**Наименование предприятия:** ООО «Транснефть – Дальний Восток», отдел автоматизированных систем управления технологического процесса.

**Направление обучения участников:** Сетевое и системное администрирование.

**Название кейса:** Создание системы по сбору и анализу записей событий активного сетевого оборудования.

**Описание:**

Для обмена информацией в автоматизированных системах управления технологическими процессами, используется выделенная технологическая сеть передачи данных (ТСПД), имеющая в своем составе активное сетевое оборудование.

Необходимо разработать комплексную систему, позволяющую проводить централизованный сбор событий («логи»), зарегистрированных на активном сетевом оборудовании с записью полученной информации в базу данных.

Система должна состоять из следующих подсистем:

1. Подсистема получения и обработки данных - организация сбора информации для получения данных от различного сетевого оборудования с использованием коммуникационного SNMP протокола, с последующей обработкой, упорядочиванием и сохранением данных;
2. Подсистема хранения – организация структурированного хранения и управления обработанных данных;
3. Подсистема мониторинга и контроля данных – организация непрерывного процесса наблюдения и проверки хранящихся данных на предмет заданных условий, параметрам или критериям;
4. Клиентская подсистема – графическая оболочка (интерфейс) для организации взаимодействия с Системой (поиск и просмотр данных, формование правил и отчетов) и настройкой всех её подсистем;
5. Подсистема оповещений – организация передачи электронных сообщений на заданные почтовые ящики и передачу сигналов в клиентскую подсистему.

Основной задачей Системы, является мониторинг сетевого оборудования, с помощью создаваемых правил (условий) и действий, которые будут выполнены по заданным значениям.

Пример работы Системы: Через графическую оболочку, администратор Системы добавляет в неё всю необходимую информацию для сбора данных с устройств: сетевой коммутатор и маршрутизатор. После подтверждения от Системы об успешном добавлении и получении информации с устройств, администратор создает правила:

1. «Активность» - Условие: Если Система перестает получать данные с оборудования, отправлять на почтовые адреса ivanovii@transneft.ru petrovpp@transneft.ru сообщения с текстом: “С оборудования **%сетевое\_имя\_оборудовния%** перестали поступать данные”.

2. «Ошибки» - Условие: Если Система в полученном с устройства тексте сообщения, обнаруживает подстроку «error», отправлять на почтовые адреса ivanovii@transneft.ru petrovpp@transneft.ru сообщения с текстом: “На оборудовании **%сетевое\_имя\_оборудовния%** в **%время\_регистрации\_события%** зарегистрировано событие: **%текст\_полученного\_события%**”.

Система после сохранения правил, учитывает их в процессе мониторинга и контроля, и в случае если запись с заданного устройства не получена или в её тексте содержится указанное строковое значение, производит отправку электронного письма на заданные почтовые ящики, с введённым сообщением с автоматической подстановкой значений по триггерам в тексте сообщения.

**Контактное лицо для взаимодействия по кейсу:**

Квашенко Александр Николаевич, KvashenkoAN@dmn.transneft.ru, 8 (4212) 40 12 40