HCE 用户指南

文档版本 01

发布日期 2024-12-02

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

Huawei Cloud EulerOS（简称HCE）是基于openEuler构建的云上操作系统。

HCE打造云原生、高性能、高安全、易迁移等能力，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	支持x86架构的默认标准镜像。
Huawei Cloud EulerOS 2.0	Huawei Cloud EulerOS 2.0 等保2.0三级版 64位	基于x86架构默认标准镜像进行等保加固的镜像版本，该镜像符合等保2.0三级安全保护的基本要求。详情请参见**Huawei Cloud EulerOS 2.0 等保2.0三级版镜像概述**。
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 2.0	Huawei Cloud EulerOS 2.0 等保2.0三级版 64位 Arm版	支持Arm架构的等保2.0三级版镜像。
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。
- 云原生混部优选体验：支持容器应用混部，打造业界优选的云原生资源利用效率；提供占用资源少、启动速度快、资源利用率高的云原生基础设施。
- 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，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5年TOP5，5.10内核贡献TOP1；南北向主流软硬件支持，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，实现用户业务高性能。

  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结合弹性云服务器做了应用优化。在HCE操作系统中部署数据库、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结合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。

  用户当前在线、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EAL 4+级别CC认证；支持SM2等国密算法。
  - 自主可控：HCE是华为云自研操作系统，可完全替代CentOS。HCE继承openEuler生态，同时又增加云上的生态能力。
- 云和端生态协同。

  HCE同时支持云侧和端侧开发应用，是云端协同的优选选择。

  云和端应用开发功能互相协同（例如通过API实现端云交互），业务运行时资源按需弹性扩展，让应用同时具备端和云的优势。

4 产品功能

- 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。
- 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Intel、AMD、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，帮助客户高效部署业务。

5 支持迁移的公共镜像

支持迁移的公共镜像和HCE系统的对应关系如下所述。

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：2.10/2.9/2.5/2.3/2.2	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 8：8.5/8.4/8.3/8.2/8.1/8.0	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：2.10/2.9/2.8/2.3	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 常用软件兼容性

HCE 2.0兼容openEuler 22.03 LTS版本兼容列表下的所有开源软件，详情请参见**oepkgs官网**。

在此基础上，HCE 2.0额外兼容以下软件：

表 7-1 HCE 2.0 软件兼容列表

架构	软件名称	操作系统	版本
x86_64	Tomcat	HCE 2.0	5.5.36
		HCE 2.0	6.0.28
		HCE 2.0	6.0.53
		HCE 2.0	7.0.54
		HCE 2.0	7.0.68
		HCE 2.0	7.0.76
		HCE 2.0	7.0.92
		HCE 2.0	7.0.107
		HCE 2.0	7.0.109
		HCE 2.0	8.0.53
		HCE 2.0	8.5.50
		HCE 2.0	8.5.56
		HCE 2.0	8.5.57
		HCE 2.0	8.5.58
		HCE 2.0	8.5.59
		HCE 2.0	8.5.60
		HCE 2.0	8.5.61

架构	软件名称	操作系统	版本
		HCE 2.0	8.5.73
		HCE 2.0	8.5.88
		HCE 2.0	8.5.93
		HCE 2.0	8.5.99
		HCE 2.0	9.0.10
		HCE 2.0	9.0.14
		HCE 2.0	9.0.37
		HCE 2.0	9.0.52
		HCE 2.0	9.0.58
		HCE 2.0	9.0.64
		HCE 2.0	9.0.78
		HCE 2.0	9.0.91
		HCE 2.0	10.0.10
		HCE 2.0	10.0.16
x86_64	Nginx	HCE 2.0	1.12.2
		HCE 2.0	1.13.1
		HCE 2.0	1.16.1
		HCE 2.0	1.18.0
		HCE 2.0	1.20.1
		HCE 2.0	1.20.2
		HCE 2.0	1.21.5
		HCE 2.0	1.22.0
		HCE 2.0	1.22.1
		HCE 2.0	1.23.0
		HCE 2.0	1.23.1
		HCE 2.0	1.23.2
		HCE 2.0	1.23.3
		HCE 2.0	1.24.0
		HCE 2.0	1.25.0

架构	软件名称	操作系统	版本
x86_64	.net	HCE 2.0	.net 5 for Linux
		HCE 2.0	.net 6 for Linux
		HCE 2.0	.net 7 for Linux
		HCE 2.0	.net 8 for Linux
x86_64	Jetty	HCE 2.0	9.4.15
		HCE 2.0	9.4.16
		HCE 2.0	9.4.31
		HCE 2.0	9.4.40
x86_64	openjdk	HCE 2.0	1.7.0
		HCE 2.0	1.8.0
		HCE 2.0	11
		HCE 2.0	17
x86_64	Keepalived	HCE 2.0	2.1.5
		HCE 2.0	2.2.4
x86_64	Springboot	HCE 2.0	1.5.19
		HCE 2.0	2.0.3
		HCE 2.0	2.2
		HCE 2.0	2.3.9
x86_64	Kafka	HCE 2.0	2.6.0
		HCE 2.0	2.7.2
		HCE 2.0	2.8.2
		HCE 2.0	3.0.0
		HCE 2.0	3.1.2
		HCE 2.0	3.2.3
		HCE 2.0	3.3.1
		HCE 2.0	3.3.2
		HCE 2.0	3.4.0
		HCE 2.0	3.4.1
		HCE 2.0	3.5.1
		HCE 2.0	3.7.1

架构	软件名称	操作系统	版本
x86_64	RabbitMQ	HCE 2.0	3.9.10
		HCE 2.0	3.10.1
		HCE 2.0	3.11.0
		HCE 2.0	3.11.28
		HCE 2.0	3.12.0
		HCE 2.0	3.12.4
		HCE 2.0	3.12.9
		HCE 2.0	3.12.13
		HCE 2.0	3.13.0
		HCE 2.0	3.13.2
		HCE 2.0	3.13.5
		HCE 2.0	3.13.6
x86_64	Zookeeper	HCE 2.0	3.5.5
		HCE 2.0	3.5.7
		HCE 2.0	3.5.9
		HCE 2.0	3.5.10
		HCE 2.0	3.6.1
		HCE 2.0	3.6.2
		HCE 2.0	3.6.4
		HCE 2.0	3.7.0
		HCE 2.0	3.7.2
		HCE 2.0	3.8.0
		HCE 2.0	3.8.4
		HCE 2.0	3.9.0
		HCE 2.0	3.9.2
x86_64	spring-cloud-gateway	HCE 2.0	2.1.3
		HCE 2.0	2.2
		HCE 2.0	3.1.4
x86_64	ElasticSearch	HCE 2.0	6.8.23
		HCE 2.0	7.5.1

架构	软件名称	操作系统	版本
		HCE 2.0	7.6
		HCE 2.0	7.6.1
		HCE 2.0	7.7.0
		HCE 2.0	7.7.1
		HCE 2.0	7.8
		HCE 2.0	7.9.0
		HCE 2.0	7.9.1
		HCE 2.0	7.9.2
		HCE 2.0	7.9.3
		HCE 2.0	7.10.0
		HCE 2.0	7.10.1
		HCE 2.0	7.11.2
		HCE 2.0	7.12.0
		HCE 2.0	7.12.1
		HCE 2.0	7.13.0
		HCE 2.0	7.13.1
		HCE 2.0	7.13.4
		HCE 2.0	7.14.0
		HCE 2.0	7.15.0
		HCE 2.0	7.15.2
		HCE 2.0	7.16.0
		HCE 2.0	7.16.1
		HCE 2.0	7.16.2
		HCE 2.0	7.16.3
		HCE 2.0	7.17.2
		HCE 2.0	7.17.6
		HCE 2.0	7.17.5
		HCE 2.0	7.17.7
		HCE 2.0	8.0.0
		HCE 2.0	8.3.3

架构	软件名称	操作系统	版本
		HCE 2.0	8.5.0
		HCE 2.0	8.8.0
		HCE 2.0	8.10.0
		HCE 2.0	8.14.3
x86_64	apollo	HCE 2.0	1.1.2
		HCE 2.0	1.2.0
		HCE 2.0	1.2.2
		HCE 2.0	1.4.1
x86_64	Minio	HCE 2.0	2023.01.31T02.24.19Z-91.1
		HCE 2.0	RELEASE.2023-10-07T15-07-38Z
		HCE 2.0	RELEASE.2023-12-23T07-19-11Z
		HCE 2.0	RELEASE.2024-01-16T16-07-38Z
		HCE 2.0	RELEASE.2024-04-28T17-53-50Z
		HCE 2.0	RELEASE.2024-07-16T23-46-41Z
x86_64	Kibana	HCE 2.0	5.1.1
		HCE 2.0	5.2.1
		HCE 2.0	5.6.16
		HCE 2.0	6.1.0
		HCE 2.0	6.2.0
		HCE 2.0	6.6.0
		HCE 2.0	6.8.23
		HCE 2.0	7.0.0
		HCE 2.0	7.10.1
		HCE 2.0	7.17.22
		HCE 2.0	8.1.0
		HCE 2.0	8.2.0

架构	软件名称	操作系统	版本
		HCE 2.0	8.3.0
		HCE 2.0	8.4.0
		HCE 2.0	8.6.0
		HCE 2.0	8.8.0
		HCE 2.0	8.10.1
		HCE 2.0	8.13.0
		HCE 2.0	8.14.13
x86_64	Prometheus	HCE 2.0	2.1.0
		HCE 2.0	2.3.2
		HCE 2.0	2.5.0
		HCE 2.0	2.6.0
		HCE 2.0	2.6.1
		HCE 2.0	2.7.1
		HCE 2.0	2.8.1
		HCE 2.0	2.9.2
		HCE 2.0	2.10.0
		HCE 2.0	2.11.2
		HCE 2.0	2.12.0
		HCE 2.0	2.13.1
		HCE 2.0	2.14.0
		HCE 2.0	2.15.2
		HCE 2.0	2.16.0
		HCE 2.0	2.17.0
		HCE 2.0	2.18.1
		HCE 2.0	2.19.3
		HCE 2.0	2.20.1
		HCE 2.0	2.22.2
		HCE 2.0	2.24.1
		HCE 2.0	2.29.1
		HCE 2.0	2.37.1

架构	软件名称	操作系统	版本
		HCE 2.0	2.45.6
		HCE 2.0	2.53.1
x86_64	rocketmq	HCE 2.0	5.1.4
x86_64	Redis	HCE 2.0	6.2.14
x86_64	MySQL	HCE 2.0	5.7.39
		HCE 2.0	8.0.28
		HCE 2.0	8.0.29
		HCE 2.0	8.0.35
		HCE 2.0	8.0.37
x86_64	postgres	HCE 2.0	15.7
x86_64	hadoop	HCE 2.0	3.3.5
x86_64	hive	HCE 2.0	3.1.3
x86_64	iceberg	HCE 2.0	1.2.0
x86_64	spark	HCE 2.0	3.3.2
x86_64	Flink	HCE 2.0	1.16.2
x86_64	eureka	HCE 2.0	3.2.0

8 HCE 支持计划

HCE采用2+4的生命周期模式，每一代版本给用户提供10年的生命周期：

说明

一代版本，例如HCE V2版本包含HCE 2.0以及之后的HCE 2.x版本。

- 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，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**。

9 计费说明

HCE初期是免费镜像，无须购买即可使用。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**。

10 安全

10.1 Huawei Cloud EulerOS 2.0 等保 2.0 三级版镜像概述

什么是 Huawei Cloud EulerOS 2.0 等保 2.0 三级版镜像

Huawei Cloud EulerOS 2.0等保2.0三级版镜像是基于Huawei Cloud EulerOS 2.0官方标准镜像，根据国家信息安全部发布的《 GB/T22239-2019信息安全技术网络安全等级保护基本要求 》中对操作系统提出的一些等级保护要求推出的镜像。

您使用本镜像可满足以下等保合规要求：

- 身份鉴别
- 访问控制
- 安全审计
- 入侵防范
- 恶意代码防范

等保镜像使用场景及优势

- 若您的业务需要满足国家网络安全等级保护制度要求，您可以选择使用该镜像。
- 选择Huawei Cloud EulerOS 2.0等保2.0三级版镜像可以帮助客户所建设云平台快速满足国家等保要求，通过等保检测评测，节省时间成本与人力成本。
- 企业满足等保需求且通过等保评测后，能够直观的向客户展示本企业信息系统的安全性，使得客户能够更加放心的与企业合作。

等保镜像计费

Huawei Cloud EulerOS 2.0等保2.0三级版镜像是免费镜像，无须购买即可使用。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。当您选用Huawei Cloud EulerOS 2.0等保2.0三级版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。计费详情，请参见**计费说明**。

HCE 2.0 等保 2.0 配置检查规则

Huawei Cloud EulerOS 2.0等保2.0三级版镜像对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范进行检查并加固。加固项如下所述。

检查项类型	检查项名称	检查内容
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	确保root是唯一的UID为0的账户。
		确保UID具有唯一的。
		确保GID是唯一的。
		确保账号名是唯一的。
		确保组名是唯一的。
		确保设置密码满足复杂度要求。
		确保限制重用历史密码的次数。
		确保定期更换密码，防止密码泄露被恶意长期利用。
		确保设置密码最短修改时间，防止多次修改继续使用近期旧密码。
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	确保配置登录失败锁定策略。
		确保设置空闲会话超时断开时间。
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	禁止Telnet等不安全的远程连接服务。
访问控制	a）应对登录的用户分配账户和权限。	确保管理员账号通过提权方式管理系统，避免直接通过root登录管理。
		确保账户umask为027或更严格。
	b）应重命名或删除默认账户，修改默认账户的默认口令。	禁止root账户通过SSH直接登录，需要用户提前创建其他管理账号。
		禁止无需登录的账号拥有登录能力。
		禁止SSH空密码登录。
		确保密码通过弱密码字典检测。
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在。	禁止存在不使用的账号。
		应当正确设置临时账号有效期。

	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	确保su命令受限使用，仅允许wheel组中的用户具有su的使用权限。
		确保su命令继承用户环境变量不会引入提权。
		确保管理用户通过sudo运行特权命令，检查/etc/sudoers配置sudo权限的用户，除管理员外不能所有用户都配置（ALL）权限。
	e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	禁止存在无属主或属组的文件或目录，根据需要重置为系统上的某个活动用户或删除。
		设置SSH主机公私钥文件的权限和所有权。
		确保每个用户的home目录权限设置为750或者更严格。
		确保删除文件非必要的SUID和SGID位。
	f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	检查重要文件，如访问控制配置文件和用户权限配置文件的权限，是否达到用户级别的粒度。
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	启用auditd服务。
		确保审计对系统sudoers的修改事件。
		确保审计修改系统时间事件。
		确保审计修改系统hosts、主机名、登录提示配置事件。
		确保审计用户和用户组信息事件。
		启用rsyslog服务。
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	满足启用安全审计功能检查项，即满足此项。
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	检查auditd日志大小、日志拆分、磁盘空间配置。
		检查是否支持将日志备份到日志服务器，请自行举证。
		确保rsyslog默认文件权限不超过640。
	d）应保护审计进程，避免受到未预期的中断。	确保auditd审计守护进程正常运行。
		确保rsyslog日志守护进程正常运行。

入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序。	卸载 X window、cups、ypbind、ypserv、telnet、openSLP等不常用或不安全软件。
	b）应关闭不需要的系统服务、默认共享和高危端口。	确保关闭不需要的系统服务、文件共享服务： debug-shell、avahi、snmp、squid、samba、ftp、tftp、postfix
		关闭21（FTP）、23（TELNET）、25（SMTP）、111（rpcbind）、427（openSLP）、631（CUPS）等高危端口。
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	应该配置SSH服务侦听IP地址，请根据实际部署情况选择性配置，如果只有1个网卡无需配置。
		应当配置认证黑白名单，请根据实际部署情况选择性配置，如果只有1个账号可以登录可以忽略本项。
	d）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	HSS和VSS的漏洞检测和修复功能可以满足。如果有其他漏洞检查方式，可自行举证并忽略此项。
	e）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	HSS入侵检测和告警功能可以满足。如果已有其他检测与告警方式，可自行举证并忽略此项。
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	检测是否安装使用HSS，如安装了其他防恶意代码软件，可自行举证并忽略此项。

10.2 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 2.0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 2.0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：修改/boot/efi/EFI/hce/grub.cfg文件，增加启动参数module.sig_enforce=1。

```
        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

  HCE 2.0 KEK证书和HCE 2.0 UEFI签名证书详见https://repo.huaweicloud.com/hce/2.0/updates/x86_64/Packages/路径下的hce-sign-certificate-1.0-1.hce2.x86_64.rpm。

11 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）**。

