Huawei Cloud EulerOS（HCE）

Service Overview

Issue 01

Date 2025-09-05

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is Huawei Cloud EulerOS?

Definition

Huawei Cloud EulerOS (HCE) is an openEuler-based cloud operating system.

HCE offers cloud native, high-performing, secure, and easy-to-maintain capabilities. This accelerates service migration to the cloud and promotes application innovation. You can use it to replace operating systems such as CentOS and EulerOS.

Huawei Cloud EulerOS Images

Version	Image	Description
Huawei Cloud EulerOS 2.0	Huawei Cloud EulerOS 2.0 Standard Edition (64-bit, x86)	x86-compatible standard image
Huawei Cloud EulerOS 2.0	Huawei Cloud EulerOS 2.0 Standard Edition (64-bit, Arm)	Arm-compatible standard image
Huawei Cloud EulerOS 1.1	Huawei Cloud EulerOS 1.1 CentOS-compatible Edition (64-bit)	x86-compatible CentOS 7.9 image **NOTE** This version is released only in the Singapore region.

2 Product Advantages

- Vertical integration of cloud services: HCE works with QingTian to provide synergy between guest and host OSs so that applications can perform better. Using HCE improves the competitiveness of Elastic Cloud Server (ECS), Cloud Container Engine (CCE), Elastic Load Balance (ELB), and database services.
- Cloud-native hybrid deployment: Online and offline containerized applications can be deployed in the same cluster to maximize resource utilization. This is an industry-leading resource allocation solution. You will get cloud-native infrastructure with less resource consumption, faster startup, and higher resource utilization.
- Efficient deployment: HCE helps VM start up faster. It improves the efficiency of batch deployment.
- Secure and reliable: The OS attains MLPS 2.0 and CC EAL4+ certifications.
- openEuler ecosystem: Huawei has been one of the top five contributors to Linux for many consecutive years and has made outstanding contribution to the Linux kernel. HCE supports mainstream southbound and northbound software and hardware. It is a great alternative to CentOS.
- Out-of-the-box OSs: KooCLI can be installed to **call cloud service APIs through the CLI**. A tool (sdkmgr) can be installed to remotely manage the HarmonyOS SDK for device-cloud developer collaboration.

3 Application Scenarios

- As the preferred choice for ECSs to improve resource utilization and achieve compelling service performance

  HCE is an excellent choice for enterprises, financial institutions, and manufacturers planning to deploy or migrate their applications and services to the cloud.

  - Application-specific optimization: When database, big data, HPC, virtualization, and container applications are deployed in HCE, MySQL and Nginx services deliver better performance than when they are deployed in other OSs.
  - Faster startup: Only required basic components are loaded to suit specific ECSs, so they can bootup faster.

- As the preferred choice for CCE containers to reduce costs and improve efficiency

  If online and offline services are deployed separately, lots of resources are left idle and the overall resource utilization is low.

  - Optimized CPU utilization: HCE uses a hybrid deployment engine and resource isolation technologies to ensure that the CPU usage of CCE containers reaches 40% to 60% while keeping the QoS lower than 1%. In this way, applications will not suffer from frame freezing and you can enjoy smoother experience.
  - Optimized auto scaling: HCE functions as an image that contains the minimum component set for CCE containers.

- As an alternative to CentOS

  The discontinuation of CentOS has created significant challenges for the O&M of existing sites and the construction of new sites. HCE is a good solution because it is:

  - Secure and reliable: HCE attains MLPS 2.0 and CC EAL4+ certifications.

- For cloud-device synergy

  HCE supports both cloud-based and device-side application development, making it an ideal choice for cloud-device synergy.

  Applications are developed in a way that the cloud and device sides work together (for example, APIs developed for device-cloud interaction), and

resources can be flexibly expanded on demand while services are running. This helps applications to gain the strengths of both device and cloud.

4 Functions

- Linux kernel 5.10 for HCE 2.0: The kernel delivers enterprise-class reliability and incorporates the latest Linux community-developed functions.
- Enhanced capabilities: Enhanced cloud native scheduling, hierarchical memory expansion, OS migration, and compatibility evaluation.
- Excellent security: The OS complies with SM series cryptographic algorithms (such as SM2) and attains MLPS 2.0/CC EAL4+ certification.
- Various compilers: HCE 2.0 provides the GCC 10.3, Binutils 2.37, and Glibc 2.34 compilers.. They can enhance the system stability and compatibility with other software.
- Interaction with mainstream architectures: The OS takes advantages of architectures such as x86 and Arm, in terms of function adaptation, performance improvement, and stability hardening, to keep running smoothly and reliably on any platform.
- Compatibility with mainstream open-source software: The OS is compatible with software such as Apache, MySQL, Tomcat, Nginx, and Flink, helping customers efficiently deploy services.

5 Public Images That Can Be Migrated

The following table lists the mapping between HCE and public images that can be migrated.

Table 5-1 x86 public images allowed to be migrated

OS Series	Source OS	Target OS
HCE	64-bit: Huawei Cloud EulerOS 1.1	Huawei Cloud EulerOS 2.0 Standard Edition (64-bit)
EulerOS	64-bit: EulerOS 2.11/2.10/2.9/2.5/2.2	Huawei Cloud EulerOS 2.0 Standard Edition (64-bit)
CentOS	64-bit: CentOS 7.9/7.8/7.7/7.6/7.5/7.4/7.3/7.2/7.1/7.0 64-bit: CentOS 8.3/8.2/8.1/8.0	Huawei Cloud EulerOS 2.0 Standard Edition (64-bit)
	64-bit: CentOS 7.9	Huawei Cloud EulerOS 1.1 CentOS-compatible Edition

Table 5-2 Arm public images allowed to be migrated

OS Series	Source OS	Target OS
EulerOS	64-bit: EulerOS 2.11/2.10/2.9/2.8 64-bit: CentOS 7.9/7.8/7.6/7.5 64-bit: CentOS 8.2	Huawei Cloud EulerOS 2.0 Standard Edition (64-bit, Arm)

6 Supported Instance Types

ECSs of the following types can run on Huawei Cloud EulerOS:

NOTE

ECS specifications vary by region. The actual specifications are displayed on the management console. If they are not displayed on the console, the instance specifications are not supported in that region.

- Huawei Cloud EulerOS 2.0 images can be used by FlexusX instances, FlexusL instances, and ECSs.

  The following table lists the supported ECS flavors.

  Table 6-1 Supported ECS types

ECS Type	Family
General computing ECSs	s7, s6, and x1
General computing-plus ECSs	c7, c6s, c6, and x1e
Memory-optimized ECSs	m7 and m6
Large-memory	e6
Disk-intensive	d6 and d7

- Huawei Cloud EulerOS 1.1

  Table 6-2 Supported ECS types

ECS Type	Family
General computing ECSs	s6
General computing-plus ECSs	c6s and c6
Memory-optimized ECSs	m6
Disk-intensive	d6

7 Support Plans

HCE provides the "2+4+2" lifecycle mode.

- 2-year mainstream support: Free software maintenance and technical support are provided, including compatibility support (compatibility with new features and new hardware such as CPUs, disks, and NICs), troubleshooting, and CVE fixing.
- 4-year extended support: Free software maintenance and technical support are provided, but only for troubleshooting and CVE fixing.
- (Optional) 2-year beyond end of support: Only troubleshooting and CVE fixing are provided for some software packages, with payment required.

Open-Source Software Notice

HCE provides an open source software notice along with the product.

Open source software licenses are granted by their holders. Open source licenses prevail all other license information with regard to the respective open source software contained in the product, including but not limited to the *End User Software Licensing Agreement*. This notice is provided on behalf of Huawei Technologies Co., Ltd. and any of its local subsidiaries which may have provided this product to you in your local country.

Download the *Huawei Cloud EulerOS 2.0 Open Source Software Notice*.

8 Billing

HCE images are currently free. Later, Huawei will provide **support plans** for HCE, including software maintenance and technical support services for different phases. These support services will generate billable expenses.

Although the OS is free, when you use an HCE image to create an ECS, you still need to pay for the required resources, such as vCPUs, memory, storage, public IP address, and bandwidth.

For details, see **Billing**.

9 Security

9.1 Secure Boot

Secure Boot

Secure Boot ensures the integrity of each component during system boot-up and prevents components that have no valid signatures from being loaded. It protects the system and user data from security threats as well as bootkit and rootkit attacks. HCE supports Secure Boot.

- Verifying that Secure Boot has been enabled

  After the OS is booted, run the following command to check whether Secure Boot is enabled:

  ```
  mokutil --sb-state
  SecureBoot enabled #Secure Boot has been enabled.
  ```

- Enabling kernel .ko signature verification

  Secure Boot is implemented by signature verification. By default, the HCE kernel is not compiled with forcibly enabled signature verification. You need to enable signature verification using the kernel parameter **module.sig_enforce**.

  To enable .ko signature verification:

  – EFI: Add **module.sig_enforce=1** to the **/boot/efi/EFI/hce/grub.cfg** file.

  – BIOS: Add **module.sig_enforce=1** to the **/boot/grub2/grub.cfg** file.

  Figure 9-1 Enabling .ko signature verification

  ```
  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 parameter	Value	Description
module.sig_enforce	0	Disables the kernel's signature verification on the .ko module. The setting takes effect after the system is rebooted.
	1	Enables the kernel's signature verification on the .ko module. The setting takes effect after the system is rebooted.

- Viewing the public key certificate for signatures in HCE 2.0:

  hce-sign-certificate-1.0-2.hce2.x86_64.rpm in https://repo.huaweicloud.com/hce/2.0/updates/x86_64/Packages/
- Reference for importing a certificate to BIOS:

  Kunpeng: https://support.huawei.com/enterprise/en/doc/EDOC1100088647/97a0d5a0

  2288H V5: https://support.huawei.com/enterprise/en/doc/EDOC1000163372/afc5c7f8?idPath=23710424|251364409|21782478|21872244

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

CAUTION

If you upgrade the OS of a server with Secure Boot enabled from HCE 2.0 released before March 2025 to HCE 2.0 released after May 2025 or upgrade shim, grub, or kernel packages separately, the OS may fail to boot after the upgrade and restart. Before the upgrade, prevent this issue by referring to "Detecting the Issue" in **How Do I Handle Secure Boot Failures Caused by Certificate Changes?** If the upgrade has been completed and the OS cannot be booted, handle this issue by referring to "Solution" in **How Do I Handle Secure Boot Failures Caused by Certificate Changes?**

9.2 Security Hardening Tools

Overview

HCE is a Linux distribution for Huawei Cloud users. By default, security hardening is not performed for OS ISO release packages.

security-tool is a Huawei-developed security hardening tool package that meets Huawei's basic security hardening requirements. By default, security-tool is not installed together with HCE. You can install security-tool as needed. After security-tool is installed, automatic security hardening is performed when the OS is started for the first time.

The security hardening items are as follows:

- System services: for example, configuring SSH, deleting postfix.service, and enabling haveged.service
- Kernel parameters: for example, kernel network protocol stack
- Accounts and passwords: for example, PAM parameters
- Authorization and authentication: for example, warning banner and umask
- File permissions: for example, cron configuration

Scenarios

security-tool provides two types of security hardening: **cybersecurity** (MLPS) and **general** (general security).

Using security-tool

Step 1 Install the security-tool package.

If the package exists in the repository, run the **yum** command to install it.

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

If no, obtain the security-tool package from the **repository** on the Huawei Cloud official website.

Step 2 Specify the type of the configuration to be hardened in the **/etc/hce_security/hce_enhance_type.conf** file.

There are two types of security hardening: **cybersecurity** and **general** (recommended). **cybersecurity** is used as an example in the following steps.

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

Step 3 Start the hce-security service.

```
systemctl start hce-security
```

Run the **systemctl status hce-security** command to check the service status. If the status is **active (exited)**, the security hardening is successful.

Figure 9-2 Checking the service status

```
[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)
```

For details about security hardening logs, see **/var/log/hce_security.log**.

You can modify the **/etc/hce_security/usr-security.conf** file to configure security hardening items. The method of modifying the configuration file is as follows:

```
#########################################################################
#
# 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.
#
################################################################################
```

----End

NOTE

Enabling SELinux affects system performance. SELinux is disabled in HCE 2.0 by default. To enable SELinux, you need to restart the OS for multiple times. SELinux cannot be enabled in one click. For details about how to enable SELinux, see **How Do I Enable SELinux on an ECS Running HCE?**

Differences Between general and cybersecurity

Check Item Type	Check Item	Check Content	general	cybersecurity	Satisfied by Default
Initial configuration	File system configuration	Partition key system directories for mounting.	-	-	No
		Ensure that unnecessary file systems are disabled.	-	-	No
		Ensure that partitions that do not need to be modified are mounted as read-only.	-	-	No
		Ensure that partitions that do not need to be mounted with devices are mounted in nodev mode.	-	-	No

		Ensure that partitions without executable files are mounted in noexec mode.	-	-	No
		Ensure that partitions that do not require SUID/SGID are mounted in nosuid mode.	-	-	No
		Avoid using USB storage.	√	-	Yes
	Software service configuration	Forbid the installation of the X Window System (X11, or simply X).	-	-	Yes
		Disable the debug-shell service.	√	-	Yes
		Disable the rsync service.	√	-	Yes
		Disable the avahi service.	√	-	Yes
		Disable the SNMP service.	√	-	Yes
		Disable the squid service.	√	-	Yes
		Avoid enabling the samba service.	√	-	Yes
		Disable the FTP service.	√	-	Yes
		Disable the TFTP service.	√	-	Yes
		Disable the DNS service.	√	-	Yes
		Disable the NFS service.	√	-	Yes
		Disable the rpcbind service.	√	√	No
		Disable the LDAP service.	√	-	Yes
		Disable the DHCP service.	√	-	Yes

		Do not install the CUPS software.	-	-	Yes
		Do not install the NIS software.	-	-	Yes
		Do not install the Telnet software.	-	-	Yes
		Do not install the NIS client.	-	-	Yes
		Do not install the LDAP client.	-	-	Yes
		Do not install debugging tools.	-	-	Yes
		Do not install development and compilation tools.	-	-	Yes
		Do not install network sniffing tools.	-	-	Yes
	Software upgrade configuration	Ensure that the GNU Privacy Guard (GPG) public key is configured.	-	-	Yes
		Ensure that gpgcheck is enabled.	-	-	Yes
		Ensure that the software repository source is configured.	-	-	Yes
	File integrity check	Ensure that the Advanced Intrusion Detection Environment (AIDE) is installed.	-	-	No
		Set periodic file integrity check.	-	-	No
	Common process hardening	Ensure that address space layout randomization (ASLR) is enabled.	√	-	Yes
		Ensure that core dumps are correctly configured.	√	-	Yes

		Restrict the number of files that can be opened by users.	-	-	No
		Ensure that link file protection is correctly configured.	√	-	Yes
		Ensure that the dmesg access permission is correctly configured.	√	-	No
		Ensure that access to the kernel symbol address is restricted.	√	-	Yes
		Restrict the ptrace for processes.	-	-	No
		Do not set the global encryption policy to **LEGACY**.	-	-	Yes
System services	Time synchronization service	Configure the ntpd service correctly.	-	-	No
		Configure the chronyd service correctly.	-	-	Yes
	Cron service	Ensure that the cron service is running normally.	√	-	Yes
		Ensure that the cron configuration permission is correct.	√	-	No
	Secure Shell (SSH) service	Ensure that the /etc/ssh/sshd_config permission is correctly configured.	√	-	Yes
		Ensure that the permission on the SSH private key file is correctly configured.	√	√	No
		Ensure that the permission on the SSH public key file is correctly configured.	√	√	No

		Ensure that IgnoreRhosts is enabled.	√	-	Yes
		Configure the authentication blacklist and whitelist correctly.	-	-	No
		Ensure that Privileged Access Management (PAM) authentication is enabled for SSH.	√	-	Yes
		Forbid login as user **root**.	-	√	No
		Forbid login using an empty password.	√	-	Yes
		Forbid host-based authentication.	√	-	Yes
		Ensure that the warning banner file path is configured.	√	-	No
		Ensure that the SSH log level is correctly configured.	√	-	Yes
		Configure the listening IP address of the SSH service.	-	-	No
		Configure an appropriate number of concurrent unauthenticated SSH connections.	√	-	No
		Forbid X11 forwarding.	√	-	No
		Set the value of **SSH MaxSessions** less than or equal to 10.	√	-	Yes
		Ensure that **MaxAuthTries** is correctly configured.	√	-	No
		Forbid PermitUserEnviron-ment.	√	-	Yes

		Set the value of **LoginGraceTime** less than or equal to 60 seconds.	√	-	No
		Ensure that the idle timeout is configured.	√	-	No
		Forbid AllowTcpForwarding.	√	-	No
		Ensure that strong SSH key exchange algorithms (KexAlgorithms) are configured.	√	-	Yes
		Ensure that strong SSH message authentication codes (MACs) are configured.	√	-	Yes
		Ensure that strong SSH Ciphers are configured.	√	-	Yes
		Do not configure the options that will be discarded by SSH.	√	-	Yes
Network services	Unused network protocols and devices	Avoid using uncommon network services.	-	-	No
		Avoid using WLANs.	-	-	Yes
	Network protocol stack in the kernel space	Disable the system from responding to ICMP broadcast packets.	√	-	Yes
		Do not receive ICMP redirect messages.	√	-	No
		Do not forward ICMP redirect messages.	√	-	Yes
		Ignore all ICMP requests.	-	-	No
		Ensure that forged ICMP packets are ignored.	√	-	Yes

		Ensure that reverse address filtering is enabled.	√	-	No
		Disable IP forwarding.	√	-	Yes
		Disable the option of receiving source route packets.	√	-	No
		Ensure that TCP-SYN cookie protection is enabled.	√	-	Yes
		Enable logging to record suspicious network packets.	√	-	No
		Do not enable tcp_timestamps.	-	-	No
		Ensure that TIME_WAIT for TCP is configured.	√	-	Yes
		Ensure that the number of queues in the SYN_RECV state is correctly configured	-	-	No
		Do not use the ARP proxy.	-	-	Yes
Firewall configuration	firewalld	Enable the firewalld service.	-	-	Yes
		Ensure that iptables is not enabled.	-	-	Yes
		Ensure that nftables is not enabled.	-	-	Yes
		Configure valid default zones.	-	-	No
		Ensure that the network interfaces are bound to the correct zones.	-	-	No
		Avoid enabling unnecessary services and ports.	-	-	No
	iptables	Enable the iptables service.	-	-	No

		Ensure that firewalld is not enabled.	-	-	No
		Ensure that nftables is not enabled.	-	-	Yes
		Configure the default rejection policy.	-	-	No
		Configure the iptables loopback policy.	-	-	No
		Configure the iptables INPUT policy.	-	-	No
		Configure the iptables OUTPUT policy.	-	-	No
		Configure association policies for the iptables INPUT and OUTPUT.	-	-	No
	nftables	Enable the nftables service.	-	-	No
		Ensure that iptables is not enabled.	-	-	Yes
		Ensure that firewalld is not enabled.	-	-	No
		Configure the default rejection policy.	-	-	No
		Configure the nftables loopback policy.	-	-	No
		Configure the nftables INPUT policy.	-	-	No
		Configure the nftables OUTPUT policy.	-	-	No
		Configure association policies for the nftables INPUT and OUTPUT.	-	-	No
Log auditing	auditd	Ensure that auditd is enabled.	√	-	Yes
		Ensure that auditd can be enabled when the system boots.	-	-	No

		Ensure that **audit_backlog_limit** is correctly configured.	-	-	No
		Ensure that the maximum size of a single log file is specified.	-	-	Yes
		Ensuring that ROTATE is enabled for audit logs.	-	-	No
		Ensure that audit logs are not automatically deleted.	-	-	Yes
		Ensure that disk space thresholds are correctly configured.	-	-	Yes
		Avoid setting a small rate limit threshold for audit logs.	-	-	Yes
		Configure the sudoers audit rule.	-	√	No
		Configure a login audit rule.	-	-	Yes
		Configure a session audit rule.	-	-	Yes
		Configure an audit rule for time change.	-	√	No
		Configure an SELinux audit rule.	-	-	No
		Configure an audit rule for the network environment.	-	√	No
		Configure an audit rule for file access control permissions.	-	-	No
		Configure an audit rule for file access failures.	-	-	No
		Configure an audit rule for file deletions.	-	-	No

		Configure an audit rule for account information modifications.	-	√	No
		Configure an audit rule for file system mounting.	-	-	No
		Configure the audit rule for privilege escalation commands.	-	-	No
		Ensure that the audit rule for kernel module changes.	-	-	Yes
		Configure an audit rule for sudo log file modifications.	-	-	No
	rsyslog	Ensure that the rsyslog service is enabled.	√	√	No
		Ensure that system authentication-related events are recorded.	-	-	Yes
		Ensure that cron logs are recorded.	√	-	Yes
		Configure the log records of each service correctly.	-	-	Yes
		Configure the default rsyslog file permission correctly.	√	√	No
		Configure a rotation policy for rsyslog.	-	-	No
		Configure the option of sending logs to a remote log server.	-	-	No
		Ensure that remote rsyslog messages are received only on the specified log host.	-	-	No

		Ensure that the option of dumping journald logs of the rsyslog service has been configured.	-	-	No
Account and password management	Account management	Forbid login capabilities for accounts that are not used for login.	-	-	No
		Forbid unused accounts.	-	-	No
		Set the account validity period correctly.	-	-	No
		Forbid non-root accounts with UID 0.	-	-	Yes
		Ensure that the UIDs are unique.	-	-	Yes
		Ensure that the GIDs are unique.	-	-	Yes
		Ensure that the account names are unique.	-	-	Yes
		Ensure that the group names are unique.	-	-	Yes
		Ensure that all groups exist in **/etc/passwd**.	-	-	Yes
		Ensure that an account has its own home directory.	-	-	Yes
		Ensure that the permissions on the home directory of the account are 750 or stricter.	-	-	Yes
		Avoid the .forward file in the home directory.	-	-	Yes
		Avoid the .netrc file in the home directory.	-	-	Yes

		Ensure that the user **PATH** variable is strictly defined.	-	-	Yes
	Password management	Ensure the password complexity.	√	√	No
		Restrict the number of reusing a historical password.	√	√	No
		Ensure that passwords do not contain the account character strings.	-	-	Yes
		Ensure that passwords are encrypted using SHA512.	√	√	No
		Ensure that the password expiration time is correctly configured.	√	√	No
		Ensure that the password expiration alarm time is correctly configured.	√	-	Yes
		Ensure that the password change period is correctly configured.	√	√	No
		Ensure that inactive passwords are locked for no more than 30 days.	√	-	Yes
		Ensure that the password protection is configured for GRUB.	-	-	Yes
		Ensure that password protection is configured in the single-user mode.	-	-	Yes
Identity authentication	Login management	Lock an account after a specific number of login failures.	√	√	No

		Prevent user **root** from accessing the system locally.	-	-	No
		Ensure that the timeout duration of sessions is correctly configured.	√	√	No
	Warning banners	Ensure that the local login warning banner contains proper information.	√	-	No
		Ensure that the remote login warning banner contains proper information.	√	-	No
		Ensure that the **motd** file contains proper information.	√	-	No
		Ensure that the /etc/issue permission is correctly configured.	√	-	Yes
		Ensure that the /etc/issue.net permission is correctly configured.	√	-	Yes
		Ensure that the /etc/motd permission is correctly configured.	√	-	Yes
Access control	SELinux	Ensure that the enforce mode is enabled.	-	-	Yes
		Ensure that the SELinux policy is correctly configured.	-	-	Yes
		Avoid the services with the **unconfined_service_t** label.	-	-	No
		Ensure that the SETroubleShoot service is not installed.	-	-	Yes

		Ensure that the Mount Conversion Service (MCS) is not installed.	-	-	Yes
	Privileged commands	Ensure that the **su** command is restricted.	√	√	No
		Ensure that the **su** command inherits the user's environment variables without escalating privileges.	√	√	No
		Ensure that common users run privileged programs using sudo.	-	-	No
		Ensure that the sudo log file is configured.	√	-	No
		Disable the SysRq key.	-	-	No
	System file permissions	Ensure that the **/etc/passwd** permission is correctly configured.	√	-	Yes
		Ensure that the **/etc/passwd-** permission is correctly configured.	√	-	Yes
		Ensure that the **/etc/shadow** permission is correctly configured.	√	-	Yes
		Ensure that the **/etc/shadow-** permission is correctly configured.	√	-	Yes
		Ensure that the /etc/group permission is correctly configured.	√	-	Yes
		Ensure that the **/etc/group-** permission is correctly configured.	√	-	Yes
		Ensure that the **/etc/gshadow** permission is correctly configured.	√	-	Yes

		Ensure that the **/etc/gshadow-** permission is correctly configured.	√	-	Yes
		Ensure that the sticky bit is set for world-writable directories.	-	-	Yes
		Forbid files or directories without owners or owning groups.	-	-	Yes
		Avoid using world-writable files.	-	-	Yes
		Forbid files with invalid links.	-	-	Yes
		Forbid executable hidden files.	-	-	Yes
		Ensure that unnecessary SUID or SGID bits in the file are deleted.	-	-	Yes
		Ensure that umask is 027 or stricter.	√	√	No

NOTE

- The symbol √ indicates that the item is executed.
- The symbol - indicates that the item is not executed.

10 Image Updates

The update records of both x86- and Arm-compatible architectures public images are included.

For details about the update records of x86-compatible public images, see **Image Update Records (x86)**.

For details about the update records of Arm-compatible public images, see **Image Update History (Arm)**.

