AUDITORIA DE SEGURANÇA LYNIS

Relatório de hardening do sistema

Auditoria de segurança automatizada da imagem, executada com Lynis numa instância recém-provisionada antes da publicação.

HOST **ip-172-31-83-68**	SISTEMA OPERATIVO **Ubuntu 26.04 LTS**
KERNEL **7.0.0-1011-aws**	ARQUITETURA **arm64**
VERSÃO DO LYNIS **3.1.7**	PERFIL **custom.prf**
DURAÇÃO **57s**	EXECUTADO POR **root**

O nosso compromisso de endurecimento

Todas as imagens que a imaxe.cloud publica vão endurecidas de origem, pela segurança de quem as coloca em produção. Não entregamos uma distribuição nua: o sistema chega com firewall que nega por omissão, SSH restrito, kernel e opções de montagem reforçados, atualizações de segurança automáticas e as ferramentas de integridade de ficheiros, rootkits, malware e auditoria instaladas e a funcionar.

Este relatório é a prova. É gerado automaticamente numa instância acabada de construir, antes de publicar a imagem, nunca é editado à mão e é publicado por inteiro, incluindo tudo o que a auditoria não pontuou. O endurecimento faz parte do produto, por isso a auditoria que o mede viaja com ele.

ÍNDICE DE HARDENING

0
Avisos
Problemas a corrigir

0
Sugestões
Melhorias a considerar

241
Testes realizados
Verificações de segurança Lynis executadas

0
Plugins ativos
Plugins de auditoria adicionais

Veredicto
O sistema atinge um índice de hardening de 100/100: uma configuração fortemente reforçada e pronta para produção.

1 Pontuação por categoria

Detalhe do resultado da auditoria por área de segurança, derivado dos avisos e sugestões de cada uma.

Kernel e arranque	100
Autenticação	100
Sistema de ficheiros e integridade	100
Rede e firewall	100
SSH	100
Pacotes e ferramentas	100

Registo e hora	100
Hardening e malware	100

2 Avisos

Descobertas que o Lynis assinala como avisos. São revistas e corrigidas antes de cada publicação.

ID DO TESTE	DESCRIÇÃO	SEVERIDADE
Sem avisos — a auditoria não encontrou problemas deste nível.		

3 Sugestões

Recomendações do Lynis. Algumas não se aplicam a imagens cloud ou são decisões de design deliberadas.

ID DO TESTE	RECOMENDAÇÃO	CATEGORIA
Sem sugestões.		

4 Verificações omitidas de propósito

A imagem executa o Lynis com um perfil que omite 23 verificações. Nenhuma delas é uma falha de endurecimento: são verificações que não se conseguem avaliar numa imagem cloud, que já estão cobertas por outro controlo, ou que dependem de dados que só existem com a instância a correr. Cada uma é listada com o seu motivo, para que a omissão seja auditável.

ID DO TESTE	MOTIVO POR QUE NÃO SE APLICA
AUTH-9284	As contas assinaladas são as de serviço da base Ubuntu (daemon, bin, sys…). Vêm sem password válida e sem shell interativa, que é precisamente o pretendido; o teste lê esse estado normal como um achado.
BOOT-5122	Não há password de GRUB porque não há consola física onde a escrever: uma instância EC2 arranca sozinha e a sua consola é uma chamada de API protegida por IAM. A password só seria um estorvo num resgate.
BOOT-5180	Falso positivo nesta imagem: a verificação não é avaliável aqui e o seu resultado não refletiria o estado real do sistema.

ID DO TESTE	MOTIVO POR QUE NÃO SE APLICA
BOOT-5264	Falso positivo nesta imagem: a verificação não é avaliável aqui e o seu resultado não refletiria o estado real do sistema.
CRYP-7902	Depende de dados que não existem enquanto a imagem é construída; resolve-se no primeiro arranque.
DEB-0810	O apt-listbugs é interativo: para a atualização para perguntar a uma pessoa. Numa imagem não assistida bloquearia as atualizações automáticas de segurança, que importam muito mais.
FILE-6310	A imagem usa um único volume raiz, que é como uma instância cloud se redimensiona e se copia. O que esta verificação quer mesmo — que /tmp, /dev/shm e /run não possam executar binários nem conter dispositivos — aqui consegue-se com opções de montagem reforçadas.
FILE-7524	As permissões são as que este produto precisa e são verificadas em cada build pela nossa própria bateria de testes; a verificação genérica assinala como erros ficheiros legítimos da aplicação.
FIRE-4512	A verificação conta regras de iptables e chama «vazio» a uma lista curta. Aqui a primeira camada de filtragem é o Security Group da AWS, fora da instância, e o ufw fecha por omissão tudo o resto: a proteção existe, só não está escrita onde este teste olha.
FIRE-4513	O teste marca como «sem uso» qualquer regra cujo contador de pacotes esteja a zero. Numa instância acabada de arrancar estão todos a zero porque ainda não chegou tráfego. O próprio Lynis avisa disto: uma regra que não disparou pode estar perfeitamente em uso.
HRDN-7220	Os compiladores são precisos na imagem para DKMS e módulos do kernel, por isso não podem ser removidos. O que se faz é restringi-los a root com permissões 0750, que é o que a verificação irmã HRDN-7222 confirma, e essa passa.
HTTP-6710	Depende de dados que não existem enquanto a imagem é construída; resolve-se no primeiro arranque.
KRNL-6000	A verificação compara os sysctl com uma lista fixa pensada para ferro. Esta imagem fixa os seus próprios valores reforçados e o kernel da AWS condiciona outros; as diferenças reportadas são decisões nossas, não descuidos.
LOGG-2154	Não se embute nenhum servidor de logs externo porque o destino dos registos é escolha do comprador, não nossa. Os registos estão completos e locais, prontos a ser enviados para onde quiser.
LOGG-2190	A rotação fica como a distribuição a entrega e é revista serviço a serviço; a verificação espera uma disposição concreta que não encaixa numa imagem pensada para ser reconfigurada depois da compra.

ID DO TESTE	MOTIVO POR QUE NÃO SE APLICA
MALW-3280	Esta verificação só pontua antivírus comerciais. A imagem leva ClamAV, com assinaturas atualizadas automaticamente, e isso é pontuado por outra verificação à parte: não vamos empacotar software pago de terceiros para ganhar um ponto.
NAME-4028	O domínio DNS não é embutido porque a instância o recebe por DHCP da VPC do comprador. O que escrevêssemos aqui seria sobrescrito no primeiro arranque.
NAME-4404	Depende de dados que não existem enquanto a imagem é construída; resolve-se no primeiro arranque.
SSH-7408	O SSH fica na porta 22 porque é a que o EC2 Instance Connect e as ferramentas de consola esperam. Mudar de porta não esconde nada de um scanner; a força bruta é travada pela autenticação por chave e pelo fail2ban.
SSH-7440	O SSH não fixa uma lista explícita de utilizadores permitidos: o comprador cria as suas próprias contas sobre esta imagem, e a nossa lista deixá-lo-ia de fora. O acesso já está restrito por autenticação só com chave, sem login de root e com fail2ban.
TOOL-5002	Não se instala nenhum agente de gestão de configuração de propósito: a imagem é construída com Ansible por SSH, que não deixa nada a correr depois. Um daemon a menos é uma superfície de ataque a menos.
USB-1000	Não se aplica ao modelo de uma instância cloud: o que verifica não existe aqui ou é coberto pela infraestrutura do fornecedor.
USB-3000	Não se aplica ao modelo de uma instância cloud: o que verifica não existe aqui ou é coberto pela infraestrutura do fornecedor.

Esta lista é lida do perfil do Lynis embutido na própria imagem, não de um documento mantido à mão: o que aparece aqui é exatamente o que a auditoria aplicou.