Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

LibreNMS: SNMP-мониторинг сети малого офиса

Автообнаружение свитчей, роутеров, принтеров и NAS с алертом о перегрузке канала

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В офисах до 50 PM сеть обычно живёт без наблюдения: свитч тихо теряет порт, принтер уходит в ошибку, NAS забивает диск, канал в интернет упирается в потолок в пик нагрузки 1С/CRM/почты. О проблеме узнают из жалоб, когда простой уже идёт. Мы разворачиваем LibreNMS как точку SNMP-мониторинга: автообнаружение, графики утилизации, алерты раньше, чем деградацию заметит бизнес.

Почему это важно бизнесу

- Простой канала в рабочие часы останавливает 1С, CRM и почту у всех сотрудников одновременно, а не у одного PM
- Тихий отказ порта свитча или блока питания обнаруживается постфактум, когда уже потеряны часы работы отдела
- Забитый диск NAS без предупреждения останавливает резервное копирование и файловые шары бухгалтерии
- Перегрев/переполнение тонера принтера в приёмной или на производстве простаивает без единой точки контроля
- Без графиков утилизации канала невозможно обосновать апгрейд тарифа провайдера цифрами, а не ощущениями

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

25.x/26.x

актуальная ветка LibreNMS (CalVer), которую разворачиваем; автообновление через daily.sh из cr…

LibreNMS docs

300 с

интервал опроса poller (service_poller_frequency) — стандарт для парка до ~200 устройств

LibreNMS docs

80%

порог алерта по утилизации порта (macros.port_usage_perc) — сигнал о перегрузке канала

наш стандарт

90%

порог CPU/памяти узла (processors.processor_usage, mempools.mempool_perc)

LibreNMS docs

75%

порог заполнения раздела storage.storage_perc на NAS и файл-серверах

LibreNMS docs

1000+

устройств на один poller до того, как включать Distributed Polling

LibreNMS docs

РЕАЛИЗАЦИЯ 1 ИЗ 3

Автообнаружение парка: свитчи, роутеры, МФУ, NAS

Что настраиваем

Площадка до 50 РМ: L2/L3-свитчи, пограничный роутер, точки доступа, МФУ/принтеры, NAS — один инстанс LibreNMS

Как мы это делаем

1. Заводим SNMP-профиль: lnms config:set snmp.community.+ <строка> для v2c или snmp.v3.+ с authPriv для критичных узлов
2. Добавляем один опорный узел вручную, затем задаём диапазон scan-подсетей в Settings → Network Discovery
3. Включаем discovery_modules.arp-table и discovery_modules.discovery-arp для автодобавления соседей по ARP, discovery_modules.discovery-protocols — по CDP/LLDP/xDP
4. Прогоняем ./scripts/snmp-scan.py по офисным /24 для точечного поиска SNMP-хостов вне ARP-таблиц пограничного роутера
5. Регистрируем /etc/cron.d/librenms: poller-wrapper.py и discovery-wrapper.py запускают poller.php/discovery.php на интервале 300 с

РЕЗУЛЬТАТ

Через один проход дискавери в реестре LibreNMS оказывается весь SNMP-парк офиса без ручного ввода IP; новый свитч или NAS подхватывается на следующем цикле дискавери без нашего участия.

КЛЮЧЕВОЙ НЮАНС

Discovery работает только от уже добавленных узлов и заданных подсетей — если забыть указать scan-диапазон, автообнаружение молча ничего не найдёт.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Алертинг по каналу и деградации оборудования

Что настраиваем

Все обнаруженные устройства: правила на утилизацию портов, память/CPU, диск, статус устройства

Как мы это делаем

1. Собираем правило в Alert Rule Builder: macros.port_usage_perc >= 80 для магистральных и WAN-портов
2. Правило на storage.storage_perc >= 75 для разделов NAS и файл-серверов, mempools.mempool_perc >= 90 для сетевых узлов
3. Правило devices.status != 1 с задержкой на 2 неудачных опроса — фильтруем ложные срабатывания на нестабильном Wi-Fi-канале
4. Настраиваем Telegram-transport (chat_id + bot token) в Global Settings → Alerting Settings, привязываем к правилам
5. Пишем Blade-шаблон алерта под правило: устройство, порт, текущее значение, ссылка на граф — без общего шаблона по умолчанию

РЕЗУЛЬТАТ

Ответственный инженер получает алерт в Telegram в момент, когда утилизация канала или диска пересекает порог, а не когда пользователи уже не могут работать — время реакции сокращается с часов до минут.

КЛЮЧЕВОЙ НЮАНС

Один общий Telegram-transport на все правила размывает приоритет — критичные (канал, диск) и информационные (флаппинг порта) алерты разводим по разным шаблонам и transport-целям.

РЕАЛИЗАЦИЯ 3 ИЗ 3

SNMPv3 и рост парка сверх одного poller

Что настраиваем

Переход с v2c community на authPriv для управляемых свитчей/роутеров + подготовка к масштабированию

Как мы это делаем

1. На управляемом сетевом оборудовании создаём SNMPv3-пользователя: createUser monitor SHA <auth-pass> AES <priv-pass>
2. В LibreNMS заводим snmp.v3.+ с authlevel authPriv, authalgo SHA, cryptoalgo AES — community v2c оставляем только на легаси-принтерах
3. Ограничиваем ACL источника SNMP-запросов на устройстве адресом poller-сервера, закрываем 161/UDP на периметре
4. При превышении ориентира по нагрузке заводим Poller Group в Settings → Poller → Groups и Dispatcher Service на несколько воркеров
5. Настраиваем systemd-юнит librenms-service вместо cron при переходе на 1-минутный опрос ключевых магистральных портов

РЕЗУЛЬТАТ

Критичные узлы опрашиваются по зашифрованному authPriv, а не по community-строке в открытом UDP; при росте парка выше пропускной способности одного poller опрос не деградирует, а масштабируется группами.

КЛЮЧЕВОЙ НЮАНС

authNoPriv шифрует только аутентификацию, но не сами OID — для управляемых свитчей и роутеров берём только authPriv, иначе SNMP-трафик читаем в открытую.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Community-строка вместо пароля**
  Публичную community v2c держат годами без ротации — это не секрет доступа, а публичный ключ; ограничиваем ACL по IP poller, ставим кастомную строку.

- **Discovery без scan-диапазона**
  Забыли задать подсети в Network Discovery — автообнаружение работает только от ARP/CDP/LLDP соседей уже добавленных узлов и новые сегменты не увидит.

- **Один Telegram-чат на все алерты**
  Критичный алерт по каналу тонет в потоке информационных флаппингов порта; разводим правила по отдельным transport-целям и приоритету шаблона.

- **Порог 80% без учёта пиковой нагрузки**
  Единый порог утилизации порта для магистрали и рабочей станции даёт шум или пропуск перегрузки; считаем порог отдельно на WAN и на access-портах.

- **authNoPriv на управляемом оборудовании**
  Аутентификация защищена, но сами счётчики и конфигурация идут открытым текстом; для свитчей/роутеров ставим только authPriv с AES.

- **Poller на 300 с для аварийных портов**
  Стандартный интервал 300 с не ловит кратковременные пики и флаппинг; для магистральных портов включаем 1-Minute Polling выборочно, а не глобально.

- **RRD-данные без ротации диска**
  RRDtool пишет файлы фиксированного размера на каждый счётчик порта — на парке в сотни устройств место на диске считаем заранее, не по факту.

- **Обновление LibreNMS без backup БД**
  daily.sh тянет миграции схемы автоматически; перед мажорным обновлением ветки снимаем дамп MariaDB и снапшот /opt/librenms, иначе откат невозможен.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- LibreNMS на одном сервере, SNMP v2c с кастомной community, ACL по IP poller
- Discovery по заданным офисным подсетям, poller раз в 300 с через cron
- 3-4 алерт-правила: канал 80%, диск 75%, память 90%, статус устройства

НОРМАЛЬНО

- SNMPv3 authPriv на всём управляемом сетевом оборудовании, v2c только на легаси
- Telegram-transport с раздельными шаблонами по приоритету алерта
- Device Sensors для UPS/температуры/тонера принтеров, отдельные правила на них
- Регулярный дамп MariaDB и снапшот конфигурации перед обновлением веток

ХОРОШО

- Poller Groups и Dispatcher Service с несколькими воркерами на растущем парке
- 1-Minute Polling выборочно на магистральных WAN/аплинк-портах
- Distributed Polling при выходе за ориентир 1000+ устройств на один сервер
- Отдельные Blade-шаблоны и эскалация transport по уровню критичности узла

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] SNMP community/v3-пользователь заведены отдельно от паролей администратора устройств?
- [ ] Диапазон подсетей для автообнаружения задан и покрывает все офисные VLAN?
- [ ] На управляемых свитчах и роутерах включён SNMPv3 authPriv, а не community v2c?
- [ ] Есть алерт-правило на утилизацию канала (macros.port_usage_perc) отдельно для WAN и access?
- [ ] Настроены пороги на диск NAS (storage_perc) и память/CPU сетевых узлов?
- [ ] Telegram/email-transport проверен тестовым алертом, а не только сохранён в настройках?
- [ ] ACL на 161/UDP ограничивает источники SNMP-запросов адресом poller-сервера?
- [ ] Есть регламент бэкапа MariaDB и /opt/librenms перед обновлением версии?
- [ ] Poller укладывается в интервал 300 с без просроченных (overdue) устройств?
- [ ] Device Sensors подключены для UPS/принтеров там, где это критично для бизнеса?

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 под ключ: сервер/Docker, SNMP-профили, автообнаружение офисных подсетей
- Настраиваем алерт-правила и Telegram/email-оповещения под приоритеты конкретного офиса
- Переводим сетевое оборудование на SNMPv3 authPriv и закрываем SNMP по ACL на периметре
- Подключаем Device Sensors для принтеров, UPS и NAS с индивидуальными порогами
- Сопровождаем обновления веток, бэкап БД и масштабирование через Poller Groups при росте парка

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 Installing LibreNMS (docs.librenms.org — 2026)

02 Auto-discovery Setup (docs.librenms.org — 2026)

03 Alerting: Rules (docs.librenms.org — 2026)

04 Alerting: Templates (docs.librenms.org — 2026)

05 Alerting: Telegram Transport (docs.librenms.org — 2026)

06 Dispatcher Service / Distributed Polling (docs.librenms.org — 2026)

07 SNMP Configuration Examples (docs.librenms.org — 2026)

08 Device Sensors (docs.librenms.org — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.