Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

LibreNMS: мониторинг сети по SNMP v3 — как мы внедряем

Разбор нашей методологии: LibreNMS 26.x, SNMPv3, авто-топология по LLDP/CDP, алерты в Telegram...

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У заказчика 20–150 коммутаторов, роутеров, точек доступа и ИБП в офисе и филиалах, а «мониторинг» — это пинг из таблицы. Мы закрываем слепую зону: LibreNMS опрашивает всё по SNMPv3 каждые 5 минут, строит карту связей, хранит графики загрузки портов и конфиги устройств в git. Без этого перегрев стойки, деградирующий SFP или петля живут неделями и всплывают уже как простой 1С, R...

Почему это важно бизнесу

- Час простоя сети офиса на 50 РМ — это остановка 1С, RDP, IP-телефонии и складского учёта одновременно
- Деградация канала (ошибки CRC, флаппинг порта) без графиков выглядит как «тормозит 1С» и месяцами ищется не там
- Утерянный конфиг коммутатора при выходе из строя = день восстановления вручную вместо 15 минут из git
- Тепловые аварии в серверных/котельных без датчиков температуры заканчиваются заменой оборудования
- SNMP v2c с community в открытом виде через туннели — готовый вектор для разведки сети злоумышленником

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

26.8.2

Актуальный релиз LibreNMS 26.x (месячные), PHP ≥ 8.4, MariaDB innodb_file_per_table=1 — ставим...

docs.librenms.org, Install

300 с

Шаг опроса poller (rrd.step); в dispatcher service_services_frequency 300, service_discovery_f...

docs.librenms.org, Dispatcher

SHA-256

Стандарт SNMPv3: authlevel=authPriv, authalgo SHA-256, cryptoalgo AES-256; для IOS 15 и Router...

наш стандарт

60 с

Fast Ping: schedule_type.ping dispatcher, service_ping_frequency 60, fping_options.timeout 500...

docs.librenms.org, Fast Ping

-w 1800

RRDCached: -w 1800 -z 1800 -f 3600 -t 4 -B -R -F, unix:/run/rrdcached.sock — снимает IOPS-штор...

docs.librenms.org, RRDCached

3600 с

Oxidized interval: конфиги снимаются ежечасно, коммит в git только при изменении; источник узл...

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Установка ядра и SNMPv3 на парке оборудования

Что настраиваем

Выделенная VM Debian 13 (4 vCPU / 8 ГБ / 120 ГБ SSD), все коммутаторы, роутеры, ИБП и Wi-Fi заказчика

Как мы это делаем

1. Ставим из git в /opt/librenms по официальной инструкции: nginx + php8.4-fpm (пул на /run/php-fpm-librenms.sock), MariaDB (innodb_file_per_table=1, lower_case_table_...
2. Вместо cron включаем dispatcher: /etc/systemd/system/librenms.service (или librenms-watchdog.service) + librenms-scheduler.timer; service_poller_workers подбираем п...
3. Профиль SNMPv3: lnms config:set snmp.v3.+ '{authlevel: authPriv, authalgo: SHA-256, cryptoalgo: AES-256}'; на устройствах отдельная RO-группа (Cisco: snmp-server gr...
4. Раскатываем SNMPv3, sysContact и sysLocation на парк плейбуком Ansible (ios_config / routeros), заодно выключаем v1/v2c community «public»
5. ./validate.php без красного — только после этого добавляем устройства: lnms device:add <ip> --v3 ... и проверяем poller-статус в Poller → Performance

РЕЗУЛЬТАТ

Через 2–3 часа после установки ядро опрашивает весь парк с 5-минутным шагом, RRD и eventlog наполняются, ни одна community-строка не ходит по сети в открытом виде. Дальнейшее добавление устройства — одна команда.

КЛЮЧЕВОЙ НЮАНС

Смотрим в Install-LibreNMS раздел про PHP-FPM пул и setfacl на rrd/logs/bootstrap/cache/storage: 80% «Permission denied» в логах — это забытые ACL, а не баг продукта.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Авто-топология, карта и алерты с подавлением шума

Что настраиваем

Все L2/L3-узлы с LLDP/CDP; правила алертов и транспорт Telegram для дежурного инженера

Как мы это делаем

1. На коммутаторах включаем LLDP (Cisco дополнительно CDP); в LibreNMS autodiscovery.xdp и autodiscovery.ospf включены по умолчанию, nets.+ ограничиваем сетями заказчи…
2. autodiscovery.bgp отключаем (lnms config:set autodiscovery.bgp false), чтобы discovery не тянул чужие AS через провайдерские пиринги; discovery_by_ip true при отсут…
3. Правила: devices.status != 1 (Critical, delay 5m), ports.ifOperStatus != 'up' AND ports.ifAlias ~ 'UPLINK' (Critical, delay 1m), processors.processor_usage >= 85 (W…
4. Транспорт Telegram (Alerts → Alert Transports: token бота, chat_id группы, формат Markdown), Recovery alerts включены, Max alerts = 1, Interval 30m — одно сообщение…
5. Карта: Overview → Maps → Network строится по xDP-соседям; для филиалов рисуем Custom Map с привязкой рёбер к uplink-портам — цвет ребра по загрузке (зелёный → жёлты…

РЕЗУЛЬТАТ

Инженер видит реальную схему связей, а не рисунок годовой давности; несимметричные каналы и петли находятся по карте. В Telegram приходит 3–8 сообщений в неделю по делу вместо сотен писем по каждому 30-секундному пропаданию пинга.

КЛЮЧЕВОЙ НЮАНС

Ключ к тишине — поле Delay в правиле: оно требует, чтобы условие держалось N минут до отправки. Без Delay любое правило по ifOperStatus превращается в спам при флаппинге порта.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Oxidized: git-история конфигов и эксплуатационный контур

Что настраиваем

Все управляемые устройства с CLI (Cisco IOS, MikroTik RouterOS, HP/Aruba); AD заказчика для входа инженеров

Как мы это делаем

1. Oxidized как отдельный systemd-сервис под пользователем oxidized; source: http на https://nms.<домен>/api/v0/oxidized с заголовком X-Auth-Token (API-токен LibreNMS)…
2. output: git (repo на отдельном томе), interval: 3600; в LibreNMS: oxidized.enabled true, oxidized.url http://127.0.0.1:8888, oxidized.features.versioning true, oxid…
3. enable_syslog true + rsyslog imudp → syslog.php; на Cisco logging trap informational; enable_syslog_hooks true и os.ios.syslog_hook (regex CONFIG_I → syslog-notify-…
4. auth_mechanism active_directory: auth_ad_url ldaps://dc01, auth_ad_binduser, auth_ad_require_groupmembership 1, auth_ad_groups.NMS-Admins.roles ["admin"], NMS-Reade…
5. Регламент: validate.php ежедневно в cron с алертом при ошибках, mysqldump librenms + tar rrd/ и .env в бэкап, ретенция syslog_purge 30, eventlog_purge 30, alert_log…

РЕЗУЛЬТАТ

Каждое изменение конфига видно как diff во вкладке Config устройства с датой и автором; восстановление коммутатора после замены — 15 минут копипастом из git. Инженеры входят доменными учётками, ротация доступа — через группу AD.

КЛЮЧЕВОЙ НЮАНС

LibreNMS сам отдаёт Oxidized имя модели по своему os, поэтому model_map в Oxidized не нужен; для нестандартных прошивок переопределяем через oxidized.maps.os (match → value), иначе бэкап молча пропускает узел.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **SNMP v2c ради «быстрее поставить»**
  Community уходит по сети открыто через все туннели. Сразу закладываем v3 authPriv, v2c — только временно на устройствах без поддержки, отдельной ACL...

- ✕ **Cron-поллер вместо dispatcher**
  При 150+ устройствах poller-wrapper не укладывается в 5 минут, графики рвутся. Ставим librenms.service (dispatcher) и подбираем service_poller_worker...

- ✕ **RRD прямо на диск без rrdcached**
  Каждые 5 минут тысячи мелких записей — IOPS-шторм и рост latency VM. Обязательно rrdcached -w 1800 -z 1800 -f 3600 -t 4 -B -R -F, RRD-каталог на SSD

- ✕ **Правила без Delay и Max alerts**
  Флаппинг одного порта даёт сотни сообщений. Delay 1–15 мин по типу события, Max alerts 1, Interval 30 мин, Recovery включён — шум уходит

- ✕ **Discovery по всем сетям и BGP**
  autodiscovery.bgp по умолчанию включён и тянет провайдерские пиры. Ограничиваем nets.+, добавляем autodiscovery.nets-exclude, BGP-обход отключаем

- ✕ **Локальный логин librenms без AD**
  Уволенный админ уносит общий пароль. Подключаем auth_mechanism active_directory через ldaps с bind-учёткой и группами NMS-Admins/NMS-Readers → роли

- ✕ **Oxidized без реестра устройств**
  Ручной список узлов расходится с NMS через месяц. Источник — только API /api/v0/oxidized плюс oxidized.reload_nodes true

- ✕ **Network Weathermap из старых гайдов**
  Плагин не работает ни на одной поддерживаемой версии PHP и открыт без авторизации — документация прямо запрещает. Используем встроенные Custom Maps

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- LibreNMS 26.x на отдельной VM, SNMPv3 authPriv на всех управляемых устройствах
- Правила Device Down / Uplink Down / CPU / Temperature с Delay, транспорт Telegram
- LLDP/CDP включены, discovery ограничен сетями заказчика (nets, nets-exclude)
- validate.php в cron ежедневно, mysqldump + rrd в общий бэкап

НОРМАЛЬНО

- Dispatcher-сервис и rrdcached вместо cron, Fast Ping через dispatcher раз в 60 с
- Oxidized по API LibreNMS, git-история конфигов, вкладка Config с diff
- Syslog от устройств в LibreNMS, ретенция 30 дней, eventlog по трапам linkDown/linkUp
- Вход инженеров через Active Directory (ldaps, роли admin / global-read по группам)

ХОРОШО

- Distributed poller в каждом филиале (poller group, общий Redis/RRDCached/DB)
- Custom Maps по площадкам с раскраской uplink по загрузке, порог 80% в правиле
- Syslog-хуки: событие «config changed» → внеплановый снимок в Oxidized
- Ежемесячный отчёт: топ-10 портов по загрузке/ошибкам, топ по температуре, SLA доступ…

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Все коммутаторы и роутеры опрашиваются по SNMPv3 authPriv, community v1/v2c удалены?
- [ ] Ядро работает через dispatcher (librenms.service) и rrdcached, а не через cron с прямой записью RRD?
- [ ] Есть правило Device Down с Delay ≥ 5 мин и правило на uplink-порты с Delay 1 мин?
- [ ] Алерты приходят дежурному в Telegram и там же приходит Recovery, а не только в почту?
- [ ] Карта связей построена по LLDP/CDP и на ней нет «висящих» узлов без соседей?
- [ ] Датчики температуры серверных и шкафов в филиалах видны в Sensors и имеют порог?
- [ ] Конфиги всех устройств лежат в git Oxidized и обновляются не реже раза в час?
- [ ] Вход в LibreNMS — доменными учётками через AD, локальный админ отключён или со сложным паролем?
- [ ] validate.php ежедневно зелёный, а БД и каталог rrd попадают в общий бэкап?
- [ ] Есть регламент: кто и за сколько минут реагирует на Critical, где лежит Procedure URL правила?

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).

- Разворачиваем LibreNMS 26.x под ключ: VM, dispatcher, rrdcached, SNMPv3 на всём парке через Ansible
- Настраиваем правила алертов с подавлением шума и транспорт в Telegram/почту дежурного
- Поднимаем Oxidized с git-историей конфигов и вкладкой diff прямо в карточке устройства
- Подключаем филиалы: IPsec/WireGuard до площадок, distributed poller там, где устройств много
- Сопровождаем: ежемесячный отчёт по загрузке и ошибкам портов, обновления LibreNMS, ревизия правил

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 Install LibreNMS: PHP ≥ 8.4, PHP-FPM, MariaDB, scheduler (docs.librenms.org — 26.8)

02 Dispatcher Service: воркеры и частоты опроса (docs.librenms.org — 26.8)

03 Auto-Discovery: xdp / ospf / bgp, nets, nets-exclude (docs.librenms.org — 26.8)

04 Alerting Rules / Transports, Fast Ping (docs.librenms.org — 26.8)

05 RRDCached и Distributed Poller (Redis, poller groups) (docs.librenms.org — 26.8)

06 Oxidized, Syslog hooks, Cleanup, Custom Maps (docs.librenms.org — 26.8)

07 Authentication: Active Directory (ldaps, auth_ad_groups.*.roles) (docs.librenms.org — 26.8)

08 Шаблон ITfresh: правила алертов и плейбук SNMPv3 (Ansible) (наш стандарт — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.