**廊坊BigData环境VPN用户授权管理指导**

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. **OU管理员的权限及职责：**

本指导的阅读受众为OU管理员角色。

***权限：***根据系统管理员的授权对本OU进行帐号的创建、修改、删除、禁用及密码修改等工作。

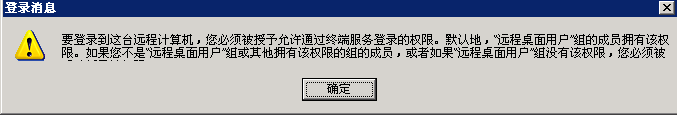
***职责：***

* 根据用户工作需要进行合理VPN授权。
* 定期清理或禁用因工作调整或离职导致的过期用户。
* 原则上对本OU内所用帐号负责。

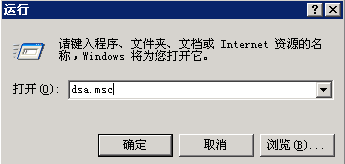
一、通过远程桌面登录10.120.5.107服务器：

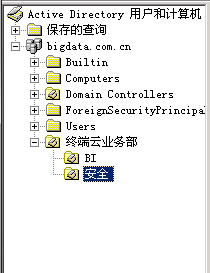


如出现以下错误提示，请联系系统管理员授予远程桌面访问权限：

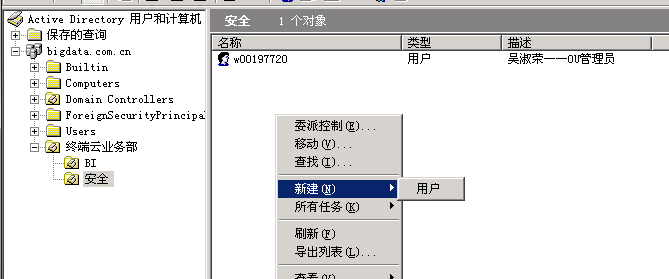


二、运行“dsa.msc”命令打开AD帐号管理控制台：





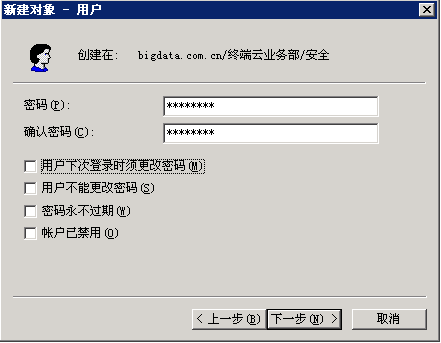
三、选择相应的OU，在右面板右键点击选择“新建->用户”添加帐号。只有被授予了OU管理权限右键菜单才会出现“新建->用户”选项，如没有该选项请联系系统管理员进行授权：



在弹出的对话框中添加用户相关信息，用户登录名应统一使用W3用户名，外包人员则使用姓名全拼，并在帐号描述里面说明：



在下一步中的需勾选“用户下次登录时须修改密码”复选框，强制用户首次登陆修改密码，避免不必要的安全隐患：

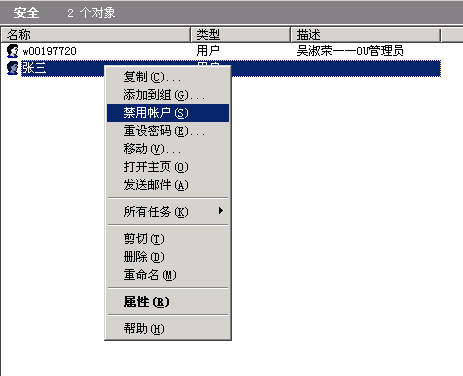


【注】：在新建帐号时不要勾选“用户下次登录时必须更改密码”复选框，否则该帐号将不能通过VPN拨入，等VPN拨入成功后再让用户通过<https://10.120.5.107/pass>页面修改帐号密码。

三、帐号操作：

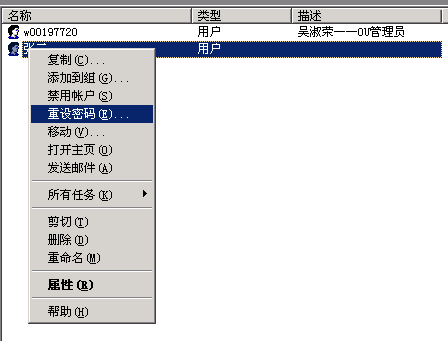
1. 禁用帐号：

右键菜单选择“禁用帐号”选项禁用相应的帐号，帐号被禁用后将不能通过VPN拨入：



1. 修改密码：

当用户忘记密码时，可通过“重置密码”选项重新生成密码（不需要提供旧密码）：



也可通过登录<https://10.120.5.107/pass>网址修改帐号密码，不过需提供旧密码：



1. 删除帐号

确定已不再使用的帐号应及时予以删除：

