



Huawei E9000 Server

V100R001

Security Technical White Paper

Issue 01

Date 2015-09-09

Copyright © Huawei Technologies Co., Ltd. 2015. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://e.huawei.com>

About This Document

Purpose

This document describes the security specifications of the E9000.

This document applies to the E9000, including its management modules MM910, switch modules, and compute nodes.

For details about the switch modules, see Chapter 4 "Switch Module Security Design".

The compute nodes include the CH121 V3, CH140 V3, CH220 V3, CH222 V3, CH226 V3, and CH242 V3.




Intended Audience



This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

Symbol	Description
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Issue	Release Date	Description
01	2015-09-09	This issue is the first official release.

Contents

About This Document.....	ii
1 Server Security Threats.....	1
2 E9000 Security Architecture.....	2
2.1 Plane Isolation.....	4
2.2 Internal Isolation of the Management Plane.....	4
3 Chassis Management Module Security Design.....	5
3.1 Authentication.....	6
3.2 Certificate Management.....	6
3.3 Log Audit.....	7
3.4 Using Secure Transport Protocols.....	7
3.5 Data Protection.....	8
3.6 User Management.....	9
3.7 Access Policy Control and Management.....	9
3.8 Key Management.....	11
3.9 Session Termination.....	12
3.10 CLI System Hardening.....	12
4 Switch Module Security Design.....	13
4.1 Ethernet Switch Modules.....	14
4.2 FC Switch Modules.....	14
5 Security Design of Out-of-Band Compute Node Management Module.....	15
5.1 Authentication.....	16
5.2 Certificate Management.....	16
5.3 Log Audit.....	17
5.4 Using Secure Transport Protocols.....	17
5.5 Data Protection.....	18
5.6 User Management.....	19
5.7 Access Policy Control and Management.....	19
5.8 Key Management.....	20
5.9 Session Termination.....	22
5.10 CLI System Hardening.....	22

6 Server System Security Design.....	23
6.1 Trusted computing.....	24
7 Secure Release.....	25
7.1 Security Tool Scanning.....	26
7.2 End-to-End Assurance.....	26
8 Acronyms and Abbreviations.....	27

1 Server Security Threats

As networks and data centers develop, servers, the core of data centers, face a variety of internal and external security threats. Servers face security threats to two systems:

- service system and management system. The service system is oriented to users. The security of the service system relies on the security of the operating system (OS) and the service system itself. Security threats impair the service system itself.
- The management system manages servers. It is located on the internal network of a data center, and needs to be accessed from the internal and external networks. The security of the management system relies on the security of server firmware. Security threats may affect management of all servers in the entire data center.

The E9000 is a blade server installed in a chassis. This document describes only the security of the chassis hardware system, that is, the security of the management interfaces provided by the chassis and the internal firmware. The security of the server OS and service system is beyond the scope of this document.

The server chassis hardware system faces the following security issues:

- External attackers exploit system vulnerabilities or bugs to obtain administrative and control rights and perform unauthorized operations.
- Internal users exploit the system vulnerabilities to obtain higher control rights, perform unauthorized operations, and destroy attack evidence.

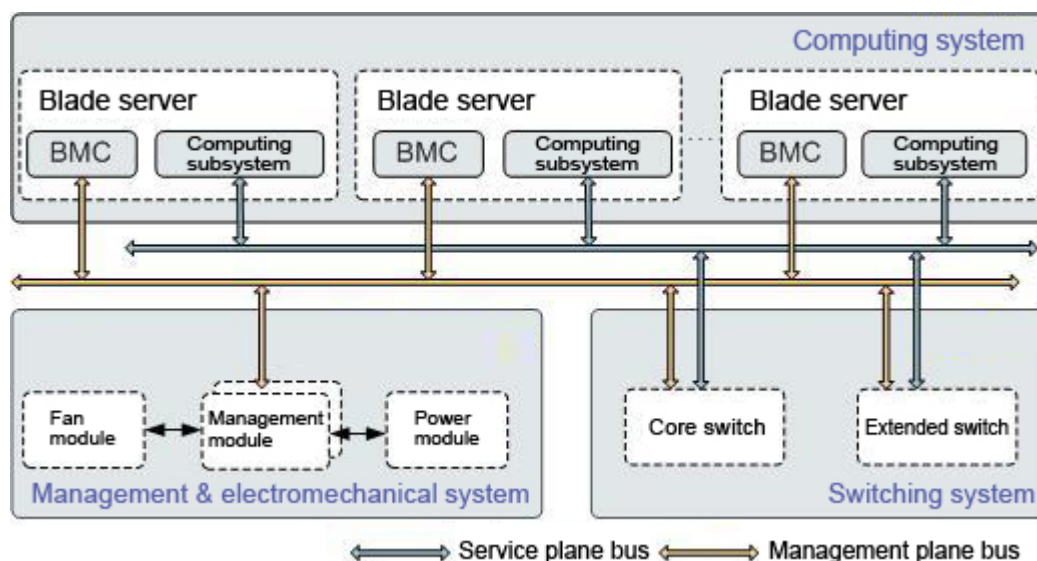
The E9000 adopts scientific architecture and component design to ensure E9000 infrastructure security and facilitate security planning and secure service deployment. Server security is a complex system. Users need to consider the security of the OS and service system in addition to the infrastructure security.

2 E9000 Security Architecture

About This Chapter

The E9000 is an enterprise-level high-end high-performance blade server for elastic computing and telecom computing. It logically consists of the computing system, switching system, and management & electromechanical system. [Figure 2-1](#) shows the system architecture.

Figure 2-1 System architecture



The computing system consists of compute nodes and storage nodes. It provides external data ports through the input/output (I/O) modules of the switching system and supports chassis-level or higher-level device management using the internal baseboard management controller (BMC).

The switching system consists of core switch modules and expansion switch modules. It performs switching between computing subsystems and provides external data ports through the I/O modules. The switching system is connected to the management & electromechanical system. The two systems can be configured as physical networks that are isolated from each other or as a physical network that integrates service switching and device management.

The management & electromechanical system manages components in the chassis and provides system power supply and cooling. This system consists of fan modules, power supply units

(PSUs), and management modules. It is connected to compute nodes, storage nodes, and switch modules.

The E9000 incorporates security schemes during the design of the hardware and software architectures.

[2.1 Plane Isolation](#)

[2.2 Internal Isolation of the Management Plane](#)

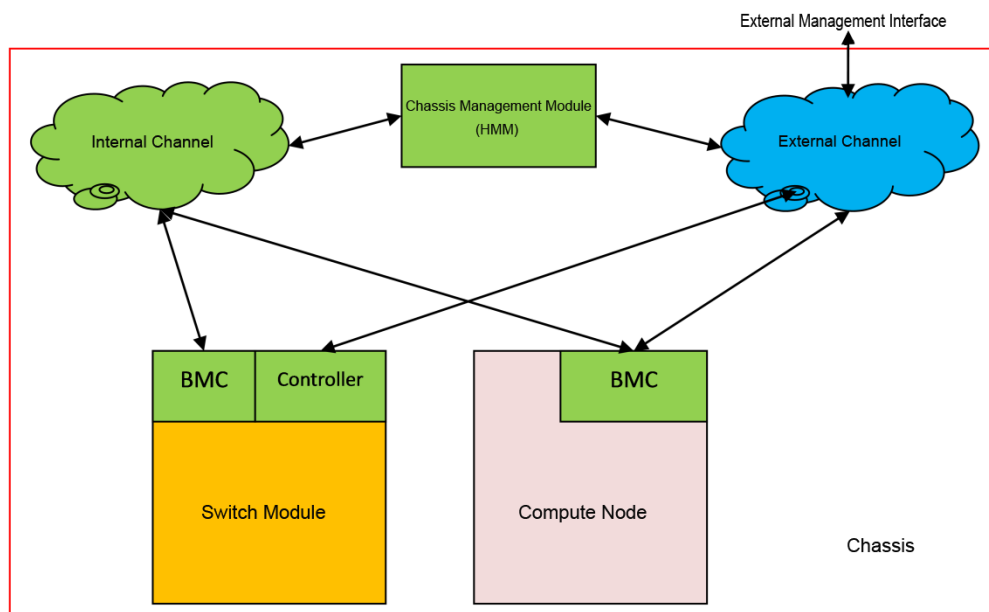
2.1 Plane Isolation

The E9000 chassis is divided into the service plane and management plane, which are physically isolated from each other. The management plane of the computing and switching systems is connected to the chassis management module over an independent bus, which is physically isolated from the service plane bus. In this way, the management system is independent of the service system, and therefore not affected by malicious access or security threats to the service system.

2.2 Internal Isolation of the Management Plane

The E9000 Hyper Module Management (HMM) module provides external management interfaces, through which the baseboard management controllers (BMCs) of compute nodes and switch modules allow external access. The HMM module also controls compute nodes and switch modules. External access and internal control share physical channels, but are logically isolated from each other using VLANs, which are not changeable. Therefore, external management interfaces cannot access internal channels. [Figure 2-2](#) shows the management system topology.

Figure 2-2 E9000 management system topology



3 Chassis Management Module Security Design

About This Chapter

As chassis server hardware, the E9000 provides only device management system software, but does not provide service system software. Security threats to the E9000 are primarily attacks to the E9000 infrastructure. The E9000 security design ensures infrastructure security and operation and maintenance (O&M) security.

[3.1 Authentication](#)

[3.2 Certificate Management](#)

[3.3 Log Audit](#)

[3.4 Using Secure Transport Protocols](#)

[3.5 Data Protection](#)

[3.6 User Management](#)

[3.7 Access Policy Control and Management](#)

[3.8 Key Management](#)

[3.9 Session Termination](#)

[3.10 CLI System Hardening](#)

3.1 Authentication

The combination of user name and password is used for the authentication performed when end users or upper-layer management systems access the HMM through a web interface, command line interface (CLI), or Simple Network Management Protocol (SNMP) interface. Device management, configuration, and information query are allowed only after the authentication is successful.

The HMM supports local and Lightweight Directory Access Protocol (LDAP) authentication.

The login passwords must meet complexity requirements to improve password strength. Protection mechanisms are provided to protect against brute force cracking. For example, a user will be locked out for five minutes if an incorrect password is entered for five consecutive times.

After the authentication is successful, the user can perform operations matching the user role (administrator, operator, or common user). For details about the user roles, see [User Management](#).

3.2 Certificate Management

The certificates refer to SSL certificates, which are used in Hypertext Transfer Protocol Secure (HTTPS) connections to authenticate websites.

SSL certificate management operations include viewing current certificate information (such as the user, issuing authority, validity period, and serial number), generating a CSR file, importing the signed certificate (in PKCS#7 format, containing only the public key) generated from the CSR file, and importing a self-defined certificate (in PKCS#12 format, containing public and private keys). When the certificate is successfully imported or the default setting is restored, the CSR file is deleted. Certificates support only the Base 64 X.509 format and can be encapsulated as PKCS#7 or PKCS#12 files. For certificates in PKCS#12, users can set the password for the private key.

By default, the HMM uses self-signed SSL certificates. The self-signed SSL certificates use the SHA256RSA algorithm (2048-bit). For the sake of security, the HMM provides the following two methods for replacing self-signed SSL certificates.

Method 1: Use certificates generated on the HMM Web

1. Log in to the HMM Web, and modify the certificate user information.
2. Generate a CSR file.
3. Export the CSR file.
4. Submit the CSR file to the CA.
5. Generate a signed certificate in the PKCS#7 format.
6. Import the signed certificate to the HMM.
7. Restart the HMM for the certificate to take effect.

Caution: The signed certificate must match the CSR file, that is, you must use the CSR file to apply for signed certificate. If the signed certificate does not match the CSR file, the signed certificate cannot be imported successfully.

Method 2: Use certificates provided by users

1. Generate a certificate using a CA server or purchase a certificate from CA.
2. Log in to the HMM Web, and import the certificate to the HMM.
3. Restart the HMM for the certificate to take effect.

3.3 Log Audit

The HMM supports operation log audit. All non-query operations performed on the HMM are logged. Users can view and audit the operation logs through the interface provided by the HMM.

The log information includes the user name, user IP address, operation time, and operation details.

Operation logs are stored in the HMM flash file system in real time. A log file will be automatically backed up when it reaches xxx KB. A maximum of xxx log backup files can be retained. When the number of log files exceeds xxx, the earliest backup file will be automatically deleted.

The principle of least privilege is applied to prevent log files from being deleted or modified mistakenly.

3.4 Using Secure Transport Protocols

Secure versions of standard transport protocols are used.

For example, the CLI, file transmission, web, and SNMP respectively use SSH, SFTP, HTTPS, and SNMPv3 as the default transport protocols. Insecure protocols, such as FTP, Telnet, HTTP, SNMPv1, and SNMP v2c, are disabled by default.

Features of standard secure transport protocols are as follows:

SSH:

1. Supports authentication using the user password or public key.
2. Uses protocol 2.
3. Supports secure algorithms: aes128-ctr, aes192-ctr, and aes256-ctr.

SFTP:

1. Only the **/tmp** directory has upload and download permission.
2. Files uploaded to the **/tmp** directory do not have execute permission by default.

HTTPS:

1. Supports TLS 1.0 and higher, but not SSL v3 or lower.
2. Supports secure algorithms: AES_128_CBC_SHA256 and AES_256_CBC_SHA256.

SNMPv3

- 2. Supports the authentication algorithms SHA and MD5.
- 2. Supports the encryption algorithms AES and DES.

Non-standard authentication and encryption protocols are used for transmission over TCP channels of KVM and VMM. Authentication is based on the challenge-response mechanism and data encryption uses AES128.

3.5 Data Protection

The HMM has no user data. The only sensitive data, including user passwords and keys, is encrypted on HMM.

The HMM also supports encryption of upgrade packages.

In addition, the HMM encapsulates the Linux shell. Users cannot access the following files after logging in through a serial port or using SSH.

Table 3-1 Encrypted HMM data

Data	Encryption Algorithms
FTP user password	Encrypted using SHA512 in the shadow file in the /etc/ directory.
SSH/SFTP user password	Encrypted using SHA512 in the shadow file in the /etc/ directory.
Telnet user password	Encrypted using SHA512 in the shadow file in the /etc/ directory.
Web user password	Encrypted using SHA512 in the shadow file in the /etc/ directory.
SNMPv3 user password	Encrypted using AES128 in the internal process file .snmpdbak.conf in the / common/usr/local/snmp/share/snmp/ directory. Encrypted using MD5 or SHA-1 (configurable) in the snmpd.conf file in the / common/var/net-snmp/ directory. This file is used for SNMP process authentication.
SNMPv1/v2c community name	Encrypted using AES128 in the snmpd.conf file in the / common/var/net-snmp/ directory.
Serial port	Encrypted using SHA512 in the shadow file in the /etc/ directory.
SSL certificates	Encrypted using AES128.
Upgrade packages	Encrypted using AES128.

The sensitive data generated during the system operation will be overwritten through automatic memory clearing immediately after the data is used.

3.6 User Management

The HMM supports CLI, SNMP, and web interfaces and provides unified user management. As long as a user is added for an interface, the user can access the system through any other interface. The system background automatically synchronizes user settings to all interfaces.

Some users may not need all or multiple types of interfaces, and access to multiple interfaces increase system risks, so HMM provides the whitelist-based user access control policy so that interfaces can be enabled or disabled for specific users. For details, see [Access Policy Control and Management](#).

A maximum of 64 users are supported. Users can be added, modified, or deleted. User permissions are classified by role or domain.

Users permissions classified by user role are as follows:

Administrator: An administrator has all configuration and control rights.

Operator: An operator have rights to query and configure information, but cannot perform operations, such as LDAP upgrade, user management, and password complexity check enabling or disabling.

Common user: A common user has rights to query information and change their own passwords.

User permissions can also be classified by domain, that is, the scope of managed resources.

The HMM allows you to create user domains (only one super domain by default) and specify the management scope (compute nodes and switch modules) for each user domain. The super domain has the rights to manage all electromechanical devices in the chassis, including the nodes, PSUs, and fan modules. Users in a domain manage only the nodes or modules specified by the domain. Users in a domain have rights to add, delete, or modify the nodes and modules specified by the domain. The operator of a user domain is the administrator of the super domain. Each user must be assigned to a domain. You must delete or move the users in a domain before deleting the domain.

3.7 Access Policy Control and Management

Access policy control and management involves configuration and management of system security policies. Configuring system security policies helps improve system security.

Password Policies

1. **Complexity:** prevents users from setting passwords that are too simple. The password complexity check is enabled by default. Password complexity requirements are as follows:

If the password complexity check is disabled, the password must contain 8 to 32 characters.

If the password complexity check is enabled, a password must meet the following requirements:

The password contains 8 to 32 characters.

The password contains at least one space or one of the following special characters: `~!@#\$\$%^&*()-_+=\|[{ }];:","<.>/?

The password contains at least two of the following combinations: lowercase letters a-z, uppercase letters A-Z, and digits 0-9

The password is case-sensitive and cannot be the same as the user name or the user name in reverse order.

Number of reserved historical passwords: prevents the user to set a password same as any of the reserved historical passwords. The value **0** indicates that this setting is disabled. The value is an integer ranging from 0 to 5. Default value: 0

Password validity period (days): specifies the validity period of a password. The value is an integer ranging from 1 to 360. The default value is **0**, which indicates that the password never expires. Users will be notified to change their passwords when the remaining validity period is less than 10 days.

Login Policies

Session timeout time (minute): A session will be terminated if no operation is performed within the specified time. The value is an integer ranging from 5 to 480. The default value is **5**.

Password lock: If this function is enabled, a user will be locked out if the number of consecutive failed login attempts reaches the specified limit. This function is enabled by default.

Login failure limit: specifies the maximum number of consecutive failed login attempts. A user will be locked out if the number of consecutive failed login attempts reaches this limit. The value is an integer ranging from 1 to 5. The default value is **5**.

A locked user can be unlocked by the system administrator using commands. Otherwise, the user will be automatically unlocked after the lock time.

Lock time: an integer ranging from 1 to 5. The default value is **5**, which indicates that a locked user will be automatically unlocked after 5 minutes.

Emergency login user: The specified user can log in to the WebUI regardless of the password validity and login policies. The default value is **root**.

Domain Access Policies

The HMM WebUI supports LDAP domain access authentication. To implement unified user access management, the domain server and domain authentication parameters can be configured.

Access Control Policies Based on Login Time, IP and MAC Addresses

The WebUI supports whitelist-based access management. A whitelist containing the login periods, IP network segment, and MAC addresses allowed is configured. Only the users who meet the conditions specified in the whitelist can access the system through the management channel and configure and manage servers. Whitelist-based access control policy: When creating or modifying a user on the web interface, you can enable or disable interfaces available for the user.

For example, if a user needs to log in to the HMM only through the web interface, you can disable the user's SSH/Telnet, SFTP, and SNMP login permissions. The user will be rejected when attempting to log in using these interfaces.

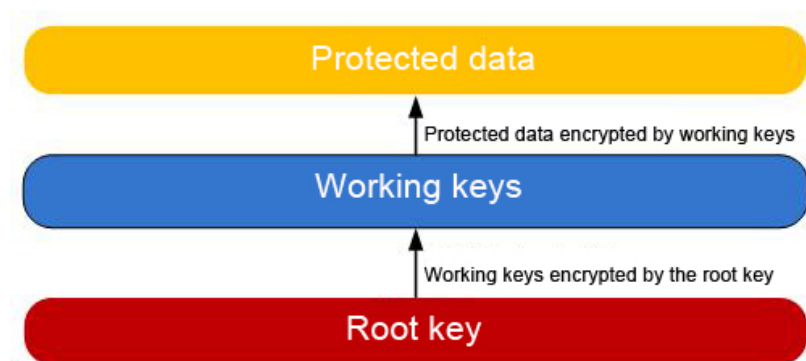
You can enable one or multiple interfaces for a user as required.

SFTP can be used only when combined with SSH/Telnet or SNMP. (Note: The HMM does not provide independent SFTP services. SFTP is used to assist upload and download operations through SSH/Telnet or SNMP.

Only administrators can configure the whitelist-based access control policy.

3.8 Key Management

HMM key management uses a two-layer structure, as shown in the following figure.



HMM key management structure

Generation of a Root Key

A root key consists of two components. Each component is of 64 bits.

Component 1 is hard-coded.

Component 2 is stored in a file system that is readable and writable.

Salt is hard-coded.

Component 2 is stored in a file system that is readable and writable. Only the system administrator has read and write permission. This facilitates updates of root keys.

The components of a root key are generated from secure random numbers. The components obtained are hard-coded and stored in the file system.

Storage of Working Keys

Working keys are encrypted using the root key and saved in a file system that is readable and writable.

Backup of Working Keys

To prevent data loss, two copies of working keys are stored in different directories of the file system.

Working Key Integrity Protection

The root key is used to encrypt working keys to control access to the file containing working keys.

Generation of Working Keys

Before a version release, an external tool is used to generate the keys and encrypted data file and save them to a file system that is readable and writable. In other words, a default file comes with the delivery.

Update of Working Keys

Manual update is supported. Run the command for updating working keys. The system then generates working keys randomly. The keys cannot be viewed.

3.9 Session Termination

A session can be terminated in either of the following ways:

Termination upon timeout: The mechanism of disconnecting silent connections upon timeout is used for CLI, web, and SFTP sessions. For example, a session will be terminated if no operation is performed within 5 minutes.

Manual termination: A user initiates a request to terminate a session. The system administrator can terminate sessions initiated by other users.

3.10 CLI System Hardening

The CLI is encapsulated so that it no longer supports Linux system commands. Only whitelisted commands can be executed on the CLI, minimizing the risks of network attacks.

4 Switch Module Security Design

[4.1 Ethernet Switch Modules](#)

[4.2 FC Switch Modules](#)

4.1 Ethernet Switch Modules

The E9000 uses Huawei CloudEngine switch platforms as Ethernet switch modules.

Details are as follows:

For details about the CX310, CX311, CX312, CX910, CX911, CX912, and CX913, see documents for CE6800.

For details about the CX110, CX111, and CX915, see documents for CE5800.

For details about the CX710, see documents for CE7800.

4.2 FC Switch Modules

The CX311, CX911, CX915 are produced by QLogic. See the QLogic 5800 series datasheet.

The CX210 and CX912 are produced by Brocade. See the Brocade 300 datasheet.

The CX220 is produced by Brocade. See the Brocade 6510 or 6505 datasheet.

5 Security Design of Out-of-Band Compute Node Management Module

- 5.1 Authentication
- 5.2 Certificate Management
- 5.3 Log Audit
- 5.4 Using Secure Transport Protocols
- 5.5 Data Protection
- 5.6 User Management
- 5.7 Access Policy Control and Management
- 5.8 Key Management
- 5.9 Session Termination
- 5.10 CLI System Hardening

5.1 Authentication

The combination of user name and password is used for the authentication performed when end users or upper-layer management systems access the iBMC through the web interface, CLI, SNMP, or IPMI LAN. Device management, configuration, and information query are allowed only after the authentication is successful.

iBMC supports local and Lightweight Directory Access Protocol (LDAP) authentication.

The login passwords must meet complexity requirements to improve password strength. Protection mechanisms are provided to protect against brute force cracking. For example, a user will be locked out for five minutes if an incorrect password is entered for five consecutive times.

After the authentication is successful, the user can perform operations matching the user role (administrator, operator, or common user). For details about the user roles, see User Management.

5.2 Certificate Management

The certificates refer to SSL certificates, which are used in Hypertext Transfer Protocol Secure (HTTPS) connections to authenticate websites.

SSL certificate management operations include viewing current certificate information (such as the user, issuing authority, validity period, and serial number), generating a CSR file, importing the signed certificate (in PKCS#7 format, containing only the public key) generated from the CSR file, and importing a self-defined certificate (in PKCS#12 format, containing public and private keys). When the certificate is successfully imported or the default setting is restored, the CSR file is deleted. Certificates support only the Base 64 X.509 format and can be encapsulated as PKCS#7 or PKCS#12 files. For certificates in PKCS#12, users can set the password for the private key.

By default, iBMC uses self-signed SSL certificates. The self-signed SSL certificates use the SHA256RSA algorithm (2048-bit). For the sake of security, iBMC provides the following two methods for replacing self-signed SSL certificates.

Method 1: Use certificates generated on the iBMC

1. Log in to the iBMC WebUI, and modify the certificate user information.
2. Generate a CSR file.
3. Export the CSR file.
4. Submit the CSR file to the CA.
5. Generate a signed certificate in the PKCS#7 format.
6. Import the signed certificate to the iBMC.
7. Restart the iBMC for the certificate to take effect.

Caution: The signed certificate must match the CSR file, that is, you must use the CSR file to apply for signed certificate. If the signed certificate does not match the CSR file, the signed certificate cannot be imported successfully.

Method 2: Use certificates provided by users

1. Generate a certificate using a CA server or purchase a certificate from CA.
2. Log in to the iBMC WebUI, and import the certificate.
3. Restart the iBMC for the certificate to take effect.

5.3 Log Audit

iBMC supports operation log audit. All non-query operations performed on the iBMC are logged. Users can view and audit the operation logs through the interface provided by iBMC.

The log information includes the user name, user IP address, operation time, and operation details.

Operation logs are stored in the iBMC flash file system in real time. A log file will be automatically backed up when it reaches xxx KB. A maximum of xxx log backup files can be retained. When the number of log files exceeds xxx, the earliest backup file will be automatically deleted.

The principle of least privilege is applied to prevent log files from being deleted or modified mistakenly.

5.4 Using Secure Transport Protocols

Secure protocols, such as SFTP, SSH, HTTPS, SNMPv3, and RMCP+(IPMI LAN), are used for access to the iBMC. Information is encrypted using secure algorithms before being transmitted. Insecure protocols, such as FTP, Telnet, HTTP, and RMCP (IPMI LAN) are disabled by default.

Secure versions of standard transport protocols are used.

For example, the CLI, file transmission, web, SNMP, and IPMI commands respectively use SSH, SFTP, HTTPS, SNMPv3, and RMCP+ (IPMI LAN) as the default transport protocols. Insecure protocols, such as FTP, Telnet, HTTP, SNMPv1, SNMP v2c, RMCP (IPMI LAN), are disabled by default.

Features of secure transport protocols are as follows:

SSH:

1. Supports authentication using the user password or public key.
2. Uses protocol 2.
3. Supports secure algorithms: aes128-ctr, aes192-ctr, and aes256-ctr.

SFTP:

1. Only the **/tmp** directory has upload and download permission.
2. Files uploaded to the **/tmp** directory do not have execute permission by default.

HTTPS:

1. Supports TLS 1.0 and higher, but not SSL v3 or lower.
2. Supports secure algorithms: AES_128_CBC_SHA256 and AES_256_CBC_SHA256.

SNMPv3:

1. Supports authentication algorithms SHA and MD5. The iBMC provides a configuration interface.
2. Supports encryption algorithms AES and DES. The iBMC provides a configuration interface.

Non-standard authentication and encryption protocols are used for transmission over TCP channels of KVM and VMM. Authentication is based on the challenge-response mechanism and data encryption uses AES128.

5.5 Data Protection

iBMC has no user data. The only sensitive data, including user passwords and keys, is encrypted on the iBMC.

The iBMC also supports encryption of upgrade packages.

In addition, the iBMC encapsulates the Linux shell. Users cannot access the following files after logging in through a serial port or using SSH.

Table 5-1 Encrypted iBMC data

Data	Encryption Algorithms
FTP user password	Encrypted using SHA256 in the passwd file in the /data/etc/ directory.
SSH/SFTP user password	Encrypted using SHA256 in the passwd file in the /data/etc/ directory.
Telnet user password	Encrypted using SHA256 in the passwd file in the /data/etc/ directory.
Web user password	Encrypted using AES128 in the ipmi file in the /etc/uuser/ directory.
SNMPv3 user password	Encrypted using MD5 or SHA-1 (configurable) in the snmpd.conf file in the /etc/net-snmp/ directory. This file is used for SNMP process authentication.
SNMPv1/v2c community name	Encrypted using AES128 in the snmpd.conf file in the /etc/snmp/ directory.
RMCP + user password	Encrypted using AES128 in the ipmi file in the /etc/uuser/ directory.
Serial port	Encrypted using SHA256 in the passwd file in the /data/etc/ directory.

SSL certificates	Encrypted using AES128.
Upgrade packages	Encrypted using AES128.

The sensitive data generated during the system operation will be overwritten through automatic memory clearing immediately after the data is used.

5.6 User Management

The iBMC supports unified user management through different interfaces, including CLI, SNMP, web, and IPMI LAN. A maximum of 16 users can be configured. Users can be added, modified, or deleted. Users are classified into different groups, including administrators, operators, common users, and custom users.

Administrator: An administrator has all configuration and control rights.

Operator: An operator has all configuration and control rights, excluding user management and security configuration.

Common user: A common user has only the permission to modify its own password and view information, excluding OS information and operation logs.

Custom user: Administrators can define the permissions of custom users as required. iBMC supports a maximum of 4 custom users. System permissions consist of user configuration, common settings, remote control, remote media, security configuration, power control, diagnosis, and query permissions. Administrators can set any combination of them as a custom user.

5.7 Access Policy Control and Management

Access policy control and management involves configuration and management of system security policies. Configuring system security policies helps improve system security.

Password Policies

1. **Complexity:** prevents users from setting passwords that are too simple. The password complexity check is enabled by default. Password complexity requirements are as follows:

If the password complexity check is disabled, the password must contain 8 to 32 characters.

If the password complexity check is enabled, a password must meet the following requirements:

The password contains 8 to 32 characters.

The password contains at least one space or one of the following special characters: `~!@#\$\$%^&*()-_+=+|[{}];:","<.>/?

The password contains at least two of the following combinations: lowercase letters a-z, uppercase letters A-Z, and digits 0-9

The password is case-sensitive and cannot be the same as the user name or the user name in reverse order.

Number of reserved historical passwords: prevents the user to set a password same as any of the reserved historical passwords. The value **0** indicates that this setting is disabled. The value is an integer ranging from 0 to 5. Default value: 0

Password validity period (days): specifies the validity period of a password. The value is an integer ranging from 1 to 360. The default value is **0**, which indicates that the password never expires. Users will be notified to change their passwords when the remaining validity period is less than 10 days.

Login Policies

Session timeout time (minute): A session will be terminated if no operation is performed within the specified time. The value is an integer ranging from 5 to 480. The default value is **5**.

Password lock: If this function is enabled, a user will be locked out if the number of consecutive failed login attempts reaches the specified limit. This function is enabled by default.

Login failure limit: specifies the maximum number of consecutive failed login attempts. A user will be locked out if the number of consecutive failed login attempts reaches this limit. The value is an integer ranging from 1 to 5. The default value is **5**.

A locked user can be unlocked by the system administrator using commands. Otherwise, the user will be automatically unlocked after the lock time.

Lock time: an integer ranging from 1 to 5. The default value is **5**, which indicates that a locked user will be automatically unlocked after 5 minutes.

Emergency login user: The specified user can log in to the WebUI regardless of the password validity and login policies. The default value is **root**.

Domain Access Policies

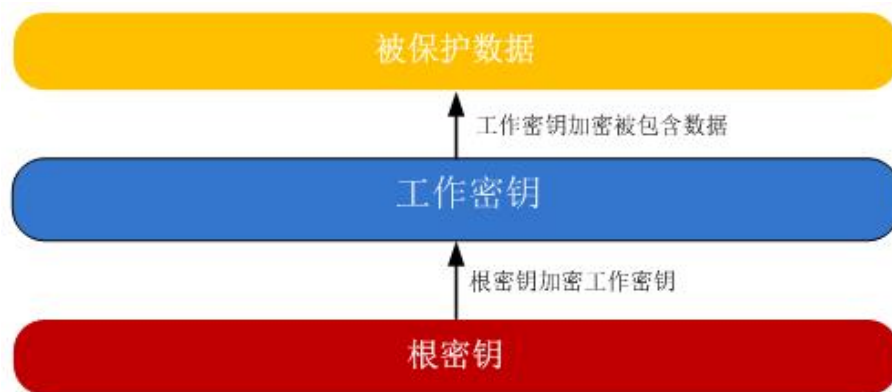
The WebUI supports LDAP domain access authentication. To implement unified user access management, the domain server and domain authentication parameters can be configured. The WebUI supports LDAP certificate verification and import.

Access Control Policies Based on Login Time, IP and MAC Addresses

The WebUI supports whitelist-based access management. A whitelist containing the login period, IP network segment, and MAC addresses allowed is configured. Only the users who meet the conditions specified in the whitelist can access the system through the management channel and configure and manage servers.

5.8 Key Management

iBMC key management uses a two-layer structure, as shown in the following figure.



Generation of a Root Key

A root key consists of two components. Each component is of 64 bits.

Component 1 is hard-coded.

Component 2 is stored in a file system that is readable and writable.

Salt is hard-coded.

Component 2 is stored in a file system that is readable and writable. Only the system administrator has read and write permission. This facilitates updates of root keys.

The components of a root key are generated from secure random numbers. The components obtained are hard-coded and stored in the file system.

Storage of Working Keys

Working keys are encrypted using the root key and saved in a file system that is readable and writable.

Backup of Working Keys

To prevent data loss, two copies of working keys are stored in different directories of the file system.

Working Key Integrity Protection

The root key is used to encrypt working keys to control access to the file containing working keys.

Generation of Working Keys

Before a version release, an external tool is used to generate the keys and encrypted data file and save them to a file system that is readable and writable. In other words, a default file comes with the delivery.

Update of Working Keys

Manual update is supported. Run the command for updating working keys. The system then generates working keys randomly. This key cannot be viewed.

5.9 Session Termination

A session can be terminated in either of the following ways:

Termination upon timeout: The mechanism of disconnecting silent connections upon timeout is used for CLI, web, and SFTP sessions. For example, a session will be terminated if no operation is performed within 5 minutes.

Manual termination: A user initiates a request to terminate a session. The system administrator can terminate sessions initiated by other users.

5.10 CLI System Hardening

The CLI is encapsulated so that it no longer supports Linux system commands. Only whitelisted commands can be executed on the CLI, minimizing the risks of network attacks.

6 Server System Security Design

6.1 Trusted computing

6.1 Trusted computing

The servers support the Trusted Platform Module (TPM) 2.0 and Intel's Trusted Execution Technology (TXT).

The servers support international standard encryption algorithms and cryptography algorithms (SM2, SM3, and SM4) developed by the Office of State Commercial Cryptography Administration (OSCCA).

The servers support integrity measurement of hardware, including the BIOS boot block, BIOS main block, and master boot record (MBR). BIOS implements hardware integrity measurement based on the TPM chip, not on Intel's TXT technology.

7 Secure Release

[7.1 Security Tool Scanning](#)

[7.2 End-to-End Assurance](#)

7.1 Security Tool Scanning

The software version was scanned by vulnerability scanners Nessus and AppScan to ensure that no high-level vulnerabilities exist.

The software version passed the malformed packet attack test and was tested by Codenomicon's tool to ensure that no critical problems exist.

Nessus

McAfee

NSFOCUS

AppScan

Codenomicon

7.2 End-to-End Assurance

Refer to the Huawei cyber white paper for Huawei's end-to-end network security assurance method.

http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_187368.pdf

8 Acronyms and Abbreviations
