Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

OpenSearch вместо Elasticsearch для офисных логов

Форк под Apache 2.0 для клиентов до 50 PM: SIEM, алерты и хранение логов без подписки X-Pack

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Клиентам до 50 РМ нужен централизованный сбор и поиск по логам (AD, Sysmon, 1С, nginx, файрвол, БД), но Elasticsearch с 7.11 ушёл под SSPL/Elastic License 2.0: платная подписка X-Pack за SIEM/алерты/reporting и недоступность в РФ после 2022. Ставим OpenSearch — форк ES 7.10 под Apache 2.0, где Security, Alerting и Anomaly Detection бесплатны, а данные на своём железе.

Почему это важно бизнесу

- Лицензионные риски: ES с 7.11 под SSPL/Elastic License 2.0 несовместимы с Open Source; OpenSearch навсегда под Apache 2.0
- Стоимость: платные функции X-Pack (SIEM, алерты, reporting) в OpenSearch бесплатны — нет подписки на каждый узел
- Суверенность логов: данные и стек живут на российских VPS, без экспорта в чужой managed-сервис и валютных платежей
- Доступность в РФ: купить Elastic-подписку после 2022 практически нельзя; OpenSearch ставится и обновляется без ограничений
- Паритет для SMB: OpenSearch = ES 7.10 по API плюс бесплатные Security, Alerting и Anomaly Detection

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2.19

актуальная стабильная ветка OpenSearch 2.x (параллельно развивается линейка 3.x)

docs.opensearch.org

Apache 2.0

лицензия OpenSearch (форк ES 7.10); Elasticsearch с 7.11 — под SSPL/Elastic License 2.0

opensearch.org/faq

50%

доля RAM под JVM-heap; -Xms = -Xmx, потолок 32 ГБ (сжатые указатели OOP)

наш стандарт + docs

10-50 ГБ

рекомендуемый размер шарда 10-50 ГБ; rollover min_size 50 ГБ для лог-нагрузки

docs.opensearch.org

5 мин

интервал ISM-job по умолчанию (plugins.index_state_management.job_interva

docs.opensearch.org

180 дней

наш стандарт ретенции: hot 90 дней NVMe + cold через ISM, снапшоты каждые 6 ч

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 2

Однонодовый стек для транспортной компании 45 PM

Что настраиваем

45 сотрудников, 8 серверов (3 Windows AD/1C/файлы + 5 Linux веб/1C/мониторинг), single-node кластер

Как мы это делаем

1. VPS-1: 8 vCPU / 24 ГБ RAM / 500 ГБ NVMe, роли cluster_manager+data+ingest, heap 12 ГБ (-Xms=-Xmx)
2. Fluent Bit на каждом Linux-хосте; на Windows — Beats с редиректом в OpenSearch, исключение в Defender через GPO
3. ISM-policy: hot 90 дней на NVMe → cold на VPS-2 (2 vCPU / 4 ГБ / 2 ТБ HDD), delete по ретенции
4. OpenSearch Dashboards на VPS-1 за nginx (Basic Auth + VPN), снапшоты в S3 каждые 6 часов
5. 3 дашборда: Безопасность (4625 по часам), Здоровье 1C (запросы >5 с), Инфраструктура (CPU/RAM/диск)

РЕЗУЛЬТАТ

За 48 часов после запуска нашли брутфорс по событиям 4625 на контроллере домена с PM бухгалтерии (старый принтер с прошитым 4-летним паролем), запрос 1С «Остатки склада» на 40 с из-за отсутствия индекса и 3-4 тыс/сут сканов ботов на внутренний портал, торчавший наружу. Всё закрыто сразу.

КЛЮЧЕВОЙ НЮАНС

Single-node без реплики теряет данные при перезагрузке VPS — обязательны снапшоты в S3 (у нас каждые 6 ч) и ISM с ролловером. Multi-node для 45 PM не нужен: hardware overhead не оправдан.

РЕАЛИЗАЦИЯ 2 ИЗ 2

Тюнинг heap и ISM: убираем тормоза и переполнение диска

Что настраиваем

типовой SMB-клиент, ~4 ГБ логов/день, индексы Windows Event/Sysmon/1С ТЖ/nginx/pfSense/PostgreSQL

Как мы это делаем

1. Дефолтный heap 1 ГБ → выставили 50% RAM (12 ГБ на 24 ГБ VPS), -Xms=-Xmx, потолок 32 ГБ
2. Шарды держим 10-50 ГБ: ISM rollover по min_size 50 ГБ + min_index_age, чтобы не плодить мелкие шарды
3. Ретенция 180 дней вместо первичных 30: hot-фаза 90 дней, затем cold-tier через ISM
4. Security plugin: RBAC по индексам, вход через AD/LDAP, TLS на transport и REST

РЕЗУЛЬТАТ

После heap 1→12 ГБ ушли паузы GC и тормоза дашбордов. Ролловер по 50 ГБ убрал деградацию от тысяч мелких шардов и раздувание cluster state. ISM автоматически двигает индексы hot→cold и удаляет по ретенции — диск VPS-1 больше не переполняется, ручной ротации нет.

КЛЮЧЕВОЙ НЮАНС

Три параметра решают 90% проблем single-node: heap = 50% RAM (Xms=Xmx), размер шарда 10-50 ГБ через rollover и ISM job_interval с явной ретенцией. Дефолты OpenSearch под лог-нагрузку не заточены.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Heap по умолчанию 1 ГБ**
  Java-heap стартует с 1 ГБ — мало для лог-нагрузки. Ставим 50% RAM, -Xms=-Xmx, но не выше 32 ГБ (сжатые указатели OOP).

- ✕ **Шарды не по 10-50 ГБ**
  Тысячи мелких шардов жрут heap и cluster state. Rollover по min_size 50 ГБ и min_index_age держит размер в норме.

- ✕ **ISM-ретенция наугад**
  Первая policy удаляла индексы на 30 дней, юрист потребовал 180. Ретенцию согласуем ДО настройки ISM, а не после инцидента.

- ✕ **Single-node без снапшотов**
  Один узел без реплики теряет индексацию при ребуте VPS. Обязательны снапшоты в S3 по расписанию (у нас каждые 6 ч).

- ✕ **Beats/Fluent Bit под Defender**
  Defender на Windows блокирует процесс агента сбора. Добавляем в исключения через GPO, иначе логи молча не идут.

- ✕ **Dashboards наружу без защиты**
  Веб-интерфейс нельзя светить в интернет. Только за nginx с Basic Auth и VPN; Security plugin — RBAC и TLS.

- ✕ **Путают с Zabbix/Prometheus**
  OpenSearch — хранилище и поиск по сырым логам, не метрики по порогам. Ставим ДОПОЛНИТЕЛЬНО к Zabbix, не вместо.

- ✕ **Свежий Elasticsearch «как раньше»**
  ES с 7.11 под SSPL/Elastic License 2.0 — платно и в РФ недоступно. Берём OpenSearch под Apache 2.0.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- OpenSearch 2.19 single-node: роли cluster_manager+data+ingest на одной VPS
- Heap = 50% RAM, -Xms=-Xmx, не выше 32 ГБ; дефолт 1 ГБ не оставлять
- ISM с явной ретенцией и rollover; Dashboards за nginx + Basic Auth + VPN

НОРМАЛЬНО

- Fluent Bit на Linux, Beats на Windows (исключение агента в Defender через GPO)
- Security plugin: TLS transport+REST, RBAC по индексам, вход через AD/LDAP
- Cold-tier на отдельной VPS (HDD) + снапшоты в S3 каждые 6 часов
- Alerting-плагин: правила в Telegram (брутфорс 4625, ошибки 1С, диск)

ХОРОШО

- Ретенция 180 дней: hot 90 дней NVMe → cold через ISM, шарды 10-50 ГБ
- Anomaly Detection на ключевых индексах (логины, ошибки БД)
- 3 дашборда руководству: Безопасность, Здоровье 1С, Инфраструктура
- Квартальные обновления OpenSearch/Dashboards, тест restore из S3

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Зафиксировать ретенцию логов с юристом/ИБ ДО настройки ISM (наш стандарт — 180 дней)
- [ ] Heap = 50% RAM, -Xms=-Xmx, потолок 32 ГБ; проверить в jvm.options
- [ ] ISM-policy: rollover min_size 50 ГБ, переход hot→cold, delete по ретенции
- [ ] Fluent Bit на Linux-хостах, Beats на Windows + исключение агента в Defender (GPO)
- [ ] Security plugin: TLS на transport и REST, сменить дефолтные пароли демо-пользователей
- [ ] RBAC по индексам, интеграция аутентификации с AD/LDAP
- [ ] Снапшоты в S3-репозиторий по расписанию (каждые 6 часов) + тест восстановления
- [ ] Dashboards только за nginx (Basic Auth) и VPN, наружу не публиковать
- [ ] Alerting-правила в Telegram: брутфорс 4625, ошибки 1С, свободное место на диске
- [ ] Контроль размера шардов и cluster state, отсутствие россыпи мелких шардов

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).

- Проектируем и разворачиваем OpenSearch 2.19 + Dashboards под ключ за 4-5 дней, без лицензий и подписок
- Настраиваем сбор с Windows Event/Sysmon, 1С ТЖ, nginx, pfSense/Mikrotik, PostgreSQL/MSSQL
- Пишем ISM-политики ретенции, heap/shard-тюнинг и снапшоты в S3 под ваш парк
- Собираем дашборды для директора и админа, алерты в Telegram, ведём на абонентке
- Бесплатный тестовый OpenSearch на 7 дней с аудитом логов по Москве и МО

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 OpenSearch Documentation — Index State Management (ISM) (docs.opensearch.org — 2026)

02 OpenSearch Documentation — Tuning your cluster / node roles (docs.opensearch.org — 2026)

03 OpenSearch — JVM heap sizing (install and configure) (docs.opensearch.org — 2026)

04 OpenSearch Documentation — Sizing shards / cluster sizing (docs.opensearch.org — 2026)

05 OpenSearch FAQ — лицензия Apache 2.0, форк ES 7.10 (opensearch.org — 2026)

06 OpenSearch Security plugin — TLS, RBAC, AD/LDAP/SAML (docs.opensearch.org — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.