Huawei Cloud EulerOS (HCE)

产品介绍

文档版本	01
发布日期	2025-09-05

华为云计算技术有限公司

商标声明


和其他华为商标均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。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 什么是 Huawei Cloud EulerOS

定义

Huawei Cloud EulerOS(简称HCE)是基于openEuler构建的云上操作系统，中文名为华为云欧拉操作系统。

HCE打造云原生、高性能、高安全、易维护等能力，加速用户业务上云，提升用户的应用创新空间，可替代CentOS、EulerOS等公共镜像。

Huawei Cloud EulerOS 镜像

发行版	镜像名称	镜像说明
Huawei Cloud EulerOS 2.0	Huawei Cloud EulerOS 2.0 标准版 64位 x86版	支持x86架构的默认标准镜像。
Huawei Cloud EulerOS 2.0	Huawei Cloud EulerOS 2.0 标准版 64位 Arm版	支持Arm架构的默认标准镜像。
Huawei Cloud EulerOS 1.1	Huawei Cloud EulerOS 1.1 CentOS兼容版 64位	支持x86架构的兼容CentOS 7.9镜像。 **说明** 仅在新加坡区域发布。

2 产品优势

- 华为云服务垂直整合：联合华为云擎天平台垂直优化、GuestOS/HostOS协同，提升应用性能，打造弹性云服务器、云容器引擎、弹性负载均衡、数据库等服务优选竞争力。
- 云原生混合部署的最佳实践：支持容器化应用的混合部署，优化云原生环境中的资源利用效率，致力于打造行业领先的资源配置方案；提供低资源占用、快速启动以及高效资源利用的云原生基础设施。
- 高效快速部署：加速虚拟机启动，提升批量部署效率。
- 安全可信：支持SM2等国密算法；具备等保2.0/CC EAL4+安全能力。
- 基于openEuler生态：国内最活跃OS开源社区，Linux社区贡献持续多年TOP5，内核贡献突出。HCE支持南北向主流软硬件，可完全替代CentOS。
- OS开箱即用：支持安装KooCLI，提供**通过CLI调用云服务API**的方法；支持安装管理鸿蒙SDK的工具sdkmgr，方便远程管理鸿蒙SDK，实现端云开发者协同。

3 应用场景

- 弹性云服务器实例下首选HCE，以优化资源利用率并实现用户业务的高性能需求。

  适用于政企、金融、制造等传统用户上云，第三方云迁移到华为云等场景。用户购买弹性云服务器服务后，可部署自有应用。

  - HCE针对弹性云服务器做了应用优化。在HCE中部署数据库、大数据、HPC、虚拟化、容器等应用时，MySQL服务性能和Nginx服务性能比部署在其他操作系统上有明显提升。
  - HCE针对弹性云服务器做了快速启动优化。HCE根据弹性云服务器配置场景按需加载基础组件，启动更快速。

- 云容器引擎实例下首选HCE，实现企业降本增效。

  当前用户在线、离线业务分离部署，导致资源闲置现象严重，整体资源利用率偏低，亟需降本增效。

  - HCE结合云容器引擎做了CPU利用率优化。HCE采用混部引擎技术和隔离技术可使云容器引擎的CPU利用率达到40%-60%，并且QoS<1%，应用不卡顿，体验更流畅。
  - HCE结合云容器引擎做了弹性优化。基于云容器引擎，HCE提供包含最小组件集合的镜像。

- HCE支持替代CentOS。

  CentOS停服影响用户存量局点运维和新建局点建设，用户亟需替代方案。

  - 安全可靠：HCE支持等保2.0安全规范；支持EAL4+级别CC认证；支持SM2等国密算法。
  - 自主可控：HCE作为华为云自研操作系统，可完全替代CentOS。HCE兼容openEuler南北向生态，同时又具备云上的生态能力。

- 云和端生态协同。

  HCE同时支持云侧和端侧开发应用，是云端协同的最佳选择。

  云和端应用开发功能互相协同（例如通过API实现云端交互），业务运行时资源按需弹性扩展，让应用同时具备云和端的优势。

4 产品功能

- HCE 2.0选择Linux kernel 5.10作为HCE的内核，为云上应用程序环境提供企业级高可靠性保障，并同步更新Linux社区的最新功能。
- 支持云原生调度增强、内存分级扩展，支持操作系统迁移、兼容性评估。
- 支持SM2等国密算法，等保2.0/CC EAL4+安全能力。
- HCE 2.0提供gcc 10.3、binutils 2.37、glibc 2.34编译器，增强稳定性并提高与其它软件的兼容性。
- 对x86、Arm等平台进行功能适配、性能调优和稳定性加固，保证操作系统在各平台都能稳定可靠地长期运行。
- 兼容常见的开源软件，如Apache、MySQL、Tomcat、Nginx、Flink等，便于客户高效部署业务。

5 支持迁移的公共镜像

支持迁移的公共镜像和HCE对应关系如下所述。

表 5-1 支持迁移的 x86 公共镜像

OS发行系列	源操作系统	目标操作系统
HCE	64bit：Huawei Cloud EulerOS 1.1	Huawei Cloud EulerOS 2.0 标准版 64位
EulerOS	64bit：EulerOS：2.11/2.10/2.9/2.5/2.2	Huawei Cloud EulerOS 2.0 标准版 64位
CentOS	64bit：CentOS 7：7.9/7.8/7.7/7.6/7.5/7.4/7.3/7.2/7.1/7.0 64bit：CentOS 8：8.3/8.2/8.1/8.0	Huawei Cloud EulerOS 2.0 标准版 64位
	64bit：CentOS 7.9	Huawei Cloud EulerOS 1.1 CentOS兼容版

表 5-2 支持迁移的 Arm 公共镜像

OS发行系列	源操作系统	目标操作系统
EulerOS	64bit：EulerOS：2.11/2.10/2.9/2.8 64bit：CentOS 7：7.9/7.8/7.6/7.5 64bit：CentOS 8：8.2	Huawei Cloud EulerOS 2.0 标准版 64位 Arm版、

6 支持的实例规格

Huawei Cloud EulerOS支持部分弹性云服务器实例规格，请根据需要选择合适的实例规格。

说明

不同区域支持的弹性云服务器实例规格存在差异，以控制台实际显示为准。对于控制台未显示的实例规格，表示该区域不支持此实例规格。

- Huawei Cloud EulerOS 2.0镜像镜像支持Flexus X实例、Flexus L实例和弹性云服务器实例。

  弹性云服务器支持的的实例规格如下表所示。

  表 6-1 支持的弹性云服务器实例规格

弹性云服务器实例类型	支持的规格族
通用计算型	s7/s6/x1
通用计算增强型	c7/c6s/c6/x1e
内存优化型	m7/m6
超大内存型	e6
磁盘增强型	d6/d7

- Huawei Cloud EulerOS 1.1 支持实例规格如下所述。

  表 6-2 支持的弹性云服务器实例规格

弹性云服务器实例类型	支持的规格族
通用计算型	s6
通用计算增强型	c6s/c6
内存优化型	m6

弹性云服务器实例类型	支持的规格族
磁盘增强型	d6

7 支持计划

HCE采用2+4+2生命周期模式：

- 2年的全面支持：提供免费的软件维护和技术支持，包括对新硬件（CPU、磁盘、网卡等）、新特性的兼容性支持、问题修复和CVE安全漏洞修复。
- 4年的扩展支持：提供免费的软件维护和技术支持，仅包括问题修复和CVE安全漏洞修复。
- 2年的延长支持（可选）：仅提供部分软件包的问题修复和CVE安全漏洞修复，需额外付费。

开源软件声明

HCE提供开源软件声明：

开源软件许可证由各自的权利持有者授予。开源许可证优先于产品中包含的相应开源软件的所有其他许可证信息，包括但不限于最终用户软件许可协议。本通知代表华为技术有限公司及其可能在您所在国家/地区向您提供本产品的任何当地子公司提供。

Huawei Cloud EulerOS 2.0开源软件声明**下载地址**。

8 计费说明

HCE初期是免费镜像，无需购买即可使用。后期按照**HCE支持计划**分阶段提供不同程度的软件维护和技术支持，会产生相应的费用。

当您选用HCE镜像创建弹性云服务器实例时，需要支付其他资源产生的费用，如vCPU、内存、存储、公网IP和带宽等。

弹性云服务器计费详情，请参见**计费说明**。

9 安全

9.1 安全启动

安全启动

通过安全启动（SecureBoot）可以保证系统启动过程中各个部件的完整性，防止没有经过合法签名的部件被加载运行，从而防止对系统及用户数据产生安全威胁并防御bootkit和rootkit攻击。HCE支持安全启动。

- 查看是否开启SecureBoot

  HCE启动成功后，可以使用下面命令判断SecureBoot是否启用。

  ```
  mokutil --sb-state
  SecureBoot enabled   #SecureBoot已启用
  ```

- 启用kernel ko签名校验

  安全启动通过校验签名来实现。HCE的内核默认未编译强制启用签名校验，需要通过kernel的启动参数module.sig_enforce进行控制。

  启用ko签名校验：

  - 对于EFI启动的机器：修改/boot/efi/EFI/hce/grub.cfg文件，增加启动参数module.sig_enforce=1。
  - 对于BIOS启动的机器：修改/boot/grub2/grub.cfg文件，增加启动参数module.sig_enforce=1。

  图 9-1 启用 ko 签名校验

  ```
          echo    'Loading Linux 5.10.0-60.18.0.50.r509_2.hce2.x86_64 ...'
          linux   /vmlinuz-5.10.0-60.18.0.50.r509_2.hce2.x86_64 root=/dev/mapper/hce-root ro crashk
  ernel=512M resume=/dev/mapper/hce-swap rd.lvm.lv=hce/root rd.lvm.lv=hce/swap crash_kexec_post_not
  ifiers panic=3 nmi_watchdog=1 quiet rd.shell=0 module.sig_enforce=1
          echo    'Loading initial ramdisk ...'
          initrdefi /initramfs-5.10.0-60.18.0.50.r509_2.hce2.x86_64.img
  ```

Kernel参数	值	说明
module.sig_enforce	0	关闭内核对ko模块的校验，重启生效。
	1	开启内核对ko模块的校验，重启生效。

- HCE 2.0签名公钥证书

  https://repo.huaweicloud.com/hce/2.0/updates/x86_64/Packages/路径下的hce-sign-certificate-1.0-2.hce2.x86_64.rpm。

- BIOS证书导入参考：

  鲲鹏服务器：https://support.huawei.com/enterprise/zh/doc/EDOC1100088653/97a0d5a0

  2288H V5：https://support.huawei.com/enterprise/zh/doc/EDOC1000163371/afc5c7f8?idPath=23710424|251364409|21782478|21872244

  2288H V6：https://support.huawei.com/enterprise/zh/doc/EDOC1100195299/fdb56216?idPath=23710424|251364409|21782478|23692812

⚠ 注意

在服务器安装了2025年3月份之前的HCE2.0版本并开启安全启动的情况下，如果打算升级到2025年5月份之后的HCE2.0版本或者单独升级shim，grub，kernel包，可能存在升级重启后，系统无法引导启动的问题。在升级OS前，可参考【常见问题】中的**如何解决证书切换导致的安全启动失败问题**章节中的【排查方法】提前进行排查。如果已经升级OS，并发生无法引导启动的问题，可参考【常见问题】中**如何解决证书切换导致的安全启动失败问题**章节中的【解决方案】进行解决。

9.2 安全加固工具

概述

HCE作为面向华为云用户的通用Linux发行版，默认发布的OS ISO安装后未进行安全加固。

security-tool是自研的符合华为相关基础安全加固要求的加固工具包，默认不随HCE安装，当需要执行加固时选择性安装，安装完成后在OS首次启动时执行自动化加固。

详细加固内容如下：

- 系统服务：例如SSH配置、删除postfix.service、启用haveged.service
- 内核参数：例如内核网络协议栈加固
- 账号口令：例如PAM参数加固
- 授权认证：例如warning banner、umask
- 文件权限：例如cron配置

使用场景

security-tool 工具当前支持2种配置：cybersecurity（等保加固配置）和general（通用加固配置）。

使用 security-tool 工具进行安全加固

步骤1 安装security-tool工具包。

若repo源中有该工具包，则可直接使用yum命令进行安装。

```
yum install -y security-tool
```

若没有，则可在华为云官网 repo 源获取 security-tool 工具包：**https://repo.huaweicloud.com/hce/2.0/updates/**。

步骤2 在/etc/hce_security/hce_enhance_type.conf中写入需要加固的配置类型。

当前支持2种配置：cybersecurity（等保加固配置）、general（通用加固配置），推荐使用general（通用加固配置）。本示例以general为例。

```
echo general > /etc/hce_security/hce_enhance_type.conf
```

步骤3 启动 hce-security服务。

```
systemctl start hce-security
```

执行完成后使用systemctl status hce-security查看服务状态，状态为 active(exited)即为加固成功。

图 9-2 查看服务状态

```
[root@localhost ~]# systemctl status hce-security
● hce-security.service - HCE Security Tool
     Loaded: loaded (/usr/lib/systemd/system/hce-security.service; disabled; vendor preset: disabled)
     Active: active (exited) since Sat 2023-10-28 14:13:09 CST; 7min ago
    Process: 42457 ExecStart=/usr/sbin/hce_security-tool.sh (code=exited, status=0/SUCCESS)
   Main PID: 42457 (code=exited, status=0/SUCCESS)
```

加固日志见/var/log/hce_security.log。

用户可自行修改 /etc/hce_security/usr-security.conf 配置自己的加固项，完成个性化加固，配置文件具体修改方式如下：

```
################################################################################
#
# HowTo:
#       # delete key, and difference caused by blankspace/tab on key is ignored
#       id@d@file@key
#
#       # modify option: find line started with key, and get the value changed
#       id@m@file@key[@value]
#
#       # modify sub-option: find line started with key, and then change the value of key2 to
value2(prepostive separator should not be blank characters) in the line
#       id@M@file@key@key2[@value2]
#
#       # check existence of commands
#       id@which@command1 [command2 ...]
#
#       # execute command on the files found
#       id@find@dir@condition@command
#
#       # any command(with or without parameter), such as 'rm -f','chmod 700','which','touch', used to
extend functions, return 0 is ok
#       id@command@file1 [file2 ...]
#
# Notes:
#       1. The comment line should start with '#'
#       2. "value" related with "key" should contain prepositive separator("=" " and so on), if there is any.
#       3. When item starts with "d", "m" or "M", "file" should be a single normal file, otherwise multi-
objects(separated by blankspace) are allowed.
#
################################################################################
```


如果云服务希望执行更多的安全加固项目，可以参考或华为云其他OS安全加固规范。

----结束

说明

SElinux开启会影响系统性能，HCE2.0默认关闭。启用SElinux需要多次重启操作系统，不具备一键开启的能力，如果需要开启，请参考**如何开启HCE操作系统的SELinux功能?** 。

general 与 cybersecurity 的差异

检查项类型	检查项名称	检查内容	general	cybersecurity	是否默认满足
初始配置	文件系统配置	应当对系统关键目录进行分区挂载	-	-	否
		确保禁用不需要的文件系统	-	-	否
		确保无需修改的分区以只读方式挂载	-	-	否
		确保无需挂载设备的分区以nodev方式挂载	-	-	否
		确保无可执行文件的分区以noexec方式挂载	-	-	否
		确保无需SUID和SGID的分区以nosuid方式挂载	-	-	否
		避免使用USB存储	√	-	是
	软件服务配置	禁止安装X Window系统	-	-	是
		禁止启用debug-shell服务	√	-	是
		禁止启用rsync服务	√	-	是
		禁止启用avahi服务	√	-	是
		禁止启用SNMP服务	√	-	是
		禁止启用squid服务	√	-	是
		避免启用samba服务	√	-	是
		禁止启用FTP服务	√	-	是
		禁止启用TFTP服务	√	-	是

		禁止启用DNS服务	√	-	是
		禁止启用NFS服务	√	-	是
		禁止启用rpcbind服务	√	√	否
		禁止启用LDAP服务	√	-	是
		禁止启用DHCP服务	√	-	是
		禁止安装CUPS服务软件	-	-	是
		禁止安装NIS服务软件	-	-	是
		禁止安装telnet软件	-	-	是
		禁止安装NIS客户端	-	-	是
		禁止安装LDAP客户端	-	-	是
		禁止安装调测类工具	-	-	是
		禁止安装开发编译类工具	-	-	是
		禁止安装网络嗅探类工具	-	-	是
	软件升级配置	确保配置GPG公钥	-	-	是
		确保配置启用gpgcheck	-	-	是
		确保配置软件仓库源	-	-	是
	文件完整性检查	确保安装AIDE	-	-	否
		应当定期检查文件完整性	-	-	否
	通用进程加固	确保启用ASLR	√	-	是
		确保core dump配置正确	√	-	是
		应当合理限制用户可打开文件数量	-	-	否
		确保链接文件保护配置正确	√	-	是
		确保dmesg访问权限配置正确	√	-	否
		确保内核符号地址受限访问	√	-	是

		应当合理限制进程ptrace能力	-	-	否
		禁止全局加解密策略配置为LEGACY	-	-	是
系统服务	时间同步服务	应当正确配置ntpd服务	-	-	否
		应当正确配置chronyd服务	-	-	是
	定时任务服务	确保cron服务正常运行	√	-	是
		确保cron配置权限正确	√	-	否
	SSH服务	确保/etc/ssh/sshd_config权限配置正确	√	-	是
		确保SSH私钥文件权限配置正确	√	√	否
		确保SSH公钥文件权限配置正确	√	√	否
		确保启用IgnoreRhosts	√	-	是
		应当合理配置认证黑白名单	-	-	否
		确保SSH使能PAM认证	√	-	是
		禁止SSH root登录	-	√	否
		禁止SSH空口令登录	√	-	是
		禁止使用HostbasedAuthentication	√	-	是
		确保配置Warning Banner文件路径	√	-	否
		确保正确配置SSH日志级别	√	-	是
		应当配置SSH服务侦听IP	-	-	否
		应当正确配置SSH并发未认证连接数	√	-	否
		禁止使用X11Forwarding	√	-	否
		应当配置SSH MaxSessions不超过10	√	-	是

		应当正确配置MaxAuthTries	√	-	否
		禁止使用PermitUserEnvironment	√	-	是
		应当配置LoginGraceTime不超过60秒	√	-	否
		确保配置空闲超时间隔时间	√	-	否
		禁止使用AllowTcpForwarding	√	-	否
		确保SSH KexAlgorithms配置强算法	√	-	是
		确保SSH MACs配置强算法	√	-	是
		确保SSH Ciphers配置强算法	√	-	是
		禁止配置SSH将弃用的选项	√	-	是
网络服务	禁用不使用的网络协议和设备	避免使用不常见网络协议	-	-	否
		避免使用无线网络	-	-	是
	内核网络协议栈	禁止系统响应ICMP广播报文	√	-	是
		禁止接收ICMP重定向报文	√	-	否
		禁止转发ICMP重定向报文	√	-	是
		应当忽略所有ICMP请求	-	-	否
		确保忽略伪造的ICMP报文	√	-	是
		确保启用反向地址过滤	√	-	否
		禁止IP转发	√	-	是
		禁止接收源路由报文	√	-	否
		确保启用TCP-SYN cookie保护	√	-	是

		应当启用日志记录可疑的网络包	√	-	否
		避免启用tcp_timestamps	-	-	否
		确保TIME_WAIT TCP协议等待时间已配置	√	-	是
		应当合理配置SYN_RECV状态队列数量	-	-	否
		禁止使用ARP代理	-	-	是
防火墙配置	配置firewalld服务	应当启用firewalld服务	-	-	是
		确保iptables未启用	-	-	是
		确保nftables未启用	-	-	是
		应当配置正确的默认区域	-	-	否
		应当确保网络接口绑定正确区域	-	-	否
		避免开启不必要的服务和端口	-	-	否
	配置iptables服务	应当启用iptables服务	-	-	否
		确保firewalld未启用	-	-	否
		确保nftables未启用	-	-	是
		应当正确配置iptables默认拒绝策略	-	-	否
		应当正确配置iptables loopback策略	-	-	否
		应当正确配置iptables INPUT策略	-	-	否
		应当正确配置iptables OUTPUT策略	-	-	否
		应当正确配置iptables INPUT、OUTPUT关联策略	-	-	否
	配置nftables服务	应当启用nftables服务	-	-	否
		确保iptables未启用	-	-	是
		确保fireweallld未启用	-	-	否

		应当配置nftables默认拒绝策略	-	-	否
		应当配置nftables loopback策略	-	-	否
		应当正确配置nftables input策略	-	-	否
		应当正确配置nftables output策略	-	-	否
		应当正确配置nftables input、output关联策略	-	-	否
日志审计	auditd	确保auditd审计已启用	√	-	是
		应当在启动阶段启用auditd	-	-	否
		应当正确配置audit_backlog_limit	-	-	否
		确保配置单个日志大小限制	-	-	是
		确保审计日志rotate已启用	-	-	否
		确保审计日志不被自动删除	-	-	是
		应当合理配置磁盘空间阈值	-	-	是
		避免配置审计日志限速阈值过小	-	-	是
		应当配置sudoers审计规则	-	√	否
		应当配置登录审计规则	-	-	是
		应当配置会话审计规则	-	-	是
		应当配置时间修改审计规则	-	√	否
		应当配置SELinux审计规则	-	-	否
		应当配置网络环境审计规则	-	√	否
		应当配置文件访问控制权限审计规则	-	-	否

		应当配置文件访问失败审计规则	-	-	否
		应当配置文件删除审计规则	-	-	否
		应当配置账号信息修改审计规则	-	√	否
		应当配置文件系统挂载审计规则	-	-	否
		应当配置提权命令审计规则	-	-	否
		应当配置内核模块变更审计规则	-	-	是
		应当配置修改sudo日志文件审计规则	-	-	否
	rsyslog	确保rsyslog服务已启用	√	√	否
		确保系统认证相关事件日志已记录	-	-	是
		确保cron服务日志已记录	√	-	是
		应当正确配置各服务日志记录	-	-	是
		应当正确配置rsyslog默认文件权限	√	√	否
		确保rsyslog日志rotate已配置	-	-	否
		应当配置发送日志到远程日志服务器	-	-	否
		应当仅在指定的日志主机上接收远程rsyslog消息	-	-	否
		确保rsyslog转储journald日志已配置	-	-	否
账号与口令管理	账号管理	禁止无需登录的账号拥有登录能力	-	-	否
		禁止存在不使用的账号	-	-	否
		应当正确设置账号有效期	-	-	否

		禁止存在UID为0的非root账号	-	-	是
		确保UID唯一	-	-	是
		确保GID唯一	-	-	是
		确保账号名唯一	-	-	是
		确保组名唯一	-	-	是
		确保/etc/passwd中的组都存在	-	-	是
		确保账号拥有自己的Home目录	-	-	是
		确保账号Home目录权限是750或更严格	-	-	是
		避免账号Home目录下存在.forward文件	-	-	是
		避免账号Home目录下存在.netrc文件	-	-	是
		确保用户PATH变量被严格定义	-	-	是
	口令管理	确保配置口令复杂度	√	√	否
		确保限制重用历史口令次数	√	√	否
		确保口令中不包含账号字符串	-	-	是
		确保口令使用SHA512算法加密	√	√	否
		确保口令过期时间设置正确	√	√	否
		确保口令过期告警时间设置正确	√	-	是
		应当设置口令修改周期设置正确	√	√	否
		确保不活跃口令锁定时间不超过30天	√	-	是
		确保Grub已设置口令保护	-	-	是
		确保单用户模式已设置口令保护	-	-	是

身份认证	登录管理	确保登录失败一定次数后锁定账号	√	√	否
		避免root用户本地接入系统	-	-	否
		确保会话超时时间设置正确	√	√	否
	确保Warning Banner包含合理的信息	确保本地登录Warning Banner包含合理的信息	√	-	否
		确保远程登录Warning Banner包含合理的信息	√	-	否
		确保motd文件包含合理的信息	√	-	否
		确保/etc/issue权限配置正确	√	-	是
		确保/etc/issue.net权限配置正确	√	-	是
		确保/etc/motd权限配置正确	√	-	是
访问控制	SELinux	应当启用enforce模式	-	-	是
		应当正确配置SELinux策略	-	-	是
		避免标签为unconfined_service_t的服务存在	-	-	否
		确保SETroubleshoot服务未安装	-	-	是
		确保MCS转换服务未安装	-	-	是
	特权命令	确保su受限使用	√	√	否
		确保su命令继承用户环境变量不会引入提权	√	√	否
		确保普通用户通过sudo运行特权程序	-	-	否
		确保配置sudo日志文件	√	-	否
		禁止使用SysRq键	-	-	否

	系统文件权限	确保/etc/passwd权限配置正确	√	-	是
		确保/etc/passwd-权限配置正确	√	-	是
		确保/etc/shadow权限配置正确	√	-	是
		确保/etc/shadow-权限配置正确	√	-	是
		确保/etc/group权限配置正确	√	-	是
		确保/etc/group-权限配置正确	√	-	是
		确保/etc/gshadow权限配置正确	√	-	是
		确保/etc/gshadow-权限配置正确	√	-	是
		确保全局可写目录已设置sticky位	-	-	是
		禁止存在无属主或属组的文件或目录	-	-	是
		禁止存在全局可写的文件	-	-	是
		禁止存在空链接文件	-	-	是
		禁止存在隐藏的可执行文件	-	-	是
		确保删除文件非必要的SUID和SGID位	-	-	是
		确保umask是027或更严格	√	√	否

说明

- “√”表示执行。
- “-”表示不执行。

10 镜像更新记录

公共镜像更新记录分为x86架构和Arm架构，具体参考如下：

x86架构公共镜像的更新记录请参见**镜像更新记录（x86）**。

Arm架构公共镜像的更新记录请参见**镜像更新记录（Arm）**。