1. Установка и настройка nxlog

* Перейти по ссылке и загрузить последнюю версию программы <https://nxlog.co/products/nxlog-community-edition/download>
* Выполнить установку программы
* Заменить или дополнить соответствующий конфигурационный файл по пути C:\Program Files\nxlog\conf для 32 разрядной ОС или C:\Program Files (x86)\nxlog\conf для 64 разрядной, при этом имя файлов должно иметь вид nxlog.conf. Далее представлена таблица соответствия конфигурационных файлов.

|  |  |
| --- | --- |
| nxlog-windows-x86.conf.template | 32 разрядные версии Windows |
| nxlog-windows-x86\_64.conf.template | 64 разрядные версии Windows |

* Отредактировать следующую часть конфигурационного файла:



В поле Host должен быть указан IP адрес или доменное имя, по которому для данной машины доступен сервер логов.

* Запустить службу nxlog через оснастку services или командной net start nxlog.

1. Пояснения

При данной конфигурации каждая строка файла, будет читаться как цельное сообщение. Для дополнительного разбиения на под поля необходимо дополнить файлы nxlog.conf на клиентской и windows-example-file-log.conf на серверной машинах соответствующими настройками. Рекомендуется для передачи формат csv (пример windows event log). Для дополнительной информации изучите документацию по следующим ссылкам:

* <https://nxlog.co/documentation/nxlog-community-edition-reference-manual-v20928#im_file>
* <https://nxlog.co/documentation/nxlog-community-edition-reference-manual-v20928#xm_csv>
* <https://syslog-ng.com/documents/html/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/reference-parsers-csv.html>
* <https://syslog-ng.com/documents/html/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/json-parser.html>