# 域内权限

## 组

组( Group)是用户账号的集合。通过向组分配权限,就可以不必向每个用户分别分配权限。例如,管理员在日常工作中,不必为单个用户账号设置独特的访问权限,只需要将用户账放到相应的安全组中。管理员通过配置安全组访问权限,就可以为所有加入安全组的用户账号配置同样的权限。使用安全组而不是单个的用户账号,可以大大简化网络的维护和管理工作

## 域本地组

域本地组成员来自林中任何域中的用户账户、全局组和通用组以及本域中的域本地组，在本域范围内可用。

## 全局组

全局组成员来自于同一域的用户账户和全局组，在林范围内可用

## 通用组

通用组成员来自林中任何域中的用户账户、全局组和其他的通用组，在全林范围内可用

可以这样简单地记忆:

域本地组来自全林,作用于本域;

全局组来自本域,作用于全林;

通用组来自林,作用于全林。

案例一：

有一个打印机连接域控，设置域本地组赋予使用打印机的权限，然后设置全局组，将人员都加入到全局组，然后将全局组加入到域本地组就可以了

案例二

有三个域hack.com(在北京)，sh.hack.com(在上海)，gz.hack.com(在广州)组成W林，然后北京财务部门，需要进行结算，但是数据在北京的一台服务器上权限比较高只有北京财务人员可以使用，同时因为北京人数不够，需要上海和广州支援，这个时候怎么办？

1、只需要在北京的建立一个域本地组，然后赋予域本地组权限可以访问财务的数据机器

2、在上海和广州分别建立全局组

3、在北京的域控上将上海和广州的全局组加入进来

# A-G-DL-P策略

A-G-DL-P策略是指将用户账号添加到全局组中,将全局组添加到域本地组中,然后为域本地 组分配资源权限

- A表示用户账号( Account)
- G表示全局组( Global Group)
- U表示通用组( Universal Group)
- DL表示域本地组( Domain Local Group)
- P表示资源权限( Permission,许可)

按照AG-DL-P策略对用户进行组织和管理是非常容易的。在AGDL-P策略形成以后,当 需要给一个用户添加某个权限时,只要把这个用户添加到某个本地域组中就可以了。

# 重要的域本地组

• 管理员组( Administrators)的成员可以不受限制地存取计算机/域的资源。它不仅是最具权 力的一个组,也是在活动目录和域控制器中默认具有管理员权限的组。该组的成员可以更 改 Enterprise Admins、 Schema admins和 Domain admins组的成员关系,是域森林中强大的 服务管理组
• 远程登录组( Remote Desktop Users)的成员具有远程登录权限。
• 打印机操作员组( Print Operators)的成员可以管理网络打印机,包括建立、管理及删除网 络打印机,并可以在本地登录和关闭域控制器。
• 账号操作员组( Account Operators)的成员可以创建和管理该域中的用户和组并为其设置权 限,也可以在本地登录域控制器,但是,不能更改属于 Administrators或 Domain admins组 的账户,也不能修改这些组。在默认情况下,该组中没有成员。
• 服务器操作员组( Server Operators)的成员可以管理域服务器,其权限包括建立管理删除 任意服务器的共享目录、管理网络打印机、备份任何服务器的文件、格式化服务器硬盘 锁定服务器、变更服务器的系统时间、关闭域控制器等。在默认情况下,该组中没有成员。
• 备份操作员组( Backup Operators)的成员可以在域控制器中执行备份和还原操作,并可以 在本地登录和关闭域控制器。在默认情况下,该组中没有成员
• 再介绍几个重要的全局组、通用组的权限。
• 域管理员组( Domain Admins)的成员在所有加入域的服务器(工作站)、域控制器和活动 目录中均默认拥有完整的管理员权限。因为该组会被添加到自己所在域的 Administrators 组中,因此可以继承 Administrators组的所有权限。同时,该组默认会被添加到每台域成员 计算机的本地 Administrators组中,这样, Domain admins组就获得了域中所有计算机的所 有权。如果希望某用户成为域系统管理员,建议将该用户添加到 Domain admins组中,而 不要直接将该用户添加到

Administrators组中。
• 企业系统管理员组( Enterprise Admins)是域森林根域中的一个组。该组在域森林中的每个 域内都是 Administrators组的成员,因此对所有域控制器都有完全访问权。
• 架构管理员组( Schema admins)是域森林根域中的一个组,可以修改活动目录和域森林的 模式。该组是为活动目录和域控制器提供完整权限的域用户组,因此,该组成员的资格是 非常重要的。
• 域用户组( Domain users)中是所有的域成员。在默认情况下,任何由我们建立的用户账号 都属于 Domain Users组,而任何由我们建立的计算机账号都属于 Domain Computers组。因 此,如果想让所有的账号都获得某种资源存取权限,可以将该权限指定给域用户组,或者 让域用户组属于具有该权限的组。域用户组默认是内置域 Users组的成员。