QB/CU

中国联通公司企标准

QB/CU 008-2024

|  |
| --- |
|  |

中国联通CentOS安全加固

技术规范

|  |
| --- |
| （V1.0） |
|  |

2024-03-22发布

2024-03-22实施

中国联通公司   发布

**目 次**

[前 言 - 2 -](#_Toc1260)

[1 范围 - 1 -](#_Toc2542)

[2 引用标准 - 1 -](#_Toc1675)

[3 缩略语 - 1 -](#_Toc6776)

[4 安全加固要求 - 2 -](#_Toc31570)

[4.1 身份鉴别 - 2 -](#_Toc5398)

[4.1.1　所有用户密码不应为空 - 2 -](#_Toc7230)

[4.1.2　应确保root是唯一的UID为0的帐户 - 2 -](#_Toc11543)

[4.1.3　应设置高复杂度密码 - 2 -](#_Toc23692)

[4.1.4　应设置密码失效时间 - 3 -](#_Toc26977)

[4.1.5　应限制密码重用 - 3 -](#_Toc28085)

[4.1.6　密码到期应提前警告 - 3 -](#_Toc10992)

[4.1.7　应禁止wheel组之外的用户以root身份登录 - 3 -](#_Toc29835)

[4.1.8 宜设置用户密码尝试失败锁定 - 4 -](#_Toc13322)

[4.1.9 宜设置密码修改最小间隔时间 - 4 -](#_Toc9)

[4.2　访问控制 - 4 -](#_Toc7750)

[4.2.1 应禁止root用户登录FTP - 4 -](#_Toc6097)

[4.2.2　应禁止匿名用户登录FTP - 5 -](#_Toc23963)

[4.2.3　应控制用户FTP上传文件权限 - 5 -](#_Toc10094)

[4.2.4　宜限制控制配置文件访问权限 - 5 -](#_Toc8462)

[4.2.5 宜限制日志文件访问权限 - 5 -](#_Toc29909)

[4.2.6　宜删除潜在危险文件 - 6 -](#_Toc9661)

[4.2.7　宜限制用户sudo权限 - 6 -](#_Toc952)

[4.2.8　宜防止SUID/SGID权限的恶意使用 - 6 -](#_Toc30555)

[4.3　SSH服务配置 - 6 -](#_Toc5289)

[4.3.1　应将SSH LogLevel设置为INFO - 6 -](#_Toc12623)

[4.3.2　应设置SSH空闲超时退出时间 - 6 -](#_Toc9759)

[4.3.3　应设置每个连接允许的验证最大尝试数量 - 7 -](#_Toc11802)

[4.3.4　SSH身份验证应强制输入密码 - 7 -](#_Toc20186)

[4.3.5　应关闭主机认证 - 7 -](#_Toc16053)

[4.3.6　应禁止SSH空密码用户登录 - 7 -](#_Toc17471)

[4.3.7　应禁用Telnet协议 - 7 -](#_Toc4607)

[4.3.8　应禁止root用户远程登录 - 8 -](#_Toc13464)

[4.3.9　宜关闭x11转发功能 - 8 -](#_Toc29811)

[4.4　安全审计 - 8 -](#_Toc7267)

[4.4.１ 应启用rsyslog服务 - 8 -](#_Toc4799)

[4.4.2 应记录登录日志 - 8 -](#_Toc14102)

[4.4.3　应保护审计记录 - 8 -](#_Toc32250)

[4.4.4 宜记录cron行为日志 - 9 -](#_Toc28418)

[4.5　入侵防范 - 9 -](#_Toc26240)

[4.5.1　宜开启地址空间布局随机化 - 9 -](#_Toc3380)

[4.5.2 宜进行软件更新 - 9 -](#_Toc27329)

1. 前 言

为保障应用系统安全稳定运行，本标准主要对使用了CentOS操作系统的服务器主机和应用系统提出安全加固技术规范，从服务器主机和应用系统的身份鉴别、访问控制、SSH服务配置、安全审计、入侵防范等方面提出要求，并给出了参考的实现方式。

本规范主要用于中国联通现网使用CentOS 操作系统的服务器主机和应用系统的安全维护，以降低网络安全风险。

本标准由中国联通网络与信息安全部提出。

本标准由中国联通公司科技创新部归口。

本标准主要起草单位：中国联通网络与信息安全部、中国联通研究院、中国联通软件研究院。

本标准主要起草人：苗守野、李浩宇、孙艺、吴连勇、王奉军、刘雨涵、文仕奇、朱晓雨、徐勇、吴章、金涛、周映、李磊。

本标准的修改和解释权属中国联通公司。

中国联通CentOS安全加固技术规范V1.0

# 范围

本标准规定了使用CentOS操作系统的服务器主机和应用系统的安全加固技术要求，包括身份鉴别、访问控制、SSH服务配置、安全审计、入侵防范等。

本标准适用于中国联通的使用CentOS操作系统的服务器主机，含物理机和虚拟机。

本标准若与国家、行业相关强制性标准、规范有矛盾时，应按国家和行业相关规定执行。

# 引用标准

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是标注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不标注日期的引用文件，其最新版本适用于本标准。

|  |  |
| --- | --- |
| [GB/T 20272-2019](javascript:void(0)) | [信息安全技术 操作系统安全技术要求](javascript:void(0)) |
| GB 17895-1999 | 计算机信息系统 安全保护等级划分准则 |
| GB/T 20271-2006 | 信息安全技术 信息系统通用安全技术要求 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 缩略语

|  |  |  |
| --- | --- | --- |
| CentOS | Community Enterprise Operating System | 社区企业操作系统 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 安全加固要求

本章描述CentOS安全加固要求，每项加固要求分为“加固要求”和“参考方法”两部分：

**“加固要求”**描述对CentOS操作系统加固的具体要求，其中以“应”、“不应”描述的加固要求为强制性要求，以“宜”、“不宜”描述的加固要求为建议要求。

**“参考方法”**描述此加固要求的参考实现方式，不同操作系统版本可能有所区别，此处内容仅供参考。

所有操作应做好记录或备份，下文不再提示。

## 4.1 身份鉴别

4.1.1　所有用户密码不应为空

**加固要求：**

所有登录用户密码不应为空，应为允许登录用户设置非空密码。

**参考方法**：

执行以下命令查看系统中是否存在空口令账号 #/bin/cat /etc/shadow | /bin/awk -F: '($2 == "" ) { print "user " $1 " does not have a password "}' 合规标准 不存在空口令的账号则合规，否则不合规。

为不合规用户设置满足密码复杂度的密码。

4.1.2　应确保root是唯一的UID为0的帐户

**加固要求：**

应确保root是唯一的UID为0的帐户。

**参考方法：**

除root以外其他UID为0的用户(查看命令cat /etc/passwd | awk -F: '($3 == 0) { print $1 }'|grep -v '^root$' )都应删除，或者为其分配新的UID。

4.1.3　应设置高复杂度密码

**加固要求：**

密码最小长度应不小于8，至少包含1位数字、大写字母、特殊字符、小写字母。

**参考方法：**

1. 配置文件备份 #cp /etc/pam.d/system-auth /etc/pam.d/system-auth.bak
2. 编辑配置文件/etc/pam.d/system-auth，在文件中找到开头为如下字样的内容： password requisite pam\_cracklib.so 将其修改为： password requisite pam\_cracklib.so try\_first\_pass minlen=8 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 #口令长度不小于8，至少包含1位数字、大写字母、特殊字符、小写字母。

4.1.4　应设置密码失效时间

**加固要求：**

设置密码失效时间，应定期修改密码，建议设置为90，减少密码被泄漏和猜测风险，使用非密码登陆方式(如密钥对)请忽略此项（下同）。

**参考方法：**

在/etc/login.defs 中将 PASS\_MAX\_DAYS 参数设置为 60-180之间，如:PASS\_MAX\_DAYS 90

需同时执行命令设置root密码失效时间：chage --maxdays 90 root。

4.1.5　应限制密码重用

**加固要求：**

应要求用户不重复使用最近使用过的密码，降低密码猜测攻击风险。

**参考方法：**

在/etc/pam.d/password-auth和/etc/pam.d/system-auth中，password sufficient pam\_unix.so行末尾配置参数remember为5-24之间。

4.1.6　密码到期应提前警告

**加固要求：**

应设置用户密码到期提前提醒天数为7天或更多。

**参考方法：**

使用vi /etc/login.defs修改配置文件，参数PASS\_WARN\_AGE 设置为7或更多。 执行命令 chage --warndays 7 root，使设置生效。

4.1.7　应禁止wheel组之外的用户以root身份登录

**加固要求：**

应禁止wheel组之外的用户以root身份登录。

**参考方法：**

检查步骤：

执行命令cat /etc/pam.d/su，查看文件中是否存在如下配置：

auth sufficient pam\_rootok.so

auth required pam\_wheel.so group=wheel

只允许wheel组的用户才能su为root则合规，否则不合规。

加固方法：

编辑文件/etc/pam.d/su

在文件开头加入如下两行(有则修改,没有则添加):

auth sufficient pam\_rootok.so

auth required pam\_wheel.so group=wheel

#注意auth与sufficient之间由两个tab建隔开，sufficient与动态库路径之间使用一个tab建隔开

说明：(这表明只有wheel组中的用户可以使用su命令成为root用户。可以把用户添加到wheel组，以使它可以使用su命令成为root用户。)

添加方法:

#usermod -G wheel username #username为需要添加至wheel组的账户名称。

4.1.8 宜设置用户密码尝试失败锁定

**加固要求：**

宜设置用户密码尝试多次失败后锁定，失败次数建议设置为5，锁定时间建议设置为900秒。

**参考方法：**

编辑/etc/pam.d/sshd中修改auth required pam\_tally2.so deny=5 unlock\_time=900。

4.1.9 宜设置密码修改最小间隔时间

**加固要求：**

设置密码修改最小时间间隔，应限制频繁进行密码更改。

**参考方法：**

在/etc/login.defs 中将参数PASS\_MIN\_DAYS设置为7-14之间，建议设置为7。

## 4.2**访问控制**

根据用户业务需要，配置其所需的最小权限。

4.2.1 应禁止root用户登录FTP

**加固要求：**

应禁止root用户登录FTP。

**参考方法：**

修改ftpusers文件，增加不能通过FTP登录的用户 1)、首先需确定ftpusers文件位置，可以通过以下命令知道 #cat /etc/pam.d/vsftpd auth required pam\_listfile.so item=user sense=deny file=/etc/vsftpd.ftpusers onerr=succeed #其中file=/etc/vsftpd/ftpusers即为当前系统上的ftpusers文件. 2)、修改file对应的文件在文件中增加用户，则该用户均不允许通过FTP登录(每个用户占一行)

重启FTP服务。

4.2.2　应禁止匿名用户登录FTP

**加固要求：**

应禁止匿名用户登录FTP。

**参考方法：**

编辑文件/etc/vsftpd/vsftpd.conf,修改参数anonymous\_enable的值为NO：

anonymous\_enable=NO。

重启FTP服务。

4.2.3　应控制用户FTP上传文件权限

**加固要求：**

应设置用户FTP上传文件权限为022。

**参考方法：**

编辑文件:/etc/vsftpd/vsftpd.conf，对如下两个参数的值进行修改，如果参数不存在则手工添加。

local\_umask=022 #设置用户上传文件的权限

anon\_umask=022 #设置匿名用户上传文件的权限

重启ftp服务。

4.2.4　宜限制控制配置文件访问权限

**加固要求：**

宜限制访问控制配置文件的权限。

**参考方法：**

赋予访问控制配置文件最小权限 ：

chmod 644 /etc/passwd

chmod 400 /etc/shadow

chmod 644 /etc/group

4.2.5 宜限制日志文件访问权限

**加固要求：**

设备应配置权限控制对日志文件的读取、修改和删除等操作。

**参考方法：**

备份需要修改权限的日志文件

设置文件权限

chmod 600 /var/log/messages

chmod 644 /var/log/dmesg

chmod 600 /var/log/maillog

chmod 600 /var/log/secure

chmod 664 /var/log/wtmp

chmod 600 /var/log/cron

4.2.6　宜删除潜在危险文件

**加固要求：**

.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。

**参考方法：**

使用locate命令查看系统是否存在如下文件".rhost、.netrc、hosts.equiv" #locate .rhost #locate .netrc #locate hosts.equiv

系统不存在".rhost、.netrc、hosts.equiv"这三个文件则合规,否则不合规。如不合规，使用rm命令删除如下三个文件: .rhost、.netrc、hosts.equiv。

4.2.7　宜限制用户sudo权限

**加固要求：**

赋予用户sudo权限时要谨慎，可满足业务需求即可，不应赋予过高权限，如不应赋予修改其他用户密码、kill其他用户进程、用户自身提权等权限，在此不一一列举。

4.2.8　宜防止SUID/SGID权限的恶意使用

**加固要求：**

宜禁止root用户之外的普通用户设置SUID和SGID权限，宜定期检查系统中的拥有SUID和SGID特殊权限的文件，查找未授权的SUID/SGID权限文件并及时修改或删除此类文件。

## 4.3　SSH服务配置

4.3.1　应将SSH LogLevel设置为INFO

**加固要求：**

应将SSH LogLevel设置为INFO，记录登录和注销信息。

**参考方法：**

编辑/etc/ssh/sshd\_config文件，取消参数LogLevel INFO的注释。

4.3.2　应设置SSH空闲超时退出时间

**加固要求：**

应设置SSH空闲超时退出时间，降低未授权用户访问其他用户SSH会话的风险。

**参考方法：**

编辑 /etc/ssh/sshd\_config，设置参数ClientAliveInterval为300到900（5-15分钟），设置参数ClientAliveCountMax为0-3之间。如：ClientAliveInterval 600，ClientAliveCountMax 2。

4.3.3　应设置每个连接允许的验证最大尝试数量

**加固要求：**

指定每个连接允许的身份验证尝试的最大数量。建议配置为4次或者更少。

**参考方法：**

编辑配置文件/etc/ssh/sshd\_config,将每个连接允许的身份验证尝试的最大数量 MaxAuthTries设置在3~6之间，建议设置为4。

4.3.4　SSH身份验证应强制输入密码

**加固要求：**

SSH进行身份验证时,应强制输入密码功能。

**加固方法：**

编辑文件/etc/ssh/sshd\_config，配置参数IgnoreRhosts为yes。

4.3.5　应关闭主机认证

**加固要求：**

应关闭主机认证功能。

**加固方法：**

编辑文件/etc/ssh/sshd\_config，配置参数HostbasedAuthentication为no。

4.3.6　应禁止SSH空密码用户登录

**加固要求：**

应禁止SSH空密码用户登录。

**加固方法：**

编辑文件/etc/ssh/sshd\_config，配置参数PermitEmptyPasswords为no。

4.3.7　应禁用Telnet协议

**加固要求：**

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，并禁止Telnet协议。

**参考方法：**

使用以下命令查看telnet和ssh服务状态： #chkconfig --list |grep "telnet|ssh" 判定条件 SSH服务启用，Telnet服务关闭则合规，否则不合规。

关闭Telnet服务： 1）、备份 #cp -p /etc/xinetd.d/telnet /etc/xinetd.d/telnet\_bak 2）、编辑文件/etc/xinetd.d/telnet，把disable项改为yes. 3）、重启xinetd服务。

开启SSH服务。

4.3.8　应禁止root用户远程登录

**加固要求：**

应禁止root用户远程登录。

**参考方法：**

编辑文件/etc/ssh/sshd\_config，修改PermitRootLogin值为no。

重启SSH服务。

4.3.9　宜关闭x11转发功能

**加固要求：**

如果没有需要使用此功能的应用应关闭该功能。

**参考方法：**

编辑配置文件/etc/ssh/sshd\_config,将X11Forwarding的值设置为no。

## 4.4　安全审计

4.4.１ 应启用rsyslog服务

**加固要求：**

应启用rsyslog服务，记录日志用于审计。

**参考方法：**

运行systemctl enable rsyslog，启用rsyslog服务。

查看/etc/rsyslog.conf配置文件，检查systemctl status rsyslog.service,状态应为Active：active（running）。

4.4.2 应记录登录日志

**加固要求：**

应记录登录日志。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。

**参考方法：**

编辑文件/etc/rsyslog.conf，增加如下配置(有则修改,无则添加)： authpriv.\* /var/log/secure或者authpriv.info /var/log/secure；

创建日志文件，并赋予其权限 #touch /var/log/secure #chmod 600 /var/log/secure；

重启syslog服务。

4.4.3　应保护审计记录

**加固要求：**

应保护审计记录，避免受到未预期的删除、修改或覆盖等。应使日志文件转储一个月，并保留6个月的信息，防止重要日志信息被覆盖。

**参考方法：**

查看/etc/rsyslog.conf文件中所配置对应的日志文件权限，应设置未特定用户只读权限-rw-------。使用more /etc/logrotate.conf|grep -v”^#\|^$”命令查看目前配置，并使用vi /etc/logrotate.conf命令修改参数rotate为6，并重启日志服务。

4.4.4 宜记录cron行为日志

**加固要求：**

宜启用记录cron行为日志功能。

**参考方法：**

编辑文件/etc/rsyslog.conf，增加如下配置(有则修改,无则添加)： cron.\* /var/log/cron；

创建日志文件，并赋予其权限 #touch /var/log/cron #chmod 600 /var/log/cron；

重启syslog服务。

## 4.5　入侵防范

4.5.1　宜开启地址空间布局随机化

**加固要求：**

宜通过将进程的内存空间地址随机化，增大入侵者预测目的地址的难度，降低进程被成功入侵的风险。

**参考方法：**

在/etc/sysctl.conf或/etc/sysctl.d/\*文件中，设置参数kernel.randomize\_va\_spcae = 2，并执行命令：sysctl-w kernel.randomize\_va\_space=2。

4.5.2 宜进行软件更新

**加固要求：**

宜检查是否已安装操作系统、OpenSSH、OpenSSL等的最新安全补丁或最新版本，尤其是对已知高危漏洞机型修复的关键更新，应及时安装，修补已知漏洞，消除安全威胁。安装前应做好兼容性测试。