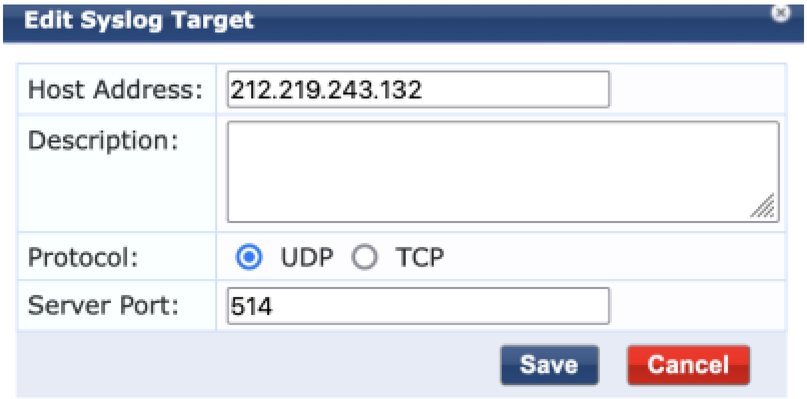
ClearPass FTICKS for Federation Operators only

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

Syslog Targets

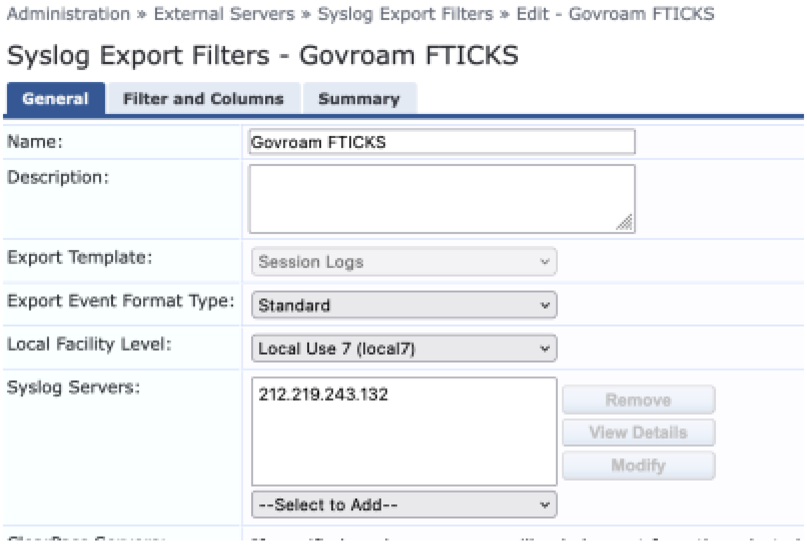
Create a new Syslog Target (Administration→External Servers→Syslog Target) for the Jisc syslog server, utilities.govroam.uk on port 514/UDP


Edit Syslog Target

Host Address:	212.219.243.132
Description:	
Protocol:	● UDP ○ TCP
Server Port:	514

Syslog Export Filter

Create a new Syslog Export Filter (Administration→External Servers→Syslog Export Filter) for the FTICKs logs:


Administration » External Servers » Syslog Export Filters » Edit - Govroam FTICKS

Syslog Export Filters - Govroam FTICKS

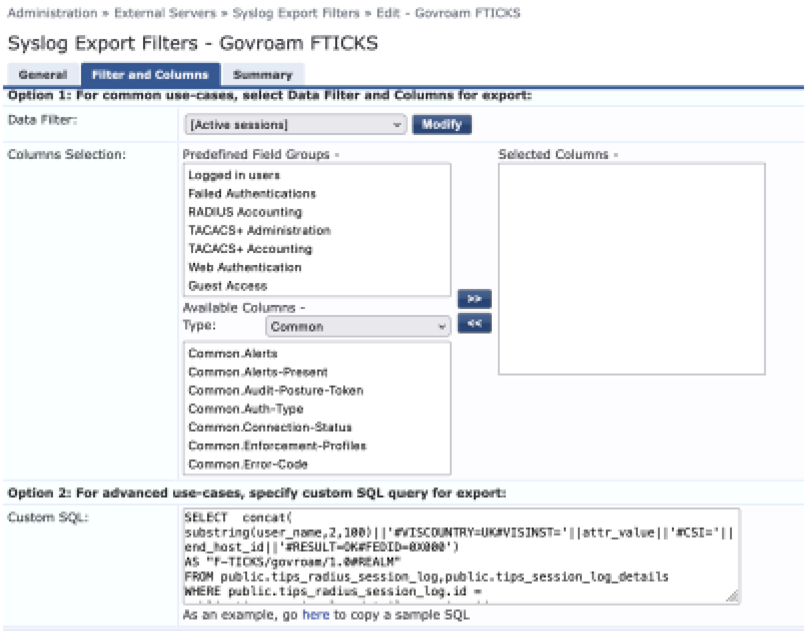
Name:	Govroam FTICKS
Description:	
Export Template:	Session Logs
Export Event Format Type:	Standard
Local Facility Level:	Local Use 7 (local7)
Syslog Servers:	212.219.243.132

where

- Export Template is \\Session Logs
- Export Event Format Type is \\Standard
- Local Facility Level is \\local7

- Syslog Servers is the Jisc one created above
- and your ClearPass servers to generate logs from

Then in the \\Filters and Columns
tab:


Administration » External Servers » Syslog Export Filters » Edit - Govroam FTICKS
Syslog Export Filters - Govroam FTICKS
General
Filter and Columns
Summary
Modify
>>
<<

Option 1: For common use-cases, select Data Filter and Columns for export:

Data Filter: [Active sessions]

Columns Selection:

Predefined Field Groups -
Logged in users
Failed Authentications
RADIUS Accounting
TACACS+ Administration
TACACS+ Accounting
Web Authentication
Guest Access

Available Columns -
Type: Common

Common.Alerts
Common.Alerts-Present
Common.Audit-Posture-Token
Common.Auth-Type
Common.Connection-Status
Common.Enforcement-Profiles
Common.Error-Code

Selected Columns -

Option 2: For advanced use-cases, specify custom SQL query for export:

Custom SQL:

```
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 =
```

As an example, go here to copy a sample SQL

ignore Option 1 and cut and paste the following int othe Custom SQL box:

```
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
```

- Replace 0X000 with the Federation ID provided by Jisc.

- 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 other 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 nongovroam services.

Limitations on logging

Despite being able to delve quite deep into the Clearpass TIPS database (see above) there are limits on what data can be logged. The

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

Permanent link:
https://wiki.govroam.uk/doku.php?id=siteadmin:clearpass_fticks&rev=1715779516

Last update: **2024/05/15 13:25**