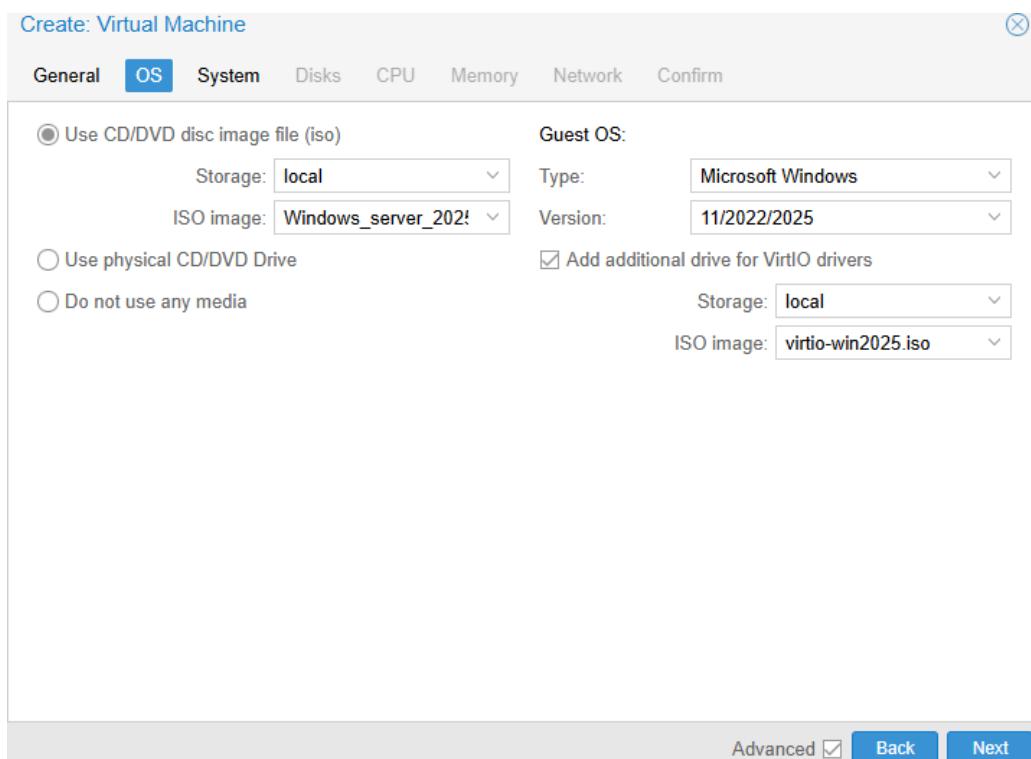
On retrouve 2 iso files :

- La VM
- Les drivers

Storage local on node 'home-s-pve01'					
	Upload	Download from URL	Remove	Search:	Name, Format
	Date				
ISO Images					
17763_3650_221105-1748.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_fr-fr.iso	2023-12-11 11:50:25	iso	5.68 GB		
LinuxMint_207.iso	2024-04-29 14:21:44	iso	1.44 GB		
OPNsense-25.1-dvd-amd64.iso	2025-04-07 21:47:36	iso	2.22 GB		
Qubes-R4.2.1-x86_64.iso	2024-04-02 14:09:49	iso	6.63 GB		
Win10_22H2_French.x64.iso	2023-11-10 22:44:42	iso	6.15 GB		
Windows_server_2025.iso	2025-05-26 21:56:14	iso	6.22 GB		
debian-11.6.0-amd64-netinst.iso	2024-03-01 10:13:03	iso	406.85 MB		
debian-12.2.0-amd64-netinst.iso	2023-11-01 11:22:44	iso	658.51 MB		
kal-linux-2023.1-installer-netinst-amd64.iso	2023-12-04 16:22:34	iso	481.30 MB		
linuxmint-21.3-cinnamon-64bit.iso	2024-04-26 16:42:03	iso	3.07 GB		
Imde-6-cinnamon-64bit.iso	2024-04-28 19:03:55	iso	2.69 GB		
pfSense-CE-2.6.0-RELEASE-amd64.iso	2023-11-01 09:47:55	iso	767.46 MB		
systemrescue-9.06-amd64.iso	2024-01-15 20:25:43	iso	784.33 MB		
ubuntu-18.04.6-live-server-amd64.iso	2024-01-28 14:10:37	iso	1.02 GB		
ubuntu-22.04.2-desktop-amd64.iso	2024-02-20 18:23:40	iso	4.93 GB		
ubuntu-22.04.4-live-server-amd64.iso	2024-03-31 22:03:15	iso	2.10 GB		
virtio-win.iso	2023-11-10 22:59:04	iso	627.52 MB		
virtio-win2025.iso	2025-05-26 22:06:33	iso	726.50 MB		

Nous allons maintenant installer la VM :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



On sélectionne bien les VirtIO driver et l'image file puis on suit les étapes et on lance la machine.

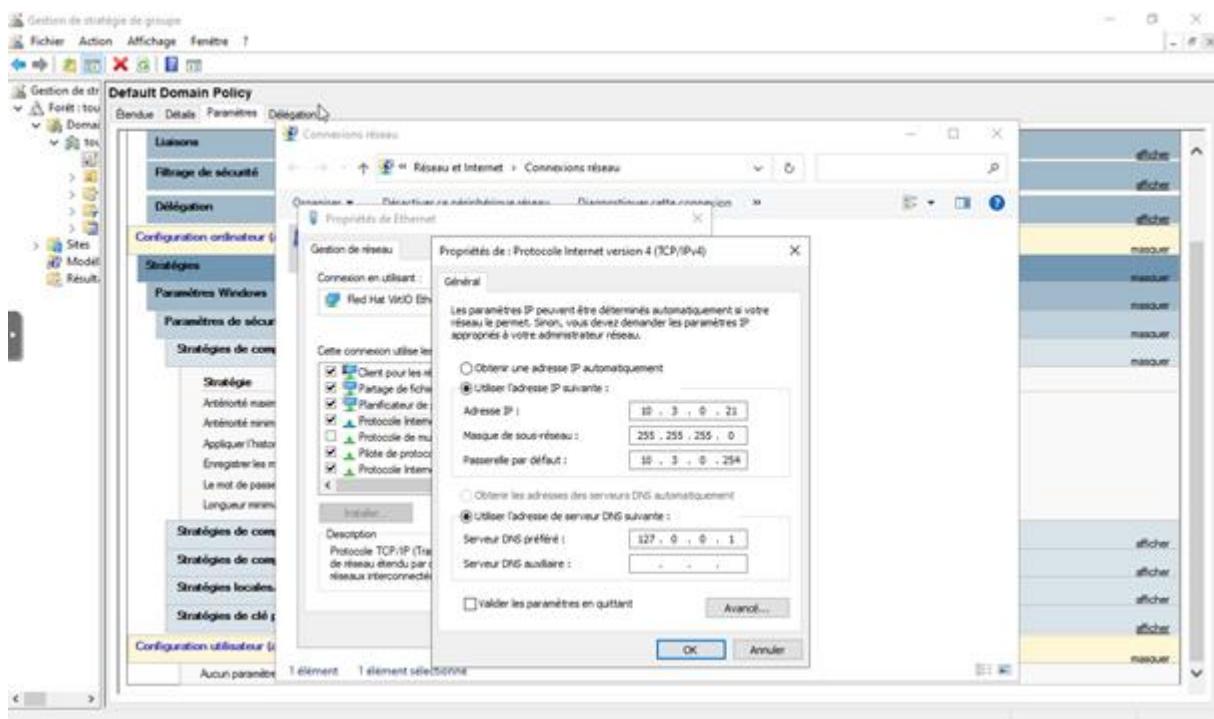
Puis lancement de la machine.

Je définis le nom d'hôte et je vérifie les mises à jour :

1. Préparer le serveur

- Configurer une adresse IP fixe et vérifier la connectivité réseau

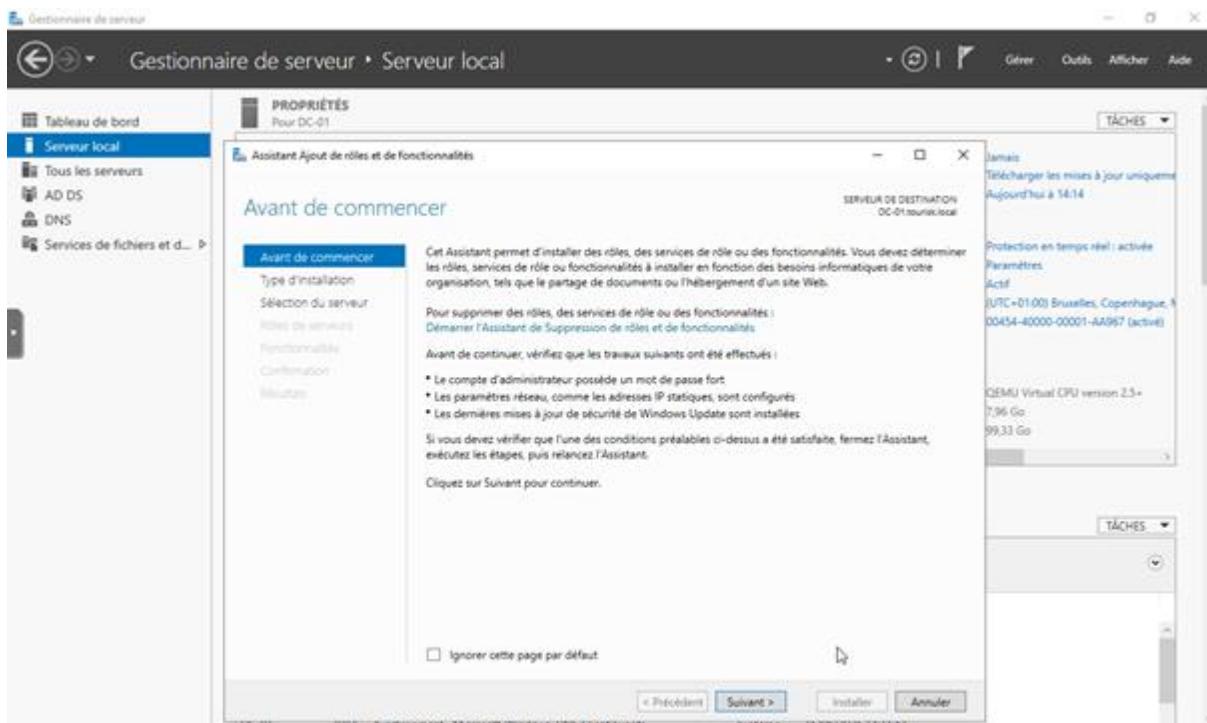
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



2. Ajouter le rôle Active Directory

- Ouvrir le Server Manager.
- Aller dans Gérer > Ajouter des rôles et fonctionnalités.
- Sélectionner Installation basée sur les rôles ou les fonctionnalités.
- Choisir le serveur cible.
- Sélectionner le rôle Services de domaine Active Directory (AD DS) et ajouter les fonctionnalités demandées
- **Poursuivre jusqu'à la page de confirmation et cliquer sur Installer**

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



3. Promotion du serveur en contrôleur de domaine

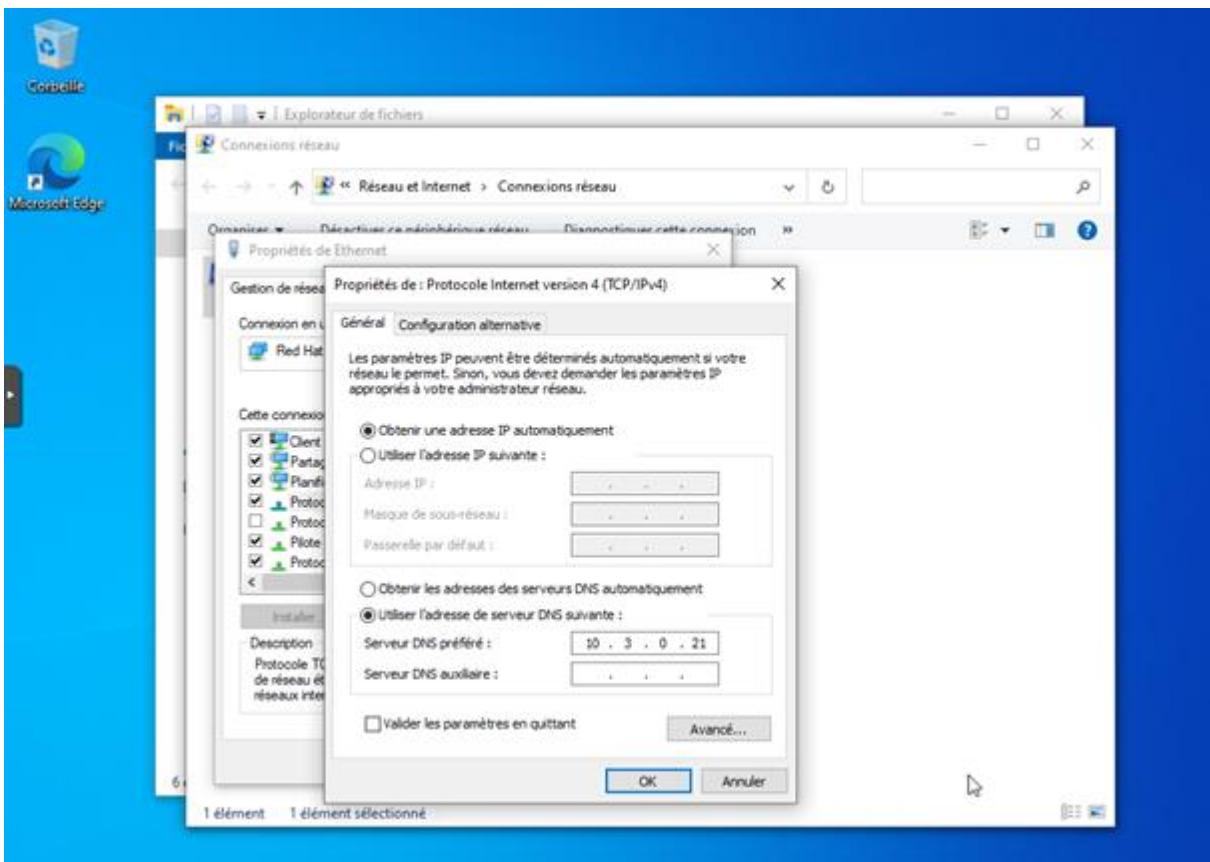
- Après l'installation, cliquer sur le lien Promouvoir ce serveur en contrôleur de domaine.
- Sélectionner Ajouter une nouvelle forêt et définir le nom du domaine racine (ex : entreprise.local).
- Définir le mot de passe du mode de restauration des services d'annuaire (DSRM).
- Suivre les étapes de configuration DNS, NetBIOS, et valider les options.
- Lancer l'installation. Le serveur redémarre automatiquement à la fin

2. Intégration d'une Machine Windows dans l'Active Directory

Préparation

- Vérifier que la machine cliente utilise le DNS du contrôleur de domaine et qu'elle est sur le même réseau

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



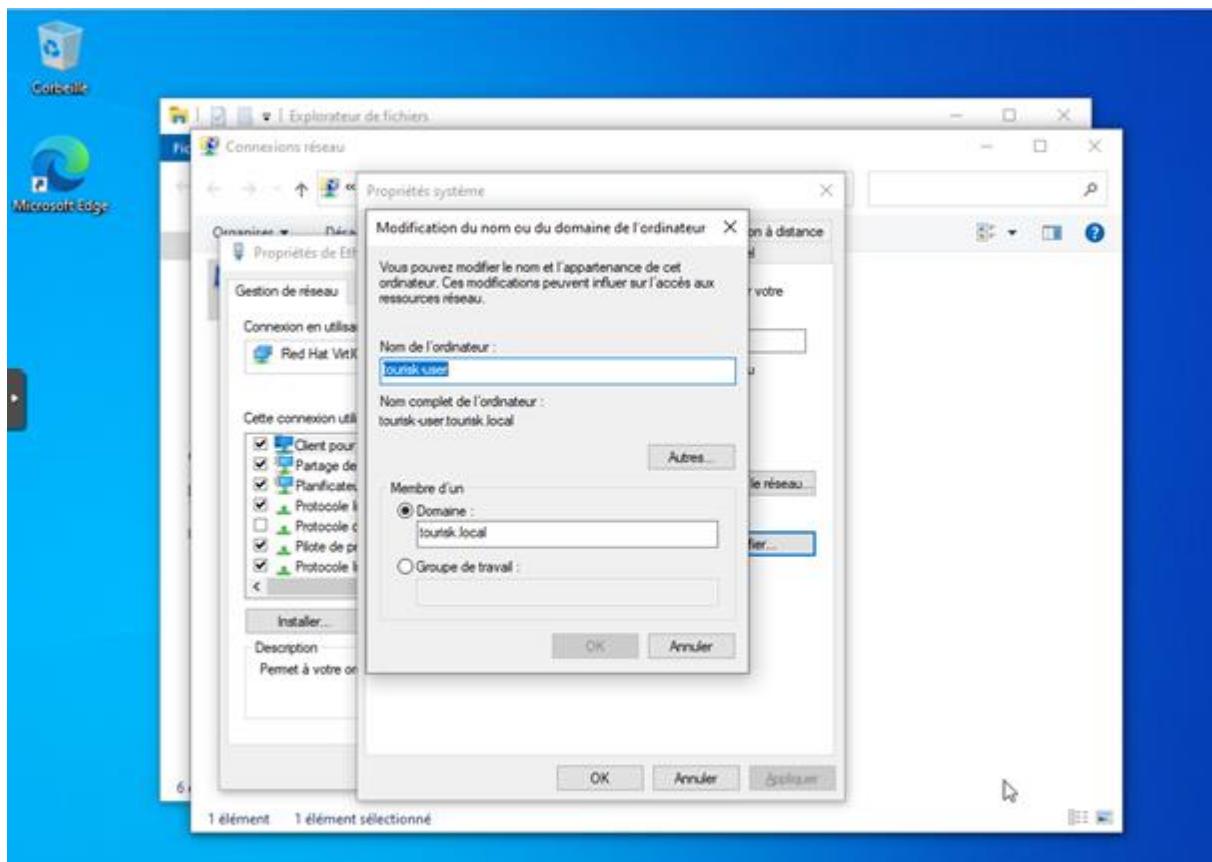
- Optionnel : Renommer le poste pour une identification claire dans l'AD.

Procédure d'intégration

Depuis l'interface graphique :

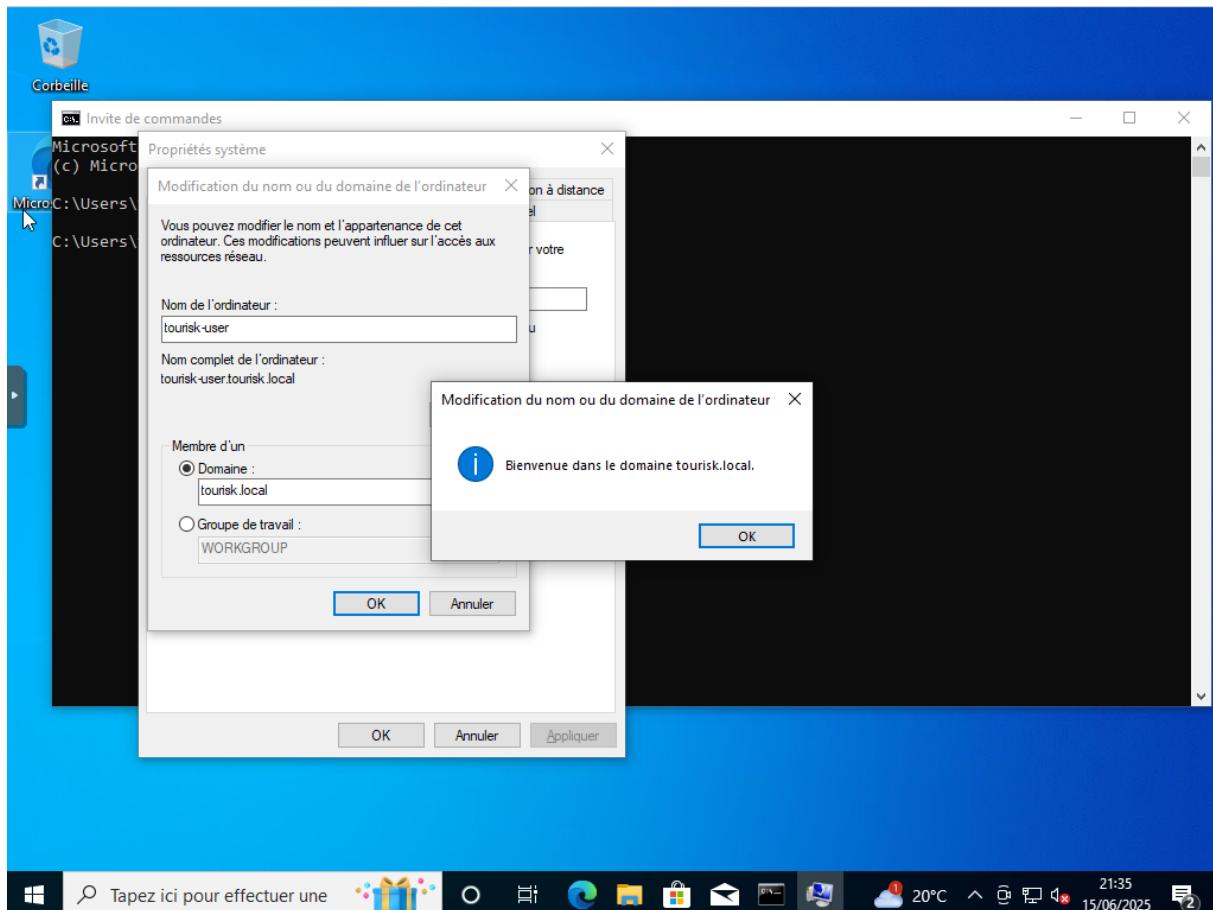
- Aller dans Paramètres > Système > Informations système > Renommer ce PC (avancé) ou clic droit sur Ce PC > Propriétés > Paramètres système avancés.
- Cliquer sur Modifier le nom de l'ordinateur.
- Sélectionner Domaine, entrer le nom du domaine AD (ex : entreprise.local).
- Saisir les identifiants d'un compte autorisé à joindre le domaine.
- Redémarrer la machine après confirmation

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Il faudra ensuite entrer les identifiants administrateurs de l'AD pour ajouter la machine au domaine

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Modification des GPO : Stratégie de Mot de Passe

Objectifs

- Longueur minimale du mot de passe : 10 caractères.
- Durée maximale de validité du mot de passe : 31 jours.

Étapes de configuration

1. Ouvrir la console de gestion des stratégies de groupe (GPMC) sur le contrôleur de domaine

Éditer la GPO du domaine (Default Domain Policy) :

- Naviguer vers : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe

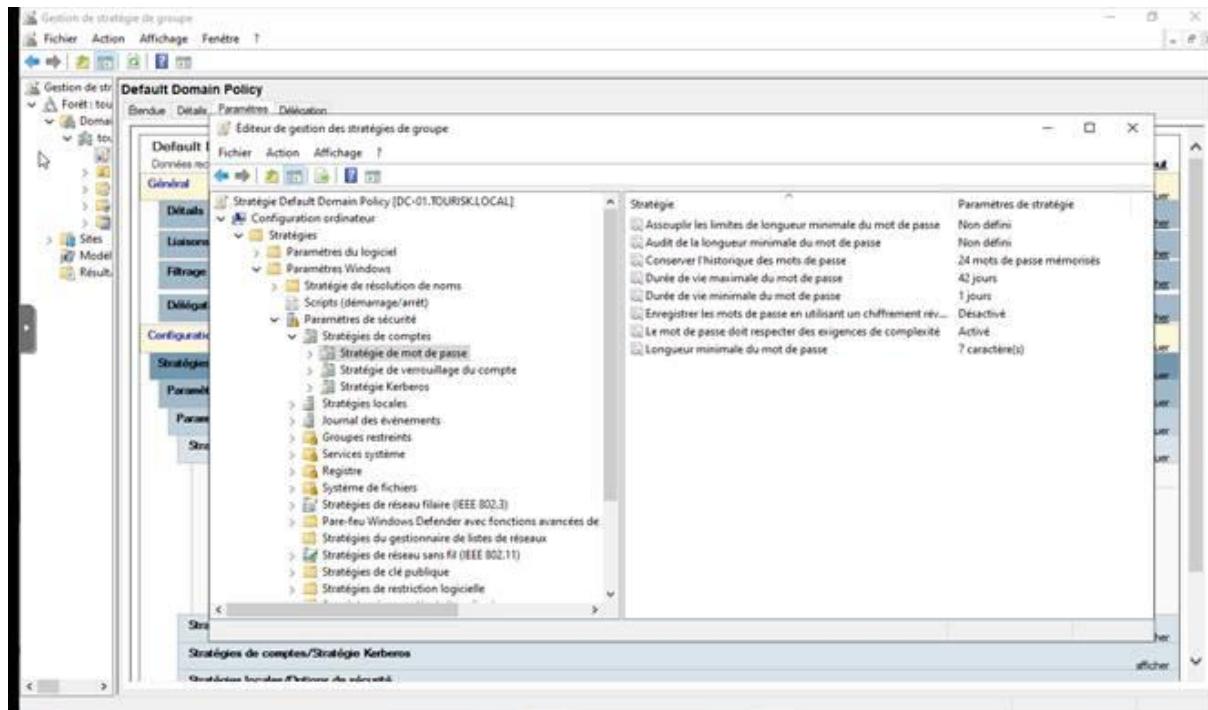
Modifier les paramètres suivants :

- Longueur minimale du mot de passe : mettre 10
- Âge maximal du mot de passe : mettre 31 jours

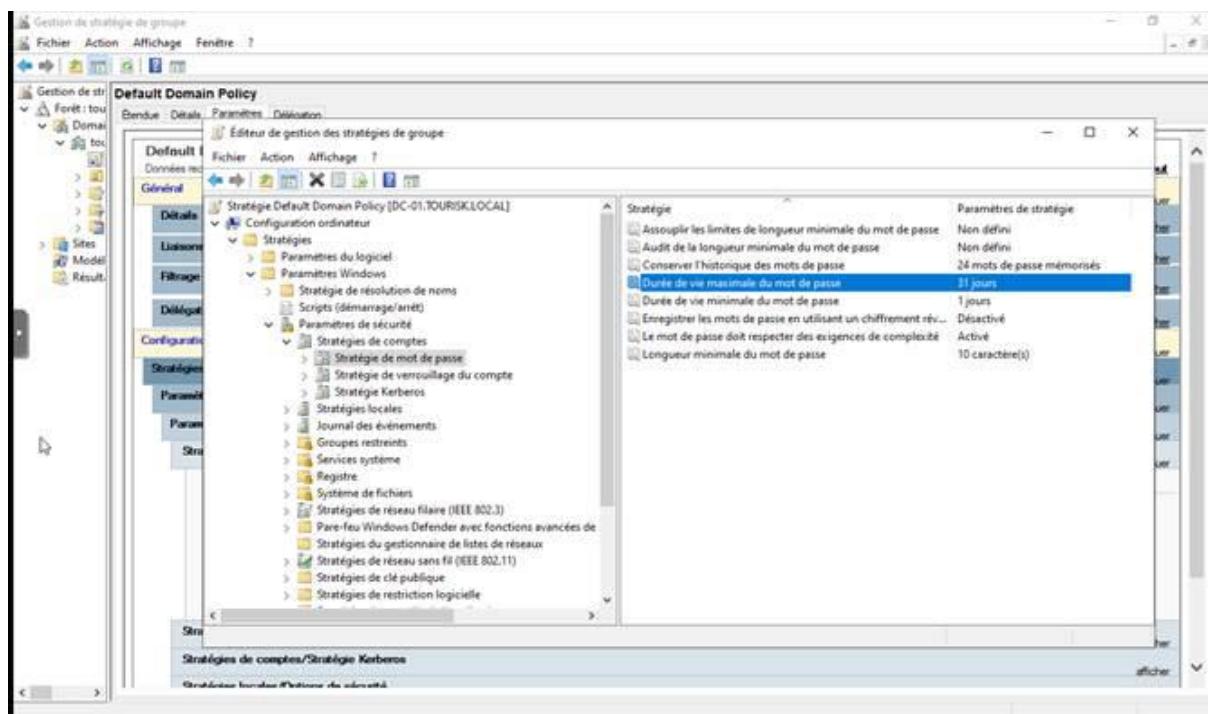
MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Appliquer et valider les modifications.

Par défaut :



Après modification :



Forcer la mise à jour des GPO sur les postes :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

- Ouvrir une invite de commande en administrateur et exécuter :
gpupdate /force

Les nouvelles règles seront appliquées lors du prochain changement de mot de passe par les utilisateurs

4. Bonnes Pratiques

- S'assurer que les utilisateurs sont informés des nouvelles règles de mot de passe.
- Vérifier la prise en compte des GPO sur les postes clients.
- Utiliser la console Active Directory Users and Computers pour vérifier l'intégration des machines et la conformité des utilisateurs aux nouvelles politiques.

ANNEXE APPLICATION WEB

WEB API

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

FastAPI 0.1.0 OAS 3.1

/openapi.json

Authorize 

auth

POST /auth/login Login

POST /auth/signup Signup

insurance

GET /insurance/insurance_requests List Insurance Requests

POST /insurance/insurance_requests Create Insurance Request

GET /insurance/insurance_requests/{request_id} Get Insurance Request

PATCH /insurance/insurance_requests/{request_id}/assign Assign Agent To Request

admin

POST /admin/agents Create Agent

DELETE /admin/agents/{agent_id} Delete Agent

GET /admin/users Get All Users

agent

PUT /agent/insurance/status Update Insurance Status

GET /agent/insurance Get Insurance Requests

DELETE /agent/insurance/{insurance_id} Delete Insurance Request

GET /agent/users Get Clients

GET /agent/users/{user_id} Get Client By Id

Authentication :

login et signup

Jwt :

Les Endpoint ont été développé selon les configurations

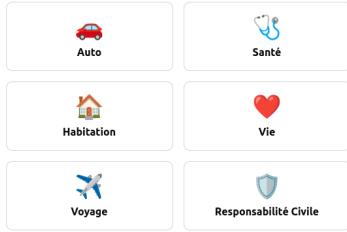
APPLICATION WEB :

CLIENT :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

🛡 Demande d'assurance – Étape 2

Type d'assurance



Durée souhaitée

1 an 2 ans 5 ans

La durée correspond à la période de validité souhaitée de votre contrat.

← Précédent

Suivant

Dernière étape :

🛡 Demande d'assurance – Étape 3

Récapitulatif de votre demande

Prénom : Frank

Nom : Chateau

Email : frank@chateau.com

Téléphone :

Type d'assurance : auto

Durée souhaitée : 1 an

Informations sur le véhicule

Marque : BMW

Modèle : slk

Année : 2010

Immatriculation : ABCDE

Usage : quotidien

Assureur précédent : AXA

Sinistres (5 ans) : 1

Commentaires / Besoins spécifiques

Je souhaite assurer mon véhicule personnel.

Envoyer la demande

← Précédent

AGENT ASSUREUR :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU

Tourisk

Bonjour, James Bond

Logout

Liste des demandes d'assurance

Type	Statut	Date de création	Actions	
habitation	accepted	14/06/2025	Voir détail	Assignée
habitation	accepted	15/06/2025	Voir détail	Assignée
habitation	pending	15/06/2025	Voir détail	Assignée
habitation	accepted	15/06/2025	Voir détail	Assignée

Tourisk

Bonjour, James Bond

Logout

Détails de la demande d'assurance

Type d'assurance : habitation

Statut : pending

Date de création : 15/06/2025 21:32:53

Commentaires : Aucun

First name :

Frank

Last name :

Chateau

Email :

frank@chateau.com

Détails spécifiques :

- first_name : Frank
- last_name : Chateau
- email : frank@chateau.com
- phone :
- insurance_type : habitation
- duration : 2
- comments : Assurance pour logement principal.
- property_type : Maison
- surface : 80
- rooms : 3
- construction_year : 2010
- address : avenue de paris
- postal_code : 75001
- city : Paris

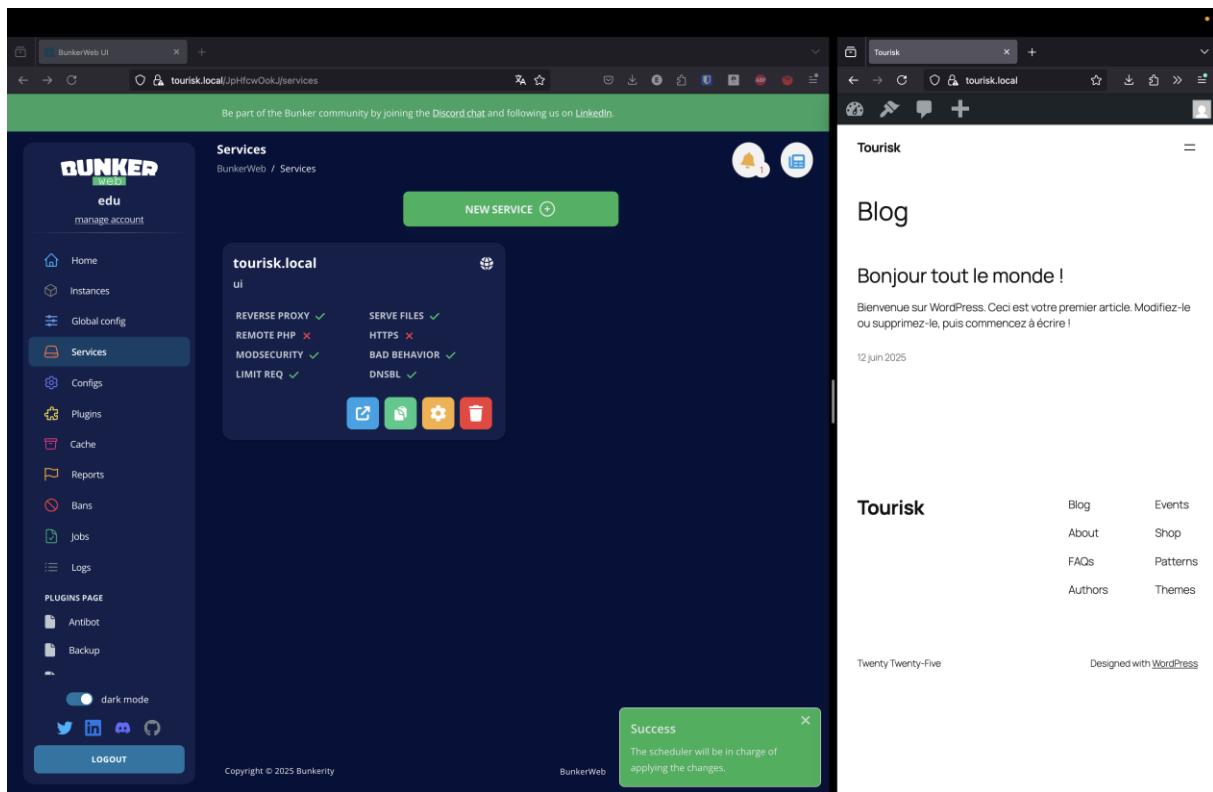
Accepter la demande

Rejeter la demande

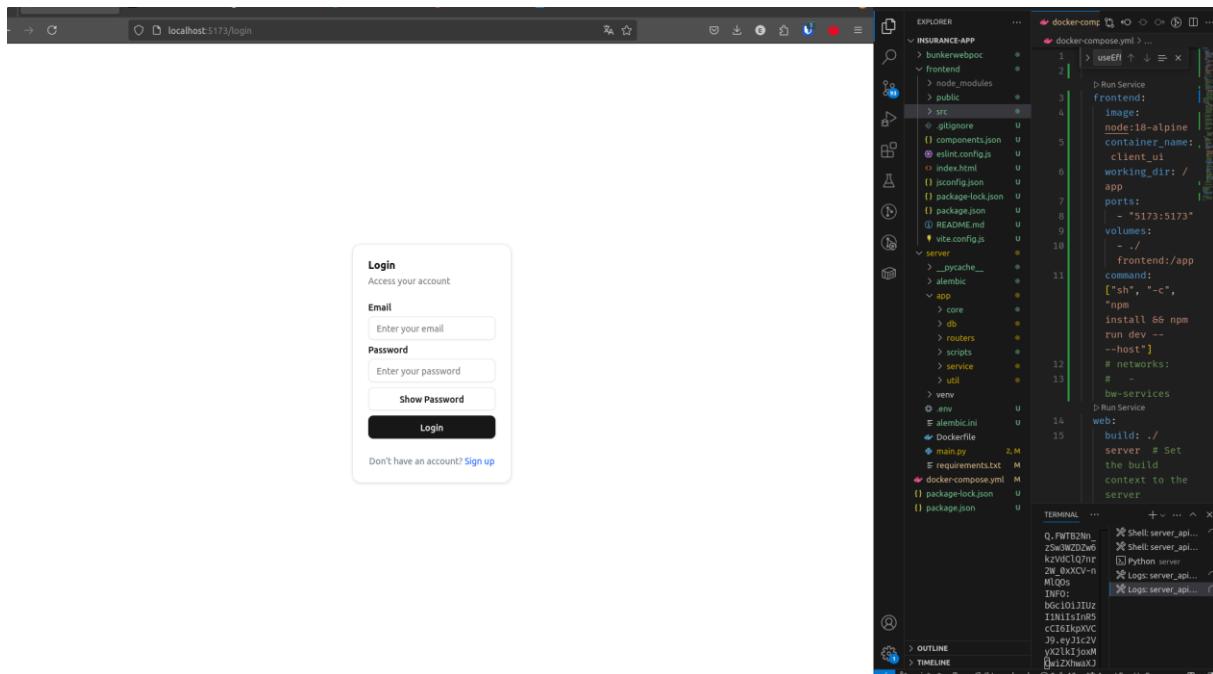
Retour

L'image du WAF configurer :

MISE EN PLACE D'UNE INFRASTRUCTURE RÉSEAU



Voici un exemple de l'aborense du projet :



Lien du projet : <https://gitlab.com/eduardevs/insurance-app>