FTICKS Logging

The Jisc NRPS keep a log of successful roams between organisation connected to them. However, about 90% of roams happen within Federations so this data is not visible. To gain a complete picture of roaming Federations need to send their own roaming information to a central point.

The mechanism for accomplishing this is Syslog, a standard (RFC 5424) approach for logging information to centralised repositories. Jisc uses ELK (Elasticsearch, Logstash and Kibana) to handle, process and display roaming data.

For doing a similar task within eduroam GEANT devised a standard syslog message body format and called it FTICKS. The requirements relevant here were:

1. Allow receipt of statistics events in a decentralised manner (i.e. from arbitrary, but legitimate sources).

2. Support semantics of established eduroam statistics collection, in particular:

a. Quantify number of authentications carried out

b. Quantify number of roaming days (total number of distinct MAC addresses seen roaming on a given day).

3. Be implementable by participants in a lightweight manner; ideally completely stateless for the participant.

4. Contain a reliable duplicate detection.

5. Require only the bare minimum of information about users to satisfy the quantification goals in requirement 2.

6. Enable participants to opt in to receive more detailed statistics than those stated in requirement 2 (at the expense of giving away more information).

7. Be extensible enough to allow for future adaptation if changes are made to the eduroam infrastructure.

8. Be independent of the server software used by participants.

The format would be:

```
F-TICKS/govroam/1.0#REALM=%R#VISINST=%{Operator-
Name}#VISCOUNTRY=GB#CSI=%{Calling-Station-Id}#RESULT=OK#
```

as a field separate makes sense because it doesn't appear in realms for the Calling-Station-Id.

This format can easily be machine parsed by the aforementioned tools.

The REALM field contains the realm of the user in the form '@holby.nhs.uk' and the CSI contains the Calling Station ID of the device making the authentication request (the user's device). More on the CSI later.

VISINT is the identity of the organisation sending the authetication request. Ideally this should be the Operator-Name of the site from which the Visitor is making their request. e.g. '1localgp.holby.nhs.uk' but the RFO should insert the originating site's identity if the originating site is unable to do so themselves. The least desirable default option is for the RFO to insert their own Operator-Name as a last resort e.g. '1holby.nhs.uk'.

RESULT should always be 'OK' because only successful authentication should be reported. Furthermore, only successful authentication attempts between two members of the same Federation should be reported. Specifically, authentication attempts within the same realm are NOT roams, by definition, and authentication attempts with realms outside of the Federation will already by logged by the Jisc NRPS.

The CSI, or Calling-Station-Id, is useful for de-duplication of messages but it's not necessary for the CSI to be the actual MAC address of the client device. For security purposes obfuscating this address is recommended. As long as the pseudo MAC sent is always the same for the same MAC (i.e. 1-to-1 mapping) then the requirement for deduplication is met and the actual device can not be identified. The suggestion is to leave the first half of the MAC untouched because this OUI can be used for high-level device type analysis.

Syslog Configuration

The most basic form of syslog is to use UDP on port 514 to send through simple messages. This is an acceptable approach. TCP is also an option, as is TLS. Please discuss with Jisc which approach you'd like to take for sending syslog.

Unix Syslog

Syslog tools are available on all versions of Unix.

Configuration fragments for syslog-ng are available but other syslog software, such as rsyslog, are just as capable.

Windows Syslog

Windows doesn't have syslog in-built in the same way as linux so requires extra tools, such as Filebeat. Filebeat processes windows logs and sends data in the form of XML to Logstash which then processes the logs in the same way as the FTICKS above.

FTICKS configuration

There are configuration fragments for RadSecProxy, FreeRADIUS and RADIATOR.

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

Permanent link:
https://wiki.govroam.uk/doku.php?id=public:fticks&rev=1619612595

Last update: **2021/04/28 12:23**