Logging for Cisco ISE

Unfortunately ISE can't generate custom logs in the format required (FTICKS) but, fortunately, it can generate syslog logs with the right information, which can be sent to a syslog server and munged into a suitable format.

This approach assumes that the member sites are configured to include their Operator-Name in RADIUS Requests.

Configuring Cisco ISE

Enabling the Operator-Name attribute

- Go to Policy → Policy Elements → Dictionaries.
- Open up the **System** dropdown.
- Open up the Radius dropdown.
- Click on **IETF**.
- Click on **unknown-126** and enter
 - Attribute Name as 'Operator-Name'
 - Data Type as STRING
 - Direction as IN
- Click Save

cisco	Identity Services Engine	Home	Context Visibility	Operations		+ Administra	tion		0
Policy	Sets Policy Elements								
Diction	naries + Conditions + F	Results							
Die	ctionaries	(م	Dictionaries > > If	ETF > Operator-N	ame				
4	* = *	<u>نې</u>			• 4	ttribute Name	Operator-Name		
	NT-Password-Hash	1		Dictionary Attrib	utes	Description	undefined_attribute_126		
	Operator-Name					* Data Type	STRING *	Enable MAC option	
	Password-Retry					* Direction	IN T		
	 Proxy-State Reply-Message 					* ID	126 (0-255)		
	Route-IPv6-Informa	tion							
	Service-Type					Allow Tagging			
	Session-Timeout		Allow	multiple instances	of this attrib	ute in a profile	V		
	Stateful-IPv6-Addre	iss-Pool	Save Reset						

Logging

This has been done with ISE 2.6 but the principle should apply to other versions.

In Administration \rightarrow System \rightarrow Logging.

In **Remote Logging Targets** create a new Logging Target with the host name of your syslog server.

The Facility Code can be anything but make sure that it matches what the filters expect on the syslog

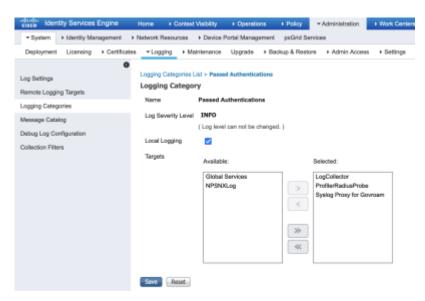
server.

Maximum Length must be set higher than the default because the ISE log line exceeds 1024 bytes and gets split across multiple logs. 2048 seems to be high enough.

Enable Comply to RFC3164

NAME AND ADDRESS OF	en responses recordenant		the serve is seen as providing and in the sec
	 Second spectra contracting to lengths longer 		
Annes (raping Teagers Teagrap (Teagering	1000	Aphing, have in the later	harter shints of
Territory Transport	(marging)		time 🗰 manual (
THE OWNER WATCH	-10.7.000	N.M.M.	
Indexton Trans	14		(with Design" in children)
	Facility Control	1000	
	The other states	100	THE REPORT OF THE
	In case of provide the line for any		
	10000 TT: 100	a .	

In Logging Categories select Passed Authentications and add the new server to the Selected Targets.



Configuring Syslog-NG

Syslog proxies

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 with Facility local6
- 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:

syslog-ng on Linux

```
source s_remote_udp {
  udp();
  unix-stream("/dev/log" max-connections(100));};
};
filter f local0 {
  facility(local0);
};
rewrite r realm {
  subst("@","",value("ISE.UserName"));
};
rewrite r facility 6 {
  set-facility("local6");
};
destination d jisc {
  syslog("212.219.243.132"
        transport("tcp")
        port("601")
        template("F-
TICKS/govroam/1.0#REALM=${ISE.UserName}#VISCOUNTRY=GB#VISINST=${ISE.Operator
-Name}#CSI=${ISE.Calling-Station-ID}#RESULT=OK#FEDID=XXXXX#")
  );
};
log {
        source(s_remote_udp);
        filter(f local0);
        filter{ match("Authentication succeeded" value ("MESSAGE"))};
        parser {
            kv-parser (prefix("ISE."));
        };
        filter{ "${ISE.NetworkDeviceName}" != "NRPS NAME"};
        filter{ "${ISE.SelectedAccessService}" != "NRPS NAME"};
        rewrite(r realm);
        rewrite(r_facility_6);
        destination(d jisc);
};
```

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

Replace **NRPS NAME** with the NRPS name as defined in the *Network Devices* and the *External RADIUS Servers* respectively.

Last update: 2024/05/15 10:20

NXLog on Windows

- Install NXLog CE on Windows
- Use this configuration (with paths changed appropriately)

```
Panic Soft
#NoFreeOnExit TRUE
define ROOT
                C:\Program Files (x86)\nxlog
define CERTDIR %R00T%\cert
define CONFDIR %R00T%\conf
define LOGDIR
                %R00T%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%
Moduledir %R00T%\modules
CacheDir %R00T%\data
Pidfile
          %R00T%\data\nxlog.pid
SpoolDir %R00T%\data
<Extension syslog>
    Module
                xm syslog
</Extension>
<Extension _exec>
    Module
                xm exec
</Extension>
<Input tcp ise>
    Module im tcp
    Host 10.10.10.10
    Port 514
    <Exec>
      if $SyslogFacility != "local6" drop();
      if $raw event !~ /CISE Passed Authentications/ drop();
      $FedID="0X000";
    </Exec>
</Input>
<Output syslog_tls>
    Module
                om ssl
                212.219.243.132
    Host
    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();
```

```
2025/09/16 13:49
```

```
</Output>
```

```
<Output syslog tcp>
    Module
                om tcp
    Host
                212.219.243.132
    Port
                601
    OutputType Syslog_TLS
                to_syslog_ietf();
    Exec
    Exec
                $SyslogFacility = "local6";
</Output>
<Route 1>
    Path
                tcp_ise => syslog_tcp
</Route>
```

- Change 0X000 to the supplied Federation ID.
- Change the 'Host' in 'Input tcp ise' to the address of the ISE host.
- (Ignore the syslog_tls part, that's for future use)
- Restart the Service

Untested Advanced Configuration

There's a limitation to the logging process which might be addressable.

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 'larkham.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.

Conditional Setting of Operator-Name

For each RADIUS Server Sequence dealing with proxying to a member organisation for authentication, go into the Advanced Attribute Settings and enable *Modify attributes in Request to External RADIUS*

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

Last update: 2024/05/15 siteadmin:fticks_logging_for_cisco_ise https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:fticks_logging_for_cisco_ise&rev=1715768419 10:20

ς	۵	n	/	۵	r
-	c			_	

different March	ty Services Engine	litera e Oceate	d Visibility > Operations	. Beiler	- Administration	. West Ourters		
	Identity Management	Home Conte Thetwork Resources	 Hisbility Operations Device Portal Manageme 	Policy nt psGrid Ser	→ Administration	 Work Centers 		
 Network Des 					ADIUS Server Segue	noss.		
	ed Settings							
Strip st	Strip start of subject name up to the first occurrence of the separator							
Strip end of subject name from the last occurrence of the separator								
	▼ Modify Attribute in the request							
Modify attributes in the request to the Enternal RADUS Server								
Update	£	 Radius:Operator-N 	ime 🙄 =	0	hange to: Iscarfolk.	govuk 🚽 🕂		
* Continue to Authorization Policy								
On Access-Accept, continue to Authorization Policy								
 Modify Attribute before access accept 								
Modify attributes before send an Access-Accept								
Add		- Select an item	0 -		+			
Save Res	ant.							

From: https://wiki.govroam.uk/dokuwiki/ - Govroam Permanent link: https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:fticks_logging_for_cisco_ise&rev=1715768419



Last update: 2024/05/15 10:20