FTICKS for NPS

NOTE: This is untested.

Installation

Download NXLog Community Edition from here:

https://nxlog.co/products/nxlog-community-edition/download

and install it. Make of note of where the nxlog.conf file is.

Configuration

Edit the *nxlog.conf* file and add the following to the end:

```
<Output syslog_tls>
    Module      om_ssl
    Host        212.219.243.132
    Port        6514
    CAFile      c:/Program Files (x86)/nxlog/data/cacert.pem
    CertFile    c:/Program Files (x86)/nxlog/data/clientreq.pem
    CertKeyFile c:/Program Files (x86)/nxlog/data/clientkey.pem
    AllowUntrusted 1
    OutputType  Syslog_TLS
    Exec        to_syslog_ietf();
</Output>

<Output syslog_tcp>
    Module      om_tcp
    Host        212.219.243.132
    Port        601
    OutputType  Syslog_TLS
    Exec        to_syslog_ietf();
</Output>

<Input eventlog>
    Module  im_msvistalog
    <QueryXML>
      <QueryList>
        <Query Id="0" Path="System">
          <Select Path="System">*[System[Provider[@Name='NPS']]]</Select>
          <Select Path="Security">*[System[Provider[@Name='Microsoft-
Windows-Security-Auditing'] and Task = 12552]]</Select>
        </Query>
      </QueryList>
```

```
    </QueryXML>
</Input>

<Route 1>
    Path        eventlog => syslog_tcp
</Route>
```

Save the file and restart the service.

The first stanza, syslog_tls, is just there for information. It's not actually used in this configuration. At a later date we'll be looking at encryption but there's a PKI to build.

This is all fairly self-explanatory. **OutputType Syslog_TLS** is needed to enforce the RFC5424 standards along with **Exec to_syslog_ietf()**. Not sure why both are needed but they really are.

In the Eventlog config the QueryXML is extracted from Windows Event Log (**Event Viewer → Custom View →**. *Server Roles**. Right click on** Network Policy...**. Choose** Properties** , Edit Filter, XML and copy the XML into the NXLog config).

From:
https://wiki.govroam.uk/dokuwiki/ - **Govroam**

Permanent link:
https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:fticks_for_ms_nps&rev=1663161170

Last update: **2022/09/14 13:12**