LYNIS SECURITY AUDIT

System hardening report

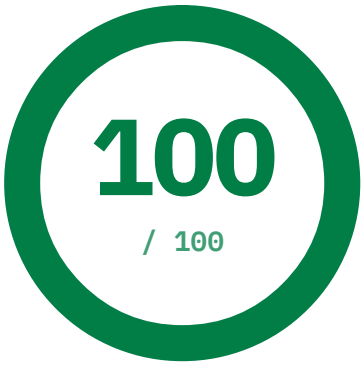
Automated security audit of the image, run with Lynis on a freshly provisioned instance before publishing.

HOST **ip-172-31-84-101**	OPERATING SYSTEM **Ubuntu 26.04 LTS**
KERNEL **7.0.0-1010-aws**	ARCHITECTURE **arm64**
LYNIS VERSION **3.1.7**	PROFILE **custom.prf**
DURATION **56s**	RUN BY **root**

Our hardening commitment

Every image imaxe.cloud publishes is hardened by default, for the security of whoever runs it. We do not hand over a bare distribution: the system ships with a default-deny firewall, SSH restricted, kernel and mount options tightened, unattended security updates, and file integrity, rootkit, malware and audit tooling installed and running.

This report is the evidence. It is generated automatically on a freshly built instance before the image is published, it is never edited by hand, and it is published in full — including everything the audit did not score. Hardening is part of the product, so the audit that measures it travels with it.



HARDENING INDEX

0 Warnings Issues that should be addressed	**0** Suggestions Improvements worth considering
241 Tests performed Lynis security checks executed	**0** Plugins enabled Additional audit plugins

Verdict

The system reaches a hardening index of 100/100: a strongly hardened configuration ready for production use.

1 Score by category

Breakdown of the audit results by security area, derived from the warnings and suggestions found in each one.

Kernel & boot	100
Authentication	100
Filesystem & integrity	100
Network & firewall	100
SSH	100
Packages & tools	100
Logging & time	100
Hardening & malware	100

2 Warnings

Findings that Lynis flags as warnings. They are reviewed and remediated before each release.

TEST ID	DESCRIPTION	SEVERITY
No warnings — the audit found no issues at this level.		

3 Suggestions

Recommendations reported by Lynis. Some do not apply to cloud images or are deliberate design decisions.

TEST ID	RECOMMENDATION	CATEGORY
No suggestions.		

4 Checks deliberately skipped

The image runs Lynis with a profile that skips 23 checks. None of them is a hardening gap: they are checks that cannot be evaluated on a cloud image, that are already covered by another control, or that depend on data which only exists once the instance is running. Each one is listed with its reason so the omission can be audited.

TEST ID	REASON WHY IT DOES NOT APPLY
AUTH-9284	The accounts it flags are the service accounts of the Ubuntu base (daemon, bin, sys...). They ship without a valid password and without an interactive shell, which is exactly what is wanted; the check reads that normal state as a finding.
BOOT-5122	There is no GRUB password because there is no physical console to type it on: an EC2 instance boots unattended and its console is an API call protected by IAM. The password would only be an obstacle for rescue work.
BOOT-5180	False positive on this image: the check cannot be evaluated here and its result would not reflect the real state of the system.
BOOT-5264	False positive on this image: the check cannot be evaluated here and its result would not reflect the real state of the system.
CRYP-7902	Depends on data that does not exist while the image is being built; it is resolved on first boot.

TEST ID	REASON WHY IT DOES NOT APPLY
DEB-0810	apt-listbugs is interactive: it pauses an upgrade to ask a human. On an unattended image it would block the automatic security updates, which matter far more.
FILE-6310	The image ships a single root volume, which is how a cloud instance is resized and snapshotted. What this check really wants — /tmp, /dev/shm and /run unable to execute binaries or hold devices — is achieved here with hardened mount options.
FILE-7524	Permissions are set to what this product needs and are verified on every build by our own test suite; the generic check flags legitimate application files as if they were mistakes.
FIRE-4512	The check counts iptables rules and calls a short list "empty". Here the first filtering layer is the AWS Security Group, outside the instance, and ufw closes everything else by default — the protection exists, it just is not written where this check looks.
FIRE-4513	The check marks as unused any rule whose packet counter is zero. On a freshly booted instance every counter is zero because no traffic has arrived yet. Lynis itself warns about this: rules that are not triggered may still be in use.
HRDN-7220	Compilers are needed on the image for DKMS and kernel modules, so they cannot be removed. Instead they are restricted to root with 0750 permissions — which is what the companion check HRDN-7222 verifies, and it passes.
HTTP-6710	Depends on data that does not exist while the image is being built; it is resolved on first boot.
KRNL-6000	The check compares sysctl values against a fixed list that assumes bare metal. This image sets its own hardened values and the AWS kernel constrains others; the differences it reports are our decisions, not oversights.
LOGG-2154	No external log server is baked in because the log destination is the buyer's choice, not ours. Logs are complete and local, ready to be shipped wherever they want.
LOGG-2190	Rotation is left as the distribution ships it and reviewed service by service; the check expects one specific layout that does not fit an image meant to be reconfigured after purchase.
MALW-3280	This check only scores commercial antivirus products. The image ships ClamAV, with signatures updated automatically, and that is scored by its own check — we are not going to bundle paid third-party software just to earn a point.
NAME-4028	The DNS domain is not baked in because the instance gets it by DHCP from the buyer's VPC. Whatever we wrote here would be overwritten at first boot.
NAME-4404	Depends on data that does not exist while the image is being built; it is resolved on first boot.
SSH-7408	SSH stays on port 22 because that is what EC2 Instance Connect and the console tooling expect. Moving the port hides nothing from a scanner; brute force is handled by key-only authentication and fail2ban.

TEST ID	REASON WHY IT DOES NOT APPLY
SSH-7440	SSH does not pin an explicit list of allowed users: the buyer creates their own accounts on top of this image, and our list would lock them out. Access is already restricted by key-only authentication, no root login and fail2ban.
TOOL-5002	No configuration-management agent is installed on purpose: the image is built with Ansible over SSH, which leaves nothing running afterwards. One less daemon is one less attack surface.
USB-1000	Does not apply to the model of a cloud instance: what it checks either does not exist here or is handled by the provider's infrastructure.
USB-3000	Does not apply to the model of a cloud instance: what it checks either does not exist here or is handled by the provider's infrastructure.

This list is read from the Lynis profile baked into the image itself, not from a document kept by hand: what you see here is exactly what the audit applied.