

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**Лабораторная работа № 9**

на тему «DevOps.»

Выполнил обучающийся гр. ВКБ42

Ковалев Д. П.

Проверил:

Доцент Куликова О.В.

Доцент Скляров А.В.

Ростов-на-Дону

2025

**Цель**: приобрести знания о методологии DevOps и получить практические навыки в применении методологии в различных условиях.

**Задание 1**. Есть сервис, где периодически что-то происходит, из-за чего он медленнее обрабатывает запросы пользователей. Нужно посмотреть логи. Важно уметь искать в логах нужное событие. Быстро ориентироваться в бесконечно больших лог-файлах, при этом не нагружая диск при открытии.

Для решения представленной выше задачи можно использовать приведенные ниже инструменты и методы:

**1. Использовать потоковую обработку логов.**

Вместо загрузки и анализа больших лог-файлов целиком, следует читать и обрабатывать логи потоками.

Утилиты командной строки:

* **grep для поиска по шаблонам:** позволяет быстро находить нужные строки в логах;
* **tail для работы с последними строками:** используется для чтения логов в режиме реального времени;
* **awk для извлечения конкретных данных:** если нужно анализировать только определенные поля (например, timestamp или статус ответа);
* **less для просмотра логов без загрузки их в память:** работает эффективно даже с очень большими файлами.

Обоснованием эффективности данных утилит является то, что:

* Логи обрабатываются построчно, что минимизирует использование памяти и снижает нагрузку на диск.
* Нет необходимости загружать весь файл в редактор.

**2. Централизация логов с помощью системы логирования.**

Использование системы сбора и анализа логов помогает быстрее находить нужные события и визуализировать метрики.

Одной из таких систем является стек ELK (Logstash, Elasticsearch, Kibana) — это современное решение для управления журналами и аналитики, которое позволяет инженерам преодолевать трудности мониторинга высоко распределенных, динамических и шумных сред. Это мощная платформа, которая собирает и обрабатывает данные из нескольких источников, сохраняет их в одном централизованном хранилище, которое может масштабироваться по мере роста данных, и предоставляет набор инструментов для анализа собранной информации.

В состав ELK-стека входят следующие утилиты:

* **Elasticsearch:** хранит логи в оптимизированной базе данных.
* **Logstash:** обрабатывает логи, фильтрует события, добавляет теги и пересылает их в Elasticsearch.
* **Kibana:** предоставляет веб-интерфейс для анализа и визуализации.

Эффективность данного метода объясняется тем, что:

* Логи индексируются, что ускоряет поиск даже в больших объемах.
* Удобный интерфейс для фильтрации и визуализации данных (например, построение графиков времени отклика).
* Позволяет задавать алерты для автоматического уведомления о проблемах.

Grafana Loki — это распределенная система журналирования и мониторинга, разработанная компанией Grafana Labs. Она предназначена для эффективного сбора, индексации и анализа журналов приложений и систем. Loki использует подход, основанный на метках (labels), вместо традиционных индексов, что делает её особенно эффективной для обработки больших объемов данных.

**3. Использовать облачные решения для обработки логов.**

Если объем логов очень большой или требуется анализ распределенной системы, можно использовать облачные решения.

Одними из программных продуктов, которые могут быть использованы для этого, являются:

* **Cloud Logging VK** — это удобный облачный сервис для сбора и анализа логов в облаке. Он позволяет хранить и обрабатывать логи приложений и сервисов в едином интерфейсе, что помогает следить за стабильной работой всей системы. Его преимуществами являются:
* **Оперативные данные**. Доступ к логам всех приложений или сервисов в режиме реального времени.
* **Удобный поиск**. можно искать, просматривать и анализировать логи при помощи текстового поиска с дополнительными фильтрами.
* **Гибкие настройки**. можно настроить сервис под свои задачи с помощью API на чтение и сбор логов. Например, установить время хранения логов, настроить роли для работы с логами.
* **Доступность и надежность**. VK Cloud обеспечивают работоспособность и отказоустойчивость сервиса и гарантируют его доступность по SLA.
* **Безопасность**. все данные надежно защищены: логи каждой группы приложений хранятся изолированно в облаке. ЦОДы уровня Tier III расположены в России.
* **Yandex Cloud Logging.** Сервис Cloud Logging позволяет читать, записывать и безопасно хранить логи пользовательских приложений и ресурсов Yandex.Cloud, объединяя сообщения в группы. Работа осуществляется при помощи консоли управления или через интерфейс командной строки. Сервис является частью общей экосистемы Yandex.Cloud и основан на serverless-технологиях и подходах. Также Cloud Logging облегчает отладку приложений и инфраструктуры пользователя и ускоряет поиск по логам облачных ресурсов. Его преимущества:
* **Cloud Logging** агрегирует данные о работе сервисов и приложений в различные лог-группы: по умолчанию и пользовательская.
* С помощью сервиса можно фильтровать и искать записи, используя логические операторы и поиск по параметрам, в том числе в формате JSON.
* **Cloud Logging** обеспечивает безопасное хранение данных: сервис собирает, обрабатывает и хранит логи изолированно для каждой группы. Максимальное время хранения записей на стадии Preview — 7 дней, минимальное — 1 час.

**4. Настройка метрик и алертов.**

Метрики помогают отслеживать производительность, а алерты предупреждают о сбоях, позволяя оперативно реагировать.

* Сбор метрик: Системы вроде Prometheus или Zabbix собирают данные о производительности (например, загрузка CPU, время ответа) с помощью агентов или экспортёров.
* Анализ данных: Данные хранятся в базе и анализируются на предмет отклонений (например, превышение времени ответа или рост ошибок 5xx).
* Настройка алертов: создаются правила, которые срабатывают при достижении определённых порогов. Например, если время ответа > 500 мс, отправляется уведомление.
* Уведомления: Система интегрируется с мессенджерами (Telegram, Slack) или почтой для автоматического оповещения о проблемах.

Проведем сравнительный анализ перечисленных методов, для выявления их преимуществ и недостатков. Данные данные позволят определить подходят ли данные методы для решения проблем в рассматриваемом сервисе.

|  |  |  |  |
| --- | --- | --- | --- |
| **Метод** | **Когда применять** | **Плюсы** | **Минусы** |
| **Потоковая обработка логов** | Если лог-файлы расположены локально, и требуется быстрая ручная диагностика | Простота реализации. Низкая нагрузка. Минимум зависимостей | Сложно анализировать большой объем логов или искать комплексные шаблоны |
| **Централизация логов (ELK/Loki)** | Когда логи масштабируются (много сервисов) и требуется постоянный мониторинг | Автоматизация. Быстрый поиск и индексация. Визуализация данных | Требует настройки инфраструктур. Может быть дорогостоящим для больших объемов логов |
| **Облачные решения (VK Cloud Logging)** | Если инфраструктура работает в облаке, и необходим анализ распределенных логов | Масштабируемость. Автоматизация и алерты. Поддержка множества источников | Зависимость от провайдера. Стоимость хранения и запросов |
| **Автоматизация анализа (скрипты)** | Если требуется регулярный поиск специфических шаблонов или автоматизация анализа | Гибкость. Можно интегрировать в CI/CD | Требует разработки и поддержки скриптов |
| **Мониторинг метрик и алертов** | Если нужно заранее предотвращать проблемы (например, мониторить задержки или ошибки) | Реагирование в реальном времени. Интеграция с мониторингом (Prometheus, Grafana) | Требуется предварительная настройка и дополнительные ресурсы |

Подводя итоги, можно сказать, что наиболее универсальным и долгосрочным решением будет централизация логов (ELK или Loki), поскольку она позволяет:

* Обрабатывать огромные объемы логов.
* Ускорять поиск через индексацию.
* Настраивать автоматические фильтры, графики и алерты.

Таким образом, если время и ресурсы позволяют, то **централизация логов** является стратегически наиболее выгодным методом.

**Задание 2**. Необходимо нарисовать график существующей инфраструктуры ПО. Периодически клиент такое тоже может попросить сделать, например, когда проходит аудит, и регуляторы в сфере деятельности компании/проекта требуют определённой отчётности об организации инфраструктуры, данных, и прочего. Популярный инструмент для рисования графиков и блок-схем.

Для реализации ИТ инфраструктуры было выбрано некоторое предприятие занимающиеся бухгалтерским учётом расположенное в Ростове-На-Дону.

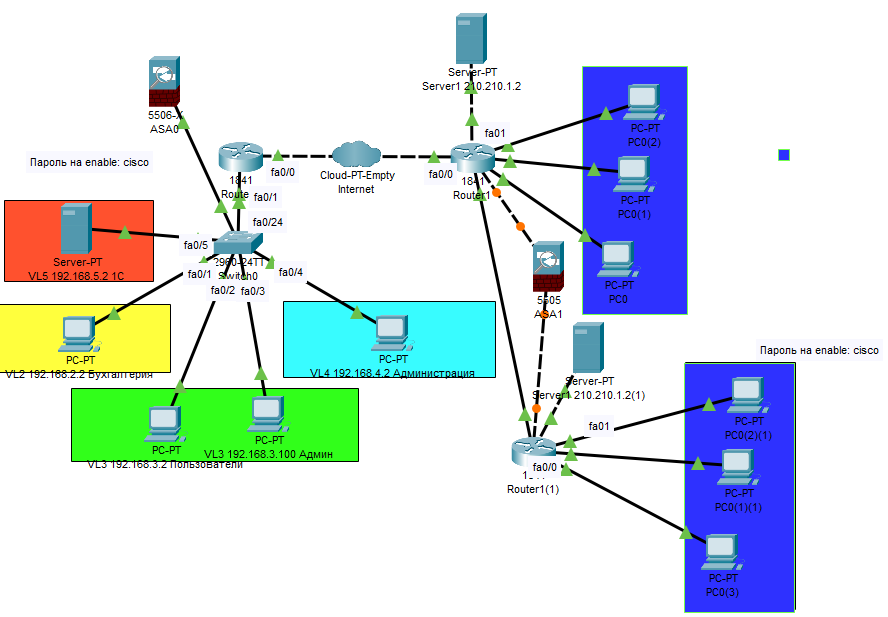


Рисунок 1 – Схема ИТ инфраструктуры

На рисунке представлена схема этой ИТ инфраструктуры с подробным описанием всех отделов включая главный офис и удалённый филиал.

**Задание 3.** Сделать анализ облачных провайдеров и выбрать подходящий под определённые требования. Например: клиент расположен в Канаде, гос регулятор выдвигает требования, что данные пользователей должны храниться только в Канаде, соответственно, сразу отпадает перечень провайдеров, которые расположены вне требуемой зоны. Важно провести глубокую аналитику всех канадских провайдеров, их перечня услуг, готовых решений, цен и так далее. Также важно смотреть на количество локаций дата центров, реальных отзывов и множество других переменных.

Для анализа облачных провайдеров было принято взять за основу для анализа облачные провайдеры из страны – Россия.

Для выбора облачного провайдера для выше приведённой инфраструктуры он должен удовлетворять следующим требованиям:

1. Дата центры должны располагаться на территории России.
2. Наличие надёжной системы защиты.
3. Низка цена услуг.

* **Timeweb Облако**
* Имеет два дата центра которые располагаются на территории России в Москве и Сочи.
* Наличие TLS защиты, Шифрование с использованием алгоритма AES-256, Защита от DDoS-атак. Наличие Многоуровневой системы аутентификации и контроля доступом Защита от DDoS-атак: Автоматическая фильтрация вредоносных запросов. Гибкий контроль доступа: Настройка прав доступа на уровне пользователей и групп.
* Средние цены и наличие 4 тарифов. Цена варьируется от 50 до 400 рублей в сутки за виртуальную машину.
* **Selectel Облако**
* Имеет два дата центра которые располагаются на территории России в Санкт-Петербурге и Новосибирске.
* Наличие TLS защиты, Шифрование с использованием алгоритма AES-256, Защита от DDoS-атак. Наличие Многоуровневой системы аутентификации и контроля доступом Защита от DDoS-атак: Автоматическая фильтрация вредоносных запросов. Гибкий контроль доступа: Настройка прав доступа на уровне пользователей и групп.
* Средние цены и наличие 4 тарифов. Цена варьируется от 50 до 400 рублей в сутки за виртуальную машину.
* **Яндекс Облако**
* Имеет три дата центра которые располагаются на территории России во Владимирской, Рязанской и Московской областях.
* Наличие TLS защиты, Шифрование с использованием алгоритма AES-256, Защита от DDoS-атак. Наличие Многоуровневой системы аутентификации и контроля доступом.
* Низкая цена и гибкие тарифы
* **Ростелеком Облако**
* Имеет два дат центра, которые располагаются на территории России в Новосибирске и Санкт-Петербурге
* Наличие TLS защиты, Шифрование с использованием алгоритма AES-256, Защита от DDoS-атак. Наличие гибкого контроля доступом.
* Средние цены и наличие 4 тарифов. Цена варьируется от 50 до 400 рублей в сутки за виртуальную машину.
* **VK Cloud**
* Имеет несколько дата центров преимущественно расположенных в Московской области
* Наличие TLS защиты, Шифрование с использованием алгоритма AES-256, Защита от DDoS-атак. Наличие Многоуровневой системы аутентификации и контроля доступом. Наличие мощной системы аудита.
* Средние цены от 2-3 рублей в час за самую слабую виртуальную машину.
* **Cloud.ru**
* Имеет один дата центр с несколькими точками подключения, расположенный в Москве.
* Наличие TLS защиты, Шифрование с использованием алгоритма AES-256, Защита от DDoS-атак. Официально сертифицирован ФСТЭК и ФСБ.
* Средние цены за одну виртуальную машину: от 630 руб/мес. Возможна покупка управляемого кластера.

Лучше всего будет выбрать облачного провайдера в виде Яндекс облако из-за более близкого расположения дата центров и низкой стоимости услуг.

**Задание 4.** Провести оптимизацию существующей инфраструктуры или её части. Под оптимизацией в основном имеется в виду снижение ценника за единицу времени работы инфраструктуры.

* **Оптимизация баз данных.** Для повышения скорости работы баз данных и ускорения выполнения запросов необходимо создать индексы на ключевых полях, используемых в запросах. Однако важно не переусердствовать с количеством индексов, так как это может замедлить процесс вставки данных.
* **Внедрение системы мониторинга.** В инфраструктуру следует интегрировать систему мониторинга, которая будет отслеживать состояние всех систем, включая сетевые, операционные системы и базы данных. Это позволит выявить неэффективное использование ресурсов. Для реализации можно использовать такие инструменты, как Zabbix или Prometheus. Второй вариант предпочтительнее, так как он бесплатен.
* **Автоматическое масштабирование.** Необходимо настроить автоматическое масштабирование для виртуальных машин или контейнеров, чтобы они автоматически увеличивались или уменьшались в зависимости от текущей нагрузки. Это поможет избежать перерасхода ресурсов и снизить затраты в периоды низкой активности.
* **Использование облачных решений.** На начальном этапе целесообразно использовать облачные серверы вместо полноценной серверной архитектуры. Это позволит снизить затраты, упростить управление и повысить эффективность. Подходящие провайдеры для аренды облачных серверов перечислены в третьем пункте.
* **Установка межсетевого экрана.** Для контроля входящего трафика и обеспечения безопасности внутренней сети инфраструктуры необходимо установить межсетевой экран.
* **Аудит изменений конфигураций.** Следует настроить систему аудита для отслеживания изменений конфигураций серверов баз данных. Это поможет выявить возможные проблемы с их работой. Для реализации можно использовать выделенный сервер администратора.