# 廊坊BigData环境VPN拨入指导

吴淑荣/00197720

2012-08-07

1. **概述**

廊坊BIGDATA的VPN帐号管理系统目的是为了解决OpenVPN用户授权问题，其使用微软的活动目录（Active Directory）作为前台，提供VPN帐号的的管理授权工作，相对于传统的OpenVPN用户管理方式，使用活动目录的方式在提高了系统易用性的同时，也极大地提高了系统的安全性：

* 可视化用户管理。
* 可对用户管理进行分级授权，提高了VPN帐号管理效率。
* 用户可以自己修改密码。
* 强制用户使用AD的密码策略，增加了系统安全性。

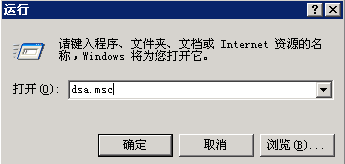
1. **VPN管理系统角色**

VPN管理系统包括3个角色：

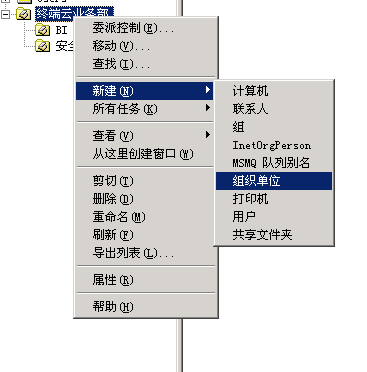
* ***系统管理员角色：*** 拥有整个系统的最高权限，通过权限委派的方式对下级OU管理员进行授权，可授的权限包括帐号的创建、修改、删除、禁用及密码修改等。
* ***OU管理员角色：***OU为“Organization Unit”的简称，OU管理员则负责本OU内VPN用户的授权管理工作，其权限由系统管理员授予。
* ***VPN用户：***VPN用户是此系统的最终用户，通过使用AD帐号，VPN用户可通过OpenVPN方式远程拨入廊坊BigData环境。

1. **操作指导：**
2. **进入用户管理界面**

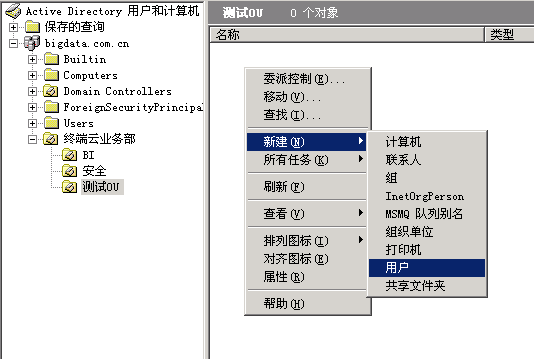
运行“dsa.msc”命令打开AD帐号管理控制台：



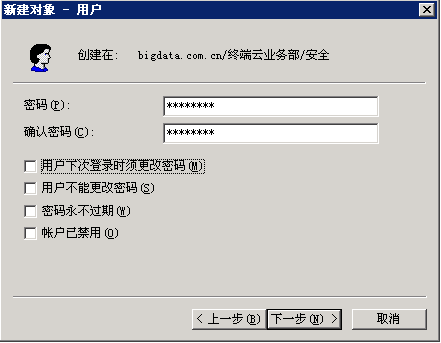
1. **新建组织单位（OU）**

****

1. **新建用户**

****

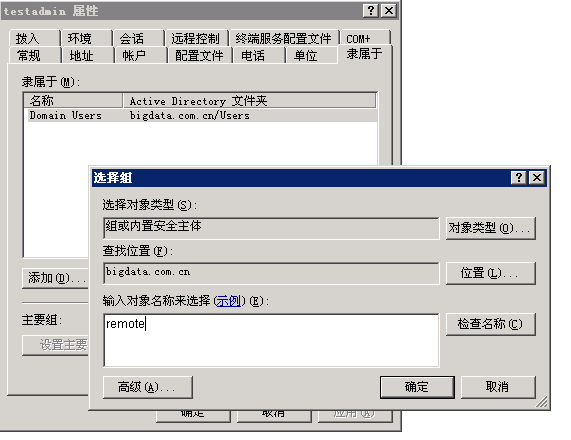
****



【注】：在新建帐号时不要勾选“用户下次登录时必须更改密码”复选框，否则该帐号将不能通过VPN拨入，等VPN拨入成功后再让用户通过<https://10.120.5.107/pass>页面修改帐号密码。也可以在远程桌面登录10.120.5.107服务器后使用“CTL+ALT+END”组合键进行修改。

1. **远程桌面访问授权**

OU管理员需要远程桌面登录AD完成帐号管理工作，因此需要授予其远程桌面登录权限。要授予此权限秩序把OU管理员帐号加到“Remote Desktop Users”组里面：

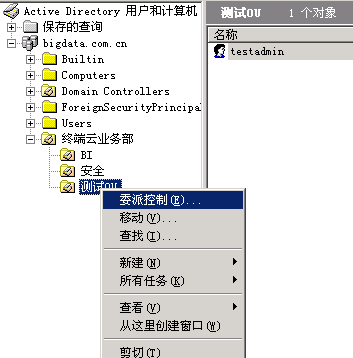
****

【注】：OU管理员之外的帐号不应授予远程桌面登录权限。

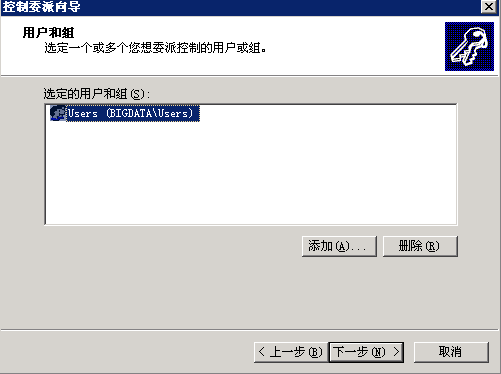
1. **委派帐号管理权限**

OU管理员角色需要完成其所负责OU的帐号管理工作，默认情况下OU管理员角色没有帐号管理权限，这些权限需要系统管理员（Administrator）通过AD的权限委派功能授予。

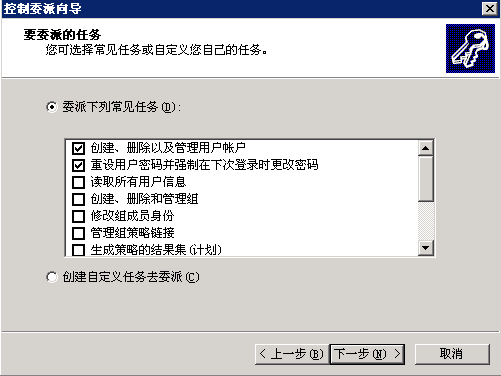
1. 右键点击相应的OU，选择“委派控制”菜单:

****

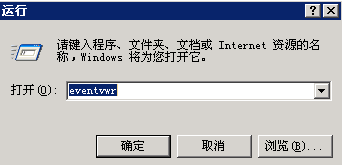
1. 委派目标选择相应的用户组，这里需选择“users”用户组：

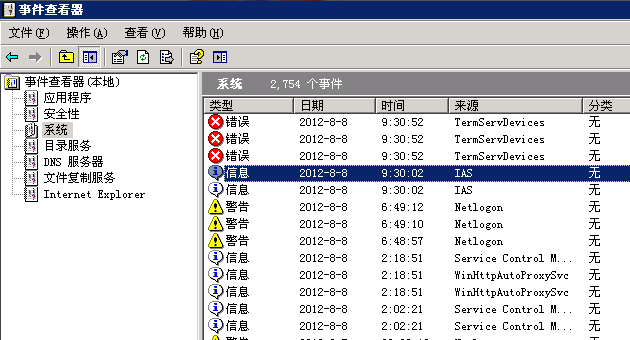
****

1. 对OU管理员的任务委派应如下图设置，不宜授予过多权限：

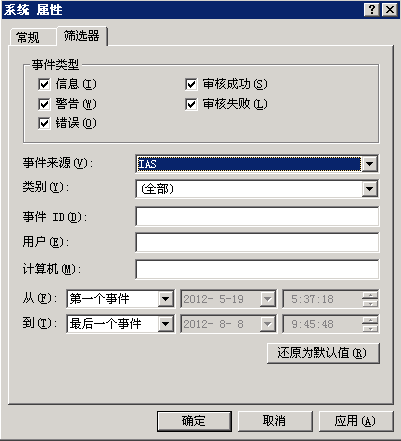
****

1. **访问日志审核**
2. 运行eventvwr命令调出日志查看器：

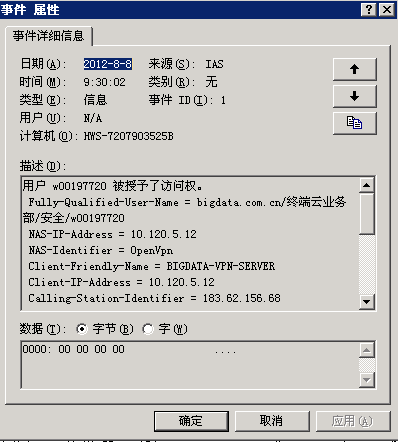
****

****

可通过“查看->筛选”菜单调出筛选对话框，并根据日志来源、ID、类型等对日志进行过滤：

****

下图显示了日志的完整内容，包含哪个用户、通过哪种途径及何时登录等详细信息，这些信息可方便后续的审计工作：

****