



LGMS
LINKGUARD MOBILITY
SOLUTIONS

Lucas Natale
Gaël Otto
Matthieu Borie
Sofia Sousa Dos Santos

22/08/2025



Contexte & Gestion de projet

présenté par Sofia

Contexte

Entreprise de type Remote-First (*34 employés*), proposant des services SAAS :

- Drive Cloud Sécurisé

Divisée en deux sites :

- Site principal : **Paris**
- Site secondaire : **Roumanie VPN site-to-site**
- **Accès nomade pour les salariés.**

Outils | Stack technique





Projet Jedha - LGMS

MB LN GO SS

Infos

LGMS
LINKGUARD MOBILITY SOLUTIONS

Infos

This card is a template. 2

4/4

LN GO SS MB

Stack Technique

This card is a template.

GIT

This card is a template.

Liens Utiles / Ressources

This card is a template.

+ Add a card

Features

Cloud File Storage

+ Add a card

Standby

VPN Solutions

+ Add a card

To make

+ Add a card

Production

WAF : ModSecurity + OWASP CRS

8/8

LN

Backup : Siège/Roumanie/Cloud S3

8/8

MB

Routeur/Pare-feu : Pfsense

31/31

MB GO

IDS:IPS : Suricata (Optionnel)

6/6

CI/CD : Github Actions + Trivy

8/8

Linux OS & Sécurité

9/9

GO

Conteneurisation : Docker

7/7

File Server Cloud : NextCloud

5/5

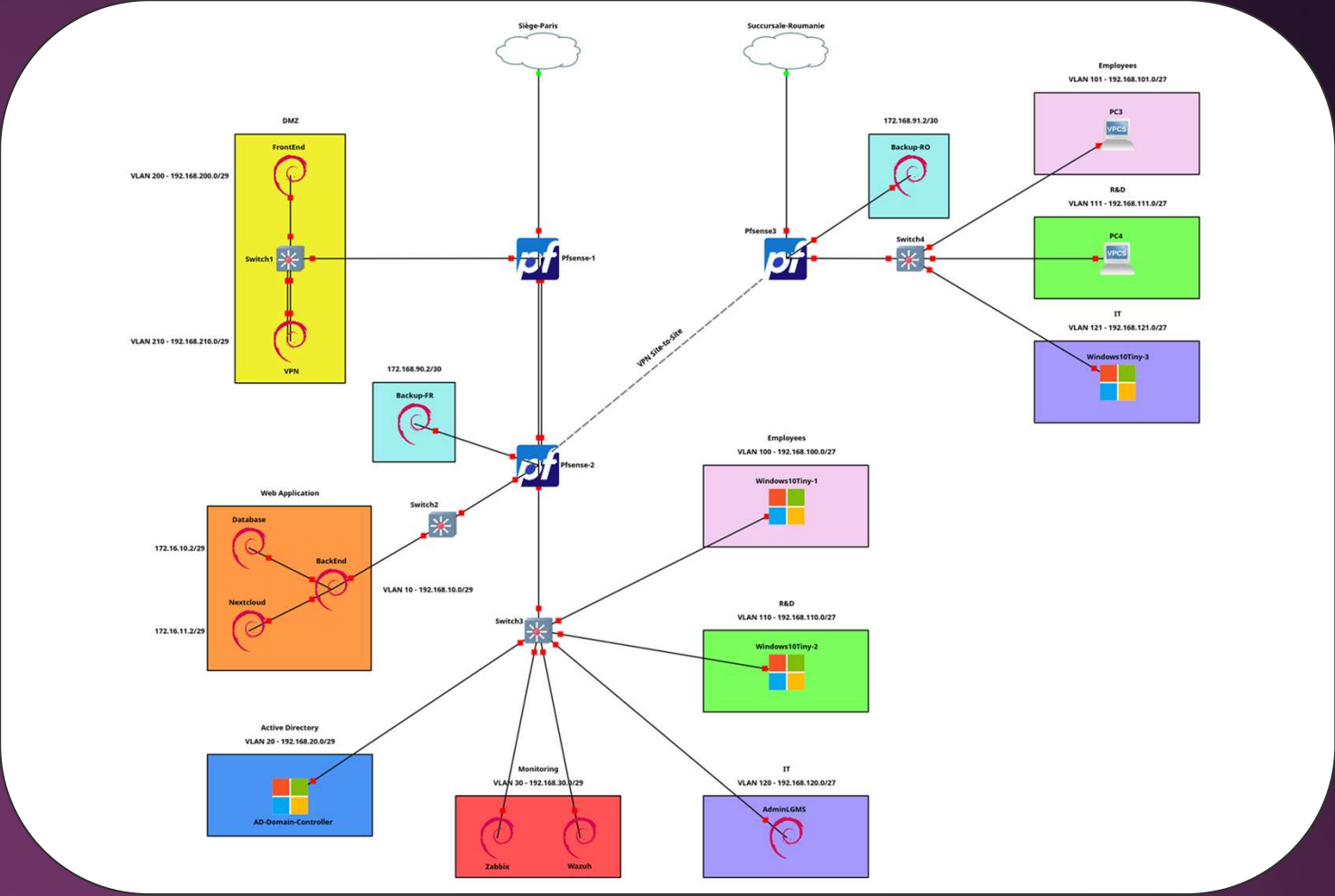
+ Add a card



Infrastructure Réseau & Sécurité

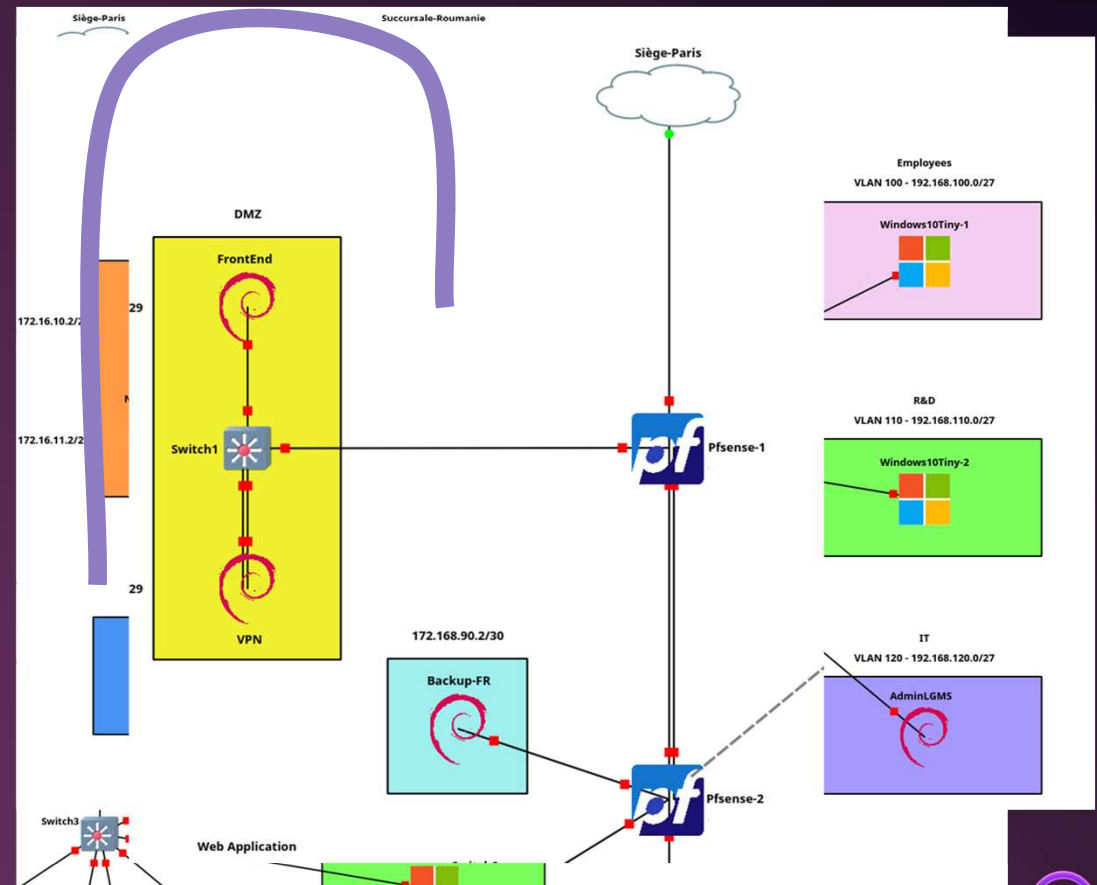
présenté par Matthieu





Infrastructure Réseau & Sécurité

- Défense en profondeur
 - Site principal : 2 pfSense et une DMZ
- 2 sites physiques
 - VPN Site-to-site
- Segmentation VLAN et switchs sécurisés
- Debian & UFW
- Active Directory
 - Authentification centralisée
 - Serveur de fichiers partagés
- Employés nomades : Wireguard



Application client & Chaine CI/CD

présenté par Lucas



Intl / LGMS

Type to search

<> Code Issues Pull requests Actions Projects 1 Security Insights Settings

LGMS Private Watch 0 Fork 0 Star 0

master 5 Branches 0 Tags

Go to file Add file <> Code

Switch branches/tags

Find or create a branch...

Branches Tags

✓ master default

deploy

gael

lucas

matthieu

View all branches

0ad8fd6 · 2 days ago 343 Commits

change branche deploy 4 days ago

· 2 days ago

stable version 2 days ago

add remove back fix 2 days ago

· 2 days ago

stable 2 days ago

Recherche et test sur modsecurity last week

add front last week

· 2 days ago

Fichier EasterEgg 2 weeks ago

Mise à jour 4 days ago

About

JedhaProject

Readme

Activity

0 stars

0 watching

0 forks

Releases

No releases published

Create a new release

Packages

No packages published

Publish your first package

Contributors 4

spideraid

cicd.yml

on: push

✓ Tests frontend 28s

○ dependency-review

✓ backend-security 36s



A large, abstract, glowing ring with a gradient of colors (yellow, orange, red, pink, purple, blue, green) against a dark background.

A stylized 'LG' logo inside a cloud-like shape.

LinkGuard

Mobility Solutions


Connexion

Inscription

Se connecter







LinkGuard
Mobility Solutions

Dashboard







Déconnexion

© 2025 LinkGuard - Mobility Solutions

Dashboard

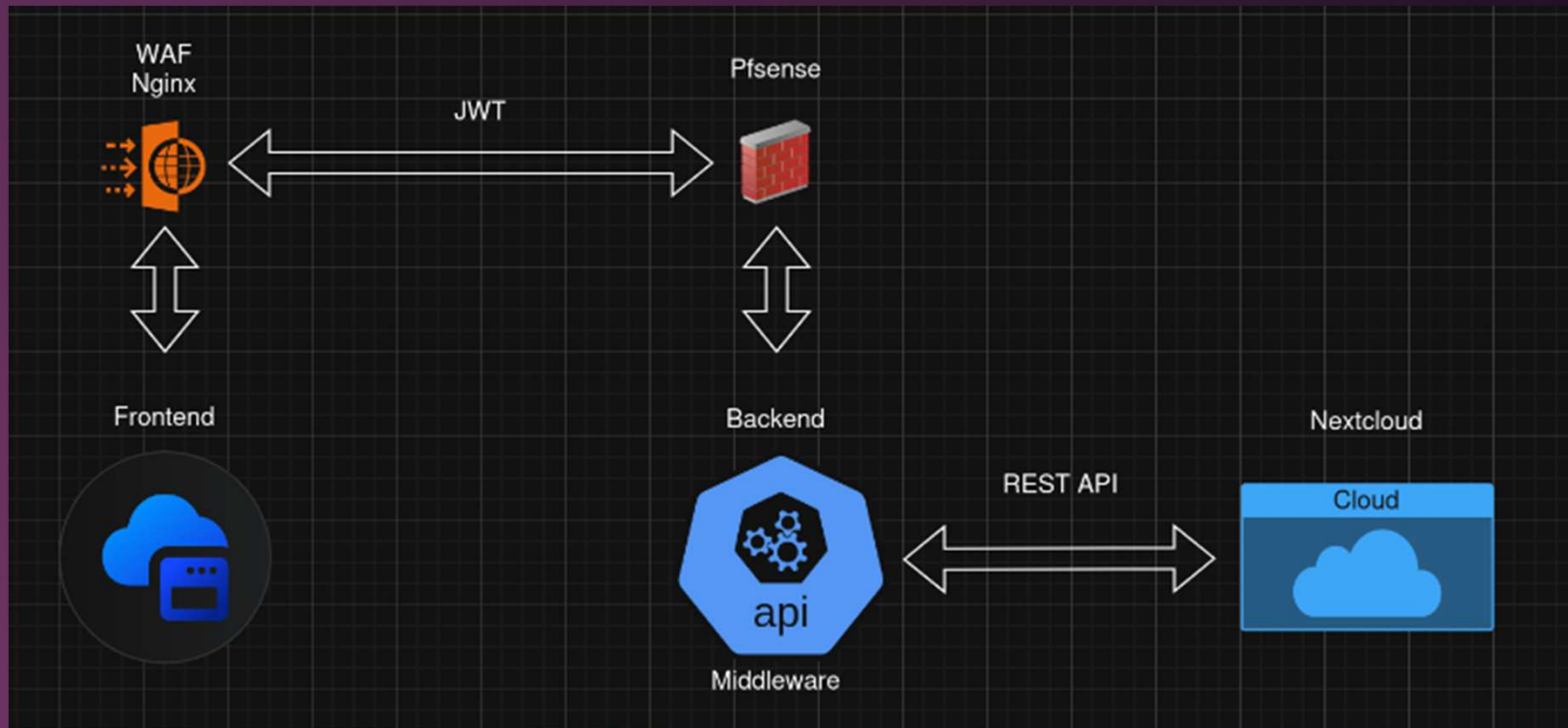
Bienvenu dans votre espace cloud

Uploader

Nom	Taille	Modifié le	Actions
 file(1)(1).svg	0.8 Ko	Sun, 17 Aug 2025 21:33:13 GMT	 
 file(1).svg	0.8 Ko	Thu, 14 Aug 2025 16:03:22 GMT	 



Système Frontend | Backend



Dockerisation du Frontend, Backend, Nextcloud

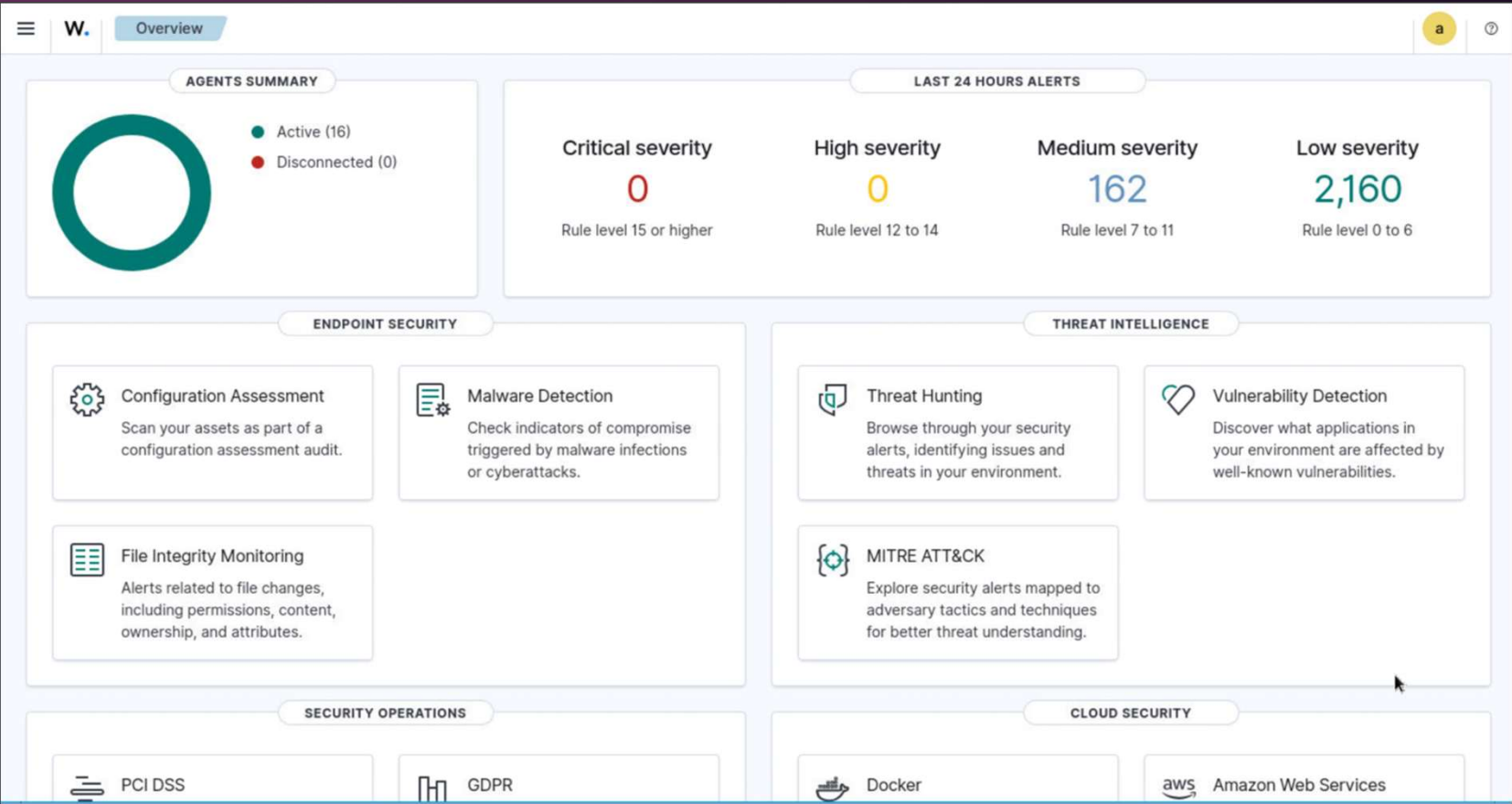
Systeme de Monitoring & Détection d'Intrusion

présenté par Sofia

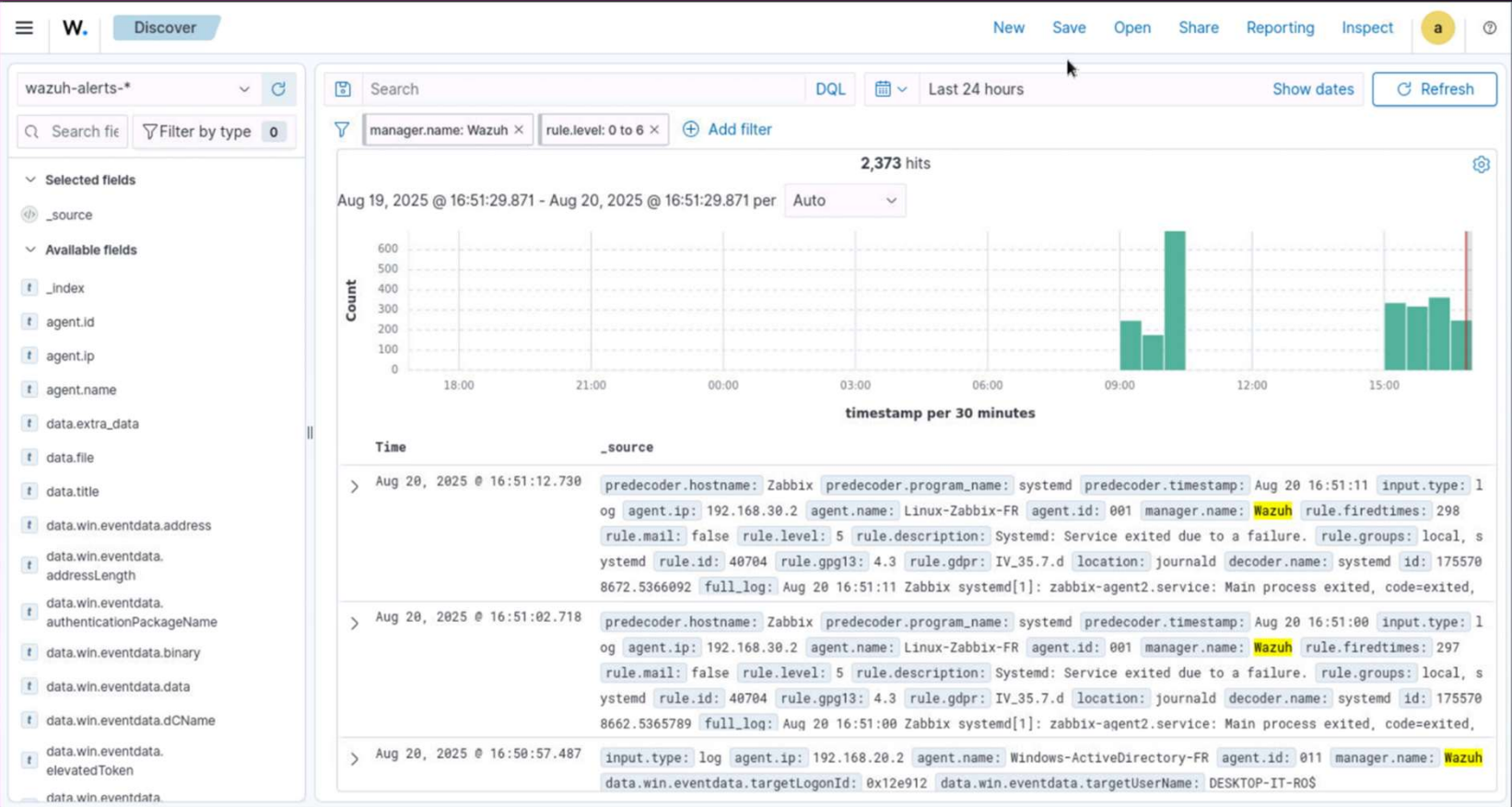


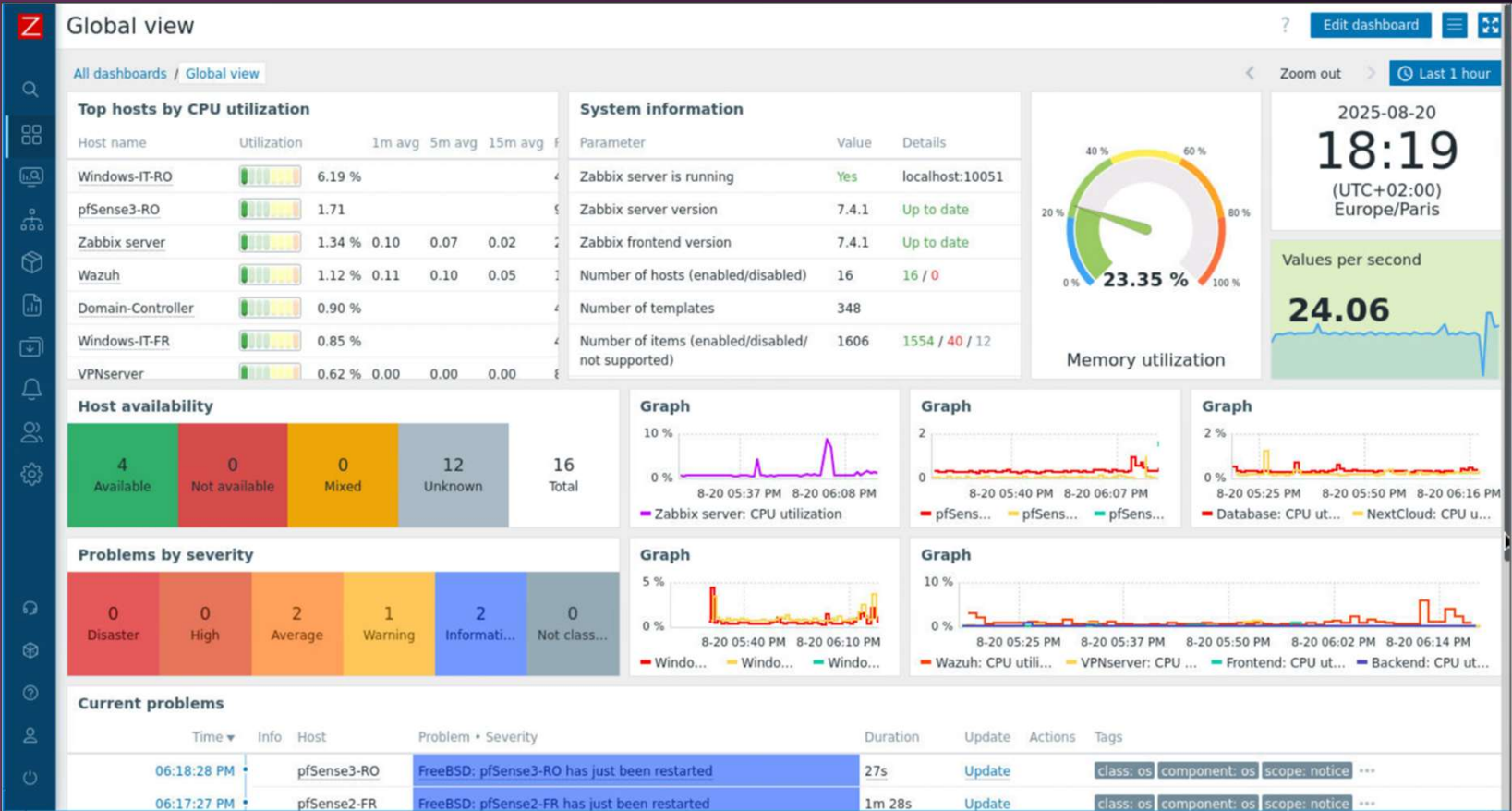
Système de Monitoring

- Wazuh
 - Détection & corrélation d'événements (SIEM)
 - Vue sur l'intégrité des endpoints et logs système
 - Zabbix
 - Supervision performance & disponibilité
 - Indicateurs : CPU, mémoire, services, alertes temps réel
- Agent Wazuh et Zabbix sur les équipements
- Suricata
 - Détection d'intrusion & analyse réseau
 - Informations sur les tentatives d'attaque & anomalies réseau



Wazuh | Dashboard Alerts







Z

Hosts

?

Create host

<

>

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software subclass: logging ***	Enabled	Latest data 143	Problems	Graphs 14	Dashboards 4	Web
Windows-IT-RO	192.168.121.2:10050	ZBX	class: os target: windows	Enabled	Latest data 106	1	Graphs 12	Dashboards 3	Web
Windows-IT-FR	192.168.110.2:10050	ZBX	class: os target: windows	Enabled	Latest data 106	Problems	Graphs 12	Dashboards 3	Web
Windows-Employees-FR	192.168.100.2:10050	ZBX	class: os target: windows	Enabled	Latest data 108	Problems	Graphs 14	Dashboards 3	Web
Wazuh	192.168.30.3:10050	ZBX	class: os target: linux	Enabled	Latest data 68	Problems	Graphs 16	Dashboards 3	Web
VPNserver	192.168.210.2:10050	ZBX	class: os target: linux	Enabled	Latest data 86	Problems	Graphs 16	Dashboards 3	Web
pfSense3-RO	10.200.200.2:10050	ZBX	class: os target: freebsd	Enabled	Latest data 129	Problems	Graphs 37	Dashboards 2	Web
pfSense2-FR	192.168.30.1:10050	ZBX	class: os target: freebsd	Enabled	Latest data 143	Problems	Graphs 44	Dashboards 2	Web
pfSense1-FR	192.168.1.1:10050	ZBX	class: os target: freebsd	Enabled	Latest data 133	Problems	Graphs 39	Dashboards 2	Web
NextCloud	172.16.11.2:10050	ZBX	class: os target: linux	Enabled	Latest data 68	Problems	Graphs 14	Dashboards 3	Web
Frontend	192.168.200.2:10050	ZBX	class: os target: linux	Enabled	Latest data 68	Problems	Graphs 16	Dashboards 3	Web
Domain-Controller	192.168.20.2:10050	ZBX	class: os target: windows	Enabled	Latest data 109	Problems	Graphs 14	Dashboards 3	Web
Database	172.16.10.2:10050	ZBX	class: os target: linux	Enabled	Latest data 68	Problems	Graphs 14	Dashboards 3	Web
Backup-RO	192.168.91.2:10050	ZBX	class: os target: linux	Enabled	Latest data 68	Problems	Graphs 14	Dashboards 3	Web
Backend	192.168.10.2:10050	ZBX	class: os target: linux	Enabled	Latest data 86	Problems	Graphs 18	Dashboards 3	Web
AdminLGMS	192.168.120.2:10050	ZBX	class: os target: linux	Enabled	Latest data 77	1	Graphs 15	Dashboards 3	Web


































































































Displaying 16 of 16 found

Zabbix 7.4.1. © 2001-2025, Zabbix SIA



Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with **highlighted** rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
08/20/2025 11:22:35		3	TCP	Generic Protocol Command Decode	172.67.157.37   	443	192.168.122.10  	48079	1:2210054   	SURICATA STREAM excessive retransmissions
08/19/2025 16:35:48		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:35:34		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:35:27		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:35:07		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:34:45		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:34:38		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:34:38		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:34:10		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:34:08		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:33:59		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum
08/19/2025 16:33:56		3	UDP	Generic Protocol Command Decode	192.168.122.10  	63816	192.168.122.43  	51820	1:2200075   	SURICATA UDPv4 invalid checksum

Automatisation Hardening & Backup

présenté par Gaël



Pourquoi Ansible ?

- Uniformisation des configurations
- Déploiement via ssh (pas d'agents)
- Exécution sur tous les serveurs simultanément
- Automatisé -> moins d'erreurs, plus de fiabilité



Ansible Playbooks

1. Bootstrap Ansible
2. Ouverture de ports temporaire pour la maintenance
3. Mise à jour des serveurs
4. Renforcement/Hardening
5. Intégrité et persistance des logs



Renforcement/Hardening

- UFW
- Fail2Ban
- Auditd
- Unattended-upgrades
- AppArmor
- Lynis
- Historique de commandes désactiver
- Journald persistant et rotation des logs
- Désactivation de la connexion ssh avec l'utilisateur "root"
- Connexion SSH uniquement par clé chiffré
- Noexec / Nodev / Nosuid sur /tmp, /var/tmp, /dev/shm



Système de Backups

- Sauvegarde sur 2 sites:
 - Backup serveur situé en France
 - Backup serveur situé en Roumanie

- Données chiffrées avant transfert (GPG)
- Sauvegarde automatique journalière
- Rotation des sauvegardes 90 Jours



Points d'amélioration & Roadmap

présenté par Lucas



Points d'améliorations

Court terme

- Règles personnalisées pour les systèmes de détection intrusion
- Sauvegarde supplémentaire dans un cloud AWS (S3 Glacier)
- Redondance Multi-WAN

Moyen terme

- Ajout de services :
 - ◆ Gestion de mail
 - ◆ Gestion de calendrier
 - ◆ Location de VPN
- Redondance Domain-Controller
- Load-balancing sur les applications web (Docker Swarm)

Long terme

- Scalabilité de l'infrastructure pour les environnements critiques (secteur public, médical)

Q & A

Merci de votre attention !