インストール（IdP）

IdPv4のインストール

実習セミナー内に準備されたLinuxサーバにJDK、Jetty、Shibboleth IdPをインストールする手順となっています。

---

1. 実習に使用する仮想サーバについて

以下は本技術ガイドで構築する前提となる環境です。

- OS、DNS、ネットワーク、時刻同期などは設定済みとなっています。（Apache HTTP Server、mod_sslもインストール済み）
- CentOS7
- メモリ2GB以上
- Apache HTTP Server 2.4 と mod_ssl
- Java 11（OpenJDK）
- Jetty 9.4
- Shibboleth IdP v4

また、実習環境ではSELinuxは無効化されているものとして手順を記載しています。下記コマンドでSELinux設定が確認できます。

```
$ /usr/sbin/getenforce
```

---

2. Java 11（OpenJDK）をインストールする

1. インストール

CentOS 7にはOpenJDKのパッケージが用意されていますので、これをyumにてインストールします。

```
# yum install java-11-openjdk-headless
```

---

3. Jetty 9.4 をインストールする

1. インストール

CentOS 7にはJettyのパッケージがないので、ダウンロードしてインストールします。
実習セミナーでは予めダウンロードした「/root/PKG」内の、jetty-distribution-9.4.*.v????????.tar.gz を使います。
さらに、Shibboleth Projectが配布している各種設定ファイル群(jetty-base)を配置します。
こちらも予め「/root/PKG」内に配置してあるものを使用します。

```
# cd /root/PKG
# tar zxv -C /opt -f jetty-distribution-9.4.*.v????????.tar.gz
# ( cd /opt ; ln -s jetty-distribution-9.4.*.v???????? /opt/jetty )

# tar zxv -C /opt -f idp-jetty-base-9.4.?.tar.gz
```

サービス起動は、”jetty”ユーザに設定

"root"ユーザではなく、Jetty起動用のユーザを使用することを推奨します。
ここでは、一般的な "jetty" ユーザを作成します。（以降、"jetty"ユーザを使用する事を前提として説明します。）

```
# groupadd -g 110 jetty
# useradd -u 110 -g jetty -d /opt/jetty-base -s /sbin/nologin -c ”Jetty daemon” jetty
useradd: 警告: ホームディレクトリが既に存在します。
skel ディレクトリからのコピーは行いません。

もしくは、
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
```

（上の手順でディレクトリ作成済みのため警告が出ますが問題ありません）
以下のコマンドでその他 Jetty 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 root:root /opt/jetty-distribution-9.4.*.v???????? /opt/jetty-base
# chmod -R g-w /opt/jetty-base
# chown jetty:jetty /opt/jetty-base/{logs,tmp}
```

自動起動スクリプトは、以下のように作成します。

```
# cp -ip /opt/jetty/bin/jetty.sh /etc/init.d/jetty
# cp -ip /opt/jetty/bin/jetty.service /etc/systemd/system/
```

jetty.serviceについては、コピー後に以下のように[Service]部分を修正します。

```
[Service]
Type=forking
EnvironmentFile=-/etc/sysconfig/jetty
PIDFile=/opt/jetty-base/tmp/jetty.pid
ExecStart=/etc/init.d/jetty start
ExecStop=/etc/init.d/jetty stop
ExecReload=/etc/init.d/jetty restart
SuccessExitStatus=143
User=jetty
Group=jetty
TimeoutStartSec=150
```

以下を実行して、修正した内容を反映させます。

```
# systemctl daemon-reload
```

以下の内容で/etc/sysconfig/jettyを作成します。

```
JAVA=/usr/lib/jvm/jre/bin/java
JETTY_HOME=/opt/jetty
JETTY_BASE=/opt/jetty-base
JETTY_RUN=/opt/jetty-base/tmp
JETTY_STATE=/opt/jetty-base/tmp/jetty.state
JETTY_START_TIMEOUT=120
```

2. 自動起動の設定

以下のコマンドで自動起動設定を有効にします。

```
# systemctl enable jetty

補足：
以下のコマンドで自動起動設定を無効にすることができます。
# systemctl disable jetty
```

3. jetty-baseの設定

以下のように関連する設定ファイルの作成や修正を行います。

/opt/jetty-base/webapps/idp.xml の修正

```
<Configure class="org.eclipse.jetty.webapp.WebAppContext">
<Set name="war"><SystemProperty name="idp.war.path" default="/opt/shibboleth-idp/war/idp.war" /></Set>
<Set name="contextPath"><SystemProperty name="idp.context.path" default="/idp" /></Set>
<Set name="extractWAR">false</Set>
<Set name="copyWebDir">false</Set>
<Set name="copyWebInf">true</Set>
</Configure>
```

/opt/jetty-base/start.d/idp-backchannel.ini を無効化

```
# mv -i /opt/jetty-base/start.d/idp-backchannel.ini /opt/jetty-base/start.d/idp-backchannel.ini.dist
```

/opt/jetty-base/start.d/start.ini の作成

```
# Any other required Jetty modules...

# Allows setting Java system properties (-Dname=value)
# and JVM flags (-X, -XX) in this file
# NOTE: spawns child Java process
--exec

# Uncomment if IdP is installed somewhere other than /opt/shibboleth-idp
#-Didp.home=/path/to/shibboleth-idp

# Newer garbage collector that reduces memory needed for larger metadata files
-XX:+UseG1GC

# Maximum amount of memory that Jetty may use, at least 1.5G is recommended
# for handling larger (> 25M) metadata files but you will need to test on
# your particular metadata configuration
-Xmx1500m

# Prevent blocking for entropy.
-Djava.security.egd=file:/dev/./urandom

# Set Java tmp location
-Djava.io.tmpdir=tmp
```

/opt/jetty-base/start.d/idp.ini の修正

```
# ---------------------------------------
# Module: idp
# Shibboleth IdP
# ---------------------------------------
--module=idp
--module=http
--module=http-forwarded


## Keystore file path (relative to $jetty.base)
jetty.sslContext.keyStorePath=../credentials/idp-userfacing.p12


（省略）

※末尾に以下を追加

## Connector port to listen on
jetty.ssl.port=443    ※利用されない
jetty.http.host=127.0.0.1
jetty.http.port=8080
```

/opt/jetty-base/modules/idp.mod の修正

```
[depend]
annotations
deploy
ext
#https
jsp
jstl
plus
resources
server
servlets
#ssl
```

/opt/jetty-base/etc/tweak-ssl.xml の作成

```
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
"http://www.eclipse.org/jetty/configure_9_4.dtd">
<Configure id="shibContextFactory" class="org.eclipse.jetty.util.ssl.SslContextFactory">
<Set name="IncludeProtocols">
<Array type="String">
<Item>TLSv1.3</Item>
<Item>TLSv1.2</Item>
</Array>
</Set>
<Set name="ExcludeProtocols">
<Array type="String">
<Item>TLSv1.1</Item>
<Item>TLSv1</Item>
<Item>SSL</Item>
<Item>SSLv2</Item>
<Item>SSLv3</Item>
</Array>
</Set>
<Set name="IncludeCipherSuites">
<Array type="String">
<Item>TLS_ECDHE.*</Item>
<Item>TLS_AES.*</Item>
<Item>TLS_RSA.*</Item>
</Array>
</Set>
<Set name="ExcludeCipherSuites">
<Array type="String">
<Item>.*NULL.*</Item>
<Item>.*RC4.*</Item>
<Item>.*MD5.*</Item>
<Item>.*DES.*</Item>
<Item>.*DSS.*</Item>
<Item>TLS_DHE.*</Item>
</Array>
</Set>
</Configure>
```

上記ファイルを参照するように /opt/jetty-base/modules/idp-backchannel.mod に追記します。

```
（省略）

[xml]
etc/idp-backchannel.xml
etc/tweak-ssl.xml
```

4. httpd の設定

以下のように設定ファイルの修正を行います。

/etc/httpd/conf/httpd.conf の修正

```
（省略）
#ServerName ex-idp-test??.gakunin.nii.ac.jp:80　← ??は各自割り振られた番番号（0番なら「00」）
↑コメントアウト（#）を削除
（省略）
```

/etc/httpd/conf.d/ssl.conf の修正

```
（省略）
<VirtualHost _default_:443>
（省略）
#ServerName ex-idp-test??.gakunin.nii.ac.jp:443　← ??は各自割り振られた番号（0番なら「00」）
↑コメントアウト（#）を削除
↓以下を追加
RequestHeader set X-Forwarded-Port 443
RequestHeader set X-Forwarded-Proto https
RequestHeader unset Forwarded
RequestHeader unset X-Forwarded-For
ProxyPass /idp/ http://localhost:8080/idp/ connectiontimeout=5 timeout=15
（省略）
```

/etc/httpd/conf.d/virtualhost-localhost80.conf の作成

※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/ http://localhost:8080/idp/ connectiontimeout=5 timeout=15
</VirtualHost>
```

---

4. Shibbolethのインストール

各ファイル名等の指定は，Version 4.2.1に準拠しています。

1. インストール

Shibboleth IdPのパッケージは、「/root/PKG」配下にあります。

以下のコマンドで移動してください。

```
# cd /root/PKG
```

shibboleth-identity-provider-4.?.?.tar.gz がすでに配置されているので、以下のコマンドを実行してください。

```
# tar xzvf shibboleth-identity-provider-4.?.?.tar.gz
# cd shibboleth-identity-provider-4.?.?
# ./bin/install.sh -Didp.conf.credentials.filemode=640 -Didp.conf.credentials.group=jetty
```

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。

> ⚠ インストール時に入力するパスワードを本運用で使う場合は、推測されにくいものを使用してください。
> ※ここで入力したパスワードは、/opt/shibboleth-idp/credentials/secrets.propertiesに記載されます。（平文）（cookiepassのほう）
> ※backpassのほうは記載されません。/opt/shibboleth-idp/credentials/idp-backchannel.p12の暗号化のために使用されます。（本技術ガイドではidp-backchannel.p12を使用しません）

```
Buildfile: /root/PKG/shibboleth-identity-provider-4.2.1/bin/build.xml

install:
Source (Distribution) Directory (press <enter> to accept default): [/root/PKG/shibboleth-identity-provider-4.3.1] ?
[Enter]  ←入力なし

Installation Directory: [/opt/shibboleth-idp] ?
[Enter]  ←入力なし
New Install. Version: 4.3.1
Hostname: [ip-??-?-?-???.ap-northeast-1.compute.internal]
ex-idp-test??.gakunin.nii.ac.jp[Enter]  ←??は各自割り振られた番号（0番なら「00」）
  （省略）
Backchannel PKCS12 Password: backpass[Enter]  ←任意のパスワード（不使用）

Re-enter password: backpass[Enter]

  （省略）
Cookie Encryption Key Password: cookiepass[Enter]  ←任意のパスワード（内部で使用）
Re-enter password: cookiepass[Enter]
  （省略）
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]  ←nii.ac.jpを設定してください。

  （省略）

BUILD SUCCESSFUL

  （省略）
```

上記のような質問に答えながら、インストールを行います。

2. パーミッションの調整

Jettyは、”jetty”ユーザで実行しているので、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 jetty:jetty /opt/shibboleth-idp/logs
# chgrp jetty /opt/shibboleth-idp/metadata
# chmod g+w /opt/shibboleth-idp/metadata
# chmod +t /opt/shibboleth-idp/metadata
```

IdPが実際に使用する証明書の秘密鍵はまだ配置されておりませんので、所有者・パーミッションは後の手順で設定します。

3. jstl-1.2.jar の配置

※jstlの別途インストールは不要

4. ディレクトリインデックスの禁止

edit-webapp内にweb.xml を作成します。

```
# cp -ip /opt/shibboleth-idp/dist/webapp/WEB-INF/web.xml /opt/shibboleth-idp/edit-webapp/WEB-INF/web.xml
# chmod u+w /opt/shibboleth-idp/edit-webapp/WEB-INF/web.xml
```

作成したweb.xml を以下の内容で修正します。

※既存の<servlet>の前に設定を追加します。

```
<filter-mapping>
<filter-name>SLF4JMDCServletFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>

<!-- Servlets and servlet mappings -->
<servlet>
<servlet-name>default</servlet-name>
<servlet-class>org.eclipse.jetty.servlet.DefaultServlet</servlet-class>
<init-param>
<param-name>dirAllowed</param-name>
<param-value>false</param-value>
</init-param>
<load-on-startup>0</load-on-startup>
</servlet>

<servlet>
<servlet-name>idp</servlet-name>
```

以下を実行して反映させます。

```
# /opt/shibboleth-idp/bin/build.sh
```

build.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。

```
Buildfile: /opt/shibboleth-idp/bin/build.xml

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


Rebuilding /opt/shibboleth-idp/war/idp.war, Version 4.3.1
Initial populate from /opt/shibboleth-idp/dist/webapp to /opt/shibboleth-idp/webpapp.tmp
Overlay from /opt/shibboleth-idp/edit-webapp to /opt/shibboleth-idp/webpapp.tmp
Creating war file /opt/shibboleth-idp/war/idp.war


BUILD SUCCESSFUL

 （省略）
```

httpdの再起動とJettyの起動を行います。（すでにJettyが起動している場合はstopしてから行ってください）

```
# systemctl restart httpd
# systemctl start jetty
```

⚠ Jettyに関する注意事項

- jetty起動に失敗したら設定修正後、/opt/jetty-base/tmp/下にファイルが残っていたら削除してから再度起動してください。
- build.shしたら sudo systemctl restart jetty しないと反映されません。

---

5. サービスの起動・停止方法

サービス	起動コマンド	停止コマンド	再起動コマンド
httpd	systemctl start httpd	systemctl stop httpd	systemctl restart httpd
jetty	systemctl start jetty	systemctl stop jetty	systemctl restart jetty

インストールが完了したら，サイト情報等の設定を行って下さい．