# Shibboleth与apache如何结合实现访问控制

## 一、shibboleth

### 1. Shibboleth 系统组件

Shibboleth系统由身份提供者（identity provider，IdP）、服务提供者（service provider，SP）以及可选的服务发现者（discovery service，DS）所组成

* **IdP**

IdP主要负责用户的认证和用户属性的传递，并在SP生成认证请求时，生成认证应答，该应答连同用户属性将会被一起传递给SP。IdP本身并不存储用户信息，而依赖于目录服务存储用户信息。

* **SP**

SP主要负责管理被保护的资源，并根据IdP传递过来的认证应答和用户属性执行访问控制。

* **OpenLDAP**

IdP的运行还需要目录服务的支持。IdP本身并不存储用户信息，而是需要借助外部的目录服务来进行存储用户信息

* **DS**

DS主要负责IdP的发现，并在SP生成认证请求时，提供可以选择的IdP列表。它是一个可选择的组件。主要应用在多IdP的环境下。



1. 用户访问被SP保护的资源
2. SP生成认证请求，并把用户重定向到DS
3. 用户重定向到DS
4. 用户选择IdP，认证请求被重定向到用户所选择的IdP
5. 用户重定向到所选择的IdP进行认证
6. IdP根据用户提供的信息生成认证应答
7. SP根据收到的认证应答来进行访问控制

在整个架构中，SP生成认证请求、IdP生成认证应答、IdP传递给SP用户属性。

### 2. Shibboleth中的访问控制

Shibboleth中的访问控制**由SP进行**。SP根据IDP传递过来的属性进行访问控制，访问控制语句可以直接写在SP的配置文件中，也可以写在单独的xml文件中，在需要的地方引用。

访问控制语句的逻辑语法比较简单，只有<AND>，<OR>，<NOT>三种逻辑。

例如：

对sp1.ecnu.edu.cn/TestShib这个资源的访问控制权限为：只有ou为LIB且title为admin的用户才可以访问。相应的访问控制语句就可以写成：

<AND>

<Rule require=”ou” >LIB</Rule>

<NOT>

<Rule require=”title”>user</Rule>

</NOT>

</AND>