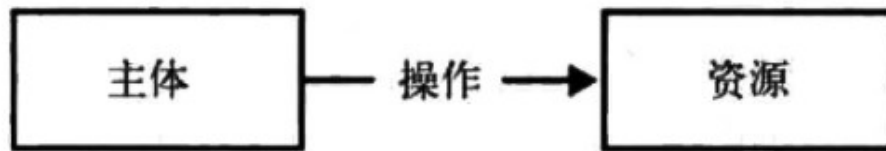


ASP.NET Core 基于策略的授权

2018年12月30日 15:06

■ 理解授权的过程



身份认证的目的是确定用户的身份主体（你是谁?），而授权是针对身份主体分配资源的操作权限(能干什么)。

■ 三要素的含义

主体：客户端身份（就声明的用户）

操作：增删改查

资源：HTTP资源（图片，JSON，用户，订单）

■ 授权过程

策略、决定和执行。

下面是一条授权策略示例：

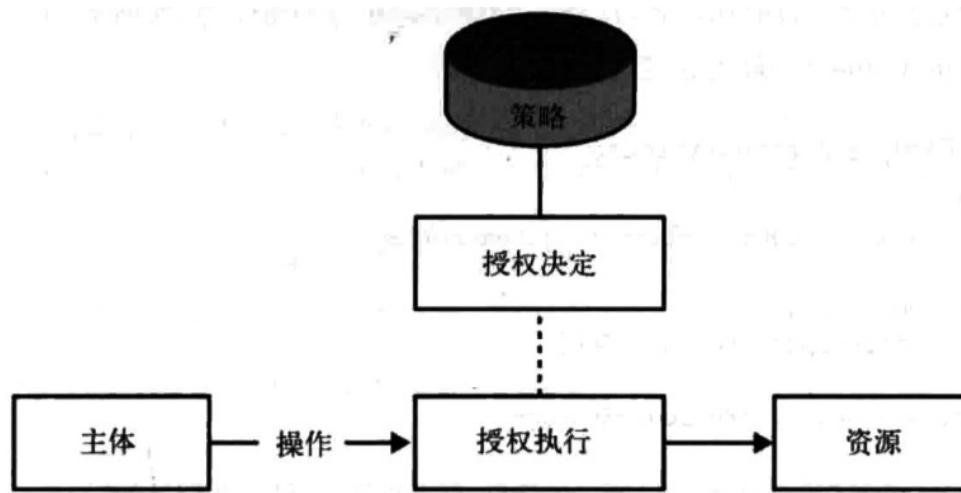
匿名用户不能查询订单

零度群资料只能由群主修改。

零度会员才能观看视频

授权决定是一个过程，主要是衡量一个由（主体，操作和资源）三元组定义的访问是否符合授权策略。

授权执行，拦截本次操作只确保执行有权限的资源。



在分布式系统中：授权决定和授权执行可能在不同的节点服务器上，比如OAuth2.0框架，可以在外部服务器进行授权决定，让资源服务器授权执行。

Microsoft.AspNetCore.Authorization

来自 <<https://github.com/aspnet/Security/tree/master/src/Microsoft.AspNetCore.Authorization>>

Microsoft.AspNetCore.Authorization.Policy

来自 <<https://github.com/aspnet/Security/tree/master/src/Microsoft.AspNetCore.Authorization.Policy>>