

Задание по учебной практике по ПМ. 03. Эксплуатация объектов сетевой инфраструктуры

Компания: «DataBridge»

Сфера: Разработка SaaS-платформы для аналитики данных. Компания-стартап, успешно привлекший первый раунд инвестиций.

Возраст: Основана в 2022 году.

Масштаб: Команда стремительно выросла с 5 до 25 человек (разработчики, data scientist-ы, отдел продаж). Все работают в одном open-space офисе.

Текущая проблема: Всё работало на ноутбуках и в публичных облаках (ящики с паролями в Google Docs, код в публичном GitHub). Инвесторы потребовали соблюдения стандартов безопасности, защиты интеллектуальной собственности и надёжной внутренней ИТ-среды. Нужно быстро построить «корпоративную» инфраструктуру с контролем доступа, внутренними серверами и политиками безопасности, не убивая при этом гибкость, необходимую разработчикам.

Суть задачи для системного администратора: Создать безопасную и контролируемую среду «с нуля» для быстрорастущей технологичной компании, заложив возможность для будущего внедрения DevOps-практик.

Техническое задание на развертывание pilotной ИТ-инфраструктуры компании «DataBridge»

1. Контекст и цель

Компания «DataBridge», разработчик SaaS-платформы для аналитики данных, столкнулась с критическим несоответствием своей ИТ-среды масштабам бизнеса и требованиям инвесторов. После роста команды с 5 до 25 человек и привлечения финансирования, текущее положение, при котором работа ведется с использованием личных ноутбуков, публичных облачных сервисов и открытых репозиториев, признано неприемлемым. Это создает риски утечки интеллектуальной собственности, несоблюдения базовых стандартов безопасности и низкой отказоустойчивости внутренних процессов.

Цель: Спроектировать, развернуть и протестировать в изолированном стенде pilotный вариант новой корпоративной ИТ-инфраструктуры. Инфраструктура должна обеспечить безопасность данных, централизованное управление, надежность базовых сервисов и создать технологический фундамент для будущего внедрения DevOps-практик без потери операционной гибкости.

2. Ключевые требования к инфраструктуре

Развертываемая инфраструктура должна удовлетворять следующим принципам:

- Безопасность: Реализация принципа минимальных привилегий, сегментация сети, защита периметра, шифрование критичных данных, аудит событий.
- Управляемость: Централизованное управление учетными записями, политиками, конфигурациями и обновлениями.

- Доступность: Обеспечение работоспособности ключевых сервисов в рабочее время за счет отказоустойчивых конфигураций в рамках стенда.
- Масштабируемость: Архитектура должна позволять относительно простое добавление новых сервисов или пользователей.
- Эффективность для разработки: Предоставление разработчикам изолированных сред для тестирования и современных инструментов без усложнения базовых процедур доступа.

3. Список необходимых к внедрению служб и компонентов

3.1. Обязательные компоненты (критичны для запуска):

| № | Компонент / Служба | Основная функция и требования |
|----------|---|--|
| 1 | Централизованная аутентификация и авторизация | Единая точка управления учетными записями пользователей и компьютеров. Интеграция со всеми остальными службами. (Пример реализации: FreeIPA / Windows Server AD). |
| 2 | Защищенная сетевая инфраструктура | Логическая сегментация сети на минимум 3 VLAN (Управление, Пользователи, Серверы). Межсетевой экран с политикой «запрещено по умолчанию». VPN-шлюз для безопасного удаленного доступа. (Пример реализации: OPNsense) |
| 3 | Внутренний репозиторий исходного кода | Приватный, защищенный аутентификацией хост для хранения кода с инструментами контроля версий, code review и управления задачами (Пример реализации: GitLab CE / Gitea / GitFlic). |
| 4 | Файловое хранилище и совместный доступ | Сетевое хранилище для общих документов, проектной документации, библиотек с разграничением прав доступа по |

| | | |
|---|---|---|
| | | ролям (Пример реализации: Samba + FreeIPA/AD / Nextcloud). |
| 5 | Система мониторинга и оповещений | Централизованный сбор метрик о состоянии серверов (CPU, RAM, Disk, Network), журналов событий и доступности служб. Настройка оповещений о сбоях (Пример реализации: Zabbix / Prometheus+Grafana + Alertmanager). |
| 6 | Система резервного копирования и восстановления | Автоматизированное регулярное резервное копирование конфигураций, критичных данных с сервисов (код, файлы) и возможность их гарантированного восстановления (Пример реализации: Кибер Бэкап / Bacula / RuBackup). |

3.2. Опциональные компоненты (повышают эффективность и готовность к DevOps):

| № | Компонент / Служба | Основная функция и требования |
|----------|---|--|
| 7 | Платформа для контейнеризации | Развертывание внутреннего регистратора Docker-образов и базовой среды для запуска контейнеров (Docker Registry, Portainer). |
| 8 | Сервис внутренней коммуникации | Развертывание защищенного корпоративного мессенджера, альтернативного публичным решениям, с возможностью аудита (Mattermost / Matrix). |
| 9 | Среда для автоматизированной сборки и тестирования (CI) | Настройка базового пайплана Continuous Integration в системе из п.3, обеспечивающего автоматическую сборку и тестирование кода при внесении изменений. |
| 10 | Система управления конфигурациями (IaC) | Внедрение инструмента для описания желаемого состояния серверов и служб в виде кода, |

| | | |
|--|--|---|
| | | обеспечивающего идемпотентность и повторяемость развертывания (Ansible). |
|--|--|---|

4. Нефункциональные требования к pilotному стенду

Документация: По итогам развертывания должна быть предоставлена полная архитектурная и эксплуатационная документация, включающая:

- Схему сети (L2/L3) с IP-адресацией и VLAN.
- Смета расходов, с предлагаемыми вариантами реализации проекта.
- Описание всех сервисов, их версий и конфигураций.
- Инструкции по базовым операциям: добавление пользователя, развертывание сервера, процедура восстановления из резервной копии.

Тестирование: Каждая из развернутых служб (п.3.1) должна быть продемонстрирована в рабочем состоянии. Например:

- Создание тестового пользователя и его аутентификация на разных сервисах.
- Размещение кода во внутреннем репозитории и клонирование его на виртуальную рабочую станцию.
- Срабатывание правила межсетевого экрана и оповещения от системы мониторинга при моделировании сбоя.
- Восстановление тестового файла из резервной копии.

Итоговый ожидаемый результат: Работоспособный, документированный виртуальный стенд, имитирующий безопасную и управляемую ИТ-инфраструктуру технологичного стартапа, готовую к демонстрации инвесторам и использованию в качестве основы для дальнейшего развития.