

中国电信集团公司文件

中国电信〔2011〕555号

关于印发操作系统等安全配置要求的通知

集团公司各省级分公司，股份公司并转各省级分公司，北京研究院：

根据《关于印发〈中国电信通信网络安全防护管理办法〉的通知》（中国电信〔2010〕531号）文件的规定，为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置工作，集团公司组织编制操作系统、数据库、应用中间件在内的通用安全配置要求。现印发你们，从下发之日起执行，相关要求如下：

一、配置要求应用范围

此配置要求是根据工信部颁布的安全防护标准、结合安全防护检查现状及主流安全厂商的配置规范编制的，是安全配置的通用基本要求。所有网络系统及其相关配套设备、业务平台、

IT 系统等在竣工验收、日常运行过程中需遵循此配置要求。

二、配置要求实施与问题反馈

各省须根据实际情况，结合专业维护和安全作业计划落实配置要求，并在实施过程中规避对业务的影响。请各省注意收集配置要求实施过程中遇到的问题，并通过集团公司网络运行维护事业部生产指挥网站运维专题网络安全防护专栏反馈，集团将跟踪各省的应用情况并对相关问题及时解答。

集团公司联系人：

网络运行维护事业部王新峰， 010-58501675，
wangxf@chinatelecom.com.cn;

北京研究院陈军， 010-58552242， 13301168936，
chenjun@ctbri.com.cn;

薄明霞，010-58552348, 13301168962, bomx@ctbri.com.cn。



配置要求支持的版本汇总

检查模块	支持系统版本号
Windows	Windows 2000 以上
Solaris	Solaris 8 以上
AIX	AIX 5.X 以上
HP-UNIX	HP-UNIX 11i 以上
Linux	内核版本 2.6 以上
Oracle	Oracle 8i 以上
SQL Server	Microsoft SQL Server 2000 以上
MySQL	MySQL 5.x 以上
IIS	IIS 5.x 以上
Apache	Apache 2.x 以上
Tomcat	Tomcat 5.x 以上
WebLogic	WebLogic 8.X 以上

中国电信 Windows 操作系统 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	2
4.1 账号.....	2
4.2 口令.....	3
4.3 授权.....	5
4.4 补丁.....	7
4.5 防护软件.....	8
4.6 防病毒软件.....	8
4.7 日志安全要求.....	9
4.8 不必要的服务.....	11
4.9 启动项.....	12
4.10 关闭自动播放功能.....	13
4.11 共享文件夹.....	13
4.12 使用 NTFS 文件系统.....	14
4.13 网络访问.....	15
4.14 会话超时设置.....	16
4.15 注册表设置.....	17
附录 A：端口及服务.....	18

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》（本规范）
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用 Windows 操作系统的设备。在未特别说明的情况下，均适用于所有运行的 Windows 操作系统，包括 Windows 2000、Windows XP、Windows2003, Windows7 , Windows 2008 以及各版本中的 Sever、Professional 版本。

本规范明确了 Windows 操作系统在安全配置方面的基本要求,适用于所有的安全等级,可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 Windows 2003 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1732-2008 《固定通信网安全防护要求》

YD/T 1734-2008 《移动通信网安全防护要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1742-2008 《接入网安全防护要求》

YD/T 1744-2008 《传送网安全防护要求》

YD/T 1746-2008 《IP 承载网安全防护要求》

YD/T 1748-2008 《信令网安全防护要求》

YD/T 1750-2008 《同步网安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

UDP	User Datagram Protocol	用户数据包协议
TCP	Transmission Control Protocol	传输控制协议

NTFS	New Technology File System	新技术文件系统
------	----------------------------	---------

4 安全配置要求

4.1 账号

编号：1

要求内容	应按照不同的用户分配不同的账号，避免不同用户间共享账号。避免用户账号和设备间通信使用的账号共享。
操作指南	1、参考配置操作 进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”： 根据系统的要求，设定不同的账户和账户组。
检测方法	1、判定条件 结合要求和实际业务情况判断符合要求，根据系统的要求，设定不同的账户和账户组 2、检测操作 进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”： 查看根据系统的要求，设定不同的账户和账户组

编号：2

要求内容	应删除与运行、维护等工作无关的账号。
操作指南	1. 参考配置操作 A) 可使用用户管理工具： 开始-运行-compmgmt.msc-本地用户和组-用户 B) 也可以通过 net 命令： 删除账号： net user account/del 停用账号： net user account/active:no
检测方法	1.判定条件 结合要求和实际业务情况判断符合要求，删除或锁定与设备运行、维护等与工作无关的账号。

	<p>注：无关的账号主要指测试帐户、共享帐号、长期不用账号（半年以上不用）等</p> <p>2.检测操作</p> <p>开始-运行-compmgmt.msc-本地用户和组-用户</p>
--	---

编号：3

要求内容	重命名 Administrator；禁用 guest（来宾）帐号。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：</p> <p>Administrator—>属性—> 更改名称</p> <p>Guest 帐号->属性—> 已停用</p>
检测方法	<p>1、判定条件</p> <p>缺省账户 Administrator 名称已更改。</p> <p>Guest 帐号已停用。</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：</p> <p>缺省帐户—>属性—> 更改名称</p> <p>Guest 帐号->属性—> 已停用</p>

4.2 口令

编号：1

要求内容	<p>密码长度要求：最少 8 位</p> <p>密码复杂度要求：至少包含以下四种类别的字符中的三种：</p> <ul style="list-style-type: none"> ● 英语大写字母 A, B, C, ... Z ● 英语小写字母 a, b, c, ... z ● 阿拉伯数字 0, 1, 2, ... 9 ● 非字母数字字符，如标点符号，@, #, \$, %, &, *等
------	---

操作指南	1、参考配置操作 进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”： “密码必须符合复杂性要求”选择“已启动”
检测方法	1、判定条件 “密码必须符合复杂性要求”选择“已启动” 2、检测操作 进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”： 查看是否“密码必须符合复杂性要求”选择“已启动”

编号：2

要求内容	对于采用静态口令认证技术的设备，账户口令的生存期不长于 90 天。
操作指南	1、参考配置操作 进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”： “密码最长存留期”设置为“90 天”
检测方法	1、判定条件 “密码最长存留期”设置为“90 天” 2、检测操作 进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”： 查看是否“密码最长存留期”设置为“90 天”

编号：3

要求内容	对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近 5 次（含 5 次）内已使用的口令。
操作指南	1、参考配置操作

	<p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：</p> <p>“强制密码历史”设置为“记住 5 个密码”</p>
检测方法	<p>1、判定条件</p> <p>“强制密码历史”设置为“记住 5 个密码”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：</p> <p>查看是否“强制密码历史”设置为“记住 5 个密码”</p>

编号：4

要求内容	<p>对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。</p>
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：</p> <p>“账户锁定阈值”设置为 6 次</p> <p>设置解锁阈值：30 分钟</p>
检测方法	<p>1、判定条件</p> <p>“账户锁定阈值”设置为小于或等于 6 次</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：</p> <p>查看是否“账户锁定阈值”设置为小于等于 6 次</p> <p>补充说明：</p> <p>设置不当可能导致账号大面积锁定，在域环境中应小心设置，Administrator 账号本身不会被锁定。</p>

4.3 授权

编号：1

要求内容	本地、远端系统强制关机只指派给 Administrators 组。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”：</p> <p>“关闭系统”设置为“只指派给 Administrators 组”</p> <p>“从远端系统强制关机”设置为“只指派给 Administrators 组”</p>
检测方法	<p>1、判定条件</p> <p>“关闭系统”设置为“只指派给 Administrators 组”</p> <p>“从远端系统强制关机”设置为“只指派给 Administrators 组”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”：</p> <p>查看“关闭系统”设置为“只指派给 Administrators 组”</p> <p>查看是否“从远端系统强制关机”设置为“只指派给 Administrators 组”</p>

编号：2

要求内容	在本地安全设置中取得文件或其它对象的所有权仅指派给 Administrators。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”：</p> <p>“取得文件或其它对象的所有权”设置为“只指派给 Administrators 组”</p>
检测方法	<p>1、判定条件</p> <p>“取得文件或其它对象的所有权”设置为“只指派给 Administrators 组”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->用</p>

	<p>户权利指派”：</p> <p>查看是否“取得文件或其它对象的所有权”设置为“只指派给 Administrators 组”</p>
--	---

编号：3

要求内容	在本地安全设置中只允许授权帐号本地、远程访问登陆此计算机。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”</p> <p>“从本地登陆此计算机”设置为“指定授权用户”</p> <p>“从网络访问此计算机”设置为“指定授权用户”</p>
检测方法	<p>1、判定条件</p> <p>“从本地登陆此计算机”设置为“指定授权用户”</p> <p>“从网络访问此计算机”设置为“指定授权用户”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”</p> <p>查看是否“从本地登陆此计算机”设置为“指定授权用户”</p> <p>查看是否“从网络访问此计算机”设置为“指定授权用户”</p>

4.4 补丁

编号：1

要求内容	在不影响业务的情况下，应安装最新的 Service Pack 补丁集。对服务器系统应先进行兼容性测试。
操作指南	<p>1、参考配置操作</p> <p>安装最新的 Service Pack 补丁集。</p> <p>例如截止到 2010 年最新版本：Windows XP 的 Service Pack 为 SP3。Windows2000 的 Service Pack 为 SP4, Windows 2003 的 Service Pack 为 SP2</p>
检测方法	1、判定条件

	2、检测操作 进入控制面板->添加或删除程序->显示更新打钩，查看是否 XP 系统已安装 SP3，Win2000 系统已安装 SP4，Win2003 系统已安装 SP2。
--	---

4.5 防护软件

编号：1

要求内容	启用自带防火墙或安装第三方威胁防护软件。根据业务需要限定允许访问网络的应用程序，和允许远程登陆该设备的 IP 地址范围。
操作指南	1、参考配置操作（以启动自带防火墙为例） 进入“控制面板—>网络连接—>本地连接”，在高级选项的设置中启用 Windows 防火墙。 在“例外”中配置允许业务所需的程序接入网络。 在“例外->编辑->更改范围”编辑允许接入的网络地址范围。 说明：分为服务器和操作终端两种情况： 服务器该项为可选，操作终端该项为必选
检测方法	1、判定条件 启用 Windows 防火墙。 “例外”中允许接入网络的程序均为业务所需。 2、检测操作 进入“控制面板—>网络连接—>本地连接”，在高级选项的设置中，查看是否启用 Windows 防火墙。 查看是否在“例外”中配置允许业务所需的程序接入网络。 查看是否在“例外->编辑->更改范围”编辑允许接入的网络地址范围。

4.6 防病毒软件

编号：1

要求内容	安装防病毒软件，并及时更新。
操作指南	1、参考配置操作

	安装防病毒软件，并及时更新。
检测方法	<p>1、判定条件</p> <p>已安装防病毒软件，病毒码更新时间不早于 1 个月，各系统病毒码升级时间要求参见各系统相关规定。</p> <p>注：对于操作终端该项为必选项，对于服务器该项为可选项</p> <p>2、检测操作</p> <p>控制面板->添加或删除程序，是否安装有防病毒软件。打开防病毒软件控制面板，查看病毒码更新日期。</p>

4.7 日志安全要求

编号：1

要求内容	设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。
操作指南	<p>1、参考配置操作</p> <p>开始->运行-> 执行 “ 控制面板->管理工具->本地安全策略->审核策略”</p> <p>审核登录事件，双击，设置为成功和失败都审核。</p>
检测方法	<p>1、判定条件</p> <p>审核登录事件，设置为成功和失败都审核。</p> <p>2、检测操作</p> <p>开始->运行-> 执行 “ 控制面板->管理工具->本地安全策略->审核策略”</p> <p>审核登录事件，双击，查看是否设置为成功和失败都审核。</p>

编号：2

要求内容	开启审核策略，以便出现安全问题后进行追查
操作指南	<p>1、参考配置操作</p> <p>对审核策略进行检查：</p>

	<p>开始-运行-gpedit.msc</p> <p>计算机配置-Windows 设置-安全设置-本地策略-审核策略</p> <p>以下审核是必须开启的，其他的可以根据需要增加：</p> <ul style="list-style-type: none"> • 审核系统登陆事件 成功，失败 • 审核帐户管理 成功，失败 • 审核登陆事件 成功，失败 • 审核对象访问 成功 • 审核策略更改 成功，失败 • 审核特权使用 成功，失败 • 审核系统事件 成功，失败 <p>2、补充说明</p> <p>可能会使日志量猛增</p>
检测方法	<p>1、判定条件</p> <p>尝试对被添加了访问审核的对象进行访问，然后查看安全日志中是否会有相关记录，或通过其他手段激活以配置的审核策略，并观察日志中的记录情况，如果存在记录条目，则配置成功。</p> <p>2、检测操作</p>

编号：3

要求内容	设置日志容量和覆盖规则，保证日志存储
操作指南	<p>1、参考配置操作</p> <p>开始-运行-eventvwr</p> <p>右键选择日志，属性，根据实际需求设置：</p> <p>日志文件大小：可根据需要制定</p> <p>超过上限时的处理方式（建议日志记录天数不小于 90 天）</p> <p>2、补充说明</p> <p>建议对每个日志均进行如上操作，同时应保证磁盘空间</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p>

	开始-运行-eventvwr，右键选择日志，属性，查看日志上限及超过上线时的处理方式
--	--

4.8 不必要的服务、端口

编号： 1

要求内容	关闭不必要的服务
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->计算机管理”，进入“服务和应用程序”：</p> <p>可根据具体应用情况参考附录 A，筛选不必要的服务。</p>
检测方法	<p>1、判定条件</p> <p>系统管理员应出具系统所必要的服务列表。</p> <p>查看所有服务，不在此列表的服务需关闭。</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->计算机管理”，进入“服务和应用程序”：</p> <p>查看所有服务，不在此列表的服务是否已关闭。</p>

编号： 2

要求内容	如需启用 SNMP 服务,则修改默认的 SNMP Community String 设置。
操作指南	<p>1、参考配置操作</p> <p>打开“控制面板”，打开“管理工具”中的“服务”，找到“SNMP Service”，单击右键打开“属性”面板中的“安全”选项卡，在这个配置界面中，可以修改 community strings，也就是微软所说的“团体名称”。</p>
检测方法	<p>1、判定条件</p> <p>community strings 已改，不是默认的“public”</p> <p>2、检测操作</p> <p>打开“控制面板”，打开“管理工具”中的“服务”，找到“SNMP</p>

	Service”，单击右键打开“属性”面板中的“安全”选项卡，在这个配置界面中，查看 community strings，也就是微软所说的“团体名称”。
--	--

编号： 3

要求内容	如对互联网开放 WindowsTerminal 服务(Remote Desktop)，需修改默认服务端口。
操作指南	<p>1、参考配置操作</p> <p>开始->运行 Regedt32</p> <p>并转到此项：</p> <p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp</p> <p>找到“PortNumber”子项，会看到默认值 00000D3D，它是 3389 的十六进制表示形式。使用十六进制数值修改此端口号，并保存新值。</p>
检测方法	<p>1、判定条件</p> <p>找到 “PortNumber” 子项，设定值非 00000D3D，即十进制 3389</p> <p>2、检测操作</p> <p>运行 Regedt32 ,找到此项并判断。</p>

4.9 启动项

要求内容	关闭无效启动项
操作指南	<p>1、参考配置操作</p> <p>“开始->运行->MSconfig” 启动菜单中，取消不必要的启动项。</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>系统管理员提供业务必须的自动加载进程和服务列表文档。</p> <p>查看 “开始->运行->MSconfig” 启动菜单：</p> <p>不需要的自动加载进程是否已禁用和取消。</p>

4.10 关闭自动播放功能

编号：1

要求内容	关闭 Windows 自动播放功能
操作指南	1、参考配置操作 开始→运行→gpedit.msc，打开组策略编辑器，浏览到计算机配置→管理模板→系统，在右边窗格中双击“关闭自动播放”，对话框中选择所有驱动器，确定即可。
检测方法	1、判定条件 所有驱动器均“关闭自动播放” 2、检测操作 “关闭自动播放”配置已启用，启用范围：所有驱动器。

4.11 共享文件夹

编号：1

要求内容	在非域环境下，关闭 Windows 硬盘默认共享，例如 C\$，D\$。
操作指南	1、参考配置操作 进入“开始→运行→Regedit”，进入注册表编辑器，更改注册表键值： HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\下，增加 REG_DWORD 类型的 AutoShareServer 键，值为 0。
检测方法	1、判定条件 HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\增加了 REG_DWORD 类型的 AutoShareServer 键，值为 0。 2、检测操作 进入“开始→运行→Regedit”，进入注册表编辑器，更改注册表键值：

	HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\ ，增加 REG_DWORD 类型的 AutoShareServer 键，值为 0。
--	--

编号：2

要求内容	设置共享文件夹的访问权限，只允许授权的账户拥有权限共享此文件夹。
操作指南	1、参考配置操作 进入“控制面板->管理工具->计算机管理”，进入“系统工具->共享文件夹”： 查看每个共享文件夹的共享权限，只将权限授权于指定账户。
检测方法	1、判定条件 查看每个共享文件夹的共享权限仅限于业务需要，不设置成为“everyone”。 2、检测操作 进入“控制面板->管理工具->计算机管理”，进入“系统工具->共享文件夹”： 查看每个共享文件夹的共享权限。

4.12 使用 NTFS 文件系统

要求内容	在不毁坏数据的情况下，将 F A T 分区改为 N T F S 格式
操作指南	1、参考配置操作 将 FAT 卷转换成 NTFS 分区 CONVERT volume /FS:NTFS[/V] [/CvtArea:filename][/NoSecurity][/X] Volume 指定驱动器号（后面加一个冒号）、装载点或卷名 /FS:NTFS 指定要被转换成 NTFS 的卷 /V 指定 CONVERT 应该用详述模式运行 /CvtArea:filename 将根目录中的一个接续文件指定为 NTFS 系统文件的占位符

	<p>/NoSecurity 指定每个人都可以访问转换的文件和目录的安全设置</p> <p>/X 如果必要，先强行卸载卷，有打开的句柄则无效</p> <p>例如：</p> <p>Covert C: /FS:NTFS</p> <p>备注：</p> <p>1、新上线系统必须要求 NTFS 分区，已上线系统在不损坏数据的情况下应用</p> <p>2、在有其他非 WIN 系统访问、存在数据共享的情况下，不建议将 F A T 分区改为 N T F S 格式</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> 

4.13 网络访问

编号：1

要求内容	禁用匿名访问命名管道和共享
------	---------------

操作指南	1、参考配置操作 “控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可匿名访问的共享设置为全部删除 “控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可匿名访问的命名管道 设置为全部删除
检测方法	1、判定条件 全部删除匿名访问命名管道和共享 2、检测操作 查看“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可匿名访问的共享、可匿名访问的命名管道是否设置为全部删除

编号：2

要求内容	禁用可远程访问的注册表路径和子路径
操作指南	1、参考配置操作 “控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可远程访问的注册表路径 设置为全部删除 “控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可远程访问的注册表路径和子路径 设置为全部删除
检测方法	1、判定条件 全部删除可远程访问的注册表路径和子路径 3、检测操作 查看“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问中，查看，可远程访问的注册表路径、可远程访问的注册表路径和子路径是否设置为全部删除

4.14 会话超时设置

编号：1

要求内容	对于远程登录的账户，设置不活动所连接时间 15 分钟
操作指南	1、参考配置操作 进入“控制面板—管理工具—本地安全策略”，在“安全策略—安全选项”：“Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间”为 15 分钟
检测方法	1、判定条件 “Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间”为 15 分钟 2、检测操作 进入“控制面板—管理工具—本地安全策略”，在“安全策略—安全选项”：查看“Microsoft 网络服务器”设置

4.15 注册表设置

编号：1

要求内容	在不影响系统稳定运行的前提下，对注册表信息进行更新。
操作指南	1、参考配置操作 <ul style="list-style-type: none"> 自动登录： HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AutoAdminLogon (REG_DWORD) 0 源路由欺骗保护： HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting (REG_DWORD) 2 删除匿名用户空链接 HKEY_LOCAL_MACHINE\SYSTEM\Current\Control\Set\Control\Lsa 将 restrictanonymous 的值设置为 1，若该值不存在，可以自己创建，类型为 REG_DWORD 修改完成后重新启动系统生效 碎片攻击保护： HKLM\System\CurrentControlSet\

	<p>Services\Tcpip\Parameters\EnablePMTUDiscovery</p> <p>(REG_DWORD) 1</p> <ul style="list-style-type: none"> Syn flood 攻击保护: <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services</p> <p>之下, 可设置:</p> <p>TcpMaxPortsExhausted。推荐值: 5。</p> <p>TcpMaxHalfOpen。推荐值数据: 500。</p> <p>TcpMaxHalfOpenRetried。推荐值数据: 400</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>点击开始->运行, 然后在打开行里输入 regedit, 然后单击确定, 查看相关注册表项进行查看;</p> <p>使用空连接扫描工具无法远程枚举用户名和用户组</p>

附录 A: 端口及服务

服务名称	端口	服务说明	关闭方法	处置建议
系统服务部分				
echo	7/TCP	RFC862_回声协议	关闭"Simple TCP/IP Services"服务。	建议关闭
echo	7/UDP	RFC862_回声协议		
discard	9/UDP	RFC863 废除协议		
discard	9/TCP	RFC863 废除协议		
daytime	13/UDP	RFC867 白天协议		
daytime	13/TCP	RFC867 白天协议		
qotd	17/TCP	RFC865 白天协议的引用		
qotd	17/UDP	RFC865 白天协议的引用		
chargen	19/TCP	RFC864 字符产生协议		

chargen	19/UDP	RFC864 字符产生协议		
ftp	21/TCP	文件传输协议(控制)	关闭"FTP Publishing Service"服务。	根据情况选择开放
smtp	25/TCP	简单邮件发送协议	关闭"Simple Mail Transport Protocol"服务。	建议关闭
nameserver	42/TCP	WINS 主机名服务	关闭"Windows Internet Name Service"服务。	建议关闭
	42/UDP			
domain	53/UDP	域名服务器	关闭"DNS Server"服务。	根据情况选择开放
	53/TCP			根据情况选择开放
dhcpc	67/UDP	DHCP 服务器 /Internet 连接共享	关闭"Simple TCP/IP Services"服务。	建议关闭
dhcpc	68/UDP	DHCP 协议客户端	关闭"DHCP Client"服务。	建议关闭
http	80/TCP	HTTP 万维网发布服务	关闭"World Wide Web Publishing Service"服务。	根据情况选择开放
epmap	135/TCP	RPC 服务	系统基本服务	无法关闭
	135/UDP			无法关闭
netbios-ns	137/UDP	NetBIOS 名称解析	在网卡的 TCP/IP 选项中"WINS"页勾选"禁用 TCP/IP 上的 NETBIOS"	根据情况选择开放
netbios-dgm	138/UDP	NetBIOS 数据报服务		根据情况选择开放
netbios-ssn	139/TCP	NetBIOS 会话服务	系统基本服务	无法关闭
snmp	161/UDP	SNMP 服务	关闭"SNMP "服务	根据情况选择开放
https	443/TCP	安全超文本传输协议	关闭"World Wide Web Publishing Service"服务	根据情况选择开放

microsoft-ds	445/UDP	SMB 服务器	运行 regedit, 打开 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters 添加名为 "SMBDeviceEnabled"的子键, 类型 dword, 值为 0 重新启动计算机	根据情况选择开放
	445/TCP			
isakmp	500/UDP	IPSec ISAKMP 本地安全机构	关闭"IPSEC Policy Agent"服务	很少使用的服务, 如不使用 ipsec, 建议关闭
RADIUS	1645/UDP	旧式 RADIUS Internet 身份验证服务	关闭"Remote Access Connection Manager"服务	建议关闭
RADIUS	1646/UDP	旧式 RADIUS Internet 身份验证服务		建议关闭
radius	1812/UDP	身份验证 Internet 身份验证服务		建议关闭
radacct	1813/UDP	计帐 Internet 身份验证服务		建议关闭
MSMQ-RPC	2105/TCP	MSMQ-RPC 消息队列	关闭"Message Queuing"服务。	建议关闭
Termsrv	3389/TCP	终端服务	关闭"Terminal Services"服务。	根据情况选择开放
其他常用服务				
Apache	80/TCP 8000/TCP	Apache HTTP 服务器	关闭"Apache2"服务。	根据情况选择开放
ms-sql-s	1433/TCP 1434/UDP	微软公司数据库	关闭 "MSSQLServer"服务。	根据情况选择开放
ORACLE	1521/TCP	甲骨文公司数据库	关闭 "OracleOraHome90 TNSListener"服务。	根据情况选择开放

remote administrator	4899/TCP	Famatech 公司远程控制软件	关闭"Remote Administrator Service"服务。	根据实际情况选择开放
sybase	5000/TCP	Sybase 公司数据库	关闭"Sybase SQLServer"字样开始的服务。	根据实际情况选择开放
pcAnywhere	5631/TCP 5632/UDP	Symantec 公司远程控制软件	关闭"pcAnywhere Host Service"字样开始的服务。	根据实际情况选择开放

中国电信 AIX 操作系统 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 帐号.....	2
4.2 口令.....	5
4.3 授权.....	7
4.4 补丁.....	10
4.5 日志.....	10
4.6 不必要的服务、端口.....	12
4.7 文件与目录权限.....	13
4.8 系统 Banner 设置.....	14
4.9 登陆超时时间设置.....	15
4.10 内核调整设置.....	15
4.11 SSH 加密协议.....	16
4.12 FTP 设置.....	18
附录 A：端口及服务.....	18

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》（本规范）
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用 AIX 操作系统的设备。本规范明确了安全配置的基本要求，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 AIX 5.X 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1732-2008 《固定通信网安全防护要求》

YD/T 1734-2008 《移动通信网安全防护要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1742-2008 《接入网安全防护要求》

YD/T 1744-2008 《传送网安全防护要求》

YD/T 1746-2008 《IP 承载网安全防护要求》

YD/T 1748-2008 《信令网安全防护要求》

YD/T 1750-2008 《同步网安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

SSH	Secure Shell Protocol	安全外壳协议
FTP	File Transfer Protocol	文件传输协议
UDP	User Datagram Protocol	用户数据包协议
TCP	Transmission Control Protocol	传输控制协议

4 安全配置要求

4.1 帐号

编号： 1

要求内容	应按照不同的用户分配不同的账号。
操作指南	1、参考配置操作 为用户创建账号： #useradd username #创建账号 #passwd username #设置密码 修改权限： #chmod 750 directory #其中 750 为设置的权限，可根据实际情况设置相应的权限，directory 是要更改权限的目录) 使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。 2、补充操作说明
检测方法	1、判定条件 能够登录成功并且可以进行常用操作； 2、检测操作 使用不同的账号进行登录并进行一些常用操作； 3、补充说明

编号： 2

要求内容	应删除或锁定与设备运行、维护等工作无关的账号。
操作指南	1、参考配置操作 删除用户：#userdel username; 锁定用户： 1)修改/etc/shadow 文件，用户名后加*LK* 2)将/etc/passwd 文件中的 shell 域设置成/bin/false 3)#passwd -l username 只有具备超级用户权限的使用者方可使用，#passwd -l username 锁定用户,用#passwd -d username 解锁后原有密码失效，登录需输入新密码，修改/etc/shadow 能保留原有密码。 2、补充操作说明 需要锁定的用户：listen,gdm,webserverd,nobody,nobody4、noaccess。
检测方法	1、判定条件 被删除或锁定的账号无法登录成功； 2、检测操作 使用删除或锁定的与工作无关的账号登录系统； 3、补充说明 需要锁定的用户：listen,gdm,webserverd,nobody,nobody4、noaccess。 解锁时间：15 分钟

编号： 3

要求内容	限制具备超级管理员权限的用户远程登录。 需要远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到超级管理员权限账号后执行相应操作。
操作指南	1、参考配置操作 编辑/etc/security/user，加上： 在 root 项上输入 false 作为 rlogin 的值 此项只能限制 root 用户远程使用 telnet 登录。用 ssh 登录，修改此项不会看到效果的 2、补充操作说明 如果限制 root 从远程 ssh 登录，修改/etc/ssh/sshd_config 文件，将 PermitRootLogin yes 改为 PermitRootLogin no，重启 sshd 服务。
检测方法	1、判定条件 root 远程登录不成功，提示“没有权限”； 普通用户可以登录成功，而且可以切换到 root 用户； 2、检测操作 root 从远程使用 telnet 登录； 普通用户从远程使用 telnet 登录； root 从远程使用 ssh 登录； 普通用户从远程使用 ssh 登录； 3、补充说明 限制 root 从远程 ssh 登录，修改/etc/ssh/sshd_config 文件，将 PermitRootLogin yes 改为 PermitRootLogin no，重启 sshd 服务。

编号： 4

要求内容	对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议，并安全配置 SSHD 的设置。
操作指南	1、参考配置操作 把如下 shell 保存后，运行，会修改 ssh 的安全设置项： <pre> unalias cp rm mv case `find /usr/etc -type f grep -c ssh_config\$` in 0) echo "Cannot find ssh_config" ;; 1) DIR=`find /usr/etc -type f 2>/dev/null \ grep ssh_config\$ sed -e "s:/ssh_config::"` cd \$DIR cp ssh_config ssh_config.tmp awk '/^#? *Protocol/ { print "Protocol 2"; next } { print }' ssh_config.tmp > ssh_config if ["`grep -El ^Protocol ssh_config`" = ""]; then echo 'Protocol 2' >> ssh_config fi </pre>

	<pre> rm ssh_config.tmp chmod 600 ssh_config ;; *) echo "You have multiple sshd_config files. Resolve" echo "before continuing." ;; esac #也可以手动编辑 ssh_config, 在 "Host *"后输入 "Protocol 2", cd \$DIR cp sshd_config sshd_config.tmp awk '/^#? *Protocol/ { print "Protocol 2"; next }; /^#? *X11Forwarding/ \ { print "X11Forwarding yes"; next }; /^#? *IgnoreRhosts/ \ { print "IgnoreRhosts yes"; next }; /^#? *RhostsAuthentication/ \ { print " RhostsAuthentication no"; next }; /^#? *RhostsRSAAuthentication/ \ { print "RhostsRSAAuthentication no"; next }; /^#? *HostbasedAuthentication/ \ { print "HostbasedAuthentication no"; next }; /^#? *PermitRootLogin/ \ { print "PermitRootLogin no"; next }; /^#? *PermitEmptyPasswords/ \ { print "PermitEmptyPasswords no"; next }; /^#? *Banner/ \ { print "Banner /etc/motd"; next }; {print}' sshd_config.tmp > sshd_config rm sshd_config.tmp chmod 600 sshd_config Protocol 2 #使用 ssh2 版本 X11Forwarding yes #允许窗口图形传输使用 ssh 加密 IgnoreRhosts yes#完全禁止 SSHD 使用.rhosts 文件 RhostsAuthentication no #不设置使用基于 rhosts 的安全验证 RhostsRSAAuthentication no #不设置使用 RSA 算法的基于 rhosts 的 安全验证 HostbasedAuthentication no #不允许基于主机白名单方式认证 PermitRootLogin no #不允许 root 登录 PermitEmptyPasswords no #不允许空密码 Banner /etc/motd #设置 ssh 登录时显示的 banner 2、补充操作说明 </pre>
--	---

	查看 SSH 服务状态： <pre># ps -elfgrep ssh</pre>
检测方法	1、判定条件 <pre># ps -elfgrep ssh</pre> 是否有 ssh 进程存在 2、检测操作 查看 SSH 服务状态： <pre># ps -elfgrep ssh</pre> 查看 telnet 服务状态： <pre># ps -elfgrep telnet</pre>

4.2 口令

编号：1

要求内容	对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。
操作指南	1、参考配置操作 <pre>chsec -f /etc/security/user -s default -a minlen=8</pre> <pre>chsec -f /etc/security/user -s default -a minalpha=1</pre> <pre>chsec -f /etc/security/user -s default -a mindiff=1</pre> <pre>chsec -f /etc/security/user -s default -a minother=1</pre> <pre>chsec -f /etc/security/user -s default -a pwdwarntime=5</pre> minlen=8 #密码长度最少 8 位 minalpha=1 #包含的字母最少 1 个 mindiff=1 #包含的唯一字符最少 1 个 minother=1 #包含的非字母最少 1 个 pwdwarntime=5 #系统在密码过期前 5 天发出修改密码的警告信息给用户 2、补充操作说明
检测方法	1、判定条件 不符合密码强度的时候，系统对口令强度要求进行提示； 符合密码强度的时候，可以成功设置； 2、检测操作 1、检查口令强度配置选项是否可以进行如下配置： <ul style="list-style-type: none"> i. 配置口令的最小长度； ii. 将口令配置为强口令。 2、创建一个普通账号，为用户配置与用户名相同的口令、只包含字符或数字的简单口令以及长度短于 8 位的口令，查看系统是否对

	口令强度要求进行提示；输入带有特殊符号的复杂口令、普通复杂口令，查看系统是否可以成功设置。
--	---

编号： 2

要求内容	对于采用静态口令认证技术的设备，帐户口令的生存期不长于 90 天。
操作指南	1、参考配置操作 方法一： chsec -f /etc/security/user -s default -a histexpire=13 方法二： 用 vi 或其他文本编辑工具修改 chsec -f /etc/security/user 文件如下值： histexpire=13 histexpire=13 #密码可重复使用的星期为 13 周（91 天） 2、补充操作说明
检测方法	1、判定条件 密码过期后登录不成功； 2、检测操作 使用超过 90 天的帐户口令登录会提示密码过期；

编号： 3

要求内容	对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近 5 次（含 5 次）内已使用的口令。
操作指南	1、参考配置操作 方法一： chsec -f /etc/security/user -s default -a histsize=5 方法二： 用 vi 或其他文本编辑工具修改 chsec -f /etc/security/user 文件如下值： histsize=5 histexpire=5 #可允许的密码重复次数
检测方法	1、判定条件 设置密码不成功 2、检测操作 cat /etc/security/user， 设置如下

	histsize=5 3、补充说明 默认没有 histsize 的标记，即不记录以前的密码。
--	---

编号： 4

要求内容	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。
操作指南	1、参考配置操作 查看帐户属性： #lsuser username 设置 6 次登陆失败后帐户锁定阈值： #chuser loginretries=6 username 备注：root 账户不在锁定范围内
检测方法	1、判定条件 运行 lsuser uasename 命令，查看帐户属性中是否设置了 6 次登陆失败后帐户锁定阈值的策略。如未设置或大于 6 次，则进行设置

4.3 授权

编号： 1

要求内容	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	1、参考配置操作 通过 chmod 命令对目录的权限进行实际设置。 2、补充操作说明 chown -R root:security /etc/passwd /etc/group /etc/security chown -R root:audit /etc/security/audit chmod 644 /etc/passwd /etc/group chmod 750 /etc/security chmod -R go-w,o-r /etc/security /etc/passwd /etc/group /etc/security 的所有者必须是 root 和 security 组成员 /etc/security/audit 的所有者必须是 iroot 和 audit 组成员 /etc/passwd 所有用户都可读，root 用户可写 -rw-r—r— /etc/shadow 只有 root 可读 -r----- /etc/group 必须所有用户都可读，root 用户可写 -rw-r—r— 使用如下命令设置： chmod 644 /etc/passwd chmod 644 /etc/group

	<p>如果是有写权限，就需移去组及其它用户对/etc 的写权限（特殊情况除外）</p> <p>执行命令#chmod -R go-w,o-r /etc</p>
检测方法	<p>1、判定条件</p> <p>1、设备系统能够提供用户权限的配置选项，并记录对用户进行权限配置是否必须在用户创建时进行；</p> <p>2、记录能够配置的权限选项内容；</p> <p>3、所配置的权限规则应能够正确应用，即用户无法访问授权范围之外的系统资源，而可以访问授权范围之内的系统资源。</p> <p>2、检测操作</p> <p>1、利用管理员账号登录系统，并创建 2 个不同的用户；</p> <p>2、创建用户时查看系统是否提供了用户权限级别以及可访问系统资源和命令的选项；</p> <p>3、为两个用户分别配置不同的权限，2 个用户的权限差异应能够分别在用户权限级别、可访问系统资源以及可用命令等方面予以体现；</p> <p>4、分别利用 2 个新建的账号访问设备系统，并分别尝试访问允许访问的内容和不允许访问的内容，查看权限配置策略是否生效。</p> <p>3、补充说明</p>

编号：2

要求内容	控制 FTP 进程缺省访问权限，当通过 FTP 服务创建新文件或目录时应屏蔽掉新文件或目录不应有的访问允许权限。
操作指南	<p>1、参考配置操作</p> <p>a. 限制某些系统帐户不准 ftp 登录： 通过修改 ftpusers 文件，增加帐户 #vi /etc/ftpusers</p> <p>b. 限制用户可使用 FTP 不能用 Telnet，假如用户为 ftpxll 创建一个/etc/shells 文件，添加一行 /bin/true； 修改/etc/passwd 文件，ftpxll:x:119:1::/home/ftpxll:/bin/true 注：还需要把真实存在的 shell 目录加入/etc/shells 文件，否则没有用户能够登录 ftp 以上两个步骤可参考如下 shell 自动执行：</p> <pre>lsuser -c ALL grep -v ^#name cut -f1 -d: while read NAME; do if [`lsuser -f \$NAME grep id cut -f2 -d= ` -lt 200]; then echo "Adding \$NAME to /etc/ftpusers" echo \$NAME >> /etc/ftpusers.new fi done sort -u /etc/ftpusers.new > /etc/ftpusers rm /etc/ftpusers.new chown root:system /etc/ftpusers chmod 600 /etc/ftpusers</pre>

	<p>c. 限制 ftp 用户登陆后在自己当前目录下活动 编辑 ftpaccess，加入如下一行 restricted-uid *(限制所有)， restricted-uid username（特定用户） ftpaccess 文件与 ftpusers 文件在同一目录</p> <p>d. 设置 ftp 用户登录后对文件目录的存取权限，可编辑 /etc/ftpaccess。</p> <pre> chmod no guest,anonymous delete no guest,anonymous overwrite no guest,anonymous rename no guest,anonymous umask no anonymous </pre> <p>2、补充操作说明 查看# cat ftpusers 说明：在这个列表里边的用户名是不允许 ftp 登陆的。</p> <pre> root daemon bin sys adm lp uucp nuucp listen nobody noaccess nobody4 </pre>
检测方法	<p>1、判定条件 权限设置符合实际需要；不应有的访问允许权限被屏蔽掉；</p> <p>2、检测操作 查看新建的文件或目录的权限，操作举例如下： #more /etc/ftpusers #more /etc/passwd #more /etc/ftpaccess</p> <p>3、补充说明 查看# cat ftpusers 说明：在这个列表里边的用户名是不允许 ftp 登陆的。</p> <pre> root daemon bin sys adm lp uucp </pre>

	nuucp listen nobody noaccess nobody4
--	--

4.4 补丁

编号：1

要求内容	应根据需要及时进行补丁装载。对服务器系统应先进行兼容性测试。
操作指南	<p>1、参考配置操作</p> <p>先把补丁集拷贝到一个目录，如/08update，然后执行</p> <pre>#smit update_all</pre> <p>选择安装目录/08update 默认 SOFTWARE to update [_update_all] 选择不提交，保存被覆盖的文件，可以回滚操作，接受许可协议</p> <pre> COMMIT software updates? no SAVE replaced files? yes ACCEPT new license agreements? yes </pre> <p>然后回车执行安装。</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>查看最新的补丁号，确认已打上了最新补丁；</p> <p>2、检测操作</p> <p>检查某一个补丁，比如 LY59082 是否安装</p> <pre>#instfix -a -ivk LY59082</pre> <p>检查文件集（filesets）是否安装</p> <pre>#lslpp -l bos.adt.libm</pre> <p>3、补充说明</p> <p>补丁下载 http://www-933.ibm.com/eserver/support/fixes/</p>

4.5 日志

编号：1

要求内容	设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。
操作指南	<p>1、参考配置操作</p> <p>修改配置文件 vi /etc/syslog.conf，加上这几行：</p> <pre>auth.info\t\t/var/adm/authlog</pre>

	<pre>*.info;auth.none\t\t/var/adm/syslog\n"</pre> <p>建立日志文件，如下命令：</p> <pre>touch /var/adm/authlog /var/adm/syslog</pre> <pre>chown root:system /var/adm/authlog</pre> <p>重新启动 syslog 服务，依次执行下列命令：</p> <pre>stopsrc -s syslogd</pre> <pre>startsrc -s syslogd</pre> <p>AIX 系统默认不捕获登录信息到 syslogd，以上配置增加了验证信息发送到/var/adm/authlog 和/var/adm/syslog</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>列出用户账号、登录是否成功、登录时间、远程登录时的 IP 地址。</p> <p>2、检测操作</p> <pre>cat /var/adm/authlog</pre> <pre>cat /var/adm/syslog</pre> <p>3、补充说明</p>

编号： 2（可选）

要求内容	启用记录cron行为日志功能和cron/at的使用情况
操作指南	<p>1、参考配置操作</p> <p>cron/At的相关文件主要有以下几个：</p> <p>/var/spool/cron/crontabs 存放cron任务的目录</p> <p>/var/spool/cron/cron.allow 允许使用crontab命令的用户</p> <p>/var/spool/cron/cron.deny 不允许使用crontab命令的用户</p> <p>/var/spool/cron/atjobs 存放at任务的目录</p> <p>/var/spool/cron/at.allow 允许使用at的用户</p> <p>/var/spool/cron/at.deny 不允许使用at的用户</p> <p>使用crontab和at命令可以分别对cron和at任务进行控制。</p> <p>#crontab -l 查看当前的cron任务</p> <p>#at -l 查看当前的 at 任务</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>查看/var/spool/cron/目录下的文件配置是否按照以上要求进行了安全配置。如未配置则建议按照要求进行配置。</p>

编号： 3

要求内容	设备应配置权限，控制对日志文件读取、修改和删除等操作。
操作指南	1、参考配置操作

	配置日志文件权限，如下命令： <code>chmod 600 /var/adm/authlog</code> <code>chmod 640 /var/adm/syslog</code> 并设置了权限为其他用户和组禁止读写日志文件。
检测方法	1、判定条件 没有相应权限的用户不能查看或删除日志文件 2、检测操作 查看 <code>syslog.conf</code> 文件中配置的日志存放文件： <code>more /etc/syslog.conf</code> 使用 <code>ls -l /var/adm</code> 查看的目录下日志文件的权限，如： <code>authlog</code> 、 <code>syslog</code> 的权限应分别为 600、644。 3、补充说明 对于其他日志文件，也应该设置适当的权限，如登录失败事件的日志、操作日志，具体文件查看 <code>syslog.conf</code> 中的配置。

4.6 不必要的服务、端口

编号：1

要求内容	列出所需要服务的列表(包括所需的系统服务)，不在此列表的服务需关闭。
操作指南	1、参考配置操作 查看所有开启的服务： <code>#ps -e -f</code> 方法一：手动方式操作 在 <code>inetd.conf</code> 中关闭不用的服务 首先复制 <code>/etc/inet/inetd.conf</code> 。 <code>#cp /etc/inet/inetd.conf /etc/inet/inetd.conf.backup</code> 然后用vi编辑器编辑 <code>inetd.conf</code> 文件，对于需要注释掉的服务在相应行开头标记" <code>#</code> "字符，重启 <code>inetd</code> 服务,即可。 重新启用该服务，使用命令： <code>refresh -s inetd</code> 方法二：自动方式操作 A.把以下复制到文本里： <pre>for SVC in ftp telnet shell kshell login klogin exec \ echo discard chargen daytime time ttdbserver dtspc; do echo "Disabling \$SVC TCP" chsubserver -d -v \$SVC -p tcp done</pre> <pre>for SVC in ntalk rstatd rusersd rwalld sprayd pcnfsd \ echo discard chargen daytime time cmsd; do echo "Disabling \$SVC UDP"</pre>

	<pre>chsubserver -d -v \$SVC -p udp</pre> <p>done</p> <pre>refresh -s inetd</pre> <p>B.执行命令： #sh dis_server.sh</p> <p>2、补充操作说明 参考附录A，根据具体情况禁止不必要的基本网络服务。 注意：改变了“inetd.conf”文件之后，需要重新启动inetd。 对必须提供的服务采用tcpwapper来保护 并且为了防止服务取消后断线，一定要启用SSHD服务，用以登录操作和文件传输。</p>
检测方法	<p>1、判定条件 所需的服务都列出来； 没有不必要的服务；</p> <p>2、检测操作 查看所有开启的服务:cat /etc/inet/inetd.conf,cat /etc/inet/services</p> <p>3、补充说明 在/etc/inetd.conf文件中禁止下列不必要的基本网络服务。 Tcp服务如下： ftp telnet shell kshell login klogin exec UDP服务如下： ntalk rstatd rusersd rwalld sprayd pcnfsd 注意：改变了“inetd.conf”文件之后，需要重新启动inetd。 对必须提供的服务采用tcpwapper来保护</p>

4.7 文件与目录权限

编号：1

要求内容	控制用户缺省访问权限，当在创建新文件或目录时 应屏蔽掉新文件或目录不应有的访问允许权限。防止同属于该组的其它用户及别的组的用户修改该用户的文件或更高限制。
操作指南	<p>1、参考配置操作 A.设置所有存在账户的权限： lsuser -a home ALL awk '{print \$1}' while read user; do chuser umask=077 \$user done vi /etc/default/login 在末尾增加 umask 027</p> <p>B.设置默认的 profile，用编辑器打开文件/etc/security/user，找到 umask 这行，修改如下： Umask=077</p>

	<p>2、补充操作说明</p> <p>如果用户需要使用一个不同于默认全局系统设置的 <code>umask</code>，可以在需要的时候通过命令行设置，或者在用户的 <code>shell</code> 启动文件中配置。</p>
检测方法	<p>1、判定条件</p> <p>权限设置符合实际需要；不应有的访问允许权限被屏蔽掉；</p> <p>2、检测操作</p> <p>查看新建的文件或目录的权限，操作举例如下：</p> <pre>#ls -l dir ; #查看目录 dir 的权限</pre> <pre>#cat /etc/default/login 查看是否有 umask 027 内容</pre> <p>3、补充说明</p> <p><code>umask</code> 的默认设置一般为 <code>022</code>，这给新创建的文件默认权限 <code>755</code> ($777-022=755$)，这会给文件所有者读、写权限，但只给组成员和其他用户读权限。</p> <p><code>umask</code> 的计算：</p> <p><code>umask</code> 是使用八进制数据代码设置的，对于目录，该值等于八进制数据代码 <code>777</code> 减去需要的默认权限对应的八进制数据代码值；对于文件，该值等于八进制数据代码 <code>666</code> 减去需要的默认权限对应的八进制数据代码值。</p>

编号： 2

要求内容	对文件和目录进行权限设置，合理设置重要目录和文件的权限
操作指南	<p>1、参考配置操作</p> <p>查看重要文件和目录权限：<code>ls -l</code></p> <p>更改权限：</p> <p>对于重要目录，建议执行如下类似操作：</p> <pre># chmod -R 750 /etc/init.d/*</pre> <p>这样只有 <code>root</code> 可以读、写和执行这个目录下的脚本。</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>用 <code>root</code> 外的其它帐户登录，对重要文件和目录进行删除、修改等操作不能够成功即为符合。</p> <p>2、检测操作</p> <p>查看重要文件和目录权限：<code>ls -l</code></p> <p>用 <code>root</code> 外的其它帐户登录，对重要文件和目录进行删除、修改等操作</p> <p>3、补充说明</p>

4.8 系统 Banner 设置

要求内容	修改系统 banner，避免泄漏操作系统名称，版本号，主机名称等，并且给出登陆告警信息
操作指南	<p>1、参考配置操作</p> <p>设置系统 Banner 的操作如下：</p> <p>在/etc/security/login.cfg 文件中，在 default 小节增加：</p> <pre>herald = "ATTENTION:You have logged onto a secured server..All accesses logged.\n\nlogin:"</pre>
检测方法	查看/etc/security/login.cfg 文件中的配置是否按照以上要求进行了配置

4.9 登陆超时时间设置

要求内容	对于具备字符交互界面的设备，配置定时帐户自动登出
操作指南	<p>1、参考配置操作</p> <p>设置登陆超时时间为 300 秒，修改/etc/security/.profile 文件，增加一行：</p> <pre>TMOUT=300; TIMEOUT=300; export readonly TMOUT TIMEOUT</pre> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>查看/etc/security/.profile 文件中的配置，是否存在登陆超时时间的设置。如未设置，则建议应按要求进行配置</p>

4.10 内核调整设置

要求内容	防止堆栈缓冲溢出
操作指南	<p>1、参考配置操作</p> <p>编辑/etc/security/limits 并且改变 core 值为 0，并增加一行在后面，如下：</p> <pre>core 0 core_hard = 0</pre> <p>保存文件后退出，执行命令：</p> <pre>echo "# Added by Nsfocus Security Benchmark" >> /etc/profile echo "ulimit -c 0" >> /etc/profile chdev -l sys0 -a fullcore=false</pre> <p>1、补充操作说明</p> <p>应用程序在发生错误的时候会把自身的敏感信息从内存里 DUMP</p>

	到文件，一旦被攻击者获取容易引发攻击。 注： 内核参数改动后需要重启服务器才生效。
检测方法	1、判定条件 能够防止 core 文件产生 2、检测操作 查看/etc/security/limits 文件： cat /etc/security/limits 是否有如下两行： core 0 core_hard = 0 查看/etc/ profile 文件： cat /etc/security/limits 是否有如下行： ulimit -c 0

4.11 SSH 加密协议

要求内容	对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议，并安全配置 SSHD 的设置。
操作指南	1、参考配置操作 把如下 shell 保存后，运行，会修改 ssh 的安全设置项： unalias cp rm mv case `find /usr /etc -type f grep -c ssh_config` in 0) echo "Cannot find ssh_config" ;; 1) DIR=`find /usr /etc -type f 2>/dev/null \\\n grep ssh_config\$ sed -e "s:/ssh_config::" cd \$DIR cp ssh_config ssh_config.tmp awk '/^#? *Protocol/ { print "Protocol 2"; next }; { print }' ssh_config.tmp > ssh_config if ["`grep -El ^Protocol ssh_config`" = ""]; then echo 'Protocol 2' >> ssh_config fi rm ssh_config.tmp chmod 600 ssh_config ;; *) echo "You have multiple sshd_config files. Resolve" echo "before continuing." ;; esac #也可以手动编辑 ssh_config，在 "Host *"后输入 "Protocol 2", cd \$DIR

	<pre> cp sshd_config sshd_config.tmp awk '/^#? *Protocol/ { print "Protocol 2"; next }; /^#? *X11Forwarding/ \ { print "X11Forwarding yes"; next }; /^#? *IgnoreRhosts/ \ { print "IgnoreRhosts yes"; next }; /^#? *RhostsAuthentication/ \ { print " RhostsAuthentication no"; next }; /^#? *RhostsRSAAuthentication/ \ { print "RhostsRSAAuthentication no"; next }; /^#? *HostbasedAuthentication/ \ { print "HostbasedAuthentication no"; next }; /^#? *PermitRootLogin/ \ { print "PermitRootLogin no"; next }; /^#? *PermitEmptyPasswords/ \ { print "PermitEmptyPasswords no"; next }; /^#? *Banner/ \ { print "Banner /etc/motd"; next }; {print}' sshd_config.tmp > sshd_config rm sshd_config.tmp chmod 600 sshd_config Protocol 2 #使用 ssh2 版本 X11Forwarding yes #允许窗口图形传输使用 ssh 加密 IgnoreRhosts yes#完全禁止 SSHD 使用.rhosts 文件 RhostsAuthentication no #不设置使用基于 rhosts 的安全验证 RhostsRSAAuthentication no #不设置使用 RSA 算法的基于 rhosts 的安全验证 HostbasedAuthentication no #不允许基于主机白名单方式认证 PermitRootLogin no #不允许 root 登录 PermitEmptyPasswords no #不允许空密码 Banner /etc/motd #设置 ssh 登录时显示的 banner 2、补充操作说明 查看 SSH 服务状态： # ps -elfgrep ssh </pre>
检测方法	<p>2、判定条件</p> <pre># ps -elfgrep ssh</pre> <p>是否有 ssh 进程存在</p> <p>2、检测操作</p> <p>查看 SSH 服务状态：</p> <pre># ps -elfgrep ssh</pre> <p>查看 telnet 服务状态：</p>

	# ps -elfgrep telnet
--	----------------------

4.12 FTP 设置

编号 1:

要求内容	禁止 root 登陆 FTP
操作指南	1、参考配置操作 Echo root >>/etc/ftpusers
检测方法	使用 root 登录 ftp

编号 2:

要求内容	禁止匿名 ftp
操作指南	1、参考配置操作 默认不支持匿名，需要做专门的配置。 检查方法: 使用ftp 做匿名登录尝试，如能登录，则删除/etc/passwd下的ftp账号。
检测方法	检查方法: 使用 ftp 做匿名登录尝试

编号 3:

要求内容	修改FTP banner 信息
操作指南	1、参考配置操作 cat << EOF >> /etc/ftpmotd Authorized uses only. All activity may be monitored and reported EOF
检测方法	1、判断依据 ftp登录尝试 2、检查操作

附录 A：端口及服务

服务名称	端口	应用说明	关闭方法	处置建议
daytime	13/tcp	RFC867 白天协议	#daytime stream tcp nowait root internal	建议关闭
	13/udp	RFC867 白天协议	#daytime dgram udp nowait root internal	
time	37/tcp	时间协议	#time stream tcp nowait root internal	

echo	7/tcp	RFC862_回声协议	#echo stream tcp nowait root internal	
	7/udp	RFC862_回声协议	#echo dgram udp nowait root internal	
discard	9/tcp	RFC863 废除协议	#discard stream tcp nowait root internal	
	9/udp		#discard dgram udp nowait root internal	
chargen	19/tcp	RFC864 字符产生 协议	#chargen stream tcp nowait root internal	
	19/udp		#chargen dgram udp nowait root internal	
ftp	21/tcp	文件传输协议(控制)	#ftp stream tcp nowait root /usr/sbin/ftpd	根据实际情况选择开 放
telnet	23/tcp	虚拟终端协议	#telnet stream tcp nowait root /usr/sbin/telnetd telnetd	根据实际情况选择开 放
sendmail	25/tcp	简单邮件发送协议	rc.tcpip/sendmail	建议关闭
names	53/udp	域名服务	/etc/rc.tcpip	根据实际情况选择开 放
	53/tcp	域名服务	/etc/rc.tcpip	根据实际情况选择开 放
login	513/tcp	远程登录	#login stream tcp nowait root /usr/sbin/rlogind rlogind	根据实际情况选择开 放
shell	514/tcp	远程命令, no passwd used	#shell stream tcp nowait root /usr/sbin/remshd remshd	根据实际情况选择开 放
exec	512/tcp	remote execution, passwd required	#exec stream tcp nowait root /usr/sbin/rexecd rexecd	根据实际情况选择开 放
ntalk	518/udp	new talk, conversation	#ntalk dgram udp wait root /usr/sbin/ntalkd ntalkd	建议关闭
ident	113/tcp	auth	#ident stream tcp wait bin /usr/sbin/identd identd	建议关闭
lpd	515/tcp	远程打印缓存	#printer stream tcp nowait root /usr/sbin/rpdaemon rpdaemon -i	强烈建议关闭
tftp	69/udp	普通文件传输协议	#tftp dgram udp nowait root internal	强烈建议关闭

kshell	544/tcp	Kerberos remote shell -kfall	#kshell stream tcp nowait root /usr/lbin/remshd remshd -K	建议关闭
klogin	543/tcp	Kerberos rlogin -kfall	#klogin stream tcp nowait root /usr/lbin/rlogind rlogind -K	建议关闭
recserv	7815/tcp	X 共享接收服务	#recserv stream tcp nowait root /usr/lbin/recserv recserv -display :0	建议关闭
dtspcd	6112/tcp	子进程控制	#dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd	强烈建议关闭
registrar	1712/tcp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据情况选择开放
	1712/udp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar /etc/opt/resmon/lbin/registrar	根据情况选择开放
	动态端口	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据情况选择开放
portmap	111/tcp	端口映射	/etc/rc.tcpip	根据情况选择开放
snmp	161/udp	简单网络管理协议 (Agent)	rc.tcpip/snmpd	根据情况选择开放
snmp	7161/tcp	简单网络管理协议 (Agent)	rc.tcpip/snmpd	根据情况选择开放
snmp-trap	162/udp	简单网络管理协议 (Traps)	rc.tcpip/snmpd	根据情况选择开放
dtlogin	177/udp	启动图形控制	usr/dt/config/Xaccess	根据情况选择开放
	6000/tcp	X 窗口服务	usr/dt/config/Xaccess	根据情况选择开放
	动态端口	启动图形控制	usr/dt/config/Xaccess	根据情况选择开放
syslogd	514/udp	系统日志服务	/etc/rc.tcpip	建议保留
nfs	2049/tcp	NFS 远程文件系统	/etc/rc.nfs	强烈建议关闭
	2049/udp	NFS 远程文件系统	/etc/rc.nfs	强烈建议关闭
rpc.ttdbserver	动态端口	HP-UX ToolTalk database server	#rpc xti tcp swait root /usr/dt/bin/rpc.ttdbserver 100083 1	强烈建议关闭

			/usr/dt/bin/rpc.ttdbserver	
rpc.cmsd	动态端口	后台进程管理服务	#rpc dgram udp wait root /usr/dt/bin/rpc.cmsd 100068 2-5 rpc.cmsd	强烈建议关闭

中国电信 HP-UX 操作系统 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	2
4.1 帐号.....	2
4.2 口令.....	3
4.3 授权.....	6
4.4 远程维护.....	9
4.5 补丁.....	11
4.6 日志.....	12
4.7 不必要的服务、端口.....	14
4.8 修改 Banner 信息.....	15
4.9 登陆超时时间设置.....	15
4.10 内核调整设置.....	15
4.11 删除潜在危险文件.....	15
4.12 FTP 设置.....	16
附录 A：端口及服务.....	17

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》（本规范）
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用 HP-UX 操作系统的设备。本规范明确了安全配置的基本要求，适用于所有的安全等级，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 HP-UX11v2\11v3 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1732-2008 《固定通信网安全防护要求》

YD/T 1734-2008 《移动通信网安全防护要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1742-2008 《接入网安全防护要求》

YD/T 1744-2008 《传送网安全防护要求》

YD/T 1746-2008 《IP 承载网安全防护要求》

YD/T 1748-2008 《信令网安全防护要求》

YD/T 1750-2008 《同步网安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

FTP	File Transfer Protocol	文件传输协议
UDP	User Datagram Protocol	用户数据包协议
TCP	Transmission Control Protocol	传输控制协议

4 安全配置要求

4.1 帐号

编号： 1

要求内容	应按照不同的用户分配不同的账号，避免不同用户间共享账号，避免用户账号和设备间通信使用的账号共享。
操作指南	1、参考配置操作 为用户创建账号： #useradd username #创建账号 #passwd username #设置密码 修改权限： #chmod 750 directory #其中 750 为设置的权限，可根据实际情况设置相应的权限，directory 是要更改权限的目录 使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。 2、补充操作说明
检测方法	1、判定条件 能够登录成功并且可以进行常用操作； 2、检测操作 使用不同的账号进行登录并进行一些常用操作； 3、补充说明

编号： 2

要求内容	应删除或锁定与设备运行、维护等工作无关的账号。
操作指南	1、参考配置操作 删除用户：#userdel username; 锁定用户： 1)修改/etc/shadow 文件，用户名后加 NP 2)将/etc/passwd 文件中的 shell 域设置成/bin/noshell 3)#passwd -l username 只有具备超级用户权限的使用者方可使用，#passwd -l username 锁定用户,用#passwd -d username 解锁后原有密码失效，登录需输入新密码，修改/etc/shadow 能保留原有密码。 2、补充操作说明 需要锁定的用户：lp,nuucp,hpdb,www,demon。 注：无关的账号主要指测试帐户、共享帐号、长期不用账号（半年以上未用）等
检测方法	1、判定条件 被删除或锁定的账号无法登录成功； 2、检测操作

	<p>使用删除或锁定的与工作无关的账号登录系统；</p> <p>3、补充说明</p> <p>需要锁定的用户：lp,nuucp,hpdb,www,demon。</p>
--	---

编号： 3

要求内容	根据系统要求及用户的业务需求，建立多帐户组，将用户账号分配到相应的帐户组。
操作指南	<p>1、参考配置操作</p> <p>创建帐户组：</p> <p>#groupadd -g GID groupname #创建一个组，并为其设置 GID 号，若不设 GID，系统会自动为该组分配一个 GID 号；</p> <p>#usermod -g group username #将用户 username 分配到 group 组中。</p> <p>查询被分配到的组的 GID：#id username</p> <p>可以根据实际需求使用如上命令进行设置。</p> <p>2、补充操作说明</p> <p>可以使用 -g 选项设定新组的 GID。0 到 499 之间的值留给 root、bin、mail 这样的系统账号，因此最好指定该值大于 499。如果新组名或者 GID 已经存在，则返回错误信息。</p> <p>当 group_name 字段长度大于八个字符，groupadd 命令会执行失败；当用户希望以其他用户组成员身份出现时，需要使用 newgrp 命令进行更改，如#newgrp sys 即把当前用户以 sys 组身份运行；</p>
检测方法	<p>1、判定条件</p> <p>可以查看到用户账号分配到相应的帐户组中；</p> <p>或都通过命令检查账号是否属于应有的组：</p> <p>#id username</p> <p>2、检测操作</p> <p>查看组文件：cat /etc/group</p> <p>3、补充说明</p> <p>文件中的格式说明：</p> <p>group_name::GID:user_list</p>

4.2 口令

编号： 1

要求内容	对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。
操作指南	<p>1 参考配置操作</p> <pre>ch_rc -a -p MIN_PASSWORD_LENGTH=8 /etc/default/security ch_rc -a -p PASSWORD_HISTORY_DEPTH=10 \ /etc/default/security ch_rc -a -p PASSWORD_MIN_UPPER_CASE_CHARS=1 \ /etc/default/security</pre>

	<pre>ch_rc -a -p PASSWORD_MIN_DIGIT_CHARS=1 \ /etc/default/security ch_rc -a -p PASSWORD_MIN_SPECIAL_CHARS=1 \ /etc/default/security ch_rc -a -p PASSWORD_MIN_LOWER_CASE_CHARS=1 \ /etc/default/security modprdef -m nullpw=NO modprdef -m rstrpw=YES</pre> <p>MIN_PASSWORD_LENGTH=8 #设定最小用户密码长度为 8 位 PASSWORD_MIN_UPPER_CASE_CHARS=1 #表示至少包括 1 个大写字母 PASSWORD_MIN_DIGIT_CHARS=1 #表示至少包括 1 个数字 PASSWORD_MIN_SPECIAL_CHARS=1 #表示至少包括 1 个特殊字符（特殊字符可以包括控制符以及诸如星号和斜杠之类的符号） PASSWORD_MIN_LOWER_CASE_CHARS=1 #表示至少包括 1 个小写字母</p> <p>当用 root 帐户给用户设定口令的时候不受任何限制，只要不超长。</p> <p>2、补充操作说明 不同的 HP-UX 版本可能会有差异，请查阅当前系统的 man page security(5) 详细说明</p>
检测方法	<p>1、判定条件 不符合密码强度的时候，系统对口令强度要求进行提示； 符合密码强度的时候，可以成功设置；</p> <p>2、检测操作 1、检查口令强度配置选项是否可以如下配置：</p> <ul style="list-style-type: none"> i. 配置口令的最小长度； ii. 将口令配置为强口令。 <p>2、创建一个普通账号，为用户配置与用户名相同的口令、只包含字符或数字的简单口令以及长度短于 8 位的口令，查看系统是否对口令强度要求进行提示；输入带有特殊符号的复杂口令、普通复杂口令，查看系统是否可以成功设置。</p>

编号： 2

要求内容	对于采用静态口令认证技术的设备，帐户口令的生存期不长于 90 天。
操作指南	<p>1、参考配置操作 以下的 shell 语句将设置除 root 外的所有有效登录的账号密码过期和过前期的收到警告设置：</p> <pre>logins -ox \</pre>

	<pre> awk -F: '(\$8 != "LK" && \$1 != "root") { print \$1 }' \ while read logname; do passwd -x 91 -n 7 -w 28 "\$logname" /usr/sbin/modprpw -m exptm=90,mintm=7,expwarn=30 \ "\$logname" done echo PASSWORD_MAXDAYS=91 >> /etc/default/security echo PASSWORD_MINDAYS=7 >> /etc/default/security echo PASSWORD_WARNDAYS=28 >> /etc/default/security /usr/sbin/modprdef -m exptm=90,expwarn=30</pre> <p>用户将在密码过期前的 30 天收到警告信息（28 天没有运行在 HP-UX 的 Trusted 模式）</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件 登录不成功；</p> <p>2、检测操作 使用超过 90 天的帐户口令登录；</p> <p>3、补充说明 测试时可以将 90 天的设置缩短来做测试。</p>

编号： 3

要求内容	对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近 5 次（含 5 次）内已使用的口令。
操作指南	<p>1、参考配置操作 vi /etc/default/passwd ， 修改设置如下 HISTORY=5</p> <p>2、补充操作说明 #HISTORY sets the number of prior password changes to keep and # check for a user when changing passwords. Setting the HISTORY # value to zero (0), or removing/commenting out the flag will # cause all users' prior password history to be discarded at the # next password change by any user. No password history will # be checked if the flag is not present or has zero value. # The maximum value of HISTORY is 26. NIS 系统无法生效，非 NIS 系统或 NIS+ 系统能够生效。</p>
检测方法	<p>1、判定条件 设置密码不成功</p> <p>2、检测操作 cat /etc/default/passwd ， 设置如下 HISTORY=5</p>

	3、补充说明 默认没有 HISTORY 的标记，即不记录以前的密码 NIS 系统无法生效，非 NIS 系统或 NIS+系统能够生效。
--	---

编号： 4

要求内容	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。
操作指南	1、参考配置操作 指定当本地用户登陆失败次数等于或者大于允许的重试次数则账号被锁定： <pre>logins -ox \ awk -F: '(\$8 != "LK" && \$1 != "root") { print \$1 }' \ while read logname; do /usr/sbin/modprpw -m umaxlntr=6 "\$logname" done modprdef -m umaxlntr=6 echo AUTH_MAXTRIES=6 >> /etc/default/security</pre> 除 root 外的有效账号都将被设置重复登录失败次数为 6 2、补充操作说明
检测方法	1、判定条件 帐户被锁定，不再提示让再次登录； 2、检测操作 创建一个普通账号，为其配置相应的口令；并用新建的账号通过错误的口令进行系统登录 6 次以上（不含 6 次）； 1、补充说明 root 账号不在锁定的限制范围内

4.3 授权

编号： 1

要求内容	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	1、参考配置操作 通过 chmod 命令对目录的权限进行实际设置。 2、补充操作说明 etc/passwd 必须所有用户都可读，root 用户可写 -rw-r—r— /etc/shadow 只有 root 可读 -r----- /etc/group 必须所有用户都可读，root 用户可写 -rw-r—r— 使用如下命令设置： <pre>chmod 644 /etc/passwd chmod 600 /etc/shadow</pre>

	<p>chmod 644 /etc/group</p> <p>如果是有写权限，就需移去组及其它用户对/etc 的写权限（特殊情况除外）</p> <p>执行命令#chmod -R go-w /etc</p>
检测方法	<p>1、判定条件</p> <p>1、设备系统能够提供用户权限的配置选项，并记录对用户进行权限配置是否必须在用户创建时进行；</p> <p>2、记录能够配置的权限选项内容；</p> <p>3、所配置的权限规则应能够正确应用，即用户无法访问授权范围之外的系统资源，而可以访问授权范围之内的系统资源。</p> <p>2、检测操作</p> <p>1、利用管理员账号登录系统，并创建 2 个不同的用户；</p> <p>2、创建用户时查看系统是否提供了用户权限级别以及可访问系统资源和命令的选项；</p> <p>3、为两个用户分别配置不同的权限，2 个用户的权限差异应能够分别在用户权限级别、可访问系统资源以及可用命令等方面予以体现；</p> <p>4、分别利用 2 个新建的账号访问设备系统，并分别尝试访问允许访问的内容和不允许访问的内容，查看权限配置策略是否生效。</p> <p>3、补充说明</p>

编号： 2

要求内容	<p>控制用户缺省访问权限，当在创建新文件或目录时 应屏蔽掉新文件或目录不应有的访问允许权限。防止同属于该组的其它用户及别的组的用户修改该用户的文件或更高限制。</p>
操作指南	<p>1、参考配置操作</p> <p>设置默认权限：</p> <p>Vi /etc/default/security 在末尾增加 umask 027</p> <p>修改文件或目录的权限，操作举例如下：</p> <p>#chmod 444 dir ; #修改目录 dir 的权限为所有人都为只读。</p> <p>根据实际情况设置权限；</p> <p>2、补充操作说明</p> <p>如果用户需要使用一个不同于默认全局系统设置的 umask，可以在需要的时候通过命令行设置，或者在用户的 shell 启动文件中配置。</p>
检测方法	<p>1、判定条件</p> <p>权限设置符合实际需要；不应有的访问允许权限被屏蔽掉；</p> <p>2、检测操作</p> <p>查看新建的文件或目录的权限，操作举例如下：</p> <p>#ls -l dir ; #查看目录 dir 的权限</p> <p>#cat /etc/default/login 查看是否有 umask 027 内容</p>

	<p>3、补充说明</p> <p>umask 的默认设置一般为 022，这给新创建的文件默认权限 755 (777-022=755)，这会给文件所有者读、写权限，但只给组成员和其他用户读权限。</p> <p>umask 的计算：</p> <p>umask 是使用八进制数据代码设置的，对于目录，该值等于八进制数据代码 777 减去需要的默认权限对应的八进制数据代码值；对于文件，该值等于八进制数据代码 666 减去需要的默认权限对应的八进制数据代码值。</p>
--	---

编号：3

要求内容	<p>如果需要启用 FTP 服务，控制 FTP 进程缺省访问权限，当通过 FTP 服务创建新文件或目录时应屏蔽掉新文件或目录不应有的访问允许权限。</p>
操作指南	<p>1、参考配置操作</p> <pre> if [["\$(uname -r)" = B.10*]]; then ftpusers=/etc/ftpusers else ftpusers=/etc/ftpd/ftpusers fi for name in root daemon bin sys adm lp \ uucp nuucp nobody hpdb useradm do echo \$name done >> \$ftpusers sort -u \$ftpusers > \$ftpusers.tmp cp \$ftpusers.tmp \$ftpusers rm -f \$ftpusers.tmp chown bin:bin \$ftpusers chmod 600 \$ftpusers </pre> <p>2、补充操作说明</p> <p>查看# cat ftpusers</p> <p>说明： 在这个列表里边的用户名是不允许 ftp 登陆的。</p> <pre> root daemon bin sys adm lp uucp nuucp listen nobody </pre>

	hpdb useradm
检测方法	<p>1、判定条件 权限设置符合实际需要；不应有的访问允许权限被屏蔽掉；</p> <p>2、检测操作 查看新建的文件或目录的权限，操作举例如下： <code>#more /etc/ [ftpd]/ftpusers</code> <code>#more /etc/passwd</code></p> <p>3、补充说明 查看<code># cat ftpusers</code> 说明：在这个列表里边的用户名是不允许 ftp 登陆的。</p> <p>root daemon bin sys adm lp uucp nuucp listen nobody hpdb useradm</p>

4.4 远程维护

编号：1

要求内容	限制具备超级管理员权限的用户远程登录。远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到超级管理员权限账号后执行相应操作。
操作指南	<p>2、参考配置操作 编辑<code>/etc/securetty</code>，加上： console 保存后退出，并限制其他用户对此文本的所有权限： <code>chown root:sys /etc/securetty</code> <code>chmod 600 /etc/securetty</code> 此项只能限制 root 用户远程使用 telnet 登录。用 ssh 登录，修改此项不会看到效果的</p> <p>2、补充操作说明 如果限制 root 从远程 ssh 登录，修改<code>/etc/ssh/sshd_config</code> 文件，将 <code>PermitRootLogin yes</code> 改为 <code>PermitRootLogin no</code>，重启 sshd 服务。</p>
检测方法	<p>1、判定条件 root 远程登录不成功，提示“没有权限”； 普通用户可以登录成功，而且可以切换到 root 用户；</p>

	<p>2、检测操作</p> <p>root 从远程使用 telnet 登录； 普通用户从远程使用 telnet 登录； root 从远程使用 ssh 登录； 普通用户从远程使用 ssh 登录；</p> <p>3、补充说明</p> <p>限制 root 从远程 ssh 登录，修改/etc/ssh/sshd_config 文件，将 PermitRootLogin yes 改为 PermitRootLogin no，重启 sshd 服务。</p>
--	--

编号：2

要求内容	对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议，禁止使用 telnet 等明文传输协议进行远程维护；
操作指南	<p>1、下载和安装 OpenSSH</p> <p>在网站上免费获取 OpenSSH http://software.hp.com/ ； 并根据安装文件说明执行安装步骤 。</p> <p>2、完成下面安装后的配置：</p> <pre>cd /opt/ssh/etc cp -p sshd_config sshd_config.tmp awk ' /^Protocol/ { \$2 = "2" }; /^X11Forwarding/ { \$2 = "yes" }; /^IgnoreRhosts/ { \$2 = "yes" }; /^RhostsAuthentication/ { \$2 = "no" }; /^RhostsRSAAuthentication/ { \$2 = "no" }; /^(^# ^)PermitRootLogin/ { \$1 = "PermitRootLogin"; \$2 = "no" }; /^PermitEmptyPasswords/ { \$2 = "no" }; /^#Banner/ { \$1 = "Banner"; \$2 = "/etc/issue" } { print }' sshd_config.tmp > sshd_config rm -f sshd_config.tmp chown root:sys ssh_config sshd_config chmod go-w ssh_config sshd_config</pre> <p>先拷贝一份配置，再用 awk 生成一份修改了安全配置的临时文件，最后替换原始配置文件 ssh_config，其中配置含义如下：</p> <p>Protocol = 2 #使用 ssh2 版本</p> <p>X11Forwarding #允许窗口图形传输使用 ssh 加密</p> <p>IgnoreRhosts =yes#完全禁止 SSHD 使用.rhosts 文件</p> <p>RhostsAuthentication=no #不设置使用基于 rhosts 的安全验证</p> <p>RhostsRSAAuthentication=no #不设置使用 RSA 算法的基于 rhosts 的</p>

	<p>安全验证。</p> <p>3、补充操作说明</p> <p>查看 SSH 服务状态：</p> <pre># ps -elfgrep ssh</pre> <p>注：禁止使用 telnet 等明文传输协议进行远程维护；如特别需要，需采用访问控制策略对其进行限制；</p>
检测方法	<p>1、判定条件</p> <pre># ps -elfgrep ssh</pre> <p>是否有 ssh 进程存在 是否有 telnet 进程存在</p> <p>2、检测操作</p> <p>查看 SSH 服务状态：</p> <pre># ps -elfgrep ssh</pre> <p>查看 telnet 服务状态：</p> <pre># ps -elfgrep telnet</pre> <p>3、补充说明</p>

4.5 补丁

编号： 1

要求内容	应根据需要及时进行补丁装载。对服务器系统应先进行兼容性测试。
操作指南	<p>1、参考配置操作</p> <p>看版本是否为最新版本。</p> <p>执行下列命令，查看版本及大补丁号。</p> <pre>#uname -a</pre> <p>HP-UX: http://us-support.external.hp.com/</p> <p>执行下列命令，查看各包的补丁号</p> <pre>#swlist</pre> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>看版本是否为最新版本。</p> <pre># uname -a</pre> <p>查看版本及大补丁号</p> <pre>#swlist</pre> <p>命令检补丁号</p> <p>2、检测操作</p> <p>在保证业务及网络安全的前提下，经过实验室测试后，更新使用最新版本的操作系统补丁</p> <p>3、补充说明</p>

--	--

4.6 日志

编号： 1

要求内容	打开 syslog 系统日志审计功能有助于系统的日常维护和故障排除，或者防止被攻击后查看日志采取防护补救措施，增强系统安全日志。
操作指南	1、参考配置操作 修改配置文件 vi /etc/syslog.conf， 配置如下类似语句： *.err;kern.debug;daemon.notice; /var/adm/messages 定义为需要保存的设备相关安全事件。 2、补充操作说明
检测方法	1、判定条件 查看/var/adm/messages，记录有需要的设备相关的安全事件。 2、检测操作 修改配置文件 vi /etc/syslog.conf， 配置如下类似语句： *.err;kern.debug;daemon.notice; /var/adm/messages 定义为需要保存的设备相关安全事件。 3、补充说明

编号： 2

要求内容	设备应配置权限，控制对日志文件读取、修改和删除等操作。
操作指南	1、参考配置操作 检查系统日志： <pre>awk < /etc/syslog.conf ' \$0 !~ /^#/ && \$2 ~ "/" { print \$2 } ' sort -u while read file do if [-d "\$file" -o -c "\$file" -o \ -b "\$file" -o -p "\$file"] then : elif [! -f "\$file"] then mkdir -p "\$(dirname "\$file")" touch "\$file" chmod 640 "\$file" else chmod o-w "\$file" fi</pre>

	<p>done</p> <p>检查其他日志：</p> <p>hostname=`uname -n`</p> <p>chmod o-w</p> <p>/tmp/snmpd.log \</p> <p>/var/X11/Xserver/logs/X0.log</p> <p>/var/X11/Xserver/logs/X1.log</p> <p>/var/X11/Xserver/logs/X2.log</p> <p>/var/adm/automount.log</p> <p>/var/adm/snmpd.log</p> <p>/var/opt/dce/svc/error.log</p> <p>/var/opt/dce/svc/fatal.log</p> <p>/var/opt/dce/svc/warning.log</p> <p>/var/opt/dde/dde_error_log</p> <p>/var/opt/hppak/hppak_error_log</p> <p>/var/opt/ignite/logs/makrec.log1</p> <p>/var/opt/ignite/recovery/fstab</p> <p>/var/opt/ignite/recovery/group.makrec</p> <p>/var/opt/ignite/recovery/passwd.makrec</p> <p>/var/sam/hpbottom.dion</p> <p>/var/sam/hpbottom.iout</p> <p>/var/sam/hpbottom.iout.old</p> <p>"/var/sam/\$hostname.dion"</p> <p>"/var/sam/\$hostname.iout"</p> <p>"/var/sam/\$hostname.iout.old"</p> <p>/var/sam/lock</p> <p>/var/sam/log/samlog</p> <p>/var/sam/log/sam_tm_work</p> <p>/var/adm/sw</p> <p>/var/adm/sw/save</p> <p>/var/adm/sw/patch</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>使用 ls -l 命令依次检查系统日志的读写权限</p> <p>3、补充说明</p>

编号：3（可选）

要求内容	设备配置远程日志功能，将需要重点关注的日志内容传输到日志服务器。
操作指南	<p>1、参考配置操作</p> <p>修改配置文件 vi /etc/syslog.conf，</p> <p>加上这一行：</p>

	<p>*.* @192.168.0.1</p> <p>可以将"*.*"替换为你实际需要的日志信息。比如: kern.* / mail.* 等等。</p> <p>可以将此处 192.168.0.1 替换为实际的 IP 或域名。</p> <p>重新启动 syslog 服务, 执行下列命令:</p> <pre>/sbin/init.d/syslogd stop start</pre> <p>2、补充操作说明</p> <p>注意: *.*和@之间为一个 Tab</p>
检测方法	<p>1、判定条件</p> <p>设备配置远程日志功能, 将需要重点关注的日志内容传输到日志服务器。</p> <p>2、检测操作</p> <p>查看日志服务器上的所收到的日志文件。</p> <p>3、补充说明</p>

4.7 不必要的服务、端口

要求内容	列出所需要服务的列表(包括所需的系统服务), 不在此列表的服务需关闭。
操作指南	<p>1、参考配置操作</p> <p>参考附录A, 根据具体情况关闭不必要的服务</p> <p>查看所有开启的服务:</p> <pre>#ps -ef</pre> <pre>#chkconfig --list</pre> <pre>#cat /etc/inet/inetd.conf</pre> <p>在inetd.conf中关闭不用的服务 首先复制/etc/inet/inetd.conf。 #cp /etc/inet/inetd.conf /etc/inet/inetd.conf.backup 然后用vi编辑器编辑inetd.conf文件, 对于需要注释掉的服务在相应行开头标记"#"字符, 重启inetd服务, 即可。</p>
检测方法	<p>1、判定条件</p> <p>所需的服务都列出来;</p> <p>没有不必要的服务;</p> <p>2、检测操作</p> <pre>#ps -ef</pre> <pre>#chkconfig --list</pre> <pre>#cat /etc/inet/inetd.conf</pre> <p>3、补充说明</p> <p>在/etc/inetd.conf文件中禁止不必要的基本网络服务。</p> <p>注意: 改变了“inetd.conf”文件之后, 需要重新启动inetd。</p> <p>对必须提供的服务采用tcpwrapper来保护</p>

4.8 修改 Banner 信息

要求内容	修改系统 Banner 信息
操作指南	1、参考配置操作 在 UNIX 下修改或增加 /etc/motd 文件中的 banner 信息 2、补充操作说明
检测方法	1、判定条件 检查/etc/motd 文件中的 banner 信息

4.9 登陆超时时间设置

要求内容	对于具备字符交互界面的设备，配置定时帐户自动登出
操作指南	2、参考配置操作 可以在用户的.profile 文件中"HISTFILESIZE="后面增加如下行： vi /etc/profile \$ TMOUT=300（可根据情况设定）;export TMOUT 改变这项设置后，重新登录才能有效 2、补充操作说明
检测方法	1、判定条件 查看/etc/profile 文件的配置，TMOUT=180

4.10 内核调整设置

要求内容	防止堆栈缓冲溢出
操作指南	1、参考配置操作 HP-UX 11iv2 和更后面的版本用以下语句： kctune -K executable_stack=0 HP-UX 11i 版本用以下语句： /usr/sbin/kmtune -s executable_stack=0 && mk_kernel && kmupdate HP-UX 11i 之前的版本不支持，请升级 2、补充操作说明 内核参数改动后需要重启服务器才生效。
检测方法	1、判定条件 能够防止堆栈缓冲溢出 2、检测操作

4.11 删除潜在危险文件

要求内容	/rhost、/netrc或/root/.rhosts、/root/.netrc文件都具有潜在的危險，
------	---

	如果没有应用，应该删除
操作指南	1、参考配置操作 Mv /.rhost /.rhost.bak Mv /.netr /.netr.bak Cd root Mv .rhost .rhost.bak Mv .netr .netr.bak 2、补充操作说明 注意系统版本，用相应的方法执行
检测方法	1、判定条件 2、检测操作 登陆系统判断 Cat /etc/passwd

4.12 FTP 设置

编号 1:

要求内容	禁止 root 登陆 FTP
操作指南	1、参考配置操作 限制 root 帐户 ftp 登录: 通过修改 ftpusers 文件，增加帐户 #vi /etc/ftpd/ftpusers root
检测方法	运行 cat /etc/ftpusers 检查文件中内容是否包含 root

编号 2:

要求内容	禁止匿名 ftp
操作指南	1、参考配置操作 在/etc/passwd文件中删除匿名用户。 使用文本编辑器打开/etc/passwd文件，删除密码域为*的行，如： ftp: *: 500: 21: Anonymous FTP: /home/ftp: /usr/bin/false
检测方法	通过 Anonymous 登录会被拒绝。

编号 3:

要求内容	修改FTP banner 信息
操作指南	1、参考配置操作 1) 首先修改/etc/inetd.conf文件 ftp stream tcp nowait root /usr/sbin/ftpd ftpd -a /etc/ftpd/ftpaccess 2) 修改/etc/ftpd/ftpaccess message [file path] login #这个字段控制的是显示在用户登录后的信息

	banner [file path] #这个字段控制的是显示在访问FTP 服务时，也就是登录前 suppresshostname yes #去除显示主机名 suppressversion yes #去除显示FTP服务器版本 3) 重新启动inetd.conf # inetd -c
检测方法	1、判断依据 使用FTP登录时，会按照设置显示banner 2、检查操作

附录 A：端口及服务

服务名称	端口	应用说明	关闭方法	处置建议
daytime	13/tcp	RFC867 白天协议	#daytime stream tcp nowait root internal	建议关闭
	13/udp	RFC867 白天协议	#daytime dgram udp nowait root internal	
time	37/tcp	时间协议	#time stream tcp nowait root internal	
echo	7/tcp	RFC862_回声协议	#echo stream tcp nowait root internal	
	7/udp	RFC862_回声协议	#echo dgram udp nowait root internal	
discard	9/tcp	RFC863 废除协议	#discard stream tcp nowait root internal	
	9/udp		#discard dgram udp nowait root internal	
chargen	19/tcp	RFC864 字符产生 协议	#chargen stream tcp nowait root internal	
	19/udp		#chargen dgram udp nowait root internal	
ftp	21/tcp	文件传输协议(控制)	#ftp stream tcp nowait root /usr/sbin/ftpd	根据情况选择开放
telnet	23/tcp	虚拟终端协议	#telnet stream tcp nowait root /usr/sbin/telnetd telnetd	根据情况选择开放
sendmail	25/tcp	简单邮件发送协议	S540sendmail stop	建议关闭
nameserver	53/udp	域名服务	S370named stop	根据情况选择开放

	53/tcp	域名服务	S370named stop	根据实际情况选择开放
apache	80/tcp	HTTP 万维网发布服务	S825apache stop	根据实际情况选择开放
login	513/tcp	远程登录	#login stream tcp nowait root /usr/lbin/rlogind rlogind	根据实际情况选择开放
shell	514/tcp	远程命令, no passwd used	#shell stream tcp nowait root /usr/lbin/remshd remshd	根据实际情况选择开放
exec	512/tcp	remote execution, passwd required	#exec stream tcp nowait root /usr/lbin/rexecd rexecd	根据实际情况选择开放
ntalk	518/udp	new talk, conversation	#ntalk dgram udp wait root /usr/lbin/ntalkd ntalkd	建议关闭
ident	113/tcp	auth	#ident stream tcp wait bin /usr/lbin/identd identd	建议关闭
printer	515/tcp	远程打印缓存	#printer stream tcp nowait root /usr/sbin/rpdaemon rpdaemon -i	强烈建议关闭
bootps	67/udp	引导协议服务端	#bootps dstream tdp nowait root internal	建议关闭
	68/udp	引导协议客户端	#bootps dgram udp nowait root internal	建议关闭
tftp	69/udp	普通文件传输协议	#tftp dgram udp nowait root internal	强烈建议关闭
kshell	544/tcp	Kerberos remote shell -kfall	#kshell stream tcp nowait root /usr/lbin/remshd remshd -K	建议关闭
klogin	543/tcp	Kerberos rlogin -kfall	#klogin stream tcp nowait root /usr/lbin/rlogind rlogind -K	建议关闭
recserv	7815/tcp	X 共享接收服务	#recserv stream tcp nowait root /usr/lbin/recserv recserv -display :0	建议关闭
dtspcd	6112/tcp	子进程控制	#dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd	强烈建议关闭

registrar	1712/tcp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据实际情况选择开放
	1712/udp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar /etc/opt/resmon/lbin/registrar	根据实际情况选择开放
	动态端口	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据实际情况选择开放
portmap	111/tcp	端口映射	S590Rpcd stop	根据实际情况选择开放
dced	135/tcp	DCE RPC daemon	S570dce stop	建议关闭
dced	135/udp	DCE RPC daemon	S570dce stop	建议关闭
snmp	161/udp	简单网络管理协议 (Agent)	S560SnmpMaster stop S565OspfMib stop S565SnmpHpunix stop S565SnmpMib2 stop	根据实际情况选择开放
snmpd	7161/tcp	简单网络管理协议 (Agent)	S560SnmpMaster stop S565OspfMib stop S565SnmpHpunix stop S565SnmpMib2 stop	根据实际情况选择开放
snmp-trap	162/udp	简单网络管理协议 (Traps)	S565SnmpTrpDst stop	根据实际情况选择开放
dtlogin	177/udp	启动图形控制	S900dtlogin.rc stop	根据实际情况选择开放
	6000/tcp	X 窗口服务	S990dtlogin.rc stop	根据实际情况选择开放
	动态端口	启动图形控制	S900dtlogin.rc stop	根据实际情况选择开放
syslogd	514/udp	系统日志服务	S220syslogd stop	建议保留
lpd	515/tcp	远程打印缓存	S720lp stop	强烈建议关闭
router	520/udp	路由信息协议	S510gated stop	根据实际情况选择开放
nfs	2049/tcp	NFS 远程文件系统	S100nfs.server stop	强烈建议关闭

	2049/udp	NFS 远程文件系统	S100nfs.server stop	强烈建议关闭
rpc.mount	动态端口	rpc 服务	S430nfs.client stop	强烈建议关闭
rpc.statd	动态端口	rpc 服务	S430nfs.client stop	强烈建议关闭
rpc.lockd	动态端口	rpc 服务	S430nfs.client stop	强烈建议关闭
rpc.ruserd	动态端口	rpc 服务	#rpc dgram udp wait root /usr/lib/netsvc/rusers/rpc.r usersd 100002 1-2 rpc.rusersd	强烈建议关闭
rpc.yppasswd	动态端口	rpc 服务	S410nis.server stop	强烈建议关闭
swagentd	2121/tcp	sw 代理	S870swagentd stop	根据情况选择开放
	2121/udp	sw 代理	S870swagentd stop	根据情况选择开放
rbootd	68/udp	remote boot server	START_RBOOTD 0	建议关闭
	1068/udp	remote boot server	START_RBOOTD 0	建议关闭
instl_boots	1067/udp	安装引导协议服务 installation bootstrap protocol server	#instl_boots dgram udp wait root /usr/sbin/instl_bootd instl_bootd	建议关闭
	1068/udp	安装引导协议服务 installation bootstrap protocol client	#instl_bootc dgram udp wait root /usr/sbin/instl_bootc instl_bootc	建议关闭
samd	3275/tcp	system mgmt daemon	samd:23456:respawn:/usr /sam/sbin/samd # system mgmt daemon	建议关闭
swat	901/tcp	SAMBA Web-based Admin Tool	swat stream tcp nowait.400 root /opt/samba/bin/swat swat	强烈建议关闭
xntpd	123/udp	时间同步服务	/sbin/rc3.d/S660xntpd stop	根据情况选择开放
rpc.ttdbserver	动态端口	HP-UX ToolTalk database server	#rpc xti tcp swait root /usr/dt/bin/rpc.ttdbserver 100083 1 /usr/dt/bin/rpc.ttdbserver	强烈建议关闭
rpc.cmsd	动态端口	后台进程管理服务	#rpc dgram udp wait root /usr/dt/bin/rpc.cmsd 100068 2-5 rpc.cmsd	强烈建议关闭
dmisp	动态端口		/sbin/rc2.d/S605Dmisp stop	强烈建议关闭
diagmond	1508/tcp	硬件诊断监控程序	S742diagnostic stop	根据情况选择开放
diaglogd	动态端口	硬件诊断程序	S742diagnostic stop	根据情况选择开放
memlogd	动态端口	内存记录服务	S742diagnostic stop	根据情况选择开放

cclogd	动态端口	chassis code logging daemon	S742diagnostic stop	根据情况选择开放
dm_memory	动态端口	Memory Monitor	S742diagnostic stop	根据情况选择开放
RemoteMonitor	2818/tcp		S742diagnostic stop	根据情况选择开放
psmctd	动态端口	Peripheral Status Monitor client/target	S742diagnostic stop	根据情况选择开放
psmond	1788/tcp	Predictive Monitor	S742diagnostic stop	根据情况选择开放
	1788/udp	Hardware Predictive Monitor	S742diagnostic stop	根据情况选择开放
hacl-hb	5300/tcp	High Availability (HA) Cluster heartbeat	S800cmcluster stop	根据情况选择开放
hacl-gs	5301/tcp	HA Cluster General Services	S800cmcluster stop	根据情况选择开放
hacl-cfg	5302/tcp	HA Cluster TCP configuration	S800cmcluster stop	根据情况选择开放
	5302/udp	HA Cluster UDP configuration	S800cmcluster stop	根据情况选择开放
hacl-local	5304/tcp	HA Cluster Commands	S800cmcluster stop	根据情况选择开放
clvm-cfg	1476/tcp	HA LVM configuration	S800cmcluster stop	根据情况选择开放

中国电信 Linux 操作系统 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	2
4.1 账号.....	2
4.2 口令.....	3
4.3 授权.....	5
4.4 远程登录.....	7
4.5 补丁.....	8
4.6 日志.....	8
4.7 不必要的服务、端口.....	10
4.8 系统 Banner 设置.....	11
4.9 登陆超时时间设置.....	11
4.10 删除潜在危险文件.....	12
4.11 FTP 设置.....	12
附录 A: 端口及服务.....	13

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》（本规范）
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用 **Linux** 操作系统的设备。本规范明确了安全配置的基本要求，适用于所有的安全等级，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以内核版本2.6及以上为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1732-2008 《固定通信网安全防护要求》

YD/T 1734-2008 《移动通信网安全防护要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1742-2008 《接入网安全防护要求》

YD/T 1744-2008 《传送网安全防护要求》

YD/T 1746-2008 《IP 承载网安全防护要求》

YD/T 1748-2008 《信令网安全防护要求》

YD/T 1750-2008 《同步网安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

FTP	File Transfer Protocol	文件传输协议
UDP	User Datagram Protocol	用户数据包协议
TCP	Transmission Control Protocol	传输控制协议

4 安全配置要求

4.1 账号

编号： 1

要求内容	应按照不同的用户分配不同的账号。避免不同用户间共享账号。避免用户账号和设备间通信使用的账号共享。
操作指南	1、参考配置操作 为用户创建账号： #useradd username #创建账号 #passwd username #设置密码 修改权限： #chmod 750 directory #其中 750 为设置的权限，可根据实际情况设置相应的权限，directory 是要更改权限的目录) 使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。 2、补充操作说明
检测方法	1、判定条件 能够登录成功并且可以进行常用操作； 2、检测操作 使用不同的账号进行登录并进行一些常用操作； 3、补充说明

编号： 2

要求内容	应删除或锁定与设备运行、维护等工作无关的账号。
操作指南	1、参考配置操作 删除用户：#userdel username; 锁定用户： 1)修改/etc/shadow 文件，用户名后加*LK* 2)将/etc/passwd 文件中的 shell 域设置成/bin/false 3)#passwd -l username 只有具备超级用户权限的使用者方可使用，#passwd -l username 锁定用户,用#passwd -d username 解锁后原有密码失效，登录需输入新密码，修改/etc/shadow 能保留原有密码。 2、补充操作说明 需要锁定的用户：listen,gdm,webservd,nobody,nobody4、noaccess。 注：无关的账号主要指测试帐户、共享帐号、长期不用账号（半年以上未用）等
检测方法	1、判定条件 被删除或锁定的账号无法登录成功；

	2、检测操作 使用删除或锁定的与工作无关的账号登录系统； 3、补充说明 需要锁定的用户：listen,gdm,webserverd,nobody,nobody4、noaccess。
--	---

编号： 3

要求内容	根据系统要求及用户的业务需求，建立多帐户组，将用户账号分配到相应的帐户组。
操作指南	1、参考配置操作 Cat /etc/passwd Cat /etc/group 2、补充操作说明
检测方法	1、判定条件 人工分析判断 2、检测操作

编号： 4

要求内容	使用 PAM 禁止任何人 su 为 root
操作指南	参考操作： 编辑su文件(vi /etc/pam.d/su)，在开头添加下面两行： auth sufficient /lib/security/pam_rootok.so auth required /lib/security/pam_wheel.so group=wheel 这表明只有wheel组的 成员可以使用su命令成为root用户。你可以把用户添加到 wheel组，以使它可以使su命令成为root用户。添加方法为： # chmod -G10 username
检测方法	1、判定条件 2、检测操作 Cat /etc/pam.d/su

4.2 口令

编号： 1

要求内容	对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。
操作指南	1、参考配置操作 vi /etc/login.defs ， 修改设置如下 PASS_MIN_LEN=8 #设定最小用户密码长度为 8 位 Linux 用户密码的复杂度可以通过 pam_cracklib module 或 pam_passwdqc module 进行设置
检测方法	1、判定条件

	<p>不符合密码强度的时候，系统对口令强度要求进行提示； 符合密码强度的时候，可以成功设置；</p> <p>2、检测操作</p> <p>1、检查口令强度配置选项是否可以如下配置：</p> <ul style="list-style-type: none"> i. 配置口令的最小长度； ii. 将口令配置为强口令。 <p>2、创建一个普通账号，为用户配置与用户名相同的口令、只包含字符或数字的简单口令以及长度短于 8 的口令，查看系统是否对口令强度要求进行提示；输入带有特殊符号的复杂口令、普通复杂口令，查看系统是否可以成功设置。</p> <p>3、补充说明</p> <p>pam_cracklib 主要参数说明：</p> <p>retry=N:重试多少次后返回密码修改错误</p> <p>difok=N:新密码必需与旧密码不同的位数</p> <p>dcredit=N: N >= 0:密码中最多有多少个数字;N < 0 密码中最少有多少个数字.</p> <p>lcredit=N:小写字母的个数</p> <p>ucredit=N 大写字母的个数</p> <p>credit=N:特殊字母的个数</p> <p>minclass=N:密码组成(大/小字母,数字,特殊字符)</p> <p>pam_passwdqc 主要参数说明：</p> <p>mix:设置口令字最小长度，默认值是 mix=disabled。</p> <p>max:设置口令字的最大长度，默认值是 max=40。</p> <p>passphrase: 设置口令短语中单词的最少个数，默认值是 passphrase=3，如果为 0 则禁用口令短语。</p> <p>atch:设置密码串的常见程序，默认值是 match=4。</p> <p>similar:设置当我们重设口令时，重新设置的新口令能否与旧口令相似，它可以是 similar=permit 允许相似或 similar=deny 不允许相似。</p> <p>random:设置随机生成口令字的默认长度。默认值是 random=42。设为 0 则禁止该功能。</p> <p>enforce:设置约束范围，enforce=none 表示只警告弱口令字，但不禁止它们使用；enforce=users 将对系统上的全体非根用户实行这一限制；enforce=everyone 将对包括根用户在内的全体用户实行这一限制。</p> <p>non-unix:它告诉这个模块不要使用传统的 getpwnam 函数调用获得用户信息。</p> <p>retry:设置用户输入口令字时允许重试的次数，默认值是 retry=3。</p> <p>密码复杂度通过/etc/pam.d/system-auth 实施</p>
--	--

编号： 2

要求内容	对于采用静态口令认证技术的设备，帐户口令的生存期不长于 90 天。
操作指南	1、参考配置操作 vi /etc/login.defs PASS_MAX_DAYS=90 #设定口令的生存期不长于 90 天
检测方法	1、判定条件 登录不成功； 2、检测操作 使用超过 90 天的帐户口令登录； 3、补充说明 测试时可以将 90 天的设置缩短来做测试；

4.3 授权

编号：1

要求内容	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	1、参考配置操作 通过 chmod 命令对目录的权限进行实际设置。 2、补充操作说明 /etc/passwd 必须所有用户都可读，root 用户可写 -rw-r—r— /etc/shadow 只有 root 可读 -r----- /etc/group 须所有用户都可读，root 用户可写 -rw-r—r— 使用如下命令设置： chmod 644 /etc/passwd chmod 600 /etc/shadow chmod 644 /etc/group 如果是有写权限，就需移去组及其它用户对/etc 的写权限（特殊情况除外） 执行命令#chmod -R go-w /etc
检测方法	1、判定条件 1、设备系统能够提供用户权限的配置选项，并记录对用户进行权限配置是否必须在用户创建时进行； 2、记录能够配置的权限选项内容； 3、所配置的权限规则应能够正确应用，即用户无法访问授权范围之外的系统资源，而可以访问授权范围之内的系统资源。 2、检测操作 1、利用管理员账号登录系统，并创建 2 个不同的用户； 2、创建用户时查看系统是否提供了用户权限级别以及可访问系统资源和命令的选项； 3、为两个用户分别配置不同的权限，2 个用户的权限差异应能够分别在用户权限级别、可访问系统资源以及可用命令等方面予以体现

	<p>现；</p> <p>4、分别利用 2 个新建的账号访问设备系统，并分别尝试访问允许访问的内容和不允许访问的内容，查看权限配置策略是否生效。</p> <p>3、补充说明</p>
--	---

编号： 2

要求内容	控制用户缺省访问权限，当在创建新文件或目录时 应屏蔽掉新文件或目录不应有的访问允许权限。防止同属于该组的其它用户及别的组的用户修改该用户的文件或更高限制。
操作指南	<p>1、参考配置操作</p> <p>设置默认权限：</p> <p>Vi /etc/login.defs 在末尾增加 umask 027，将缺省访问权限设置为 750</p> <p>修改文件或目录的权限，操作举例如下：</p> <p>#chmod 444 dir ; #修改目录 dir 的权限为所有人都为只读。</p> <p>根据实际情况设置权限；</p> <p>2、补充操作说明</p> <p>如果用户需要使用一个不同于默认全局系统设置的 umask，可以在需要的时候通过命令行设置，或者在用户的 shell 启动文件中配置。</p>
检测方法	<p>1、判定条件</p> <p>权限设置符合实际需要；不应有的访问允许权限被屏蔽掉；</p> <p>2、检测操作</p> <p>查看新建的文件或目录的权限，操作举例如下：</p> <p>#ls -l dir ; #查看目录 dir 的权限</p> <p>#cat /etc/login.defs 查看是否有 umask 027 内容</p> <p>3、补充说明</p> <p>umask 的默认设置一般为 022，这给新创建的文件默认权限 755 (777-022=755)，这会给文件所有者读、写权限，但只给组成员和其他用户读权限。</p> <p>umask 的计算：</p> <p>umask 是使用八进制数据代码设置的，对于目录，该值等于八进制数据代码 777 减去需要的默认权限对应的八进制数据代码值；对于文件，该值等于八进制数据代码 666 减去需要的默认权限对应的八进制数据代码值。</p>

编号： 3

要求内容	如果需要启用 FTP 服务，控制 FTP 进程缺省访问权限，当通过 FTP 服务创建新文件或目录时应屏蔽掉新文件或目录不应有的访问允许权限。
操作指南	<p>1、参考配置操作</p> <p>以 vsftp 为例</p> <p>打开/etc/vsftpd/chroot_list 文件，将需要限制的用户名加入到文件中</p>

	2、补充操作说明
检测方法	1、判定条件 权限设置符合实际需要；不应有的访问允许权限被屏蔽掉； 2、检测操作 查看新建的文件或目录的权限，操作举例如下： 3、补充说明

4.4 远程登录

编号：1

要求内容	限制具备超级管理员权限的用户远程登录。 远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到超级管理员权限账号后执行相应操作。
操作指南	1、参考配置操作 编辑/etc/passwd，帐号信息的 shell 为/sbin/nologin 的为禁止远程登录，如要允许，则改成可以登录的 shell 即可，如/bin/bash 2、补充操作说明 如果限制 root 从远程 ssh 登录，修改/etc/ssh/sshd_config 文件，将 PermitRootLogin yes 改为 PermitRootLogin no，重启 sshd 服务。
检测方法	1、判定条件 root 远程登录不成功，提示“没有权限”； 普通用户登录成功，而且可以切换到 root 用户； 2、检测操作 root 从远程使用 telnet 登录； 普通用户从远程使用 telnet 登录； root 从远程使用 ssh 登录； 普通用户从远程使用 ssh 登录； 3、补充说明 限制 root 从远程 ssh 登录，修改/etc/ssh/sshd_config 文件，将 PermitRootLogin yes 改为 PermitRootLogin no，重启 sshd 服务。

编号：2

要求内容	对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议，并安全配置 SSHD 的设置。
操作指南	1、参考配置操作 正常可以通过#/etc/init.d/sshd start 来启动 SSH； 通过#/etc/init.d/sshd stop 来停止 SSH 2、补充操作说明 查看 SSH 服务状态： <pre># ps -ef grep ssh</pre>

	注：禁止使用 telnet 等明文传输协议进行远程维护；如特别需要，需采用访问控制策略对其进行限制；
检测方法	1、判定条件 <pre># ps -ef grep ssh</pre> 是否有 ssh 进程存在 是否有 telnet 进程存在 2、检测操作 查看 SSH 服务状态： <pre># ps -ef grep ssh</pre> 查看 telnet 服务状态： <pre># ps -ef grep telnet</pre> 3、补充说明

4.5 补丁

编号：1

要求内容	在保证业务网络稳定运行的前提下，安装最新的 OS 补丁。补丁在安装前需要测试确定。
操作指南	1、参考配置操作 看版本是否为最新版本。 执行下列命令，查看版本及大补丁号。 <pre>#uname -a</pre> 2、补充操作说明
检测方法	1、判定条件 看版本是否为最新版本。 <pre># uname -a</pre> 查看版本及大补丁号 RedHat Linux: http://www.redhat.com/support/errata/ Slackware Linux: ftp://ftp.slackware.com/pub/slackware/ SuSE Linux: http://www.suse.com/us/support/security/index.html TurboLinux: http://www.turbolinux.com/security/ 2、检测操作 在系统安装时建议只安装基本的 OS 部份，其余的软件包则以必要为原则，非必需的包就不装。 3、补充说明

4.6 日志

编号：1

要求内容	启用 syslog 系统日志审计功能
操作指南	1、参考配置操作 #cat /etc/syslog.conf 查看是否有#authpriv.* /var/log/secure 2、补充操作说明 将 authpriv 设备的任何级别的信息记录到/var/log/secure 文件中，这主要是一些和认证、权限使用相关的信息。
检测方法	1、判定条件 查看是否有#authpriv.* /var/log/secure 2、检测操作 #cat /etc/syslog.conf 3、补充说明 将 authpriv 设备的任何级别的信息记录到/var/log/secure 文件中，这主要是一些和认证、权限使用相关的信息。

编号：2

要求内容	系统日志文件由 syslog 创立并且不可被其他用户修改；其它的系统日志文件不是全局可写
操作指南	1、参考配置操作 查看如下等日志的访问权限 #ls -l 查看下列日志文件权限 /var/log/messages 、 /var/log/secure 、 /var/log/maillog 、 /var/log/cron、 /var/log/spooler、 /var/log/boot.log 2、补充操作说明
检测方法	1、判定条件 2、检测操作 使用 ls -l 命令依次检查系统日志的读写权限 3、补充说明

编号：3（可选）

要求内容	启用记录cron行为日志功能
操作指南	1、参考配置操作 Vi /etc/syslog.conf # Log cron stuff cron.* cron.*
检测方法	1、判定条件 2、检测操作

	cron.*
--	--------

编号：4（可选）

要求内容	设备配置远程日志功能，将需要重点关注的日志内容传输到日志服务器。
操作指南	1、参考配置操作 修改配置文件 vi /etc/syslog.conf， 加上这一行： *. * @192.168.0.1 可以将"*. *"替换为你实际需要的日志信息。比如：kern.* ; mail.* 等等。 可以将此处 192.168.0.1 替换为实际的 IP 或域名。 2、补充操作说明
检测方法	1、判定条件 设备配置远程日志功能，将需要重点关注的日志内容传输到日志服务器。 2、检测操作 查看日志服务器上的所收到的日志文件。 3、补充说明

4.7 不必要的服务、端口

编号：1

要求内容	关闭不必要的服务。
操作指南	1、参考配置操作 查看所有开启的服务： #ps -ef #chkconfig --list #cat /etc/xinetd.conf 在xinetd.conf中关闭不用的服务 首先复制/etc/xinetd.conf。 #cp /etc/xinetd.conf /etc/xinetd.conf.backup 然后用vi编辑器编辑 xinetd.conf文件，对于需要注释掉的服务在相应行开头标记"#"字符，重启xinetd服务,即可。 2、补充操作说明 参考附录A，根据需要关闭不必要的服务
检测方法	1、判定条件 所需的服务都列出来； 没有不必要的服务； 2、检测操作

	<pre>#ps -ef #chkconfig --list #cat /etc/xinetd.conf</pre> <p>3、补充说明</p> <p>在/etc/xinetd.conf文件中禁止不必要的基本网络服务。</p> <p>注意：改变了“/etc/xinetd.conf”文件之后，需要重新启动xinetd。</p> <p>对必须提供的服务采用tcpwrapper来保护</p>
--	---

4.8 系统 Banner 设置

要求内容	修改系统 banner，避免泄漏操作系统名称，版本号，主机名称等，并且给出登陆告警信息
操作指南	<p>1、参考配置操作</p> <p>在缺省情况下，当你登录到 linux 系统，它会告诉你该 linux 发行版的名称、版本、内核版本、服务器的名称。应该尽可能的隐藏系统信息。</p> <p>首先编辑“/etc/rc.d/rc.local”文件，在下面显示的这些行前加一个“#”，把输出信息的命令注释掉。</p> <pre># This will overwrite /etc/issue at every boot. So, make any changes you want to make to /etc/issue here or you will lose them when you reboot. #echo "" > /etc/issue #echo "\$R" >> /etc/issue #echo "Kernel \$(uname -r) on \$a \$(uname -m)" >> /etc/issue #cp -f /etc/issue /etc/issue.net #echo >> /etc/issue</pre> <p>其次删除"/etc"目录下的 issue.net 和 issue 文件：</p> <pre># mv /etc/issue /etc/issue.bak # mv /etc/issue.net /etc/issue.net.bak</pre>
检测方法	查看 Cat /etc/rc.d/rc.local 注释住处信息

4.9 登陆超时时间设置

要求内容	对于具备字符交互界面的设备，配置定时帐户自动登出
操作指南	1、参考配置操作 通过修改账户中“TMOUT”参数，可以实现此功能。TMOUT 按秒计算。编辑 profile 文件（vi /etc/profile），在“HISTFILESIZE=”后面加入下面这行： 建议 TMOUT=300（可根据情况设定） 2、补充操作说明 改变这项设置后，必须先注销用户，再用该用户登录才能激活这个功能
检测方法	1、判定条件 查看 TMOUT=300

4.10 删除潜在危险文件

要求内容	.rhosts, .netrc, hosts.equiv等文件都具有潜在的危险，如果没有应用，应该删除
操作指南	1、参考配置操作 执行：find / -name .netrc，检查系统中是否有.netrc 文件， 执行：find / -name .rhosts，检查系统中是否有.rhosts 文件 如无应用，删除以上文件： Mv .rhost .rhost.bak Mv .netrc .netrc.bak 2、补充操作说明 注意系统版本，用相应的方法执行
检测方法	1、判定条件 2、检测操作

4.11 FTP 设置

编号 1:

要求内容	禁止 root 登陆 FTP
操作指南	1、参考配置操作 在 ftpaccess 文件中加入下列行 root
检测方法	使用 root 帐号登录 ftp 会被拒绝

编号 2:

要求内容	禁止匿名 ftp
操作指南	1、参考配置操作 以 vsftpd 为例：

	打开vsftd.conf文件，修改下列行为： anonymous_enable=NO
检测方法	匿名账户不能登录

编号 3:

要求内容	修改FTP banner 信息
操作指南	1、参考配置操作 使用vsftpd，则修改下列文件的内容： /etc/vsftpd.d/vsftpd.conf 使用wu-ftp，则需要修改文件/etc/ftpaccess，在其中添加： banner /path/to/ftpbanner 在指定目录下创建包含ftp的banner信息的文件
检测方法	1、判断依据 通过外部ftp客户端登录，banner按照预先设定的显示 2、检查操作

附录 A：端口及服务

服务名称	端口	应用说明	关闭方法	处置建议
daytime	13/tcp	RFC867 白天协议	chkconfig daytime off	建议关闭
	13/udp	RFC867 白天协议	chkconfig daytime off	
time	37/tcp	时间协议	chkconfig time off	
	37/udp	时间协议	chkconfig time-udp off	
echo	7/tcp	RFC862_回声协议	chkconfig echo off	
	7/udp	RFC862_回声协议	chkconfig echo-udp off	
discard	9/tcp	RFC863 废除协议	chkconfig discard off	
	9/udp		chkconfig discard-udp off	
chargen	19/tcp	RFC864 字符产生协议	chkconfig chargen off	根据情况选择开放
	19/udp		chkconfig chargen-udp off	
ftp	21/tcp	文件传输协议(控制)	chkconfig gssftp off	根据情况选择开放
telnet	23/tcp	虚拟终端协议	chkconfig krb5-telnet off	根据情况选择开放
sendmail	25/tcp	简单邮件发送协议	chkconfig sendmail off	建议关闭
nameserver	53/udp	域名服务	chkconfig named off	根据情况选择开放
	53/tcp	域名服务	chkconfig named off	根据情况选择开放
apache	80/tcp	HTTP 万维网发布	chkconfig httpd off	根据情况选

		服务		择开放
login	513/tcp	远程登录	chkconfig login off	根据情况选择开放
shell	514/tcp	远程命令, no passwd used	chkconfig shell off	根据情况选择开放
exec	512/tcp	remote execution, passwd required	chkconfig exec off	根据情况选择开放
ntalk	518/udp	new talk, conversation	chkconfig ntalk off	建议关闭
ident	113/tcp	auth	chkconfig ident off	建议关闭
printer	515/tcp	远程打印缓存	chkconfig printer off	强烈建议关闭
bootps	67/udp	引导协议服务端	chkconfig bootps off	建议关闭
	68/udp	引导协议客户端	chkconfig bootps off	建议关闭
tftp	69/udp	普通文件传输协议	chkconfig tftp off	强烈建议关闭
kshell	544/tcp	Kerberos remote shell -kfall	chkconfig kshell off	建议关闭
klogin	543/tcp	Kerberos rlogin -kfall	chkconfig klogin off	建议关闭
portmap	111/tcp	端口映射	chkconfig portmap off	根据情况选择开放
snmp	161/udp	简单网络管理协议 (Agent)	chkconfig snmp off	根据情况选择开放
snmp trap	161/tcp	简单网络管理协议 (Agent)	chkconfig snmp off	根据情况选择开放
snmp-trap	162/udp	简单网络管理协议 (Traps)	chkconfig snmptrap off	根据情况选择开放
syslogd	514/udp	系统日志服务	chkconfig syslog off	建议保留
lpd	515/tcp	远程打印缓存	chkconfig lpd off	强烈建议关闭
nfs	2049/tcp	NFS 远程文件系统	chkconfig nfs off	强烈建议关闭
	2049/udp	NFS 远程文件系统	chkconfig nfs off	强烈建议关闭
nfs.lock	动态端口	rpc 服务	chkconfig nfslock off	强烈建议关闭
ypbind	动态端口	rpc 服务	chkconfig ypbind off	强烈建议关闭

中国电信 Solaris 操作系统 安全配置要求及操作指南

中国电信集团公司 发布

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	2
4.2 口令.....	3
4.3 授权.....	6
4.4 远程维护.....	9
4.5 补丁.....	10
4.6 日志.....	11
4.7 不必要的服务、端口.....	12
4.8 系统 Banner 设置.....	13
4.9 FTP 设置.....	13
4.10 删除潜在危险文件.....	14
4.11 登陆超时时间设置.....	14
4.12 内核调整设置.....	15
附录 A：服务及端口.....	16

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》（本规范）
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用 Solaris 操作系统的设备。本规范明确了安全配置的基本要求，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 Solaris 8/10 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1732-2008 《固定通信网安全防护要求》

YD/T 1734-2008 《移动通信网安全防护要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1742-2008 《接入网安全防护要求》

YD/T 1744-2008 《传送网安全防护要求》

YD/T 1746-2008 《IP 承载网安全防护要求》

YD/T 1748-2008 《信令网安全防护要求》

YD/T 1750-2008 《同步网安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

FTP	File Transfer Protocol	文件传输协议
UDP	User Datagram Protocol	用户数据包协议
TCP	Transmission Control Protocol	传输控制协议

4 安全配置要求

4.1 账号

编号： 1

要求内容	应按照不同的用户分配不同的账号。
操作指南	1、参考配置操作 为用户创建账号： #useradd username #创建账号 #passwd username #设置密码 修改权限： #chmod 750 directory #其中 750 为设置的权限，可根据实际情况设置相应的权限，directory 是要更改权限的目录) 使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。 2、补充操作说明
检测方法	1、判定条件 能够登录成功并且可以进行常用操作； 2、检测操作 使用不同的账号进行登录并进行一些常用操作； 3、补充说明

编号： 2

要求内容	应删除或锁定与设备运行、维护等工作无关的账号。
操作指南	1、参考配置操作 删除用户：#userdel username; 锁定用户： 1)修改/etc/shadow 文件，用户名后加*LK* 2)将/etc/passwd 文件中的 shell 域设置成/bin/false 3)#passwd -l username 只有具备超级用户权限的使用者方可使用，#passwd -l username 锁定用户,用#passwd -d username 解锁后原有密码失效，登录需输入新密码，修改/etc/shadow 能保留原有密码。 2、补充操作说明 需要锁定的用户：listen,gdm,webserverd,nobody,nobody4、noaccess。
检测方法	1、判定条件 被删除或锁定的账号无法登录成功； 2、检测操作 使用删除或锁定的与工作无关的账号登录系统； 3、补充说明 需要锁定的用户：listen,gdm,webserverd,nobody,nobody4、noaccess。

编号： 3

要求内容	限制具备超级管理员权限的用户远程登录。远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到超级管理员权限账号后执行相应操作。
操作指南	<p>1、参考配置操作</p> <p>限制 root 远程 telnet 登录： 编辑/etc/default/login，加上： CONSOLE=/dev/console # If CONSOLE is set, root can only login on that device.</p> <p>限制 root 远程 ssh 登录： 修改 /etc/ssh/sshd_config 文件，将 PermitRootLogin yes 改为 PermitRootLogin no，重启 sshd 服务。</p> <p>Solaris 8上没有该路径 /usr/local/etc下有该文件 Solaris 9上有该路径/文件 重启sshd服务： Solaris10以前： #/etc/init.d/sshd stop #/etc/init.d/sshd start Solaris10： #svcadm disable ssh #svcadm enable ssh</p> <p>2、补充操作说明</p> <p>Solaris8 上默认是没有安装 ssh 的，需要安装软件包。</p>
检测方法	<p>1、判定条件</p> <p>root 远程登录不成功，提示 “Not on system console”； 普通用户可以登录成功，而且可以切换到 root 用户；</p> <p>2、检测操作</p> <p>root 从远程使用 telnet 登录； 普通用户从远程使用 telnet 登录； root 从远程使用 ssh 登录； 普通用户从远程使用 ssh 登录；</p> <p>3、补充说明</p> <p>。</p>

4.2 口令

编号： 1

要求内容	对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。
操作指南	<p>1、参考配置操作</p> <p>vi /etc/default/passwd ，修改设置如下</p>

	<p>PASSLENGTH = 8 #设定最小用户密码长度为 8 位</p> <p>MINALPHA=2; MINNONALPHA=1 #表示至少包括两个字母和一个非字母；具体设置可以参看补充说明。</p> <p>当用 root 帐户给用户设定口令的时候不受任何限制，只要不超长。</p> <p>2、补充操作说明</p> <p>Solaris10 默认如下各行都被注释掉，并且数值设置和解释如下：</p> <p>MINDIFF=3 # Minimum differences required between an old and a new password.</p> <p>MINALPHA=2 # Minimum number of alpha character required.</p> <p>MINNONALPHA=1 # Minimum number of non-alpha (including numeric and special) required.</p> <p>MINUPPER=1 # Minimum number of upper case letters required.</p> <p>MINLOWER=1 # Minimum number of lower case letters required.</p> <p>MAXREPEATS=0 # Maximum number of allowable consecutive repeating characters.</p> <p>MINSPECIAL=0 # Minimum number of special (non-alpha and non-digit) characters required.</p> <p>MINDIGIT=8 # Minimum number of digits required.</p> <p>WHITESPACE=YES</p> <p>Solaris8 默认没有这部分的数值设置需要手工添加</p> <p>NIS 系统无法生效，非 NIS 系统或 NIS+系统能够生效。</p>
检测方法	<p>1、判定条件</p> <p>不符合密码强度的时候，系统对口令强度要求进行提示；</p> <p>符合密码强度的时候，可以成功设置；</p> <p>2、检测操作</p> <p>1、检查口令强度配置选项是否可以如下配置：</p> <ul style="list-style-type: none"> i. 配置口令的最小长度； ii. 将口令配置为强口令。 <p>2、创建一个普通账号，为用户配置与用户名相同的口令、只包含字符或数字的简单口令以及长度短于 8 位的口令，查看系统是否对口令强度要求进行提示；输入带有特殊符号的复杂口令、普通复杂口令，查看系统是否可以成功设置。</p> <p>3、补充说明</p> <p>对于 Solaris 8 以前的版本，PWLEN 对应 PASSLENGTH 等，需根据/etc/default/passwd 文件说明确定。</p> <p>NIS 系统无法生效，非 NIS 系统或 NIS+系统能够生效。</p>

编号： 2

要求内容	对于采用静态口令认证技术的设备，帐户口令的生存期不长于 90 天。
操作指南	1、参考配置操作 vi /etc/default/passwd 文件： MAXWEEKS=13 密码的最大生存周期为 13 周；（Solaris 8&10） PWMAX= 90 #密码的最大生存周期；（Solaris 其它版本） 2、补充操作说明 对于 Solaris 8 以前的版本，PWMIN 对应 MINWEEKS,PWMAX 对应 MAXWEEKS 等，需根据/etc/default/passwd 文件说明确定。 NIS 系统无法生效，非 NIS 系统或 NIS+系统能够生效。
检测方法	1、判定条件 登录不成功； 2、检测操作 使用超过 90 天的帐户口令登录； 3、补充说明 测试时可以将 90 天的设置缩短来做测试； NIS 系统无法生效，非 NIS 系统或 NIS+系统能够生效。

编号： 3

要求内容	对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近 5 次（含 5 次）内已使用的口令。
操作指南	1、参考配置操作 vi /etc/default/passwd ， 修改设置如下 HISTORY=5 2、补充操作说明 #HISTORY sets the number of prior password changes to keep and # check for a user when changing passwords. Setting the HISTORY # value to zero (0), or removing/commenting out the flag will # cause all users' prior password history to be discarded at the # next password change by any user. No password history will # be checked if the flag is not present or has zero value. # The maximum value of HISTORY is 26. NIS 系统无法生效，非 NIS 系统或 NIS+系统能够生效。
检测方法	1、判定条件 设置密码不成功 2、检测操作 cat /etc/default/passwd ， 设置如下 HISTORY=5 3、补充说明 默认没有 HISTORY 的标记，即不记录以前的密码 NIS 系统无法生效，非 NIS 系统或 NIS+系统能够生效。

编号： 4

要求内容	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。
操作指南	<p>1、参考配置操作</p> <p>指定当本地用户登陆失败次数等于或者大于允许的重试次数则账号被锁定：</p> <pre>vi /etc/user_attr</pre> <pre>vi /etc/security/policy.conf</pre> <p>设置 LOCK_AFTER_RETRIES=YES</p> <p>设置重试的次数：</p> <pre>vi /etc/default/login</pre> <p>在文件中将 RETRIES 行前的#去掉，并将其值修改为 RETRIES=7。</p> <p>保存文件退出。</p> <p>2、补充操作说明</p> <p>默认值为：</p> <pre>LOCK_AFTER_RETRIES=NO</pre> <pre>lock_after-retries=no</pre> <p>RETRIES=5，即等于或大于 5 次时被锁定。</p> <p>root 账号不在锁定的限制范围内</p> <p>NIS 系统无法生效，非 NIS 系统或 NIS+ 系统能够生效。</p>
检测方法	<p>1、判定条件</p> <p>帐户被锁定，不再提示让再次登录；</p> <p>2、检测操作</p> <p>创建一个普通账号，为其配置相应的口令；并用新建的账号通过错误的口令进行系统登录 6 次以上（不含 6 次）；</p>

4.3 授权

编号： 1

要求内容	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	<p>1、参考配置操作</p> <p>通过 chmod 命令对目录的权限进行实际设置。</p> <p>2、补充操作说明</p> <p>etc/passwd 必须所有用户都可读，root 用户可写 -rw-r—r—</p> <p>/etc/shadow 只有 root 可读 -r-----</p> <p>/etc/group 必须所有用户都可读，root 用户可写 -rw-r—r—</p> <p>使用如下命令设置：</p> <pre>chmod 644 /etc/passwd</pre> <pre>chmod 600 /etc/shadow</pre> <pre>chmod 644 /etc/group</pre> <p>如果是有写权限，就需移去组及其它用户对/etc 的写权限（特殊情况除外）</p> <p>执行命令#chmod -R go-w /etc</p>

检测方法	<p>1、判定条件</p> <p>1、设备系统能够提供用户权限的配置选项，并记录对用户进行权限配置是否必须在用户创建时进行；</p> <p>2、记录能够配置的权限选项内容；</p> <p>3、所配置的权限规则应能够正确应用，即用户无法访问授权范围之外的系统资源，而可以访问授权范围之内的系统资源。</p> <p>2、检测操作</p> <p>1、利用管理员账号登录系统，并创建 2 个不同的用户；</p> <p>2、创建用户时查看系统是否提供了用户权限级别以及可访问系统资源和命令的选项；</p> <p>3、为两个用户分别配置不同的权限，2 个用户的权限差异应能够分别在用户权限级别、可访问系统资源以及可用命令等方面予以体现；</p> <p>4、分别利用 2 个新建的账号访问设备系统，并分别尝试访问允许访问的内容和不允许访问的内容，查看权限配置策略是否生效。</p> <p>3、补充说明</p>
------	--

编号： 2

要求内容	控制用户缺省访问权限，当在创建新文件或目录时 应屏蔽掉新文件或目录不应有的访问允许权限。防止同属于该组的其它用户及别的组的用户修改该用户的文件或更高限制。
操作指南	<p>1、参考配置操作</p> <p>设置默认权限：</p> <p><code>vi /etc/default/login</code> 在末尾增加 <code>umask 027</code></p> <p>修改文件或目录的权限，操作举例如下：</p> <p><code>#chmod 444 dir</code> ; #修改目录 <code>dir</code> 的权限为所有人都为只读。</p> <p>根据实际情况设置权限；</p> <p>2、补充操作说明</p> <p>如果用户需要使用一个不同于默认全局系统设置的 <code>umask</code>，可以在需要的时候通过命令行设置，或者在用户的 <code>shell</code> 启动文件中配置。</p>
检测方法	<p>1、判定条件</p> <p>权限设置符合实际需要；不应有的访问允许权限被屏蔽掉；</p> <p>2、检测操作</p> <p>查看新建的文件或目录的权限，操作举例如下：</p> <p><code>#ls -l dir</code> ; #查看目录 <code>dir</code> 的权限</p> <p><code>#cat /etc/default/login</code> 查看是否有 <code>umask 027</code> 内容</p> <p>3、补充说明</p> <p><code>umask</code> 的默认设置一般为 <code>022</code>，这给新创建的文件默认权限 <code>755</code> (<code>777-022=755</code>)，这会给文件所有者读、写权限，但只给组成员和其他用户读权限。</p> <p><code>umask</code> 的计算：</p> <p><code>umask</code> 是使用八进制数据代码设置的，对于目录，该值等于八进制</p>

	数据代码 777 减去需要的默认权限对应的八进制数据代码值；对于文件，该值等于八进制数据代码 666 减去需要的默认权限对应的八进制数据代码值。
--	--

编号：3

要求内容	控制 FTP 进程缺省访问权限，当通过 FTP 服务创建新文件或目录时应屏蔽掉新文件或目录不应有的访问允许权限。
操作指南	<p>1、参考配置操作</p> <p>a. 限制某些系统帐户不准 ftp 登录： 通过修改 ftpusers 文件，增加帐户 #vi /etc/ftpusers #Solaris 8 #vi /etc/ftpd/ftpusers #Solaris 10</p> <p>b. 限制用户可使用 FTP 不能用 Telnet，假如用户为 ftpxll 创建一个/etc/shells 文件，添加一行 /bin/true; 修改/etc/passwd 文件，ftpxll:x:119:1::/home/ftpxll:/bin/true 注：还需要把真实存在的 shell 目录加入/etc/shells 文件，否则没有用户能够登录 ftp</p> <p>c. 限制 ftp 用户登陆后在自己当前目录下活动 编辑 ftpaccess，加入如下一行 restricted-uid *(限制所有)， restricted-uid username（特定用户） ftpaccess 文件与 ftpusers 文件在同一目录</p> <p>d. 设置 ftp 用户登录后对文件目录的存取权限，可编辑 /etc/ftpd/ftpaccess。</p> <pre>chmod no guest,anonymous delete no guest,anonymous overwrite no guest,anonymous rename no guest,anonymous umask no anonymous</pre> <p>2、补充操作说明 查看# cat ftpusers 说明： 在这个列表里边的用户名是不允许 ftp 登陆的。</p> <pre>root daemon bin sys adm lp uucp nuucp listen nobody noaccess nobody4</pre>

检测方法	<p>1、判定条件 权限设置符合实际需要；不应有的访问允许权限被屏蔽掉；</p> <p>2、检测操作 查看新建的文件或目录的权限，操作举例如下： <pre>#more /etc/ftpusers #Solaris 8 #more /etc/ftpd/ftpusers #Solaris 10 #more /etc/passwd #more /etc/ftpaccess #Solaris 8 #more /etc/ftpd/ftpaccess #Solaris 10</pre> </p> <p>3、补充说明 查看# cat ftpusers 说明： 在这个列表里边的用户名是不允许 ftp 登陆的。 <pre>root daemon bin sys adm lp uucp nuucp listen nobody noaccess nobody4</pre> </p>

4.4 远程维护

编号： 1

要求内容	对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议，禁止使用 telnet 等明文传输协议进行远程维护；
操作指南	<p>1、参考配置操作 Solaris 10 以前的版本需另外安装，才能使用 SSH。 Solaris 10 启用 SSH 的命令： svcadm enable ssh Solaris 10 禁用 Telnet 的命令： svcadm disable telnet Solaris 8 如果安装 openssh 正常可以通过#/etc/init.d/sshd start 来启动 SSH; 通过#/etc/init.d/sshd stop 来停止 SSH</p> <p>2、补充操作说明 查看 SSH 服务状态：</p>

	<pre># ps -elf grep ssh</pre> <p>Solaris 10 还可以通过命令：</p> <pre># svc -a grep ssh</pre> <p>若为 online，即为生效。</p>
检测方法	<p>1、判定条件</p> <pre># ps -elf grep ssh</pre> <p>是否有 ssh 进程存在</p> <p>Solaris 10 还可以通过命令# svc -a grep ssh</p> <p>SSH 服务状态查看结果为：online</p> <p>telnet 服务状态查看结果为：disabled</p> <p>2、检测操作</p> <p>查看 SSH 服务状态：</p> <pre># ps -elf grep ssh</pre> <p>查看 telnet 服务状态：</p> <pre># ps -elf grep telnet</pre> <p>3、补充说明</p> <p>查看 SSH 服务状态：</p> <p>Solaris 10 还可以使用</p> <pre># svc -a grep ssh</pre> <p>查看 telnet 服务状态：</p> <p>Solaris 10 还可以使用</p> <pre># svc -a grep telnet</pre>

4.5 补丁

编号： 1

要求内容	在保证业务及网络安全的前提下，经过实验室测试后，更新使用最新版本的操作系统补丁
操作指南	<p>1、参考配置操作</p> <p>Solaris 提供了两个命令来管理补丁，Patchadd 和 patchrm。这两个命令是在 Solaris 2.6 版本开始提供的，在 2.6 以前的版本中，每个补丁包中都提供了一个 installpatch 程序和一个 backoutpatch 程序来完成补丁的安装和卸载。</p> <p>注意：</p> <p>由于在安装 Patch 时需要更新文件，故此 Solaris 官方推荐在安装补丁时进入单用户模式安装。</p> <p>例如：</p> <pre># cd /var/tmp</pre> <pre># patchadd 110668-04</pre>

检测方法	1、判定条件 查看最新的补丁号，确认已打上了最新补丁； 2、检测操作 #showrev -p 命令检补丁号 3、补充说明

4.6 日志

编号： 1

要求内容	设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。
操作指南	1、参考配置操作 修改文件：vi /etc/default/login ， 设置 SYSLOG=YES。 , SOLARIS10 是 wtmpx 文件,Solaris8 是 wtmp,wtmps,文件中记录着所有登录过主机的用户，时间，来源等内容，这两个文件不具可读性，可用 last 命令来看。 2、补充操作说明
检测方法	1、判定条件 列出用户账号、登录是否成功、登录时间、远程登录时的 IP 地址。 2、检测操作 查看文件：more /etc/default/login 中的 SYSLOG=YES /var/adm/wtmpx 或者 wtmp,wtmps 文件中记录着所有登录过主机的用户，时间，来源等内容，该文件不具可读性，可用 last 命令来看。 # last 3、补充说明 如果/var/adm/wtmpx 或者 wtmp,wtmps 文件会增长很快，大小达到 2G 以上，可先压缩，FTP 出来后，删除该文件，再创建空文件，一定要创建空文件，否则可能出现系统无法启动。

编号： 2（可选）

要求内容	启用记录 cron 行为日志功能
操作指南	1、参考配置操作 对所有的cron行为进行审计： 在 /etc/default/cron里设置"CRONLOG=yes" 来记录corn的动作。
检测方法	1、判定条件 CRONLOG=YES 2、检测操作

	运行 <code>cat /etc/default/cron</code> 查看CRONLOG状态，并记录
--	---

编号： 3

要求内容	设备应配置权限，控制对日志文件读取、修改和删除等操作。
操作指南	<p>1、参考配置操作</p> <p>修改文件权限：</p> <pre>chmod 644 /var/adm/messages chmod 644 /var/adm/utmpx chmod 644 /var/adm/wtmpx chmod 600 /var/adm/sulog</pre> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>没有相应权限的用户不能查看或删除日志文件</p> <p>2、检测操作</p> <p>查看 <code>syslog.conf</code> 文件中配置的日志存放文件：</p> <pre>more /etc/syslog.conf</pre> <p>使用 <code>ls -l /var/adm</code> 查看的目录下日志文件的权限，<code>messages</code>、<code>utmpx</code>、<code>wtmpx</code> 的权限应为 644，如下所示：</p> <pre>-rw-r--r-- 1 root root message -rw-r--r-- 1 root bin utmpx -rw-r--r-- 1 adm adm wtmpx</pre> <p><code>sulog</code> 的权限应为 600，如下所示：</p> <pre>-rw----- 1 root root sulog</pre> <p>3、补充说明</p> <p>对于其他日志文件，也应该设置适当的权限，如登录失败事件的日志、操作日志，具体文件查看 <code>syslog.conf</code> 中的配置。</p>

4.7 不必要的服务、端口

编号：

要求内容	关闭不必要的服务、端口
操作指南	<p>1、参考配置操作</p> <p>查看所有开启的服务：</p> <pre>#ps -eaf #svcs -a 'solaris 10'</pre> <p>在<code>inetd.conf</code>中关闭不用的服务 首先复制<code>/etc/inet/inetd.conf</code>。 <code>#cp /etc/inet/inetd.conf /etc/inet/inetd.conf.backup</code> 然后用vi编辑器编辑<code>inetd.conf</code>文件，对于需要注释掉的服务在相应行开头标记"<code>#</code>"字符，重启<code>inetd</code>服务,即可。</p> <p>对于Solaris 10，直接关闭某个服务，如<code>telnet</code>,可用如下命令：</p> <pre>svcadm disable svc:/network/telnet</pre>

	<p>重新启用该服务，使用命令：</p> <pre>svcadm enable svc:/network/telnet</pre> <p>Solaris8 修改/etc/inet/inetd.conf 和/etc/inet/services 文件,注释掉对的服务以及 TCP/IP 端口</p> <p>重启 inetd 进程</p> <pre>>kill -HUP <inetd></pre> <p>2、补充操作说明</p> <p>可根据具体应用情况参考附录A，筛选不必要的服务。</p> <p>并在/etc/inetd.conf文件中建议禁止不必要的基本网络服务。</p> <p>注意：改变了“inetd.conf”文件之后，需要重新启动inetd。</p> <p>对必须提供的服务采用tcpwrapper来保护</p>
检测方法	<p>1、判定条件</p> <p>所需的服务都列出来；</p> <p>没有不必要的服务；</p> <p>2、检测操作</p> <p>Solaris10查看所有开启的服务：svcs -a</p> <p>Solaris8 查看所有开启的服务 :cat /etc/inet/inetd.conf,cat /etc/inet/services</p> <p>3、补充说明</p> <p>在/etc/inetd.conf文件中禁止不必要的基本网络服务。</p>

4.8 系统 Banner 设置

要求内容	修改系统 banner，避免泄漏操作系统名称，版本号，主机名称等，并且给出登陆告警信息
操作指南	<p>1、参考配置操作</p> <p>用 root 用户登陆 SOLARIS 系统，使用 vi 编辑器编辑 /etc/motd 文件，在 motd 文件里的删除系统敏感的信息</p>
检测方法	判断/etc/motd 文件

4.9 FTP 设置

编号 1:

要求内容	禁止 root 登陆 FTP
操作指南	<p>1、参考配置操作</p> <p>在文件/etc/ftpusers中增加超级用户。</p> <p>然后让 inetd 重新读配置文件</p>
检测方法	查看/etc/ftpusers 文件中是否存在 root

编号 2:

要求内容	禁止匿名 ftp
------	----------

操作指南	1、参考配置操作 不要使用匿名ftp，只需在文件/etc/passwd中把ftp用户注释掉即可。
检测方法	查看/etc/passwd 文件中是否存在 FTP

编号 3:

要求内容	修改FTP banner 信息
操作指南	1、参考配置操作 如果系统存在 /etc/default/ftpd 文件，把 ftpd 文件里的 BANNER="" 字段设置为空或其它不明感的字符。 如果/etc/default/ftpd文件不存在， 创建/etc/default/ftpd 文件，在 ftpd 文件里写入 BANNER=""。
检测方法	1、判断依据 cat /etc/default/ftpd 2、检查操作 BANNER= 内容不包括 FTP 或版本的敏感信息

4.10 删除潜在危险文件

要求内容	rhosts, .netrc等文件都具有潜在的危險，如果没有应用，应该删除
操作指南	1、参考配置操作 执行：find / -name .netrc，检查系统中是否有.netrc 文件， 执行：find / -name .rhosts，检查系统中是否有.rhosts 文件 如无应用，删除以上文件： mv.rhost.rhost.bak mv..netrc..netrc.bak 2、补充操作说明 注意系统版本，用相应的方法执行
检测方法	1、判定条件 2、检测操作 登陆系统判断 Cat /etc/passwd

4.11 登陆超时时间设置

要求内容	对于具备字符交互界面的设备，应配置定时帐户自动登出
操作指南	1、参考配置操作 可以在用户的.profile 文件中"HISTFILESIZE="后面增加如

	<p>下行：</p> <pre>vi /etc/profile \$ TMOUT=180;export TMOUT</pre> <p>改变这项设置后，重新登录才能有效</p> <p>2、补充操作说明</p> <p>若修改了 login 文件，如下：</p> <pre>vi /etc/default/login # TIMEOUT sets the number of seconds (between 0 and 900) to wait before # abandoning a login session. TIMEOUT=180</pre> <p>这里的超时设置针对登录过程，而不是登录成功后的 shell 会话超时设置</p>
检测方法	查看 TMOUT=180

4.12 内核调整设置

要求内容	防止堆栈缓冲溢出
操作指南	<p>1、参考配置操作</p> <p>对/etc/system 文件做备份。 #cp /etc/system /etc/system.backup 用 vi 编辑器编辑 system 文件，在 system 文件的最后加如下 2 行内容。</p> <pre>set noexec_user_stack=1 set noexec_user_stack_log =1</pre> <p>保存文件，退出编辑器。</p> <p>然后改变文件权限：#chmod 750 /etc/system</p> <p>2、补充操作说明</p> <p>系统的内核参数都在此，一但改错系统无法正常启动，需要光盘引导。内核参数改动后需要重启服务器才生效。</p>
检测方法	<p>1、判定条件</p> <p>能够防止堆栈缓冲溢出</p> <p>2、检测操作</p> <p>查看/etc/system 文件：cat /etc/system；是否有如下两行：</p> <pre>set noexec_user_stack=1 set noexec_user_stack_log =1</pre> <p>查看文件权限：#chmod 750 /etc/system</p> <p>3、补充说明</p>

附录 A：服务及端口

服务名称	端口	服务说明	关闭方法	处置建议
echo	7/tcp	RFC862_回声协议	#echo stream tcp6 nowait root internal	建议关闭
	7/udp		#echo dgram udp6 wait root internal	
discard	9/tcp	RFC863 废除协议	#discard stream tcp6 nowait root internal	
	9/udp	RFC863 废除协议	#discard dgram udp6 wait root internal	
daytime	13/tcp	RFC867 白天协议	#daytime stream tcp6 nowait root internal	
	13/udp		#daytime dgram udp6 wait root internal	
chargen	19/tcp	RFC864 字符产生协议	#chargen stream tcp6 nowait root internal	
	19/udp		#chargen dgram udp6 wait root internal	
ftp	21/tcp	文件传输协议(控制)	#ftp stream tcp6 nowait root /usr/sbin/in.ftpd in.ftpd	根据实际情况选择开放
telnet	23/tcp	虚拟终端协议	#telnet stream tcp6 nowait root /usr/sbin/in.telnetd in.telnetd	根据实际情况选择开放
smtp	25/tcp	简单邮件发送协议	/etc/rc*.d/s_*sendmail	建议关闭
time	37/tcp	时间服务	#time stream tcp6 nowait root internal	建议关闭
	37/udp		#time dgram udp6 wait root internal	
name	42/udp	Host Name Server	#name dgram udp wait root /usr/sbin/in.tnamed in.tnamed	根据实际情况选择开放
finger	79/tcp	Finger Server	finger stream tcp6 nowait nobody /usr/sbin/in.fingerd in.fingerd	高风险服务，建议关闭
http	80/tcp	HTTP	#http stream tcp nowait nobody /opt/webserver/bin/httpd httpd	强烈建议关闭
sunrpc	111/tcp	sunrpc portmap	/etc/rc*.d/s*_rpc	根据实际情况选择开放
	111/udp		/etc/rc*.d/s*_rpc	根据实际情况选择开放
ntp	123/udp	Network Time Protocol	/etc/rc*.d/s*_ntpd	根据实际情况选择开放
snmp	161/udp	简单网络管理协议	/etc/rc*.d/s*_snmpdx	根据实际情况选择开放
dtlogin	177/udp	dtlogin	/etc/rc*.d/s*_dtlogin	根据实际情况选

				择开放
exec	512/tcp	Remote Process Execution	#exec stream tcp nowait root /usr/sbin/in.rexecd in.rexecd	根据情况选择开放
biff	512/udp	comsat	#comsat dgram udp wait root /usr/sbin/in.comsat in.comsat	建议关闭
login	513/tcp	Remote Login	#login stream tcp nowait root /usr/sbin/in.rlogind in.rlogind	根据情况选择开放
shell	514/tcp	shell	#shell stream tcp nowait root /usr/sbin/in.rshd in.rshd	根据情况选择开放
syslog	514/udp	syslogd	/etc/rc*.d/s_*syslog	建议保留
printer	515/tcp	spooler	#printer stream tcp6 nowait root /usr/lib/print/in.lpd in.lpd	强烈建议关闭
talk	517/udp	talk	#talk dgram udp wait root /usr/sbin/in.talkd in.talkd	建议关闭
route	520/udp	routed	在该文件中的 if 前加注释符	根据情况选择开放
uucp	540/tcp	uucp daemon	#uucp stream tcp nowait root /usr/sbin/in.uucpd in.uucpd	根据情况选择开放
submissi on	587/tcp	Mail Message Submission	/etc/rc*.d/s_*sendmail	根据情况选择开放
	587/udp	Mail Message Submission	/etc/rc*.d/s_*sendmail	根据情况选择开放
sm_conf g	603/tcp	SUNWsma	#sm_config stream tcp nowait root /opt/SUNWsma/bin/sma_configd sma_configd	根据情况选择开放
sun-dr	665/tcp	Remote Dynamic Reconfiguration	#sun-dr stream tcp wait root /usr/lib/dcs dcs	建议关闭
sdtp erf m e	834/udp	CDE protocol	/etc/rc*.d/s_*dtlogin	根据情况选择开放
WBEM	898/tcp	Sun wbem	/etc/rc*.d/s_*wbem	建议关闭
sdtp erf m e t e r	953/udp	CDE sdtp erf m e t e r	/etc/rc*.d/s_*dtlogin	根据情况选择开放
xaudio	1103/tcp	X Audio Server	#xaudio stream tcp wait root /usr/openwin/bin/Xaserver Xaserver -noauth -inetd	建议关闭

lockd	4045/tcp	NFS lock daemon/manager	/etc/rc*.d/s_*nfs.client	根据情况选择开放
WBEM	5987/tcp	Sun wbem	/etc/rc*.d/s_*wbem	建议关闭
X11	6000/tcp	X Window	/etc/rc*.d/s_*dtlogin	根据情况选择开放
dtspc	6112/tcp	CDE subprocess control	#dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd	强烈建议关闭
fs	7100/tcp	font-service	#fs stream tcp wait nobody /usr/openwin/lib/fs.auto fs	根据情况选择开放
dwhttpd	8888/tcp	dwhttpd	/etc/rc*.d/s_*ab2mgr	建议关闭
htt_serve	9010/tcp	htt_serve	/etc/rc*.d/s_*lilim	建议关闭
lockd	4045/udp	NFS lock daemon/manager	/etc/rc*.d/s_*nfs.client	强烈建议关闭
clustmon	12000/tcp	SUNWmond	#clustmon stream tcp nowait root /usr/sbin/in.mond in.mond	根据情况选择开放
ttsession	动态端口 □>32768/tcp	ToolTalk	/etc/rc*.d/s_*dtlogin	强烈建议关闭
snmpXdmid	动态端口 □>32768/tcp	SNMP to DMI mapper daemon	/etc/rc3.d/s*dmi	强烈建议关闭
sadmind	动态端口 □>32768/TCP&udp	Solstice	#100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind	强烈建议关闭
rquotad	动态端口 □>32768/TCP&udp	rquotaprog quota rquota	#rquotad/1 tli rpc/datagram_v wait root /usr/lib/nfs/rquotad rquotad	强烈建议关闭
rusersd	动态端口 □>32768/TCP&udp	rusers	#rusersd/2-3 tli rpc/datagram_v,circuit_v wait root /usr/lib/netshvc/rusers/rpc.rusersd rpc.rusersd	强烈建议关闭
sprayd	动态端口 □>32768/TCP&udp	spray	#sprayd/1 tli rpc/datagram_v wait root /usr/lib/netshvc/spray/rpc.sprayd rpc.sprayd	强烈建议关闭
rwalld	动态端口 □>32768/TCP&udp	rwall shutdown	#walld/1 tli rpc/datagram_v wait root /usr/lib/netshvc/rwall/rpc.rwalld rpc.rwalld	强烈建议关闭

	dp			
rstatd	动态端 □>32768/TCP&udp	rstat rup perfometer rstat_svc	#rstatd/2-4 tli rpc/datagram_v wait root /usr/lib/netsvc/rstat/rpc.rstatd rpc.rstatd	强烈建议关闭
ttdbserverd	动态端 □>32768/TCP&udp	ttdbserver tooltalk	#100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd rpc.ttdbserverd	强烈建议关闭
kcms	动态端 □>32768/TCP&udp	SunKCMS Profile Server	#100221/1 tli rpc/tcp wait root /usr/openwin/bin/kcms_server kcms_server	强烈建议关闭
cachefs	动态端 □>32768/TCP&udp	CacheFS Daemon	#100235/1 tli rpc/ticotsord wait root /usr/lib/fs/cachefs/cachefs Daemon	强烈建议关闭

中国电信 MS SQL Server 数据库安全配置要求及参考操作

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	1
4.2 授权.....	4
4.3 口令.....	5
4.4 日志.....	5
4.5 不必要的存储过程.....	6
4.6 加密通信协议.....	8
4.7 补丁.....	9
4.8 连接超时设置.....	9
4.9 可信 IP 地址访问控制.....	10
4.10 连接数设置.....	10

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》（本规范）
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

本规范适用于中国电信使用 MS SQL Server 数据库的设备。本规范明确了 MS SQL Server 数据库安全配置方面的基本要求，适用于所有的安全等级。

由于版本不同，配置操作有所不同，本规范以 MS SQL Server2000 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1732-2008 《固定通信网安全防护要求》

YD/T 1734-2008 《移动通信网安全防护要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1746-2008 《IP 承载网安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

SA	Super Administrator	超级管理员账户
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据包协议
IP	Internet Protocol	网络协议

4 安全配置要求

4.1 账号

编号： 1

要求内容	应按照用户分配账号，避免不同用户间共享账号。
------	------------------------

操作指南	<p>1、参考配置操作</p> <p>sp_addlogin 'user_name_1','password1'</p> <p>sp_addlogin 'user_name_2','password2'</p> <p>或在企业管理器中直接添加远程登陆用户</p> <p>建立角色，并给角色授权，把角色赋给不同的用户或修改用户属性中的角色和权限</p> <p>2、补充操作说明</p> <p>user_name_1 和 user_name_2 是两个不同的账号名称，可根据不同用户，取不同的名称；</p>
检测方法	<p>1、判定条件</p> <p>不同名称的用户可以连接数据库</p> <p>2、检测操作</p> <p>在查询分析器中用 user_name_1/password1 连接数据库成功</p> <p>3、补充说明</p>

编号：2

要求内容	应删除与数据库运行、维护等工作无关的账号。
操作指南	<p>1、参考配置操作</p> <p>SQL SERVER 企业管理器->安全性->登陆中删除无关帐号；</p> <p>SQL SERVER 企业管理器->数据库->对应数据库->用户中删除无关帐号；</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>首先删除不需要的用户，已删除数据库不能登陆使用</p> <p>注：无关的账号主要指测试帐户、共享帐号、长期不用账号（半年以上不用）等</p> <p>2、检测操作</p> <p>在 MS SQL SERVER 查询分析器的登陆界面中使用已删除帐号登陆</p>

	3、补充说明
--	--------

编号：3

要求内容	禁止账号过高的用户启动 SQL server
操作指南	<p>参考配置操作</p> <p>新建 SQL server 服务账号后，建议将其从 User 组中删除，且不要把该账号提升为 Administrators 组的成员。授予以下 windows SQLRunAs 账户最少的权限启动 SQL Server 数据库。</p>
检测方法	查看启动账号权限

编号：4

要求内容	禁止 SA 账户远程登录
操作指南	<p>1. 参考配置操作</p> <p>1) 在服务器端使用企业管理器，并且选择"使用 Windows 身份验证"连接上 SQL Server。</p> <p>2) 展开"SQL Server 组"，鼠标右键点击 SQL Server 服务器的名称，选择"属性"，再选择"安全性"选项卡。</p> <p>3) 在"身份验证"下，只选择"Windows "。</p> <p>4) 重新启动 SQL Server 服务。</p> <p>(可以在 dos 或命令行下面 net stop mssqlserver 停止服务，net start mssqlserver 启动服务)。</p>
检测方法	SA 帐号不能连接 SQL server

编号：5

要求内容	非 SA 权限的用户不能够访问数据库系统表
操作指南	<p>1. 参考配置操作</p> <p>打开 SQLserver 的登录属性，点击数据库访问，分别点击 master、model、msdb、tempdb 这四个系统库，在下方的数据库角色允许中只选择 db_sysadmin。其他角色都不能被选择。</p>

检测方法	除 system administrator 角色外，其他角色的用户访问系统数据库均被拒绝。
------	--

4.2 授权

编号： 1

要求内容	在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	<p>1、参考配置操作</p> <p>a) 更改数据库属性，取消业务数据库帐号不需要的服务器角色；</p> <p>b) 更改数据库属性，取消业务数据库帐号不需要的“数据库访问许可”和“数据库角色中允许”中不需要的角色。</p> <p>2、补充操作说明</p> <p>操作 a)用于修改数据库帐号的最小系统角色</p> <p>操作 b)用于修改用户多余数据库访问许可权限和数据库内角色</p>
检测方法	<p>1、判定条件</p> <p>调整业务帐号权限后业务测试正常</p> <p>2、检测操作</p> <p>对业务系统数据库交互部分进行功能测试</p> <p>3、补充说明</p>

编号： 2

要求内容	使用数据库角色（ROLE）来管理对象的权限。
操作指南	<p>1、参考配置操作</p> <p>c) 企业管理器->数据库->对应数据库->角色-中创建新角色；</p> <p>d) 调整角色属性中的权限，赋予角色中拥有对象对应的 SELECT、INSERT、UPDATE、DELETE、EXEC、DRI 权限</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>对应用户没有赋予不必要的权限</p>

	2、检测操作
--	--------

4.3 口令

编号： 1

要求内容	对用户的属性进行安全检查，包括空密码、密码更新时间等。修改目前所有账号的口令，确认为强口令。特别是 sa 账号，需要设置至少 10 位的强口令。
操作指南	1、参考配置操作 查看用户状态 运行查询分析器，执行 <pre>select * from sysusers</pre> <pre>Select name, Password from syslogins where password is null order by name # 查看口令为空的用户</pre> 2、补充操作说明
检测方法	1、判定条件 1. createdate、updatedate 时间为确认时间。 2. password 字段不为 null。 2、检测操作 1. 检查 createdate、updatedate 时间。 2. 检查 password 字段是否为 null。 3、补充说明 更改口令： Use master <pre>exec sp_password '旧口令', '新口令', 用户名</pre>

4.4 日志

编号： 1

要求内容	数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间。
操作指南	1、参考配置操作 打开数据库属性，选择安全性，将安全性中的审计级别调整为“全部”，身份验证调整为“SQL Server 和 Windows”

	2、补充操作说明
检测方法	1、判定条件 登录成功和失败测试，检查相关信息是否被记录 2、检测操作 3、补充说明

编号：2

要求内容	数据库应配置日志功能，记录对与数据库相关的安全事件。
操作指南	1、参考配置操作 数据库默认开启日志记录 2、补充操作说明 增加帐号登陆审计：打开数据库属性，选择安全性，将安全性中的审计级别调整为“全部”，身份验证调整为“SQL Server 和 Windows”
检测方法	1、判定条件 SQL Server 日志中是否存在数据库相关事件日志信息。对用户登录进行记录，包括用户登录使用的账号、登录是否成功、登录时间以及远程登录时用户使用的 IP 地址。 2、检测操作 打开企业管理器，查看数据库“管理”中的“SQL Server 日志”，查看当前的日志记录和存档的日志记录是否包含相关数据库安全事件 3、补充说明

4.5 不必要的存储过程

编号：1

要求内容	停用不必要的存储过程，同时在系统中删除或重命名相关 dll
操作指南	1、参考配置操作 以停用 xp_cmdshell 扩展存储过程为例： <pre>use master sp_dropextendedproc 'xp_cmdshell'</pre>

	<p>用以上命令可删除其他存储过程。</p> <p>一般情况下建议删除的存储过程有：</p> <p>Sp_OACreate</p> <p>Sp_OADestroy</p> <p>Sp_OAGetErrorInfo</p> <p>Sp_OAGetProperty</p> <p>Sp_OAMethod</p> <p>Sp_OASetProperty</p> <p>Sp_OAStop</p> <p>Xp_regaddmultistring</p> <p>Xp_regdeletekey</p> <p>Xp_regdeletevalue</p> <p>Xp_regenumvalues</p> <p>Xp_regremovemultistring</p> <p>xp_sdebug</p> <p>xp_availablemedia</p> <p>xp_cmdshell</p> <p>xp_deletemail</p> <p>xp_dirtree</p> <p>xp_dropwebtask</p> <p>xp_dsninfo</p> <p>xp_enumdsn</p> <p>xp_enumerrorlogs</p> <p>xp_enumgroups</p> <p>xp_enumqueuedtasks</p> <p>xp_eventlog</p> <p>xp_findnextmsg</p> <p>xp_fixeddrives</p> <p>xp_getfiledetails</p> <p>xp_getnetname</p> <p>xp_grantlogin</p> <p>xp_logevent</p> <p>xp_loginconfig</p> <p>xp_logininfo</p> <p>xp_makewebtask</p> <p>xp_msver xp_perfend</p> <p>xp_perfmonitor</p> <p>xp_perfsample</p> <p>xp_perfstart</p> <p>xp_readerrorlog</p> <p>xp_readmail</p> <p>xp_revokelogin</p> <p>xp_runwebtask</p>
--	--

	xp_schedulersignal xp_sendmail xp_servicecontrol xp_snmp_getstate xp_snmp_raisetrap xp_sprintf xp_sqlinventory xp_sqlregister xp_sqltrace xp_sscanf xp_startmail xp_stopmail xp_subdirs xp_unc_to_drive xp_dirtree
检测方法	1、判定条件 SQL Server 2000 下：从对象资源管理器打开 master 数据库->扩展存储过程查看，不必要的扩展存储过程已删除 2、检测操作 Exec 存储过程(参数 1，参数 2) 3、补充说明

4.6 加密通信协议

编号： 1

要求内容	使用通讯协议加密。
操作指南	1、参考配置操作 启动服务器网络配置工具，在“常规”中选择“强制协议加密” 2、补充操作说明 更改通讯协议加密后需要重新启动 SQL Server 数据库
检测方法	1、判定条件 2、检测操作 查找注册表默认实例 HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\MSSQLServer\\MSSQLServer\\SuperSocketNetLib\\Encrypt 或

	HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Microsoft SQL Server\\ 实例名\\MSSQLServer\\SuperSocketNetLib\\Encrypt" rs="eq">1< 3、补充说明
--	---

4.7 补丁

编号： 1

要求内容	系统安装了最新的安全补丁（注：在保证业务及网络安全的前提下，经过兼容性测试后）
操作指南	1、参考配置操作 检查当前所有已安装的数据库产品的版本信息，运行 SQL 查询分析器，执行： select @@version 安装补丁详细操作请参照其中的 readme 文件 SQL Server2000 的版本和补丁号对应关系如下： 8.00.194 —-----SQL Server 2000 RTM 8.00.384 —----- (SP1) 8.00.534 —----- (SP2) 8.00.760 —----- (SP3) 8.00.2039—----- (SP4) 2、补充操作说明
检测方法	1、判定条件 确保数据库是最新版本，无明显漏洞 2、检测操作 在 SQL Server 2000 下：打开 Microsoft SQL Server 企业管理器 -> 工具->SQL Server 配置属性，查看版本信息

4.8 连接超时设置

编号： 1

要求内容	在某些应用环境下，对数据库连接超时进行设置
操作指南	1、参考配置操作 打开数据库企业管理器->工具->SQL Server 配置属性->连接，设置其中的远程服务连接超时时间，如 15 分钟（参考设置）。

	2、补充操作说明 如果数据库在维护时被访问，该项为必选；如果被业务系统所访问，该项为可选
检测方法	1、判定条件 15 分钟以上的无任何操作的空闲数据库连接被自动断开

4.9 可信 IP 地址访问控制

编号： 1

要求内容	通过数据库所在操作系统或防火墙限制，只有信任的 IP 地址才能通过监听器访问数据库。
操作指南	1、参考配置操作 在防火墙中做限制，只允许与指定的 IP 地址建立 1433 的通讯。当然，从更为安全的角度来考虑，应该把 1433 端口改成其他的端口。 1. 在“Windows 防火墙”对话框中，单击“例外”选项卡。 2. 单击“添加端口”。 3. 键入您要允许的端口名称，键入端口号，然后单击“TCP”或“UDP”以提示这是 TCP 还是 UDP 端口。 4. 单击“更改范围”。 5. 指定要为其阻止此端口的一系列计算机，然后单击“确定”。
检测方法	1、判定条件 在非信任的客户端以数据库账户登陆被提示拒绝。 2、检测操作 打开“Windows 防火墙”。 单击“例外”选项卡，然后验证您的配置是否已应用于 Windows 防火墙。 3、补充说明

4.10 连接数设置

要求内容	根据机器性能和业务需求，设置最大最小连接数。
-------------	------------------------

操作指南	<p>1、参考配置操作</p> <p>执行 sql 指令：</p> <pre>sp_configure 'user connections', 需要的连接数 go reconfigure with override</pre> <p>补充操作说明</p> <p>连接数值：缺省值为 0（32767 的并发连接）。</p>
检测方法	<p>1、判定条件</p> <p>当连接数超过设定值时，会出现“已达到连接的最大限制”提示</p> <p>2、检测操作</p> <p>执行 sp_configure 查看当前使用的值</p>

中国电信 MySQL 数据库 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	1
4.2 口令.....	3
4.3 授权.....	4
4.4 日志.....	5
4.5 补丁.....	6
4.6 网络连接.....	6
4.7 可信 IP 地址访问控制.....	7
4.8 连接数设置.....	7

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》（本规范）
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

本规范适用于中国电信使用 MySQL 数据库的设备。本规范明确了 MySQL 数据库安全配置方面的基本要求，适用于所有安全等级。

由于版本不同，配置操作有所不同，本规范以UNIX平台上MySQL5.0\5.1 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1732-2008 《固定通信网安全防护要求》

YD/T 1734-2008 《移动通信网安全防护要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1746-2008 《IP 承载网安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

IP	Internet Protocol	网络协议
----	-------------------	------

4 安全配置要求

4.1 账号

编号：1

要求内容	以普通帐户安全运行 mysqld，禁止 mysql 以管理员帐号权限运行。
操作指南：	1、参考配置操作 Unix 下可以通过在/etc/my.cnf 中设置： [mysql.server]

	user=mysql 2、补充操作说明
检查方法:	1、判定条件 各种操作系统下以管理员权限运行。 Unix 下禁止以 root 账号运行 mysqld; 2、检测操作 检查进程属主和运行参数是否包含--user=mysql 类似语句: <pre># ps -ef grep mysqld</pre> <pre>#grep -i user /etc/my.cnf</pre>

编号：2

要求内容	应按照用户分配账号，避免不同用户间共享账号
操作指南	1. 参考配置操作 //创建用户 <pre>mysql> mysql> insert into</pre> <pre>mysql.user(Host,User>Password,ssl_cipher,x509_issuer,x509_sub</pre> <pre>ject) values("localhost","pppadmin",password("passwd"),",",");</pre> 这样就创建了一个名为： phplamp 密码为： 1234 的用户。 然后登录一下。 <pre>mysql>exit;</pre> <pre>@>mysql -u phplamp -p</pre> <pre>@>输入密码</pre> <pre>mysql>登录成功</pre> 2. 补充操作说明
检测方法	1. 判定条件 不用名称的用户可以连接数据库 2. 检测操作 使用不同用户连接数据库

编号：3

要求内容	应删除或锁定与数据库运行、维护等工作无关的账号
-------------	-------------------------

操作指南	<p>1. 参考配置操作</p> <p>DROP USER 语句用于删除一个或多个MySQL 账户。要使用 DROP USER，必须拥有 mysql 数据库的全局 CREATE USER 权限或 DELETE 权限。账户名称的用户和主机部分与用户表记录的User 和Host 列值相对应。</p> <p>使用 DROP USER，您可以取消一个账户和其权限，操作如下：</p> <p>DROP USER user;</p> <p>该语句可以删除来自所有授权表的帐户权限记录。</p> <p>2. 补充操作说明</p> <p>要点：</p> <p>DROP USER 不能自动关闭任何打开的用户对话。而且，如果用户有打开的对话，此时取消用户，则命令不会生效，直到用户对话被关闭后才生效。一旦对话被关闭，用户也被取消，此用户再次试图登录时将会失败。</p>
检测方法	<p>检测操作：</p> <p>mysql 查看所有用户的语句</p> <p>输入指令 select user();</p> <p>依次检查所列出的账户是否为必要账户，删除无用户或过期账户。</p> <p>注：无关的账号主要指测试帐户、共享帐号、长期不用账号（半年以上不用）等</p>

4.2 口令

编号：1

要求内容	检查帐户默认密码和弱密码
操作指南	<p>1. 参考配置操作</p> <p>修改帐户弱密码</p> <p>如要修改密码，执行如下命令：</p> <p>mysql> update user set password=password('test!p3') where user='root';</p> <p>mysql> flush privileges;</p> <p>2. 补充操作说明</p>
检测方法	<p>1. 判定条件</p> <p>密码长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。</p> <p>2. 检测操作</p> <p>检查本地密码：(注意，管理帐号 root 默认是空密码)</p> <p>mysql> use mysql;</p> <p>mysql> select Host,User>Password,Select_priv,Grant_priv from user;</p>

4.3 授权

编号: 1

要求内容	在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	1、参考配置操作 合理设置用户权限，撤销危险授权。 2、补充操作说明
检测方法	1 判定条件 确保数据库没有不必要的或危险的授权 2 检测操作 查看数据库授权情况： mysql> use mysql; mysql> select * from user; mysql> select * from db; mysql> select * from host; mysql> select * from tables_priv; mysql> select * from columns_priv; 回收不必要的或危险的授权，可以执行 revoke 命令： mysql> help revoke Name: 'REVOKE' Description: Syntax: REVOKE priv_type [(column_list)] [, priv_type [(column_list)]] ... ON [object_type] { * *.* db_name.* db_name.tbl_name tbl_name db_name.routine_name } FROM user [, user] ...

4.4 日志

编号：1

要求内容 操作指南	<p>数据库应配置日志功能，</p> <p>mysql 有以下几种日志：</p> <p>错误日志： -log-err</p> <p>查询日志： -log （可选）</p> <p>慢查询日志： -log-slow-queries （可选）</p> <p>更新日志： -log-update</p> <p>二进制日志： -log-bin</p> <p>在 mysql 的安装目录下，打开 my.ini,在后面加上上面的参数，保存后重启 mysql 服务就行了。</p> <p>例如：</p> <p>#Enter a name for the binary log. Otherwise a default name will be used.</p> <p>#log-bin=</p> <p>#Enter a name for the query log file. Otherwise a default name will be used.</p> <p>#log=</p> <p>#Enter a name for the error log file. Otherwise a default name will be used.</p> <p>log-error=</p> <p>#Enter a name for the update log file. Otherwise a default name will be used.</p> <p>#log-update=</p> <p>上面只开启了错误日志，要开其他的日志就把前面的“#”去掉</p> <p>1、补充操作说明</p> <p>show variables like 'log_%';查看所有的 log 命令</p>
--------------	--

	2、 show variables like 'log_bin';查看具体的 log 命令
检测方法	<p>1 判定条件</p> <p>启用审核记录对数据库的操作，便于日后检查。</p> <p>2 检测操作</p> <p>打开/etc/my.cnf 文件，查看是否包含如下设置：</p> <pre>[mysqld] log = filename</pre>

4.5 补丁

编号：1

要求内容	系统安装了最新的安全补丁（注：在保证业务及网络安全的前提下，经过兼容性测试后）
操作指南	<p>1、参考配置操作</p> <p>下载并安装最新 mysql 安全补丁，</p> <p>2、补充操作说明</p> <p>安全警报和补丁下载网址是 http://www.mysql.com</p>
检测方法	<p>1 判定条件</p> <p>确保数据库为企业版，并且安装了最新安全补丁。如果是不安全的社区版，建议替换为企业版(收费)</p> <p>2 检测操作</p> <p>使用如下命令查看当前补丁版本：</p> <pre>mysql> SELECT VERSION()</pre>

4.6 网络连接

编号：1

要求内容	禁止网络连接，防止猜解密码攻击，溢出攻击和嗅探攻击。（仅限于应用和数据库在同一台主机的情况）
操作指南	<p>1、参考配置操作</p> <p>如果数据库不需远程访问，可以禁止远程 tcp/ip 连接，通过在 mysqld 服务器中参数中添加 --skip-networking 启动参数来使 mysql 不监听任何 TCP/IP 连接，增加安全性。</p> <p>2、补充操作说明</p>

检测方法	1 判定条件 远程无法连接 2 检测操作 <pre>#cat /etc/my.cnf #ps -ef grep -i mysql</pre> 或从客户机远程 telnet mysqlserver 3306
------	---

4.7 可信 IP 地址访问控制

编号： 1

要求内容	通过数据库所在操作系统或防火墙限制，只有信任的 IP 地址才能通过监听器访问数据库。
操作指南	1、参考配置操作 执行命令：mysql> GRANT ALL PRIVILEGES ON db.* • -> -> TO 用户名@'IP 子网/掩码'; 只有通过指定 IP 地址段的用户才可以登录 2、补充操作说明
检测方法	1、判定条件 在非信任的客户端以数据库账户登陆被提示拒绝。 2、检测操作 用户从其它子网登录，将被拒绝 3、补充说明

4.8 连接数设置

要求内容	根据机器性能和业务需求，设制最大最小连接数。
操作指南	1、参考配置操作 编辑 MySQL 配置文件：my.cnf 或者是 my.ini 在[mysqld]配置段添加： <pre>max_connections = 1000</pre> 保存，重启 MySQL 服务。
检测方法	1、判定条件

	<p>2、检测操作</p> <p>用命令：SHOW [FULL] PROCESSLIST 显示哪些线程正在运行</p> <p>mysql admin -uroot -p variables</p> <p>输入 root 数据库账号的密码后可看到</p> <p> max_connections 1000 </p> <p>3、补充说明</p>
--	--

中国电信 Oracle 数据库 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	1
4.2 口令.....	4
4.3 授权.....	7
4.4 日志.....	10
4.5 补丁.....	13
4.6 Listener.....	13
4.7 可信 IP 地址访问控制.....	14
4.8 连接超时设置.....	15
4.9 数据传输安全.....	15
4.10 连接数设置.....	16

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》（本规范）
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用 Oracle 数据库的设备。本规范明确了 Oracle 数据库安全配置的基本要求，适用于所有的安全等级，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 UNIX 平台上 Oracle 10g 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》
YD/T 1732-2008 《固定通信网安全防护要求》
YD/T 1734-2008 《移动通信网安全防护要求》
YD/T 1736-2008 《互联网安全防护要求》
YD/T 1738-2008 《增值业务网—消息网安全防护要求》
YD/T 1740-2008 《增值业务网—智能网安全防护要求》
YD/T 1758-2008 《非核心生产单元安全防护要求》
YD/T 1746-2008 《IP 承载网安全防护要求》
YD/T 1752-2008 《支撑网安全防护要求》
YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

3 缩略语

DBA	Database Administrator	数据库管理员
-----	------------------------	--------

4 安全配置要求

4.1 账号

编号： 1

要求内容	应按照用户分配账号，避免不同用户间共享账号
------	-----------------------

操作指南	1、参考配置操作 <pre>create user abc1 identified by password1;</pre> <pre>create user abc2 identified by password2;</pre> 建立 role，并给 role 授权，把 role 赋给不同的用户 2、补充操作说明 <i>abc1</i> 和 <i>abc2</i> 是两个不同的账号名称，可根据不同用户，取不同的名称；
检测方法	1、判定条件 不同名称的用户可以连接数据库 2、检测操作 connect abc1/password1 连接数据库成功

编号： 2

要求内容	应删除或锁定与数据库运行、维护等工作无关的账号
操作指南	1、参考配置操作 <pre>alter user username account lock;</pre> <pre>drop user username cascade;</pre> 2、补充操作说明
检测方法	1、判定条件 首先锁定不需要的用户 在经过一段时间后，确认该用户对业务确无影响的情况下，可以删除 注：无关的账号主要指测试帐户、共享帐号、长期不用账号（半年以上不用）等 2、检测操作

编号： 3

要求内容	禁止以管理员帐号权限运行 oracle。
操作指南：	1、参考配置操作 打开 spfile，修改设置来禁止 SYSDBA 用户从远程登陆： REMOTE_LOGIN_PASSWORDFILE=NONE 2、补充操作说明

检查方法:	1、判定条件 不能通过 Sql*Net 远程以数据库超级管理员权限用户连接到数据库。
-------	--

编号：4

要求内容	启用数据字典保护，只有 SYSDBA 用户才能访问数据字典基础表
操作指南	1、参考配置操作 通过设置下面初始化参数来限制只有 SYSDBA 权限的用户才能访问数据字典。 <code>O7_DICTIONARY_ACCESSIBILITY = FALSE</code> 2、补充操作说明
检测方法	1、判定条件 以普通 dba 用户登陆到数据库，不能查看 X\$开头的表，比如： <code>select * from sys. x\$kspapi;</code> 2、检测操作 1) 以 Oracle 用户登陆到系统中。 2) 以 sqlplus '/as sysdba' 登陆到 sqlplus 环境中。 3) 使用 show parameter 命令来检查参数 <code>O7_DICTIONARY_ACCESSIBILITY</code> 是否设置为 FALSE。 <code>Show parameter O7_DICTIONARY_ACCESSIBILITY</code> 3、补充说明

编号：5

要求内容	限制在 DBA 组中的操作系统用户数量，通常 DBA 组中只有 Oracle 安装用户。
操作指南	1、参考配置操作 通过/etc/passwd 文件来检查是否有其它用户在 DBA 组中。 2、补充操作说明
检测方法	3、判定条件 无其它用户属于 DBA 组。 4、检测操作

	通过/etc/passwd 文件来检查是否有其它用户在 DBA 组中。
	5、补充说明

4.2 口令

编号： 1

要求内容	对于采用静态口令进行认证的数据库，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。
操作指南	1、参考配置操作 为用户建 profile，调整 PASSWORD_VERIFY_FUNCTION，指定密码复杂度 <pre>CREATE PROFILE "TEST_PROFILE" LIMIT PASSWORD_VERIFY_FUNCTION VERIFY_FUNCTION; ALTER USER "USER_NAME" PROFILE "TEST_PROFILE";</pre> 2、补充操作说明
检测方法	1、判定条件 修改密码为不符合要求的密码，将失败 2、检测操作 <pre>alter user abcd1 identified by abcd1;</pre> 将失败 3、补充说明

编号： 2（可选）

要求内容	对于采用静态口令认证技术的数据库，账户口令的生存期不长于 90 天。
操作指南	1、参考配置操作 为用户建相关 profile，指定 PASSWORD_GRACE_TIME 为 90 天 2、补充操作说明 在 90 天内，需要修改密码
检测方法	1、判定条件 到期不修改密码，密码将会失效。连接数据库将不会成功 2、检测操作

	<p>connect username/password 报错</p> <p>3、补充说明</p> <p>1. 以 DBA 用户登陆到 sqlplus 中。</p> <p>2. 通过语句 select * from dba_profiles ;</p> <p>查看 PASSWORD_GRACE_TIME 的设置。</p>
--	--

编号： 3

要求内容	对于采用静态口令认证技术的数据库，应配置数据库，使用户不能重复使用最近 5 次（含 5 次）内已使用的口令。
操作指南	<p>1、参考配置操作</p> <p>为用户建 profile,指定 PASSWORD_REUSE_MAX 为 5</p> <p>2、补充操作说明</p> <p>当前使用的密码，必需在密码修改 5 次后才能再次被使用</p>
检测方法	<p>1、判定条件</p> <p>重用修改 5 次内的密码，将不能成功</p> <p>2、检测操作</p> <p>alter user username identified by password1;如果 password1 在 5 次修改密码内被使用，该操作将不能成功</p> <p>3、补充说明</p>

编号： 4

要求内容	对于采用静态口令认证技术的数据库，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。
操作指南	<p>1、参考配置操作</p> <p>为用户建 profile，指定 FAILED_LOGIN_ATTEMPTS 为 6</p> <p>2、补充操作说明</p> <p>如果连续 6 次连接该用户不成功，用户将被锁定</p>
检测方法	<p>1、判定条件</p> <p>连续 6 次用错误的密码连接用户，第 7 次时用户将被锁定</p>

	2、检测操作 connect username/password，连续 6 次失败，用户被锁定 超级用户除外 3、补充说明
--	--

编号： 5

要求内容	修改默认帐户密码
操作指南	1、参考配置操作 1. 可通过下面命令来更改默认用户的密码： ALTER USER XXX IDENTIFIED BY XXX; 2. 下面是默认用户列表： ANONYMOUS CTXSYS DBSNMP DIP DMSYS EXFSYS HR LBACSYS MDDATA MDSYS MGMT_VIEW ODM ODM_MTR OE OLAPSYS ORDPLUGINS ORDSYS OUTLN

	PM QS QS_ADM QS_CB QS_CBADM QS_CS QS_ES QS_OS QS_WS RMAN SCOTT SH SI_INFORMTN_SCHEMA SYS SYSMAN SYSTEM TSM SYS WK_TEST WKPROXY WKSYS WMSYS XDB 2、补充操作说明
检测方法	1、判定条件 不能以用户名作为密码或使用默认密码的账户登陆到数据库。 2、检测操作 1. 以 DBA 用户登陆到 sqlplus 中。 2. 检查数据库默认账户是否使用了用户名作为密码或默认密码。

4.3 授权

编号： 1

要求内容	在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	<p>1、参考配置操作</p> <p>grant 权限 to username;</p> <p>revoke 权限 from username;</p> <p>授权原则：</p> <ul style="list-style-type: none"> ■ 角色授予遵循最小化原则 ■ 对象权限授予遵循最小化原则 ■ 系统权限授予遵循最小化原则 ■ public 用户组不存在不合理的执行权限 ■ 禁止对非 DBA 用户提供系统级权限 <p>2、补充操作说明</p> <p>用第一条命令给用户赋相应的最小权限</p> <p>用第二条命令收回用户多余的权限</p> <p>注：禁止对非 DBA 用户提供系统级权限</p>
检测方法	<p>select * from user_sys_privs;</p> <p>select * from user_role_privs;</p> <p>select * from user_tab_privs;</p> <p>检查用户拥有权限</p>

编号： 2

要求内容	限制具备数据库超级管理员（SYSDBA）权限的用户远程登录。
操作指南	<p>1、参考配置操作</p> <p>在 spfile 中设置 REMOTE_LOGIN_PASSWORDFILE=NONE 来禁止 SYSDBA 用户从远程登陆。</p> <p>2、补充操作说明</p> <p>REMOTE_LOGIN_PASSWORDFILE 参数在 init.ora 文件中设置。</p> <p>1) remote_login_passwordfile=none</p> <p>不使用密码文件登录；</p>

	<p>不允许远程用户用 sys 登录系统；</p> <p>可以在线修改 sys 的密码；</p> <p>2) remote_login_passwordfile=exclusive</p> <p>只允许一个数据库使用该密码文件；</p> <p>允许远程登录；</p> <p>允许非 sys 用户以 sysdba 身份管理数据库；</p> <p>可以在线修改 sys 的密码；</p> <p>3) remote_login_passwordfile=shared</p> <p>可以多个数据库使用密码文件。实际上是这样的: Oracle 数据库在启动时,首先查找的是 orapw<sid>的口令文件,如果该文件不存在,则开始查找,orapw 的口令文件；</p> <p>如果口令文件命名为 orapw,多个数据库就可以共享.；</p> <p>允许远程登录；</p> <p>只能用 sys 进行 sysdba 管理；</p> <p>可以在线修改 sys 的密码。</p>
检测方法	<p>1、判定条件</p> <p>REMOTE_LOGIN_PASSWORDFILE 设置为 NONE。</p> <p>2、检测操作</p> <p>1) 以 DBA 用户登陆到 sqlplus 中。</p> <p>2) 使用 show parameter 命令来检查参数</p> <p>REMOTE_LOGIN_PASSWORDFILE 是否设置为 NONE。</p> <p>Show parameter REMOTE_LOGIN_PASSWORDFILE</p> <p>3、补充说明</p> <p>此配置影响远程以 Sql*Net 方式对数据库的管理</p> <p>此配置也可能使某些第三方 ORACLE 管理工具不正常</p>

编号：3

要求内容	使用数据库角色（ROLE）来管理对象的权限。
操作指南	<p>1、参考配置操作</p> <p>1. 使用 Create Role 命令创建角色。</p>

	<p>2. 使用用 Grant 命令将相应的系统、对象或 Role 的权限赋予应用用户。</p> <p>2、补充操作说明</p>
检测方法	<p>3、判定条件</p> <p>对应用用户不要赋予 DBA Role 或不必要的权限。</p> <p>4、检测操作</p> <p>1. 以 DBA 用户登陆到 sqlplus 中。</p> <p>2. 通过查询 dba_role_privs、dba_sys_privs 和 dba_tab_privs 等视图来检查是否使用 ROLE 来管理对象权限。</p> <p>5、补充说明</p>

4.4 日志

编号：1

要求内容	<p>数据库应配置日志功能，对用户登录信息进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间以及远程登录时用户使用的 IP 地址。</p>
操作指南	<p>1、参考配置操作</p> <p>创建 ORACLE 登录触发器，记录相关信息，但对 IP 地址的记录会有困难</p> <p>1.建表 LOGON_TABLE</p> <p>2.建触发器</p> <pre>CREATE TRIGGER TRI_LOGON AFTER LOGON ON DATABASE BEGIN INSERT INTO LOGON_TABLE VALUES (SYS_CONTEXT('USERENV', 'SESSION_USER'), SYSDATE); END;</pre> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>登录测试，检查相关信息是否被记录</p>

	<p>2、检测操作</p> <p>3、补充说明</p> <p>触发器对短连接业务的资源开销比较大，使用时要慎重考虑，但对长连接的业务资源开销基本没有影响。</p> <p>触发器与 AUDIT 会有相应资源开销，请检查系统资源是否充足。特别是 RAC 环境，资源消耗较大。</p>
--	---

编号：2

要求内容	<p>数据库应配置日志功能，记录用户对数据库的操作，包括但不限于以下内容：账号创建、删除和权限修改、口令修改、读取和修改数据库配置、读取和修改业务用户的话费数据、身份数据、涉及通信隐私数据。记录需要包含用户账号，操作时间，操作内容以及操作结果。</p>
操作指南	<p>1、参考配置操作</p> <p>创建 ORACLE 登录触发器，记录相关信息，但对 IP 地址的记录会有困难</p> <p>1.建表 LOGON_TABLE</p> <p>2.建触发器</p> <pre>CREATE TRIGGER TRI_LOGON AFTER LOGON ON DATABASE BEGIN INSERT INTO LOGON_TABLE VALUES (SYS_CONTEXT('USERENV', 'SESSION_USER'), SYSDATE); END;</pre> <p>2、补充操作说明</p>
检测方法	<p>2、判定条件</p> <p>做相关操作，检查是否记录成功</p> <p>4、检测操作</p> <p>1、补充说明</p>

	触发器与 AUDIT 会有相应资源开销，请检查系统资源是否充足。特别是 RAC 环境，资源消耗较大。
--	--

编号：3

要求内容	数据库应配置日志功能，记录对与数据库相关的安全事件。
操作指南	<p>1、参考配置操作</p> <p>创建 ORACLE 登录触发器，记录相关信息，但对 IP 地址的记录会有困难</p> <p>1.建表 LOGON_TABLE</p> <p>2.建触发器</p> <pre>CREATE TRIGGER TRI_LOGON AFTER LOGON ON DATABASE BEGIN INSERT INTO LOGON_TABLE VALUES (SYS_CONTEXT('USERENV', 'SESSION_USER'), SYSDATE); END;</pre> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>做相关测试，检查是否记录成功</p> <p>2、检测操作</p> <p>3、补充说明</p> <p>触发器与 AUDIT 会有相应资源开销，请检查系统资源是否充足。特别是 RAC 环境，资源消耗较大。</p>

编号：4

要求内容	根据业务要求制定数据库审计策略。
操作指南	<p>1、参考配置操作</p> <p>1. 通过设置参数 audit_trail = db 或 os 来打开数据库审计。</p> <p>2. 然后可使用 Audit 命令对相应的对象进行审计设置。</p>

	2、补充操作说明
检测方法	<p>1、判定条件</p> <p>对审计的对象进行一次数据库操作，检查操作是否被记录。</p> <p>2、检测操作</p> <p>1. 检查初始化参数 audit_trail 是否设置。</p> <p>2. 检查 dba_audit_trail 视图中或\$ORACLE_BASE/admin/adump 目录下是否有数据。</p> <p>3、补充说明</p> <p>AUDIT 会有相应资源开销，请检查系统资源是否充足。特别是 RAC 环境，资源消耗较大。</p>

4.5 补丁

编号： 1

安全要求：	安装了最新的安全补丁（注：在保证业务及网络安全的前提下，经过兼容性测试后）
操作指南：	本地检查当前数据库补丁版本，以 oracle 身份执行如下命令： \$opatch lsinventory SQL> select * from v\$version;
检查方法：	<p>1、判定条件</p> <p>所有必要的漏洞补丁都已安装。</p> <p>2、检测操作</p> <p>去 ORACLE 查看安全警报，安装最新安全补丁 确保数据库补丁是最新版本，无明显漏洞</p> <p>3、补充说明</p>

4.6 Listener

编号： 1

要求内容	为数据库监听器（LISTENER）的关闭和启动设置密码。
操作指南	<p>1、参考配置操作</p> <p>通过下面命令设置密码：</p> <p>\$ lsnrctl</p> <p>LSNRCTL> change_password</p>

	<p>Old password: <OldPassword> Not displayed</p> <p>New password: <NewPassword> Not displayed</p> <p>Reenter new password: <NewPassword> Not displayed</p> <p>Connecting to</p> <p>(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=prolin1)(PORT=1521)(IP=FIRST)))</p> <p>Password changed for LISTENER</p> <p>The command completed successfully</p> <p>LSNRCTL> save_config</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>使用 lsnrctl start 或 lsnrctl stop 命令起停 listener 需要密码</p> <p>2、检测操作</p> <p>检查 \$ORACLE_HOME/network/admin/listener.ora 文件中是否设置参数 PASSWORDS_LISTENER。</p> <p>3、补充说明</p>

4.7 可信 IP 地址访问控制

编号： 1

要求内容	通过数据库所在操作系统或防火墙限制，只有信任的 IP 地址才能通过监听器访问数据库。
操作指南	<p>1、参考配置操作</p> <p>只需在服务器上的文件 \$ORACLE_HOME/network/admin/sqlnet.ora 中设置以下行：</p> <p>tcp.validnode_checking = yes</p> <p>tcp.invited_nodes = (ip1,ip2...)</p> <p>2、补充操作说明</p> <p>如果网络层已经做过访问控制，该项为可选项，否则为必选项</p> <p>可信内网地址指：专用维护终端、访问数据库应用服务器、堡垒机</p>

	其他地址段禁止。
检测方法	<p>1、判定条件</p> <p>在非信任的客户端以数据库账户登陆被提示拒绝。</p> <p>2、检测操作</p> <p>检查 \$ORACLE_HOME/network/admin/sqlnet.ora 文件中是否设置参数 tcp.validnode_checking 和 tcp.invited_nodes。</p> <p>3、补充说明</p>

4.8 连接超时设置

要求内容	在某些应用环境下可设置数据库连接超时，比如数据库将自动断开超过 15 分钟的空闲远程连接。
操作指南	<p>1、参考配置操作</p> <p>在 sqlnet.ora 中设置下面参数：</p> <p>SQLNET.EXPIRE_TIME=15</p> <p>2、补充操作说明</p> <p>如果数据库在维护时被访问，该项为必选；如果被业务系统所访问，该项为可选</p>
检测方法	<p>1、判定条件</p> <p>15 分钟以上的无任何操作的空闲数据库连接被自动断开</p> <p>2、检测操作</p> <p>检查 \$ORACLE_HOME/network/admin/sqlnet.ora 文件中是否设置参数 SQLNET.EXPIRE_TIME。</p>

4.9 数据传输安全

要求内容	使用 Oracle 提供的高级安全选件来加密客户端与数据库之间或中间件与数据库之间的网络传输数据。
操作指南	<p>1、参考配置操作</p> <p>1. 在 Oracle Net Manager 中选择 “Oracle Advanced Security”。</p> <p>2. 然后选择 Encryption。</p>

	<p>3. 选择 Client 或 Server 选项。</p> <p>4. 选择加密类型。</p> <p>5. 输入加密种子（可选）。</p> <p>6. 选择加密算法（可选）。</p> <p>7. 保存网络配置，sqlnet.ora 被更新。</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>通过网络层捕获的数据库传输包为加密包。</p> <p>2、检测操作</p> <p>检 查 \$ORACLE_HOME/network/admin/sqlnet.ora 文 件 中 是 否 设 置 sqlnet.encryption 等参数。</p> <p>3、补充说明</p>

4.10 连接数设置

要求内容	根据机器性能和业务需求，设置最大最小连接数。
操作指南	<p>1、参考配置操作</p> <p>以管理员登录数据库，执行下列命令修改进程连接数，如修改到 200</p> <pre>alter system set processes=200 scope=spfile;</pre> <p>修改会话数</p> <pre>alter system set sessions=225 scope=spfile;</pre> <p>重启数据库，启用参数</p> <pre>shutdown immediate;</pre> <pre>startup;</pre> <p>3、补充操作说明</p> <p>可能需要同时修改 unix 系统参数：/etc/proc/kernel 中 semmns。</p>
检测方法	<p>1、判定条件</p> <p>执行 select count(*) from v \$ session;检查会话数能够接近 200</p> <p>2、检测操作</p> <p>执行 show parameter processes;可以看到 processes 和 sessions 参数以按照</p>

	设定修改。
	3、补充说明

中国电信 Apache 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	1
4.2 授权.....	2
4.3 日志.....	3
4.4 禁止访问外部文件.....	3
4.5 目录列出.....	4
4.6 错误页面重定向.....	4
4.7 拒绝服务防范.....	5
4.8 隐藏 Apache 的版本号.....	5
4.9 关闭 TRACE.....	5
4.10 禁用 CGI.....	6
4.11 监听地址绑定.....	7
4.12 补丁.....	7
4.13 更改默认端口.....	7
4.14 删除缺省安装的无用文件.....	7
4.15 HTTP 加密协议.....	8
4.16 连接数设置.....	8
4.17 禁用非法 HTTP 方法.....	9

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》（本规范）
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用的 Apache 服务器。本规范提出了 Apache 服务器安全配置要求，适用于所有的安全等级，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 unix 平台上 Apache2.0\2.2 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

3 缩略语

CGI	Common Gateway Interface	通用网关接口
HTTP	HyperText Transfer Protocol	超文本传输协议

4 安全配置要求

4.1 账号

要求内容	以专门的用户帐号和组运行 Apache。
操作指南	<p>1、根据需要为 Apache 创建用户、组</p> <p>2、参考配置操作</p> <p>如果没有设置用户和组，则新建用户，并在 Apache 配置文件中指定</p> <p>(1) 创建 apache 组: <code>groupadd apache</code></p> <p>(2) 创建 apache 用户并加入 apache 组: <code>useradd apache -g</code></p>

	<p>apache</p> <p>(3) 将下面两行加入 Apache 配置文件 httpd.conf 中</p> <p>User apache</p> <p>Group apache</p> <p>2、补充操作说明</p> <p>1、根据不同用户，取不同的名称。</p> <p>2、为用户设置适当的家目录和 shell。</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>检查 httpd.conf 配置文件。</p> <p>检查是否使用非专用账户（如 root）运行 apache</p>

4.2 授权

编号:1

要求内容	严格控制Apache 主目录的访问权限，非超级用户不能修改该目录中的内容
操作指南	<p>1、参考配置操作</p> <p>Apache 的主目录对应于Apache Server配置文件httpd.conf的Server Root控制项中，应为：</p> <p>Server Root /usr/local/apache</p>
检测方法	<p>1、判定条件</p> <p>非超级用户不能修改该目录中的内容</p> <p>2、检测操作</p> <p>尝试修改，看是否能修改</p>

编号: 2

要求内容	严格设置配置文件和日志文件的权限，防止未授权访问
操作指南	<p>1、参考配置操作：</p> <p>使用命令“chmod 600 /etc/httpd/conf/httpd.conf”设置配置文件为属主可读写，其他用户无权限</p> <p>使用命令“chmod 644 /var/log/httpd/*.log”设置日志文件为属主可读写，其他用户只读权限</p>
检测方法	<p>1、判定条件 2、检测操作</p> <p>使用命令查看配置文件和日志文件的权限</p> <p>[root@centos ~]# ls -l /etc/httpd/conf/httpd.conf</p> <p>-rw-r--r-- 1 root root 7571 May 13 17:45</p> <p>/etc/httpd/conf/httpd.conf</p>

	[root@centos ~]# ls -l /var/log/httpd
--	---------------------------------------

4.3 日志

要求内容	设备应配置日志功能，对运行错误、用户访问等进行记录，记录内容包括时间，用户使用的 IP 地址等内容。
操作指南	<p>1、参考配置操作</p> <p>编辑 httpd.conf 配置文件，设置日志记录文件、记录内容、记录格式。</p> <p>其中，错误日志：</p> <p>LogLevel notice #日志的级别</p> <p>ErrorLog ../logs/error_log #日志的保存位置（错误日志）</p> <p>访问日志：</p> <p>LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Accept}i\" \"%{Referer}i\" \"%{User-Agent}i\" combined</p> <p>CustomLog ../logs/access_log combined （访问日志）</p> <p>ErrorLog 指令设置错误日志文件名和位置。错误日志是最重要的日志文件，Apache httpd 将在这个文件中存放诊断信息和处理请求中出现的错误。若要将错误日志送到 Syslog，则设置：ErrorLog syslog。</p> <p>CustomLog 指令指定了保存日志文件的具体位置以及日志的格式。访问日志中会记录服务器所处理的所有请求。</p> <p>LogFormat 设置日志格式，建议设置为 combined 格式。LogLevel 用于调整记录在错误日志中的信息的详细程度，建议设置为 notice。</p>
检测方法	<p>1、判定条件</p> <p>查看 logs 目录中相关日志文件内容，记录完整。</p> <p>2、检测操作</p> <p>查看相关日志记录。</p> <p>3、补充说明</p>

4.4 禁止访问外部文件

要求内容	禁止 Apache 访问 Web 目录之外的任何文件。
操作指南	<p>1、参考配置操作</p> <p>编辑 httpd.conf 配置文件，</p> <pre><Directory /> Order Deny,Allow Deny from all </Directory></pre> <p>2、补充操作说明</p> <p>设置可访问目录，</p> <pre><Directory /web> Order Allow,Deny Allow from all</pre>

	</Directory> 其中/web 为网站根目录。
检测方法	1、判定条件 无法访问 Web 目录之外的文件。 2、检测操作 访问服务器上不属于 Web 目录的一个文件，结果应无法显示。 3、补充说明

4.5 目录列出

要求内容	禁止 Apache 列表显示文件
操作指南	1、参考配置操作 (1) 编辑 httpd.conf 配置文件， <Directory "/web"> Options Indexes FollowSymLinks #删掉 Indexes AllowOverride None Order allow,deny Allow from all </Directory> 将 Options Indexes FollowSymLinks 中的 Indexes 去掉，就可以禁止 Apache 显示该目录结构。Indexes 的作用就是当该目录下没有 index.html 文件时，就显示目录结构。 (2)重新启动 Apache 服务
检测方法	1、判定条件 当 WEB 目录中没有默认首页如 index.html 文件时，不会列出目录内容 2、检测操作 直接访问 http://ip/xxx (xxx 为某一目录)

4.6 错误页面重定向

要求内容	Apache 错误页面重定向
操作指南	1、参考配置操作 (1) 修改 httpd.conf 配置文件： ErrorDocument 400 /custom400.html ErrorDocument 401 /custom401.html ErrorDocument 403 /custom403.html ErrorDocument 404 /custom404.html ErrorDocument 405 /custom405.html ErrorDocument 500 /custom500.html Customxxx.html 为要设置的错误页面。 (2)重新启动 Apache 服务
检测方法	1、判定条件 指向指定错误页面

	2、检测操作 URL 地址栏中输入 http://ip/xxxxxxx~~~（一个不存在的页面）
--	--

4.7 拒绝服务防范

要求内容	根据业务需要，合理设置 session 时间，防止拒绝服务攻击
操作指南	1、参考配置操作 (1) 编辑 httpd.conf 配置文件， Timeout 10 #客户端与服务器端建立连接前的时间间隔 KeepAlive On KeepAliveTimeout 15 #限制每个 session 的保持时间是 15 秒 注：此处为一建议值，具体的设定需要根据现实情况。 (2)重新启动 Apache 服务
检测方法	1、判定条件 2、检测操作 检查 httpd.conf 配置文件是否设置。

4.8 隐藏 Apache 的版本号

要求内容	隐藏 Apache 的版本号及其它敏感信息。
操作指南	1、参考配置操作 修改 httpd.conf 配置文件： ServerSignature Off ServerTokens Prod
检测方法	1、判定条件 2、检测操作 检查 httpd.conf 配置文件。

4.9 关闭 TRACE

要求内容	关闭 TRACE，防止 TRACE 方法被访问者恶意利用
操作指南	1、参考配置操作 使用命令 “vi /etc/httpd/conf/httpd.conf” 修改配置文件，添加 “TraceEnable Off” 注：适用于 Apache 2.0 以上版本
检测方法	1、判定条件 2、检测操作 客户端： #nc 1.1.1.4 80 输入下面两行内容后，两次回车 OPTIONS * HTTP/1.1 HOST:1.1.1.4 服务器返回： HTTP/1.1 200 OK

	Date: Wed, 13 May 2009 07:09:31 GMT Server: Apache/2.2.3 (CentOS) Allow: GET,HEAD,POST,OPTIONS,TRACE Content-Length: 0 Connection: close Content-Type: text/plain; charset=UTF-8 表示支持 TRACE 方法, 注意查看是否还支持其他方法, 如: PUT, DELETE 等, 一般情况下都不应该出现在生产主机上
--	--

4.10 禁用 CGI

要求内容	如果服务器上不需要运行 CGI 程序, 建议禁用 CGI
操作指南	1、参考配置操作 (1) 使用命令 “ vi /etc/httpd/conf/httpd.conf ” 修改配置文件, 把 cgi-bin 目录的配置和模块都注释掉 <pre>#LoadModule cgi_module modules/mod_cgi.so #ScriptAlias /cgi-bin/ "/var/www/cgi-bin/" #<Directory "/var/www/cgi-bin"> # AllowOverride None # Options None # Order allow,deny # Allow from all #</Directory></pre>
检测方法	1、判定条件 2、检测操作 使用命令 “ vi /etc/httpd/conf/httpd.conf ” 查看配置文件 <pre>LoadModule cgi_module modules/mod_cgi.so #加载的模块 ScriptAlias /cgi-bin/ "/var/www/cgi-bin/" <Directory "/var/www/cgi-bin"> AllowOverride None Options None Order allow,deny Allow from all </Directory></pre>

4.11 监听地址绑定

要求内容	服务器有多个 IP 地址时，只监听提供服务的 IP 地址
操作指南	1、参考配置操作 使用命令“ vi /etc/httpd/conf/httpd.conf ”修改配置文件，修改 Listen x.x.x.x:80
检测方法	1、判定条件 2、检测操作 使用命令“ cat /etc/httpd/conf/httpd.conf grep Listen ”查看是否 绑定 IP 地址

4.12 补丁

要求内容	在不影响业务的情况下，升级解决高危漏洞，而且该补丁要通过实验测试。
操作指南	1、参考配置操作： 访问 http://httpd.apache.org/download.cgi ，查看最新的 apache 版本， 在实验室测试通过的前提下，编译升级 apache，以解决高危漏洞。
检测方法	1、判定条件 2、检测操作 根据 apache 安装路径使用命令行查看版本情况。如： /usr/local/apache/bin/apachectl -v 与需要的版本进行对比。

4.13 更改默认端口

要求内容	更改 Apache 服务器非公众服务默认端口
操作指南	1、参考配置操作 (1) 修改 httpd.conf 配置文件，更改默认端口到 xx 端口（不常见端口） Listen x.x.x.x:xx 端口 (2) 重启 Apache 服务 2、补充操作说明
检测方法	1、判定条件 使用 XX 端口登陆页面成功 2、检测操作 登陆 http://ip:XX 3、补充说明

4.14 删除缺省安装的无用文件

要求内容	删除缺省安装的无用文件。
操作指南	1、参考配置操作

	删除缺省 HTML 文件： <pre># rm -rf /usr/local/apache2/htdocs/*</pre> 删除缺省的 CGI 脚本： <pre># rm -rf /usr/local/apache2/cgi-bin/*</pre> 删除 Apache 说明文件： <pre># rm -rf /usr/local/apache2/manual</pre> 删除源代码文件： <pre># rm -rf /path/to/httpd-2.2.4*</pre> 根据安装步骤不同和版本不同，某些目录或文件可能不存在或位置不同。
检测方法	1、判定条件 2、检测操作 检查对应目录。

4.15 HTTP 加密协议

要求内容	对于通过 HTTP 协议进行远程维护的设备，设备应支持使用 HTTPS 等加密协议。
操作指南	1、参考配置操作 不同的 apache 版本，可能对 ssl 的支持不一样。有的在编译的时候，就支持 mod_ssl 模块，有的未支持。 此处建议，根据不同情况，做具体处理。由于步骤繁琐，不统一提出配置操作建议。
检测方法	1、判定条件 2、检测操作 <pre>rpm -q mod_ssl</pre>

4.16 连接数设置

要求内容	根据机器性能和业务需求，设置最大最小连接数。
操作指南	1、参考配置操作 使用 <code>httpd -l</code> 检查 Apache 的工作模式，如列出 <code>prefork.c</code> ，则进行下列操作： 修改 <code>httpd.conf</code> 文件 找到 <pre><IfModule prefork.c> StartServers 8 MinSpareServers 5 MaxSpareServers 20 MaxClients 150 MaxRequestsPerChild 1000 </IfModule></pre> 修改

	<p><i>MaxClients</i> 150</p> <p>为需要的连接数，如 1500</p> <p><i>ServerLimit</i> 1500 //连接数大于 256 需设置此项</p> <p><i>MaxClients</i> 1500</p> <p>然后保存退出。</p> <p>重新启动 http 服务：</p> <p>/etc/rc.d/init.d/httpd restart</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>httpd.conf 文件中的内容已被修改</p> <p>2、检测操作</p> <p>通过 ps -ax grep httpd 命令确认 httpd 进程已启动。</p> <p>通过 ps -ef grep httpd wc -l 命令检查现在的连接数</p> <p>3、补充说明</p>

4.17 禁用非法 HTTP 方法

要求内容	禁用PUT、DELETE等危险的HTTP 方法；
操作指南	<p>1、参考配置操作</p> <p>编辑 httpd.conf 文件，只允许 get、post 方法</p> <p><LimitExcept GET POST ></p> <p>Deny from all</p> <p></LimitExcept></p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>查看 httpd.conf 文件，检查如下内容，是否只允许 get、post 方法</p> <p><LimitExcept GET POST ></p> <p>Deny from all</p> <p></LimitExcept></p>

中国电信 IIS 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	1
4.2 口令.....	3
4.3 授权.....	5
4.4 日志.....	6
4.5 更改默认安装路径.....	8
4.6 不必要的服务组件.....	8
4.7 删除危险的实例文件.....	10
4.8 删除不必要的脚本映射.....	10
4.9 补丁.....	11
4.10 目录列出.....	11
4.11 自定义错误信息.....	12
4.12 SSL 加密通信.....	12
4.13 上传目录权限设置.....	12
4.14 HTTP 加密协议.....	13
4.15 连接数设置.....	13
4.16 禁用非法 HTTP 方法.....	14

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》（本规范）
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用的 IIS 服务器。本规范提出了 IIS 安全配置要求，适用于所有的安全等级，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 IIS 6.0 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

3 缩略语

HTTP	HyperText Transfer Protocol	超文本传输协议
FTP	File Transfer Protocol	文本传输协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SSL	Secure Sockets Layer	安全套接层

4 安全配置要求

4.1 账号

编号：1

要求内容	应按照用户分配账号。避免用户账号和设备间通信使用的账号共享（对于 IIS 用户定义分为两个层次：一、IIS 自身操作用户，二、IIS 发布应用访问用户）
操作指南	1、参考配置操作 1、为不同维护人员创建账号：进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：根据系统的要求，

	<p>设定不同的账户和账户组.对应设置 IIS 系统管理员的权限。</p> <p>2、为创建账号设置权限：进入 IIS 管理器->相应网站“属性”->“目录安全性”->“匿名访问和身份验证控制”的“编辑”：其中分为“匿名访问身份”及“基本（Basic）验证”。“基本身份验证”包含：“集成 windows 身份验证”、“Windows 域服务器的摘要身份验证”、“基本身份验证”、“.NET Passport 身份验证”；可依据维护人员进行不同权限访问控制配置。</p>
检测方法	<p>1、判定条件</p> <p>结合要求和实际业务情况判断符合要求，根据系统的要求，设定不同的账户和账户组。</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：查看根据系统的要求，设定不同的账户和账户组。</p> <p>进入 IIS 管理器->相应网站“属性”->“目录安全性”->“匿名访问和身份验证控制”查看相应配置。</p>

编号：2

要求内容	应删除或锁定与设备运行、维护等工作无关的账号。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：删除或锁定与设备运行、维护等与工作无关的账号。</p> <p>IIS 安装后生成帐号: IUSR_主机名、IWAM_主机名、ASPNET 三用户，依据应用情况建议只保留系统维护帐号。</p> <p>1.IUSR_主机名:Internet 来宾帐户，匿名访问 Internet 信息服务的内置帐户。如果删除影响页面浏览，建议保留。</p> <p>2.IWAM_主机名: 启动 IIS 进程帐户，用于启动进程外应用程序的 Internet 信息服务的内置帐户。建议保留。</p> <p>3.ASPNET: ASP.NET 计算机帐户，用于运行 ASP.NET 辅助进程(aspnet_wp.exe)的帐户。IIS 系统安装后会默认支持 ASP，如网</p>

	站无动态内容，可禁用该帐户，如网站有动态内容需保留此账户。
检测方法	<p>1、判定条件</p> <p>结合要求和实际业务情况判断符合要求，删除或锁定与设备运行、维护等与工作无关的账号。</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：查看是否删除或锁定与设备运行、维护等与工作无关的账号。如网站无动态内容，系统只保留管理员、IUSR_主机名、IWAM_主机名、维护人员账号，无其他账号，如网站有动态内容系统保留管理员、IUSR_主机名、IWAM_主机名、ASPNET、维护人员账号，无其他账号。</p>

编号：3

要求内容	禁用超级用户启用 IIS
操作指南	<p>1、参考配置操作</p> <p>在控制面板->管理工具->服务，选择“www 服务”属性，在设置启动属性中指定使用一个普通账号启动本服务。</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>查看，控制面板->管理工具->服务，选择“www 服务”属性，查看服务启动的账号。</p>

4.2 口令

编号：1

要求内容	对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类（IIS 基于 Windows 系统，可通过提升 Windows 自身密码安全等级实现）
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：“密码必须符合复杂性要求”选择“已启动”</p>

检测方法	<p>1、判定条件</p> <p>“密码必须符合复杂性要求”选择“已启动”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：查看是否“密码必须符合复杂性要求”选择“已启动”</p>
------	---

编号：2

要求内容	对于采用静态口令认证技术的设备，维护人员使用的账户口令的生存期不长于90天(IIS 基于 Windows 系统,可通过提升 Windows 帐户策略实现)
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：“密码最长存留期”设置为“90 天”</p>
检测方法	<p>1、判定条件</p> <p>“密码最长存留期”设置为“90 天”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：查看是否“密码最长存留期”设置为“90 天”</p>

编号：3

要求内容	对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近 5 次（含 5 次）内已使用的口令（IIS 基于 Windows 系统，可通过提升 Windows 帐户策略实现）
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：“强制密码历史”设置为“记住 5 个密码”</p>
检测方法	<p>1、判定条件</p> <p>“强制密码历史”设置为“记住 5 个密码”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“帐户策略-></p>

	密码策略”：查看是否“强制密码历史”设置为“记住 5 个密码”
--	---------------------------------

编号：4

要求内容	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号（IIS 基于 Windows 系统，可通过提升 Windows 帐户策略实现）
操作指南	1、参考配置操作 进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：“账户锁定阈值”设置为 6 次
检测方法	1、判定条件 “账户锁定阈值”设置为小于或等于 6 次 2、检测操作 进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：查看是否“账户锁定阈值”设置为小于等于 6 次

4.3 授权

要求内容	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限（对于 IIS 用户定义分为两个层次：一、IIS 自身操作用户，二、IIS 发布应用访问用户；设备权限的配置基于上述两方面考虑）
操作指南	1、参考配置操作 原则： （1）文件夹和文件的访问权限：安放在 NTFS 文件系统上的文件夹和文件，一方面要对其权限加以控制，对不同的用户组和用户进行不同的权限设置；另外，可利用 NTFS 的审核功能对某些特定用户组成员读文件的企图等方面进行审核，有效地通过监视如文件访问、用户对象的使用等发现非法用户进行非法活动的前兆，及时加以预防制止。 （2）目录的访问权限：已经设置成 Web 目录的文件夹，可以通

	<p>过操作 Web 站点属性页面实现对 www 目录访问权限的控制，而该目录下的所有文件和子 文件夹都将继承这些安全性。www 服务除了提供 NTFS 文件系统提供的权限外，还提供读取权限，允许用户读取或下载 WWW 目录中的文件；执行权限，允许用户运行 www 目录下的程序和脚本。</p> <p>参考操作：</p> <p>（1）启动“域用户管理器”-> “规则”选单下的“审核”选项-> “审核规则”</p> <p>（2）启动 ISM（Internet 服务器管理器）-> 启动 Web 属性页面并选择“目录”选项卡；-> 选择 www 目录；-> 选择“编辑属性”中的“目录属性”进行设置：“脚本资源访问”、“读取”、“写入”、“目录浏览”、“记录访问”、“索引资源”。</p>
检测方法	<p>1、判定条件</p> <p>检测用户权限审核及 ISM 目录安全属性。</p> <p>2、检测操作</p> <p>（1）启动“域用户管理器”-> “规则”选单下的“审核”选项-> “审核规则”，检测 “审核规则”配置状态。</p> <p>（2）启动 ISM（Internet 服务器管理器）-> 启动 Web 属性页面并选择“目录”选项卡；-> 选择 www 目录；-> “编辑属性”中的“目录属性”，查看配置状态。</p>

4.4 日志

编号：1

要求内容	启用日志功能
操作指南	<p>1、参考配置操作</p> <p>打开 IIS 管理工具，右击要管理的站点，选择“属性”。在“网站”的“启用日志记录”部分，日志格式支持“Microsoft IIS 日志文件格式”、“W3C”，“W3C”日志格式存在日志记录时间与服务器时间不统一的问题，所以应尽量采用 IIS 日志格式。（根据需要，如有特殊要求可以采用其他格式的日志，如 W3C 扩展日志文件格式）</p>

检测方法	<p>1、判定条件</p> <p>启用日志记录，并采用 IIS 日志格式。</p> <p>2、检测操作</p> <p>开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性”检查是否“启用日志记录”并采用“Microsoft IIS 日志文件格式”。</p>
------	---

编号：2

要求内容	设备应配置日志功能，记录与设备相关的安全事件。
操作指南	<p>1、参考配置操作</p> <p>(1) 进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中配置相应“审核对象访问”、“审核目录服务器访问”、“审核系统事件”、“审核帐号管理”、“审核过程追踪”等选项。</p> <p>(2) 运行 IIS 管理器->“Internet 信息服务”->“应用相关站点”属性->“网站”->“属性”->“高级”，选择“时间”、“日期”、“扩展属性”</p>
检测方法	<p>1、判定条件</p> <p>确定系统相关“审核策略”。</p> <p>确定 IIS 相关“站点属性”日志详细记录。</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，查看“本地策略->审核策略”配置“成功”、“失败”的选择记录。</p>

编号：3

要求内容	设备应配置权限，控制对日志文件读取、修改和删除等操作。
操作指南	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中配置相应“审核策略更改”配置相应选项。</p>
检测方法	<p>1、判定条件</p> <p>确定系统相关“审核策略”</p>

	2、检测操作 进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中配置相应“审核策略更改”选项选择状态。
--	---

4.5 更改默认安装路径


要求内容	更改 IIS 默认安装路径。
操作指南	1、参考配置操作 开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性”。 IIS 安装后的默认主目录是“%system%inetpubwwwroot”，为更好地抵抗踩点、刺探等攻击行为，应该删除默认目录，更改主目录位置，同时也要避免安装在系统盘上，参考操作如下图所示： <div data-bbox="489 900 1174 1603" data-label="Image"> </div>
检测方法	1、判定条件 更改 IIS 默认安装路径。 2、检测操作 开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性”。查看是否更改 IIS 默认安装路径。

4.6 不必要的服务组件

编号：1

要求内容	IIS 是架设 WEB、FTP、SMTP 服务器的一套整合软件，如果不是必须，不得安装 FTP、SMTP 服务。
操作指南	1、参考配置操作 已经安装的上述不必服务，可以通过“控制面板” -> “添加/删除程序” -> “添加删除 IIS 组件” -> “internet 信息服务（IIS）”中删除不必要的服务组件。
检测方法	1、判定条件 查看 FTP、SMTP 服务没有被安装。 2、检测操作 可以通过“控制面板” -> “添加/删除程序” -> “添加删除 IIS 组件” -> “internet 信息服务（IIS）”中检查是否删除不必要的服务组件。

编号：2

要求内容	如果业务系统不需要 ASP 支持，必须按照下图的方法将默认启用的“asp.net”功能扩展禁止。
操作指南	1、参考配置操作 
检测方法	1、判定条件 2、检测操作 开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“web 服务扩展”。检查是否禁用“asp.net”功能。

4.7 删除危险的实例文件

要求内容	删除可能带来风险的实例文件。														
操作指南	<p>1、参考配置操作</p> <p>进入相应目录，删除实例文件</p> <table> <tr> <td>IIS</td><td>c:\inetpub\iissamples</td></tr> <tr> <td>Admin Scripts</td><td>c:\inetpub\scripts</td></tr> <tr> <td>Admin Samples</td><td>%systemroot%\system32\inetsrv\adminsamples</td></tr> <tr> <td>IISADMPWD</td><td>%systemroot%\system32\inetsrv\iisadmpwd</td></tr> <tr> <td>IISADMIN</td><td>%systemroot%\system32\inetsrv\iisadmin</td></tr> <tr> <td>Data access</td><td>c:\Program Files\Common Files\System\msadc\Samples</td></tr> <tr> <td>MSADC</td><td>c:\program files\common files\system\msadc</td></tr> </table>	IIS	c:\inetpub\iissamples	Admin Scripts	c:\inetpub\scripts	Admin Samples	%systemroot%\system32\inetsrv\adminsamples	IISADMPWD	%systemroot%\system32\inetsrv\iisadmpwd	IISADMIN	%systemroot%\system32\inetsrv\iisadmin	Data access	c:\Program Files\Common Files\System\msadc\Samples	MSADC	c:\program files\common files\system\msadc
IIS	c:\inetpub\iissamples														
Admin Scripts	c:\inetpub\scripts														
Admin Samples	%systemroot%\system32\inetsrv\adminsamples														
IISADMPWD	%systemroot%\system32\inetsrv\iisadmpwd														
IISADMIN	%systemroot%\system32\inetsrv\iisadmin														
Data access	c:\Program Files\Common Files\System\msadc\Samples														
MSADC	c:\program files\common files\system\msadc														
检测方法	<p>1、判定条件</p> <p>删除可能带来风险的实例文件。</p> <p>2、检测操作</p> <p>进入 c:\inetpub; c:\Program Files\Common Files\System\msadc\Samples 查看是否删除可能带来风险的实例文件。</p>														

4.8 删除不必要的脚本映射

要求内容	删除不必要的脚本映射。
操作指南	<p>1、参考配置操作</p> <p>开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性” -> 主目录 -> 配置，然后从列表中删除</p> <p>以下不必要的脚本，包括：.httr、.idc、.stm、.shtm、.printer、.htw、.ida 和 .idq。</p> <p>删除的原则：只保留需要的脚本映射。</p>
检测方法	<p>1、判定条件</p> <p>删除不必要的脚本映射。</p> <p>2、检测操作</p> <p>开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右</p>

	键点击“属性” -> 主目录 -> 配置： 查看是否删除不必要的脚本映射。
--	--

4.9 补丁

要求内容	在不影响业务的情况下，将 IIS 升级到最新补丁，而且该补丁经过试验测试。
操作指南	1、参考配置操作 下载 IIS 补丁包 对于 IIS4.0 和 IIS5.0，访问 http://www.microsoft.com/downloads/en/resultsForProduct.aspx?displaylang=en&productId=1254887e-e07d-4d64-91a1-dd6ed2149f21&stype=ss_sd&nr=10&sortCriteria=Popularity&sortOrder=Ascending （英文版）；和 http://www.microsoft.com/downloads/zh-cn/resultsForProduct.aspx?displaylang=en&productId=1254887e-e07d-4d64-91a1-dd6ed2149f21&stype=ss_sd&nr=10&sortCriteria=Popularity&sortOrder=Ascending （中文版）；下载最新更新并安装，或升级到 IIS6.0 或 7.0
检测方法	1、判定条件 已安装 IIS 最新补丁包。 2、检测操作 控制面板->添加或删除程序->显示更新打钩，查看是否安装 IIS 补丁包。

4.10 目录列出

要求内容	禁止 IIS 列表显示文件
操作指南	1、参考配置操作 开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性” -> 主目录，保证“目录浏览”没有被勾选。
检测方法	1、判定条件 2、检测操作

	开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性” -> 主目录，查看相应配置。
--	---

4.11 自定义错误信息

要求内容	错误页面重定向
操作指南	1、参考配置操作 开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性” -> 自定义错误，自定义错误消息为指定的 URL 或文件指针。
检测方法	1、判定条件 指向指定错误页面 2、检测操作 URL 地址栏中输入 http://ip/xxxxxxx~~~（一个不存在的页面）

4.12 SSL 加密通信

要求内容	对敏感数据的传输，应该使用 SSL 加密，防止数据被嗅探。
操作指南	1、参考配置操作 进入“控制面板->管理工具->Internet 信息服务(IIS)管理器”，在管理器中，右键选择站点的“属性”，点击“目录安全性”选项卡，点击“安全通信”的编辑按钮，启用 SSL。
检测方法	1、判定条件 未启用 SSL 进行通信 2、检测操作 进入“控制面板->管理工具->Internet 信息服务(IIS)管理器”，在管理器中，右键选择站点的“属性”，点击“目录安全性”选项卡，点击“安全通信”的编辑按钮，查看是否启用 SSL。

4.13 上传目录权限设置

要求内容	禁止动态脚本在上传目录的运行权限，防止攻击者绕过过滤系统上传 webshell。
操作指南	1、参考配置操作

	<p>进入“控制面板->管理工具->Internet 信息服务(IIS)管理器”，在管理器中，右键选择站点中上传目录的“属性”，点击“主目录”选项卡，点击“应用程序设置”的“执行权限”下拉菜单，选择“无”。</p>
检测方法	<p>1、判定条件</p> <p>询问开发工程师，找到存放上传文件的目录，检查相关上传目录是否启用了“执行权限”。</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->Internet 信息服务(IIS)管理器”，在管理器中，右键选择站点中上传目录的“属性”，点击“主目录”选项卡，查看相应权限。</p>

4.14 HTTP 加密协议

要求内容	对于通过 HTTP 协议进行远程维护的设备，设备应支持使用 HTTPS 等加密协议。
操作指南	<p>1、参考配置操作</p> <p>在控制面板->管理工具->IIS 管理器，双击“web 根目录”，在属性中的高级设置中选择支持 ssl 的 443 端口</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>查看，控制面板->管理工具->IIS 管理器，双击“web 根目录”，在属性中的高级设置中是否启用了 ssl。</p>

4.15 连接数设置

要求内容	根据机器性能和业务需求，设置最大最小连接数。
操作指南	<p>1、参考配置操作</p> <p>增加网站的连接限制。若要这样做，请按照下列步骤操作：</p> <ol style="list-style-type: none"> 1. 单击 开始，指向 所有程序，都指向 管理工具，然后单击 Internet Information Services (IIS) 管理器。 2. 展开 ComputerName，然后展开 网站。 3. 用鼠标右键单击您想要配置的网站，然后单击 属性。 4. 单击 性能 选项卡。 5. 在网站连接，单击连接限制，然后键入想要设置的连接限制

	<p>数。</p> <p>6. 单击 确定，然后退出 IIS 管理器。</p>
检测方法	<p>1、判定条件</p> <p>网站的连接数高于设定值时，以下内容的错误信息将记录在 Web 服务器上 Httperr.log 文件中：</p> <p>HTTP/1.1 GET / 503 1 ConnLimit DefaultAppPool</p> <p>2、检测操作</p> <p>选择开始 – 管理工具- 性能 – 加入 web 服务的连接计数，查看当前连接数</p>

4.16 禁用非法 HTTP 方法

要求内容	禁用PUT、DELETE等危险的HTTP 方法；
操作指南	<p>1、参考配置操作</p> <p>IIS 管理器中的 Web 服务扩展节点，选择 webdav 禁用。</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>在 IIS 管理器中的 Web 服务扩展节点中，查看 webdav 是否被禁用。</p>

中国电信 TOMCAT 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	1
4.2 口令.....	2
4.3 授权.....	3
4.4 日志.....	4
4.5 HTTP 加密协议.....	5
4.6 更改默认管理端口.....	5
4.7 错误页面重定向.....	6
4.8 目录列出.....	7
4.9 系统 Banner 信息.....	7
4.10 连接数设置.....	8
4.11 禁用非法 HTTP 方法.....	8

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》（本规范）
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》

1 范围

适用于中国电信使用的 TOMCAT 服务器。本规范提出了 TOMCAT 安全配置要求，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 UNIX 平台上 TOMCAT6.x 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1736-2008《互联网安全防护要求》

YD/T 1738-2008《增值业务网—消息网安全防护要求》

YD/T 1740-2008《增值业务网—智能网安全防护要求》

YD/T 1758-2008《非核心生产单元安全防护要求》

YD/T 1752-2008《支撑网安全防护要求》

3 缩略语

HTTP	HyperText Transfer Protocol	超文本传输协议
------	-----------------------------	---------

4 安全配置要求

4.1 账号

编号：1

要求内容	应按照用户分配账号。避免不同用户间共享账号。
操作指南	1、参考配置操作 修改 tomcat/conf/tomcat-users.xml 配置文件，修改或添加帐号。 <user username="tomcat" password=" Manager!@34" roles="manager"> 2、补充操作说明 1、根据不同用户，取不同的名称。 2、Tomcat 从 5.5 这个版本及以后发行的版本默认都不存在 admin.xml

	配置文件。
检测方法	1、判定条件 各账号都可以登录 Tomcat Web 服务器为正常 2、检测操作 访问 http://ip:8080/manager/html 管理页面，进行 Tomcat 服务器管理

编号：2

要求内容	应删除或锁定与设备运行、维护等工作无关的账号。
操作指南	1、参考配置操作 修改 tomcat/conf/tomcat-users.xml 配置文件，删除与工作无关的帐号。 例如 tomcat1 与运行、维护等工作无关，删除 tomcat1 帐号。
检测方法	1、判定条件 被删除的与工作无关的账号 tomcat1 不能正常登陆。 2、检测操作 访问 http://ip:8080/manager/html 管理页面，使用删除帐号进行登陆尝试。

编号：3

要求内容	禁用超级用户启用 tomcat
操作指南	1、参考配置操作 在普通用户的模式下，运行 tomcat 的启动脚本
检测方法	1、判定条件 2、检测操作 查看当前系统的 tomcat 进程，确认程序启动时使用的身份。

4.2 口令

要求内容	对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。
操作指南	1、参考配置操作 在 tomcat/conf/tomcat-user.xml 配置文件中设置密码 <user username="tomcat" password="Manager!@34" roles="manager"> 2、补充操作说明 口令要求：长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。

检测方法	<p>1、判定条件 检查 tomcat/conf/tomcat-user.xml 配置文件中的帐号口令是否符合配置口令复杂度要求。</p> <p>2、检测操作 (1) 人工检查配置文件中帐号口令是否符合； (2) 使用 tomcat 弱口令扫描工具定期对 Tomcat Web 服务器进行远程扫描，检查是否存在弱口令帐号。</p> <p>3、补充说明 使用弱口令扫描工具进行检查时应注意扫描的线程数，避免对服务器造成不必要的资源消耗；选择在服务器负荷较低的时间段进行扫描检查。</p>
------	---

4.3 授权

编号1:

要求内容	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
操作指南	<p>1、参考配置操作 编辑 tomcat/conf/tomcat-user.xml 配置文件，修改用户角色权限授权 tomcat 具有远程管理权限： <user username="tomcat" password="Manager!@34" roles="admin,manager"></p> <p>2、补充操作说明 Tomcat 用户角色分为：role1，tomcat，admin，manager 四种。 role1：具有读权限； tomcat：具有读和运行权限； admin：具有读、运行和写权限； manager：具有远程管理权限。 注：Tomcat 6.0.18 版本只有 admin 和 manager 两种用户角色，且 admin 用户具有 manager 管理权限。</p>
检测方法	<p>1、判定条件 登陆远程管理页面，使用 tomcat 账号进行登陆，登陆成功。</p> <p>2、检测操作 登陆 http://ip:8080/manager/html 页面，使用 tomcat 账号登陆，进行远程管理。</p>

编号：2

要求内容	禁用manager功能
操作指南	<p>1、参考配置操作 将以下目录 \$CATALINA_HOME/server/webapps/manager，移除到非 \$CATALINA_HOME/server/webapps 目录</p>
检测方法	<p>1、判定条件</p>

	2、检测操作 查看\$CATALINA_HOME/server/webapps/manager 是否存在
--	--

4.4 日志

编号：1

要求内容	设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。
操作指南	1、参考配置操作 编辑 server.xml 配置文件，在<HOST>标签中增加记录日志功能 将以下内容的注释标记<!-- -->取消 <pre><valve classname="org.apache.catalina.valves.AccessLogValve" Directory="logs" prefix="localhost_access_log." Suffix=".txt" Pattern="common" resolveHosts="false"/></pre> 2、补充操作说明 classname: This MUST be set to org.apache.catalina.valves.AccessLogValve to use the default access log valve. &<60 Directory: 日志文件放置的目录，在 tomcat 下面有个 logs 文件夹，那里是专门放置日志文件的，也可以修改为其他路径； Prefix: 这个是日志文件的名称前缀，日志名称为 localhost_access_log.2010-xx-xx.txt，前面的前缀就是这个 localhost_access_log Suffix: 文件后缀名 Pattern: common 方式时，将记录访问源 IP、本地服务器 IP、记录日志服务器 IP、访问方式、发送字节数、本地接收端口、访问 URL 地址等相关信息在日志文件中 resolveHosts: 值为 true 时，tomcat 会将这个服务器 IP 地址通过 DNS 转换为主机名，如果是 false，就直接写服务器 IP 地址
检测方法	1、判定条件 查看 logs 目录中相关日志文件内容，记录完整 2、检测操作 查看 localhost_access_log.2010-xx-xx.txt 中相关日志记录 3、补充说明

编号：2

要求内容	启用访问模块审计、错误信息日志功能
操作指南	1、参考配置操作 2、补充操作说明 编辑 server.xml 配置文件，在<HOST>标签中增加记录日志功能

	<p>将以下内容的注释标记<!-- -->取消</p> <pre><valve classname="org.apache.catalina.valves.AccessLogValve" Directory="logs" prefix="localhost_access_log." Suffix=".txt" Pattern="common" resolveHosts="false"/></pre>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>3、补充说明</p> <p>检查 server.xml 配置文件，在<HOST>标签中，查看以下内容是否被注释标记<!-- -->取消</p> <pre><valve classname="org.apache.catalina.valves.AccessLogValve" Directory="logs" prefix="localhost_access_log." Suffix=".txt" Pattern="common" resolveHosts="false"/></pre>

4.5 HTTP 加密协议

要求内容	对于通过 HTTP 协议进行远程维护的设备，设备应支持使用 HTTPS 等加密协议。
操作指南	<p>1、参考配置操作</p> <p>(1)使用 JDK 自带的 keytool 工具生成一个证书</p> <pre>JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore /path/to/my/keystore</pre> <p>(2)修改 tomcat/conf/server.xml 配置文件，更改为使用 https 方式，增加如下行：</p> <pre>Connector classname="org.apache.catalina.http.HttpConnector" port="8443" minProcessors="5" maxProcessors="100" enableLookups="true" acceptCount="10" debug="0" scheme="https" secure="true" > Factory classname="org.apache.catalina.SSLServerSocketFactory" clientAuth="false" keystoreFile="/path/to/my/keystore" keystorePass="runway1@" protocol="TLS"/> /Connector></pre> <p>其中 keystorePass 的值为生成 keystore 时输入的密码</p> <p>(3)重新启动 tomcat 服务</p>
检测方法	<p>1、判定条件</p> <p>使用 https 方式登陆 tomcat 服务器页面，登陆成功</p> <p>2、检测操作</p> <p>使用 https 方式登陆 tomcat 服务器管理页面</p>

4.6 更改默认管理端口

要求内容	使用 HTTP 协议的设备，更改 tomcat 服务器默认端口
操作指南	1、参考配置操作 (1) 修改 tomcat/conf/server.xml 配置文件，更改默认管理端口到 xx <Connector port="xx" maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"、 enableLookups="false" redirectPort="8443" acceptCount="100" connectionTimeout="300" disableUploadTimeout="true" /> (2) 重启 tomcat 服务 2、补充操作说明
检测方法	1、判定条件 使用 xx 端口登陆页面成功 2、检测操作 登陆 http://ip:xx 3、补充说明

4.7 错误页面重定向

要求内容	Tomcat 错误页面重定向
操作指南	1、参考配置操作 (1)配置 tomcat/conf/web.xml 文件: 在最后</web-app>一行之前加入以下内容: <error-page> <error-code>404</error-code> <location>/noFile.htm</location> </error-page> <error-page> <exception-type>java.lang.NullPointerException</exception-type> <location>/ error.jsp</location> </error-page> 第一个<error-page></error-page>之间的配置实现了将 404 未找到 jsp 网页的错误导向 noFile.htm 页面，也可以用类似方法添加其他的错误代码导向页面，如 403,500 等。 第二个<error-page></error-page>之间的配置实现了当 jsp 网页出现 java.lang.NullPointerException 导常时，转向 error.jsp 错误页面，还需要在第个 jsp 网页中加入以下内容: <% @ page errorPage="/error.jsp" %> 典型的 error.jsp 错误页面的程序写法如下: <% @ page contentType="text/html;charset=GB2312"%> <% @ page isErrorPage="true"%>

	<pre><html> <head><title>错误页面</title></head> <body>出错了: </p> 错误信息: <%= exception.getMessage() %>
 Stack Trace is : <pre><% java.io.CharArrayWriter cw = new java.io.CharArrayWriter(); java.io.PrintWriter pw = new java.io.PrintWriter(cw,true); exception.printStackTrace(pw); out.println(cw.toString()); %></pre> </body> </html></pre> <p>当出现 NullPointerException 异常时 tomcat 会把网页导入到 error.jsp, 且会打印出出错信息。</p> <p>(2)重新启动 tomcat 服务</p> <p>(3)要求错误页面不能太大</p>
检测方法	<p>1、判定条件 指向指定错误页面</p> <p>2、检测操作 URL 地址栏中输入 http://ip:8800/manager12345</p>

4.8 目录列出

要求内容	禁止 tomcat 列表显示文件
操作指南	<p>1、参考配置操作</p> <p>(1) 编辑 tomcat/conf/web.xml 配置文件,</p> <pre><init-param> <param-name>listings</param-name> <param-value>true</param-value> </init-param></pre> <p>把 true 改成 false</p> <p>(2)重新启动 tomcat 服务</p>
检测方法	<p>1、判定条件 当 WEB 目录中没有默认首页如 index.html,index.jsp 等文件时, 不会列出目录内容</p> <p>2、检测操作 直接访问 http://ip:8800/webadd</p>

4.9 系统 Banner 信息

要求内容	修改系统 Banner 信息
操作指南	<p>1、参考配置操作</p> <p>修改 catalina.jar 中 Serverinfo.properties 中的以下参数(修改以掩饰真实</p>

	版本信息): server.build=<BuildDate> server.number=X
检测方法	1、判定条件 2、检测操作 检查 catalina.jar 中 Serverinfo.properties 中的参数

4.10 连接数设置

要求内容	根据机器性能和业务需求，设置最大最小连接数。
操作指南	<p>1、参考配置操作</p> <p>编辑 server.xml 文件，样例如下：</p> <pre><Connector port="8080" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" acceptCount="100" /></pre> <p>maxThreads="150" 表示最多同时处理 150 个连接</p> <p>minSpareThreads="25" 表示即使没有人使用也开这么多空线程等待</p> <p>maxSpareThreads="75" 表示如果最多可以空 75 个线程</p> <p>acceptCount="100" 当同时连接的人数达到 maxThreads 时，还可以接收排队的连接，超过这个连接的则直接返回拒绝连接</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>此项设置，需根据应用的具体情况，分别配置相应的参数。</p> <p>3、补充说明</p>

4.11 禁用非法 HTTP 方法

要求内容	禁用PUT、DELETE等危险的HTTP 方法；
操作指南	<p>1、参考配置操作</p> <p>编辑 web.xml 文件中配置</p> <p>org.apache.catalina.servlets.DefaultServlet 的</p> <pre><init-param></pre>

	<pre><param-name>readonly</param-name> <param-value>>false</param-value> </init-param></pre> <p>readonly 参数默认是 true，即不允许 delete 和 put 操作。</p> <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>检查 web.xml 文件中配置 org.apache.catalina.servlets.DefaultServlet 的<init-param></p> <pre><param-name>readonly</param-name> <param-value>>false</param-value> </init-param></pre> <p>其中 param-value 为 false，则符合要求。</p>

中国电信 WebLogic 安全配置要求及操作指南

目 录

目 录.....	I
前 言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 缩略语.....	1
4 安全配置要求.....	1
4.1 账号.....	1
4.2 口令.....	4
4.3 日志.....	5
4.4 Keystore 和 SSL 设置.....	9
4.5 Sockets 最大打开数量.....	10
4.6 文件和目录权限.....	11
4.7 WebLogic 运行模式.....	12
4.8 Sender Server Header.....	12
4.9 删除 Sample 程序.....	12
4.10 设定默认出错页面.....	14
4.11 session 超时时间.....	14
4.12 补丁.....	15
4.13 HTTP 加密协议.....	15
4.14 连接数设置.....	15

前 言

为了在工程验收、运行维护、安全检查等环节，规范并落实安全配置要求，中国电信编制了一系列的安全配置要求及操作指南，明确了操作系统、数据库、应用中间件在内的通用安全配置要求及参考操作。

该系列安全配置要求及操作指南的结构及名称预计如下：

- (1) 《中国电信 Windows 操作系统安全配置要求及操作指南》
- (2) 《中国电信 AIX 操作系统安全配置要求及操作指南》
- (3) 《中国电信 HP-UX 操作系统安全配置要求及操作指南》
- (4) 《中国电信 Linux 操作系统安全配置要求及操作指南》
- (5) 《中国电信 Solaris 操作系统安全配置要求及操作指南》
- (6) 《中国电信 MS SQL server 数据库安全配置要求及操作指南》
- (7) 《中国电信 MySQL 数据库安全配置要求及操作指南》
- (8) 《中国电信 Oracle 数据库安全配置要求及操作指南》
- (9) 《中国电信 Apache 安全配置要求及操作指南》
- (10) 《中国电信 IIS 安全配置要求及操作指南》
- (11) 《中国电信 Tomcat 安全配置要求及操作指南》
- (12) 《中国电信 WebLogic 安全配置要求及操作指南》（本规范）

1 范围

适用于中国电信使用的 Weblogic 服务器。本规范提出了 Weblogic 服务器安全配置要求，适用于所有的安全等级，可作为编制设备入网测试、安全验收、安全检查规范等文档的参考。

由于版本不同，配置操作有所不同，本规范以 unix 平台上 Weblogic9.x 为例，给出参考配置操作。

2 规范性引用文件

GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

YD/T 1736-2008 《互联网安全防护要求》

YD/T 1738-2008 《增值业务网—消息网安全防护要求》

YD/T 1740-2008 《增值业务网—智能网安全防护要求》

YD/T 1758-2008 《非核心生产单元安全防护要求》

YD/T 1752-2008 《支撑网安全防护要求》

3 缩略语

SSL	Secure Sockets Layer	安全套接层
HTTP	HyperText Transfer Protocol	超文本传输协议

4 安全配置要求

4.1 账号

编号：1

要求内容	为不同的管理用户分配不同的角色
参考操作	以管理员身份登录控制台 1. 点击左侧面板”Security”文件夹，展开”REALM” 2. 点击”Users”文件夹，修改非特权用户为角色 Administrators、Deployers、Monitors、Operators 之一

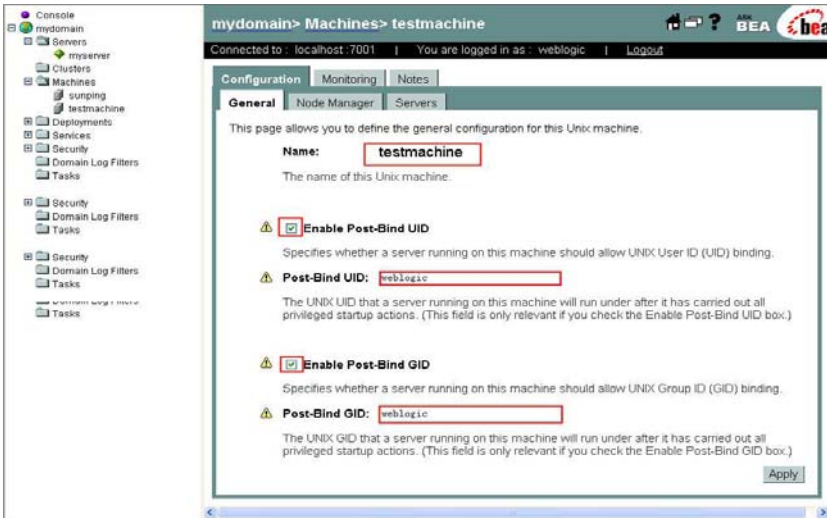

检测方法	1、判定条件 2、检测操作 以管理员身份登录控制台 1. 点击左侧面板”Security”文件夹，展开”REALM” 2. 点击”Users”文件夹，查看用户所属组及组、全局角色配置
------	---

编号：2

要求内容	应删除与设备运行、维护等工作无关的账号
参考操作	以管理员身份登录控制台 1. 点击左侧面板”Security”文件夹，展开”REALM” 2. 点击”Users”文件夹，删除与设备运行、维护等工作无关的账号
检测方法	1、判定条件 没有与设备运行、维护等工作无关的账号

编号：3

要求内容	禁止以特权用户身份运行 WebLogic
操作指南	1、参考配置操作 以WebLogic管理员身份登录管理控制台,执行: 1. 在左面板，点击”Machine”文件夹 2. 在右面板，选择”Configure a New Unix Machine link” 3. 输入 unix 机器名,勾选” Enable Post-bind UID field”并输入用户名,该用户名必须对 BEA_HOME 及子目录有完全控制权限，输入对应组(用户名和组名须事先在 OS 中单独创建),点击”Apply”按钮. 注意：不要使用默认的 nobody 用户，如下图所示：

	 <p>4. 选择“Servers”标签. 从”Available list” 移动 每个想要的服务器实例到 “Chosen list”. 然后击”Apply”按钮</p> 
检测方法	<p>1、判定条件</p> <p>以特权用户身份启动应用服务器，绑定端口之后改变 UID 和 GID 到非特权用户和组</p> <p>2、检测操作</p> <p>以root身份执行：</p> <pre># ps -ef grep -i weblogic</pre> <p>以WebLogic管理员身份登录管理控制台,执行：</p> <ol style="list-style-type: none"> 1. 在左面板，点击”Machine”文件夹 2. 在右面板，查看是否配置”Unix Machine link”

编号 4:

要求内容	开启主机名认证，设置 Hostname Verification 值为”Bea Hostname Verifier”
参考操作	<p>设置Hostname Verification值为”Bea Hostname Verifier”</p> <p>以管理员身份登录管理控制台：</p> <ol style="list-style-type: none"> 1. 点击左面板域名文件夹，然后点击“servers”文件夹，点击要管理的

	<p>服务器名</p> <p>2. 在右侧面板的”configuration”面板下的”Keystore &SSL”标签中, 点击Advanced option中 “Show”项, 查看Client attribute下的Hostname Verification 值, 设置为”Bea Hostname Verifier”</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>以管理员身份登录管理控制台:</p> <p>1. 点击左面板域名文件夹, 然后点击“servers”文件夹, 点击要管理的服务器名</p> <p>2. 在右侧面板的”configuration”面板下的”Keystore &SSL”标签中, 点击Advanced option中 “Show”项, 查看Client attribute下的Hostname Verification 值</p>

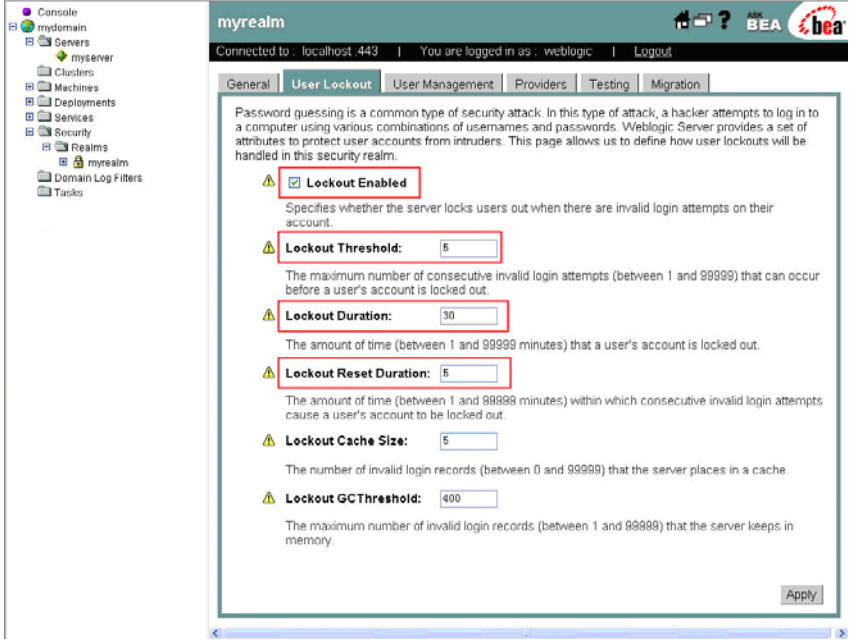
4.2 口令

编号: 1

要求内容	对于采用静态口令认证技术的设备, 口令长度至少 8 位, 并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类
操作指南	<p>以管理员身份登录控制台</p> <p>1. 点击左侧面板”Security”文件夹, 展开”REALM”</p> <p>2. 点击”Users”文件夹, 设置口令长度至少 8 位, 并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类</p> <p>检查 WebLogic 安装目录下的 weblogic.properties 配置文件中参数 weblogic.system.minPasswordLen=8</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p>

编号: 2

要求内容	对于采用静态口令认证技术的设备, 应配置当用户连续认证失败次数超过 6 次 (不含 6 次), 锁定该用户使用的账号
操作指南	<p>1、参考配置操作</p> <p>设定帐号锁定次数和时间</p> <p>以管理员身份登录控制台</p> <p>1. 点击左侧面板”Security”文件夹, 展开”REALM”</p> <p>2. 点击右侧面板中的”User Lock”标签, 设定 Lockout Enabled, Lockout</p>

	<p>Threshold 值为 5，Lockout Duration 为 30（分钟）</p> 
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>以管理员身份登录控制台</p> <p>1. 点击左侧面板”Security”文件夹，展开”REALM”</p> <p>2. 点击右侧面板中的”User Lock”标签，查看锁定阈值，锁定持续时间，锁定重置持续时间</p>

4.3 日志

编号 1:

要求内容	开启日志功能
参考操作	<p>以管理员身份登录管理控制台</p> <p>1. 点击域名，在右侧面板选择“Configuration”标签</p> <p>2. 选择logging标签，设置域级日志，勾选如下图红色标记部分</p>

Console

mydomain

Servers

Clusters

Machines

Deployments

Services

Security

Realms

myrealm

Users

Groups

Global Roles

myrealm

Users

Groups

Global Roles

myrealm

Users

Groups

Global Roles

myrealm

Users

Groups

Global Roles

myrealm

Users

Groups

Global Roles

Providers

Adjudication

Auditing

Authentication

Authorization

Credential Mapping

Keystores (Deprecated)

Role Mapping

Domain Log Filters

Tasks

Configuration

Monitoring

Control

Notes

General

JTA

SNMP

Logging

A domain is the basic administration unit for WebLogic Server instances (servers) that is represented in its own configuration file (config.xml). A domain consists of one or more servers (and their associated resources) that you manage with a single Administration Server. (The Administration Server is the server that runs this Administration Console.) This page allows you to define the general configuration of this WebLogic Server domain.

Name: mydomain
The name of this WebLogic Server domain.

☐ **Enable Administration Port**
Specifies whether the administration port should be enabled for this WebLogic Server domain. Because the administration port uses SSL, checking this box means that SSL must be configured. (SSL is located under each server's Keystores & SSL tab). This field requires a restart of all WebLogic Server instances in the domain.

Administration Port: 8002
The common secure administration port for this WebLogic Server domain, which Managed Servers use to communicate with the Administration Server. (This field is relevant only if you check the Enable Administration Port box.)

☒ **Production Mode**
Specifies whether the servers in this WebLogic Server domain run in production mode. This impacts subsystem features, such as the Application Pooler, and influences default field values.

☒ **Configuration Auditing:** logaudit
Specifies whether the Administration Server generates Audit Events and/or log messages when a user changes or invokes management operations on domain resources.

☐ **Enable Cluster Constraints**
Specifies if any cluster that may be a target of a deployment needs to have all its servers be running for the deployment to succeed.

Advanced Options [Show] [Apply]

[View domain log](#) [View Domain-wide Security Settings](#)

Console

mydomain

Servers

Clusters

Machines

Deployments

Services

Security

Domain Log Filters

Tasks

mydomain

Connected to : localhost:7001 | You are logged in as : weblogic | Logout

Configuration

Monitoring

Control

Notes

General

JTA

SNMP

Logging

Because each WebLogic Server domain can run concurrent, multiple instances of WebLogic Server, WebLogic logging services collect messages that are generated on multiple server instances into a single, domain-wide message log. You can use this domain-wide message log to see the overall status of the domain. This page allows you to define the configuration of the message log for this WebLogic Server domain.

☐ **Domain File Name:** .\mydomain.log
The name of the file that stores this WebLogic Server domain log's current log messages. If the pathname is not absolute, the path is assumed to be relative to the root directory of the machine on which the Administration Server is running.

Rotation Type: By Time
The criteria for moving old log messages to a separate file.

Minimum File Size: 5000 k
The size (between 1 and 85535 kilobytes) that triggers the Administration Server to move log messages to a separate file. After the log file reaches the specified minimum size, the next time the Administration Server checks the file size, it will rename the current domain log file and create a new one to store subsequent messages. (This field is relevant only if you set Rotation Type to By Size.)

Rotation Time: 00:00
The start time for a time-based rotation sequence of the log file, in the format k:m, where k is 1-24. (This field is only relevant if you set Rotation Type to By Time.)

File Time Span: 24 hours
The interval (between 1 and 24 hours) at which this WebLogic Server domain saves old log messages to another file.

☒ **Limit Number of Retained Log Files**
Specifies whether the number of files that this WebLogic Server domain creates to store old messages should be limited. After the limit is reached, the oldest file will be overwritten.

Log Files To Retain: 30
The maximum number of log files that this WebLogic Server domain creates when it rotates the log. (This field is relevant only if you check the Limit Number of Retained Log Files box.)

[Apply]

[View domain log](#) [View Domain-wide Security Settings](#)

3. 点击域名下 servers 下的服务器名，在右侧面板选择“Logging”标签，选择 Domain，勾选“Log to Domain Log file”
4. 同上，点击 Server 标签，配置服务器级日志，勾选“Log to stdout”等，如下红色标记项

mydomain> Servers> myserver

Connected to: localhost:7001 | You are logged in as: weblogic | Logout

Configuration | Protocols | **Logging** | Monitoring | Control | Deployments | Services | Notes

Server | Domain | HTTP | JDBC | JTA

This page allows you to define the general logging settings for this server.

Server File Name:

The name of the file that stores this server's current log messages. If the pathname is not absolute, the path is assumed to be relative to the root directory of the machine on which this server is running.

☒ **Log to Stdout**

Specifies whether the server should send messages to standard out (in addition to the log file).

☐ **Debug to Stdout**

Specifies whether this server sends messages of Debug severity to standard out, in addition to sending them to the log file. (This field is relevant only if you check the Log to Stdout box.)

Stdout Severity Threshold:

The minimum severity of a message this server sends to standard out. (This field is relevant only if you check the Log to Stdout box.)

Rotation Type:

The criteria for moving old log messages to a separate file.

Minimum File Size: k

The size (1 - 85535 kilobytes) that triggers this server to move log messages to a separate file. (This field is relevant only if you set Rotation Type to By Size.)

Rotation Time:

The start time for a time-based rotation sequence of the log file, in the format k:aa, where k is 1-24. (This field is only relevant if you set Rotation Type to By Time.)

File Time Span: hours

The interval (in hours) at which old log messages are saved to another file. (This field is relevant only if you set Rotation Type to By Time.)

☒ **Limit Number of Retained Log Files**

Specifies whether the number of files that this WebLogic Server creates to store old messages should be limited. After the server reaches this limit, it overwrites the oldest file.

Log Files To Retain:

The maximum number of log files that this WebLogic Server creates when it rotates the log. (This field is relevant only if you check the Limit Number of Retained Log Files box.)

☒ **Instrument Stack Traces**

Specifies whether this server returns stack traces for RMI calls that generate exceptions.

Apply

[View server log](#) [View JNDI tree](#)

5. 同上，点击“HTTP”标签，按如下红色标记部分进行配置

mydomain> Servers> myserver

Connected to: localhost:7001 | You are logged in as: weblogic | Logout

Configuration | Protocols | **Logging** | Monitoring | Control | Deployments | Services | Notes

Server | Domain | **HTTP** | JDBC | JTA

This page allows you to define the HTTP logging settings for this server.

☒ **Enable HTTP Logging**

Specifies whether this server logs HTTP requests. (The remaining fields on this page are relevant only if you check this box.)

HTTP Log File Name:

The name of the file that stores HTTP requests. If the pathname is not absolute, the path is assumed to be relative to the root directory of the machine on which this server is running.

Format:

The format of the HTTP log file. Both formats are defined by the W3C. With the extended log format, you use server directives in the log file to customize the information that the server records.

Log Buffer Size: k

The maximum size (between 0 and 1024 kilobytes) of the buffer that stores HTTP requests.

Rotation Type:

The criteria for moving old log messages to a separate file.

Maximum Log File Size: k

The maximum size (in kilobytes) of the HTTP log file. After the log file reaches this size, the server renames it as LogFileN.n. A value of 0 indicates that the log file can grow indefinitely. (This field is relevant only if you set Rotation Type to size.)

Rotation Period: minutes

The number of minutes (between 1 and a positive 32-bit integer) at which this server saves old HTTP requests to another log file. This field is relevant only if you set Rotation Type to date.

Rotation Time:

The start time for a time-based rotation sequence of the log file, in the format MM-dd-yyyy-k:mm:ss, where k is 1-24. (This field is only relevant if you set Rotation Type to date.)

☒ **Limit Number of Retained Log Files**

Specifies whether the number of files that this WebLogic Server retains to store old messages should be limited. After the server reaches this limit, it overwrites the oldest file.

Log Files To Retain:

The maximum number of log files that this server retains when it rotates the log. (This field is relevant only if you check the Limit Number of Retained Log Files box.)

Flush Every: seconds

The interval (between 1 and 360 seconds) at which this server checks the size of the buffer that stores HTTP requests. When the buffer exceeds the size that is specified in the Log Buffer Size field, the server writes the data to the HTTP request log file.

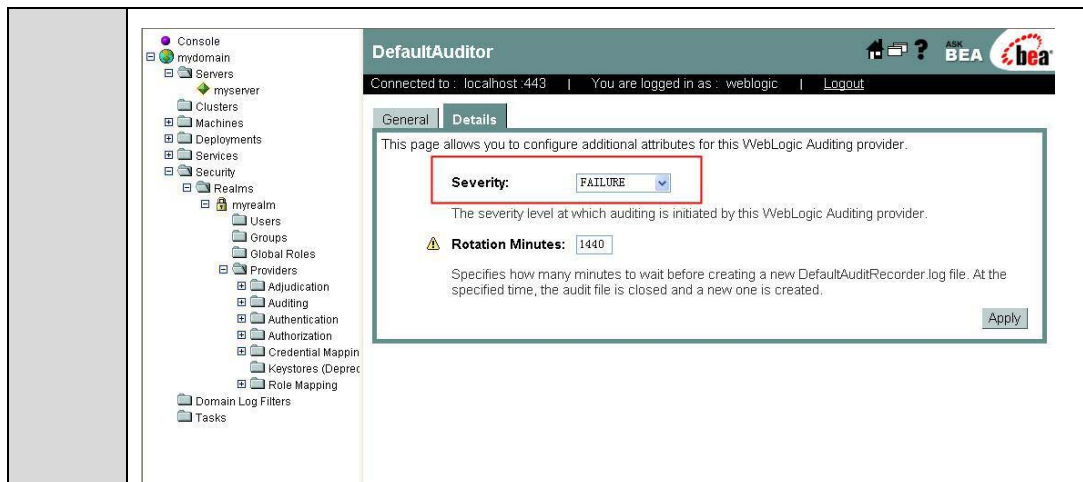
Apply

[View server log](#) [View JNDI tree](#)

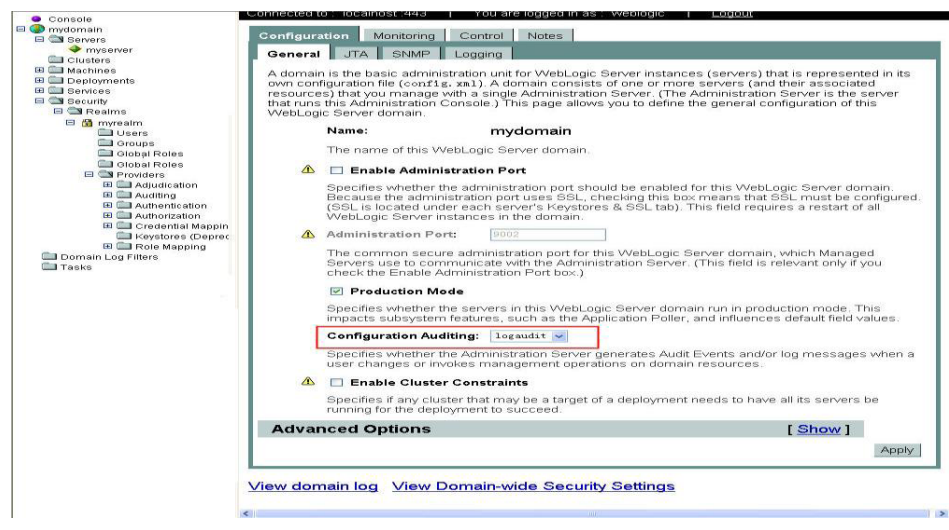
检测方法	1、判定条件 开启日志功能
------	-----------------------------

编号 2:

要求内容	配置日志审计
参考操作	<p>以管理员身份登录控制台</p> <ol style="list-style-type: none"> 1. 点击左侧面板Security文件夹,展开provider,然后点击Auditing文件夹 2. 查看是否配置Auditor, 如无则选择”Configure a new Default Auditor”并设置审计级另为FAILURE. 3. 点击左侧面板中域名下的服务器, 在右侧面板“General”标签中设置 Configuration Auditing为logAudit
检测方法	<p>1、判定条件</p> <p>配置了审计, 设置审计级另为 FAILURE, Configuration Auditing 为 logAudit</p> <p>2、检测操作</p> <p>以管理员身份登录控制台</p> <ol style="list-style-type: none"> 1. 点击左侧面板 Security 文件夹,展开 provider,然后点击 Auditing 文件夹 2. 查看是否配置 Auditor, 对照如下图的红色标记部分配置 



3. 点击左侧面板中域名下的服务器，对照如下图的红色标记部分配置

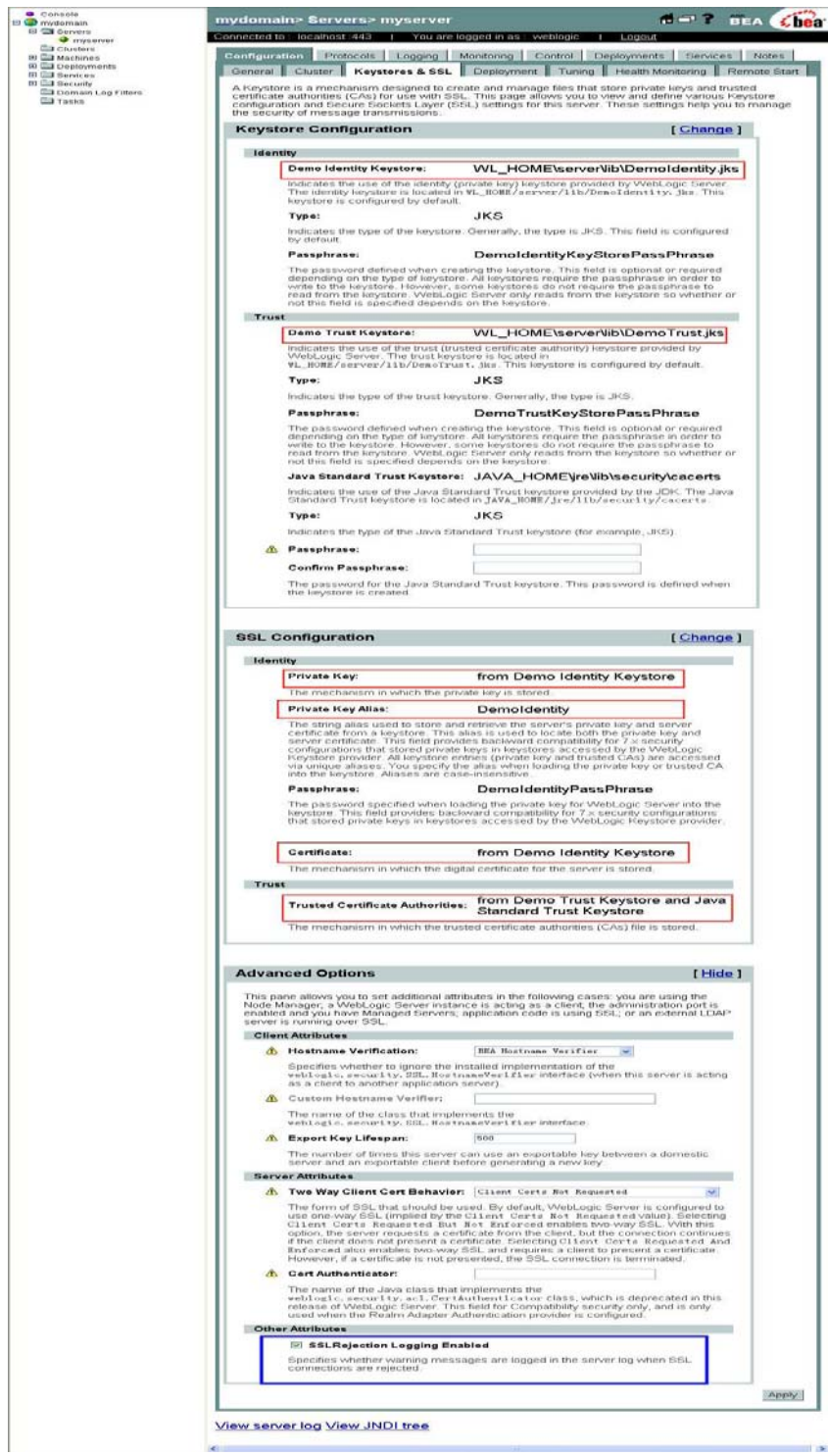


4.4 Keystore 和 SSL 设置

编号 1:

要求内容	合理设置 WebLogic Keystore 和 SSL
操作指南	<p>创建用户自己的私有密钥和数字证书</p> <p>以管理员身份登录管理控制台：</p> <ol style="list-style-type: none"> 1. 点击左面板域名文件夹，然后点击“servers”文件夹，点击要管理的服务器名 2. 在右侧面板的”configuration”面板下的”Keystore &SSL”标签中，点击Keystore configuration中 “Change”项，改变默认私有密钥设置 3. 同上点击SSL configuration中 “Change”项，改变默认私有密钥设置 4. 同上点击”Advanced option”中”Show”项，勾选” SSLRejection Logging Enabled”
检测方法	<p>以管理员身份登录管理控制台：</p> <ol style="list-style-type: none"> 1. 点击左面板域名文件夹，然后点击“servers”文件夹，点击要管理的服务器名

2. 在右侧面板的“configuration”面板下的“Keystore & SSL”标签中查看
如下图相应红色标记部分和蓝色标记部分



4.5 Sockets 最大打开数量

编号 1:

要求内容	合理设置应用服务器 Sockets 最大打开数量
操作指南	1、参考配置操作：

	以管理员身份登录管理控制台 1. 点击左侧面板的域名文件夹，然后点击Servers文件夹，双击要管理的服务器 2. 在右侧面板的“Configuration”面板下选择“Tuning”标签 3. 设置“Maximum Open Sockets”为 254 或其它用户设定值 备注：此项操作需开发人员在测试机修改后测试，应用正常然后再在生产机器上修改
检测方法	以管理员身份登录管理控制台 1. 点击左侧面板的域名文件夹，然后点击Servers文件夹，双击要管理的服务器 2. 在右侧面板的“Configuration”面板下选择“Tuning”标签，查看Maximum Open Sockets 值

4.6 文件和目录权限

编号：1

要求内容	合理设置文件与目录权限，没有不必要的权限，也不存在不必要的文件
参考操作	对启动和环境脚本限制权限为710，确认BEA_HOME属主为weblogic用户，对不必要的工具文件设置权限为700并改后缀名为.predeleted 以root 身份执行以下操作： # chown -R “weblogicuser” \$BEA_HOME # find \$BEA_HOME/ -name *.sh xargs `chmod 710` #检查不必要工具文件，并将限制权限为 700 # tar cvf beahome.`date '+%y%m%d'`.tar \$BEA_HOME # find \$WL_HOME/ -name config_builder.sh xargs `chmod 700` # find \$WL_HOME/ -name startWLBuilder.sh xargs `chmod 700` # find \$WL_HOME/ -name jcommon-0.7.0.jar xargs `chmod 700` # find \$WL_HOME/ -name PointBase xargs `chmod 700` # find \$WL_HOME/ -name medrec xargs `chmod 700` #检查不必要工具文件，并改名为.predeleted #mv config_builder.sh config_builder.sh.predeleted #mv startWLBuilder.sh startWLBuilder.sh.predeleted #mv jcommon-0.7.0.jar jcommon-0.7.0.jar.predeleted #mv PointBase PointBase.predeleted #mv medrec medrec .predeleted
检测方法	以root 身份执行以下操作： # ls -alR \$BEA_HOME # find \$BEA_HOME/ -name *.sh xargs `ls -al`

	<pre>#查找不必要的工具文件 #find \$BEA_HOME/ -name config_builder.sh xargs `ls -al` #find \$BEA_HOME/ -name startWLBuilder.sh xargs `ls -al` #find \$BEA_HOME/ -name jcommon-0.7.0.jar xargs `ls -al` #find \$WL_HOME/ -name PointBase xargs `ls -al` #find \$WL_HOME/ -name medrec xargs `ls -al`</pre>
--	---

4.7 WebLogic 运行模式

编号：1

要求内容	更改运行模式为”Production Mode”
参考操作	<p>以管理员身份登录管理控制台</p> <ol style="list-style-type: none"> 1. 点击域名，在右侧面板选中”Genaral”标签 2. 勾选” Production Mode”，更改运行模式为” Production Mode”
检测方法	<p>以root身份执行：</p> <ol style="list-style-type: none"> 1. <pre># find \$BEA_HOME/ -name myserver.log grep -i “Production Mode”</pre> <pre># find \$BEA_HOME/ -name setEnv.sh grep -i “Production Mode”</pre> 2. 以管理员身份登录管理控制台,点击域名，在右侧面板选中”Genaral”标签,查看是否勾选” Production Mode”

4.8 Sender Server Header

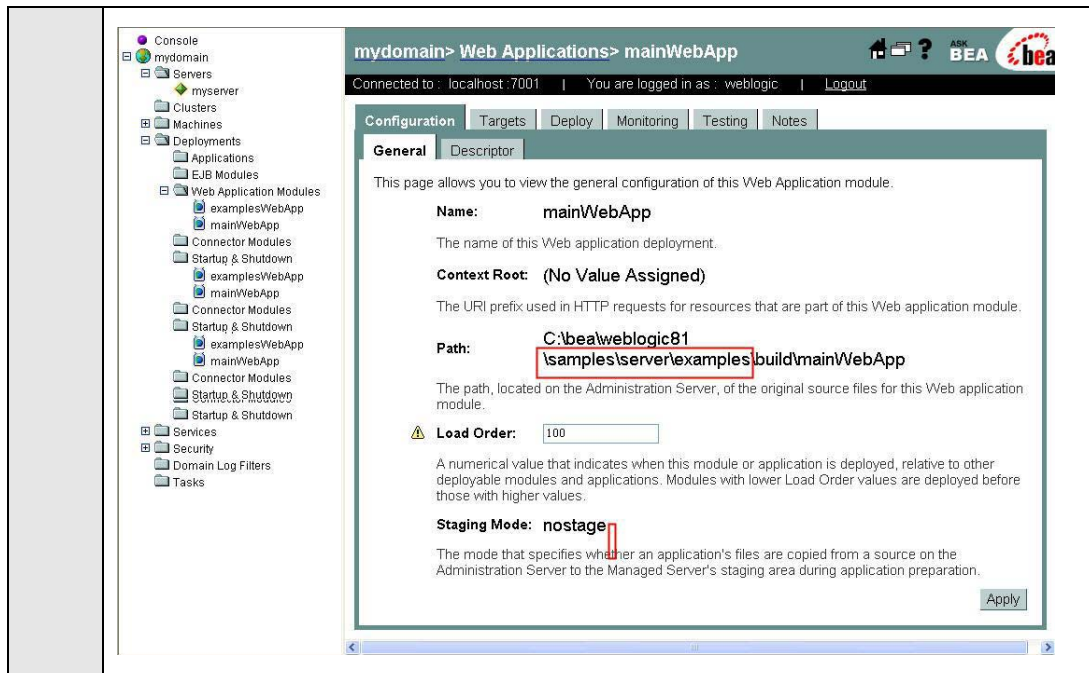
编号：1

要求内容	禁用 Send Server header
参考操作	<p>以管理员身份登录管理控制台</p> <ol style="list-style-type: none"> 1. 点击域名下的Servers文件夹，选择要管理的服务器 2. 在右侧面板”Protocols”面板下，点击HTTP标签 3. 去掉 Send Server header 项前面的勾,禁止 Send Server header
检测方法	<p>以管理员身份登录管理控制台</p> <ol style="list-style-type: none"> 1. 点击域名下的Servers文件夹，选择要管理的服务器 2. 在右侧面板”Protocols”面板下，点击HTTP标签 3. 检查是否勾选 Send Server header

4.9 删除 Sample 程序

编号: 1

要求内容	删除 sample 程序												
参考操作	<p>以管理员身份登录管理控制台</p> <p>1. 点击”Deployment”文件夹，查看是否有如下形式应用存在：</p> <div><p>Current Deployments</p><p>The deployment order of these applications or modules is determined by their Load Order. Click the Change button next to a displayed module to change it's deployment order.</p><table><tr><th>Load Order</th><th>Name</th><th>Deployment Type</th><th></th></tr><tr><td>100</td><td>examplesWebApp</td><td>Web Application</td><td>Change</td></tr><tr><td>100</td><td>mainWebApp</td><td>Web Application</td><td>Change</td></tr></table></div> <p>2. <code>#find \$BEA_HOME/ -name sample xargs `rm -rf`</code></p>	Load Order	Name	Deployment Type		100	examplesWebApp	Web Application	Change	100	mainWebApp	Web Application	Change
Load Order	Name	Deployment Type											
100	examplesWebApp	Web Application	Change										
100	mainWebApp	Web Application	Change										
检测方法	<p>1. 以root权限执行</p> <p><code>#find \$BEA_HOME/ -name sample -print</code></p> <p>2. 以管理员身份登录管理控制台</p> <p>a) 点击”Deployment”文件夹，查看是否有如下形式应用存在：</p> <div><p>Current Deployments</p><p>The deployment order of these applications or modules is determined by their Load Order. Click the Change button next to a displayed module to change it's deployment order.</p><table><tr><th>Load Order</th><th>Name</th><th>Deployment Type</th><th></th></tr><tr><td>100</td><td>examplesWebApp</td><td>Web Application</td><td>Change</td></tr><tr><td>100</td><td>mainWebApp</td><td>Web Application</td><td>Change</td></tr></table></div> <p>b) 展开”Deployment”子文件夹，查看是否存在以上形式内容，其path中包含“samples“目录，如下图</p>	Load Order	Name	Deployment Type		100	examplesWebApp	Web Application	Change	100	mainWebApp	Web Application	Change
Load Order	Name	Deployment Type											
100	examplesWebApp	Web Application	Change										
100	mainWebApp	Web Application	Change										



4.10 设定默认出错页面

编号: 1

要求内容	重新在应用程序 web.xml 中定义默认出错页面
参考操作	编辑<Application HOME>/WEB-INF/web.xml，加入 error-page 定义
检测方法	<p>1、判断依据：</p> <pre><error-page>␣ <exception-type>*/</exception-type>␣ <location>error.html</location>␣ </error-page>␣</pre> <p>2、检查操作： 以root身份执行：</p> <pre># cat <Application HOME>/WEB-INF/web.xml</pre>

4.11 session 超时时间

编号: 1

要求内容	根据具体应用，合理设置 session 超时时间
参考操作	在应用程序的 web.xml 中定义 session 超时时间，例如，以下设置表示 session 超时时间为 15 分钟

	<pre><session-config> <session-timeout>15</session-timeout> </session-config></pre>
检测方法	检查是否在应用程序的 web.xml 中定义了 session 超时时间

4.12 补丁

编号：1

要求内容	在不影响业务的情况下，升级到最新补丁，而且该补丁要通过实验测试
参考操作	<p>安装最新安全相关补丁包，安全补丁下载需要 BEA 公司授权，WebLogic 安全公告 URL：</p> <p>http://dev2dev.bea.com/advisoriesnotifications/</p>
检测方法	<p>1. 以管理员身份登录管理控制台，右键点击左侧面板 ConWLe 图标，选择“View Server & Browser Info”，查看版本号</p> <p>2. 以 root 身份执行：</p> <pre># cat \$BEA_HOME/logs/log.txt</pre>

4.13 HTTP 加密协议

要求内容	对于通过 HTTP 协议进行远程维护的设备，设备应支持使用 HTTPS 等加密协议。
操作指南	<p>1、参考配置操作</p> <p>以管理员身份登录管理控制台：</p> <ol style="list-style-type: none"> 1. 点击左面板域名文件夹，然后点击“servers”文件夹，点击要管理的服务器名 2. 在右侧面板的“configuration”面板下的“Keystore & SSL”标签中，启用 ssl configure
检测方法	<p>1、判定条件</p> <p>2、检测操作</p>

4.14 连接数设置

要求内容	根据机器性能和业务需求，设置最大最小连接数。
操作指南	1、参考配置操作

	<p>以管理员身份登录管理控制台</p> <ol style="list-style-type: none"> 1. 点击左侧面板的域名文件夹，然后点击Servers文件夹，双击要管理的服务器 2. 在右侧面板的“Configuration”面板下选择“Tuning”标签 3. 设置” Maximum Open Sockets”为 254 或其它用户设定值 <p>2、补充操作说明</p>
检测方法	<p>1、判定条件</p> <p>2、检测操作</p> <p>检查当前的连接数</p>

拟文部门：网络运行维护事业部

会签部门：网络发展部、企业信息化部。

中国电信集团公司综合部

2011年6月14日印发
