StoredID

Shibboleth IdPでStoredIDを利用するための設定方法(MySQL)

StoredIDは eduPersonTargetedID (ePTID)を生成する方法の一つです。 ComputedIDと比較して、以下の利点があります。

- 使用中のePTIDを失効させ新しいIDを再生成できる
- 万が一のSHA-1のコリジョンを防ぐことができる
- インシデント発生時に、IdP側でePTIDから個人を特定するのが容易である

目次

データベースの設定方法やePTIDの送信方法については以下にも情報がありますので、適宜参照してください。

- GakuNinShare:Shibboleth IdP 3 - NameID設定 のstoredIdの項
- GakuNinShare:Shibboleth IdP 3 - eduPersonTargetedID属性の送信

1. データベース(MariaDB)のインストール

MariaDB をインストールし初期設定を行います。
以下のコマンドを実行してmariadbの自動起動の設定及びMariaDBのrootパスワードの設定を実施してください。

```
# yum install mariadb mariadb-server
# systemctl enable mariadb ← 自動起動を設定
# systemctl start mariadb
# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none): ← そのままEnter入力
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] ← rootパスワードを設定
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] ← そのままEnter入力
... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] ← そのままEnter入力
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] ← そのままEnter入力
 - Dropping test database...
... Success!
 - Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] ← そのままEnter入力
... Success!

Cleaning up...



All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

2. データベースにテーブルを作成する

MariaDB上にデータベース shibboleth を作成し、テーブル shibpid を追加します。

```
# mysql -u root -p
Enter password: ← 設定したrootパスワードを入力
Welcome to the MariaDB monitor.  Commands end with ; or ¥g.
Your MariaDB connection id is 46
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '¥h' for help. Type '¥c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE shibboleth;
MariaDB [(none)]> CONNECT shibboleth
MariaDB [shibboleth]> CREATE TABLE shibpid (
    localEntity VARCHAR(255) NOT NULL,
    peerEntity VARCHAR(255) NOT NULL,
    persistentId VARCHAR(50) NOT NULL,
    principalName VARCHAR(50) NOT NULL,
    localId VARCHAR(50) NOT NULL,
    peerProvidedId VARCHAR(50) NULL,
    creationDate TIMESTAMP NOT NULL,
    deactivationDate TIMESTAMP NULL,
    PRIMARY KEY (localEntity, peerEntity, persistentId)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

また、テーブル shibpid にアクセスするためのデータベースユーザを新規作成します。

```
MariaDB [shibboleth]> CREATE USER 'データベースユーザ名'@'localhost' IDENTIFIED BY 'データベースパスワード';
MariaDB [shibboleth]> GRANT INSERT, SELECT, UPDATE, DELETE ON shibboleth.* TO 'データベースユーザ名'@'localhost';
MariaDB [shibboleth]> FLUSH PRIVILEGES;
MariaDB [shibboleth]> quit
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

---

3. JDBCドライバー(mysql-connector-javaパッケージ)をインストールする

以下のコマンドでMariaDB向けJDBCドライバーMySQL Connector/J（mysql-connector-javaパッケージ）をインストールしてください。

```
# yum install mysql-connector-java
```

JARファイルは /usr/share/java/mysql-connector-java.jar にインストールされているので、 edit-webapp/WEB-INF/lib/ にシンボリックリンクを作成したあとビルドスクリプトを実行しidp.warを再生成します。

```
# ln -s /usr/share/java/mysql-connector-java.jar /opt/shibboleth-idp/edit-webapp/WEB-INF/lib/
# /opt/shibboleth-idp/bin/build.sh
Installation Directory: [/opt/shibboleth-idp]
[Enter]  ←入力なし
Rebuilding /opt/shibboleth-idp/war/idp.war ...
...done

BUILD SUCCESSFUL
Total time: 3 seconds
```

mysql-connector-javaインストール時にJava8がインストールされ、Java11ではなくJava8が利用されている可能性があります。
以下のように確認し、Java8が選択されていたらJava11を利用するように切り替えてください。

```
# alternatives --config java

There are 2 programs which provide 'java'.

Selection Command
-----------------------------------------------
1 java-11-openjdk.x86_64 (/usr/lib/jvm/java-11-openjdk-11.0.8.10-0.el7_8.x86_64/bin/java)
*+ 2 java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.262.b10-0.el7_8.x86_64/jre/bin/java)

Enter to keep the current selection[+], or type selection number: 1[Enter] ← Java11が表示されている「1」を選択
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

mysql-connector-javaパッケージを更新した場合は再度ビルドスクリプトを実行してください。

---

4. /opt/shibboleth-idp/conf/global.xml を修正する

/opt/shibboleth-idp/conf/global.xmlでbean MyDataSourceを定義します。

```
    <!-- Use this file to define any custom beans needed globally. -->
    <!-- A DataSource bean suitable for use in the idp.persistentId.dataSource property. -->
    <bean id="MyDataSource"
          class="org.apache.commons.dbcp2.BasicDataSource"
          p:driverClassName="com.mysql.jdbc.Driver"
          p:url="jdbc:mysql://localhost:3306/shibboleth"
          p:username="データベースユーザー名"
          p:password="データベースパスワード"
          p:maxTotal="10"
          p:maxIdle="5"
          p:maxWaitMillis="15000"
          p:testOnBorrow="true"
          p:validationQuery="select 1"
          p:validationQueryTimeout="5" />

    <!--
    Algorithm whitelists and blacklists that override or merge with library defaults. Normally you can leave
    these empty or commented and use the system defaults, but you can override those defaults using these lists.
    Each <value> element is an algorithm URI, or you can use <util:constant> elements in place of literal values.
    -->
```

global.xml ファイルのパーミッションを設定します。

```
# chgrp jetty /opt/shibboleth-idp/conf/global.xml
# chmod 640 /opt/shibboleth-idp/conf/global.xml
```

---

5. /opt/shibboleth-idp/conf/saml-nameid.properties を修正する

idp.persistentId.sourceAttribute, idp.persistentId.salt, idp.persistentId.generatorとidp.persistentId.storeを設定します。
idp.persistentId.saltには他人が推測できないランダムな値を指定してください。古いIdPから設定を引き継ぐ場合は同じ値を指定してください。

すでにComputedIDを使用している場合はsourceAttributeとsaltは設定されているはずですので、後ろ2つを設定してください。

```
# For computed IDs, set a source attribute and a secret salt:
idp.persistentId.sourceAttribute = uid  ← アンコメントして修正
#idp.persistentId.useUnfilteredAttributes = true
# Do *NOT* share the salt with other people, it's like divulging your private key.
#idp.persistentId.algorithm = SHA
idp.persistentId.salt = XXXXXXXXXXXXXXX   ← アンコメントして修正

# To use a database, use shibboleth.StoredPersistentIdGenerator
idp.persistentId.generator = shibboleth.StoredPersistentIdGenerator   ← アンコメントして修正
# For basic use, set this to a JDBC DataSource bean name:
idp.persistentId.dataSource = MyDataSource  ← アンコメントして修正
# For advanced use, set to a bean inherited from shibboleth.JDBCPersistentIdStore
#idp.persistentId.store = MyPersistentIdStore
```

---

6. /opt/shibboleth-idp/conf/attribute-resolver.xml を修正する

storedID 用の id="eduPersonTargetedID" の AttributeDefinition と DataConnector をアンコメントします。その際、computedID 用のものがアンコメントされている場合はコメントアウトします。

```
(省略)
    <!-- Attribute Definition for eduPersonTargetedID (computedID) -->
    <!--
    <resolver:AttributeDefinition xsi:type="ad:SAML2NameID" id="eduPersonTargetedID" nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent" sourceAttributeID="computedID">
        <resolver:Dependency ref="computedID" />
        <resolver:AttributeEncoder xsi:type="enc:SAML1XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" encodeType="false" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="
eduPersonTargetedID" encodeType="false" />
    </resolver:AttributeDefinition>
    --> ← コメントアウト
    <!-- Pseudo Attribute Definition for %{idp.persistentId.sourceAttribute} -->
    <!--
        Uncomment this if there is an attribute named %{idp.persistentId.sourceAttribute}
        only on LDAP and you don't already have an Attribute Definition for it.
    -->
    <!--
    <resolver:AttributeDefinition id="%{idp.persistentId.sourceAttribute}" xsi:type="ad:Simple" sourceAttributeID="%{idp.persistentId.
sourceAttribute}">
        <resolver:Dependency ref="myLDAP" />
    </resolver:AttributeDefinition>
    --> ← コメントアウト
    <!-- Computed targeted ID connector -->
    <!--
    <resolver:DataConnector id="computedID" xsi:type="dc:ComputedId"
                            generatedAttributeID="computedID"
                            sourceAttributeID="%{idp.persistentId.sourceAttribute}"
                            salt="%{idp.persistentId.salt}">
        <resolver:Dependency ref="%{idp.persistentId.sourceAttribute}" />
    </resolver:DataConnector>
    --> ← コメントアウト

    <!-- Attribute Definition for eduPersonTargetedID (storedID) -->
    <!-- --> ← アンコメント
    <resolver:AttributeDefinition xsi:type="ad:SAML2NameID" id="eduPersonTargetedID" nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent" sourceAttributeID="storedID">
        <resolver:Dependency ref="storedID" />
        <resolver:AttributeEncoder xsi:type="enc:SAML1XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" encodeType="false" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="
eduPersonTargetedID" encodeType="false" />
    </resolver:AttributeDefinition>
    <!-- --> ← アンコメント
    <!-- Pseudo Attribute Definition for %{idp.persistentId.sourceAttribute} -->
    <!--
        Uncomment this if there is an attribute named %{idp.persistentId.sourceAttribute}
        only on LDAP and you don't already have an Attribute Definition for it.
    -->
    <!-- --> ← アンコメント(idp.persistentId.sourceAttributeで指定した属性がLDAPで定義されているのみで、attribute-resolver.xmlに対応
するresolver:AttributeDefinitionが存在しない場合)
    <resolver:AttributeDefinition id="%{idp.persistentId.sourceAttribute}" xsi:type="ad:Simple" sourceAttributeID="%{idp.persistentId.
sourceAttribute}">
        <resolver:Dependency ref="myLDAP" />
    </resolver:AttributeDefinition>
    <!-- --> ← アンコメント(idp.persistentId.sourceAttributeで指定した属性がLDAPで定義されているのみで、attribute-resolver.xmlに対応
するresolver:AttributeDefinitionが存在しない場合)
    <!-- Stored targeted ID connector -->
(省略)
    <!-- --> ← アンコメント
    <resolver:DataConnector id="storedID" xsi:type="dc:StoredId"
                            generatedAttributeID="storedID"
                            sourceAttributeID="%{idp.persistentId.sourceAttribute}"
                            salt="%{idp.persistentId.salt}">
        <resolver:Dependency ref="%{idp.persistentId.sourceAttribute}" />
        <dc:BeanManagedConnection>MyDataSource</dc:BeanManagedConnection>
    </resolver:DataConnector>
    <!-- --> ← アンコメント
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

---

7. Jettyを再起動する

すべての作業が終わりましたらJettyを再起動してください。