AUDIT DE SÉCURITÉ LYNIS

Rapport de durcissement du système

Audit de sécurité automatisé de l'image, exécuté avec Lynis sur une instance fraîchement provisionnée avant publication.

HÔTE **ip-172-31-84-101**	SYSTÈME D'EXPLOITATION **Ubuntu 26.04 LTS**
NOYAU **7.0.0-1010-aws**	ARCHITECTURE **arm64**
VERSION DE LYNIS **3.1.7**	PROFIL **custom.prf**
DURÉE **56s**	EXÉCUTÉ PAR **root**

Notre engagement de durcissement

Toutes les images publiées par imaxe.cloud sont durcies par défaut, pour la sécurité de celui qui les met en production. Nous ne livrons pas une distribution nue : le système arrive avec un pare-feu qui refuse par défaut, un SSH restreint, un noyau et des options de montage renforcés, des mises à jour de sécurité automatiques, ainsi que les outils d'intégrité des fichiers, de rootkits, de malwares et d'audit installés et en marche.

Ce rapport en est la preuve. Il est généré automatiquement sur une instance fraîchement construite, avant la publication de l'image, il n'est jamais retouché à la main et il est publié en entier — y compris tout ce que l'audit n'a pas noté. Le durcissement fait partie du produit, donc l'audit qui le mesure voyage avec lui.

INDICE DE DURCISSEMENT

0
Avertissements
Problèmes à corriger

0
Suggestions
Améliorations à envisager

241
Tests effectués
Contrôles de sécurité Lynis exécutés

0
Plugins actifs
Plugins d'audit supplémentaires

Verdict
Le système atteint un indice de durcissement de 100/100 : une configuration fortement durcie, prête pour la production.

1 Score par catégorie

Répartition du résultat de l'audit par domaine de sécurité, dérivée des avertissements et suggestions de chacun.

Noyau et démarrage	100
Authentification	100
Système de fichiers et intégrité	100
Réseau et pare-feu	100
SSH	100
Paquets et outils	100

2 Avertissements

Constats que Lynis signale comme avertissements. Ils sont examinés et corrigés avant chaque publication.

ID DU TEST	DESCRIPTION	SÉVÉRITÉ
Aucun avertissement — l'audit n'a trouvé aucun problème de ce niveau.		

3 Suggestions

Recommandations de Lynis. Certaines ne s'appliquent pas aux images cloud ou relèvent de choix de conception délibérés.

ID DU TEST	RECOMMANDATION	CATÉGORIE
Aucune suggestion.		

4 Contrôles volontairement ignorés

L'image exécute Lynis avec un profil qui ignore 23 contrôles. Aucun n'est une faille de durcissement : ce sont des contrôles impossibles à évaluer sur une image cloud, déjà couverts par une autre mesure, ou qui dépendent de données n'existant qu'une fois l'instance démarrée. Chacun est listé avec son motif pour que l'omission soit auditable.

ID DU TEST	MOTIF DE NON-APPLICABILITÉ
AUTH-9284	Les comptes signalés sont les comptes de service de la base Ubuntu (daemon, bin, sys…). Ils arrivent sans mot de passe valide et sans shell interactif, ce qui est précisément voulu ; le test lit cet état normal comme un constat.
BOOT-5122	Il n'y a pas de mot de passe GRUB parce qu'il n'y a pas de console physique pour le saisir : une instance EC2 démarre seule et sa console est un appel d'API protégé par IAM. Le mot de passe ne serait qu'une gêne lors d'un sauvetage.
BOOT-5180	Faux positif sur cette image : le contrôle ne peut pas être évalué ici et son résultat ne refléterait pas l'état réel du système.

ID DU TEST	MOTIF DE NON-APPLICABILITÉ
BOOT-5264	Faux positif sur cette image : le contrôle ne peut pas être évalué ici et son résultat ne refléterait pas l'état réel du système.
CRYP-7902	Dépend de données qui n'existent pas pendant la construction de l'image ; résolu au premier démarrage.
DEB-0810	apt-listbugs est interactif : il interrompt une mise à jour pour interroger un humain. Sur une image sans surveillance, il bloquerait les mises à jour de sécurité automatiques, bien plus importantes.
FILE-6310	L'image utilise un unique volume racine, la forme sous laquelle une instance cloud se redimensionne et se sauvegarde. Ce que ce contrôle veut vraiment — que /tmp, /dev/shm et /run ne puissent ni exécuter de binaires ni contenir de périphériques — est obtenu ici par des options de montage durcies.
FILE-7524	Les permissions sont celles dont ce produit a besoin et sont vérifiées à chaque build par notre propre suite de tests ; le contrôle générique signale comme erreurs des fichiers applicatifs légitimes.
FIRE-4512	Le contrôle compte les règles iptables et qualifie une liste courte de « vide ». Ici la première couche de filtrage est le Security Group AWS, à l'extérieur de l'instance, et ufw ferme tout le reste par défaut : la protection existe, elle n'est simplement pas écrite là où ce test regarde.
FIRE-4513	Le contrôle marque comme inutilisée toute règle dont le compteur de paquets est à zéro. Sur une instance fraîchement démarrée, ils sont tous à zéro car aucun trafic n'est encore arrivé. Lynis le signale lui-même : une règle non déclenchée peut très bien être en usage.
HRDN-7220	Les compilateurs sont nécessaires dans l'image pour DKMS et les modules du noyau : on ne peut pas les retirer. Ils sont donc réservés à root avec des permissions 0750, ce que vérifie le contrôle jumeau HRDN-7222, qui lui passe.
HTTP-6710	Dépend de données qui n'existent pas pendant la construction de l'image ; résolu au premier démarrage.
KRNL-6000	Le contrôle compare les sysctl à une liste figée pensée pour du matériel physique. Cette image fixe ses propres valeurs durcies et le noyau AWS en impose d'autres ; les écarts signalés sont nos décisions, pas des oublis.
LOGG-2154	Aucun serveur de logs externe n'est intégré, car la destination des journaux relève du choix de l'acheteur, pas du nôtre. Les journaux sont complets et locaux, prêts à être expédiés où il le souhaite.
LOGG-2190	La rotation reste celle livrée par la distribution et est revue service par service ; le contrôle attend une disposition précise qui ne convient pas à une image destinée à être reconfigurée après achat.

ID DU TEST	MOTIF DE NON-APPLICABILITÉ
MALW-3280	Ce contrôle ne note que les antivirus commerciaux. L'image embarque ClamAV, avec des signatures mises à jour automatiquement, et cela est noté par un contrôle distinct : nous n'allons pas empaqueter un logiciel payant tiers pour gagner un point.
NAME-4028	Le domaine DNS n'est pas intégré car l'instance le reçoit par DHCP depuis le VPC de l'acheteur. Ce que nous écririons ici serait écrasé au premier démarrage.
NAME-4404	Dépend de données qui n'existent pas pendant la construction de l'image ; résolu au premier démarrage.
SSH-7408	SSH reste sur le port 22, celui qu'attendent EC2 Instance Connect et les outils de console. Changer de port ne cache rien à un scanner ; la force brute est arrêtée par l'authentification par clé et fail2ban.
SSH-7440	SSH ne fige pas une liste explicite d'utilisateurs autorisés : l'acheteur crée ses propres comptes sur cette image, et notre liste l'enfermerait dehors. L'accès est déjà restreint par l'authentification par clé uniquement, l'interdiction du login root et fail2ban.
TOOL-5002	Aucun agent de gestion de configuration n'est installé, volontairement : l'image est construite avec Ansible via SSH, qui ne laisse rien tourner ensuite. Un démon de moins, c'est une surface d'attaque de moins.
USB-1000	Ne s'applique pas au modèle d'une instance cloud : ce qui est contrôlé n'existe pas ici ou relève de l'infrastructure du fournisseur.
USB-3000	Ne s'applique pas au modèle d'une instance cloud : ce qui est contrôlé n'existe pas ici ou relève de l'infrastructure du fournisseur.

Cette liste est lue dans le profil Lynis intégré à l'image elle-même, et non dans un document tenu à la main : ce que vous voyez ici est exactement ce que l'audit a appliqué.