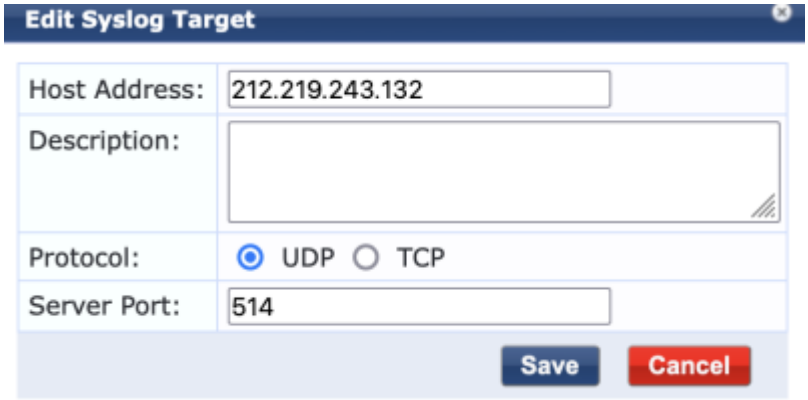
ClearPass FTICKS for Federation Operators only

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

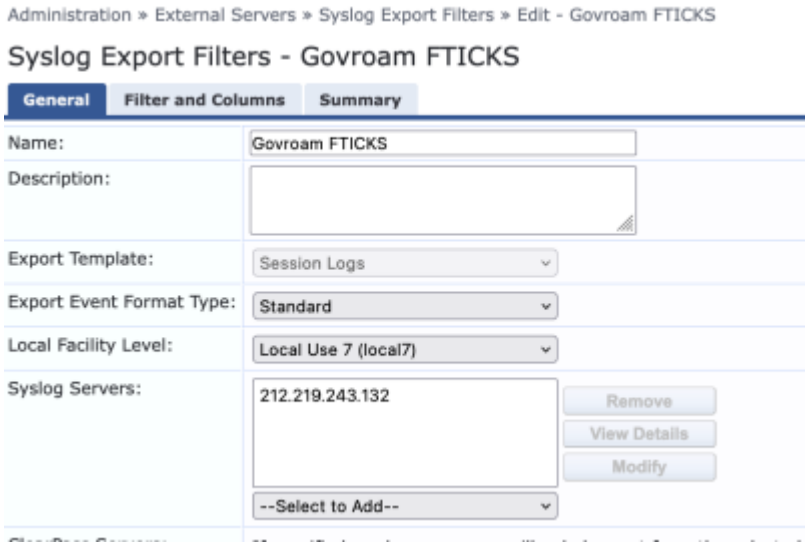
Syslog Targets

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



Syslog Export Filter

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

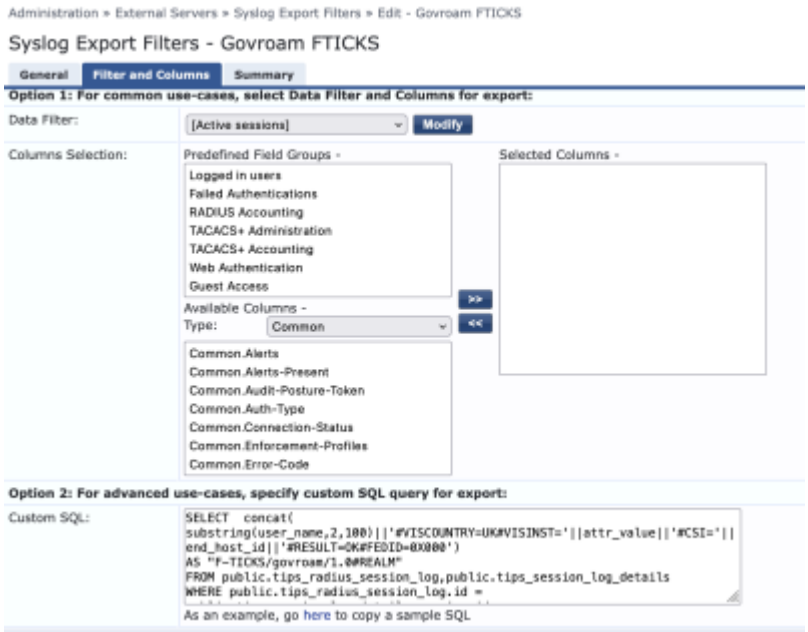


where

- 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:



Ignore Option 1 and cut and paste the following into the Custom SQL box:

```
SELECT  concat(
substring(user_name,2,100)||'#VISCOUNTRY=GB#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 non-govroam services.

SERIOUS LIMITATION

The big caveat with the above is that FTICKS logs will ONLY be generated where there is an Operator-Name variable set in the originating Access Request from the member site. No FTICKS if there isn't. Even if Clearpass inserts an Operator-Name, still no FTICKs logs.

Thus as many as possible of your member sites need to configured their servers to set Operator-Name. This rules out any site using NPS as their ORPS unfortunately.

Limitations on logging

Problem: Not all member organisations can or do set the Operater-Name attribute in their Requests. Ideally the RFO should be able to insert an O-N with a value set on behalf of your site but only some RADIUS servers are capable of doing this (FreeRADIUS, RadSecProxy, RADIATOR). The next best option is to insert a generic value for the Federation. i.e:

When an RFO, scarfolk.gov.uk, gets a request from a site, say arkham.nhs.uk:

1. If the Operator-Name is set to, say, 1arkham.nhs.uk then leave it as is.
2. If the Operator-Name is missing the insert an Operator-Name with the value '1arkham.nhs.uk' no matter which of the several holby,nhs.uk servers the request comes from.
3. If there's no way to set the Operator-Name as in (2) then just insert an Operator-Name of, say, '1scarfolk.gov.uk'.

This way the home site will, at best, see an Operator-Name with the source site's value or, at worst, with it set to the Federation's value.

However, this conditional setting of Operator-Name isn't something found in servers like ClearPass, ISE or NPS. NPS is completely incapable of setting the Operator-Name. ClearPass can't do any sort of conditional setting. ISE might be able to.

With ClearPass you delete and add attributes to the Access Request but you can't conditionally replace or modify them. So the options are to either do nothing, which is what the configuration above does, and not try to add an Operator-Name where missing. Or, to add an Operator-Name with the default value of the RFO. Despite ClearPass allowing database access and has the ability to set and expand variables, there's no way to conditionally set the Operator-Name using the underlying FreeRADIUS variables.

Overwriting the Operator-Name is an option but not a great one. Not only does it meant that sites which do set the Operator-Name will not be able to be identified outside of the Federation, but the FTICKS log won't be generated anyway.