Shibboleth IdPv4 uppgradering

Introduktion

Uppgraderingen till Shibboleth IdPv4 är lite mer komplicerad än en vanlig uppgradering av Shibboleth. Innan man uppgradera till v4, måste man ha redan anpassat konfigurationsfilerna till den nya versionen.

Om din IdP version är under v3.4 så måste du uppgradera till senaste 3.4 version först. De här instruktionerna är testad på IdPer på version 3.4.6.

Testa först!

Ta en backup eller snapshot innan du påbörjar uppgradering och helst på en test IdP innan du uppgradera din produktion IdP!

Anpassa IdPv3.4.X konfiguration för IdPv4

Du **måste** ha uppdaterat dina konfigurationsfiler (särskilt attribute-resolver.xml och attribute-filter.xml) till att vara kompatibla med IdP v3.4 och v4 **innan** du påbörjar uppgradering. Kontrollera loggfilerna för att säkerställa att inga DEPRECATED varningar förekommer. Alla varningar måste lösas innan uppgradering till v4. De flesta DEPRECATED varningar förekommer på grund av legacy (IdP v2) konfiguration i attribute-resolver och attribute-filter. De nya standard attribute-resolver och attribute-filter filer finns här:

Example of a standard attribute resolver for Shibboleth IdP v4 and above och Example of a standard attribute filter for Shibboleth IdP v3.4.0 and above

Dessa filer uppfyller de nya rekommendationer för entitetskategorier inom SWAMID. Dessa filer kan dock inte användas rakt av. Det är rekommenderat att utgå ifrån dessa filer och "migrerar in" lokala anpassningar från nuvarande konfigurationen, sedan testa så mycket som möjligt - helst på en test IdP. ***Det är rekommenderat att produktionssätta de nya filer ett tag innan uppgraderingen till IdPv4 så man kan säkerställa att attribute resolvern och filtern fungerar som de ska.***

IdPv4 uppgraderingen

Här beskriver vi de steg som har testats och fungerar för SWAMID IdPer som tidigare installerats med hjälp av SWAMIDs idp-installer. Dessa steg är testad på Centos 7.

Centos specifik

IdPv4 kräver Java 11. Avinstallera Java 8 och installera Java 11.

Uppgradera Java version

```
# yum remove java-1.8.0-openjdk-headless java-1.8.0-openjdk
# yum install java-11-openjdk-headless java-11-openjdk
# alternatives --config java
There is 2 program that provides 'java'.

  Selection    Command
-----------------------------------------------
*+ 1           /usr/java/jre1.8.0_151/bin/java
   2           java-11-openjdk.x86_64 (/usr/lib/jvm/java-11-openjdk-11.0.7.10-4.el7_8.x86_64/bin/java)

Enter to keep the current selection[+], or type selection number: 2
```

Debian specifik

IdPv4 kräver Java 11. Avinstallera Java 8 och installera Java 11

Uppgradera Java version

```
# apt remove openjdk-8-jdk-headless
# apt install openjdk-11-jdk-headless
# update-java-alternatives
```

Debian och Centos

Följande steg är samma oavsett om du kör Debian eller Centos. Jetty måste uppgraderas från 9.3 till 9.4.

Jetty

Shibboleth IdP v4 kräver Jetty 9.4 och ganska mycket har ändrats jämfört med 9.3. SWAMID operations har därför paketerat en jetty-base mapp som är anpassad för SWAMID IdPer. Du kan ladda ner den och packa upp i jetty mappen, därefter finns bara några ändringar som du behöver göra. Tar-filen är baserad på en jetty-base som Shibboleth projektet publicerar. Det finns mer information om hur man konfigurerar jetty-base hos Shibboleths Wiki (https://wiki.shibboleth.net/confluence/display/IDP4/Jetty94)

Ladda ner den senaste version av Jetty 9.4. https://www.eclipse.org/jetty/download.html Vid skrivande stund, 9.4.32.v20200930

```
# cd /opt
# wget https://repo1.maven.org/maven2/org/eclipse/jetty/jetty-distribution/9.4.32.v20200930/jetty-distribution-9.4.32.v20200930.zip
# unzip jetty-distribution-9.4.32.v20200930
```

Ladda ner SWAMIDs jetty-base och packa upp: swamid-jetty-base.tar.gz

```
# cd jetty-distribution-9.4.32.v20200930
# tar zxf /path/to/swamid-jetty-base.tar.gz
```

Följande filer i jetty-base behöver kontrolleras och uppdateras:

- alla filer under start.d
  - https.12 och idp-backchannel.p12 hanteras nu i separata filer, kontrollera path till filerna och byta "changeit" till det riktiga lösenordet för keystore-filerna.
  - start.ini kan behöva justeras om du vill ändra hur mycket minne Jetty kan använda

Mer information om jetty-base finns på Shibboleths wiki, https://wiki.shibboleth.net/confluence/display/IDP4/Jetty94

Länka om jetty till rätt distribution mapp. Först måste du se till att Jetty är avstängd.

```
# cd /opt
# chown -R jetty.jetty jetty-distribution-9.4.32.v20200930
# service jetty stop
# rm jetty
# ln -s jetty-distribution-9.4.32.v20200930 jetty
```

Uppdatera /etc/default/jetty. Förutom ändringar till JAVA_HOME, så måste man omdirigera JETTY_START_LOG och JETTY_RUN till lämplig fil resp. mapp. På Centos och Debian så är /var/run (de default mappar) skapat vid boot med fel rättigheter för att Jetty användaren ska kunna skriva till /var/run/jetty.

/etc/default/jetty

```
export JAVA_HOME=/etc/alternatives/jre_11
export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
export JETTY_HOME=/opt/jetty
export JETTY_BASE=/opt/jetty/jetty-base
export JETTY_USER=jetty
export JETTY_START_LOG=/opt/jetty/logs/start.log
export JETTY_RUN=/tmp
```

Kontrollera Jetty start script

```
# cd /etc/init.d
# rm jetty
# ln -s /opt/jetty/bin/jetty.sh jetty
```

Shibboleth IdP v4.X

Ladda ner och packa upp den senaste version av IdP v4, i skrivande stund 4.0.1. Backa upp din shibboleth-idp mapp innan du uppgradera.

```
# cd /opt
# wget http://shibboleth.net/downloads/identity-provider/latest/shibboleth-identity-provider-4.0.1.tar.gz
# tar zxvf shibboleth-identity-provider-4.0.1.tar.gz
# cp -r shibboleth-idp shibboleth-idp.orig
```

Ta bort eventuella gamla jar filer från edit-webapp

Vi har sett att det finns äldre versioner av httpcore, httpclient, commons-dbcp2, commons-pool2 under mapp /opt/shibboleth-idp/edit-webapp/WEB-INF/lib. Om du har dessa jar-filer i /opt/shibboleth-idp/edit-webapp/WEB-INF/lib, ta bort dem. Nyare versioner finns med i Shibboleth IdPv4.

Följande legacy delen av web.xml som idp-installern la till en gång i tiden verkar orsaker problem för nya Jetty. Rekommendationen är att kommentera bort hela security-constraint och login-config som visas nedan (om de finns)

Delar av web.xml som eventuellt behöver kommenteras bort

```
<!-- IdP-installer has appended these settings to the config which uncomments entries documented above -->
<!--
   Uncomment to use container managed authentication. The new servlet spec (3.1)
   supports "**" as a wildcard syntax to avoid role usage, which is normally desirable.
   Older containers usually support "*" when proprietary options are used (e.g., Jetty
   requires setting the Strict property on the SecurityManager.)
   -->
   <security-constraint>
       <display-name>Web Login Service</display-name>
       <web-resource-collection>
           <web-resource-name>user authentication</web-resource-name>
           <url-pattern>/Authn/RemoteUser</url-pattern>
           <url-pattern>/profile/SAML2/SOAP/ECP</url-pattern>
           <http-method>GET</http-method>
           <http-method>POST</http-method>
       </web-resource-collection>
       <auth-constraint>
           <role-name>**</role-name>
       </auth-constraint>
       <user-data-constraint>
           <transport-guarantee>CONFIDENTIAL</transport-guarantee>
       </user-data-constraint>
   </security-constraint>

<!-- Uncomment if you want BASIC auth managed by the container. -->
   <login-config>
       <auth-method>BASIC</auth-method>
       <realm-name>ShibUserPassAuth</realm-name>
   </login-config>
```

MySQL Connector och HikariCP jar-filer

Om du inkluderar andra JAR filer i /opt/shibboleth-idp/edit-webapp/WEB-INF/lib såsom MySQL connector och HikariCP så är det bra att uppgradera dessa till senaste versionen. SWAMID operations har testat med mysql-connector-java-5.1.48-bin.jar och HikariCP-3.4.5.jar.

MySQL Java connector https://dev.mysql.com/downloads/connector/j/5.1.html

HikariCP https://mvnrepository.com/artifact/com.zaxxer/HikariCP

Kontrollera web.xml i edit-webapp/WEB-INF

Vi rekommendera att du jämföra edit-webapp/WEB-INF/web.xml med den version som finns i shibboleth-identity-provider-4.0.1/webapp/WEB-INF. Detta för att kontrollera att din web.xml under edit-webapp är korrekt och aktuell.

Kör uppgradering av Shibboleth:

```
# cd /opt
# rm shibboleth-identity-provider
# ln -s shibboleth-identity-provider-4.0.1 shibboleth-identity-provider
# cd shibboleth-identity-provider
# bin/install.sh
```

Starta Jetty

```
# service jetty start
```

Kontrollera jetty loggar om någonting inte fungerar. Kontrollera sedan idp-process.log för att hitta eventuella problem med IdPn. Testa med https://release-check.swamid.se