Продолжаю тему настройки и использования централизованной системы сбора логов на основе elasticsearch. Сегодня расскажу, как настроить сбор и анализ логов аудита samba в ELK Stack. Я буду не только собирать логи, но и обрабатывать их и добавлять метаданные для построения графиков и дашбордов.

(далее...)