1. Генерация сертификатов

* cd ~
* mkdir CA
* cd CA
* mkdir certs crl newcerts private
* echo «01» > serial
* cp /dev/null index.txt
* cp /etc/pki/tls/openssl.cnf openssl.cnf
* sudo vim openssl.cnf

*[CA\_default]*

*dir = .*

* openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem -days 365 -config openssl.cnf
* openssl req -nodes -new -x509 -keyout serverkey.pem -out serverreq.pem -days 365 -config openssl.cnf

[!] common name = server ip or domain name

[!] email = «поле должно быть пустым»

* openssl x509 -x509toreq -in serverreq.pem -signkey serverkey.pem -out tmp.pem
* openssl ca -config openssl.cnf -policy policy\_anything -out servercert.pem -infiles tmp.pem
* rm tmp.pem
* (для каждого клиента) openssl req -nodes -new -x509 -keyout clientkey.pem -out clientreq.pem -days 365 -config openssl.cnf

[!] common name = client ip or domain name

[!] email = «поле должно быть пустым»

* (для каждого клиента) openssl x509 -x509toreq -in clientreq.pem -signkey clientkey.pem -out tmp.pem
* (для каждого клиента) openssl ca -config openssl.cnf -policy policy\_anything -out clientcert.pem -infiles tmp.pem
* (для каждого клиента) rm tmp.pem

1. Установка сертификата на syslog-ng сервер

* cd /etc/syslog-ng
* sudo mkdir cert.d ca.d
* скопировать serverkey.pem и servercert.pem в cert.d
* скопировать cacert.pem в ca.d
* cd /etc/syslog-ng/ca.d
* openssl x509 -noout -hash -in cacert.pem
* sudo ln -s cacert.pem <вывод предыдущей команды>.0
* Отредактировать конфигурационные файлы, для которых будет использоваться tls к следующему виду:

*source example\_tls\_source {*

*tcp (ip(0.0.0.0) port (6514)*

*tls( key\_file(«/etc/syslog-ng/cert.d/serverkey.pem»)*

*cert\_file(«/etc/syslog-ng/cert.d/servercert.pem»)*

*ca\_dir(«/etc/syslog-ng/ca.d»))*

*); };*

./server-tls/linux-event-log.conf.template

./server-tls/linux-example-file-log.conf.template

./server-tls/windows-event-log.conf.template

./server-tls/windows-old-event-log.conf.template

./server-tls/windows-example-file-log.conf.template

1. Установка сертификата на syslog-ng клиент

* cd /etc/syslog-ng
* sudo mkdir cert.d ca.d
* скопировать clientkey.pem и clientcert.pem в cert.d
* скопировать cacert.pem в ca.d
* cd /etc/syslog-ng/ca.d
* openssl x509 -noout -hash -in cacert.pem
* sudo ln -s cacert.pem <вывод предыдущей команды>.0
* Отредактировать конфигурационные файлы, для которых будет использоваться tls к следующему виду:

*destination example\_tls\_destination {*

*tcp («192.168.0.1» port (6514)*

*tls( key\_file(«/etc/syslog-ng/cert.d/serverkey.pem»)*

*cert\_file(«/etc/syslog-ng/cert.d/servercert.pem»)*

*ca\_dir(«/etc/syslog-ng/ca.d»))*

*); };*

./linux-event-log-client/linux-event-log.conf.template

./linux-example-file-client/linux-example-file-log.conf.template

1. Установка сертификата на nxlog клиент

* Скопировать файлы clientkey.pem clientcert.pem и cacert.pem в директорию C:\Program Files\nxlog\conf для 32 разрядной ОС или C:\Program Files (x86)\nxlog\conf для 64 разрядной.
* Отредактировать соединения, для которых будет использоваться tls, в конфигурационном файле следующим образом:

*Module om\_ssl*

*Host 192.168.0.1*

*Port 6518*

*CAFile %ROOT%\cert\cacert.pem*

*CertFile %ROOT%\cert\clientcert.pem*

*CertKeyFile %ROOT%\cert\clientkey.pem*

Если используется формат syslog необходимо дополнительно добавить строку:

*OutputType Syslog\_TLS*

./windows-event-client/nxlog-windows-old-x86.conf.template

./windows-event-client/nxlog-windows-old-x86\_64.conf.template

./windows-event-client/nxlog-windows-x86.conf.template

./windows-event-client/nxlog-windows-x86\_64.conf.template

./windows-example-file-client/nxlog-windows-x86.conf.template

./ windows-example-file-client/nxlog-windows-x86\_64.conf.template

1. Включение SSL в kibana

* cd /etc/kibana/
* sudo mkdir cert.d/
* скопировать serverkey.pem и servercert.pem в cert.d
* update /etc/kibana/kibana.yml

./server-kibana-ssl/kibana.yml.template

* Установить cacert.pem и servercert.pem в браузер (если в сертификате прописан только IP адрес то ssl Google Chrome работать не будет).

1. Конфигурация xpack

* cd /usr/share/elasticsearch
* sudo /bin/elasticsearch-plugin install x-pack
* cd /usr/share/kibana
* sudo /bin/kibana-plugin install x-pack
* cd /usr/share/elasticsearch
* sudo /bin/x-pack/setup-passwords interactive
* Добавить логин и пароль для пользователя kibana в /etc/kibana/kibana.yml. Опционально можно также добавить ключ дополнительного шифрования.

./server-xpack/kibana.yml.template

* Обновить конфигурационные файлы syslog-ng для использования логина и пароля пользователя elastic.

./server-xpack/linux-event-log.conf.template

./server-xpack/linux-example-file-log.conf.template

./server-xpack/windows-event-log.conf.template

./server-xpack/windows-old-event-log.conf.template

./server-xpack/windows-example-file-log.conf.template