تدقيق أمني بواسطة LYNIS

تقرير تقوية النظام

تدقيق أمني آلي للصورة، نُفِّذ باستخدام Lynis على مثيل مُجهَّز حديثًا قبل النشر.

المضيف **ip-172-31-83-68**	نظام التشغيل **Ubuntu 26.04 LTS**
النواة **7.0.0-1011-aws**	المعمارية **arm64**
إصدار LYNIS **3.1.7**	الملف التعريفي **custom.prf**
المدة **57s**	نُفِّذ بواسطة **root**

التزامنا بالتقوية

كل صورة تنشرها imaxe.cloud تأتي مُقوّاة افتراضيًا، حفاظًا على أمن من يشغّلها في بيئة الإنتاج. نحن لا نسلّم توزيعة مجرّدة: يصل النظام بجدار حماية يرفض افتراضيًا، وSSH مقيّد، ونواة وخيارات تركيب مُحصّنة، وتحديثات أمنية تلقائية، وأدوات سلامة الملفات والجذور الخفية والبرمجيات الخبيثة والتدقيق مثبّتة وقيد التشغيل.

هذا التقرير هو الدليل. يُنشأ تلقائيًا على نسخة مبنية حديثًا قبل نشر الصورة، ولا يُحرَّر يدويًا أبدًا، ويُنشر كاملًا بما في ذلك كل ما لم يمنحه التدقيق نقاطًا. التقوية جزء من المنتج، لذا فإن التدقيق الذي يقيسها يرافقه.

مؤشر التقوية

0	0
تحذيرات	اقتراحات
مشكلات ينبغي معالجتها	تحسينات تستحق الدراسة
241	**0**
الاختبارات المنفذة	الإضافات المفعلة
فحوصات أمان Lynis المنفذة	إضافات تدقيق إضافية

الخلاصة

يحقق النظام مؤشر تقوية 100/100: تكوين مُقوّى بدرجة عالية وجاهز للإنتاج.

1 النتيجة حسب الفئة

تفصيل نتيجة التدقيق حسب مجال الأمان، مشتق من التحذيرات والاقتراحات في كل مجال.

النواة والإقلاع	100
المصادقة	100
نظام الملفات والسلامة	100
الشبكة والجدار الناري	100
SSH	100
الحزم والأدوات	100
السجلات والوقت	100
التقوية ومكافحة البرمجيات الخبيثة	100

2 التحذيرات

نتائج يصنفها Lynis كتحذيرات. تُراجَع وتُعالَج قبل كل إصدار.

معرّف الاختبار	الوصف	الخطورة
لا تحذيرات — لم يجد التدقيق مشكلات من هذا المستوى.		

3 الاقتراحات

توصيات Lynis. بعضها لا ينطبق على صور السحابة أو يمثل قرارات تصميم مقصودة.

معرّف الاختبار	التوصية	الفئة
لا اقتراحات.		

4 فحوص تم تخطيها عن قصد

تشغّل الصورة Lynis بملف تعريف يتخطى 23 فحصًا. لا يمثّل أي منها ثغرة في التقوية: فهي فحوص لا يمكن تقييمها على صورة سحابية، أو تغطيها ضوابط أخرى بالفعل، أو تعتمد على بيانات لا توجد إلا بعد تشغيل النسخة. وكل فحص مُدرج مع سببه حتى يكون الاستثناء قابلًا للتدقيق.

معرّف الاختبار	سبب عدم الانطباق
AUTH-9284	الحسابات التي يشير إليها هي حسابات خدمات نظام أوبونتو الأساسي (daemon وbin وsys...). تأتي بلا كلمة مرور صالحة وبلا صدفة تفاعلية، وهو المطلوب تمامًا؛ لكن الفحص يقرأ هذه الحالة الطبيعية كأنها ملاحظة.
BOOT-5122	لا توجد كلمة مرور لـ GRUB لأنه لا توجد وحدة تحكم فعلية تُكتب عليها: نسخة EC2 تُقلع وحدها، ووحدة تحكمها استدعاء واجهة برمجية محميّ بـ IAM. كلمة المرور لن تكون سوى عائق عند الإنقاذ.
BOOT-5180	نتيجة إيجابية خاطئة على هذه الصورة: لا يمكن تقييم الفحص هنا ولن تعكس نتيجته الحالة الحقيقية للنظام.
BOOT-5264	نتيجة إيجابية خاطئة على هذه الصورة: لا يمكن تقييم الفحص هنا ولن تعكس نتيجته الحالة الحقيقية للنظام.
CRYP-7902	يعتمد على بيانات غير موجودة أثناء بناء الصورة؛ ويُحسم عند أول إقلاع.
DEB-0810	أداة apt-listbugs تفاعلية: توقف الترقية لتسأل إنسانًا. وعلى صورة تعمل دون إشراف ستعطّل التحديثات الأمنية التلقائية، وهي أهم بكثير.
FILE-6310	تستخدم الصورة وحدة تخزين جذرية واحدة، وهي الصيغة التي تُوسَّع بها النسخ السحابية وتُؤخذ لها لقطات. أما ما يريده هذا الفحص فعلًا — ألا تستطيع /tmp و/dev/shm و/run تنفيذ الملفات أو احتواء الأجهزة — فيتحقق هنا عبر خيارات تركيب مُحصَّنة.

معرّف الاختبار	سبب عدم الانطباق
FILE-7524	الأذونات مضبوطة على ما يحتاجه هذا المنتج ويجري التحقق منها في كل بناء عبر مجموعة اختباراتنا؛ أما الفحص العام فيَعُدّ ملفات التطبيق المشروعة أخطاءً.
FIRE-4512	يعدّ الفحص قواعد iptables ويصف القائمة القصيرة بأنها «فارغة». هنا الطبقة الأولى للترشيح هي مجموعة الأمان في AWS خارج النسخة، وufw يغلق كل ما عداها افتراضيًا: الحماية موجودة، لكنها ليست مكتوبة حيث ينظر هذا الفحص.
FIRE-4513	يعتبر الفحص كل قاعدة عدّاد حزمها صفر قاعدةً «غير مستخدمة». وعلى نسخة أُقلعت للتو تكون كلها أصفارًا لأن حركة المرور لم تصل بعد. ولينِس نفسه ينبّه إلى ذلك: القاعدة التي لم تُفعَّل قد تكون قيد الاستخدام تمامًا.
HRDN-7220	المُصرِّفات لازمة في الصورة من أجل DKMS ووحدات النواة، فلا يمكن حذفها. وبدل ذلك تُقصر على المستخدم الجذر بأذونات 0750، وهو ما يتحقق منه الفحص الشقيق HRDN-7222، وذاك ينجح.
HTTP-6710	يعتمد على بيانات غير موجودة أثناء بناء الصورة؛ ويُحسم عند أول إقلاع.
KRNL-6000	يقارن الفحص قيم sysctl بقائمة ثابتة مصمَّمة للعتاد الفعلي. هذه الصورة تضبط قيمها المُحصَّنة الخاصة، وبعضها تفرضه نواة AWS؛ فالفروق التي يبلّغ عنها قراراتنا لا سهوٌ منا.
LOGG-2154	لا يُدمج أي خادم سجلات خارجي لأن وجهة السجلات اختيار المشتري لا اختيارنا. السجلات كاملة ومحلية وجاهزة لإرسالها إلى حيث يشاء.
LOGG-2190	يُترك التدوير كما توفّره التوزيعة ويُراجَع خدمةً خدمة؛ فالفحص يتوقع ترتيبًا بعينه لا يناسب صورة يُعاد ضبطها بعد الشراء.
MALW-3280	هذا الفحص يمنح النقاط لمنتجات مكافحة الفيروسات التجارية فقط. الصورة تحمل ClamAV بتوقيعات تُحدَّث تلقائيًا، وهذا يقيسه فحص آخر مستقل: لن نضمّ برمجيات مدفوعة من طرف ثالث لكسب نقطة واحدة.
NAME-4028	اسم نطاق DNS لا يُدمج في الصورة لأن النسخة تتلقاه عبر DHCP من شبكة المشتري الافتراضية. وأي قيمة نكتبها هنا ستُستبدل عند أول إقلاع.
NAME-4404	يعتمد على بيانات غير موجودة أثناء بناء الصورة؛ ويُحسم عند أول إقلاع.
SSH-7408	يبقى SSH على المنفذ 22 لأنه ما تتوقعه EC2 Instance Connect وأدوات وحدة التحكم. تغيير المنفذ لا يخفي شيئًا عن الماسح؛ أما التخمين العنيف فتوقفه المصادقة بالمفتاح وfail2ban.
SSH-7440	لا يثبّت SSH قائمة صريحة بالمستخدمين المسموح لهم: فالمشتري ينشئ حساباته الخاصة فوق هذه الصورة، وقائمتنا ستُبقيه خارجًا. الوصول مقيَّد أصلًا بالمصادقة بالمفتاح فقط، ومنع دخول الجذر، وfail2ban.
TOOL-5002	لا يُثبَّت أي وكيل لإدارة الإعدادات عن قصد: تُبنى الصورة باستخدام Ansible عبر SSH، ولا يترك بعده أي خدمة قيد التشغيل. خدمة أقل تعني سطح هجوم أقل.
USB-1000	لا ينطبق على نموذج النسخة السحابية: فما يفحصه إما غير موجود هنا أو تتكفّل به بنية المزوّد التحتية.
USB-3000	لا ينطبق على نموذج النسخة السحابية: فما يفحصه إما غير موجود هنا أو تتكفّل به بنية المزوّد التحتية.

تُقرأ هذه القائمة من ملف تعريف Lynis المدمج داخل الصورة نفسها، لا من مستند يُحدَّث يدويًا: ما تراه هنا هو تمامًا ما طبّقه التدقيق.