



Nagios XI — Supervision réseau StadiumCompany

BTS SIO SISR

2025-2026

Sommaire.

Nagios XI — Supervision réseau StadiumCompany

01

1. Contexte et présentation du projet

- 1.1 Présentation de StadiumCompany
- 1.2 Problématique
- 1.3 Solution retenue : Nagios XI
- 1.4 Hôtes supervisés

02

2. Accès à Nagios XI et Auto-Discovery

- 2.1 Accès à l'interface web
- 2.2 Auto-Discovery

03

3. Configuration des hôtes et services

- 3.1 Services configurés sur chaque hôte
- 3.2 Hermes-AD — Contrôleur de domaine
- 3.3 GLPI — Serveur Helpdesk
- 3.4 HAProxy — Load Balancer (LAN_DMZ)

04

4. Problèmes rencontrés et résolutions

- 4.1 Problème 1 — Le symbole ! dans Manage Hosts
- 4.2 Problème 2 — Arguments invalides (!!!!!!!)
- 4.3 Problème 3 — Check_period manquant
- 4.4 Ce que ces problèmes apportent

05

5. Résultats de la supervision

- 5.1 Dashboard final — Vue globale
- 5.2 Services opérationnels
- 5.3 Simulation d'une panne

06

6. Bilan du projet

- 6.1 Apports pour StadiumCompany
- 6.2 Difficultés rencontrées
- 6.3 Conclusion

1. Contexte et présentation du projet

1.1 Présentation de StadiumCompany

StadiumCompany est l'organisation fictive utilisée dans le cadre de la formation BTS SIO à l'IRIS MediaSchool. Elle dispose d'une infrastructure réseau complète virtualisée sur VMware ESXi, comprenant plusieurs serveurs Windows et Linux répartis sur plusieurs VLANs.

VLAN	Réseau / Rôle
LAN_SERVER	172.20.1.0/24 — Serveurs (AD, DNS, DHCP, Nagios, GLPI, OCS...)
LAN_EQUIPE	172.20.2.0/24 — Postes clients
LAN_WIFI	172.20.3.0/24 — Accès sans fil
LAN_DMZ	172.20.4.0/24 — Services exposés (Zimbra, HAProxy, IIS)

Le pare-feu pfSense Heimdall assure le routage inter-VLAN et la sécurité entre les différents segments réseau. Les règles de filtrage de pfSense jouent un rôle important dans ce projet de supervision.

1.2 Problématique

L'infrastructure de StadiumCompany compte de nombreux serveurs critiques répartis sur plusieurs VLANs. Sans outil de supervision centralisé, un administrateur ne peut pas savoir en temps réel si un serveur est tombé en panne ou si un service a cessé de fonctionner.

Exemple : si Hermes-AD tombe, plus aucun utilisateur ne peut s'authentifier. Si GLPI tombe, le helpdesk est inaccessible. Sans supervision, ces pannes peuvent passer inaperçues pendant des heures.

1.3 Solution retenue : Nagios XI

Nagios XI est un logiciel de supervision réseau et système professionnel. Il permet de surveiller en temps réel l'état des serveurs et de leurs services, et d'envoyer des alertes automatiques en cas de panne.

- Surveillance automatique 24h/24 sans intervention humaine
- Détection immédiate des pannes avant que les utilisateurs ne le signalent
- Tableau de bord centralisé avec l'état de toute l'infrastructure
- Historique des incidents et des statuts

1.4 Hôtes supervisés

Hôte	IP	VLAN	Rôle
Hermes-AD	172.20.1.2	LAN_SERVER	Contrôleur de domaine Active Directory + DNS
GLPI	172.20.1.8	LAN_SERVER	Helpdesk et gestion de parc informatique
HAProxy	172.20.4.5	LAN_DMZ	Load Balancer — répartiteur de charge
localhost	127.0.0.1	—	Serveur Nagios XI lui-même (auto-supervision)
nagiosxi	172.20.1.9	LAN_SERVER	Interface web Nagios XI

2. Accès à Nagios XI et Auto-Discovery

2.1 Accès à l'interface web

Paramètre	Valeur
URL d'accès	https://172.20.1.9/nagiosxi
Identifiant	nagiosadmin
Version	Nagios XI — Trial

The screenshot displays the Nagios XI Home Dashboard. At the top, there are navigation tabs for Views, Dashboards, Reports, Configure, Tools, Admin, and Enterprise. The main content area is divided into several sections:

- Host Status Summary:** A table showing the status of hosts. It includes columns for Up, Down, Unreachable, and Pending. The 'Unhandled' row shows 1 problem.
- Service Status Summary:** A table showing the status of services. It includes columns for OK, Warning, Unknown, Critical, and Pending. The 'Unhandled' row shows 21 problems.
- Need Help?:** A section with links to Support Forum, Help Resources, Nagios AnswerHub, and Phone Support.
- Trial Resources:** A section with links to View Pricing, Compare Editions, Attend a Webinar, Request a Quickstart, and Request a Demo.
- Getting Started:** A section with cards for Run a Wizard, Account Settings, and Notifications.
- Administrative Tasks:** A section with cards for Add a User, Mail Settings, Explore the CCM, and Run Autodiscovery.
- Popular Wizards:** A section with cards for Amazon S3, MySQL Server, Google Cloud, NCPA, Docker, and SNMP Walk.

2.2 Auto-Discovery

L'outil Auto-Discovery de Nagios XI a été utilisé pour scanner automatiquement le réseau 172.20.1.0/24 et détecter les machines disponibles. Ce scan est similaire à un scan nmap — il détecte toutes les machines qui répondent sur le réseau.

The screenshot shows the Nagios XI interface for 'Auto-Discovery Jobs'. The top navigation bar includes 'Views', 'Dashboards', 'Reports', 'Configure', 'Tools', 'Admin', and 'Enterprise'. The left sidebar has 'Quick View' and 'Details' sections. The main content area displays a table of auto-discovery jobs. The table has the following data:

Scan Target	Exclusions	Schedule	Last Run	Devices Found	Created By	Status	Actions
172.20.1.0/24	-	Once	2023-01-01 00:25:25	2 New / 2 Total	nagiosadmin	Finished	[Refresh] [Print] [Close]

3. Configuration des hôtes et services

3.1 Services configurés sur chaque hôte

Pour chaque hôte supervisé, des services ont été configurés manuellement via le Core Config Manager afin de surveiller les fonctionnalités critiques de chaque serveur.

Hôte	Service	Port	Commande	Rôle
Hermes-AD	PING-DISPONIBILITE	ICMP	check_ping	Vérifie que le serveur AD répond
Hermes-AD	LDAP - Active Directory	389	check_tcp	Vérifie que l'AD est opérationnel
Hermes-AD	SMB - Partage de fichiers	445	check_tcp	Vérifie le partage Windows
Hermes-AD	TCP - NetBIOS	139	check_tcp	Vérifie les communications Windows
GLPI	HTTP - Interface Web	80	check_tcp	Vérifie que l'interface GLPI répond
GLPI	MariaDB - Base de données	3306	check_tcp	Vérifie que la BDD est active
HAProxy	PING	ICMP	check_ping	Non joignable — bloqué par pfSense

Nagios XI Views Dashboards Reports Configure Tools Admin Enterprise

Core Config Manager

Service Management

Common Settings Check Settings Alert Settings Misc Settings

Config Name *
Hermes-AD

Description *
SMB -Partage de fichiers

Display name
DNS-Port 53

Check command
check_tcp

Command view
\$USER1\$/check_tcp -H \$HOSTADDRESS\$ -p \$ARG1\$ \$ARG2\$

\$ARG1\$ 445

\$ARG2\$

\$ARG3\$

\$ARG4\$

\$ARG5\$

\$ARG6\$

\$ARG7\$

\$ARG8\$

Add Arguments + Delete Arguments -

Run Check Command

Manage Hosts 1

Manage Templates 0

Manage Host Groups 0

Manage Service Groups 1

Active

Save Cancel

Chaque service est configuré avec : vérification toutes les 5 minutes (check_interval : 5), 3 tentatives avant alerte (max_check_attempts : 3), surveillance 24h/24 7j/7 (check_period : 24x7).

Nagios XI Views Dashboards Reports Configure Tools Admin Enterprise

Core Config Manager

Service Management

Common Settings Check Settings Alert Settings Misc Settings

Initial state
Warning Critical OK Unknown

Obsess over service
On Off Skip Null

Check interval
5 min

Event handler

Event handler enabled
On Off Skip Null

Retry interval
1 min

Low flap threshold

High flap threshold

Max check attempts *
3 attempts

Flap detection enabled
On Off Skip Null

Flap detection options
Critical Warning OK Unknown

Active checks enabled
On Off Skip Null

Passive checks enabled
On Off Skip Null

Check period *
24x7

Retain status information
On Off Skip Null

Retain non-status information
On Off Skip Null

Freshness threshold

Check freshness
On Off Skip Null

Process perf data
On Off Skip Null

Is Volatile
On Off Skip Null

Save Cancel

3.2 Hermes-AD — Contrôleur de domaine

Hermes-AD est le serveur le plus critique de StadiumCompany. Il héberge l'Active Directory et le DNS principal. 4 services ont été configurés pour surveiller ses fonctionnalités essentielles.

Host	Service	Status	Duration	Attempt	Last Check	Status Information
Hermes-AD (Contrôleur de domaine Active Directory)	LDAP-Active directory	Ok	0s	1/1	2023-01-01 00:28:56	TCP OK - 0.001 second response time on 172.20.1.2 port 389
	PING-DISPONIBILITE	Ok	-9s	1/3	2023-01-01 00:29:38	PING OK - Paquets perdus = 0%, RTA = 0.38 ms
	SMB -Partage de fichiers	Ok	-48s	1/3	2023-01-01 00:30:23	TCP OK - 0.001 second response time on 172.20.1.2 port 445
	TCP -Vérification des port	Ok	-31s	1/3	2026-05-02 22:46:17	TCP OK - 0.001 second response time on 172.20.1.2 port 139
localhost	Current Load	Ok	43260 12h 55m 4s	1/4	2026-05-02 22:47:06	OK - Charge moyenne: 0.93, 0.39, 0.22
	Current Users	Ok	43374 4h 57m 22s	1/4	2026-05-02 22:47:31	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
	HTTP	Ok	43366 15h 5m 49s	1/4	2026-05-02 22:43:21	HTTP OK: HTTP/1.1 302 Found - 466 bytes in 0.000 second response time
	Memory Usage	Ok	43296 11h 23m 29s	1/4	2023-01-01 00:29:10	OK - 1516 / 1935 MB (78%) Free Memory, Used: 419 MB, Shared: 324 MB, Cached: 841 MB
	PING	Ok	43365 15h 5m 49s	1/4	2023-01-01 00:29:49	PING OK - Paquets perdus = 0%, RTA = 0.04 ms
	Root Partition	Ok	43378 4h 55m 43s	1/4	2023-01-01 00:30:34	DISK OK - free space / 2088 MB (28.63% inode=61%)
	SSH	Ok	43370 4h 55m 17s	1/4	2026-05-02 22:46:23	SSH OK - OpenSSH_8.4p1 Debian-5-deb1ubuntu (protocol 2.0)
	Service Status - cronpd	Ok	43368 15h 4m 51s	1/4	2026-05-02 22:47:16	• cron service - Regular background program processing daemon
	Service Status - httpd	Ok	43376 4h 54m 27s	1/4	2026-05-02 22:42:54	• apache2.service - The Apache HTTP Server
	Service Status - mysqld	Ok	43366 15h 4m 44s	1/4	2026-05-02 22:46:30	• mariadb.service - MariaDB 10.5.21 database server
Swap Usage	Ok	43372 4h 53m 31s	1/4	2023-01-01 00:29:24	SWAP OK - 100% libre (1905 MB sur un total de 1905 MB)	

3.3 GLPI — Serveur Helpdesk

GLPI est le serveur de gestion de parc et helpdesk de StadiumCompany. 2 services ont été configurés : la vérification de l'interface web (HTTP port 80) et de la base de données MariaDB (port 3306).

Host	Service	Status	Duration	Attempt	Last Check	Status Information
GLPI (Serveur GLPI - Helpdesk)	HTTP - interface Web GLPI	Ok	23m 8s	1/3	2023-01-01 00:32:46	TCP OK - 0.001 second response time on 172.20.1.8 port 80
	MariaDB-Base de donnees	Ok	21m 50s	1/3	2023-01-01 00:33:59	TCP OK - 0.004 second response time on 172.20.1.8 port 3306
Hermes-AD (Contrôleur de domaine Active Directory)	LDAP-Active directory	Ok	3d 19h 34m 22s	1/1	2023-01-01 00:33:07	TCP OK - 0.001 second response time on 172.20.1.2 port 389
	PING-DISPONIBILITE	Ok	3d 19h 33m 13s	1/3	2023-01-01 00:34:40	PING OK - Paquets perdus = 0%, RTA = 0.41 ms
	SMB -Partage de fichiers	Ok	3d 19h 32m 34s	1/3	2023-01-01 00:33:52	TCP OK - 0.001 second response time on 172.20.1.2 port 445
	TCP -Vérification des port	Ok	3d 19h 31m 51s	1/3	2023-01-01 00:34:47	TCP OK - 0.001 second response time on 172.20.1.2 port 139

3.4 HAProxy — Load Balancer (LAN_DMZ)

HAProxy est le répartiteur de charge de StadiumCompany, situé dans le VLAN DMZ (172.20.4.5). Une tentative d'ajout à la supervision Nagios a été effectuée, mais la machine apparaît en statut DOWN dans Nagios.

Limitation réseau : HAProxy est dans le LAN_DMZ (172.20.4.x) alors que Nagios est dans le LAN_SERVER (172.20.1.x). Les règles de filtrage du pare-feu pfSense Heimdall bloquent le trafic ICMP entre ces deux VLANs, ce qui empêche Nagios de joindre HAProxy. Pour résoudre ce problème, il faudrait créer une règle pfSense autorisant le trafic depuis 172.20.1.9 (Nagios) vers 172.20.4.5 (HAProxy). Cela n'a pas été réalisé dans le cadre de ce projet afin de ne pas modifier les règles de sécurité de l'infrastructure.

Host	Status	Duration	Attempt	Last Check	Status Information
GLPI (Serveur GLPI - Helpdesk)	Up	33m 8s	1/3	2023-01-01 00:47:39	PING OK - Paquets perdus = 0%, RTA = 0.38 ms
HAProxy (Serveur HAProxy - Load Balancer)	Down	2m 49s	3/3	2023-01-01 00:47:58	CRITICAL - Host Unreachable (172.20.4.5)
Hermes-AD (Contrôleur de domaine Active Directory)	Up	3d 19h 48m 7s	1/5	2023-01-01 00:47:27	OK - 172.20.1.2 rta 0.275ms lost 0%
localhost	Up	5558d 21h 55m 26s	1/10	2023-01-01 00:48:37	OK - 127.0.0.1 rta 0.011ms lost 0%
nagiosxi	Up	1219d 22h 52m 48s	1/5	2023-01-01 00:50:00	OK - 172.20.1.9 rta 0.012ms lost 0%

4. Problèmes rencontrés et résolutions

La configuration de Nagios XI a nécessité plusieurs diagnostics et corrections. Ces problèmes, bien que bloquants, ont été l'occasion d'approfondir la compréhension du fonctionnement interne de Nagios.

4.1 Problème 1 — Le symbole ! dans Manage Hosts

Lors de la configuration des services sur Hermes-AD, les services n'apparaissaient pas dans le Service Status malgré un Apply Configuration réussi.

En lisant directement le fichier de configuration en ligne de commande, le problème a été identifié : le champ `host_name` contenait `!Hermes-AD` au lieu de `Hermes-AD`. Dans Nagios, le `!` signifie EXCLUDE cet hôte — les services étaient donc appliqués à tout le monde sauf Hermes-AD.

```
register 1
}

define service {
    host_name          !Hermes-AD
    service_description PING-DISPONIBILITE
    display_name       Hermes-AD (Controleur de domaine Active Directory)
    check_command      check_ping!!!!!!!
    register           1
}

define service {
    host_name          !Hermes-AD
    service_description RDP - Bureau à distance
    display_name       Hermes-AD (Controleur de domaine Active Directory)
    check_command      check_tcp!!!!!!!
    register           1
}

define service {
    host_name          !Hermes-AD
    service_description TCP -Vérification des port
    display_name       Hermes-AD (Controleur de domaine Active Directory)
    check_command      check_tcp!!!!!!!
    register           1
}

#####
#
# Services configuration file
#
# END OF FILE
#
#####

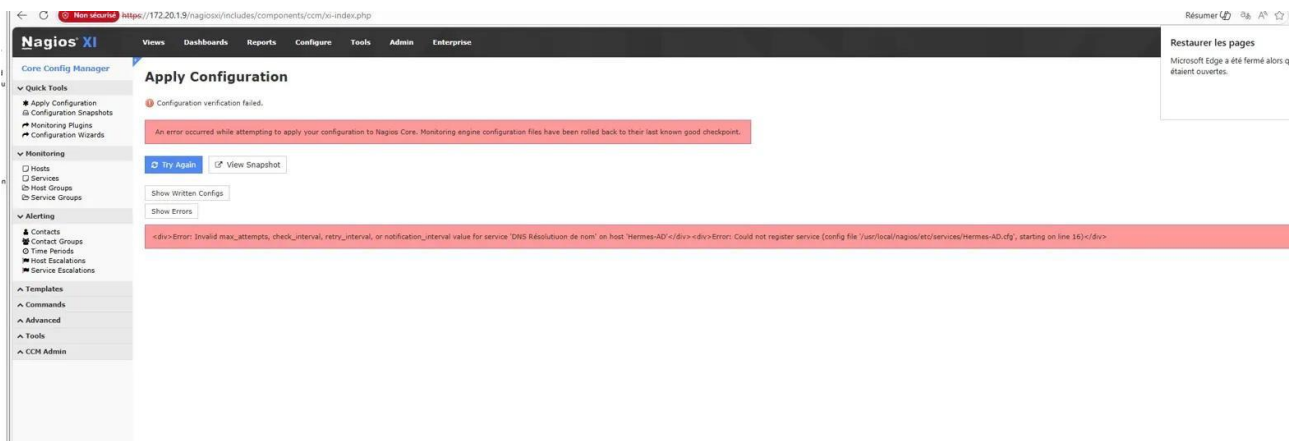
(root@nagiosxi)~[~]
#
```

Solution : suppression et recréation des services en désactivant le bouton ! dans la fenêtre Manage Hosts.

4.2 Problème 2 — Arguments invalides (!!!!!!!)

Après correction du problème précédent, de nouvelles erreurs sont apparues : les commandes `check_tcp` et `check_ping` contenaient de nombreux points d'exclamation superflus (`check_tcp!445!!!!!!!`) dans les fichiers de configuration.

Ces ! supplémentaires représentaient des arguments vides, ce qui rendait les commandes invalides pour Nagios Core.



Solution : correction directe dans les fichiers .cfg via la commande sed et l'éditeur nano depuis le terminal du serveur Nagios.

4.3 Problème 3 — Check_period manquant

Lors de la création de certains services, le champ Check period n'avait pas été renseigné dans l'onglet Check Settings. Ce champ obligatoire définit les plages horaires de surveillance.

Solution : ajout du paramètre 24x7 dans le Check Settings de chaque service concerné.

4.4 Ce que ces problèmes apportent

Ces incidents ont permis de comprendre en profondeur le fonctionnement interne de Nagios : la lecture directe des fichiers .cfg en ligne de commande est une compétence essentielle pour tout administrateur système. L'interface graphique de Nagios XI masque parfois des détails de configuration qui ne sont visibles qu'en lisant les fichiers XML générés par le Core Config Manager.

5. Résultats de la supervision

5.1 Dashboard final — Vue globale

Le dashboard final de Nagios XI présente l'état de l'ensemble de l'infrastructure supervisée. 4 hôtes sont UP (Hermes-AD, GLPI, localhost, nagiosxi) et 1 hôte est DOWN (HAProxy — bloqué par pfSense).

Showing 1-5 of 5 total records

Host	Status	Duration	Attempt	Last Check	Status Information
GLPI (Serveur GLPI - Helpdesk)	Up	33m 8s	1/3	2023-01-01 00:47:39	PING OK - Paquets perdus = 0%, RTA = 0.38 ms
HAProxy (Serveur HAProxy - Load Balancer)	Down	2m 49s	3/3	2023-01-01 00:47:58	CRITICAL - Host Unreachable (172.20.4.5)
Hermes-AD (Controlleur de domaine Active Directory)	Up	3d 19h 49m 7s	1/5	2023-01-01 00:47:27	OK - 172.20.1.2 rta 0.275ms lost 0%
localhost	Up	5558d 21h 55m 26s	1/10	2023-01-01 00:48:37	OK - 127.0.0.1 rta 0.011ms lost 0%
nagiosxi	Up	1219d 22h 52m 48s	1/5	2023-01-01 00:50:00	OK - 172.20.1.9 rta 0.012ms lost 0%

5.2 Services opérationnels

L'ensemble des services configurés sur Hermes-AD et GLPI sont en statut OK. Nagios surveille en temps réel 6 services critiques de l'infrastructure.

Showing 1-15 of 23 total records

Host	Service	Status	Duration	Attempt	Last Check	Status Information
GLPI (Serveur GLPI - Helpdesk)	HTTP - Interface Web GLPI	Ok	23m 8s	1/3	2023-01-01 00:32:46	TCP OK - 0.001 second response time on 172.20.1.8 port 80
	MariaDB-Base de donnees	Ok	21m 50s	1/3	2023-01-01 00:33:59	TCP OK - 0.004 second response time on 172.20.1.8 port 3306
Hermes-AD (Controlleur de domaine Active Directory)	LDAP- Active directory	Ok	3d 19h 34m 22s	1/1	2023-01-01 00:33:07	TCP OK - 0.001 second response time on 172.20.1.2 port 389
	PING-DISPONIBILITE	Ok	3d 19h 33m 13s	1/3	2023-01-01 00:34:40	PING OK - Paquets perdus = 0%, RTA = 0.41 ms
	SMB -Partage de fichiers	Ok	3d 19h 32m 34s	1/3	2023-01-01 00:33:52	TCP OK - 0.001 second response time on 172.20.1.2 port 445
	TCP -Vérification des port	Ok	3d 19h 31m 51s	1/3	2023-01-01 00:34:47	TCP OK - 0.001 second response time on 172.20.1.2 port 139

5.3 Simulation d'une panne

Pour valider le bon fonctionnement de la supervision, le serveur Hermes-AD a été éteint volontairement depuis la console VMware. Nagios a détecté la panne après 3 tentatives échouées (conformément au paramètre max_check_attempts) et a changé le statut en DOWN.

The screenshot shows the Nagios XI interface with a sidebar on the left containing navigation options like 'Home Dashboard', 'Host Status', and 'Service Status'. The main content area is titled 'Host Status' and shows a table with 3 records. The first record, 'Hermes-AD (Controlleur de domaine Active Directory)', is highlighted in red and has a status of 'Down'. The table also shows 'localhost' as 'Up' and 'nagiosxi' as 'Up'. Above the table, there are summary statistics for 'Host Status Summary' and 'Service Status Summary'. The 'Host Status Summary' shows 1 Down, 0 Unreachable, and 0 Pending. The 'Service Status Summary' shows 0 OK, 0 Warning, 0 Unknown, and 0 Critical. The interface also includes a search bar and pagination controls.

Ce test confirme que Nagios détecte correctement les pannes et qu'une alerte aurait été envoyée à l'administrateur en environnement de production.

6. Bilan du projet

6.1 Apports pour StadiumCompany

- Surveillance automatique 24h/24 des serveurs critiques sans intervention humaine
- Détection immédiate des pannes sur Hermes-AD (AD/DNS) et GLPI (Helpdesk)
- Visibilité centralisée sur l'état de l'infrastructure via un seul dashboard
- Base extensible — HAProxy pourrait être ajouté avec une règle pfSense supplémentaire

6.2 Difficultés rencontrées

Difficulté	Solution apportée
Services non visibles (! dans Manage Hosts)	Lecture du fichier .cfg en terminal — identification et correction du symbole !
Arguments invalides (!!!!!!!)	Correction via commande sed et éditeur nano directement dans les fichiers cfg
Check period manquant	Ajout du paramètre 24x7 dans Check Settings de chaque service
HAProxy inaccessible (pfSense)	Limitation documentée — nécessiterait une règle pfSense supplémentaire

6.2 Conclusion

Ce projet m'a permis de mettre en place une supervision réseau complète sur l'infrastructure StadiumCompany. La configuration de Nagios XI, bien que complexe, m'a appris à diagnostiquer des problèmes en lisant directement les fichiers de configuration en ligne de commande — une compétence fondamentale pour tout administrateur système et réseau.

La limitation rencontrée avec HAProxy illustre également un concept important en administration réseau : la segmentation par VLAN et les règles de filtrage pfSense protègent l'infrastructure mais peuvent nécessiter des ajustements pour permettre à des outils de supervision de fonctionner correctement.