Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Защита Linux-сервера: наш стандарт hardening на Debian

Как мы укрепляем production-серверы Debian 13: SSH, nftables, автопатчи, бэкапы, мониторинг

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Клиент арендует VPS под 1С, сайт или почту, сервер настраивают один раз и забывают: патчи не ставятся, SSH открыт всему интернету, бэкап существует на словах. Итог предсказуем — брутфорс, майнер или шифровальщик, письмо хостера о ботнете и простой в несколько дней. Мы закрываем это стандартным контуром hardening для Debian: периметр, автопатчи, бэкапы, мониторинг, аудит.

Почему это важно бизнесу

- Восстановление после компрометации сервера — дни простоя 1С и почты: останавливаются продажи и бухгалтерия
- Утечка персональных данных с незакрытого сервиса — штрафы по 152-ФЗ и проверка регулятора
- Хостер блокирует VPS за участие в ботнете без предупреждения — сайт и почта падают мгновенно
- Контур защиты — часы работ по шаблону; инцидент — недели разборов и внеплановый бюджет на порядок больше

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

13.6

базовая ОС внедрений: Debian 13 trixie, ядро 6.12 LTS, репозитории stable + security

Debian 13.6, debian.org

≤24 ч

security-патчи ежесуточно: APT::Periodic::Unattended-Upgrade "1" в apt.conf.d/20auto-upgrades

unattended-upgrades, Debian wiki

maxretry 3

fail2ban sshd: 3 ошибки за findtime 10m → бан 1 ч, bantime.increment удваивает срок повторным

fail2ban 1.1, наш стандарт

3-2-1

схема бэкапов restic: keep-hourly 24 / keep-daily 30 / keep-monthly 12 + офсайт S3-репозиторий

restic 0.19, наш стандарт

80+

целевой Lynis hardening index после настройки; ниже 80 — сервер не принимаем в эксплуатацию

Lynis 3.x, cisofy.com

60 с

интервал опроса ключевых метрик Zabbix agent 2; алерты CPU/RAM/диск от 85%, SSL за 14 дней

Zabbix 7.0 LTS

РЕАЛИЗАЦИЯ 1 ИЗ 3

Периметр: SSH-hardening и nftables

Что настраиваем

Любой VPS или выделенный сервер клиента на Debian 12/13 — веб, 1С, почта, БД; закрываем до передачи в эксплуатацию

Как мы это делаем

1. Drop-in /etc/ssh/sshd_config.d/00-hardening.conf: PermitRootLogin no, PasswordAuthentication no, KbdInteractiveAuthentication no, MaxAuthTries 3, AllowGroups sshuse…
2. Ключи только ed25519, у каждого админа персональный; работа через sudo-пользователя, root-пароль — в сейфе для консоли хостера
3. nftables: таблица inet filter, policy drop на input; открываем только 22 (со списка наших IP), 80/443; сервисные порты 1С и БД — только через WireGuard
4. fail2ban 1.1: jail sshd, backend=systemd, banaction=nftables-multiport, maxretry 3, findtime 10m, bantime 1h, bantime.increment=true
5. Проверка снаружи: скан портов с внешнего узла + sshd -T; эталонный список открытых портов фиксируем в паспорте сервера

РЕЗУЛЬТАТ

Шум брутфорса падает с 10–15 тысяч попыток в сутки до нуля осмысленных: пароль перебрать нельзя, root недоступен, лишние порты не отвечают. Эталон портов позволяет за минуту заметить, что на сервере появилось что-то новое.

КЛЮЧЕВОЙ НЮАНС

sshd берёт первое совпадение параметра — drop-in должен сортироваться раньше остальных drop-in (префикс 00-, иначе его перебьёт 50-cloud-init.conf), итог проверяем через sshd -T. Перед рестартом sshd держим вт…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Автообновления: unattended-upgrades и контроль ядра

Что настраиваем

Все Linux-серверы на абонентке; включаем в первый день, дальше только контролируем отчёты

Как мы это делаем

1. В apt.conf.d/20auto-upgrades: Update-Package-Lists "1" и Unattended-Upgrade "1"; в 50unattended-upgrades оставляем Origins-Pattern Debian-Security
2. Unattended-Upgrade::Mail + MailReport "on-change": сводка установленных патчей по каждому серверу падает на дежурную почту
3. needrestart после патчей: находим сервисы со старыми библиотеками (openssl, glibc) и перезапускаем их в тот же день
4. Ядро: метапакет linux-image-amd64 + плановое окно ребута раз в месяц — новые ядра приходят отдельным пакетом и без перезагрузки не активируются
5. Major-апгрейд (12→13) — только вручную раз в 2–3 года: полный бэкап, release notes trixie, согласованное окно простоя

РЕЗУЛЬТАТ

Между выходом DSA-бюллетеня и установкой патча проходит меньше суток вместо квартального ручного цикла. На принимаемых серверах регулярно находим 100+ непоставленных security-обновлений — после включения механизма долг больше не копится.

КЛЮЧЕВОЙ НЮАНС

Образ VPS у провайдера бывает собран 2–3 года назад, а unattended-upgrades в нём выключен. Проверяем systemctl status apt-daily-upgrade.timer и делаем apt full-upgrade до передачи сервера в работу.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Бэкапы restic, мониторинг Zabbix и регулярный аудит

Что настраиваем

Данные: /etc, /var/www, дампы БД, выгрузки 1С; офсайт — S3 в другом ЦОДе; мониторинг — наш кластер Zabbix 7.0 LTS

Как мы это делаем

1. restic init в S3-репозиторий, systemd-timer на почасовой снапшот; перед снапшотом — pg_dump/mysqldump в спул, пароль репозитория хранится вне сервера
2. Ротация: restic forget --keep-hourly 24 --keep-daily 30 --keep-monthly 12 --prune; на S3-ключах политикой закрыто удаление объектов
3. Проверка: еженощный restic check, раз в месяц --read-data-subset=5%, раз в квартал — учебное восстановление случайного сервера с замером времени
4. Zabbix agent 2, шаблон Linux by Zabbix agent: CPU/RAM/диск с порогом 85%, systemd-юниты, возраст снапшота (>26 ч — алерт), SSL за 14 дней; алерты в Telegram
5. lynis audit system ежемесячно + auditd с правилами на /etc/passwd, sudoers и системные бинарники; журнал уходит на внешний syslog

РЕЗУЛЬТАТ

Взлом или шифровальщик перестают быть катастрофой: точка восстановления не старше часа, восстановление по регламенту — 2–3 часа. О деградации узнаём из Telegram раньше пользователей, а не из письма хостера.

КЛЮЧЕВОЙ НЮАНС

Бэкап без регулярного тестового восстановления — это гипотеза, а не бэкап. Метрику «возраст последнего удачного снапшота» держим в мониторинге наравне с CPU: молчащий бэкап — самый частый скрытый отказ.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Образ хостера трёхлетней давности**
  Свежий VPS часто развёрнут из старого шаблона с сотней недостающих security-патчей; начинаем с apt full-upgrade и включения таймеров apt-daily
- ✕ **apt upgrade не обновляет ядро**
  Новое ядро — отдельный пакет: без метапакета linux-image-amd64 и планового ребута сервер годами живёт на уязвимом ядре при «чистом» apt
- ✕ **Drop-in sshd молча игнорируется**
  sshd берёт первое значение параметра: «поздний» drop-in проигрывает более раннему вроде 50-cloud-init.conf; используем префикс 00- и проверяем sshd -T
- ✕ **Отключили пароль — заперли себя**
  PasswordAuthentication no до проверки ключа отрезает доступ; меняем конфиг только со второй активной сессией и рабочим входом по ключу
- ✕ **fail2ban банит в пустоту**
  На Debian 13 ядро правил — nftables; старый banaction под iptables не попадает в живые цепочки; проверяем fail2ban-client status sshd и nft list rule…
- ✕ **Снапшот хостера считают бэкапом**
  Снапшот живёт рядом с VPS и гибнет вместе с аккаунтом или при шифровании; обязательна офсайт-копия в другом ЦОДе с отдельными ключами доступа
- ✕ **Мониторят сервер, но не бэкап**
  CPU и диск под контролем, а последний снапшот — месяц назад; добавляем в Zabbix метрику возраста снапшота restic с порогом 26 часов
- ✕ **Забытые сервисы наружу**
  Тестовая БД или панель, поднятая разработчиком «на минуту», слушает публичный IP; policy drop в nftables и регулярный внешний скан закрывают класс пр…

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- SSH: PermitRootLogin no, вход только по ключам, fail2ban на jail sshd
- nftables с policy drop: снаружи отвечают только реально нужные порты
- unattended-upgrades на security-репозиторий + ежемесячный ребут под ядро
- Ежедневный бэкап вне сервера с ротацией минимум 30 дней

НОРМАЛЬНО

- Доступ к SSH, 1С и БД только с белых IP или через WireGuard
- restic по схеме 3-2-1: почасовые снапшоты, офсайт S3, еженощный restic check
- Zabbix 7.0 LTS: метрики, systemd-юниты, SSL, возраст бэкапа, алерты в Telegram
- needrestart после патчей + еженедельный отчёт unattended-upgrades на почту

ХОРОШО

- Квартальные учения по восстановлению с замером RTO и письменным протоколом
- auditd + внешний syslog: журналы переживают компрометацию сервера
- Lynis hardening index 80+ как приёмочный критерий каждого сервера
- Паспорт сервера: эталон портов, версий и конфигов под контролем в git

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Root-вход по SSH запрещён и вход по паролю отключён на всех серверах (подтверждено выводом sshd -T)?
- [ ] Список открытых наружу портов снят с внешнего IP и совпадает с эталоном из паспорта сервера?
- [ ] Security-патчи ставятся автоматически, задержка от выхода бюллетеня — не больше суток?
- [ ] Ядро актуально: метапакет linux-image установлен, окно ребута реально исполняется?
- [ ] Есть офсайт-бэкап в другом ЦОДе, и последний тест восстановления датирован текущим кварталом?
- [ ] Мониторинг шлёт алерты в мессенджер, включая возраст последнего бэкапа и срок SSL-сертификатов?
- [ ] fail2ban активен, и его баны видны в действующих правилах nftables?
- [ ] Рейтинг Lynis по каждому серверу — 80+ и зафиксирован в отчёте аудита?
- [ ] Журналы SSH-входов и auditd уходят на внешний сборщик и хранятся не меньше 90 дней?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит Linux-серверов по 50 пунктам hardening: отчёт Lynis, карта открытых портов, оценка рисков
- Настройка под ключ: SSH, nftables, fail2ban, unattended-upgrades — один день на сервер
- Бэкап-контур restic с офсайт S3 и квартальными учениями по восстановлению
- Подключение к нашему Zabbix 7.0 LTS: алерты в Telegram, дежурный инженер, отчёты руководителю

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Debian 13 «trixie» — Release Notes и security-поддержка (debian.org — 13.6/2026)

02 Debian Wiki: UnattendedUpgrades (wiki.debian.org — 2026)

03 OpenSSH sshd_config(5) — параметры аутентификации (man.openbsd.org — 10.x)

04 nftables HOWTO (проект Netfilter) (wiki.nftables.org — 1.1)

05 fail2ban: jail.conf и nftables-actions (github.com/fail2ban — 1.1.0)

06 restic: политика forget/keep и проверка репозитория (restic.readthedocs.io — 0.19)

07 Zabbix 7.0 LTS Manual: Linux by Zabbix agent (zabbix.com — 7.0 LTS)

08 Lynis: hardening index и профили аудита (cisofy.com — 3.x)

Основано на официальной документации продуктов и нашей практике внедрения.