Server2008R2携手Win7打造全新安全组合Microsoft认证考试
 Windows Server 2008 R2 和Windows 7客户端一起使用时可以提供更好更安全的计算环境，DirectAccess是Windows7的一项新功能，该功能可以允许用户在没有VPN的情况下建立一个远程连接， 而Remote Workspace以及Presentation Virtualization和Remote Desktop Gateway功能可以允许用户随时随地安全可靠地访问其公司台式电脑。本文中，我们将探讨这些功能如何让Server 2008 R2/Windows 7组合帮助企业提高Windows网络的安全性。 由于微软公司对可信赖计算的重视，每种新版本的服务器和客户端操作系统都在变得更加安全。Windows Server 2008，特别是其最新代表R2为IT管理员提供了很多内置安全机制。但是，保护服务器安全还只是解决了一半安全问题。客户端也常常成为攻击者的攻击对象，尤其是在现在的现状下，用户们都使用笔记本在公司外面访问公司资源而完全不受IT部门的控制。如果你的企业需要一种高水平的安全保障(在目前的合规环境下，谁不想希望保障安全性?)，你应该事先部署Windows 7客户端以及Windows Server 2008 R2，现在让我们看看可以如何利用这些先进的安全功能。 注意： 很多企业的政策就是等到第一个服务包(SP)发行之后再部署新的客户端操作系统，那么我们需要等待SP1发布后再部署Windows7吗?Gartner公司并不支持这种做法，windows 7的SP1对于系统的稳定性和安全性并没有影响。 DirectAccess 如何允许远程用户安全连接到公司网络并在不造成安全威胁的情况下访问他们所需要的资源呢?最常见

的解决方案就是建立一个VPN服务器，VPN能够通过公共网络(互联网) 提供一个安全加密的渠道进行通信，那么，使用VPN有什么问题呢?VPN解决方案为最终用户增加了操作的复杂性，在某些情况下，用户必须在客户端机器上安装一些特殊软件，并且必须为每次session建立VPN连接，他们必须输入认证证书或者使用智能卡，并且有时候连接不能成功，有时还会掉线需要重新连接等问题。 DirectAccess解决了验证用户身份的麻烦，第一次验证身份成功后，之后就能进行自动连接，而不会降低安全性。另外支持双条件验证，可以使用智能卡或者生物识别技术登录到网络。DirectAccess可以同时验证计算机和用户本身，并且DA将创建两个Ipsec通道，其中一个通道只能使用计算机证书，该通道将允许计算机访问DNS服务器和域控制器以下载组策略和请求用户验证，另一个通道则需要计算机证书和用户证书，能够允许用户访问内部资源和应用程序服务器。 DA的session既可以在客户端和DA服务器/Ipsec网关服务器之间进行加密，也可以进行端对端加密(一直到应用服务器端，如 Exchange服务器等)。这里的注意事项就是，对于端对端加密，应用服务器运行的Windows Server 2008 或者2008 R2必须配置为使用Ipv6和Ipsec。 DirectAccess使用的是Ipv6，Ipv6是用于加密在互联网发送信息的下一代互联网Ipsec协议(3DES，AES)，但这并不是说你必须运行Ipv6网络来使用DA，因为它也同样包括Ipv6/Ipv4过度技术。Windows 7和Windows Server 2008 R2支持一种被称为IP-HTTPS的新技术，该技术可以将ipv6封包加入到Ipv4 HTTPS的session中，这使位于web proxy或者防火墙后面的计算机也能够进行连接。有了VPN，NAP(网络接入保护)可以

用来确保计算机在接入公司网络前的即时安全更新、反病毒等。 DirectAccess的另一个优点就是能够让用户进行控制，DA可以让IT管理员在即使没有连接到VPN的情况下也能管理远程系统，可以通过远程计算机连接到互联网随时随地运用新的组策略或者分发软件更新，即使用户没有登录。这使远程计算机能够及时响应公司的政策，另外，也可以限制特定用户访问内部资源的范围。 RemoteApp和Desktop RemoteApp是Remote Desktop Services的执行功能，该功能可以当用户在Remote Desktop服务器上运行的时候让应用程序就像在本地计算机运行一样，这属于展示虚拟化(presentation virtualization)的一种形式。这与传统的终端服务有所不同，传统服务是通过终端服务器来共享整个用户桌面，而现在个人应用程序也可以以共享的形式提供给用户。RemoteApp是Windows Server 2008中推出的功能，而Windows 7中的RemoteApp amp. Desktop连接，管理员可以方便地向使用Windows 7客户端计算机的用户提供 Remote App程序和虚拟化桌面，这些资源将出现在客户端的开始菜单中，就像本地资源一样。 那么，安全优势在哪里呢?虚拟化应用程序可以接受IT管理员更加严格的控制，你不再需要担心运行在个人计算机上的大量应用程序是否已进行安全更新，这样也就没有因为运行未修复程序而造成的安全威胁。管理员可以添加或者移除资源，并且RemoteApp amp.displaylang=en Remote Desktop Gateway是Terminal Services Gateway的代替品，在Windows Server 2008 R2 标准版、企业版和数据中心版中发挥着服务器的作用，远程用户可以通过启用Remote Desktop访问远程桌面服务器或者其他计算机，它通过HTTPS使用RDP

来创建互联网上的安全加密连接，Server 2008 R2 RD Gateway同时还支持选项功能，可以让你限制远程桌面客户端只能连接到使用安全设备重新定向的远程桌面服务器，这有助于避免远程客户端上的恶意软件蔓延到企业机器。 在Windows Server 2008 R2 和Windows 7上运行的最新版本的RDP Protocol (RDP v7)同样提供图形渲染和多媒体功能以提供更好的桌面服务，例如，现在支持Aero玻璃效果，多显示器、DirectShow等，并且性能也整体提高了。 AppLocker AppLocker是Windows 7 和Server 2008 R2 中的新功能，取代了难以操作和范围有限的旧的Software Restriction Policies，AppLocker为用户提供更好的灵活性，并且其规则更加难以规避。AppLocker允许你创建规则来控制哪些文件可以运行，并可以将这些规则运用与特定的用户或者组(担不是计算机。) 你可以根据文件属性(如发行者、产品名称、文件名称或者文件版本)来制定规则，这些都在数字签名(发行者规则)中可以找到，你还可以基于目录路径来限制程序(路径规则)，或者你可以使用加密hash来鉴定想要控制的程序(hash规则)，你还可以为这些规则类型创建例外情况。 在默认情况下(也被认为是最佳安全做法)，AppLocker配置为拒绝所有文件，除了那些明确允许的文件外。 更好的BitLocker BitLocker驱动器加密最早出现在Vista系统中，这对笔记本来说是个很不错的功能，但是其作用也是有限的，只能用于加密系统分区。在 Server 2008 和Vista SP1中，该加密功能则可以加密其他分区(非系统)。现在，Server 2008 R2 和Windows 7中，BitLocker可以用于加密可移动驱动器。由于USB驱动已经无处不在，这个功能将有助益提高安全性，因为员工在USB上携带公司数据将带来很大

的风险，USB的可携带性让其很容易丢失和被盗。 Windows Server 2008 R2和Windows 7的BitLocker To Go新功能可以让IT管理员使用组策略迫使用户在写入移动驱动器前启用BitLocker，使更加安全。恢复密钥可以存储在Active Directory中。你同样可以阻止用户连接非加密USB驱动器到计算机，政策可以在以下路径配置：Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives 。 总结 Windows操作系统的每个版本都添加了新的安全功能，目前Windows Server 2008 R2和即将发布的Windows 7则成为安全关注重点，与Windows客户端操作系统以往版本不同的是，在测试阶段的windows7已经被证明是非常稳定和安全，因此企业们(尤其是那些仍然在使用XP系统的企业)应该考虑尽早部署这个组合。 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