第一章：Shiro 的简介

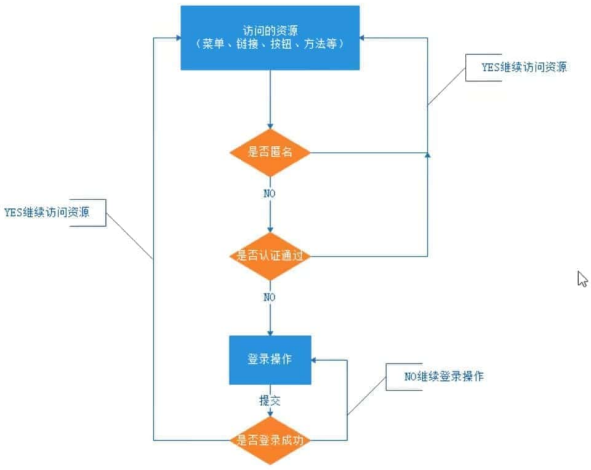
一、权限的相关概念

(一) 权限管理

权限管理的概念：根据系统设置的安全策略，用户只能访问自己被授权的资源。权限管理一般包括访问权限和数据权限

(二) 认证

1. 认证的概念：判断用户是否为合法用户的过程
2. 认证流程



3. 关键对象

Subject：主体：访问系统的用户，主体可以是用户、程序等，进行认证的都称为主体；

Principal：身份信息是主体（subject）进行身份认证的标识，标识必须具有唯一性，如用户名、手机号、邮箱地址等，一个主体可以有多个身份，但是必须有一个主身份（Primary Principal）。

credential：凭证信息：是只有主体自己知道的安全信息，如密码、证书等。

(三) 授权

1. 授权的概念：访问控制

授权，即访问控制，控制谁能访问哪些资源。主体进行身份认证后，系统会为其分配对应的权限，当访问资源时，会校验其是否有访问此资源的权限。

这里首先理解4个对象。

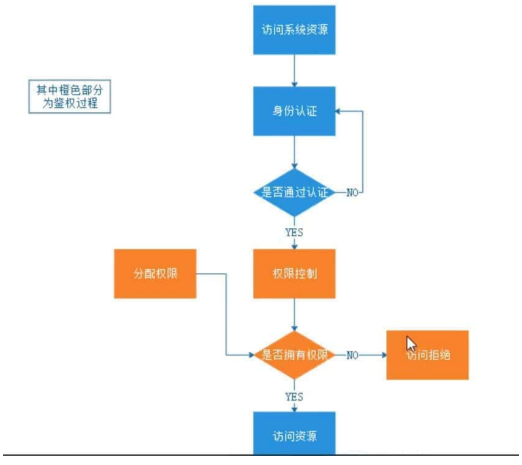
用户对象user：当前操作的用户、程序。

资源对象resource：当前被访问的对象

角色对象role：一组"权限操作许可权"的集合。

权限对象permission：权限操作许可权

2. 授权流程



3. 关键对象

授权可简单理解为who对what进行How操作

Who： 主体（Subject），可以是一个用户、也可以是一个程序

What： 资源（Resource），如系统菜单、页面、按钮、方法、系统商品信息等。

访问类型：商品菜单，订单菜单、分销商菜单

数据类型：我的商品，我的订单，我的评价

How： 权限许可（Permission）

我的商品（资源）===>访问我的商品(权限许可)

分销商菜单（资源）===》访问分销商列表（权限许可）

二、Shiro 的简介

1. 介绍：一种通用的安全认证框架

Shiro是apache旗下一个开源框架，它将软件系统的安全认证相关的功能抽取出来，实现用户身份认证，权限授权、加密、会话管理等功能，组成了一个通用的安全认证框架。

2. 特点

Shiro 是一个强大而灵活的开源安全框架，能够非常清晰的处理认证、授权、管理会话以及密码加密。如下是它所具有的特点：

· 易于理解的 Java Security API；

· 简单的身份认证（登录），支持多种数据源（LDAP，JDBC 等）；

· 对角色的简单的签权（访问控制），也支持细粒度的鉴权；

· 支持一级缓存，以提升应用程序的性能；

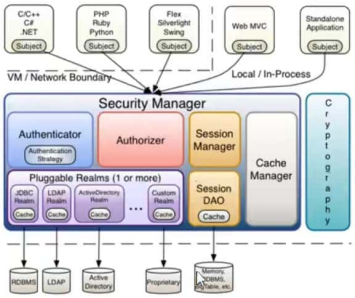
· 内置的基于 POJO 企业会话管理，适用于 Web 以及非 Web 的环境；

· 异构客户端会话访问；

· 非常简单的加密 API；

· 不跟任何的框架或者容器捆绑，可以独立运行。

3. 架构



- Subject

Subject主体，外部应用与subject进行交互，subject将用户作为当前操作的主体，这个主体：可以是一个通过浏览器请求的用户，也可能是一个运行的程序。Subject在shiro中是一个接口，接口中定义了很多认证授相关的方法，外部程序通过subject进行认证授，而subject是通过SecurityManager安全管理器进行认证授权

- SecurityManager

SecurityManager权限管理器，它是shiro的核心，负责对所有的subject进行安全管理。通过SecurityManager可以完成subject的认证、授权等，SecurityManager是通过Authenticator进行认证，通过Authorizer进行授权，通过SessionManager进行会话管理等。SecurityManager是一个接口，继承了Authenticator，Authorizer，SessionManager这三个接口

- Authenticator

Authenticator即认证器，对用户登录时进行身份认证

- Authorizer

Authorizer授权器，用户通过认证器认证通过，在访问功能时需要通过授权器判断用户是否有此功能的操作权限。

- Realm（数据库读取+认证功能+授权功能实现）

Realm领域，相当于datasource数据源，securityManager进行安全认证需要通过Realm获取用户权限数据
比如：
如果用户身份数据在数据库那么realm就需要从数据库获取用户身份信息。
注意：
不要把realm理解成只是从数据源取数据，在realm中还有认证授权校验的相关的代码。

- SessionManager

SessionManager会话管理，shiro框架定义了一套会话管理，它不依赖web容器的session，所以shiro可以使用在非web应用上，也可以将分布式应用的会话集中在一点管理，此特性可使它实现单点登录。

- SessionDAO

properties

SessionDAO即会话dao，是对session会话操作的一套接口
比如：
可以通过jdbc将会话存储到数据库
也可以把session存储到缓存服务器