旧: Shibboleth IdP Ver2→Ver3へのアップグレード演習

1. はじめに

本メニューでは、IdPをカスタマイズします。
IdP Ver2が正常に起動している環境に対して、Ver3にアップグレードします。
設定ファイルについては、基本的には自動的にコンバートされたものを使用して認証確認まで行います。

---

2. 実習セミナーでは

以下の手順で作業を進めてください。

・Tomcat 6の停止、自動起動設定の停止

```
# service tomcat6 stop
# chkconfig tomcat6 off
```

・Shibboleth Ver2のバックアップ

以下のように/root直下に移動して、念のためバックアップを行います。

```
# cd /root
# tar zcfv shibidp-v2-backup.tar.gz /opt/shibboleth-idp
```

・Tomcat 7のインストール

ShibbolethIdP Ver3はTomcat 6上で使用できないので、Tomcat 7をインストールします。
現在CentOS 6環境のため標準パッケージにはないので、Apache Software Foundationが配布するTomcatパッケージを使用します。
パッケージは、以下のように/root/PKG配下に配置しています。

```
# cd /root/PKG
# mkdir /usr/java
# tar zxv -C /usr/java -f apache-tomcat-7.?.??.tar.gz
# ln -s /usr/java/apache-tomcat-7.?.?? /usr/java/tomcat
```

・起動スクリプトの配置

> ここで使用する /etc/rc.d/init.d/tomcat7 は新規インストール手順で配布しているものと同一です。

```
# unzip tomcat7.zip
# chmod a+x tomcat7
# cp tomcat7 /etc/rc.d/init.d/
```

・"tomcat"ユーザで起動

起動スクリプトを修正し、"tomcat"ユーザで起動するようにします。
以下のように設定します。（/etc/rc.d/init.d/tomcat7）

```
# Remove -XX:MaxPermSize=256m if you are not using Sun/Oracle JVM nor OpenJDK.
export JAVA_OPTS="-server -Xmx1500m -XX:MaxPermSize=256m "
export LANG=en_US.UTF-8
TOMCAT_USER=tomcat
```

また、以下のコマンドでその他Tomcat関連の設定ファイルやディレクトリの所有者、パーミッションを設定します。

```
# chown -R tomcat:tomcat /usr/java/tomcat/{temp,logs,work}
# chown tomcat:tomcat /usr/java/tomcat/webapps
# chmod +t /usr/java/tomcat/webapps
# chgrp tomcat /usr/java/tomcat/conf/*.*
# chmod g+r /usr/java/tomcat/conf/*.*
# mkdir -p /usr/java/tomcat/conf/Catalina/localhost
```

・自動起動の設定

```
# chkconfig --add tomcat7
# chkconfig --level 345 tomcat7 on
# service tomcat7 start
```

・profileの修正

/etc/profileもしくは/etc/profile.d/java-tomcat.shを下記のように修正します。

```
# /etc/profile
JAVA_HOME=/usr/lib/jvm/jre
MANPATH=$MANPATH:$JAVA_HOME/man
CATALINA_HOME=/usr/java/tomcat
CATALINA_BASE=$CATALINA_HOME
PATH=$JAVA_HOME/bin:$CATALINA_HOME/bin:$CATALINA_HOME/bin:$PATH
export PATH JAVA_HOME CATALINA_HOME

# System wide environment and startup programs, for login setup
```

追加した環境変数を読み込みます。

```
 # source /etc/profile
```

・httpdの設定

/etc/httpd/conf.d/virtualhost-localhost80.conf を以下の内容で作成してください。これはShibboleth IdPが提供するreload-metadata.sh等のコマンドを使った操作を可能にするためのものです。

```
<VirtualHost localhost:80>
ProxyPass /idp/ ajp://localhost:8009/idp/
</VirtualHost>
```

・server.xmlの修正

$CATALINA_BASE/conf/server.xmlを下記のように修正します。

他の用途で使用する予定がなければConnector port="8080"をコメントアウトしてください。

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
-->
```

Connector port="8009"に以下のように追加してください。

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
enableLookups="false" tomcatAuthentication="false" address="127.0.0.1" maxPostSize="100000" />
```

・ShibbolethIdP Ver3のインストール

パッケージは、以下のように/root/PKG配下に配置しています。

```
# cd /root/PKG
# unzip shibboleth-identity-provider-3.?.?.zip
# cd shibboleth-identity-provider-3.?.?
# ./bin/install.sh
```

install.shシェルスクリプトを実行すると、以下のような問い合わせがあります。
手順に従って、進めてください。

```
Source (Distribution) Directory: [/root/PKG/shibboleth-identity-provider-3.1.1]
[Enter]  ←入力なし

Installation Directory: [/opt/shibboleth-idp]
[Enter]  ←入力なし

A V2 Installation has been detected. Configuration will be preserved into
.v2 folders and appropriate files copied forward.

Hostname: [ex-idp-test**.gakunin.nii.ac.jp]
[Enter]  ←入力なし
SAML EntityID: [https://ex-idp-test**.gakunin.nii.ac.jp/idp/shibboleth]
[Enter]  ←入力なし
Attribute Scope: [gakunin.nii.ac.jp]
nii.ac.jp[Enter]

Cookie Encryption Key Password: cookiepass[Enter]  ←任意のパスワード
Re-enter password: cookiepass[Enter]  ←任意のパスワード
Warning: /opt/shibboleth-idp/dist does not exist.
 （省略）
Rebuilding /opt/shibboleth-idp/war/idp.war ...
...done

BUILD SUCCESSFUL
```

- The V2 configuration files are copied to a new directory, conf.v2
- The packed V2 warfile is copied to a new directory, war.v2
- The directories logs and metadata are left untouched (note that leaving the latter in place means that new example metadata for the IdP is not generated).
- Specific legacy files that are generally compatible with V3 (attribute-resolver.xml, attribute-filter.xml, relying-party.xml) are pre-populated into the new config directory; these make up the bulk of your older configuration, save for authentication.
- The relying-party.xml file is also copied to metadata-providers.xml
- The rest of the configuration is populated as for a new installation.
- Finally, services.properties is altered to enable a legacy relying party configuration.

・ldap.propertiesの修正

/opt/shibboleth-idp/conf/ldap.propertiesに、参照しているLDAPの情報を設定します。

```
## Connection properties ##
#idp.authn.LDAP.ldapURL = ldap://localhost:10389
idp.authn.LDAP.ldapURL = ldap://localhost
#idp.authn.LDAP.useStartTLS = true
idp.authn.LDAP.useStartTLS = false
 （省略）
#idp.authn.LDAP.baseDN = ou=people,dc=example,dc=org
idp.authn.LDAP.baseDN = o=test_o,dc=ac,c=JP
#idp.authn.LDAP.subtreeSearch = false
idp.authn.LDAP.subtreeSearch = true
 （省略）
#idp.authn.LDAP.bindDN = uid=myservice,ou=system
idp.authn.LDAP.bindDN = cn=olmgr,o=test_o,dc=ac,c=JP
#idp.authn.LDAP.bindDNCredential = myServicePassword
idp.authn.LDAP.bindDNCredential = csildap
```

・Tomcatの設定

Tomcatを”tomcat”ユーザで実行する場合は、ログファイルを出力できるようディレクトリの所有者を変更します。
同様に、設定ファイルやメタデータの保存ディレクトリなどの所有者・パーミッションも変更します。

```
# chown -R tomcat:tomcat /opt/shibboleth-idp/logs
# chgrp -R tomcat /opt/shibboleth-idp/conf
# chmod -R g+r /opt/shibboleth-idp/conf
# chgrp tomcat /opt/shibboleth-idp/metadata
# chmod g+w /opt/shibboleth-idp/metadata
# chmod +t /opt/shibboleth-idp/metadata
# chgrp tomcat /opt/shibboleth-idp/credentials/server.key
# chmod g+r /opt/shibboleth-idp/credentials/server.key
```

・idp.war の登録

${CATALINA_BASE}/conf/Catalina/localhost/idp.xml という新規ファイルを以下の内容で作成し、idp.warをTomcatが認識できるようにします。

```
<Context docBase="/opt/shibboleth-idp/war/idp.war"
         privileged="true"
         antiResourceLocking="false"
         swallowOutput="true" />
```

httpdとTomcatを再起動します。

```
# service tomcat7 stop
# service httpd restart
# service tomcat7 start
```

※画面のカスタマイズ方法はv2から変わっています。views/login.vm等をご参照ください。
参考: GakuNinShare:ロゴの変更

・その他

Tomcat 6は不要になっていますので削除してください。

```
# yum erase tomcat6
```

---

3. 手順書

以下は、英語での情報が記載されたwiki.shibboleth.netのURLです。手順の詳細にご興味がある方はご参照ください。

参考: UpgradingFromV2

なお、実習セミナーでは不要としておりますが、バージョン2でバックチャネルの設定をしていた場合は IdPv3セッティング > Back-Channelの設定 に従って設定してください。

また、バージョン2にuApprove.jp等を入れていた場合は、不要な設定が残っていないかApacheの設定ファイルを確認してください。

参考: [InCommon Wiki] Upgrading to Shibboleth IdP V3

---

4. 動作確認

① 各自が使用するSPの接続確認用ページにアクセスします。

```
例）1番を割り振られた場合
https://ex-sp-test01.gakunin.nii.ac.jp/
```

② ログインボタンをクリックします。

③ DSの所属機関の選択画面が表示されるので、各自が使用するIdPを選択します。

④ Ver3にアップグレードした各自が使用するIdPのログイン画面が表示されることを確認します。（v3ではページ下部にチェックボックスが表示される部分が異なります）

⑤ Username/Passwordを入力して認証を行います。

⑥ 正しく属性受信の確認ページが表示される事を確認してください。

この手順で最低限の動作はしますが、設定ファイルのメンテナンス性が非常に悪く、設定ファイルの不一致により他のページに記載のあるIdPv3に対する手順をそのまま実行することもできません。特に本番運用向けには続けて次の Shibboleth IdP の設定をVer3形式に変換 の手順を実行することをお勧めします。

TOP NEXT