FTICKS for NPS

NOTE: This is untested.

This only applies to Federation Operators and not to individual sites

Here we provide one option for a syslog proxy server but you set up any syslog server as long as it has the following behaviour:

- Uses the FTICKS format
- Proxies to utilities.govroam.uk on port 514/UDP with Facility local5
- Includes in the FTICKS '#FEDID=0X000#' where 0X000 is replaced by the Federation ID supplied by Jisc.
- Filters down the proxied log to just those for
    - Successful authentications
    - Only authentications between member sites (i.e. NOT those to or from the Jisc NRPS, or within an organisation)

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 to read, making sure that the ROOT points to the directory it's installed in:

```
Panic Soft
#NoFreeOnExit TRUE

define ROOT     C:\Program Files (x86)\nxlog
define CERTDIR  %ROOT%\cert
define CONFDIR  %ROOT%\conf
define LOGDIR   %ROOT%\data
define LOGFILE  %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data

<Extension _syslog>
```

```
    Module      xm_syslog
</Extension>

<Extension _exec>
    Module      xm_exec
</Extension>

<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>
    <Exec>
# Don't send log if going to or coming from a NRPS
# Change to math the ClientName and ProxyPolicyName as appropriate
      if $ClientName =~ /NRPS/i drop();
      if $ProxyPolicyName =~ /NRPS/i drop();

# Replace with the provided Federation ID
      $FederationID = "XXXXX";

# Send Client Name as the Operator Name if present, otherwise use a default.
# Replace 1something.here with the Federation's Operator Name
      if $ClientName == ''
```

```
      {
        $OperatorName = "1something.here";
      }
      else
      {
        $OperatorName = $ClientName;
      }
    </Exec>
</Input>

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

Replace *XXXXX* with the Federation ID supplied by Jisc.

Replace *1something.here* with your realm, prefixed by '1'.

The Client Name and the Proxy Policy Name for receiving from/sending to the Jisc NRPS would have to contain 'NRPS' for the above to work. Otherwise change the above so that requests to/from the NRPS are excluded from the logging.

Save the file and restart the service.

To make this work properly, the Client Name has to be in the form of a realm e.g. 1holby.nhs.uk for each of the Clients.

The 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).

Some customisation might be needed to filter only for traffic between sites, rather than traffic to/from Jisc NRPS.

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

Permanent link:
https://wiki.govroam.uk/doku.php?id=siteadmin:fticks_for_ms_nps&rev=1716192006

Last update: **2024/05/20 08:00**