一. 前言

【版权与独立性说明】 1. 本文声明所介绍技术产品是基于北京君云时代科技有限公司进行的研究工作和取得的研 究成果，“君云时代”（简称，下同） 对本文及相应技术产品内容单独完全享有版权，任何形式的侵权盗用行为将会 被依法追究责任。 2. 文中介绍技术流程与操作要点不一定完全体现镜像功能，具体细节以实际操作为准，解释权 归“君云时代”所有，欢迎广大用户及技术爱好者参与使用并提出宝贵建议。 3. 如有各类建议及投诉意见，请及时 拨打技术支持电话: 4008005185 转10449，我们将真诚为您反馈处理结果。

【公司简介】 北京君云时代科技有限公司成立于 2015 年，是国内内少数几家业务完全基于 云计算的服务型 公司， 专注互联网业务，提供一站式运维服务解决方案，包括 但不仅限于云上咨询服务、方案设计、系统实施、应用迁移、系统管理、混合 云管理，数据中心建设等服务，为企业搭建云计算时代的 IT 基础技术框架及运 维服务。我们的使命是帮助企业建立标准化的运维体系促进开发规范，并通过 专业的运营分析数据 帮助企业节省成本，创造更多的业务营收，从而真正帮助 企业有效的使用云计算和大数据， 实现运维真正的价值。

【联系我们】 1.公司地址： 北京市朝阳区大望路 SOHO 现代城 5 号楼 1002

2.公司网站： http://www.cldera.com

2.通讯联络： 电话技术支持: 4008005185 转 10449

一. 安全加固

1.修改远程桌面连接端口
运行 Regedt32 并转到此项:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
找到“PortNumber”子项,修改此端口号，改为20169，并保存。

2.禁止不常用服务

禁用不必要的服务不但可以降低服务器的资源占用减轻负担，而且可以增强安全性。下面列出了禁用的服

务:
Application Experience Lookup Service
Automatic Updates
Computer Browser
Error Reporting Service
Network Location Awareness
Print Spooler
Remote Registry
Secondary Logon
Server
Smartcard
TCP/IP NetBIOS Helper
Workstation
Windows Audio
Windows Time
Wireless Configuration

3.设置组策略，加强系统安全策略

设置帐号锁定阀值为5次无效登录，锁定时间为30分钟;
通过网络访问此计算机中删除Everyone组;
在用户权利指派下，从通过网络访问此计算机中删除Power Users和Backup Operators;
为交互登录启动消息文本。
启用 不允许匿名访问SAM帐号和共享;
启用 不允许为网络验证存储凭据或Passport;
启用 在下一次密码变更时不存储LANMAN哈希值;
启用 清除虚拟内存页面文件;
禁止IIS匿名用户在本地登录;
启用 交互登录:不显示上次的用户名;
从文件共享中删除允许匿名登录的DFS$和COMCFG;
禁用活动桌面。

4.防ping处理

在安全策略组上防ping。

5.修改管理员帐号名称与来宾帐号名称

此步骤主要是为了防止入侵者使用默认的系统用户名或者来宾帐号马上进行暴利破解，在更改完后，不要忘记修改强悍的密码。
控制面板－－管理工具－－本地安全策略－－本地策略－－安全选项，在右边栏的最下方。