确保Windows2003系统域上的D 安全 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/266/2021_2022__E7_A1_AE_E4_BF_9DWind_c100_266192.htm 确保Windows Server 2003域上的域名解析系统(domain name system，简称DNS)安全，是非常基本的一个要求。活动目录(Active Directory，简称AD)使用DNS来定位域控制器以及其他域服务所需的资源(比如文件，打印机，邮件等等)。由于DNS是活动目录域体系不可或缺的一部分，所以从一开始就应当确保它的安全。 在Windows Server 2003上安装DNS时，不要修改“ 活动目录集成DNS ”的默认设置。微软在2000中开始提供这种设定。 这意味着系统仅仅在DNS服务器上保存DNS数据，而不会保存或复制域控制器和全局目录服务器上的相关信息。这样不仅可以提升运行速度，而且还提升了三种服务器的运作效率。 对DNS服务器和客户端(或其他服务器)之间的数据传输进行加密也是至关重要的。DNS使用TCP/UDP的53端口.通过在你的安全界线上不同的点对这个端口进行过滤，你可以确保DNS服务器只接受认证过的连接。 另外，这也是一个部署IPSec的好时机，来对DNS客户端和服务器之间的数据传输进行加密。开启IPSec可以确保所有客户端和服务器之间的通讯得到确认和加密。这意味着你的客户端仅仅和认证过的服务器通讯，并有助于阻止请求欺骗或损害。 配置完毕DNS服务器之后，继续监视连接，就像你留意企业中其他高价值目标一样。DNS服务器需要可用的带宽以服务客户的请求。 如果你看到某个源机器上朝着DNS服务器发出了大量的网络通讯，你可能是遭受了“ 拒绝服务攻击 ”(denial-of-service，简称DoS)。直接

从源头切断连接，或者断掉服务器的网络连接，直到你调查清楚问题之后再说。记住，一次成功的对DNS服务器的DoS攻击会直接导致活动目录瘫痪。 使用默认的设置(动态安全更新)，只有认证过的客户端才可以注册并更新服务器上的入口信息。这可以阻止攻击者修改你的DNS入口信息，从而误导客户到精心伪造的网站上以窃取财务资料等重要信息。 你同样可以使用配额以阻止客户端对DNS的洪水攻击。客户端通常只能注册10个记录。通过限制单个客户可注册的目标数目，你可以阻止一个客户端对它自己的DNS服务器进行DoS攻击。 注意:确定你对DHCP服务器，域控制器，以及多宿主服务器(multi-homed)使用了不同的定额。这些服务器依据他们提供的功能不同，可能需要注册上百个目标或用户。 DNS服务器将对一个授权区域内的任何查询请求作出响应。要想对外部世界隐藏你的内部网络架构，通常需要设置一个分隔的姓名空间，这一般意味着一台DNS服务器负责你的内部DNS架构，另一台DNS服务器则负责外部以及Internet的DNS架构。通过阻止外部用户访问内部DNS服务器，你可以防止内部非开放资源的泄露。 最后 不管你是运行一个Windows网络，或者是UNIX和Windows的混合体，DNS的安全都应该是你网络的核心。采取措施以保护DNS免受外部和内部的攻击。