ClearPass FTICKS for Federation Operators only

There are a number of steps required to set up FTICKS logging.

1. Configure Clearpass to send logs in the right format to a syslog server.

```
SELECT  concat(
substring(user_name,2,100)||'#VISCOUNTRY=UK#VISINST='||attr_value||'#CSI='||
end_host_id||'#RESULT=OK#FEDID=0X000')
AS "F-TICKS/govroam/1.0#REALM"
FROM public.tips_radius_session_log,public.tips_session_log_details
WHERE public.tips_radius_session_log.id =
public.tips_session_log_details.session_id
AND public.tips_session_log_details.attr_name = 'Radius:IETF:Operator-Name'
AND public.tips_radius_session_log.timestamp > --START-TIME--
AND public.tips_radius_session_log.timestamp <= --END-TIME--
AND public.tips_radius_session_log.auth_method='PROXY'
AND public.tips_radius_session_log.service_name not like '%NRPS%'
AND public.tips_radius_session_log.request_status = 1
ORDER BY public.tips_radius_session_log.timestamp asc
```

The line “public.tips_radius_session_log.service_name not like '%NRPS%'” is where the authentications to/from the NRPS are filtered out. The names of the services which proxy to/from the NRPS needs to have a name which could be matched by an SQL query. The example here must have 'NRPS' in the name.

The line “AND public.tips_radius_session_log.request_status = 1” ensures that only logs of successful authentications are pass on.

There might need to be othe lines in there to ensure that the only logs sent to Jisc are ones that match a proxy between two sites specifically for govroam, rather than all proxied logs for non-govroam services.

1. Set up a syslog server to proxy the FTICKs log from Clearpass to the Jisc syslog server.

Here are two options for possible syslog servers and config but you set up any syslog server as long as it has the following behaviour:

- Proxies to utilities.govroam.uk on port 601/TCP
- Includes in the FTICKS '#FEDID=0X000#' where 0X000 is replaced by the Federation ID supplied.
- 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)

The two options:

1. syslog-ng on linux

2. NXLog CE on Windows

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

Permanent link:
https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:clearpass_fticks&rev=1715759918

Last update: **2024/05/15 07:58**