

通过WindowsServer终端服务实现远程管理Microsoft认证考试  
PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/557/2021\\_2022\\_\\_E9\\_80\\_9A\\_E8\\_BF\\_87Wind\\_c100\\_557312.htm](https://www.100test.com/kao_ti2020/557/2021_2022__E9_80_9A_E8_BF_87Wind_c100_557312.htm) 企业的服务器都是存放在一个相对独立的机房中。如果每次去维护服务器都需要跑到机房中去的话，那不是要麻烦死了。笔者现在是通过微软服务器的终端服务来实现服务器的远程管理。笔者通过客户端连接软件连接到服务器上的终端服务。经过身份验证后笔者的本机桌面就会显示服务器的桌面。并且笔者可以在自己的桌面上执行服务器上的应用程序、存储文件、网络资源。除了速度稍有影响之外，就跟在本机上进行操作差不多。

一、终端服务器的本质。当笔者通过网络连接到终端服务器后，需要运行服务器上的一些程序。其实这些应用程序是在终端服务器上执行的，而不是在本机上执行。也就是说笔者的电脑的作用就好像是键盘与鼠标。即笔者只在他的计算机上通过键盘与鼠标来操作应用程序，然后将终端服务器所传送来的结果显示在屏幕上。而且通过终端服务，多人可以同时服务器进行管理。如在微软的服务器上部署有邮件服务、数据库服务等应用服务。此时邮件管理员、数据库管理员、服务器管理员等等可以同时连接到服务器上，执行位于终端服务器内的应用程序。所以终端服务对于企业网络管理员来说，是很实用的一个工具。特别是企业网络规模比较大，有相对独立的计算机房。此时管理员去服务器前面维护不怎么方便，那么管理员通过远程来维护服务器则是最方便的办法。

二、远程连接的权限控制。虽然远程连接为网络管理员提供了很大的方便。但是其也很有可能给服务器带来一定的安全隐

患。为此网络管理员在方便了日常工作的同时，也需要关注终端服务的安全问题。微软终端服务器在安全上也采取了一些措施。如要允许网络管理员通过终端服务来管理服务器的话，必须满足两个前提条件。一是启动服务器上的远程桌面功能，二是将用户账户加入到远程桌面用户组。这两个是网络管理员连接到服务器所必须的条件。要把用户加入到远程桌面用户组的方法，要视这台服务器的具体配置来看。服务器的相关服务配置不同，其设置的方法也不同。大致来说，有如下几种。一是在服务器上如果没有安装终端服务器而只是启动了远程桌面管理的话，网络管理员也可以通过终端服务来进行远程管理。也就是说，远程桌面是终端服务的一个简化版本。此时，如果要把用户加入到远程桌面用户组可以通过如下步骤来实现。网络管理员可以依次选择“开始”、“设置”、“控制面板”、“系统”。在打开的对话框中选择“远程”标签，选择“允许用户远程连接到此计算机”复选框来启动远程连接的功能。然后单击“选择远程用户”按钮，把用户加入到远程桌面用户组。为了安全起见，最好能够为这个账户配置相关的安全策略。如可以通过密码策略，强制实现密码的复杂性.可以让对这个账户的登陆时间事件审核.设置当密码输入错误超过三次时自动锁定这个账户等的功能。通过这些措施来保障用户名与密码的安全性.从而保障远程维护的安全性。二是服务器部署了终端服务器，而且这个服务器又处在微软域环境中则配置起来就相对复杂一些，不过其安全性也会更高。此时网络管理员也首先需要启用远程桌面的功能。此时网络管理员也可以依次选择“开始”、“设置”、“控制面板”、“系统”。在打开的对话框中选择

“远程”标签，选择“允许用户远程连接到此计算机”复选框来启动远程连接的功能。不过在配置帐户的时候就有所区别。如果这台服务器本身就是域控制器，则需要通过活动目录用户及计算机来进行设置。网络管理员打开“活动目录用户与计算机”窗口，然后将用户加入到远程桌面用户组内。如果这台服务器不是域控制器，而是域环境内的普通服务器，则可以通过依次打开“开始”、“管理工具”、“计算机管理”、“系统工具”、“本地用户和组”命令，将用户加入到远程桌面用户组之内。到此时为止，跟上面的没有很大的不同，只是操作的地方存在差异而已。上面这种方式，可以直接在“远程”标签处把用户加入到远程桌面用户组中。而此时则需要通过专门的用户管理界面来配置帐户。这从根本来说，不会造成他们的安全性差异。而之所以在域环境中能够为终端服务提供更好的安全性，主要是因为下面这个设置。在域环境中，远程桌面用户还必须具备“允许通过终端服务登陆”的权限。如果这台服务器就是域控制器，则这个远程桌面用户组默认情况下是没有“允许通过终端服务登陆”这个权限。这主要也是出于安全性的考虑。网络管理员必须明确设定这台服务器(域控制器)可以通过终端服务实现远程登陆。也就是说网络管理员必须另外赋予该组这个权限之后管理员错菜可以进行远程连接。若要赋予这个权限，网络管理员需要依次打开“开始”、“管理工具”、“域控制器安全策略”、“安全设置”、“本地策略”、“用户权限分配”，在打开的窗口中，再次点击“通过终端服务允许登陆”选项，把这个远程桌面用户组加入进去即可。这个操作虽然简单，但是却极大的提高了终端服务远程连接的安全性。

因为有时候由于人为的疏忽，管理员可能在不需要这个终端服务的情况下，也会允许这个用户组具有这个权限(默认情况下有)。而不会在不需要的时候，主动去禁用这个权限。所以这个措施可以大大的提高服务器的安全性，降低因为启用了终端服务而对此造成的安全隐患。这里要注意的是，这个设置不会马上起效。设置完成之后，网络管理员必须等到此策略应用域控制后才有效。默认情况下，系统会每隔五分钟去检测一下是否有新的安全策略，如果有的话，则会马上应用。如果网络管理员等不及的话，则可以重新启动服务器。不过笔者不建议这么做。这主要是因为服务器频繁启动对于服务器的稳定性不利。而且此时可能有其他用户连接到服务器生正在进行操作，会影响他们的数据保存等等。如果网络管理员连五分钟也等不及，需要马上启用这个策略(如出于测试的需要)，则可以采用gp0update /force命令来强制立即启用策略。如此这个权限设置就会马上生效。

### 三、用户授权问题。

出于微软的商业策略，微软在终端服务上有授权的限制。当网络管理员安装终端服务器之后，虽然可以供多人同是执行位于终端服务器内的应用程序，但是这有一个120天的限制。终端服务器在120天后系统会拒绝用户来连接，即拒绝网络管理员通过终端服务登陆服务器。此时网络管理员如果仍然需要利用这个终端服务的话，则必须在企业网络中有一台已经被激活的“终端服务器授权服务器”，并且取得合法的授权连接数量。也就是说等到120天之后，网络管理员必须经过“终端服务器授权服务器”的授权后，才可以连接到终端服务器。换句话说，此时企业还需要一定的付出。不过相对于其收益来说，这个付出也是有必要的。通常情况下，网络管理

员可以先试用3到4个月来直观感受一下其带来的便利性。等到试用满意后再考虑是否要部署“终端服务器授权服务器”。更多优质资料尽在百考试题论坛 百考试题在线题库 微软认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)