

DevOps в банке

Игнатов Юрий
Экспресс 42



О чем доклад

- История внедрения DevOps-практик в банке
- Про инструменты
- Про людей

Банковская специфика

- Повышенные требования к безопасности
- Повышенные требования к качеству
- Большое количество отделов и команд
- Большое количество продуктов у команды

Банковская специфика

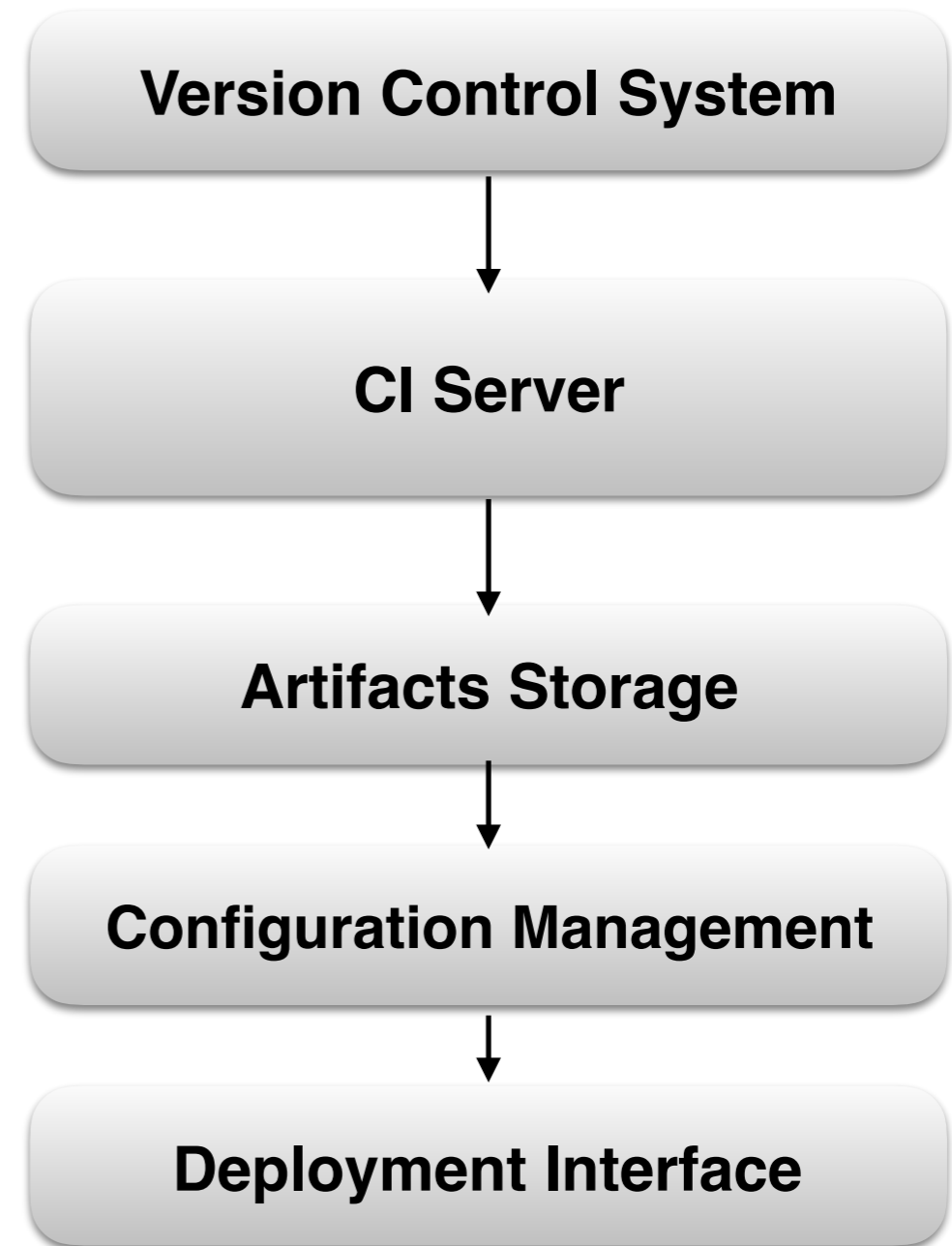
- Узкая специализация сотрудников и отсутствие коллективной ответственности за результат
- Необходимость в большом количестве взаимодействий и встреч между командами
- Разнообразный технологический стек
- Много вендорских компонент

Цели

- Унификация технологического стека
- Создание общих практик
- Повышение квалификации сотрудников
- Автоматизация процессов поставки ПО
- Обратная связь на каждом этапе поставки ПО

Пайплайн поставки ПО

- Разработка
- Сборка
- Тестирование
- Хранение артефактов
- Конфигурирование
- Выкатка



Пайплайн поставки ПО

- Continuous Integration ✓
- Continuous Delivery ✓
- Continuous Code Quality ?
- Continuous Monitoring ?
- Continuous ...

Целевой инфраструктурый стек

- Jira и ее друзья: Confluence, Bitbucket, Bamboo
- Sonarqube – анализ качества кода
- Artifactory – хранилище артефактов
- Bamboo + Ansible – развертывание и настройка
- ELK – централизованное логирование

Анализ качества кода



- Поддержка популярных языков (заявлено 20+)
- Поиск потенциальных багов и уязвимостей
- Интеграция с CI и Quality Gates
- Визуализация технического долга

sonarqube



Quality Gate

Passed

Bugs & Vulnerabilities

Leak Period: last 30 days
last analysis 9 months ago

375 ^E

🐛 Bugs

58 ^E

🔒 Vulnerabilities

0

🐛 New Bugs

0

🔒 New Vulnerabilities

Code Smells

139d ^A

Debt

started 6 years ago

5.9k

⊕ Code Smells

3h

New Debt

33

⊕ New Code Smells

Coverage



58.4%

Coverage

1.8k

Unit Tests

80.6%

Coverage on
28 New Lines to Cover

sonarqube

sonarqube.com Projects Issues Rules Quality Profiles Quality Gates

Open Source / Apache Abdera

Issues Measures Code Activity

Display Mode

Issues Effort

Type

- Bug 200
- Vulnerability 13
- Code Smell 7,869

Resolution

Unresolved	13	Fixed	0
False Positive	0	Won't fix	0
Removed	0		

Severity

Status

Creation Date

Rule

Tag

Module

Directory

Return to List Abdera Extensions - JSON / src/.../org/apache/abdera/ext/sor/JSONServlet.java

```
53     }
54   }
55   return abdera;
56 }
57
58 @Override
59 antel.. protected void doGet(HttpServletRequest request, HttpServletResponse
60 jmsne..
61
62 antel.. String url = request.getPathInfo();
63         if (url != null && url.length() > 1)
64             url = URLDecoder.decode(url, "UTF-8");
65
66         else {
67             response.sendError(400);
68
69         return;
70     }
71     url = url.substring(1);
```

Add a "try/catch" block for "decode". ...

Vulnerability Critical Open Not assigned 20min effort

Add a "try/catch" block for "sendError". ...

Vulnerability Critical Open Not assigned 20min effort

Хранение артефактов

Исходный код	Артефакт
Текст	Бинарник
Diffable	Not diffable
Версионирование по содержимому	Версионирование по имени
Перезаписывается	Не должен перезаписываться



JFrog Artifactory

- Репозитории для популярных технологий
 - MVN / SBT / RubyGems / PyPI / NPM / Generic
 - Yum / Deb / NuGet
 - Множество других типов, даже Docker Registry
- Прокси к внешним репозиториям
- Управление жизненным циклом артефакта
- Контроль доступа
- API и поиск

ANSIBLE

- Подходит для сложных проектов
- Хорошо показал себя с Windows
- Быстрый старт и простота обучения
- Инфраструктура как код и безопасники

Ansible become

```
EXEC ssh <stuff> <hostname>  
  /bin/sh -c 'sudo -k && sudo -u root  
    /bin/sh -c '''  
      /usr/bin/python <module>  
      '''
```

Чего еще не хватает?

- Окружения для разработки и тестирования
 - Существующие сервера – произведение искусства
 - Конфигурация уплыла уже далеко
 - Сетевые политики настроены по принципу точка-точка



Чего еще не хватает?

- Реестр информации о точках интеграции
 - Большое множество внутренних API и сервисов
 - Большое количество окружений
 - Уведомить всех о перестановках – долго
 - Еще дольше ждать, пока все переконфигурируются



Чего еще не хватает?

- Централизованное логирование
 - Получить логи от другой команды – долго
 - Не все члены команды имеют возможность смотреть в логи
 - Сквозное логирование запросов



Проблематика

- Подготовить такой пайплайн – месяц
- Внедрить его вместо старых процессов – еще два
 - Согласования
 - Обучение команды
 - Релизы раз в месяц
- Промежуточный этап (dev, test на новом пайплайне, а staging и production еще нет)
- Люди не хотят изменений

DevOps —

- Culture, Automation, Measurement, and Sharing
- Коллективная ответственность за продукт
- Бизнес, аналитики, разработка, тестирование и эксплуатация – одна команда
- Может, что-то еще

DevOps –

- “DevOps – Автодеплой” :(

Новые обязанности

- Shifting left
- Написание и сопровождение инфраструктурного кода
- Доработка продукта для нового пайплайна
 - изменения в конфигурации
 - service discovery
 - healthchecks
 - идентификаторы запросов для сквозного логирования
 - поддержка стратегий выкатки
- Отслеживание трендов качества кода и работа по улучшению качества
- “Раньше файл по FTP залил и все работает, а теперь нужно в этот ваш git комитить”

Делаем для людей

- Первое время работаем с инициативной группой
- Проводим тренинги, мастер-классы
- Описываем свой опыт и делимся им с другими командами

Делаем для людей

- Деплой с кнопки, деплоить может каждый
- Вынести версии ПО для деплоя на окружения из Ansible-репозитория в веб-интерфейс, чтобы не приходилось учить Git и Ansible
- Человекочитаемые сообщения об ошибках (Блоки в Ansible)
- Документация до внедрения

Метрики скорости

- **Mean Lead Time** – время на билд, тесты, деплой
- **Daily Change Rate** – успешных изменений в день
- **Mean Time To Environment** – время на подготовку нового окружения
- **Mean Time To Detect** – как долго баг может быть необнаруженным

Метрики качества

- **Build Failure Rate** – процент неуспешных сборок
- **Deployment Failure Rate** – процент неуспешных выкаток
- **Infra-Related Failure Rate** – процент неуспешных выкаток/сборок из-за проблем инфраструктуры
- **Automated Detection Rate** – процент проблем, выявленных на этапах тестирования