IdP Overview of Log Files

SWITCH

SWITCHaai Team
aai@switch.ch

Apache log files

- `access.log`
  - `aai-login.example.org.access.log`
- `error.log`
  - `aai-login.example.org.error.log`
  - LogLevel in `/etc/apache2/apache2.conf` (default “warn”)

Location: `/var/log/apache2`

Configuration defined in the virtual host definition

- Directory: `/etc/apache2/sites-available/`
- File: `aai-login.example.org.conf`

Tomcat log files

- `catalina.out`
  - Console output (`System.err/out`) from Tomcat
  - Default location: `/var/log/tomcat7/`
  - Configured in `/etc/tomcat7/logging.properties`
- `{catalina,localhost}.YYYY-MM-DD.log`
  - Same as `catalina.out`
- `localhost_access_log.YYYY-MM-DD.txt`
  - Access information associated with a request: IP address, time, request method (GET or POST)
  - Default location: `/var/log/tomcat7/`
  - Configured in `/etc/tomcat7/server.xml`

Shibboleth log files (1)

- Logging framework called “Logback”
- Implementation of SLF4J
- Manual:
  - `http://logback.qos.ch/manual/index.html`
- On-the-fly configuration reloading
  - Change log level without restarting the IdP
  - Reload interval set in `services.properties`
    - entry `idp.service.logging.checkInterval = PT5M`
- Option: send email alerts

Shibboleth log files (2)

- Location: `/opt/shibboleth-idp/logs`
- Four log files produced by default
  - `idp-process.log`: detailed description of the IdP processing requests
  - `idp-warn.log`: only warnings and errors
  - `idp-audit.log`: attribute release auditing records
  - `idp-consent-audit.log`: user decisions over attribute release and terms of use acceptance
- Daily rollover with compression, 6 months history

Shibboleth log files (3)

Configured in `/opt/shibboleth-idp/conf/logback.xml`

- 3 main classes: Logger, Appender (output destination) and Layout
- Default settings usually OK
- Example changes
  - LDAP Auth. Module or authentication events
  - new Logger or Appender…
- Log messages have 5 levels: TRACE, DEBUG, INFO, WARN, ERROR

SMTPAppender in logback.xml

```
<appender name="EMAIL”
    class="ch.qos.logback.classic.net.SMTPAppender">
    <smtpHost>localhost</smtpHost>
    <to>staff1@example.org</to>
    <from>idp_host@example.org</from>
    <subject>TESTING: %logger{20} - %m</subject>
    <layout class="ch.qos.logback.classic.PatternLayout">
      <pattern>%date %-5level %logger{35} - %message%n</pattern>
    </layout>
</appender>

<root level="DEBUG">
    <appender-ref ref="IDP_PROCESS"/>
    <appender-ref ref="IDP_WARN" />
    <appender-ref ref="EMAIL" />
</root>
```

http://logback.qos.ch/manual/appenders.html

Hands On 1

Why is Tomcat not starting up?

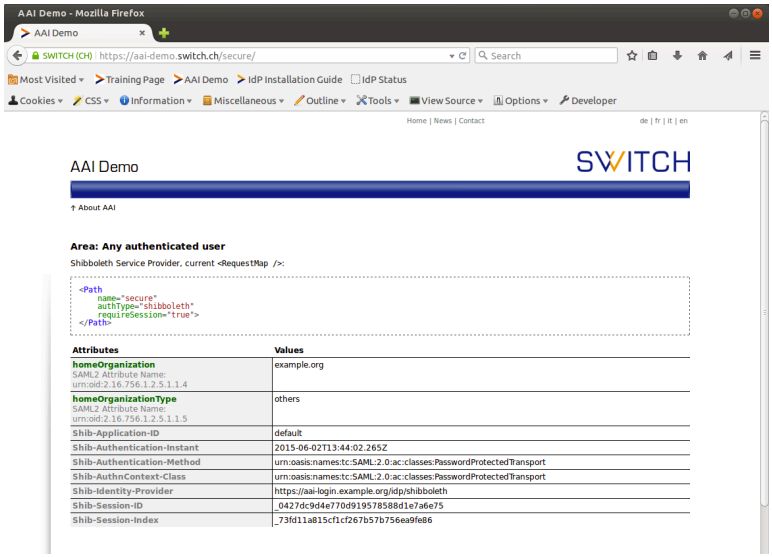
1. Edit `/etc/tomcat7/server.xml` and edit jasper listener in Server Element (wrong class!)

   ```
   <Listener
   className="org.apache.catalina.JasperListener"/>
   ```

2. Restart Tomcat
3. Look at `/var/log/tomcat7/catalina.out`
   - Find the entry `java.lang.ClassNotFoundException`
4. Undo edit jasper listener in `server.xml` and restart Tomcat

Hands On 2

- Find out why not all of the attributes appear



Hands On 2

1. cd `/opt/shibboleth-idp/conf/`
2. Edit `ldap.properties` and insert wrong value:
   Change entry `idp.attribute.resolver.LDAP.searchFilter` to value `(uid=$requestContext.Name)`
3. Edit `logback.xml`:
   - Set log level to DEBUG for logger `org.ldaptive.auth.Authenticator`
   - Insert additional logger for the attribute resolver:
     `<logger name="net.shibboleth.idp.attribute.resolver" level="DEBUG"/>`
4. Restart Tomcat and log in to the IdP (AAI Demo Service)
5. Look at the `idp-process.log` and find the log entries:
   `[org.ldaptive.auth.Authenticator:284]`
   `[net.shibboleth.idp.attribute.resolver.dc.ldap.impl.Template…:203]`
6. Undo wrong value: set `$requestContext.principalName` and restart Tomcat