LYNIS 安全审计

系统加固报告

镜像的自动化安全审计，在发布前于新配置的实例上使用 Lynis 执行。

主机 **ip-172-31-84-101**	操作系统 **Ubuntu 26.04 LTS**
内核 **7.0.0-1010-aws**	架构 **arm64**
LYNIS 版本 **3.1.7**	配置文件 **custom.prf**
耗时 **56s**	执行者 **root**

我们的加固承诺

imaxe.cloud 发布的每一个镜像都默认经过加固，以保障使用者的生产环境安全。我们交付的不是一个未经处理的发行版：系统出厂即带有默认拒绝的防火墙、受限的 SSH、加固的内核与挂载选项、无人值守的安全更新，以及已安装并运行的文件完整性、Rootkit、恶意软件和审计工具。

本报告即是凭证。它在镜像发布前于全新构建的实例上自动生成，从不人工修改，并完整公开，包括审计未计分的全部内容。加固是产品的一部分，因此衡量加固的审计也随产品一同交付。

加固指数

0	0
警告	建议
需要处理的问题	值得考虑的改进
241	**0**
已执行测试	已启用插件
已执行的 Lynis 安全检查	附加审计插件

结论

系统加固指数达到 100/100：配置经过高度加固，可用于生产环境。

1 分类得分

按安全领域细分的审计结果，由各领域的警告和建议推导得出。

内核与启动	100
身份认证	100
文件系统与完整性	100
网络与防火墙	100
SSH	100
软件包与工具	100
日志与时间	100
加固与恶意软件防护	100

2 警告

Lynis 标记为警告的发现项。每次发布前都会审查并修复。

测试 ID	描述	严重程度
无警告 — 审计未发现此级别的问题。		

3 建议

Lynis 给出的建议。其中一些不适用于云镜像，或属于有意的设计决策。

测试 ID	建议内容	类别
无建议。		

4 有意跳过的检查

该镜像运行 Lynis 时所用的配置文件跳过了 23 项检查。它们都不是加固缺口：这些检查要么在云镜像上无法评估，要么已由其他控制措施覆盖，要么依赖只有实例运行后才存在的数据。每一项都附有原因，以便对这些省略进行核查。

测试 ID	不适用的原因
AUTH-9284	它标记的是 Ubuntu 基础系统的服务账户（daemon、bin、sys…）。这些账户本来就没有有效密码、没有交互式 shell，这正是我们要的；检查把这种正常状态当成了问题。
BOOT-5122	没有设置 GRUB 密码，因为没有可以输入密码的物理控制台：EC2 实例无人值守地启动，它的控制台是一次受 IAM 保护的 API 调用。密码只会在救援时碍事。
BOOT-5180	本镜像上的误报：该检查在此无法评估，其结果并不反映系统的真实状态。
BOOT-5264	本镜像上的误报：该检查在此无法评估，其结果并不反映系统的真实状态。
CRYP-7902	依赖构建镜像时尚不存在的数据；将在首次启动时确定。
DEB-0810	apt-listbugs 是交互式的：它会中断升级去询问人工。在无人值守的镜像上，它会阻塞自动安全更新，而后者要重要得多。
FILE-6310	本镜像使用单一根卷，这正是云实例扩容和快照的形态。该检查真正想要的——/tmp、/dev/shm 和 /run 不能执行二进制文件、不能承载设备——在这里通过加固的挂载选项实现。

测试 ID	不适用的原因
FILE-7524	权限按本产品的需要设定，并在每次构建时由我们自己的测试套件核验；通用检查会把应用程序的正当文件误判为错误。
FIRE-4512	该检查数 iptables 规则条数，条数少就判为“空”。在这里，第一道过滤是实例之外的 AWS 安全组，其余一切由 ufw 默认拒绝：防护是存在的，只是没写在这项检查查看的地方。
FIRE-4513	该检查把数据包计数为零的规则一律判为“未使用”。刚启动的实例上所有计数都是零，因为还没有流量到达。Lynis 自己也提示过：没有被触发的规则完全可能正在使用。
HRDN-7220	镜像里需要编译器来支持 DKMS 和内核模块，无法删除。我们的做法是用 0750 权限把它们限制给 root 使用——这正是配套检查 HRDN-7222 所验证的，而那一项是通过的。
HTTP-6710	依赖构建镜像时尚不存在的数据；将在首次启动时确定。
KRNL-6000	该检查拿 sysctl 值去比对一份为物理机设想的固定清单。本镜像设定了自己的加固值，另一些则由 AWS 内核限定；它报出的差异是我们的决定，而非疏漏。
LOGG-2154	镜像不预置外部日志服务器，因为日志送往何处由买家决定，而不是我们。日志完整且保存在本地，随时可以转发到任何地方。
LOGG-2190	日志轮转沿用发行版自带的配置，并逐个服务复核；该检查期待一种特定布局，并不适合一个购买后需要重新配置的镜像。
MALW-3280	该检查只为商业杀毒产品计分。本镜像自带 ClamAV，病毒库自动更新，这由另一项检查单独计分——我们不会为了一个分数而捆绑第三方付费软件。
NAME-4028	DNS 域名不写死在镜像里，因为实例是从买家的 VPC 通过 DHCP 获取的。我们在这里写什么，首次启动都会被覆盖。
NAME-4404	依赖构建镜像时尚不存在的数据；将在首次启动时确定。
SSH-7408	SSH 保留在 22 端口，因为 EC2 Instance Connect 和控制台工具都期望它。改端口并不能瞒过扫描器；暴力破解由密钥认证和 fail2ban 拦下。
SSH-7440	SSH 不固定允许登录的用户名单：买家会在本镜像之上创建自己的账户，我们写死的名单反而会把他们挡在门外。访问已经由仅密钥认证、禁止 root 登录和 fail2ban 加以限制。
TOOL-5002	我们有意不安装任何配置管理代理：镜像通过 SSH 用 Ansible 构建，之后不留下任何常驻进程。少一个守护进程，就少一处攻击面。
USB-1000	不适用于云实例的运行模式：所检查的对象在这里并不存在，或者由云服务商的基础设施负责。
USB-3000	不适用于云实例的运行模式：所检查的对象在这里并不存在，或者由云服务商的基础设施负责。

此列表读取自烘焙在镜像内部的 Lynis 配置文件，而非人工维护的文档：这里显示的正是审计实际应用的内容。