WAZUH

Mise en œuvre de l'inventaire système

Configuration centralisée Syscollector et exploitation de la rubrique IT Hygiene

Auteur	Adel Sadek
Date	30 juin 2026
Périmètre	Serveurs Linux supervisés par SRV-LOG-01
Version	1.0

Objet du document. Cette documentation ne reprend pas l'installation de Wazuh. Elle décrit uniquement la configuration centralisée réalisée le 30 juin 2026 afin de constituer un inventaire de sécurité exploitable depuis IT Hygiene.

Infrastructure supervisée : SRV-LOG-01, www-kasavanille et srv-catelsys

1. Contexte, objectif et périmètre

La session du 30 juin 2026 a consisté à enrichir une installation Wazuh déjà opérationnelle avec le module Syscollector. L'objectif est de disposer, depuis le dashboard, d'une vision centralisée, actualisée et vérifiable de l'état des serveurs Linux : système d'exploitation, logiciels, processus, réseau, comptes et services.

Wazuh utilise Syscollector pour effectuer des scans périodiques sur les endpoints supervisés. Les informations remontées sont ensuite consolidées dans le dashboard, notamment dans la rubrique IT Hygiene. Cette visibilité est utile pour l'inventaire des actifs, l'analyse de l'exposition et les opérations de sécurité.

Résultat obtenu. Deux endpoints Linux Debian remontent correctement leur inventaire dans IT Hygiene : www-kasavanille et srv-catelsys. Les vues System, Software, Processes, Network, Identity et Services sont accessibles et alimentées.

Contenu de cette documentation

Section	Sujet traité	Preuve intégrée
2	Organisation des groupes Wazuh	Configurations default et joomla-web
3	Configuration Syscollector	Bloc agent.conf avec scan périodique et services
4	Consultation IT Hygiene	Vue d'ensemble des endpoints
5	Inventaire collecté	Système, paquets, processus, réseau, identité, services
6	Apports sécurité et prochaines actions	Utilisation opérationnelle et suite du déploiement

Serveurs observés

Agent	Système relevé	Version / noyau observés	Usage principal dans le périmètre
www-kasavanille	Debian GNU/Linux	Debian 12 (bookworm) ; noyau 6.1.0-37-cloud-amd64	Serveur Linux supervisé
srv-catelsys	Debian GNU/Linux	Debian 11 (bullseye) ; noyau 5.10.0-32-amd64	Serveur web Joomla / Apache dans le périmètre

Les informations de version et de noyau ci-dessus proviennent de la vue System capturée pendant la session.

2. Configuration centralisée par groupes

La configuration est administrée depuis l'interface Wazuh, via les fichiers agent.conf associés aux groupes. Cette approche permet d'appliquer un socle commun aux serveurs tout en conservant des règles spécialisées pour les systèmes Joomla et Apache.

Le groupe default porte l'inventaire général. Le groupe joomla-web complète ce socle avec une surveillance spécifique du serveur web : intégrité de fichiers et collecte des journaux Apache.

2.1 Groupe default : socle d'inventaire commun

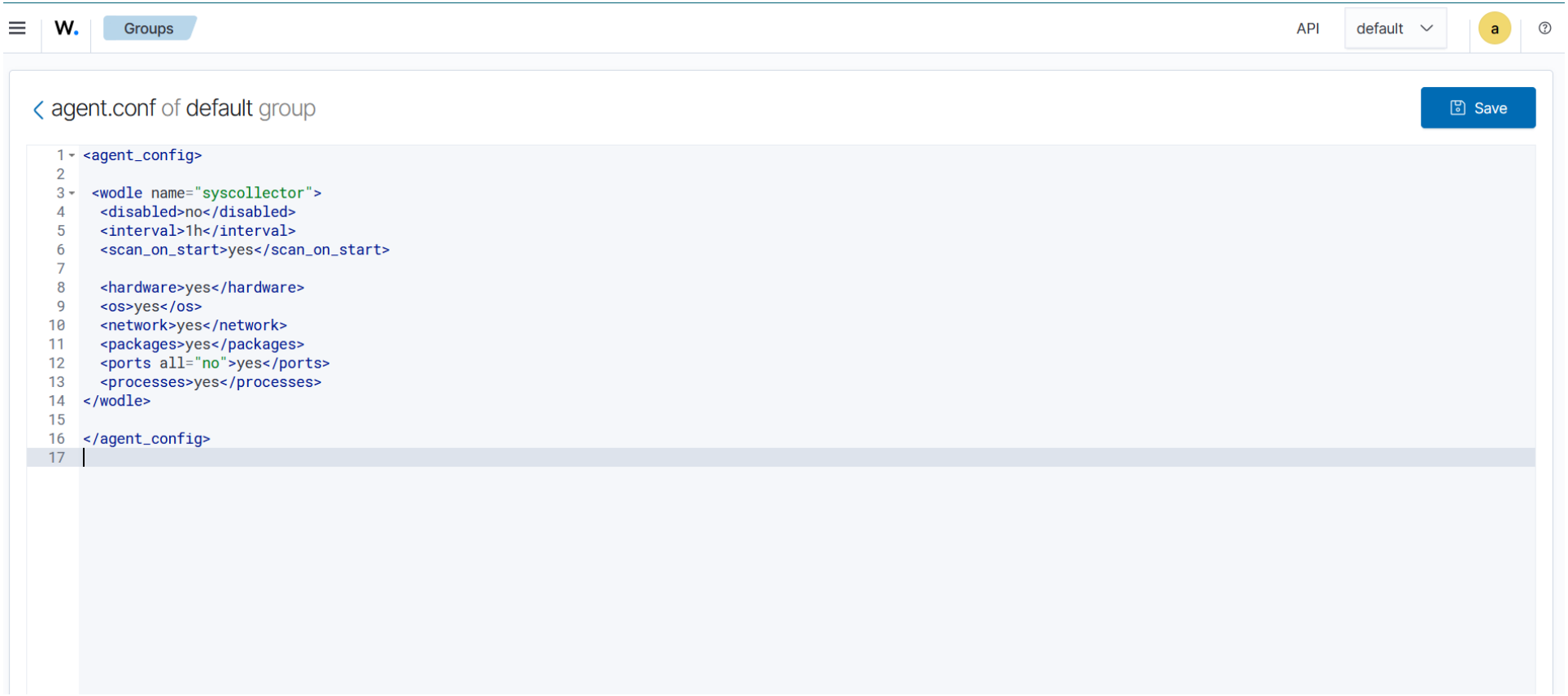


Figure 1 - *Configuration initiale du groupe default : activation du module Syscollector pour l'inventaire matériel, OS, réseau, paquets, ports et processus.*

Point de contrôle. Le paramètre <packages>yes</packages> permet de remonter le nom et la version des paquets. C'est la base nécessaire à une future comparaison avec les vulnérabilités et à la gestion de l'exposition logicielle.

2.2 Groupe joomla-web : surveillance applicative et intégrité

Le groupe joomla-web cible les serveurs hébergeant Joomla. Il ajoute une surveillance FIM (File Integrity Monitoring) en temps réel sur les répertoires les plus sensibles : le site web, la configuration Apache et les emplacements de tâches planifiées.

Figure 2 - *Configuration du groupe joomla-web : surveillance FIM de /var/www/html, /etc/apache2 et des répertoires cron ; collecte des logs Apache.*

Éléments configurés dans le groupe joomla-web

Élément surveillé	Finalité de sécurité	Mode
/var/www/html	Détecter les créations, suppressions ou modifications de fichiers Joomla et de contenus web	FIM temps réel
/etc/apache2	Détecter la modification de virtual hosts, modules et paramètres du serveur web	FIM temps réel
/etc/cron.d et /var/spool/cron	Détecter les mécanismes de persistance via tâches planifiées	FIM temps réel
/var/log/apache2/*.log	Centraliser et analyser les journaux d'accès et d'erreur Apache	Collecte de logs

3. Configuration Syscollector complétée par les services

Après validation des données système, le module Syscollector a été enrichi pour inventorier les services. L'ajout de <services>yes</services> permet de rendre visible la liste des unités et services découverts sur les endpoints dans l'onglet Services de IT Hygiene.

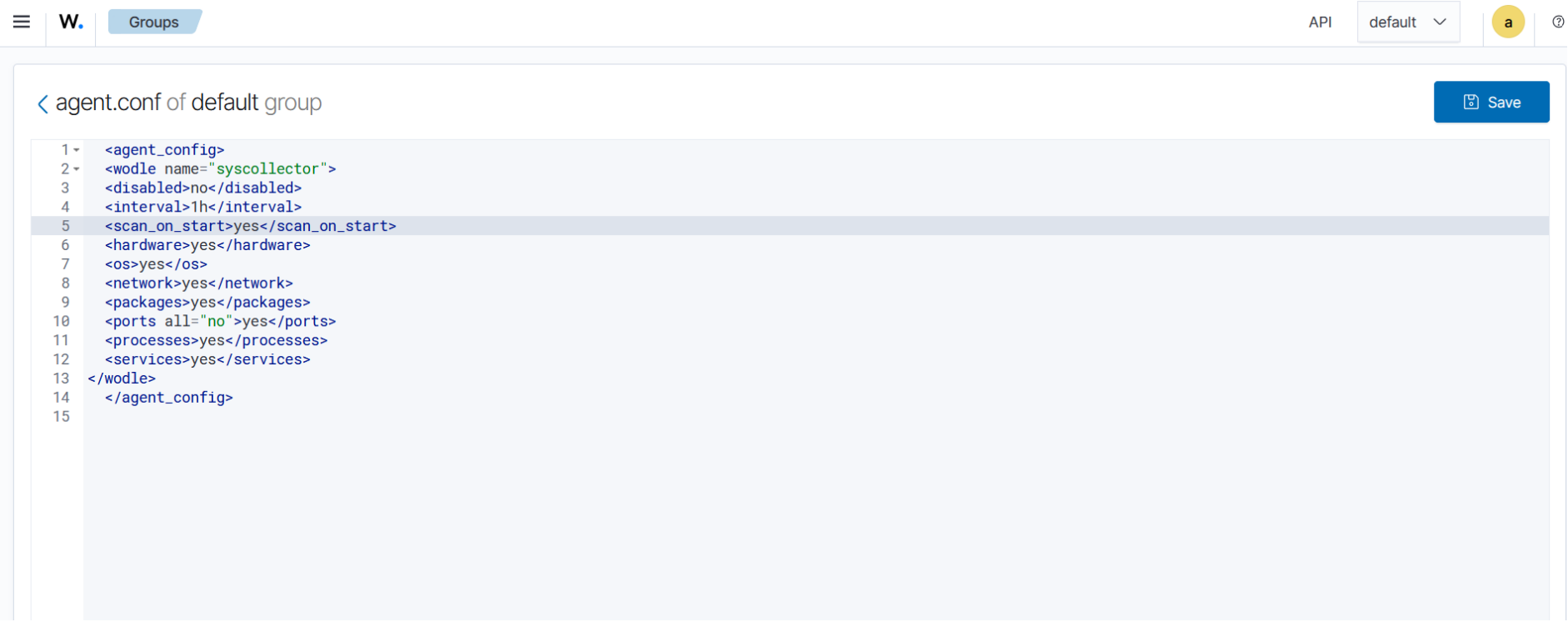


Figure 3 - *Configuration finale du groupe default : Syscollector exécute un scan toutes les heures et au démarrage, y compris pour les services.*

Paramètres actifs du module Syscollector

Paramètre	Valeur	Rôle
disabled	no	Module Syscollector activé
interval	1h	Rafraîchissement régulier de l'inventaire
scan_on_start	yes	Collecte immédiate au démarrage de l'agent
hardware / os / network	yes	Inventaire matériel, système et interfaces réseau
packages	yes	Inventaire des paquets et de leurs versions
ports all="no"	yes	Inventaire des ports d'écoute détectés
processes	yes	Inventaire des processus en cours
services	yes	Inventaire des services détectés

Pourquoi c'est important. L'inventaire doit être centralisé et actualisé pour être exploitable. Il permet de comprendre rapidement quel logiciel, quel processus,

quelle interface ou quel service est présent sur chaque endpoint, sans se connecter manuellement à chaque serveur.

4. Consultation centralisée dans IT Hygiene

Les données collectées par Syscollector sont consultées depuis la rubrique IT Hygiene du dashboard Wazuh. Cette page fournit une synthèse de l'environnement supervisé avant de permettre une analyse détaillée par catégorie.

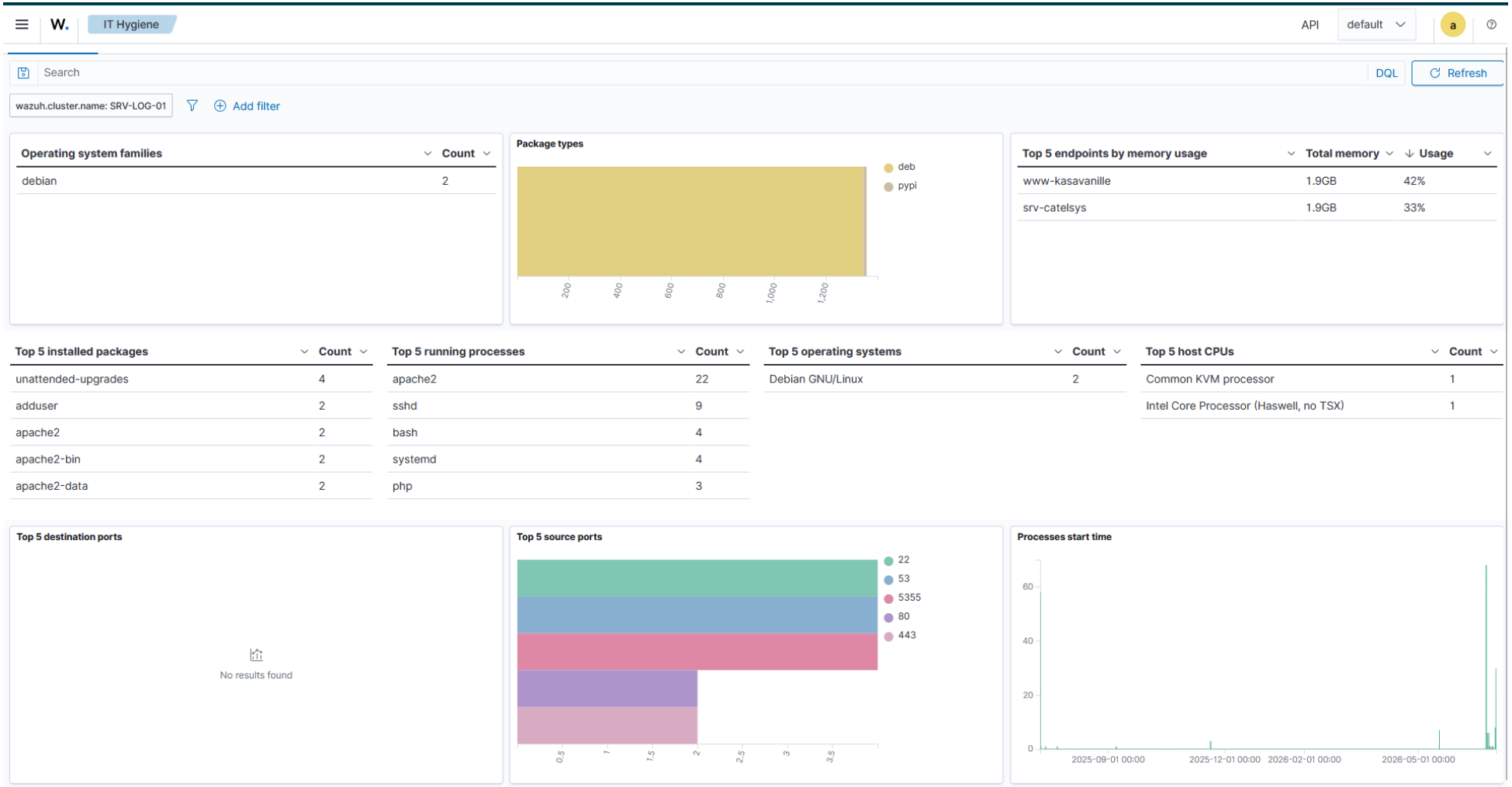


Figure 4 - *Dashboard IT Hygiene : aperçu des endpoints Debian, paquets, processus et données réseau disponibles.*

Constats visibles dans la synthèse

- Deux endpoints Debian sont présents dans la vue d'ensemble : www-kasavanille et srv-catelsys.
- Les paquets logiciels, processus, ports et ressources système sont déjà consolidés dans les widgets.
- Les éléments Apache, SSH, Bash, PHP et systemd apparaissent dans les processus les plus représentés.
- Le dashboard permet de basculer vers les vues détaillées sans connexion directe au serveur concerné.

5. Résultats de l'inventaire collecté

5.1 Systèmes d'exploitation et architecture

La vue System centralise les informations de base nécessaires à la gestion d'un parc : plateforme, nom du système, version, noyau et architecture. Ces données permettent notamment d'identifier les serveurs qui demandent une attention particulière lors d'un suivi de cycle de vie ou de vulnérabilités.

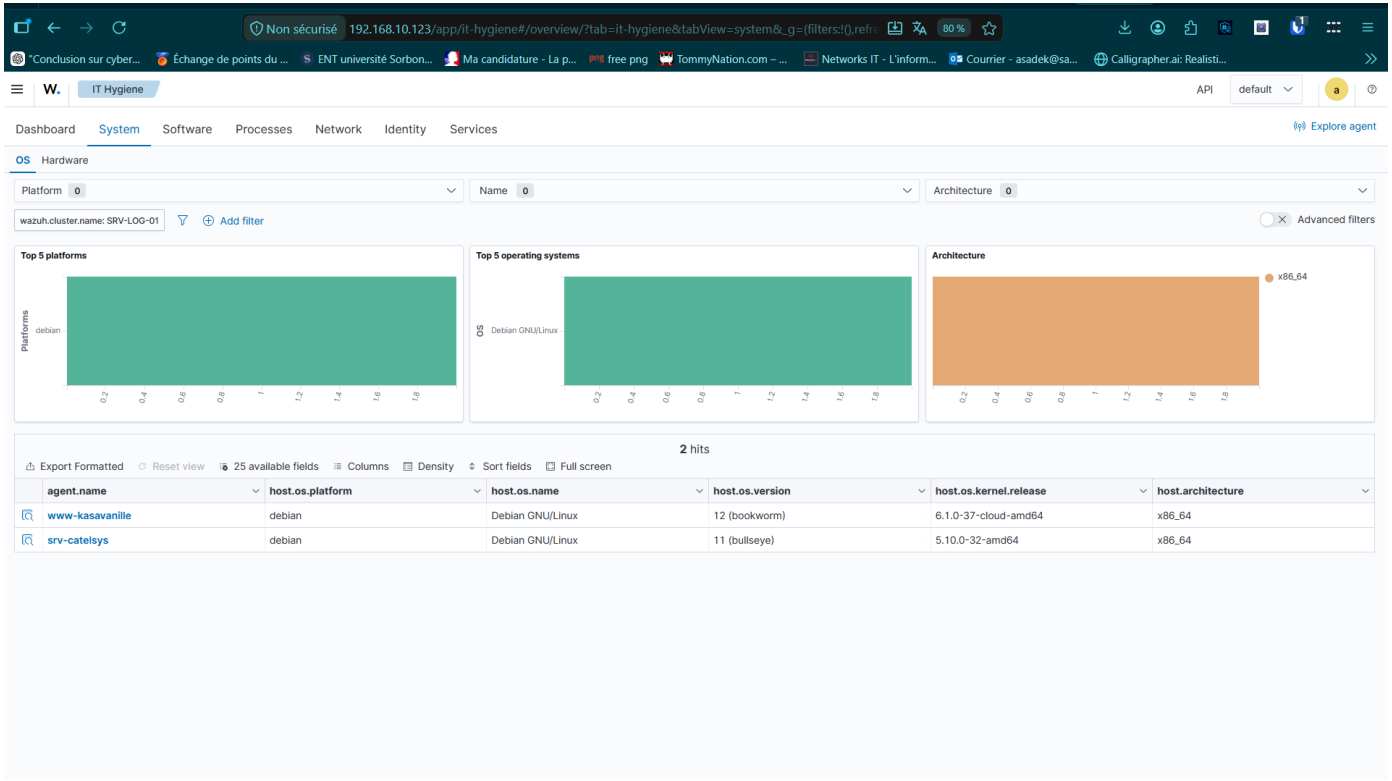


Figure 5 - *IT Hygiene > System : deux endpoints Debian x86_64 avec leurs versions et noyaux respectifs.*

Observation. srv-catelsys apparaît sous Debian 11 (bullseye) tandis que www-kasavanille apparaît sous Debian 12 (bookworm). Cette différence doit être prise en compte dans le suivi des correctifs et des versions de paquets disponibles.

5.2 Logiciels et versions de paquets

La vue Software > Packages permet de connaître les logiciels installés et leurs versions. C'est le point de départ pour identifier les composants utilisés, repérer un logiciel non attendu ou préparer un suivi des mises à jour et des CVE.

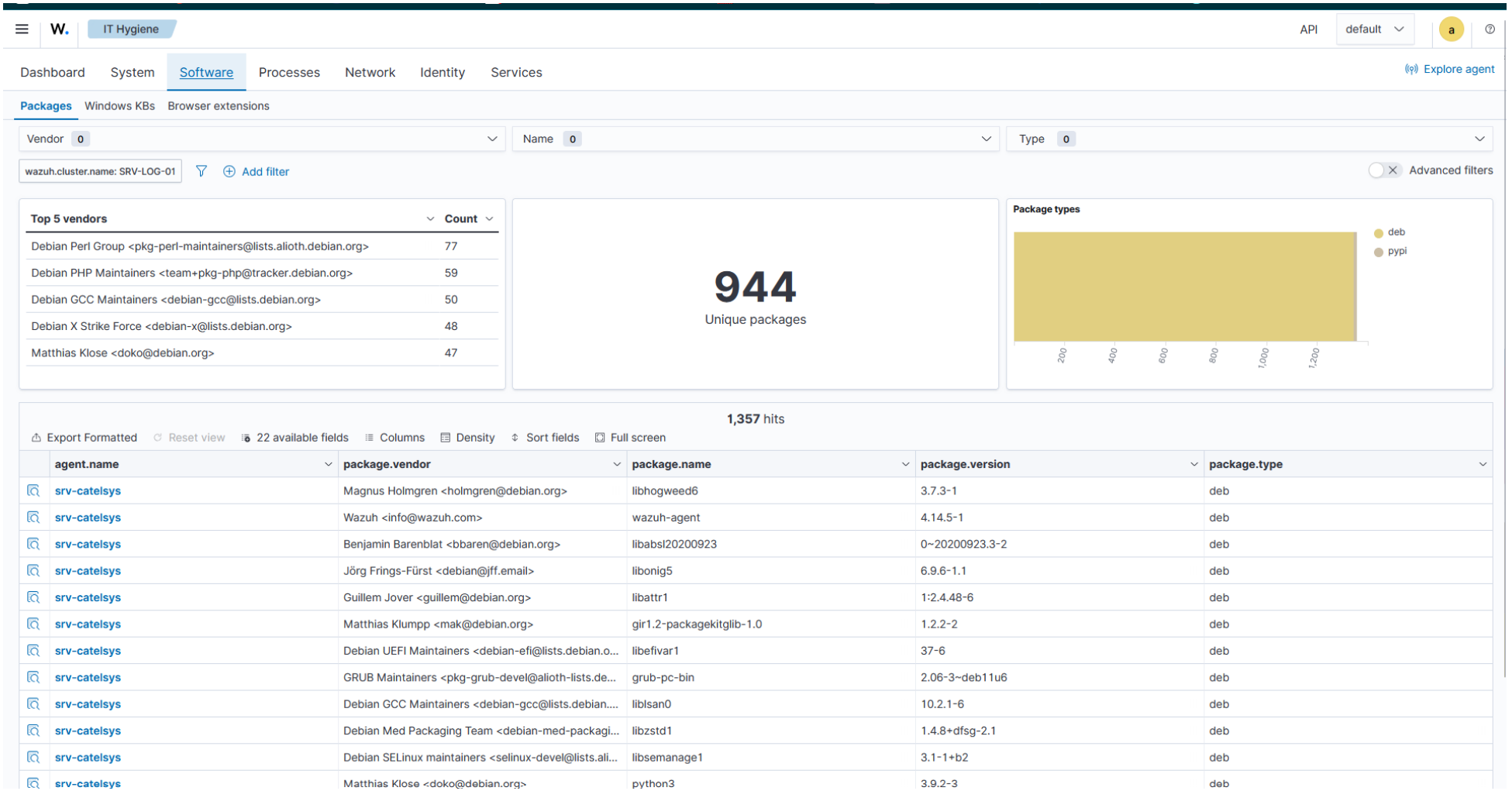


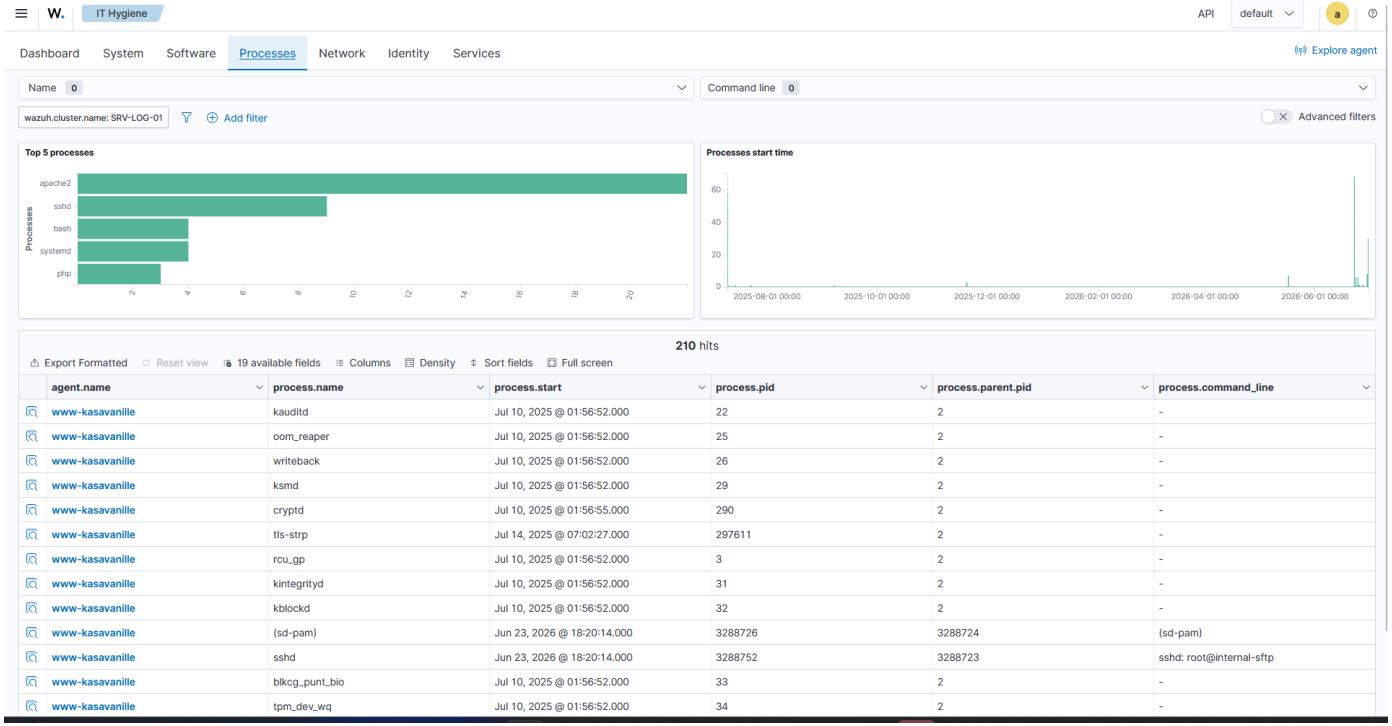
Figure 6 - *IT Hygiene > Software > Packages : packages Debian inventoriés, avec nom, fournisseur, version et type.*

La capture affiche 944 paquets uniques et 1 357 enregistrements dans la vue sélectionnée. Elle confirme notamment la remontée de la version de l'agent Wazuh et des bibliothèques système présentes sur srv-catelsys.

Usage opérationnel. La recherche par nom permet de vérifier rapidement les versions de composants critiques tels que apache2, php, openssl, openssh-server, mariadb, postfix ou wazuh-agent.

5.3 Processus et lignes de commande

La vue Processes expose les processus détectés, leur PID, leur processus parent et, lorsque disponible, leur ligne de commande. Cette information aide à qualifier l'activité d'un serveur et à investiguer les exécutions inhabituelles.



agent.name	process.name	process.start	process.pid	process.parent.pid	process.command_line
www-kasavanille	kauditd	Jul 10, 2025 @ 01:56:52.000	22	2	-
www-kasavanille	oom_reaper	Jul 10, 2025 @ 01:56:52.000	25	2	-
www-kasavanille	writeback	Jul 10, 2025 @ 01:56:52.000	26	2	-
www-kasavanille	ksmd	Jul 10, 2025 @ 01:56:52.000	29	2	-
www-kasavanille	cryptd	Jul 10, 2025 @ 01:56:55.000	290	2	-
www-kasavanille	tls-strp	Jul 14, 2025 @ 07:02:27.000	297611	2	-
www-kasavanille	rcu_gp	Jul 10, 2025 @ 01:56:52.000	3	2	-
www-kasavanille	kintegrityd	Jul 10, 2025 @ 01:56:52.000	31	2	-
www-kasavanille	kblockd	Jul 10, 2025 @ 01:56:52.000	32	2	-
www-kasavanille	(sd-pam)	Jun 23, 2026 @ 18:20:14.000	3288726	3288724	(sd-pam)
www-kasavanille	sshd	Jun 23, 2026 @ 18:20:14.000	3288752	3288723	sshd: root@internal-sftp
www-kasavanille	blkcg_punt_bio	Jul 10, 2025 @ 01:56:52.000	33	2	-
www-kasavanille	tpm_dev_wq	Jul 10, 2025 @ 01:56:52.000	34	2	-

Figure 7 - *IT Hygiene > Processes : exemples de processus et de lignes de commande collectés sur les endpoints supervisés.*

Exemples observables dans la capture

- apache2 et php : composants associés au service web.
- sshd : processus de service SSH ; une ligne de commande est visible pour une session root@internal-sftp.
- systemd, bash et processus noyau : éléments habituels du fonctionnement du système Linux.

Point de vigilance. L'inventaire de processus ne remplace pas une détection EDR complète, mais il donne un contexte précieux pour repérer un binaire inattendu, une commande inhabituelle ou une exécution anormale à investiguer.

5.4 Réseau : adresses et interfaces

La vue Network regroupe les interfaces réseau, adresses IP, masques et types de réseau remontés par les agents. Elle contribue à maintenir une cartographie technique à jour et facilite la vérification des interfaces réellement actives.

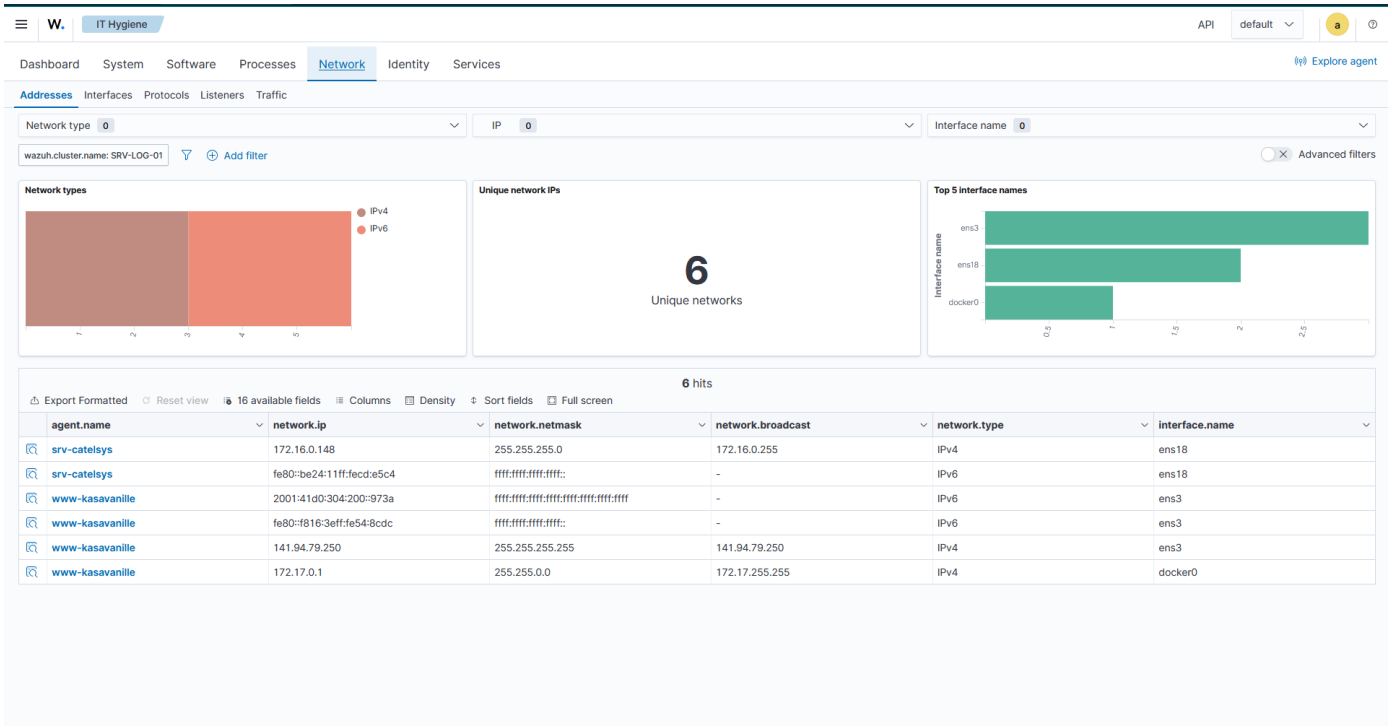


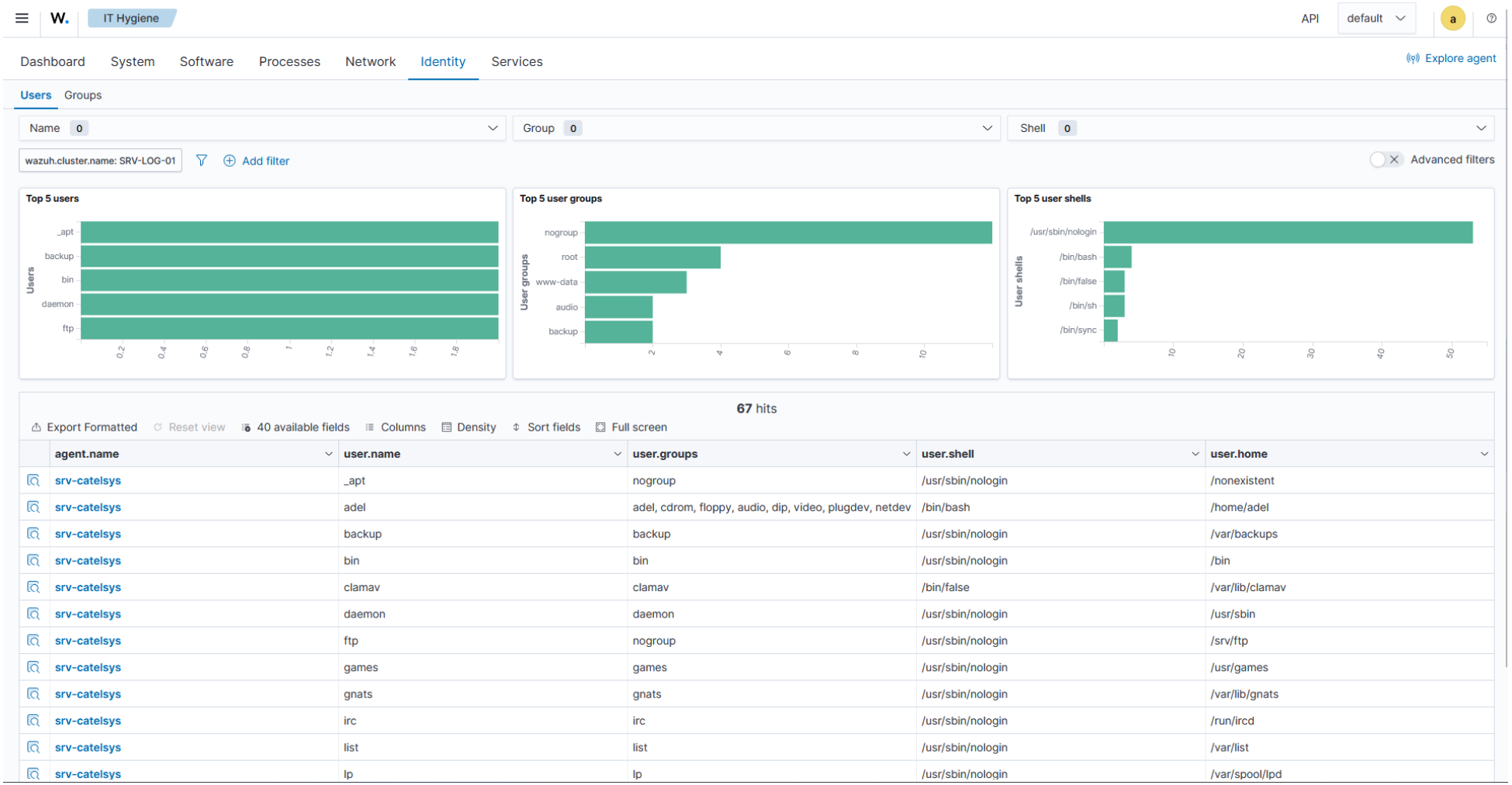
Figure 8 - *IT Hygiene > Network > Addresses : adresses IPv4/IPv6 et interfaces telles que ens18, ens3 et docker0.*

La capture montre notamment srv-catelsys avec l'adresse IPv4 172.16.0.148 sur ens18, ainsi que des interfaces appartenant à www-kasavanille, dont ens3 et docker0. Ces données peuvent être croisées avec les règles réseau, les VLAN et les services exposés.

Apport sécurité. La visibilité réseau aide à détecter l'apparition d'une interface inconnue, d'une adresse non attendue ou d'un service qui s'expose sur une interface qui ne devrait pas être utilisée.

5.5 Identité : comptes, groupes et shells

La vue Identity consolide les comptes locaux, leurs groupes, le shell associé et le répertoire personnel. Elle permet de vérifier les comptes techniques, les comptes administratifs et les comptes disposant d'un shell interactif.



agent.name	user.name	user.groups	user.shell	user.home
srv-catelsys	_apt	nogroup	/usr/sbin/nologin	/nonexistent
srv-catelsys	adel	adel, cdrom, floppy, audio, dip, video, plugdev, netdev	/bin/bash	/home/adel
srv-catelsys	backup	backup	/usr/sbin/nologin	/var/backups
srv-catelsys	bin	bin	/usr/sbin/nologin	/bin
srv-catelsys	clamav	clamav	/bin/false	/var/lib/clamav
srv-catelsys	daemon	daemon	/usr/sbin/nologin	/usr/sbin
srv-catelsys	ftp	nogroup	/usr/sbin/nologin	/srv/ftp
srv-catelsys	games	games	/usr/sbin/nologin	/usr/games
srv-catelsys	gnats	gnats	/usr/sbin/nologin	/var/lib/gnats
srv-catelsys	irc	irc	/usr/sbin/nologin	/run/ircd
srv-catelsys	list	list	/usr/sbin/nologin	/var/list
srv-catelsys	lp	lp	/usr/sbin/nologin	/var/spool/lpd

Figure 9 - *IT Hygiene > Identity > Users : comptes locaux, groupes, shells et répertoires personnels de srv-catelsys.*

La capture confirme la présence de comptes systèmes avec des shells non interactifs, ainsi que du compte adel avec le shell /bin/bash et le répertoire /home/adel. Cette distinction est utile pour identifier les comptes qui peuvent ouvrir une session interactive.

Bon réflexe. Un changement de compte, de groupe privilégié ou de shell peut être un indicateur de dérive de configuration ou de persistance. Les éléments inhabituels doivent être comparés à la configuration attendue du serveur.

5.6 Services détectés

Après ajout de <services>yes</services>, l'onglet Services de IT Hygiene permet de consulter les services détectés sur les endpoints. Cette vue donne un inventaire utile pour appliquer le principe du moindre service : seuls les services nécessaires à la mission du serveur devraient être activés et maintenus.

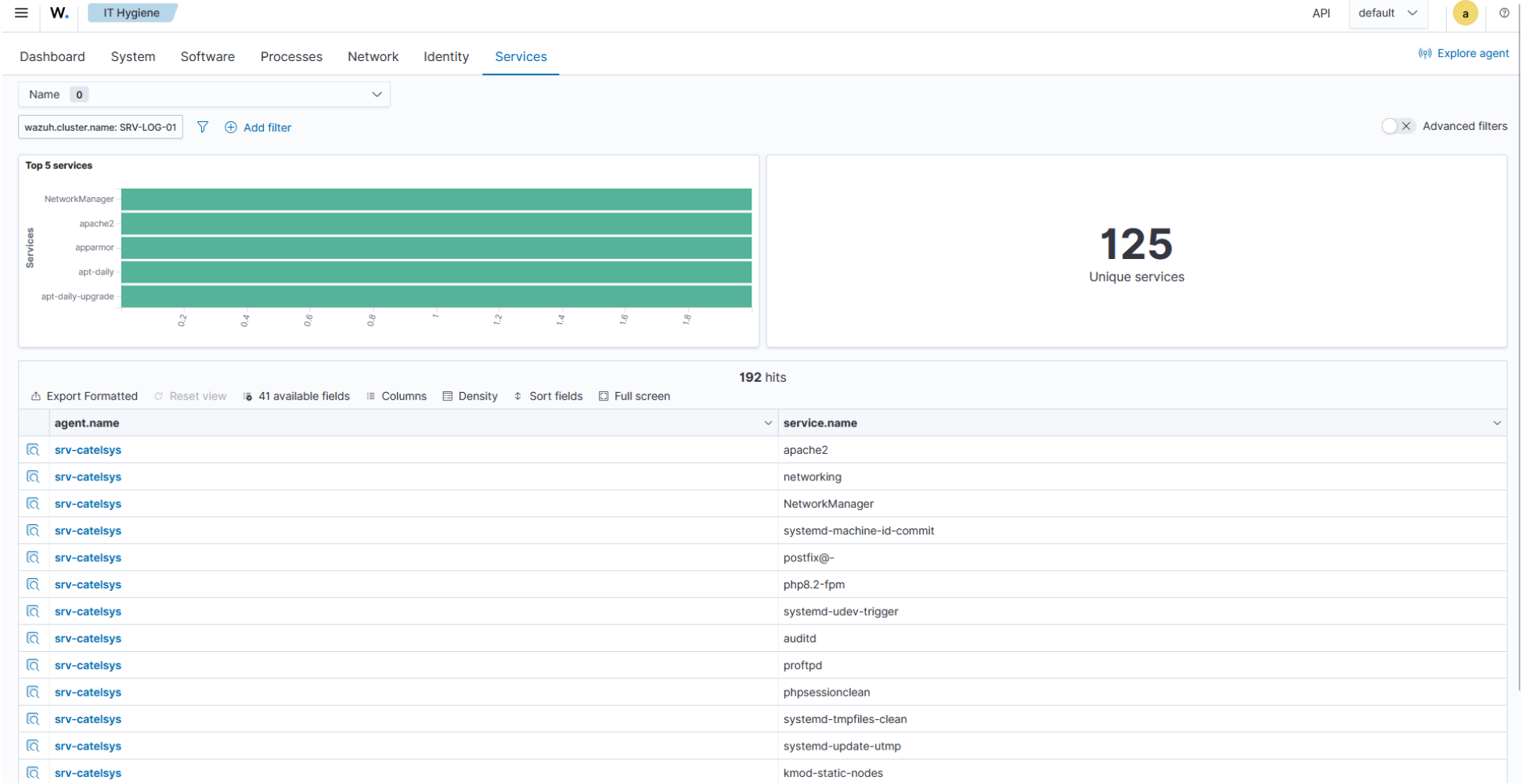


Figure 10 - *IT Hygiene > Services : 125 services uniques observés, dont apache2, php8.2-fpm, auditd, proftpd et NetworkManager.*

Lecture de la vue Services

- apache2 et php8.2-fpm confirment l'activité du service web sur srv-catelsys.
- auditd est présent, ce qui est pertinent pour compléter la journalisation système.
- proftpd et postfix@- apparaissent dans la liste : ces services doivent être validés selon le rôle attendu du serveur.

- Le nombre de services visibles donne une base de travail pour identifier ceux qui sont inutiles ou à durcir.

Résultat clé. L'objectif initial de visualiser les services dans Wazuh est atteint : 125 services uniques sont affichés dans IT Hygiene après l'activation du scan des services.

6. Apports sécurité et exploitation opérationnelle

L'inventaire obtenu ne constitue pas une simple liste technique. Il transforme les agents Wazuh en points de collecte capables d'alimenter une vision centralisée de l'environnement. Cette base facilite les contrôles réguliers et réduit le temps de diagnostic lors d'un incident.

Besoin opérationnel	Information déjà disponible	Utilisation possible
Connaître les versions installées	Paquets et versions dans Software	Préparer les mises à jour et le suivi des composants critiques
Identifier une exposition réseau	Interfaces, adresses et ports	Vérifier les interfaces attendues et les services exposés
Contrôler les comptes locaux	Utilisateurs, groupes, shells et homes	Repérer un compte inattendu ou un shell interactif non justifié
Réduire la surface d'attaque	Inventaire des services	Valider les services nécessaires et désactiver les services inutiles
Investiguer une activité	Processus et lignes de commande	Qualifier une exécution inconnue ou rapprocher un événement de sécurité d'un processus
Surveiller une application web	FIM et logs Apache du groupe joomla-web	Détecter des modifications sensibles et analyser les journaux web

Prochaines actions recommandées

- Vérifier la liste des services de chaque serveur et désactiver ceux qui ne sont pas justifiés par le rôle métier.
- Utiliser la recherche Software pour suivre les versions de apache2, PHP, OpenSSL, OpenSSH, MariaDB et Postfix.
- Activer et vérifier la détection de vulnérabilités à partir des paquets remontés par Syscollector.
- Produire des alertes FIM de test sur /var/www/html afin de valider la détection de modification de fichiers web.
- Définir les alertes critiques à transmettre ultérieurement sur Telegram, après filtrage et prévention des doublons.

7. Conclusion

La configuration réalisée aujourd'hui confirme le bon fonctionnement de l'inventaire centralisé Wazuh sur les endpoints Linux du périmètre. Le groupe default collecte désormais le matériel, le système, le réseau, les paquets, les ports, les processus et les services. Le groupe joomla-web complète cette base avec une surveillance de l'intégrité du serveur web et la collecte des logs Apache.

Les captures IT Hygiene démontrent que les données sont exploitables depuis le dashboard : informations système, versions de paquets, processus, interfaces, comptes et services. L'inventaire constitue une base solide avant la mise en place du suivi de vulnérabilités, de règles de détection plus spécifiques et de mécanismes de réponse automatisée.

Statut final. Configuration Syscollector opérationnelle ; inventaire visible dans IT Hygiene ; inventaire des services validé après ajout de <services>yes</services>.

Références techniques

- Wazuh Documentation - System inventory : https://documentation.wazuh.com/current/user-manual/capabilities/system-inventory/index.html
- Wazuh Documentation - How system inventory works : https://documentation.wazuh.com/current/user-manual/capabilities/system-inventory/how-it-works.html
- Wazuh Documentation - System inventory configuration : https://documentation.wazuh.com/current/user-manual/capabilities/system-inventory/configuration.html
- Wazuh Documentation - Viewing system inventory data in IT Hygiene : https://documentation.wazuh.com/current/user-manual/capabilities/system-inventory/viewing-system-inventory-data.html
- Wazuh Documentation - Centralized configuration (agent.conf) : https://documentation.wazuh.com/current/user-manual/reference/centralized-configuration.html
- Wazuh Documentation - Agent grouping : https://documentation.wazuh.com/current/user-manual/agent/agent-management/grouping-agents.html

Captures d'écran : interface Wazuh Dashboard fournie pendant la session du 30 juin 2026. Les captures constituent les preuves de configuration et de résultats documentées dans ce rapport.