

**Linux主机操作系统加固规范**

2021年5月23日

**目 录**

[第1章 概述 3](#_Toc73454408)

[1.1 适用范围 3](#_Toc73454409)

[1.2 适用版本 3](#_Toc73454410)

[第2章 账号管理、认证授权 4](#_Toc73454411)

[2.1 账号 4](#_Toc73454412)

[2.1.1 用户口令设置 4](#_Toc73454413)

[2.1.2 root用户远程登录限制 4](#_Toc73454414)

[2.1.3 检查是否存在除root之外UID为0的用户 5](#_Toc73454415)

[2.1.4 root用户环境变量的安全性 5](#_Toc73454416)

[2.1.5 远程连接的安全性配置 6](#_Toc73454417)

[2.1.6 用户的umask安全配置 6](#_Toc73454418)

[2.1.7 重要目录和文件的权限设置 6](#_Toc73454419)

[2.1.8 查找未授权的SUID/SGID文件 7](#_Toc73454420)

[2.1.9 检查任何人都有写权限的目录 8](#_Toc73454421)

[2.1.10 查找任何人都有写权限的文件 8](#_Toc73454422)

[2.1.11 检查没有属主的文件 9](#_Toc73454423)

[2.1.12 检查异常隐含文件 9](#_Toc73454424)

[第3章 日志审计 11](#_Toc73454425)

[3.1 日志 11](#_Toc73454426)

[3.1.1 syslog登录事件记录 11](#_Toc73454427)

[3.2 审计 11](#_Toc73454428)

[3.2.1 Syslog.conf的配置审核 11](#_Toc73454429)

[第4章 系统文件 13](#_Toc73454430)

[4.1 系统状态 13](#_Toc73454431)

[4.1.1 系统core dump状态 13](#_Toc73454432)

# 概述

## 适用范围

本配置标准的使用者包括：服务器系统管理员、应用管理员、网络安全管理员。

## 适用版本

LINUX系列服务器；

# 账号管理、认证授权

## 账号

### 用户口令设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux用户口令安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-01-01 |
| **安全基线项说明** | 帐号与口令-用户口令设置 |
| **检测操作步骤** | 1、询问管理员是否存在如下类似的简单用户密码配置，比如：  root/root, test/test, root/root1234  2、执行：more /etc/login，检查PASS\_MAX\_DAYS/PASS\_MIN\_LEN/PASS\_MIN\_DAYS/PASS\_WARN\_AGE参数  3、执行：awk -F: '($2 == "") { print $1 }' /etc/shadow, 检查是否存在空口令账号 |
| **基线符合性判定依据** | 建议在/etc/login文件中配置：PASS\_MIN\_LEN=6  不允许存在简单密码，密码设置符合策略，如长度至少为6  不存在空口令账号 |
| **备注** |  |

### root用户远程登录限制

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux远程登录安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-01-02 |
| **安全基线项说明** | 帐号与口令-root用户远程登录限制 |
| **检测操作步骤** | 执行：more /etc/securetty，检查Console参数 |
| **基线符合性判定依据** | 建议在/etc/securetty文件中配置：CONSOLE = /dev/tty01 |
| **备注** |  |

### 检查是否存在除root之外UID为0的用户

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux超级用户策略安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-01-03 |
| **安全基线项说明** | 帐号与口令-检查是否存在除root之外UID为0的用户 |
| **检测操作步骤** | 执行：awk -F: '($3 == 0) { print $1 }' /etc/passwd |
| **基线符合性判定依据** | 返回值包括“root”以外的条目，则低于安全要求； |
| **备注** | 补充操作说明  UID为0的任何用户都拥有系统的最高特权，保证只有root用户的UID为0 |

### root用户环境变量的安全性

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux超级用户环境变量安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-01-04 |
| **安全基线项说明** | 帐号与口令-root用户环境变量的安全性 |
| **检测操作步骤** | 执行：echo $PATH | egrep '(^|:)(\.|:|$)'，检查是否包含父目录，  执行：find `echo $PATH | tr ':' ' '` -type d \( -perm -002 -o -perm -020 \) -ls，检查是否包含组目录权限为777的目录 |
| **基线符合性判定依据** | 返回值包含以上条件，则低于安全要求；  find `echo $PATH | tr ':' ' '` -type d \( -perm -777 -o -perm -777 \) -ls |
| **注** | 补充操作说明  确保root用户的系统路径中不包含父目录，在非必要的情况下，不应包含组权限为777的目录 |

### 远程连接的安全性配置

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux远程连接安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-02-01 |
| **安全基线项说明** | 帐号与口令-远程连接的安全性配置 |
| **检测操作步骤** | 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 |
| **基线符合性判定依据** | 返回值包含以上条件，则低于安全要求； |
| **备注** | 补充操作说明  如无必要，删除这两个文件 |

### 用户的umask安全配置

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux用户umask安全基线要求项 |
| **安全基线项说明** | 帐号与口令-用户的umask安全配置 |
| **检测操作步骤** | 执行：more /etc/profile more /etc/csh.login more /etc/csh.cshrc more /etc/bashrc检查是否包含umask值 |
| **基线符合性判定依据** | umask值是默认的，则低于安全要求 |
| **备注** | 补充操作说明 直接vi /etc/bashrc  建议设置用户的默认umask=077 数据库机器不装。 |

### 重要目录和文件的权限设置

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux目录文件权限安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-02-03 |
| **安全基线项说明** | 文件系统-重要目录和文件的权限设置 |
| **检测操作步骤** | 执行以下命令检查目录和文件的权限设置情况：  ls –l /etc/  ls –l /etc/rc.d/init.d/  ls –l /tmp  ls –l /etc/inetd.conf  ls –l /etc/passwd  ls –l /etc/shadow  ls –l /etc/group  ls –l /etc/security  ls –l /etc/services  ls -l /etc/rc\*.d |
| **基线符合性判定依据** | 若权限过低，则低于安全要求； |
| **备注** | 补充操作说明  对于重要目录，建议执行如下类似操作：  # chmod -R 750 /etc/rc.d/init.d/\*  这样只有root可以读、写和执行这个目录下的脚本。 |

### 查找未授权的SUID/SGID文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux SUID/SGID文件安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-02-04 |
| **安全基线项说明** | 文件系统-查找未授权的SUID/SGID文件 |
| **检测操作步骤** | 用下面的命令查找系统中所有的SUID和SGID程序，执行：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0") {print $2 }'`; do  find / \( -perm -04000 -o -perm -02000 \) -type f -xdev -print  Done |
| **基线符合性判定依据** | 若存在未授权的文件，则低于安全要求； |
| **备注** | 补充操作说明  建议经常性的对比suid/sgid文件列表，以便能够及时发现可疑的后门程序 |

### 检查任何人都有写权限的目录

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux目录写权限安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-02-05 |
| **安全基线项说明** | 文件系统-检查任何人都有写权限的目录 |
| **检测操作步骤** | 在系统中定位任何人都有写权限的目录用下面的命令：  for PART in `awk '($3 == "ext2" || $3 == "ext3") \  { print $2 }' /etc/fstab`; do  find / -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print  Done |
| **基线符合性判定依据** | 若返回值非空，则低于安全要求； |
| **备注** |  |

### 查找任何人都有写权限的文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux文件写权限安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-02-06 |
| **安全基线项说明** | 文件系统-查找任何人都有写权限的文件 |
| **检测操作步骤** | 在系统中定位任何人都有写权限的文件用下面的命令：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0") {print $2 }'`; do  find $PART -xdev -type f \( -perm -0002 -a ! -perm -1000 \) -print  Done |
| **基线符合性判定依据** | 若返回值非空，则低于安全要求； |
| **备注** |  |

### 检查没有属主的文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux文件所有权安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-02-07 |
| **安全基线项说明** | 文件系统-检查没有属主的文件 |
| **检测操作步骤** | 定位系统中没有属主的文件用下面的命令：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0") {print $2 }'`; do  find $PART -nouser -o -nogroup -print  done  注意：不用管“/dev”目录下的那些文件。 |
| **基线符合性判定依据** | 若返回值非空，则低于安全要求； |
| **备注** | 补充操作说明  发现没有属主的文件往往就意味着有黑客入侵你的系统了。不能允许没有主人的文件存在。如果在系统中发现了没有主人的文件或目录，先查看它的完整性，如果一切正常，给它一个主人。有时候卸载程序可能会出现一些没有主人的文件或目录，在这种情况下可以把这些文件和目录删除掉。 |

### 检查异常隐含文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux隐含文件安全基线要求项 |
| **安全基线编号** | SBL-Linux-02-02-08 |
| **安全基线项说明** | 文件系统-检查异常隐含文件 |
| **检测操作步骤** | 用“find”程序可以查找到这些隐含文件。例如：  # find / -name ".. \*" -print –xdev  # find / -name "…\*" -print -xdev | cat -v  同时也要注意象“.xx”和“.mail”这样的文件名的。（这些文件名看起来都很象正常的文件名） |
| **基线符合性判定依据** | 若返回值非空，则低于安全要求； |
| **备注** | 补充操作说明  在系统的每个地方都要查看一下有没有异常隐含文件（点号是起始字符的，用“ls”命令看不到的文件），因为这些文件可能是隐藏的黑客工具或者其它一些信息（口令破解程序、其它系统的口令文件，等等）。在UNIX下，一个常用的技术就是用一些特殊的名，如：“…”、“.. ”（点点空格）或“..^G”（点点control-G），来隐含文件或目录。 |

# 日志审计

## 日志

### syslog登录事件记录

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux登录审计安全基线要求项 |
| **安全基线编号** | SBL-Linux-03-01-01 |
| **安全基线项说明** | 日志审计-syslog登录事件记录 |
| **检测操作步骤** | 执行命令：more /etc/syslog.conf  查看参数authpriv值 |
| **基线符合性判定依据** | 若未对所有登录事件都记录，则低于安全要求； |
| **备注** |  |

## 审计

### Syslog.conf的配置审核

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux配置审计安全基线要求项 |
| **安全基线编号** | SBL-Linux-03-02-01 |
| **安全基线项说明** | 日志审计-Syslog.conf的配置审核 |
| **检测操作步骤** | 执行：more /etc/syslog.conf，查看是否设置了下列项：  kern.warning;\*.err;authpriv.none\t@loghost  \*.info;mail.none;authpriv.none;cron.none\t@loghost  \*.emerg\t@loghost  local7.\*\t@loghost |
| **基线符合性判定依据** | 若未设置，则低于安全要求； |
| **备注** | 补充操作说明  建议配置专门的日志服务器，加强日志信息的异地同步备份 |

# 系统文件

## 系统状态

### 系统core dump状态

|  |  |
| --- | --- |
| **安全基线项目名称** | 操作系统Linux core dump 状态安全基线要求项 |
| **安全基线编号** | SBL-Linux-04-01-01 |
| **安全基线项说明** | 系统文件-系统core dump状态 |
| **检测操作步骤** | 执行：more /etc/security/limits.conf 检查是否包含下列项：  \* soft core 0  \* hard core 0 |
| **基线符合性判定依据** | 若不存在，则低于安全要求 |
| **备注** | 补充操作说明  core dump中可能包括系统信息，易被入侵者利用，建议关闭 |