АУДИТ БЕЗОПАСНОСТИ LYNIS

Отчёт об усилении защиты системы

Автоматизированный аудит безопасности образа, выполненный Lynis на только что развёрнутом инстансе перед публикацией.

ХОСТ **ip-172-31-84-101**	ОПЕРАЦИОННАЯ СИСТЕМА **Ubuntu 26.04 LTS**
ЯДРО **7.0.0-1010-aws**	АРХИТЕКТУРА **arm64**
ВЕРСИЯ LYNIS **3.1.7**	ПРОФИЛЬ **custom.prf**
ДЛИТЕЛЬНОСТЬ **56s**	ЗАПУЩЕН **root**

Наши обязательства по укреплению

Все образы, которые публикует imaxe.cloud, укреплены по умолчанию — ради безопасности тех, кто запускает их в продакшене. Мы не отдаём голый дистрибутив: система поставляется с межсетевым экраном, запрещающим по умолчанию, ограниченным SSH, укреплёнными параметрами ядра и монтирования, автоматическими обновлениями безопасности, а также с установленными и работающими средствами контроля целостности файлов, поиска руткитов, антивирусной защиты и аудита.

Этот отчёт — доказательство. Он формируется автоматически на только что собранном экземпляре, до публикации образа, никогда не правится вручную и публикуется целиком, включая всё, что аудит не оценил баллами. Укрепление — часть продукта, поэтому аудит, который его измеряет, идёт вместе с ним.

ИНДЕКС ЗАЩИЩЁННОСТИ

0
Предупреждения
Проблемы, требующие устранения

0
Рекомендации
Улучшения, которые стоит рассмотреть

241
Выполнено проверок
Выполненные проверки безопасности Lynis

0
Включённые плагины
Дополнительные плагины аудита

Вердикт
Система достигает индекса защищённости 100/100: сильно укреплённая конфигурация, готовая к продакшену.

1 Оценка по категориям

Разбивка результатов аудита по областям безопасности на основе предупреждений и рекомендаций в каждой из них.

Ядро и загрузка	100
Аутентификация	100
Файловая система и целостность	100
Сеть и межсетевой экран	100
SSH	100
Пакеты и инструменты	100

2 Предупреждения

Замечания, которые Lynis помечает как предупреждения. Они проверяются и устраняются перед каждым выпуском.

ID ТЕСТА	ОПИСАНИЕ	СЕРЬЁЗНОСТЬ
Предупреждений нет — аудит не выявил проблем этого уровня.		

3 Рекомендации

Рекомендации Lynis. Некоторые не применимы к облачным образам или являются осознанными проектными решениями.

ID ТЕСТА	РЕКОМЕНДАЦИЯ	КАТЕГОРИЯ
Рекомендаций нет.		

4 Намеренно пропущенные проверки

Образ запускает Lynis с профилем, который пропускает 23 проверок. Ни одна из них не является пробелом в укреплении: это проверки, которые невозможно оценить в облачном образе, которые уже покрыты другим механизмом или которые зависят от данных, появляющихся только на работающем экземпляре. Каждая указана с причиной, чтобы пропуск можно было проверить.

ID ТЕСТА	ПРИЧИНА, ПО КОТОРОЙ НЕ ПРИМЕНИМО
AUTH-9284	Учётные записи, на которые она указывает, — служебные записи базовой Ubuntu (daemon, bin, sys…). Они идут без действующего пароля и без интерактивной оболочки, что как раз и требуется; проверка принимает это нормальное состояние за находку.
BOOT-5122	Пароля GRUB нет, потому что нет физической консоли, где его вводить: экземпляр EC2 загружается сам, а его консоль — это вызов API, защищённый IAM. Пароль лишь мешал бы при аварийном восстановлении.

ID ТЕСТА	ПРИЧИНА, ПО КОТОРОЙ НЕ ПРИМЕНИМО
BOOT-5180	Ложное срабатывание на этом образе: проверку здесь невозможно оценить, и её результат не отражал бы реальное состояние системы.
BOOT-5264	Ложное срабатывание на этом образе: проверку здесь невозможно оценить, и её результат не отражал бы реальное состояние системы.
CRYP-7902	Зависит от данных, которых нет во время сборки образа; определяется при первом запуске.
DEB-0810	apt-listbugs интерактивен: он останавливает обновление, чтобы спросить человека. На образе без оператора это заблокировало бы автоматические обновления безопасности, которые куда важнее.
FILE-6310	Образ использует единственный корневой том — именно так облачную машину расширяют и снимают снапшоты. То, чего эта проверка добивается по сути (чтобы /tmp, /dev/shm и /run не могли исполнять файлы и содержать устройства), здесь достигается укреплёнными параметрами монтирования.
FILE-7524	Права выставлены под нужды этого продукта и проверяются при каждой сборке нашим собственным набором тестов; универсальная проверка помечает как ошибку законные файлы приложения.
FIRE-4512	Проверка считает правила iptables и называет короткий список «пустым». Здесь первый уровень фильтрации — Security Group в AWS, вне экземпляра, а всё остальное ufw закрывает по умолчанию: защита есть, просто она записана не там, куда смотрит эта проверка.
FIRE-4513	Проверка помечает как неиспользуемое любое правило с нулевым счётчиком пакетов. На только что запущенном экземпляре они все нулевые, потому что трафика ещё не было. Об этом предупреждает сам Lynis: несработавшее правило вполне может быть рабочим.
HRDN-7220	Компиляторы нужны в образе для DKMS и модулей ядра, убрать их нельзя. Вместо этого они ограничены пользователем root и правами 0750 — именно это проверяет парная проверка HRDN-7222, и она проходит.
HTTP-6710	Зависит от данных, которых нет во время сборки образа; определяется при первом запуске.
KRNL-6000	Проверка сверяет значения sysctl с фиксированным списком, рассчитанным на «железо». Этот образ задаёт собственные укреплённые значения, а часть определяется ядром AWS; сообщаемые расхождения — наши решения, а не упущения.
LOGG-2154	Внешний сервер журналов не зашивается: место назначения логов выбирает покупатель, а не мы. Журналы полны и лежат локально, готовые к отправке куда угодно.

ID ТЕСТА	ПРИЧИНА, ПО КОТОРОЙ НЕ ПРИМЕНИМО
LOGG-2190	Ротация оставлена такой, какой её поставляет дистрибутив, и проверяется по каждой службе; проверка ждёт одной конкретной схемы, которая не подходит образу, рассчитанному на перенастройку после покупки.
MALW-3280	Эта проверка начисляет баллы только коммерческим антивирусам. В образе есть ClamAV с автоматически обновляемыми сигнатурами, и это оценивает отдельная проверка: мы не станем включать платное стороннее ПО ради одного балла.
NAME-4028	DNS-домен не зашивается, потому что экземпляр получает его по DHCP из VPC покупателя. Всё, что мы бы здесь записали, было бы перезаписано при первом запуске.
NAME-4404	Зависит от данных, которых нет во время сборки образа; определяется при первом запуске.
SSH-7408	SSH остаётся на порту 22, потому что именно его ожидают EC2 Instance Connect и консольные инструменты. Смена порта ничего не скрывает от сканера; перебор останавливают вход по ключу и fail2ban.
SSH-7440	SSH не задаёт жёсткий список разрешённых пользователей: покупатель создаёт свои учётные записи поверх этого образа, и наш список закрыл бы ему доступ. Доступ и так ограничен входом только по ключу, запретом root-логина и fail2ban.
TOOL-5002	Агент управления конфигурацией не устанавливается намеренно: образ собирается Ansible по SSH, который затем ничего не оставляет запущенным. Одной службой меньше — одной поверхностью атаки меньше.
USB-1000	Неприменимо к модели облачного экземпляра: проверяемого здесь либо не существует, либо это берёт на себя инфраструктура провайдера.
USB-3000	Неприменимо к модели облачного экземпляра: проверяемого здесь либо не существует, либо это берёт на себя инфраструктура провайдера.

Этот список читается из профиля Lynis, встроенного в сам образ, а не из документа, который ведут вручную: здесь показано ровно то, что применил аудит.