Nagios Log Server – Sending nxlogs with SSL

Nagios®

The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to setup encryption between Nagios Log Server and nxlog on Windows using self signed certificates.

Target Audience

This document is intended for use by Nagios Log Server Administrators who would like encryption between NLS and their Windows nxlog clients.

Generate a root CA

Run these two commands to generate a root ca key on your Nagios Log Server, and self sign it.

```
openssl genrsa -out rootCA.key 2048
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
```

Create the certificates

This next part will create two certificates, that are signed by your CA. When prompted for your common name enter the IP of your server.

This one is for Nagios Log Server.

```
openssl genrsa -out device-nls.key 2048
openssl req -new -key device-nls.key -out device-nls.csr
openssl x509 -req -in device-nls.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out device-
nls.crt -days 500 -sha256
```

This one is for the client device.

```
openssl genrsa -out device.key 2048
openssl req -new -key device.key -out device.csr
openssl x509 -req -in device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out device.crt
-days 500 -sha256
```

Now, lets move the certificate files we just created.

```
cp *.key /etc/pki/tls/private/
cp *.csr /etc/pki/tls/private/
cp *.crt /etc/pki/tls/certs/
cp *.pem /etc/pki/tls/certs/
```

Add the input to Nagios Log Server

Before we add the input, we need to open up the port in iptables.

```
iptables -A INPUT -p tcp -m tcp --dport 7777 -j ACCEPT
iptables-save
```

We now need to create a tcp input for our SSL connection. Navigate to **Administration → Global Configuration → + Add Input → Custom**. Once there, create a name for this Input and add the following.

```
tcp {
    port => 7777
    type => "nxlogs"
    ssl_cacert => "/etc/pki/tls/certs/rootCA.pem"
```


Revision 1.0 – February, 2016

```
    ssl_cert => "/etc/pki/tls/certs/device-nls.crt"
    ssl_key => "/etc/pki/tls/private/device-nls.key"
    ssl_enable => true
    format => 'json'
}
```

Save the Input, and then click Apply Configuration.

Configuring nxlog on the Windows client

From your Nagios Log Server machine, copy over the file we created earlier from **/etc/pki/tls/certs/device.crt** to your nxlog cert directory on the Windows machine to **C:\Program Files (x86)\nxlog\cert\device.crt**.

Now, we need to modify the nxlog.conf. With this configuration, I first copied the original configuration that Nagios Log Server generated for my machine. I've commented out the old configuration, and added the new output below.

```
#original non-SSL support
#<Output out>
#    Module om_tcp
#    Host 192.168.4.186
#    Port 3515
#
#    Exec  $tmpmessage = $Message; delete($Message); rename_field("tmpmessage","message");
#    Exec  $raw_event = to_json();
#
#      # Uncomment for debug output
#      # Exec file_write('%ROOT%\data\nxlog_output.log', $raw_event + "\n");
#</Output>

#added for SSL support
<Output out>
    Module          om_ssl
    Host            192.168.4.186
    Port            7777
    CertFile        C:\Program Files (x86)\nxlog\cert\device.crt
    OutputType      LineBased
    AllowUntrusted  True
</Output>
```

Save the file, and restart your nxlog service.

Additional information

If you would like to verify that traffic is encrypted, you can verify with tcpdump. I've included a sample with this document.

The command I am using for this is `tcpdump -nnvXSs 0 host 192.168.3.15`

```
        192.168.3.15.56697 > 192.168.4.186.3515: Flags [P.], cksum 0x939c (correct), seq
743751542:743752638, ack 2190259146, win 256, length 1096
        0x0000:  0000 0000 0000 0000 8006 1537 c0a8 030f  E..pX7@....7....
        0x0010:  c0a8 04ba dd79 0dbb 2c54 bf76 828c b3ca  .....y..,T.v....
        0x0020:  5018 0100 939c 0000 7b22 4576 656e 7454  P.......{"EventT
        0x0030:  696d 6522 3a22 3230 3136 2d30 312d 3235  ime":"2016-01-25
        0x0040:  2031 343a 3334 3a31 3122 2c22 486f 7374  .14:34:11","Host
        0x0050:  6e61 6d65 223a 2277 696e 326b 382d 6463  name":"win2k8-dc
        0x0060:  2e74 6573 7464 6f6d 6169 6e2e 636f 6d22  .testdomain.com"
        0x0070:  2c22 4b65 7977 6f72 6473 223a 2d39 3231  ,"Keywords":-921
        0x0080:  0000 0000 0000 0000 0000 0000 0000 0000  0000000000000000
        0x0090:  2c22 4576 656e 7454 7970 6522 3a22 4155  ,"EventType":"AU
        0x00a0:  4449 545f 0000 0000 0000 0000 2c22 5365  DIT_SUCCESS","Se
```

```
        0x00b0:  0000 0000 0000 0000 6c75 6522 3a32 2c22  verityValue":2,"
        0x00c0:  0000 0000 0000 0000 223a 2249 4e46 4f22  Severity":"INFO"
        0x00d0:  2c22 4576 656e 7449 4422 3a34 3633 342c  ,"EventID":4634,
        0x00e0:  2253 6f75 7263 654e 616d 6522 3a22 4d69  "SourceName":"Mi
        0x00f0:  6372 6f73 6f66 742d 5769 6e64 6f77 732d  crosoft-Windows-
        0x0100:  0000 0000 0000 0000 2d41 7564 6974 696e  Security-Auditin
        0x0110:  6722 2c22 5072 6f76 0000 0000 0000 0000  g","ProviderGuid
        0x0120:  223a 227b 0000 0000 0000 0000 2d35 3437  ":"{54849625-547
        0x0130:  382d 3439 3934 2d41 3542 412d 3345 3342  8-4994-A5BA-3E3B
        0x0140:  0000 0000 0000 0000 7d22 2c22 5665 7273  0328C30D}","Vers
        0x0150:  696f 6e22 3a30 2c22 5461 736b 223a 3132  ion":0,"Task":12
        0x0160:  3534 352c 224f 7063 6f64 6556 616c 7565  545,"OpcodeValue
        0x0170:  223a 302c 2252 6563 6f72 644e 756d 6265  ":0,"RecordNumbe
        0x0180:  7222 3a34 3836 3732 2c22 5072 6f63 6573  r":48672,"Proces

       192.168.3.15.56709 > 192.168.4.186.7777: Flags [P.], cksum 0xf17d (correct), seq
476707367:476707905, ack 3278412591, win 256, length 538
        0x0000:  4500 0242 58b8 4000 8006 16e4 c0a8 030f  E..BX.@.........
        0x0010:  c0a8 04ba dd85 1e61 1c69 fa27 c368 9b2f  .......a.i.'.h./
        0x0020:  5018 0100 f17d 0000 1703 0100 206c 53d0  P....}.......lS.
        0x0030:  75dc 94da 349a c281 27ed faf2 9945 27b3  u...4...'....E'.
        0x0040:  99c2 b056 4ced 048e a196 8c17 1317 0301  ...VL...........
        0x0050:  01f0 25f5 4919 424a 5d12 6cdf b5b6 206e  ..%.I.BJ].l....n
        0x0060:  8d16 4757 0758 18fc 56b0 cccd 0d2c bd2b  ..GW.X..V....,.+
        0x0070:  4046 fa61 ea2a 7143 13e4 7a6c 0509 1b3a  @F.a.*qC..zl...:
        0x0080:  8e8c 9b0d 7db4 e95a bc5a 48c7 b309 2934  ....}..Z.ZH...)4
        0x0090:  af46 4fb1 4054 fd38 b109 5425 8194 1d02  .FO.@T.8..T%....
        0x00a0:  5324 5b37 6b91 2571 6f4e 985c 7d19 0fb9  S$[7k.%qoN.\}...
        0x00b0:  5909 9745 d52a e542 de58 70e7 8a99 5553  Y..E.*.B.Xp...US
        0x00c0:  32db 9b74 ba80 462f 4d80 ddfc ba3d 0b51  2..t..F/M....=.Q
        0x00d0:  6978 aa5e ea93 e166 f6e1 8677 c58b 8569  ix.^...f...w...i
        0x00e0:  2a9f 6b87 02ba 910c c259 e460 e2e8 4f9d  *.k......Y.`..O.
        0x00f0:  106c 9737 9aab 5c71 c953 6705 3789 d0d0  .l.7..\q.Sg.7...
        0x0100:  f3df 4436 48ef f80c e9f0 e401 954a 46e7  ..D6H........JF.
        0x0110:  b63b 87c6 d235 bc74 5f20 4ad5 b767 051e  .;...5.t_.J..g..
        0x0120:  2220 2365 45a5 52f3 8efa 356a 83f1 76b1  ".#eE.R...5j..v.
```

Troubleshooting

If you are not receiving logs, there are a couple of files to check for logs.

On the client windows machine look in -
`C:\Program Files (x86)\nxlog\data\nxlog.log`

On the Nagios Log Server look in -
`/var/log/logstash/logstash.log`

If you see an SSL related error on the Nagios Log Server, verify the permissions of your folder / files containing the certificates.

```
ls -l /etc/pki/tls/certs/
ls -l /etc/pki/tls/private/
```