



openEuler

1.0

安全加固指南

发布日期 2020-02-08

目 录

法律声明.....	iv
前言.....	v
1 操作系统加固概述.....	6
1.1 加固目的	6
1.2 加固方案	6
1.3 加固影响	7
2 加固指导.....	9
2.1 系统服务	9
2.1.1 加固 SSH 服务	9
2.2 文件权限	16
2.2.1 设置文件的权限和属主	16
2.2.2 删除无主文件	16
2.2.3 处理空链接文件	17
2.2.4 设置守护进程的 umask 值	17
2.2.5 为全局可写目录添加粘滞位属性.....	18
2.2.6 删除非授权文件的全局可写属性.....	18
2.2.7 限制 at 命令的使用权限.....	19
2.2.8 限制 cron 命令的使用权限	19
2.3 内核参数	20
2.3.1 加固内核参数	20
2.4 授权认证	22
2.4.1 设置网络远程登录的警告信息.....	22
2.4.2 禁止通过 CTRL+ALT+DEL 重启系统.....	23
2.4.3 设置终端的自动退出时间	23
2.4.4 设置用户的默认 umask 值为 077	23
2.4.5 设置 GRUB2 加密口令	24
2.4.6 安全单用户模式	25
2.4.7 禁止交互式启动	25
2.5 账户口令	26

2.5.1 屏蔽系统帐户	26
2.5.2 限制使用 su 命令的帐户	26
2.5.3 设置口令复杂度	26
2.5.4 设置口令有效期	28
2.5.5 设置口令的加密算法	29
2.5.6 登录失败超过三次后锁定	29
2.5.7 加固 su 命令	30
3 附录.....	31
3.1 文件和目录权限含义	31
3.2 umask 值含义	31

法律声明

版权所有 © 2020 华为技术有限公司。

您对“本文档”的复制、使用、修改及分发受知识共享(Creative Commons)署名一相同方式共享 4.0 国际公共许可协议(以下简称“CC BY-SA 4.0”)的约束。为了方便用户理解，您可以通过访问 <https://creativecommons.org/licenses/by-sa/4.0/> 了解 CC BY-SA 4.0 的概要 (但不是替代)。CC BY-SA 4.0 的完整协议内容您可以访问如下网址获取：
<https://creativecommons.org/licenses/by-sa/4.0/legalcode>。

商标声明

openEuler 为华为技术有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

免责声明

本文档仅作为使用指导，除非适用法强制规定或者双方有明确书面约定，华为技术有限公司对本文档中的所有陈述、信息和建议不做任何明示或默示的声明或保证，包括但不限于不侵权，时效性或满足特定目的的担保。

前言

概述



本文档给出 openEuler 的加固介绍和加固方法，指导用户进行安全加固。

读者对象

本文档主要适用于需要对 openEuler 进行安全加固的管理员。管理员需要熟悉操作系统安全架构和安全技术。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 须知	用于传递设备或环境安全警示信息。如不可避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
 说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

1 操作系统加固概述

介绍对 openEuler 系统进行加固的目的和加固方案。

1.1 加固目的

1.2 加固方案

1.3 加固影响

1.1 加固目的

操作系统作为信息系统的核心，承担着管理硬件资源和软件资源的重任，是整个信息系统安全的基础。操作系统之上的各种应用，要想获得信息的完整性、机密性、可用性和可控性，必须依赖于操作系统。脱离了对操作系统的安全保护，仅依靠其他层面的防护手段来阻止黑客和病毒等对网络信息系统的攻击，是无法满足安全需求的。

因此，需要对操作系统进行安全加固，构建动态、完整的安全体系，增强产品的安全性，提升产品的竞争力。

1.2 加固方案

本章描述 openEuler 的安全加固方案，包括加固方式和加固内容。

加固方式

openEuler 默认搭载系统安全加固包 `security-tool`，在安装时生成安全加固服务。系统在首次启动时自动运行安全加固服务，执行默认的安全策略配置。用户可以根据需求定制安全加固工具或者通过修改相关配置定制加固方案，本文档介绍相关的加固方法。

加固内容

openEuler 系统加固内容主要分为以下 5 个部分：

- 系统服务
- 文件权限

- 内核参数
- 授权认证
- 账号口令

1.3 加固影响

对文件权限、账户口令等安全加固，可能造成用户使用习惯变更，从而影响系统的易用性。影响系统易用性的常见加固项请参见表 1-1。

表1-1 加固影响说明

加固项	建议加固	易用性影响	openEuler 默认是否设置了该加固项
字符界面等待超时限制	当字符界面长时间处在空闲状态，字符界面会自动退出。 说明 当用户通过 SSH 登录，超时时间由 /etc/profile 文件的 TMOU 字段和 /etc/ssh/sshd_config 文件的 ClientAliveInterval 字段两个值中较小的值决定。建议加固为 300 秒。	用户长时间不操作字符界面，字符界面会自动退出。	否
口令复杂度限制	口令长度最小为 8 位，口令至少包含大写字母、小写字母、数字和特殊字符中的 3 种。	系统中所有用户不能设置简单的口令，口令必须符合复杂度要求。	否
限定登录失败时的尝试次数	当用户登录系统时，口令连续输错 3 次，账户将被锁定 60 秒，锁定期间不能登录系统。	用户不能随意登录系统，账户被锁定后必须等待 60 秒。	是
用户默认 umask 值限制	设置所有用户的默认 umask 值为 077，使用户创建文件的默认权限为 600、目录权限为 700。	用户需要按照需求修改指定文件或目录的权限。	是
口令有效期	口令有效期的设置通过修改 /etc/login.defs 文件实现，加固默认值为口令最大有效期 90 天，两次修改口令的最小间隔时间为 0，口令过期前开始提示天数为 7。	口令过期后用户重新登录时，提示口令过期并强制要求修改，不修改则无法进入系统。	否
su 权限限制	su 命令用于在不同账户之间切换。	普通账户执行	是

加固项	建议加固	易用性影响	openEuler 默认是否设置了该加固项
	为了增强系统安全性，有必要对 su 命令的使用权进行控制，只允许 root 和 wheel 群组的账户使用 su 命令，限制其他账户使用。	su 命令失败，必须加入 wheel 群组才可以 su 成功。	
禁止 root 账户直接 SSH 登录系统	设置/etc/ssh/sshd_config 文件的 PermitRootLogin 字段的值为 no，用户无法使用 root 账户直接 SSH 登录系统。	用户需要先使用普通账户 SSH 登录后，再切换至 root 账户。	否
SSH 强加密算法	SSH 服务的 MACs 和 Ciphers 配置，禁止对 CBC、MD5、SHA1 算法的支持，修改为 CTR、SHA2 算法。	当前 windows 下使用的部分低版本的 Xshell、PuTTY 不支持 aes128-ctr、aes192-ctr、aes256-ctr、hmac-sha2-256、hmac-sha2-512 算法，可能会出现无法通过 SSH 登录系统的情况，请使用最新的 PuTTY（0.63 版本以上）、Xshell（5.0 版本及以上版本）登录。	是

2 加固指导

用户可以通过修改加固策略配置文件或加固脚本进行系统加固。本节介绍各加固项的含义以及 openEuler 是否已默认加固，并给出加固方法，指导用户进行安全加固。

- 2.1 系统服务
- 2.2 文件权限
- 2.3 内核参数
- 2.4 授权认证
- 2.5 账户口令

2.1 系统服务

2.1.1 加固 SSH 服务

说明

SSH（Secure Shell）是目前较可靠，专为远程登录会话和其他网络服务提供安全性保障的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。透过 SSH 可以对所有传输的数据进行加密，并防止 DNS 欺骗和 IP 欺骗。OpenSSH 是 SSH 协议的免费开源实现。

加固 SSH 服务，是指修改 SSH 服务中的配置来设置系统使用 OpenSSH 协议时的算法、认证等参数，从而提高系统的安全性。表 2-1 中详细说明了各加固项含义、建议加固值及其默认策略。

实现

服务端加固操作如下：

- 步骤 1 打开服务端 SSH 服务的配置文件/etc/ssh/sshd_config，在该文件中修改或添加对应加固项及其加固值。
- 步骤 2 保存/etc/ssh/sshd_config 文件。

步骤 3 重启 SSH 服务，命令如下：

```
systemctl restart sshd
```

----结束

客户端加固操作如下：

步骤 1 打开客户端 SSH 服务的配置文件/etc/ssh/ssh_config，在该文件中修改或添加对应加固项及其加固值。

步骤 2 保存/etc/ssh/ssh_config 文件。

步骤 3 重启 SSH 服务，命令如下：

```
systemctl restart sshd
```

----结束

加固项说明

- 服务端加固策略

SSH 服务的所有加固项均保存在配置文件/etc/ssh/sshd_config 中，服务端各加固项的含义、加固建议以及 openEuler 默认是否已经加固为建议加固值请参见表 2-1。

表2-1 SSH 服务端加固项说明

加固项	加固项说明	加固建议	openEuler 默认是否已加固为建议值
Protocol	设置使用 SSH 协议的版本	2	是
SyslogFacility	设置 SSH 服务的日志类型。加固策略将其设置为“AUTH”，即认证类日志	AUTH	是
LogLevel	设置记录 sshd 日志消息的层次	VERBOSE	是
X11Forwarding	设置使用 SSH 登录后，能否使用图形化界面	no	是
MaxAuthTries	最大认证尝试次数	3	否
PubkeyAuthentication	设置是否允许公钥认证。	yes	是
RSAAuthentication	设置是否允许只有 RSA 安全验证	yes	是
IgnoreRhosts	设置是否使用 rhosts 文件和 shosts 文件进行验证。rhosts 文件和 shosts 文件用于记录可以访问远程计算机的计	yes	是

加固项	加固项说明	加固建议	openEuler 默认是否已加固为建议值
	计算机名及关联的登录名		
RhostsRSA Authentication	设置是否使用基于 rhosts 的 RSA 算法安全验证。rhosts 文件记录可以访问远程计算机的计算机名及关联的登录名	no	是
Hostbased Authentication	设置是否使用基于主机的验证。基于主机的验证是指已信任客户机上的任何用户都可以使用 SSH 连接	no	是
PermitRootLogin	是否允许 root 账户直接使用 SSH 登录系统 说明 若需要直接使用 root 账户通过 SSH 登录系统，请修改/etc/ssh/sshd_config 文件的 PermitRootLogin 字段的值为 yes。	no	否
PermitEmptyPasswords	设置是否允许用口令为空的账号登录	no	是
PermitUserEnvironment	设置是否解析 ~/.ssh/environment 和 ~/.ssh/authorized_keys 中设定的环境变量	no	是
Ciphers	设置 SSH 数据传输的加密算法	aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305@openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com	是
ClientAliveInterval	设置系统等待的超时时间（单位秒）。超过指定时间未收到来自客户端的数据，则断开连接	300	否
ClientAliveCountMax	设置超时次数。服务器发出请求后，客户端没有响应的次数达到一定值，连接自动断开	0	否

加固项	加固项说明	加固建议	openEuler 默认是否已加固为建议值
Banner	指定登录 SSH 前后显示的提示信息 的文件	/etc/issue .net	是
MACs	设置 SSH 数据校验的哈希算法	hmac- sha2- 512,hma c-sha2- 512- etm@ope nssh.com ,hmac- sha2- 256,hma c-sha2- 256- etm@ope nssh.com ,hmac- sha1,hma c-sha1- etm@ope nssh.com	是
StrictModes	设置 SSH 在接收登录请求之前是否 检查用户 HOME 目录和 rhosts 文件 的权限和所有权	yes	是
UsePAM	使用 PAM 登录认证	yes	是
AllowTcpFo rwarding	设置是否允许 TCP 转发	no	是
Subsystem sftp /usr/libexec/ openssh/sftp -server	sftp 日志记录级别，记录 INFO 级别 以及认证日志。	-l INFO - f AUTH	是
AllowAgent Forwarding	设置是否允许 SSH Agent 转发	no	是
GatewayPort s	设置是否允许连接到转发客户端端口	no	是
PermitTunne l	Tunnel 设备是否允许使用	no	是
KexAlgorith ms	设置 SSH 密钥交换算法	curve255 19- sha256,c urve2551 9- sha256@	

加固项	加固项说明	加固建议	openEuler 默认是否已加固为建议值
		@libssh.org,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256	
LoginGraceTime	限制用户必须在指定的时限内认证成功，0 表示无限制。默认值是 60 秒。	60	否

说明

默认情况下，登录 SSH 前后显示的提示信息保存在/etc/issue.net 文件中，/etc/issue.net 默认信息为“Authorized users only. All activities may be monitored and reported.”。

- 客户端加固策略

SSH 服务的所有加固项均保存在配置文件/etc/ssh/ssh_config 中，客户端各加固项的含义、加固建议以及 openEuler 默认是否已经加固为建议加固值请参见表 2-2。

表2-2 SSH 客户端加固项说明

加固项	加固项说明	加固建议	open Euler 默认是否已加固为建议值
KexAlgorithms	设置 SSH 密钥交换算法	ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1	否
VerifyHostKeyDNS	是否	ask	否

加固项	加固项说明	加固建议	open Euler 默认是否已加固为建议值
	使用 DNS 或者 SSHFP 资源记录验证 Host Key		

📖 说明

对于使用 dh 算法进行密钥交换的第三方客户端和服务端工具，要求允许建立连接的最低长度为 2048bits。

其他安全建议

- SSH 服务仅侦听指定 IP 地址

出于安全考虑，建议用户在使用 SSH 服务时，仅在必需的 IP 上进行绑定侦听，而不是侦听 0.0.0.0，可修改/etc/ssh/sshd_config 文件中的 ListenAddress 配置项。

 - a. 打开并修改/etc/ssh/sshd_config 文件


```
vi /etc/ssh/sshd_config
```

修改内容如下，表示绑定侦听 IP 为 192.168.1.100，用户可根据实际情况修改需要侦听的 IP

```
...
ListenAddress 192.168.1.100
...
```
 - b. 重启 SSH 服务


```
systemctl restart sshd.service
```
- 限制 SFTP 用户向上跨目录访问

SFTP 是 FTP over SSH 的安全 FTP 协议，对于访问 SFTP 的用户建议使用专用账号，只能上传或下载文件，不能用于 SSH 登录，同时对 SFTP 可以访问的目录进行限定，防止目录遍历攻击，具体配置如下：

📖 说明

sftpgroup 为示例用户组，sftpuser 为示例用户名。

- a. 创建 SFTP 用户组

- ```
groupadd sftpgroup
```
- b. 创建 SFTP 根目录  

```
mkdir /sftp
```
- c. 修改 SFTP 根目录属主和权限  

```
chown root:root /sftp
chmod 755 /sftp
```
- d. 创建 SFTP 用户  

```
useradd -g sftpgroup -s /sbin/nologin sftpuser
```
- e. 设置 SFTP 用户的口令  

```
passwd sftpuser
```
- f. 创建 SFTP 用户上传目录  

```
mkdir /sftp/sftpuser
```
- g. 修改 SFTP 用户上传目录属主和权限  

```
chown root:root /sftp/sftpuser
chmod 777 /sftp/sftpuser
```
- h. 修改/etc/ssh/sshd\_config 文件  

```
vi /etc/ssh/sshd_config
```

修改内容如下：

```
#Subsystem sftp /usr/libexec/openssh/sftp-server -l INFO -f AUTH
Subsystem sftp internal-sftp -l INFO -f AUTH
...

Match Group sftpgroup
 ChrootDirectory /sftp/%u
 ForceCommand internal-sftp
```

#### 📖 说明

- %u 代表当前 sftp 用户的用户名，这是一个通配符，用户原样输入即可。
- 以下内容必须加在/etc/ssh/sshd\_config 文件的末尾。

```
Match Group sftpgroup
 ChrootDirectory /sftp/%u
 ForceCommand internal-sftp
```

- i. 重启 SSH 服务

```
systemctl restart sshd.service
```

- SSH 远程执行命令

OpenSSH 通用机制，在远程执行命令时，默认不开启 tty，如果执行需要密码的命令，密码会明文回显。出于安全考虑，建议用户增加-t 选项，确保密码输入安全。如下：

```
ssh -t testuser@192.168.1.100 su
```

#### 📖 说明

192.168.1.100 为示例 IP，testuser 为示例用户。

## 2.2 文件权限

### 2.2.1 设置文件的权限和属主

#### 说明

Linux 将所有对象都当作文件来处理，即使一个目录也被看作是包含有多个其他文件的大文件。因此，Linux 中最重要的就是文件和目录的安全性。文件和目录的安全性主要通过权限和属主来保证。

openEuler 默认对系统中的常用目录、可执行文件和配置文件设置了权限和属主。

#### 实现

以/bin 目录为例，修改文件权限和文件属主的操作如下：

- 修改文件权限。例如将/bin 目录权限设置为 755。

```
chmod 755 /bin
```

- 修改文件属主。例如将/bin 目录的拥有者和群组设置为 root:root。

```
chown root:root /bin
```

### 2.2.2 删除无主文件

#### 说明

系统管理员在删除用户/群组时，存在着忘记删除该用户/该群组所拥有文件的问题。如果后续新创建的用户/群组与被删除的用户/群组同名，则新用户/新群组会拥有部分不属于其权限的文件，建议将此类文件删除。

#### 实现

删除用户 ID 不存在的文件

步骤 1 查找用户 ID 不存在的文件。

```
find / -nouser
```

步骤 2 删除查找到的文件。其中 *filename* 为用户 ID 不存在文件的文件名。

```
rm -f filename
```

----结束

删除群组 ID 不存在的文件

步骤 1 查找用户 ID 不存在的文件。

```
find / -nogroup
```

步骤 2 删除查找到的文件。其中 *filename* 为用户 ID 不存在文件的文件名。

```
rm -f filename
```



----结束

## 2.2.3 处理空链接文件

### 说明

无指向的空链接文件，可能会被恶意用户利用，影响系统安全性。建议用户删除无效的空链接文件，提高系统安全性。

### 特殊场景

openEuler 系统安装完成后，可能存在空链接文件，这些空链接文件可能有对应用途（有些空链接文件是预制的，会被其他组件依赖）。请用户根据实际环境进行处理，处理方式请参见[实现](#)。

例如，openEuler 支持 UEFI 和 legacy BIOS 两种安装模式，两种引导场景支持的 grub 相关包默认都安装，当用户选择 legacy BIOS 模式安装时，形成空链接文件“/etc/grub2-efi.cfg”；当用户选择 UEFI 模式安装时，会形成空链接文件“/etc/grub2.cfg”，需要用户根据实际情况处理空链接。

### 实现

步骤 1 通过如下命令查找系统中的空链接文件。

```
find dirname -type l -follow 2>/dev/null
```

#### 📖 说明

*dirname* 为搜索目录的名称，通常需要关注系统关键目录：/bin、/boot、/usr、/lib64、/lib、/var 等。

步骤 2 如果此类文件无实际作用，可通过如下命令删除。

```
rm -f filename
```

#### 📖 说明

*filename* 为 [步骤 1](#) 找出的文件名。

----结束

## 2.2.4 设置守护进程的 umask 值

### 说明

umask 值用来为新创建的文件和目录设置缺省权限。如果没有设定 umask 值，则生成的文件具有全局可写权限，存在一定的风险。守护进程负责系统上某个服务，让系统可以接受来自用户或者是网络客户的要求。为了提高守护进程所创建文件和目录的安全性，建议设置其 umask 值为 0027。umask 值代表的是权限的“补码”，umask 值和权限的换算方法请参见 [3.2 umask 值含义](#)。

### 📖 说明

openEuler 默认已设置守护进程的 `umask` 值为 0027。

## 实现

在配置文件 `/etc/sysconfig/init` 中新增一行：`umask 0027`。

## 2.2.5 为全局可写目录添加粘滞位属性

### 说明

任意用户可以删除、修改全局可写目录中的文件和目录，为了确保全局可写目录中的文件和目录不会被任意删除，需要为全局可写目录添加粘滞位属性。

## 实现

步骤 1 搜索全局可写目录。

```
find / -type d -perm -0002 ! -perm -1000 -ls | grep -v proc
```

步骤 2 为全局可写目录添加粘滞位属性。`dirname` 为实际查找到的目录名。

```
chmod +t dirname
```

----结束

## 2.2.6 删除非授权文件的全局可写属性

### 说明

全局可写文件可被系统中的任意用户修改，影响系统完整性。

## 实现

步骤 1 列举系统中所有的全局可写文件。

```
find / -type d \(-perm -o+w \) | grep -v proc
find / -type f \(-perm -o+w \) |
grep -v proc
```

步骤 2 查看步骤 1 列举的所有文件(粘滞位位的文件和目录可以排除在外)，删除文件或去掉其全局可写权限。使用以下命令去掉权限，其中 `filename` 为对应文件名：

```
chmod o-w filename
```

### 📖 说明

可通过如下命令确定对应文件或目录是否设置了粘滞位，若回显中包含 `T` 标记，则为粘滞位文件或目录。命令中的 `filename` 为需要查询文件或目录的名称。

```
ls -l filename
```

----结束

## 2.2.7 限制 at 命令的使用权限

### 说明

at 命令用于创建在指定时间自动执行的任务。为避免任意用户通过 at 命令安排工作，造成系统易受攻击，需要指定可使用该命令的用户。

### 实现

步骤 1 删除/etc/at.deny 文件。

```
rm -f /etc/at.deny
```

步骤 2 将/etc/at.allow 的文件属主改为 root:root。

```
chown root:root /etc/at.allow
```

步骤 3 控制/etc/at.allow 的文件权限，仅 root 可操作。

```
chmod og-rwx /etc/at.allow
```

----结束

## 2.2.8 限制 cron 命令的使用权限

### 说明

cron 命令用于创建例行性任务。为避免任意用户通过 cron 命令安排工作，造成系统易受攻击，需要指定可使用该命令的用户。

### 实现

步骤 1 删除/etc/cron.deny 文件。

```
rm -f /etc/at.deny
```

步骤 2 将/etc/cron.allow 的文件属主改为 root:root。

```
chown root:root /etc/cron.allow
```

步骤 3 控制/etc/cron.allow 的文件权限，仅 root 可操作。

```
chmod og-rwx /etc/cron.allow
```

----结束

## 2.3 内核参数

### 2.3.1 加固内核参数

#### 说明

内核参数决定配置和应用特权的状态。内核提供用户可配置的系统控制，这一系统控制可微调或配置，该功能特性可通过控制各种可配置的内核参数，来提高操作系统的安全特性。比如：通过微调或配置网络选项，可有效提高系统的安全性。

#### 实现

步骤 1 将表 2-3 中的加固项写入/etc/sysctl.conf 文件中。

#### 📖 说明

写入方式如下：

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

表2-3 内核参数加固策略说明

| 加固项                                       | 加固项说明                                                                  | 加固建议 | openEuler 默认是否已加固为建议值 |
|-------------------------------------------|------------------------------------------------------------------------|------|-----------------------|
| net.ipv4.icmp_echo_ignore_broadcasts      | 是否接受 ICMP 广播报文。加固策略为不接受。                                               | 1    | 是                     |
| net.ipv4.conf.all.rp_filter               | 验证数据包使用的实际源地址是否与路由表相关，以及使用该特定源 IP 地址的数据包是否通过接口获取其响应。加固策略为启用该项。         | 1    | 是                     |
| net.ipv4.conf.default.rp_filter           |                                                                        | 1    | 是                     |
| net.ipv4.ip_forward                       | IP Forwarding 可阻止未授权的 IP 数据包渗透至网络。加固策略为禁用该特性。                          | 0    | 是                     |
| net.ipv4.conf.all.accept_source_route     | accept_source_route 指允许数据包的发送者指定数据包的发送路径，以及返回给发送者的数据包所走的路径。加固策略为禁用该特性。 | 0    | 是                     |
| net.ipv4.conf.default.accept_source_route |                                                                        | 0    | 是                     |
| net.ipv4.conf.all.accept_redirects        | 是否发送 ICMP 重定向报文。加固                                                     | 0    | 是                     |

| 加固项                                        | 加固项说明                                                                 | 加固建议 | openEuler 默认是否已加固为建议值 |
|--------------------------------------------|-----------------------------------------------------------------------|------|-----------------------|
| net.ipv4.conf.default.accept_redirects     | 策略为禁止发送。                                                              | 0    | 是                     |
| net.ipv6.conf.all.accept_redirects         |                                                                       | 0    | 是                     |
| net.ipv6.conf.default.accept_redirects     |                                                                       | 0    | 是                     |
| net.ipv4.conf.all.send_redirects           | 是否将 ICMP 重定向报文发送至其他主机。只有当主机作为路由时，应启用该策略。加固策略为禁用该项。                    | 0    | 是                     |
| net.ipv4.conf.default.send_redirects       |                                                                       | 0    | 是                     |
| net.ipv4.icmp_ignore_bogus_error_responses | 忽略伪造的 ICMP 数据包，不会将其记录到日志，将节省大量的硬盘空间。加固策略为启用该项。                        | 1    | 是                     |
| net.ipv4.tcp_syncookies                    | SYN Attack 是一种通过占用系统资源迫使系统重启的 DoS 攻击。加固策略为开启 TCP-SYN cookie 保护。       | 1    | 是                     |
| kernel.dmesg_restrict                      | 加固 dmesg 信息，仅允许管理员查看。                                                 | 1    | 是                     |
| kernel.sched_autogroup_enabled             | 该选项决定内核是否对线程进行自动分组调度。开启后调度组之间互相竞争时间片，调度组内的线程再竞争调度组分配到的时间片。加固策略为不启用该项。 | 0    | 否                     |
| kernel.sysrq                               | 禁用魔术键。<br>说明<br>建议禁用魔术键，避免由于直接发送命令到内核对系统造成影响，增强内核安全性。                 | 0    | 是                     |
| net.ipv4.conf.all.secure_redirects         | 设置系统是接收来自任何主机的 ICMP 重定向消息还是从默认网关列表中的网关处接收 ICMP 重定向消息。加固策略为采用前者。       | 0    | 是                     |
| net.ipv4.conf.default.secure_redirects     |                                                                       | 0    | 是                     |

步骤 2 加载 sysctl.conf 文件中设置的内核参数

```
sysctl -p /etc/sysctl.conf
```

----结束

## 其它安全建议

- **net.ipv4.icmp\_echo\_ignore\_all**: 忽略 ICMP 请求。  
出于安全考虑，建议开启此项（当前默认值为 0，开启将值设为 1）。  
但开启后会忽略所有接收到的 icmp echo 请求的包(会导致机器无法 ping 通)，建议用户根据实际组网场景决定是否开启此项。
- **net.ipv4.conf.all.log\_martians/net.ipv4.conf.default.log\_martians**: 对于仿冒/源路由/重定向数据包开启日志记录。  
出于安全考虑，建议开启此项（当前默认值为 0，开启将值设为 1）。  
但是开启后会记录带有不允许的地址的数据到内核日志中，存在冲日志风险，建议用户根据实际使用场景决定是否开启此项。
- **net.ipv4.tcp\_timestamps**: 关闭 tcp\_timestamps。  
出于安全考虑，建议关闭 tcp\_timestamps（当前默认值为 1，关闭将值设为 0）。  
但是关闭此项会影响 TCP 超时重发的性能，建议用户根据实际使用场景决定是否关闭此项。
- **net.ipv4.tcp\_max\_syn\_backlog**: 决定了 SYN\_RECV 状态队列的数量。  
该参数决定了 SYN\_RECV 状态队列的数量，超过这个数量，系统将不再接受新的 TCP 连接请求，一定程度上可以防止系统资源耗尽。建议由用户根据实际使用场景配置合适的值。

## 2.4 授权认证

### 2.4.1 设置网络远程登录的警告信息

#### 说明

设置网络远程登录的警告信息，用于在登录进入系统之前向用户提示警告信息，明示非法侵入系统可能受到的惩罚，吓阻潜在的攻击者。同时也可以隐藏系统架构及其他系统信息，避免招致对系统的目标性攻击。

#### 实现

该设置可以通过修改/etc/issue.net 文件的内容实现。将/etc/issue.net 文件原有内容替换为如下信息（openEuler 默认已设置）：

```
Authorized users only. All activities may be monitored and reported.
```

## 2.4.2 禁止通过 CTRL+ALT+DEL 重启系统

### 说明

操作系统默认能够通过“Ctrl+Alt+Del”进行重启，禁止该项特性可以防止因为误操作而导致数据丢失。

### 实现

通过屏蔽内核 keyboard 中的“Ctrl+Alt+Del”响应函数解决。

```
rm -f /etc/systemd/system/ctrl-alt-del.target
rm -f /usr/lib/systemd/system/ctrl-alt-del.target
```

#### 说明

如下文件保留的原因是 XEN 驱动需要调用，系统已无法响应“Ctrl+Alt+Del”操作，因此无影响：

```
/usr/lib/systemd/system/ctrl-alt-del.target
```

## 2.4.3 设置终端的自动退出时间

### 说明

无人看管的终端容易被侦听或被攻击，可能会危及系统安全。因此需要终端在停止运行一段时间后能够自动退出。

### 实现

自动退出时间由/etc/profile 文件的 TMOUT 字段（单位为秒）控制，在/etc/profile 的尾部添加如下配置：

```
export TMOUT=300
```

## 2.4.4 设置用户的默认 umask 值为 077

### 说明

umask 值用于为用户新创建的文件和目录设置缺省权限。如果 umask 的值设置过小，会使群组用户或其他用户的权限过大，给系统带来安全威胁。因此设置所有用户默认的 umask 值为 0077，即用户创建的目录默认权限为 700，文件的默认权限为 600。umask 值代表的是权限的“补码”，umask 值和权限的换算方法请参见 3.2 umask 值含义。

#### 说明

openEuler 默认已设置用户的默认 umask 值为 077。

## 实现

步骤 1 分别在/etc/bashrc 文件和/etc/profile.d/目录下的所有文件中加入“umask 0077”。

```
echo "umask 0077" >> $FILE
```

### 📖 说明

`$FILE` 为具体的文件名，例如：`echo "umask 0077" >> /etc/bashrc`

步骤 2 设置/etc/bashrc 文件和/etc/profile.d/目录下所有文件的属主为 root，群组为 root。

```
chown root.root $FILE
```

### 📖 说明

`$FILE` 为具体的文件名，例如：`chown root.root /etc/bashrc`

----结束

## 2.4.5 设置 GRUB2 加密口令

### 说明

GRUB 是 GRand UnifiedBootloader 的缩写，它是一个操作系统启动管理器，用来引导不同系统（如 Windows、Linux），GRUB2 是 GRUB 的升级版。

系统启动时，可以通过 GRUB2 界面修改系统的启动参数。为了确保系统的启动参数不被任意修改，需要对 GRUB2 界面进行加密，仅在输入正确的 GRUB2 口令时才能修改启动参数。

### 📖 说明

GRUB2 默认设置的口令为 `openEuler#12`，建议用户首次登录时修改默认密码并定期更新，避免密码泄露后，启动选项被篡改，导致系统启动异常。

### 实现

步骤 1 使用 `grub2-mkpasswd-pbkdf2` 命令生成加密的口令

### 📖 说明

GRUB2 加密算法使用 sha512。

```
grub2-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.5A45748D892672FDA02DD3B6F7AE390AC6E6D532A600D4AC477D25C7D0
87644697D8A0894DFED9D86DC2A27F4E01D925C46417A225FC099C12DBD3D7D49A7425.2BD2F5BF4907
DCC389CC5D165DB85CC3E2C94C8F9A30B01DACAA9CD552B731BA1DD3B7CC2C765704D55B8CD962D2AEF
19A753CBE9B8464E2B1EB39A3BB4EAB08
```

### 📖 说明

在 Enter password 和 Reenter password 输入相同的口令。



grub.pbkdf2.sha512.10000.5A45748D892672FDA02DD3B6F7AE390AC6E6D532A600D4AC477D25C7D087644697D8A0894DFED9D86DC2A27F4E01D925C46417A225FC099C12DBD3D7D49A7425.2BD2F5BF4907DCC389CC5D165DB85CC3E2C94C8F9A30B01DACAA9CD552B731BA1DD3B7C2C2C765704D55B8CD962D2AEF19A753CBE9B8464E2B1EB39A3BB4EAB08 为 openEuler#12 经过 grub2-mkpasswd-pbkdf2 加密后的输出，每次输出的密文不同。

步骤 2 使用 vi 工具打开 /boot/efi/EFI/openEuler/grub.cfg 的开始位置追加如下字段：

```
set superusers="root"
password_pbkdf2 root
grub.pbkdf2.sha512.10000.5A45748D892672FDA02DD3B6F7AE390AC6E6D532A600D4AC477D25C7D087644697D8A0894DFED9D86DC2A27F4E01D925C46417A225FC099C12DBD3D7D49A7425.2BD2F5BF4907DCC389CC5D165DB85CC3E2C94C8F9A30B01DACAA9CD552B731BA1DD3B7CC2C2C765704D55B8CD962D2AEF19A753CBE9B8464E2B1EB39A3BB4EAB08
```

#### 📖 说明

- superusers 字段用于设置 GRUB2 的超级管理员的账户名。
- password\_pbkdf2 字段后的参数，第 1 个参数为 GRUB2 的账户名，第 2 个为该账户的加密口令。

----结束

## 2.4.6 安全单用户模式

### 说明

单用户模式是以 root 权限进入系统，如不设置密码，将存在较大安全隐患。

### 实现

该设置可以通过修改 /etc/sysconfig/init 文件内容实现。将 SINGLE 选项配置为 SINGLE=/sbin/sulogin。

## 2.4.7 禁止交互式启动

### 说明

使用交互式引导，控制台用户可以禁用审计、防火墙或其他服务，削弱了系统安全性。用户可以禁止使用交互式引导，提升安全性。openEuler 默认已禁止。

### 实现

该设置可以通过修改 /etc/sysconfig/init 文件内容实现。将 PROMPT 选项配置为 PROMPT=no。

## 2.5 账户口令

### 2.5.1 屏蔽系统帐户

#### 说明

除了用户帐户外，其他账号称为系统账户。系统账户仅系统内部使用，禁止用于登录系统或其他操作，因此屏蔽系统账户。

#### 实现

将系统帐户的 Shell 修改为/sbin/nologin。

```
usermod -L -s /sbin/nologin $systemaccount
```

#### 📖 说明

*\$systemaccount* 指系统帐户。

### 2.5.2 限制使用 su 命令的帐户

#### 说明

su 命令用于在不同帐户之间切换。为了增强系统安全性，有必要对 su 命令的使用权进行控制，只允许 root 和 wheel 群组的帐户使用 su 命令，限制其他帐户使用。

#### 实现

su 命令的使用控制通过修改/etc/pam.d/su 文件实现，配置如下：

```
auth required pam_wheel.so use_uid
```

表2-4 pam\_wheel.so 配置项说明

| 配置项     | 说明           |
|---------|--------------|
| use_uid | 基于当前帐户的 uid。 |

### 2.5.3 设置口令复杂度

#### 说明

用户可以通过修改对应配置文件设置口令的复杂度要求，建议用户根据实际情况设置口令复杂度。

## 实现

口令复杂度通过/etc/pam.d/password-auth 和/etc/pam.d/system-auth 文件中的 pam\_pwquality.so 和 pam\_pwhistory.so 模块实现。用户可以通过修改这两个模块中的配置项修改口令复杂度要求。

## 设置举例

这里给出一个配置口令复杂度的例子，供用户参考。

### 密码复杂度要求

1. 口令长度至少 8 个字符。
2. 口令必须包含如下至少 3 种字符的组合：
  - 至少一个小写字母
  - 至少一个大写字母
  - 至少一个数字
  - 至少一个特殊字符：`~!@#\$\$%^&\*()-\_+=\|[{ }];:","<.>/?和空格
3. 口令不能和帐号或者帐号的倒写一样。
4. 不能修改为过去 5 次使用过的旧口令。

### 配置实现

在/etc/pam.d/password-auth 和/etc/pam.d/system-auth 文件中添加如下配置内容：

```
password requisite pam pwquality.so minlen=8 minclass=3 enforce for root
try first pass local users only retry=3 dcredit=0 ucredit=0 lcredit=0 ocredit=0
password required pam pwhistory.so use_authok remember=5 enforce_for_root
```

### 配置项说明

pam\_pwquality.so 和 pam\_pwhistory.so 的配置项请分别参见表 2-5 和表 2-6。

表2-5 pam\_pwquality.so 配置项说明

| 配置项        | 说明                              |
|------------|---------------------------------|
| minlen=8   | 口令长度至少包含 8 个字符                  |
| minclass=3 | 口令至少包含大写字母、小写字母、数字和特殊字符中的任意 3 种 |
| ucredit=0  | 口令包含任意个大写字母                     |
| lcredit=0  | 口令包含任意个小写字母                     |
| dcredit=0  | 口令包含任意个数字                       |
| ocredit=0  | 口令包含任意个特殊字符                     |
| retry=3    | 每次修改最多可以尝试 3 次                  |

| 配置项              | 说明               |
|------------------|------------------|
| enforce_for_root | 本设置对 root 帐户同样有效 |

表2-6 pam\_pwhistory.so 配置项说明

| 配置项              | 说明                   |
|------------------|----------------------|
| remember=5       | 口令不能修改为过去 5 次使用过的旧口令 |
| enforce_for_root | 本设置对 root 帐户同样有效     |

## 2.5.4 设置口令有效期

### 说明

出于系统安全性考虑，建议设置口令有效期限，且口令到期前通知用户更改口令。

### 实现

口令有效期的设置通过修改/etc/login.defs 文件实现，加固项如表 2-7 所示。表中所有的加固项都在文件/etc/login.defs 中。表中字段直接通过修改配置文件完成。

表2-7 login.defs 配置项说明所示

| 加固项           | 加固项说明         | 建议加固 | openEuler 默认是否已加固为建议值 |
|---------------|---------------|------|-----------------------|
| PASS_MAX_DAYS | 口令最大有效期       | 90   | 否                     |
| PASS_MIN_DAYS | 两次修改口令的最小间隔时间 | 0    | 否                     |
| PASS_WARN_AGE | 口令过期前开始提示天数   | 7    | 否                     |

### 说明

login.defs 是设置用户帐号限制的文件，可配置口令的最大过期天数、最大长度约束等。该文件里的配置对 root 用户无效。如果/etc/shadow 文件里有相同的选项，则以/etc/shadow 配置为准，即/etc/shadow 的配置优先级高于/etc/login.defs。口令过期后用户重新登录时，提示口令过期并强制要求修改，不修改则无法进入系统。

## 2.5.5 设置口令的加密算法

### 说明

出于系统安全考虑，口令不允许明文存储在系统中，应该加密保护。在不需要还原口令的场景，必须使用不可逆算法加密。设置口令的加密算法为 sha512，openEuler 默认已设置。通过上述设置可以有效防范口令泄露，保证口令安全。

### 实现

口令的加密算法设置通过修改/etc/pam.d/password-auth 和/etc/pam.d/system-auth 文件实现，添加如下配置：

```
password sufficient pam unix.so sha512 shadow nullok try first pass
use_authtok
```

表2-8 pam\_unix.so 配置项说明

| 配置项    | 说明                 |
|--------|--------------------|
| sha512 | 使用 sha512 算法对口令加密。 |

## 2.5.6 登录失败超过三次后锁定

### 说明

为了保障用户系统的安全，建议用户设置口令出错次数的阈值（建议 3 次），以及由于口令尝试被锁定用户的自动解锁时间（建议 300 秒）。

用户锁定期间，任何输入被判定为无效，锁定时间不因用户的再次输入而重新计时；解锁后，用户的错误输入记录被清空。通过上述设置可以有效防范口令被暴力破解，增强系统的安全性。

#### 说明

openEuler 默认口令出错次数的阈值为 3 次，系统被锁定后自动解锁时间为 60 秒。

### 实现

口令复杂度的设置通过修改/etc/pam.d/password-auth 和/etc/pam.d/system-auth 文件实现，设置口令最大的出错次数 3 次，系统锁定后的解锁时间为 300 秒的配置如下：

```
auth required pam faillock.so preauth audit deny=3 even deny root
unlock time=300
auth [default=die] pam faillock.so authfail audit deny=3 even deny root
unlock time=300
auth sufficient pam faillock.so authsucc audit deny=3 even deny root
unlock_time=300
```

表2-9 pam\_faillock.so 配置项说明

| 配置项             | 说明                         |
|-----------------|----------------------------|
| authfail        | 捕获用户登录失败的事件。               |
| deny=3          | 用户连续登录失败次数超过 3 次即被锁定。      |
| unlock_time=300 | 普通用户自动解锁时间为 300 秒（即 5 分钟）。 |
| even_deny_root  | 同样限制 root 帐户。              |

## 2.5.7 加固 su 命令

### 说明

为了增强系统安全性，防止使用“su”切换用户时将当前用户环境变量带入其他环境，openEuler 默认已做配置。总是在使用 su 切换用户时初始化 PATH。

### 实现

通过修改/etc/login.defs 实现，配置如下：

```
ALWAYS_SET_PATH=yes
```

# 3 附录

介绍文件权限的含义和 `umask` 值的含义。

## 3.1 文件和目录权限含义

### 3.2 `umask` 值含义

## 3.1 文件和目录权限含义

Linux 系统中文件和目录权限用于限定谁能通过何种方式对文件和目录进行访问和操作。文件和目录的访问权限分为只读，只写和可执行三种。

有三种不同类型的用户可对文件和目录进行访问：

- 文件所有者：文件的创建者。
- 同组用户：与文件所有者在同一个属组的用户。
- 其他用户：与文件所有者不在同一个属组的用户。

文件和目录的权限含义通过以下例子说明：

假设 `/usr/src` 的权限为 `755`，将每位数字转化为二进制后为：111101101，含义如下：

- 左侧三个 bit 位 111 表示文件所有者的权限依次为：可读、可写、可执行。
- 中间三个 bit 位 101 表示同组用户的权限依次为：可读、不可写、可执行。
- 右侧三个 bit 位 101 表示其他用户的权限依次为：可读、不可写、可执行。

## 3.2 `umask` 值含义

当用户新创建文件或目录时，该文件或目录具有一个缺省权限。该缺省权限由 `umask` 值来指定。

`umask` 值代表的是权限的“补码”，即用缺省最大权限值减去 `umask` 值得到实际权限值。文件的缺省最大权限为可读可写，目录的缺省最大权限为可读可写可执行。即一个文件的实际缺省权限为 `666` 减去 `umask` 值。目录的实际缺省权限为 `777` 减去 `umask` 值。