Windows 登录脚本可以限制并发登录吗

Windows 登录脚本可以限制并发登录吗

在 Windows 服务器中，使用一个 Windows 登录脚本来限制并发会话靠谱吗？

事实上，这种解决方案存在很多缺点和弱点，并不能满足大中型 IT 基础设施的安全性需求。

一、使用登陆脚本限制并发会话，恶意用户可以轻易删除登陆脚本

利用登陆脚本来限制 Windows 上的并发会话乃是这样：在 Windows 服务器中，并发会话是基于一个隐藏的共享。当用户打开一个会话时登录脚本会创建一个文件，当用户关闭会话时这个文件又被删除。当第二个用户试图打开会话时，脚本会检查文件是否已经存在，如果存在，登录就会被拒绝。

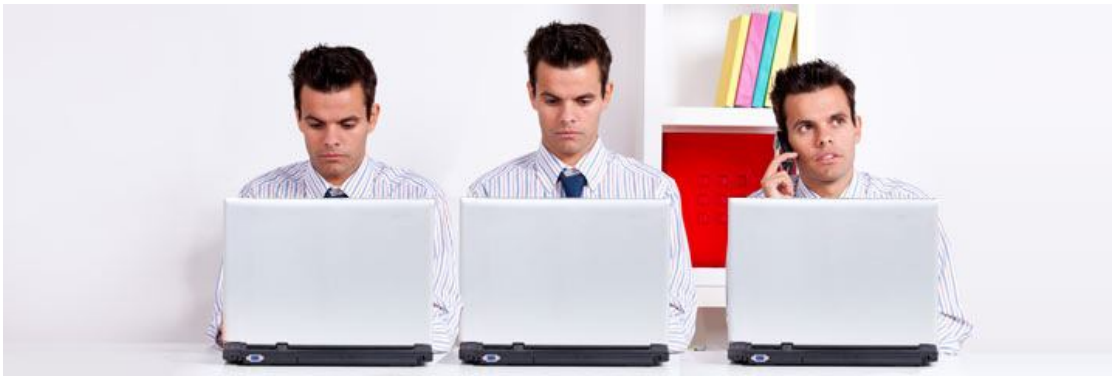
然而，在这种方案中，登录脚本是以用户身份执行的。你需要给每个用户访问权限，使他们可以访问共享的会话文件。这样一来，任何恶意用户都可以轻易删除脚本。（如果你不给出访问权限，windows 登陆脚本就不能创建或删除会话文件。）

二、使用登陆脚本限制并发会话，网络安全得不到保障

也许 windows 登陆脚本的开发人员会说：这种共享是隐藏的，不会对网络安全造成威胁。但是，这并不能有效保障网络安全，因为稍微聪明的用户都能轻易检索到共享文件的路径。况且，任何一个用户都能创建或删除文件，也能限制他人登录（让某些人可以登录某些人不能登录），这样你的网络安全也就得不到保障。

那么，怎样才是防止或限制并发登录最好的方式呢？

那就是**将控制并发登录作为访问控制解决方案的一部分。**



UserLock 是一种独特的解决方案，无论是基于单个用户、用户组或是会话类型，UserLock 都能够限制和防止并发登录到你的 Windows 网络。

UserLock 提供强大的访问控制，通过**允许或拒绝登录（包括并发登录）**、**工作站访问**和**使用/连接时间**来保护 Windows 网络中的所有数据。使用 UserLock，你可以根据个人用户、用户组或是组织单位定义和设置一个批准用户登录的程序。你也可以按会话类型（终端、 Wi-Fi/Radius 、工作站等） 进行定义和设置。

UserLock 还提供对所有网络访问实时的**会话监测和报告**。一旦检测到任何可疑的访问事件，UserLock 会自动提醒安全管理员，安全管理员可以随即快速反应，进行远程锁定、 注销或重置相应的会话。

UserLock 提供不限于本地 Windows 的安全控制

使用 Windows Active Directory，你也可以进入用户的账户，限制其从特定的计算机上登录。然而，在用户组或组织单位中，Windows Active Directory 无法对其限制。UserLock 提供不限于本地 Windows 的安全控制，可从一个用户到另一个用户，一个组到另一个组，或一个部门到另一个部门。UserLock 可阻止用户、用户组或企业部门的多种工作站的登陆。如：自己的工作站、IP 范围、部门、楼层或大楼等。