auth添加权限判断接口功能，结合主机名（ip）和角色权限区域权限（专业权限），判断用户是否拥有某种权限

|  |  |  |
| --- | --- | --- |
| Interface: | /checkaojprivilege |  |
| Request Json: | {" tokenid ": "" ,"aojid":1,"aojsupervision":[]} | "aojsupervision"数组 |
| Response Json: | {"result":,"errorinfo":"","typeurl":"checkaojprivilege"} | 200：有权限404：无权限2：用户或角色被删除不存在4：本机无权限5：未找到本用户6：参数错误 |

规约功能:

 规约根据权限区域id，把对此权限区域有权限的主机ip写入redis string结构的value中，键key的格式：Auth:HostLimiting:Aojid:String，value填写ip值；

lib库使用：

 CRedisDbOpt \*g\_pRedis = NULL;

 g\_pRedis = new CRedisDbOpt;

if (g\_pRedis == NULL)

{

kprintf(DAC\_K\_MOD\_DAC,DAC\_K\_LOG\_SCENE\_CSI,DAC\_K\_LOG\_ERROR,"rds对象创建失败! ");

 return ret;

 }

 g\_pRedis->createRedisConnection(3);

 char cKey[] = " Auth:HostLimiting:1:String ";

 char val[] = "192.168.2.1";

g\_pRedis->rdsSet(cKey,val); //设置当前有权限的ip

g\_pRedis-> rdsDel(cKey); //删除此权限对应的ip 键值对