Централизованные системы логирования - ELK стек

Код: PTRN-044

Длительность: 8 ч.

Описание:

E.L.K. — это отличный стек для хранения, управления и мониторинга логов. Данный курс дает понимание зачем и в каких случаях его использование оптимально для решения поставленных задач.
Чем полезен курс:

- Понять в каких случаях стоит применять данный стек;
- Уметь быстро настраивать стек;
- Научиться настраивать визуализацию необходимой информации.

Цели:

Познакомить участников с возможностями ELK (Elasticsearch, Logstash и Kibana) стека для широкого спектра задач по сбору, хранению и анализу данных.

Разбираемые темы:

Теория (4 часа)

1. Введение
   - Как приложение пишет логи, когда и куда?
   - Типовые примеры работы с логами.
   - Проблематика (логи на серверах в файлах, доступность команде).
   - Примеры использования (эксплуатация, тестирование, аналитика в реальном времени, аналитика по истории, аудит).
2. ELK и друзья
   - Устройство ELK.
   - Как начать использовать ELK?
   - Механизмы сбора логов (файлы, приложением, Kafka).
   - Практика структурированных логов (работа с Multiline).
   - Сокрытие приватных данных при сборе логов.
   - Работа с данными, язык запросов ElasticSearch.
   - Визуализация в Kibana + XPack.
   - Нотификации и алерты.
   - Подготовленные командой General Banking Bamboo plans.
3. Истории команд.
   - Из индустрии, интернета, от опыта Экспресс 42.

Практика (4 часа)

1. Работа с заранее подготовленным потоком событий
   - Работа с поиском, поиск ошибок (к пр. веб сервера) за период времени.
   - Создание визуализаций по поисковым выборкам.
   - Описание dashboards as a code. Работа с импортом/экспортом.
   - Алертинг в ELK.
2. Разбираем варианты сбора и отправки лог данных
   - Из приложения.
   - Из файлов (конфигурация Filebeat, etc).
   - Linux Syslog / Windows Event Viewer.
   - Сокрытие приватных данных.
   - Интеграция с другими системами (Bamboo, Network Hardware, etc).
3. Обработка логов на стороне ELK
   - Grok patterns.
   - Преобразование типов данных

Целевая аудитория:

Системные администраторы, инфраструктурные инженеры, разработчики, продвинутые тестировщики.

Предварительная подготовка – общее:

Базовое знание ОС Linux.