Продолжаю цикл статей по настройке централизованной системы сбора логов ELK Stack. Сегодня расскажу, как собирать логи с Windows Server различных версий в elasticsearch. Данные предложенным способом можно будет собирать не только с серверных систем, но и со всех остальных, где используется журнал windows.

(далее...)