使用WindowsDNA设计、部署和管理一个可伸缩的电子商务网站（2） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/241/2021_2022__E4_BD_BF_E7_94_A8Wind_c40_241491.htm 记住记录需要大量的信息，这将允许我们对其他的服务使用那些资源。点击okey。下一个更改是直接进入注册中，工作于注册中的任何时间，记住你想要遵循人们常常讨论的这样一个规则，做一个你的注册的备份并从这个备份中工作。 当然我们要在这个演示中打破这个规则。我们打开这个注册并且我们的第一个设置被设置为TCP参数。我们不想用完用户端口，于是我们将其设置得非常大。一个大的窗口尺寸对于高速网络工作的更好并且当窗口填满后TCP就停止了。 接下来，我们进入H关键字区域计算机系统（H Key Local Machine System）。我们就这样进行。当前的控制设置、服务，然后是TCP关键字，它在这个清单的下面。这些参数连接在其中。我们要添加一个叫做最大用户端口的新的值。 现在，最大的端口已经在那里了。如果不在，你就向前并添加入最大用户端口。你要输入的字符串是oxffe并且你要让它作为一个reg s z而离开它。通过输入它，你将允许我们的系统拥有它所需要的资源。这个设置为非常高级的用户打开端口。 我们也要增加TCP窗口尺寸的值，这些我们已经增加了。而且，它是一个reg s z，值为ox4470。这就为高速网络将窗口尺寸设置的更大。 最后，我们要将处理器线程的最大设置设定为一个很小的值。这改变了对于每一个IIS对MTS所允许的CPU的线程数量，并且这么做减小了系统资源内容的数量。因此我们必须去除TCIP关键字。 我们将要扩展W3SVC关键字以及ASP部分，然后是其下的参数。那

是处理器线程的最大值。现在它是空的。我建议将其设定为10，原因是10在刚开始的时候是非常好的设置。 现在，记住你要为你的特定计算机上的性能自己进行监控。你要降低监视性能值。如果性能下降了，就回到先前的值。如果你感觉到低了，则将其增加。 在这个演示中你已经看到的是为了可用性和可靠性优化你的系统和电子商务站点的最好的实例，通过使用管理控制台或注册编辑器。 我们现在回到幻灯屏幕。在这部分内容中另一些最好的操作是将html输出尽可能地保持到最小。记住，小于2KB。我们要将图像文件保持得很小。平均大约为20KB。约小约好。尽可能的重复使用这些图像文件。记住，你可以利用用户缓存的优势。保持较短的文件名和路径以减少字节数。 分析你的html输出。以28k波特的速率对每个字节计数。向下进行的时候请记住这些。 一些附加的优化和建议是你可能要中止在你的IIS系统或其他你可能有的服务器中的不需要的服务。移去不需要的网址和Internet 信息服务器的服务（Internet Information Server services）。最好将示例站点去掉，如果你不需要使用它们的话。 去掉不需要的扩展映像。确定IIS被设定位自动引导以便在死机时，将会直接的将其重新引导。这是你要注意的一个安全性问题。 去掉你的屏幕保护。使用空白。如果你发现受到了限制你可以增加一些处理器，最后你可以升级到Sequel Server 7.0，这允许你使用网络负载平衡并考虑将你的搜寻和检验数据库选项分离到其他的服务器中。这允许你扩展，继续向前，你可以扩大和缩小，按照你的需要。 我们学习了一些什么？好的，我们以及在较高层次上总览了WIN DNA。我们已经见到了2级层列和3级层列的不同之处。我们已经看到

了怎样优化我们的网站并在最后看到了怎样着重这个网站。我们现在要讨论的，是如果你在安全性上有问题的话你的网站将没有任何价值，这是因为一个安全的网站才是更优秀的网站。这是非常有用的，安全性将最终关乎到生存与否。 接下来我们将讨论创建安全环境，现在。记住，最大的问题以及大多数人所遗忘的是物理安全。研究显示的和统计数据所表明的都说明最普通的黑客不是来自外部的威胁，而是来自有怨气的雇员。 你要确定在物理上保护你的服务器。确定它们不被震动。确定它们在上锁的罩子里。确定你的网络是安全的，有一个防火墙或代理系统。确定你的系统是安全的，对于账目有防范禁闭的策略。 确定你有一个安全性策略的设置。确定你有安全性的持续操作。确定某人的职责而不是仅让他们在有空的时候随便看看。 让我们看一下安全性网站结构。这是一个巨大的网站结构，向前。这是一个我们工作于其中的巨大的网站结构。我们为你们显示这个幻灯片的原因是你可以看见网络用户和防火墙，并请注意我们有一个外级区域和一个开发服务器，以及我们的ERP系统，并请注意在它和DMZ（不戒备区域）之间的防火墙。 注意在我们的不戒备区域中，我们有sequel组件，集成服务器，IIS服务器。通过这些将我们的不戒备区域和分级服务器与我们的后端服务器分离开来，我们将后端服务器从任何来自Internet的攻击中保护起来，也避免了Internet被来自我们的网络内部所攻击。 为了保护某些区域你要记住可以使用鉴别和启动目录设计模型。确定你的服务器任务是正确的。用户的组、文件系统或注册、成员信息都是正确的。确定你的格式被正确的设定了，你的cookies，最后来到鉴定。通过Decom Config NTS进行编

译和反编译。确定任务。CIP、CIPM、新型商业洽谈型服务器，所有的这些是你要保护的区域，焦点是，当然，在于对于端口攻击在象IP端口这样的网络协议上；sequel服务器和ODPCDS终端。大部分人不考虑在站点服务器中创建一个保护以及用CSC文件创建一个连接字符串。 现在我们在Windows 2000中有一个Windows NT中的工具，它具有大量的安全机制，但你必须到具体的地方去对目标项进行安全性设置。 在Windows 2000中，我们有这个新的安全性管理工具，我们称之为安全配置和分析工具（Security Configuration and Analysis Tool）。现在安全性触及系统的许多不同方面。你需要更好的配置分析工具，而安全配置和分析工具（Security Configuration and Analysis Tool）让我们做到了这些。 我们可以在宏的级别上进行配置。我们也可以在宏的级别上进行分析和报告。在我们开始分析和管理工具前，让我们谈论一些别的工具和技巧。 当我们开始这个部分时，我们要讨论后门，它现在是一个的主要问题。拒绝的服务。我们要讨论服务器编排，这是一个新出现的问题，我们要讨论更多的工具和更多的其他问题。 当我们讨论后门时，我们当然要谈到Back Orifice。每个人都听说过Back Orifice。这是后门。它是一个允许黑客访问一个系统旁路安全控制的程序，按字面意思是进入你系统的后门。Back Orifice工具在98年的八月是由Cult of the Dead Cow所介绍了的。 这个黑客工具通过传播受到了大量的关注。你可以察看对于Cult of the Dead Cow的网址。Back Orifice可以做什么？好的，它可以允许通过对于使用95、98以及可能WIN 2000的计算机进行远程控制。 如果我设法使你安装了它，我就拥有了你的计算机。攻击者将控制你的屏幕和

键盘。它记录下击键。它可以锁住或重新启动计算机。它可以进入详细的系统信息。它可以搜集密钥。它可以拷贝、重命名、删除、察看和搜寻文件和目录。Cult of the Dead Cow说实际上Back Orifice可以比坐在键盘前的你拥有对于系统的更多的控制。 实际上它可以在这个终端中做任何事情，包括注册控制；这并不是一个空洞的恐吓。 服务被拒绝。在最近的新闻中有很多问题是关于拒绝服务的。有无数的拒绝服务形式的攻击。实际上拒绝服务攻击就是，它使合法的用户不能使用这个系统并使系统保持忙碌使网站陷入泥潭。 也有直接的播送攻击，这更通常的情况下是指smurf攻击。两周内出现的关于安全性的最新的问题是交互网站脚本安全性的曝光。现在，这是威胁每个人的新问题，不仅仅是微软。 