Shibboleth IdP - Logipalvelimen käyttö (Keskitetyt logit)

Shibboleth-IdP tukee natiivisti keskitettyä logipalvelua oman F-Tticks toteutuksensa kautta. F-ticks on helppo konfiguroida käyttöön ja logien muotoa voi säädellä vapaasti. Seuraavassa esimerkissä käymme läpi hieman monimutkaisemman konfiguraation joka on toteutettu kahden noodin Shibboleth IdP klusteriin siten että molemmat palvelimet toimivat syslogservereinä, jolloin kummallakin palvelimella on sama sisältö audit logeista.

Käytössä:

- Centos 7.7
- Shibboleth-IdP 3.4.6

F-Ticks

F-ticks tyylisen logituksen voi konfiguroida suoraan Shibboleth-IdP:n konfiguraatio tiedostossa seuraavanlaisesti:

/opt/shibboleth-idp/conf/idp.properties

```
# F-TICKS auditing - set a salt to include hashed username
idp.fticks.federation=<TUNNISTE>
idp.fticks.algorithm=SHA-256
idp.fticks.salt=<SUOLA>
idp.fticks.loghost=<SYSLOG PALVELIN>
idp.fticks.logport=514
```

Pelkästään tämä ei vielä riitä siihen että viestit lähtisivät Syslog serverille, sinun pitää vielä liittää IDP-FTICKS -lisääjä oikeaan loggeriin logback.xml tiedostossa.

/opt/shibboleth-idp/conf/logback.xml

```
<logger name="Shibboleth-Audit" level="ALL">
  <appender-ref ref="${idp.audit.appender:-IDP_AUDIT}"/>
  <appender-ref ref="IDP_FTICKS" />
</logger>
```

Rsyslog

Jos olet pystyttämässä omaa syslog palvelua, muista ottaa käyttöön UDP tai TCP viestien vastaanotto. Jos haluat voi myös edelleen ohjata Shibboleth-Audit viestit omaan tiedostoonsa tai/ja toiseen serveriin, tästä lisää myöhemmin.

/etc/rsyslog.conf

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp.so
#$InputTCPServerRun 514

.
.

#### RULES ####
# Shibboleth-Audit logit omaan tiedostoonsa
:msg, contains, "Shibboleth-Audit"                    /var/log/shibboleth-audit
```

Palomuurit

Kuten Rsyslog kohdasta huomasitkin, käyttää logitus porttia 514 ja riippuen siitä kumpaa lähetysmuotoa käytät (TCP vai UDP), pitää sinun sallia syslog serverin päässä liikenne viestien lähettäjältä porttiin 514 oikealla protokollalla.

- UDP viestit vain lähetetään, mutta viestien perillemenoa ei varmisteta
- TCP viestit lähetetään ja varmistutaan siitä että viesti meni perille.

Kaksi syslog serveriä

Tarvittaessa voit konfiguroida useampia lisääjiä ja lisätä näitä tarvittavan määrän loggeriin. Toinen vaihtoehtoinen tapa on pitää konfiguraatio kuten yllä (Ilman kahta lisääjää) ja käyttää vain lokaalia syslog serveriä jossa toteutetaan logien edelleen lähetys. Seuraavassa esimerkissä teemme lisääjän Shibboleth IdP:hen joka käyttää vakioarvoa (localhost) koska arvoa ei ole määritelty idp.properties fileessä (joka on meidän tapauksessa tarkoituskin).

/opt/shibboleth-idp/conf/logback.xml

```
<appender name="IDP_FTICKS2" class="ch.qos.logback.classic.net.SyslogAppender">
  <syslogHost>${idp.fticks.loghost2:-localhost}</syslogHost>
  <port>${idp.fticks.logport:-514}</port>
  <facility>AUTH</facility>
  <suffixPattern>[%thread] %logger %msg</suffixPattern>
</appender>

<!-- Lisäämme tämän myös edelliseen loggeriin -->

<logger name="Shibboleth-Audit" level="ALL">
  <appender-ref ref="${idp.audit.appender:-IDP_AUDIT}"/>
  <appender-ref ref="IDP_FTICKS" />
  <appender-ref ref="IDP_FTICKS2" />
</logger>
```

Sama esimerkki käyttäen rsyslogia viestien sijoitteluun ja edelleenlähetykseen, yhdellä lisääjäällä (Ilman ylläolevaa konfiguraatiota).

/etc/rsyslog.conf

```
#### RULES ####
# Shibboleth-Audit logit omaan tiedostoonsa
:msg, contains, "Shibboleth-Audit"                      /var/log/shibboleth-audit.log
# Shibboleth-Audit logien edelleen lähetys toiselle syslog serverille.
:msg, contains, "Shibboleth-Audit"                      @<Toinen syslog serveri>

# Vaihtoehtoinen konfiguraatio jos teet logitukset ristiin kahden noden välillä, looppien välttämiseksi
edelleenlähetä vain omat logit, ei muualta tulevia.
#### RULES ####
if $msg contains "Shibboleth-Audit" then {
  /var/log/shibboleth-audit
  if $hostname == "<LOCALHOST>" then @<REMOTE_HOST>
  & stop
}
```