

LDAPにエントリがない場合にIdP上でエラーにする方法

概要

Shibboleth IdPにおいて、属性の生成手段としてLDAPサーバを参照する方法がありますが、LDAPサーバにエントリが存在しない場合の挙動について注意が必要です。Shibboleth IdPのデフォルト設定における挙動は以下の通りです。

- LDAPにエントリが存在しない場合も処理は中断しない
- SPに向けて空の属性が送信される

SP側に属性を送信する前にIdP上でエラーにするには、ここで紹介する設定が必要になります。同時に、Template AttributeDefinitionなど他の要因でエラーが発生した場合もIdP上でエラーとなります。現在の運用でエラーが発生していないことをログにより確認しておいてください。

前提条件

- [Shibboleth IdP 3.3.x向けテンプレート](#) (3.3.0以降)のattribute-resolver.xmlを使用していること
LDAP DataConnectorに以下のような設定が含まれます。

```
noResultIsError="%{idp.attribute.resolver.LDAP.noResultIsError:true}"
```

設定方法

- services.properties

idp.service.attribute.resolver.maskFailuresの値をfalseに変更します。

conf/services.properties

```
idp.service.attribute.resolver.maskFailures = false
```

差分

```
#idp.service.attribute.resolver.resources = shibboleth.AttributeResolverResources
#idp.service.attribute.resolver.failFast = false
idp.service.attribute.resolver.checkInterval = PT15M
-#idp.service.attribute.resolver.maskFailures = true
+idp.service.attribute.resolver.maskFailures = false

#idp.service.attribute.filter.resources = shibboleth.AttributeFilterResources
# NOTE: Failing the filter fast leaves no filters enabled.
```

- errors.xml

IdP上でエラーとするため、<util:map id="shibboleth.LocalEventMap">の子要素として以下の要素を追加します。

conf/services.properties

```
<entry key="UnableToResolveAttributes" value="true"/>
```

差分

```
<util:map id="shibboleth.LocalEventMap">
  <entry key="ContextCheckDenied" value="true" />
  <entry key="AttributeReleaseRejected" value="true" />
  <entry key="TermsRejected" value="true" />
  <entry key="RuntimeException" value="false" />
+  <entry key="UnableToResolveAttributes" value="true"/>
  <!--
  <entry key="IdentitySwitch" value="false" />
  <entry key="NoPotentialFlow" value="false" />
  -->
</util:map>
```

確認方法

aacli.shで設定が正しいか確認することができます。

- LDAPにエントリ(ユーザ)が存在しない場合

```
$ /opt/shibboleth-idp/bin/aacli.sh -n user1 -r https://sp.example.ac.jp/shibboleth-sp
{ "error": "UnableToResolveAttributes" }
```

- LDAPにエントリ(ユーザ)が存在する場合

```
$ /opt/shibboleth-idp/bin/aacli.sh -n user1 -r https://sp.example.ac.jp/shibboleth-sp
{
  "requester": "https://sp.example.ac.jp/shibboleth-sp",
  "principal": "user1",
  "attributes": [

    {
      "name": "eduPersonPrincipalName",
      "values": [
        "ScopedStringAttributeValue{value=user1, scope=example.ac.jp}"
      ]
    }
  ]
}
```