Huawei Cloud Security White Paper

Issue 3.2

Date 2020-08-14

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2020. 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


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: https://www.huawei.com

Email: support@huawei.com

Introduction

Recent years have seen the rapid evolution of threats to cloud security, with new threats emerging at an alarming and increasing pace. Huawei Cloud, like most Cloud Service Providers (CSP) and cloud customers, has risen to the challenge by continuing to learn, explore, and mature, benefiting hugely from the process. In early 2017 Huawei Technologies Co., Ltd. ("Huawei") formally established its Cloud Business Unit ("Cloud BU"), raising the curtain on a new era for Huawei Cloud. Not just taking these emerging security challenges in stride, Huawei Cloud also sees in them opportunities to offer our customers secure and trustworthy cloud services through collaboration with our ecosystem partners and in accordance with our committed lines of business, furthering our objective to both safeguard and add value to our customers' business.

A comprehensive set of highly effective cloud security strategies and practices has emerged through integrating leading cloud security concepts from across the industry and established security best practices from the world's leading CSPs with Huawei's expertise from years of cybersecurity experience, including its cloud security technologies and operational practices. As a result, Huawei Cloud has implemented multi-layered security architecture that provides in-depth defense and complies with all relevant regulations. Moreover, Huawei Cloud builds security into and continues to improve the security of its most commonly used Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) cloud services. Supporting all this is Huawei Cloud BU's highly autonomous and flat organization; its highly capable research and development (R&D) and operations and maintenance (O&M) teams, which stay abreast of the latest security developments; its cloud-optimized DevOps/DevSecOps[1] methodology and workflow; and its ever- flourishing cloud security ecosystem. Huawei Cloud will, together with our ecosystem partners, continue to make our customers our top priority and deliver high-quality cloud services with value-added security functions, advanced cloud security services, and security consulting services. The goal is to not only effectively protect the interests of our tenants, helping them with their business growth, but also enhance Huawei Cloud's market competitiveness and achieve long term, sustainable, and mutually beneficial results for Huawei Cloud, our customers, and our partners.

Huawei Cloud herein releases Huawei Cloud Security White Paper (the "White Paper"). The White Paper shares Huawei Cloud's extensive cloud security experience with our users and the industry at large, so as to help us all better understand and learn from each other, while jointly promoting the openness and progress of both the cloud industry and cloud security industry.

This White Paper is intended for readers across a wide variety of industries and regions:

 Copyright © Huawei Technologies Co., Ltd.

- From our tenants, ecosystem partners, and communities to general Internet users;
- From small-, medium-, and large-sized enterprise customers to individual users;

From the decision-making executive level and the management level to cloud service-related technical personnel such as employees with positions in IT, security, and privacy, and to personnel in other cloud service-related positions, including marketing, procurement and contracting, and compliance audit, among others.

Note:

1. DevOps is an end-to-end engineering process and tool chain practice from R&D to O&M that has been created by the high-tech industry practitioners, as opposed to theorists, and matured along with the development of Web 2.0 and cloud services. Cloud services and other online features entail continuous integration and continuous deployment (CI/CD) that DevOps can support, as opposed to the traditional waterfall process and Security Development Lifecycle (SDL), which are no longer suited for the new demands. Security must be seamlessly embedded into and highly automated throughout the entire engineering process. As a result, a new security lifecycle management process called DevSecOps came into being. Based on Huawei's study on DevSecOps practices at world leading CSPs and major online service companies at home and abroad, an indisputable fact is that these companies are adopting DevOps/DevSecOps processes and tool chain practices company-wide at an accelerating rate. And the positive outcome of DevOps/DevSecOps adoption also proves that security risks that traditional IT security personnel are intuitively concerned with are unfounded. With security seamlessly embedded into DevOps, DevSecOps will not only not weaken security, but rather, it will effectively elevate security through a high degree of automation.

 Copyright © Huawei Technologies Co., Ltd.

Contents

 Copyright © Huawei Technologies Co., Ltd.

 Copyright © Huawei Technologies Co., Ltd.

1 Cloud Security Strategy

Increasingly complex cybersecurity threats and challenges are emerging at an alarming rate, as cloud services-related technologies and information and communications technologies (ICT) as a whole continue to evolve and progress. Cloud security threats in particular are becoming increasingly difficult to tackle. In fact, cybersecurity has become a multi-faceted challenge for cloud technology vendors and security companies across the globe. Only through collaboration at a global scale between vendors, service providers, and customers, as well as industry standards bodies, policy-, and law-makers, will we be able to effectively address these challenges and deliver positive measurable results. Along the way, we are committed to sharing our knowledge and experience, as well as staying both pragmatic and cooperative. By joining forces, we will be able to successfully handle unforeseen cloud security risks rooted in the misuse and abuse of technologies.

As a leading provider of ICT technologies and solutions worldwide, Huawei fully understands the importance of cybersecurity and cloud security to governments and customers around the world, their deep concerns regarding these areas, and the close attention that must be paid to them by government bodies and technology companies alike.

The cloud era has brought with it an endless variety of new security challenges, pervasive threats, and persistent attacks[1]. Huawei is increasingly cognizant of these security concerns and attaches high priority, through heavy investment, to technological competency, regulatory compliance, and ecosystem growth in cyber and cloud security. Furthermore, we have adopted practical and effective measures to continue accelerating our R&D in cloud security technologies and services, not only raising the security posture of our cloud products and services but also improving our cloud security compliance and ecosystem. We are committed to establishing mutual trust with stakeholders and helping our cloud customers manage their cloud security risks. Huawei asserts that the establishment of an open, transparent cloud security solution framework will be instrumental to sustainable progress across the entire cloud service industry, and especially to the promotion of cloud technology innovation.

Huawei Cloud upholds Mr. Ren Zhengfei's directive to "**Place the company's responsibility for safeguarding our customers' cybersecurity and business above our own commercial interests.**" Embracing a security-first corporate culture, Huawei Cloud continues to leverage company-level security competencies and make headway in cloud security through practical measures and steadfast

 Copyright © Huawei Technologies Co., Ltd.

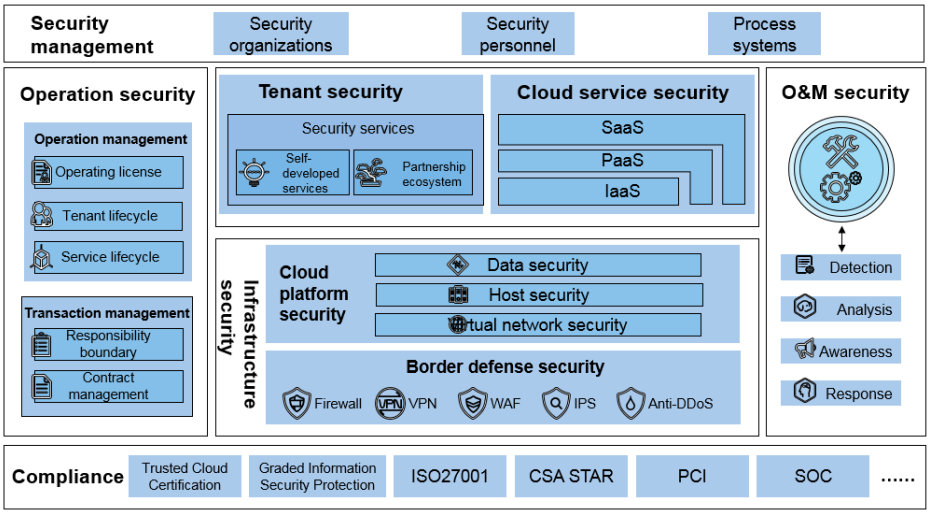
efforts. Cloud security at Huawei dates back to year 2000 when Huawei started R&D in the field of security technologies and Huawei Security Test Lab opened for business. In the nearly 20 years since then, Huawei has spared no effort in strengthening our security capabilities, striving to enhance the R&D and O&M of our cloud services and cloud security services every step of the way, and eventually bearing fruit in the form of Huawei Cloud's full-stack multi-layered security control environment:

- 2003: launched the industry's first firewall that was based on a network processor (NP) architecture.
- 2008: established a joint venture with Symantec Corporation named Huawei-Symantec Technologies Co. Ltd., focusing on security product R&D.
- 2011: opened Security Competence Center to specialize in product security capability R&D
- 2012: ranked No. 1 in market share in mainland China's cybersecurity product market.
- 2015: launched online cloud-based security solutions and services.
- 2016: deployed cloud security capabilities and solutions worldwide, for example Key Management Service (KMS) and Anti-DDoS Service went online in Germany and Spain.
- 2017: released a series of value-added advanced cloud security services such as the terabyte-level Anti-DDoS Service and Database Security Service (DBSS), which features a built-in database firewall.
- 2018: launched the dedicated hardware security module (DHSM).

Cybersecurity and privacy protection are Huawei's top priorities. Moving forward, Huawei Cloud hereby makes the following cybersecurity commitment: **Huawei Cloud shall take data protection as our core; technological security capabilities as our foundations; compliance with applicable cybersecurity laws, regulations, and industry standards as our castle walls; and the wider security ecosystem as our moat. Leveraging Huawei's unique software and hardware advantages, Huawei Cloud shall establish and maintain industry leadership and competitiveness with well-managed cloud security infrastructure and services to protect Huawei Cloud services across regions and industries.** This commitment will serve as one of Huawei Cloud's key development strategies. Huawei Cloud not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, Huawei Cloud continues to build and mature in areas such as our security-related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to our customers. We will also openly and transparently tackle cloud security challenges standing should-to-shoulder with our customers and partners as well as relevant governments in order to meet all the security requirements of our cloud users.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Huawei Cloud security protection framework



- **Organization**: The Global Security and Privacy Committee (GSPC), being the highest cybersecurity management organization at Huawei, is responsible for company-level security policy decisions and the authorization of overall security strategies company-wide. As a key member of the GSPC, the Global Security and Privacy Officer (GSPO) is responsible for leading and guiding team efforts in developing security strategies, conducting joint and unified planning, as well as managing and supervising security organizations across departments such as R&D, supply chain management, marketing and sales, engineering, technical services, and other related function groups and business programs. The GSPO is also to ensure that cybersecurity is systematically practiced in each and every applicable function, area, and process, and work to actively enhance communication between governments, customers, partners, employees, and other stakeholders. Additionally, Huawei Cloud continues to fine-tune its recently-established flat organization that befits the continuous integration and continuous deployment (CI/CD) of cloud services.
- **Processes**: Security activities are fully integrated into key business processes at Huawei, including but not limited to R&D, supply chain management, marketing and sales, engineering, and technical services. The importance of security to quality management is systematically and effectively enforced in accordance with administrative policies and technical standards. Huawei monitors and improves our business processes by means of conducting internal audits on them and subjecting them to security accreditation and attestation by different nations' government agencies in charge of cybersecurity and independent third party audit/test agencies. As an example, Huawei obtained BS7799-2/ISO27001 certification for our security management system in 2004 and has maintained it ever since. By leveraging existing company-level business processes, Huawei Cloud has integrated the Security Development Lifecycle (SDL) that is adopted company-wide into the cloud service-oriented DevOps engineering workflow and related technical capabilities. As a result, the DevSecOps methodology and tool chain are taking shape with characteristics unique to Huawei. It will not only support the increasingly agile online releases of Huawei Cloud services, but also ensure end-to-end security from R&D to deployment.

 Copyright © Huawei Technologies Co., Ltd.

- **Personnel management**: Huawei Cloud strictly enforces Huawei's long-standing and highly effective personnel management mechanisms. All Huawei employees, partners, and contracted consultants must comply with the company's applicable security policies and undertake regular security training, cultivating a security-aware culture across the entire company and beyond. Huawei rewards employees who actively enforce cybersecurity policies and takes punitive actions against employees who violate policies, up to and including legal action.
- **Technical capabilities**: Huawei Cloud focuses on data protection, leverages the company's own strong security R&D capabilities, and develops and adopts world-leading technologies, striving toward the creation of a highly reliable and intelligent cloud security system and highly automated cloud security O&M. Additionally, real-time Big Data analysis of cloud security events helps zero in on the detection of Huawei Cloud's major security risks, threats, and attacks, and take measures for risk prevention, mitigation, and resolution. Huawei Cloud employs a robust multi-layered technological framework for cloud security threat protection, spanning monitoring, analysis, and response capabilities that can support the rapid detection, isolation, and recovery of security risks, threats, and attacks. Huawei Cloud's advanced technologies bring tenants convenience, security, and business value.
- **Compliance**: In regions within our cloud services coverage, Huawei Cloud actively facilitates dialogues with local regulators in order to better understand their concerns and requirements, share Huawei Cloud's knowledge and experience, and continue to bolster the legal and regulatory compliance posture of Huawei Cloud's technologies, services, and security. Furthermore, Huawei Cloud shares with our customers the reports of legal and regulatory compliance audits, avoiding non-compliance violations caused by inadequate information disclosure to our customers. Huawei Cloud also ensures that our tenant contracts accurately specify the security responsibilities of both sides. Huawei Cloud continues to foster and strengthen customers' trust in our services by obtaining cross-industry, cross-region cloud security certifications as well as other security certifications targeting key industries and regions, striving toward a secure cloud environment built for and trusted by regulators, customer executives, and tenants.
- **Ecosystem**: Huawei believes that no single organization or company has sufficient resources to tackle the increasingly complex risks and threats to cloud security. Therefore, Huawei Cloud calls on all our security partners worldwide to join forces in developing a cloud security business and technology ecosystem and in providing security services to our tenants. Huawei Cloud Marketplace welcomes security technology vendors, as well as organizations and individuals with competitive advantages to be a part of this ecosystem and provide cloud security services. At the same time, we also invite our cloud business partners to leverage their own unique experiences and insights in cloud services and the cloud security industry, and package their security services into best-of-the-breed cloud security solutions. Huawei Cloud is eager to share the cloud security market with all like-minded partners.

In addition, Huawei will continue to actively participate in the development of security standards by cloud security organizations and telecommunication standards organizations both in China and abroad. Huawei strives to not only

ensure the security of our customers worldwide but also contribute to the industry to the best of our ability.

In summary, Huawei is willing to stay open and transparent with governments, customers, partners, and industry organizations worldwide in developing all forms of interaction and collaboration in the field of cybersecurity. Together, we will be able to effectively address cloud security threats and challenges around the globe.

Note:

1. Cloud Security Alliance (CSA) has an ongoing project and work group that focuses on covering the latest cloud security challenges, threats and attacks in an organized manner. For details, refer to **CSA Cloud Security Top Threats**.

 Copyright © Huawei Technologies Co., Ltd.

2 Shared Responsibility Model

Cybersecurity at a traditional data center is tasked with protecting all that data center's technology assets so that all applications and services can operate without risk of outage in a stable, secure, and high-performance manner, ranging from internal-facing data center O&M to customer-facing IaaS, PaaS, and SaaS cloud services. However, there are significant differences between data centers running cloud services and those geared towards traditional IT. In terms of the overall security design and day-to-day security practices, cloud services-oriented data centers attaches more priority than traditional IT data centers to the following aspects:

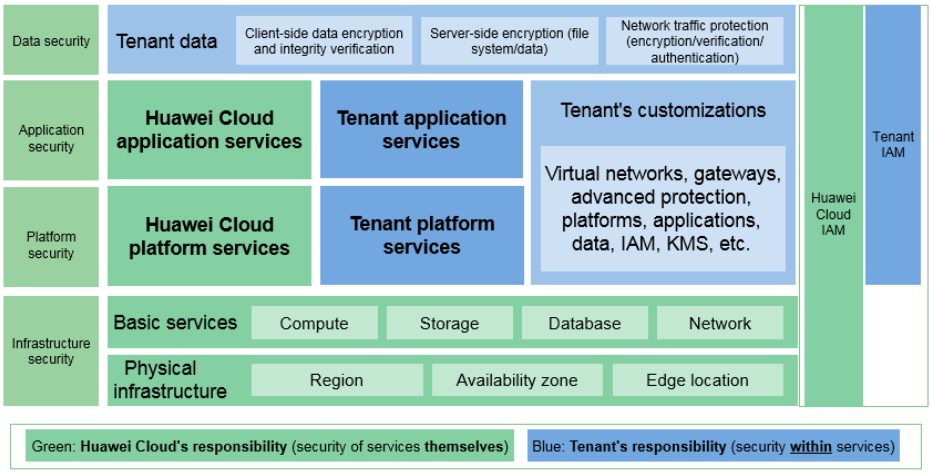
- Cloud security solution comprehensiveness and optimization (primarily through automation)
- Providing a highly adaptive, multi-layered, defense-in-depth architecture that spans infrastructure, platform, application, and data security
- Technological diversity and extensibility
- The highly customizable configuration, integration, and orchestration of security and privacy protection capabilities for both the CSP's O&M and tenants' O&M

In addition, Huawei Cloud security services support the customization of a variety of advanced security settings as per each tenant's security needs. These security services boast deep integration with security features, settings, and controls across the multi-layered architecture, seamless orchestration of a number of silo technologies as well as Big Data analytics and the resulting increasingly automated cloud security O&M.

In the following chapters we will describe how Huawei Cloud, as a CSP, makes such advanced cloud security systems and services a reality, while adhering to security best practices in both R&D and O&M. But first, this chapter introduces Huawei Cloud services' shared responsibility model, which Huawei Cloud has defined in accordance with industry common practices, as shown in the following figure.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Huawei Cloud shared responsibility model



Huawei Cloud is responsible for the green part, and tenants are responsible for the blue part. Huawei Cloud is responsible for the security of cloud services and provides secure cloud services. Tenants are responsible for the internal security of cloud services and securely use the cloud services.

Data security: Security management of tenants' service data in Huawei Cloud, including data integrity authentication, encryption, and access control.

Application security: Security management of application systems that support O&M and user services in Huawei Cloud, covering application design, development, release, configuration, and use.

Platform security: Security management of microservice, management, middleware, and other platforms in Huawei Cloud, covering platform design, development, release, configuration, and use.

Basic service security: Security management of computing, networking, and storage provided by Huawei Cloud, including the underlying management (such as the virtualization control layer) and usage management (such as VM management) of cloud computing, cloud storage, and cloud database services, as well as the management of virtual networks, load balancing, security gateways, VPNs, and private lines.

Physical infrastructure security: Security management of equipment rooms and environments for Huawei Cloud regions, availability zones (AZs), and terminals, and management of physical servers and network devices.

The primary responsibilities of Huawei Cloud are developing and operating the physical infrastructure of Huawei Cloud data centers; the IaaS, PaaS, and SaaS services provided by Huawei Cloud; and the built-in security functions of a variety of services. Furthermore, Huawei Cloud is also responsible for the secure design, implementation, and O&M of the multi-layered defense-in-depth, which spans the physical, infrastructure, platform, application, and data layers, in addition to the identity and access management (IAM) cross-layer function.

The primary responsibilities of the tenant are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a tenant subscribes on Huawei Cloud, including its customization of Huawei Cloud services according to its needs as well as the

O&M of any platform, application, and IAM services that the tenant deploys on Huawei Cloud. At the same time, the tenant is also responsible for the customization of the security settings at the virtual network layer, the platform layer, the application layer, the data layer, and the cross-layer IAM function, as well as the tenant's own in-cloud O&M security and the effective management of its users and identities.

2.1 Huawei Cloud's Security Responsibilities

Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers on which our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also the overall cloud O&M security and, in an even broader sense, the security compliance of our infrastructure and services. (Refer to section 3.1 Security Compliance for details on security compliance.)

- On the one hand, Huawei Cloud works to ensure the secure development, configuration, and deployment of our cloud products in order to operate our cloud infrastructure and services. On the other hand, Huawei Cloud is responsible for the O&M security of our cloud services, for instance, rapid security incident detection, isolation, and response in order to ensure fast recovery for our cloud services. At the same time, Huawei Cloud adopts a vulnerability management mechanism befitting cloud services to not only ensure prompt response to cloud service vulnerabilities but also support rapid release and continuous deployment of tenant-facing services. To support CSP O&M lifecycle management and avoid impact to tenant services, Huawei Cloud implements measures that not only continuously improve cloud products' default security settings, but also front-load security patching to the development phase and simplify security patch deployment. Additionally, Huawei Cloud's security responsibilities are also reflected in developing highly competitive value-added cloud security services for our tenants.
- Of all aspects of O&M security, Huawei Cloud attaches the highest priority to infrastructure security and privacy protection. Infrastructure consists primarily of the physical environment supporting cloud services, in-house-developed software and hardware, and the systems and facilities for the O&M of computing, storage, network, database, platform, application, IAM, and advanced security services. In addition, for third-party security technologies or services with which Huawei Cloud supports in-depth integration, Huawei Cloud is responsible for the O&M security of those technologies and services when they operate within Huawei Cloud.
- Huawei Cloud is responsible for supporting the secure configuration and version upkeep of our cloud services.
- With regard to tenant data, Huawei Cloud is responsible for providing comprehensive data protection functions to achieve confidentiality, integrity, availability, durability, authentication, authorization, and non-repudiation while also being responsible for the security of related functions. However, Huawei Cloud is merely the trustee of tenant data whereas a tenant retains sole ownership of its data and controls its data usage. Huawei Cloud prohibits any O&M personnel from accessing tenant data without proper authorization.

- Huawei Cloud pays close attention to changes in internal and industry security compliance requirements and is responsible for ensuring regulatory and industry compliance as required for Huawei Cloud services. Huawei Cloud shares our compliance practices with our tenants and conducts internal and independent evaluations on our compliance posture for security standards specific to the industries that Huawei Cloud serves, with evaluation results kept reasonably transparent to our tenants.
- Huawei Cloud engages our business partners to provide tenants with cloud security consulting services and assist tenants in not only the security configuration of their virtual networks and virtual systems (including virtual hosts and guest virtual machines) as well as system- and DB-level security patch management, but also the configurations of virtual firewalls, API gateways, security incident response, disaster recovery, and advanced security services such as anti-DoS/DDoS protection.

2.2 Tenants' Security Responsibilities

Tenants of Huawei Cloud are responsible for security inside the IaaS, PaaS, and SaaS cloud services to which they subscribe, particularly the secure and effective management of the tenant-customized configurations of cloud services. This includes but is not limited to the security configurations to protect and securely operate virtual networks, virtual host and guest VM OSs, virtual firewalls, API gateways and advanced security services, all types of cloud services, tenant data, and identity and key management.

- Tenant-specific security responsibilities are ultimately based on cloud services that a tenant subscribes to, with the tenant's responsibilities tied to the specific default or customized security configurations that the tenant chooses to implement. With regards to each Huawei Cloud service, the tenant is solely responsible for the security configurations of all tenant-managed cloud service resources whereas Huawei Cloud is only responsible for providing tenants with the cloud resources, functional capabilities, and performance capabilities required for the execution of specific security tasks by the tenant.
- The tenant is responsible for the security configurations that the tenant deems necessary inside any services that the tenant subscribes to, such as the security policy configurations of tenant-managed virtual firewalls, gateways, and advanced security services; the security configurations and management tasks (for example, software version and security patch management) for the tenant's virtual networks, virtual hosts, and guest VMs; and the security configurations of platform-level services such as container security management and Big Data analytics. The tenant is also responsible for the security management of any application software, service or utility that it deploys and operates on Huawei Cloud.
- When configuring cloud services, the tenant is responsible for conducting adequate pre-production testing of security configurations in order to prevent adverse effects on their applications and to minimize business impact. For the security of the majority of cloud services, the tenant needs to configure only accounts and grant them the necessary permissions to access resources, and to properly manage account credentials. A small number of cloud services require executing other tasks in order to achieve desired security effectiveness. Taking the database service as an example, while Huawei Cloud ensures the overall security of the service, the tenant must set up user accounts and

access control rules. In addition, because monitoring and management services as well as advanced security services boast numerous security configurations, tenants may seek technical support and professional service from Huawei Cloud and our partners to ensure optimal security.

- The tenant always owns and has full control of its data no matter which Huawei Cloud service it subscribes to. The tenant is responsible for security configurations that are necessary to ensure its data confidentiality, integrity, availability as well as identify authentication and authorization for data access. When using Identity and Access Management (IAM) and Data Encryption Workshop (DEW), the tenant is responsible for properly managing its own service accounts, passwords and keys, and adhering to industry best security practices for password and key creation, reset, and renewal. The tenant is also responsible for setting up individual user accounts and multi-factor authentication (MFA), using secure data transfer protocols as per industry standards for communication with Huawei Cloud resources, and enabling account activity logging for monitoring and audit purposes.
- The tenant is solely responsible for the regulatory and industry security compliance of any application and service that the tenant deploys and operates on Huawei Cloud that is not part of Huawei Cloud's service offerings. Accordingly, the tenant is responsible for the evaluation of its compliance with security standards specific to the industry or industries that it serves.

 Copyright © Huawei Technologies Co., Ltd.

3 Security Compliance and Privacy Protection

Strictly adhering to the customer-centric core values, Huawei Cloud fully understands the importance of customers' personal data security, respects and protects customers' privacy rights, and takes the privacy protection vision of "Respect and protect privacy, and let people enjoy the fully connected, intelligent world". Huawei Cloud solemnly and actively takes relevant responsibilities, considers cybersecurity and privacy protection as top priorities, and ensures that cybersecurity and privacy protection requirements can preferentially obtain support resources.

3.1 Security Compliance

Huawei Cloud will continue to ensure that its infrastructure and major cloud services pass evaluations conducted by independent, authoritative, and industry-reputable third-party security organizations as well as reviews by security certification agencies. Huawei Cloud provides on its infrastructure only those cloud services that comply with mandatory security standards and regulations. Industry security evaluations and certifications demonstrate Huawei Cloud's security strategies, policies, and risk management mechanisms in the people/organization, process, and technology aspects throughout the R&D and O&M lifecycle of its infrastructure and cloud services. Customers can also gain an unbiased and in-depth understanding of Huawei Cloud's capabilities and effectiveness in user data protection and cloud service security. One example that Huawei Cloud has achieved is the CSA STAR Gold certification, which is based on ISO/IEC 27001 and also includes the Cloud Control Matrix (CCM) security requirements, which cover 16 control domains including governance and risk management, data/application/infrastructure security, IAM, data center security, change control and configuration management, business continuity management and operational resilience, human resources, and supply chain management, etc.

Based on Huawei Cloud's shared responsibility model, Huawei Cloud also proactively established and continues to enhance its security compliance capabilities in its infrastructure (across the physical environment, network, and platform layers) to ensure the security and compliance of its services in supporting the business of cloud tenants.

 Copyright © Huawei Technologies Co., Ltd.

To date, Huawei Cloud has obtained the following security evaluations and certifications:

- GB 50174 Code for Design of Electronic Information System Room, Section A
- TIA 942 Telecommunications Infrastructure Standard for Data Centers, T3+ Standard
- CSA-STAR Gold
- ISO/IEC 27001
- ISO/IEC 27017
- CC EAL3+[1]
- PCI DSS[2]
- BSIMM
- China Graded Information Security Protection Level-3/Level-4[3]
- China Data Center Alliance (DCA) Trusted Cloud Certification, Gold Medal for Huawei Cloud O&M, Five Star Plus Certification, the highest grade, for Huawei Cloud OS
- Cybersecurity Review by Cyberspace Administration of China
- ITSS Cloud Computing Service Capability Evaluation Level 1 (Enhanced Level)
- SOC1 Type2 / SOC2 Type2
- SOC 3
- ISO 27018
- ISO 20000
- ISO 22301
- MTCS Level 3 (highest level of Singapore multi-layer cloud security certification)
- ISO 29151
- ISO 27701
- BS 10012
- OSPAR
- NIST CSF

In addition, Huawei Cloud proactively seeks out and adopts industry best security practices. For example, Huawei Cloud leverages the Minimum Security Baselines set out by the Center of Internet Security (CIS) and has integrated them into the Huawei Cloud DevSecOps process. CIS security baselines are a set of industry best practices for network and system security configurations and operations, which cover people (behavior of both end users and administration personnel), processes (network and system management) and technologies (software and hardware). This reaffirms that Huawei Cloud continues to stay aligned with the industry in complying with security standards and regulations.

Note

1. Huawei Cloud OS has achieved Common Criteria (CC) Evaluation Assurance Level (EAL) 3+ certification, with CC EAL4+ certification in progress.

 Copyright © Huawei Technologies Co., Ltd.

2. Payment Card Industry Data Security Standard (PCI DSS) is an information security standard applicable to any organization that handles payment transactions using major credit and debit cards.
3. Some Huawei Cloud nodes have passed the Level-4 assessment.

3.2 Privacy Protection

On the basis of Huawei's privacy protection system and industry best practices, Huawei Cloud has established its own privacy protection system, which complies with Huawei's top priorities of cybersecurity and privacy protection as well as privacy protection laws and regulations in and outside China. Huawei Cloud invests a large number of professionals and resources to support the research and application of new technologies and ensure the effective operation of the privacy protection system, ensuring that Huawei Cloud is leading the industry in terms of privacy protection and achieving Huawei Cloud's privacy protection objectives: Safeguard strict service boundaries, protect customers' personal data security, and help customers implement privacy protection.

Huawei Cloud has established a comprehensive, standard, and unified privacy protection system to enable privacy protection of the cloud platform and help customers implement privacy protection. Huawei Cloud formulates seven privacy protection principles (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability), and adopts the industry-recognized and advanced concept Privacy by Design (PbD[1]) as guidance to form its own privacy protection concept based on the actual situation. The privacy protection concept has been widely applied to various aspects of Huawei Cloud, including organization and personnel management, personal data security management on the cloud platform, and privacy services provided to customers. In addition, Huawei Cloud uses Privacy Impact Assessment (PIA[2]) to identify privacy risks and takes appropriate measures to eliminate or reduce risks. Huawei Cloud respects users' privacy rights. It provides a clear Privacy Statement and customer feedback channels in prominent positions on the official website, helping customers understand the privacy protection information of Huawei Cloud.

The Huawei Cloud research team is committed to developing Privacy Enhancing Technologies (PETs) to accumulate privacy protection engineering technical capabilities, so as to meet different privacy protection needs of customers. Huawei Cloud already has a series of PETs, including equivalence class, differential privacy, anti-tracking, blockchain-based private payment, and privacy-preserving computation.

For more information about Huawei Cloud privacy protection policies and statements, visit the official website of Huawei Cloud.

Note

1. First method of privacy protection for product R&D cycles. After recent years of development, PbD gradually evolves into the management concept of privacy protection. PbD advocates the comprehensive, early, and proactive integration of privacy protection into business and activities to help organizations take the initiative in privacy protection.

 Copyright © Huawei Technologies Co., Ltd.

2. PIA is widely used and recognized as a common privacy assessment and design tool in the industry. PIA helps organizations identify and reduce business privacy risks, and identify and minimize potential privacy risks.

 Copyright © Huawei Technologies Co., Ltd.

4 Security Organization and Personnel

In order to continuously improve employees' security awareness, protect customer interests, and boost product and service reputation, Huawei advocates company-wide for a mindset and practice wherein "everyone understands security", cultivating a security culture that is present 24/7, as well as dynamic and competitive throughout the company. The impact of such a culture runs through talent recruitment, new-hire orientation, initial and ongoing training, internal transfer, and internal re-training, all the way up to employment termination. Each Huawei Cloud employee is actively engaged in the buildup and upkeep of Huawei Cloud security, conducting security activities in accordance with company-level and Huawei Cloud BU-level policies and standards.

4.1 Security Organization

Huawei prioritizes cybersecurity as one of the company's key strategies, and therefore implements it top-to-bottom through its entire governance structure. From an organizational structure perspective, the GSPC functions as the highest cybersecurity management organizational unit, making decisions on and issuing approvals of the company's overall cybersecurity strategy. The GSPO and its office are responsible for formulating and executing Huawei's end-to-end cybersecurity framework. The GSPO reports directly to the company's CEO.

While upholding Huawei's cybersecurity strategy and standards, Huawei Cloud security group enjoys autonomy in its security planning and management activities. Huawei Cloud combines its R&D and O&M business functions for cloud services and cloud security services. As a result, its organizational structure is flat by design in order to accommodate the DevOps and DevSecOps processes as best suited for cloud services. Such flat organizational structure and cloud service-oriented processes meet the requirements of the rapid and continuous integration, delivery, and deployment of technologies and services. They also ensure that cloud services can meet the necessary security quality standards in order to effectively manage security risks. It is through functions such as the O&M of cloud service security and the R&D of cloud security engineering capabilities and cloud security services and solutions that Huawei Cloud is able to mature our service security compliance and security O&M, and effectively protect the interests of our tenants. Due to the unique importance of cloud security to Huawei Cloud, the cloud security group reports directly to the president of Huawei Cloud.

 Copyright © Huawei Technologies Co., Ltd.

4.2 Security and Privacy Protection Personnel

Huawei's technical security personnel consists of some of the world's leading experts and specialists in information security, product security, application security, system security, network security, cloud service security, O&M security, and privacy protection. Their primary responsibilities are as follows:

- Develop and implement cloud service DevOps/DevSecOps workflow and cloud security audit process; develop and promote the adoption of corresponding security tools chains for aforementioned workflow and process
- Actively participate in security quality assurance (QA) activities and security evaluations; conduct and/or manage internal and third party penetration tests and security assessments; track, investigate, and resolve any and all identified security threats
- Design, develop, maintain, and operate Huawei Cloud infrastructure security framework and its inherent security and privacy protection controls for business and IT applications, data and intellectual property, and so on
- Design, develop, maintain, and operate myriad security features for the IaaS, PaaS, and SaaS services of Huawei Cloud as well as its overall cloud security solutions
- Ensure compliance with data and privacy protection laws and regulations in each industry, region, and country that Huawei Cloud operates; advocate privacy protection best practices in cloud technologies and services; promote the release of cloud technologies and services that comply with privacy protection standards
- Design and develop a sustainable ecosystem for cloud security technologies and services

4.3 Internal Audit Personnel

Huawei's internal audit team reports directly to Huawei's Board of Directors and executive management. Stringent auditing activities play a key role in both promoting the adoption of cybersecurity processes and standards and assuring the delivery of results.

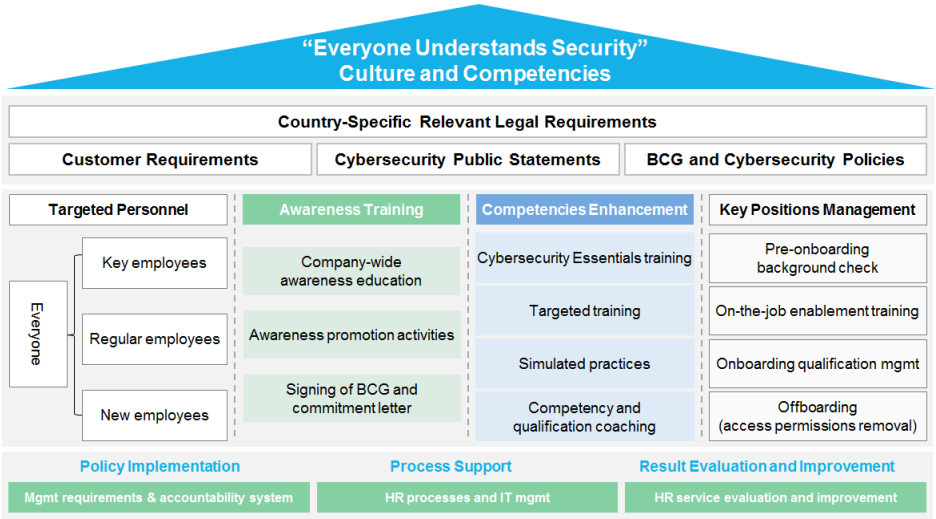
Huawei has set up a dedicated security audit team to periodically review compliance with security laws and regulations worldwide as well as internal security requirements. The team dedicates over ten members to perform a two-month long annual audit on Huawei Cloud operations worldwide, paying close attention to such Huawei Cloud aspects as legal, regulatory, and procedural compliance; business goal and milestone accomplishment; integrity of decision-making information; and security O&M risks.

Audit results are reported to Huawei's Board of Directors and executive management, who ensure that any and all identified issues are properly resolved and closed.

4.4 Human Resource Management

Consistent with that of the entire company, the HR management framework for Huawei Cloud security personnel has been long established on the basis of applicable laws. Cloud security requires HR to ensure that our staff's backgrounds and qualifications meet the requirements of Huawei Cloud services. Huawei Cloud employees must consistently demonstrate the required knowledge, skills, and experience. The behavior of each Huawei Cloud employee must comply with applicable laws, policies, and processes, as well as the Huawei Business Conduct Guidelines (BCG). A general breakdown of the framework is shown in **Figure 4-1**.

Figure 4-1 Huawei Cloud's security-integrated HR process framework



4.4.1 Security Awareness Education

To raise cybersecurity awareness company-wide, avoid non-compliance risks, and ensure normal business operations, Huawei provides employee security awareness training in three ways: company-wide awareness training, awareness promotion events, and the signing of BCG commitment agreements.

- **Company-wide awareness training**: Cybersecurity awareness courses are held periodically for employees to continually refresh their cybersecurity knowledge and help them understand relevant policies and systems. This way, they will be able to distinguish acceptable from unacceptable behavior, assume the responsibilities they have for any wrongdoing regardless of their intent, and abide by all company rules and legal requirements.
- **Awareness promotion events**: Company-wide cybersecurity awareness promotion activities are conducted in a variety of formats, such as community events, classic case study presentations, Cybersecurity Week, and animated security promotion films.
- **BCG commitment agreement signing**: Cybersecurity is covered in the BCG. Huawei holds BCG courses, exams, and signing activities annually to communicate cybersecurity requirements company-wide and raise employees' security awareness. By signing the cybersecurity agreement, employees commit to abiding by the company's cybersecurity policies and regulations.

 Copyright © Huawei Technologies Co., Ltd.

4.4.2 Security Competency

By utilizing industry best practices, Huawei has established a comprehensive cybersecurity training program, which implements security competency trainings for new hires as well as existing and newly-promoted employees. This program boosts employees' security competencies and ensures that employees are capable of delivering to our customers secure products, services, and solutions that are compliant with all relevant laws and regulations.

- **Cybersecurity fundamentals training**: Huawei offers security fundamentals training plans tailored to different roles and positions. Any new hire must take the cybersecurity and privacy protection on-boarding course and pass its exam by the end of his or her probation period in order to change status to full time employee. Existing employees must also regularly take courses befitting their job roles and responsibilities and pass the corresponding exams. Additionally, Managers are required to attend cybersecurity trainings and seminars.
- **Tailored trainings**: Through Big Data analytics, security issues typical in product R&D are detected and responsible parties identified. Tailor-made security trainings including relevant case studies, training classes, and practice questions are delivered to those responsible parties in order for them to contribute to the continuous improvement in security quality.
- **Practical drills**: Through the adoption of industry best practices, a platform for practicing cybersecurity field exercises has been developed with a scenario-based real world environment for employees to conduct red team and blue team exercises, and to facilitate participation in such exercises and exchanges among employees. This platform helps improve employees' overall skill level when it comes to hands-on security techniques.
- **Career development with security competency**: In order to help employees raise their security awareness and competency and more effectively benefit from cybersecurity trainings, Huawei integrates cybersecurity into our competency and qualification (C&Q) criteria. Employees must attend cybersecurity courses and pass the corresponding exams as part of the promotion vetting process.

4.4.3 Key Position Management

In order to streamline internal personnel management and to minimize any potential impact of personnel management on our business continuity and security, Huawei Cloud implements a specialized personnel management program for key positions such as O&M engineers. This program includes:

- **On-boarding security review**: Any new hire must pass a security review to ensure that his or her background and qualifications meet our cloud security requirements.
- **On-the-job security training and enablement**: Employees must undergo cybersecurity trainings and pass the corresponding exams on topics such as cybersecurity awareness, customer service code of conduct, and customer data and privacy protection. Furthermore, they must periodically adjust their training plans and take refresher courses/exams in order to keep up with changes in services, security threats, and regulations.
- **On-boarding qualifications management**: Key position personnel must pass the cybersecurity on-boarding exam and obtain the certification. The

 Copyright © Huawei Technologies Co., Ltd.

certification administration system issues an electronic certificate that is valid for no more than two years to any key position employee who has passed the exam. Prior to certificate expiry, the employees will be reminded by the system to retake the exam in order to renew the certificate.

- **Off-boarding security review**: A security clearance checklist is used to conduct the off-boarding security review for employee transfer or termination. This includes performing off-boarding tasks such as modifying or revoking accounts and privileges.

4.5 Security Violation Accountability

Huawei has established a rigorous security responsibility system and implemented accountability measures against security violations. On the one hand, Huawei Cloud carries out our responsibilities in accordance with the shared responsibility model and takes full responsibility for any security violation caused by Huawei Cloud in order to minimize tenant business impact. On the other hand, Huawei Cloud mandates that every employee be responsible for his/her actions and results at work, not only for the technologies and services of concern, but also in terms of bearing legal responsibility. Huawei Cloud employees are made well aware that if ever a security issue arises due to a security violation by an employee, it may have grave consequences for customers and the company as a whole. Therefore, Huawei Cloud always holds employees accountable based on behavior and results, regardless of their intent. Huawei Cloud will determine the nature of an employee's security violation and the level of his or her accountability based on the consequences and take disciplinary actions accordingly. Cases will be handed over to law enforcement if legal violations are involved. Direct and indirect management must also bear responsibility for their negligence, substandard management, and condonation for security violation(s) by their employee(s). In handling security violations, Huawei Cloud also factors in the perpetrator's attitude and cooperation during the investigation and adjusts the punishment severity accordingly before meting it out.

 Copyright © Huawei Technologies Co., Ltd.

5 Infrastructure Security

Huawei Cloud considers infrastructure security to be a core component of its multi-dimensional full-stack cloud security framework. Without infrastructure security that complies with security standards and regulations, cloud service security would be built on shifting sand, and entirely inadequate in its role of enabling and adding value to tenant business and safeguarding tenant security. To cloud service tenants, a CSP's infrastructure has a relatively low degree of transparency and openness, which directly affects the trustworthiness of the CSP's cloud security. The security compliance and standards compliance certification conducted by third-party assessment organizations can reflect the unremitting efforts made by CSPs in infrastructure and cloud service security. On the secure infrastructure base built through Huawei Cloud, tenants can be more confident in moving their business to Huawei Cloud and leveraging our cloud services to grow their business. This chapter will address the security design and practices in the physical environment, network, platform, application (specifically application programming interface, hereafter referred to as API) and data aspects of Huawei Cloud's security framework.

5.1 Physical and Environmental Security

Huawei Cloud has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of *GB 50174 Code for Design of Electronic Information System Room* and T3+ standard of *TIA-942 Telecommunications Infrastructure Standard for Data Centers.* Huawei Cloud data centers are located on suitable physical sites, as determined from solid site surveys. During the design, construction, and operation stages, the data centers have proper physical zoning and well-organized placement of information systems and components, which helps prevent potential physical and environmental risk scenarios (for example, fire or electro-magnetic leakage) as well as unauthorized access. Furthermore, sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The Huawei Cloud O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and environmental safety of Huawei Cloud data centers.

 Copyright © Huawei Technologies Co., Ltd.

5.1.1 Physical Security

- **Data center site selection**: When choosing a location for a Huawei Cloud data center, Huawei Cloud factors in the risks of potential natural disasters and environmental threats, making sure to always avoid hazardous and disaster-prone regions and minimize the potential operational interruption by the surrounding environment of a Huawei Cloud data center. For example, Huawei Cloud data centers are always located in areas where there are no potentially hazard-causing laboratories, chemical plants, or other hazardous zones within 400 meters. Site selection also ensures the availability and redundancy of supporting utilities for data center operations, such as power, water, and telecommunication circuits.
- **Physical access control**: Huawei Cloud enforces stringent data center access control for both personnel and equipment. Security guards, stationed 24/7 at every entrance to each Huawei Cloud data center site as well as at the entrance of each building on site, are responsible for registering and monitoring visitors and staff, managing their access scope on an as-needed basis. Different security strategies are applied to the physical access control systems at different zones of the data center site for optimal physical security. Security guards strictly review and regularly audit user access privileges. Important physical components of a data center are stored in designated safes with crypto-based electronic access code protection in the data center storage warehouses. Only authorized personnel can access and operate the safes. Work orders must be filled out before any physical components within the data center can be carried out of the data center. Personnel removing any data center components must be registered in the warehouse management system (WMS). Designated personnel perform periodic inventories on all physical equipment and warehouse materials. Data center administrators not only perform routine safety checks but also audit data center visitor logs on an as-needed basis to ensure that unauthorized personnel have no access to data centers.
- **Safety measures**: Huawei Cloud data centers employ industry standard data center physical security technologies to monitor and eliminate physical hazards and physical security concerns. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and computer cage areas. CCTV is also integrated with infrared sensors and physical access control systems. Security guards routinely patrol data centers and set up online electronic patrol systems such that unauthorized access and other physical security incidents promptly trigger sound and light alarms.

5.1.2 Environmental Safety

- **Electrical safety**: Huawei Cloud data centers employ a multi-level safety assurance solution to ensure 24/7 service availability and continuity. Daily electricity consumption at data centers relies on dual power supply from different power substations. Data centers are equipped with diesel generators, which are run in the event of power outage, and also Uninterruptible Power Supply (UPS), which provides temporary power as a backup. Data center power lines have voltage regulator and overvoltage protection. Power supply equipment is configured with redundancy and power lines run in parallel to ensure power supply to data center computer systems.

 Copyright © Huawei Technologies Co., Ltd.

- **Temperature and humidity control**: Huawei Cloud data centers are fitted with high precision air conditioning and automatic adjustment of centralized humidifiers to ensure that computer systems operate optimally within their specified ranges of temperature and humidity. Hot and cold air channels for computer cabinets are properly designed and positioned. Cold air channels are sealed to prevent isolated hot spots. The space beneath the raised floor is used as a static pressure box to supply air to computer cabinets.
- **Fire control**: Huawei Cloud data centers comply with Level-1 design and use Class-A fireproof materials for their construction in compliance with country-specific fire control regulations. Flame retardant and fire-resistant cables are used in pipelines and troughs, alongside power leakage detection devices. Automatic fire alarm and fire extinguishing system is deployed to quickly and accurately detect and report fires. Automatic alarm system links with power supply, monitoring, and ventilation systems such that the fire extinguishing system can activate itself even when unattended, autonomously keeping fires under control.
- **Routine monitoring**: Huawei Cloud personnel conduct daily patrols and routine inspections of power, temperature, humidity, and fire controls in all data centers, which allows for the timely discovery of safety hazards and ensures smooth operation of all data center equipment.
- **Water supply and drainage**: The water supply and drainage system at each Huawei Cloud data center is designed, implemented, and operated to an exacting standard, ensuring that main valves function as per specification and key personnel are aware of valve locations. This prevents water damage to the data center equipment, especially computer information systems. Data center buildings reside on elevated ground with peripheral green drains and each floor is raised, which speeds up water drainage and reduces the risk of flooding. Data center buildings all meet Level-1 water resistance requirements, ensuring that rainwater does not seep through roofs and walls into the data center, and that there is proper drainage in case of a flood.
- **Anti-static control**: Huawei Cloud data centers are paved with anti-static flooring materials and have wires connect raised floor brackets to grounding networks, discharging static electricity from computer equipment. Data center roofs are fitted with lightning belts, and power lines are fitted with multiple-level lighting arresters, diverting the current safely to grounding networks.

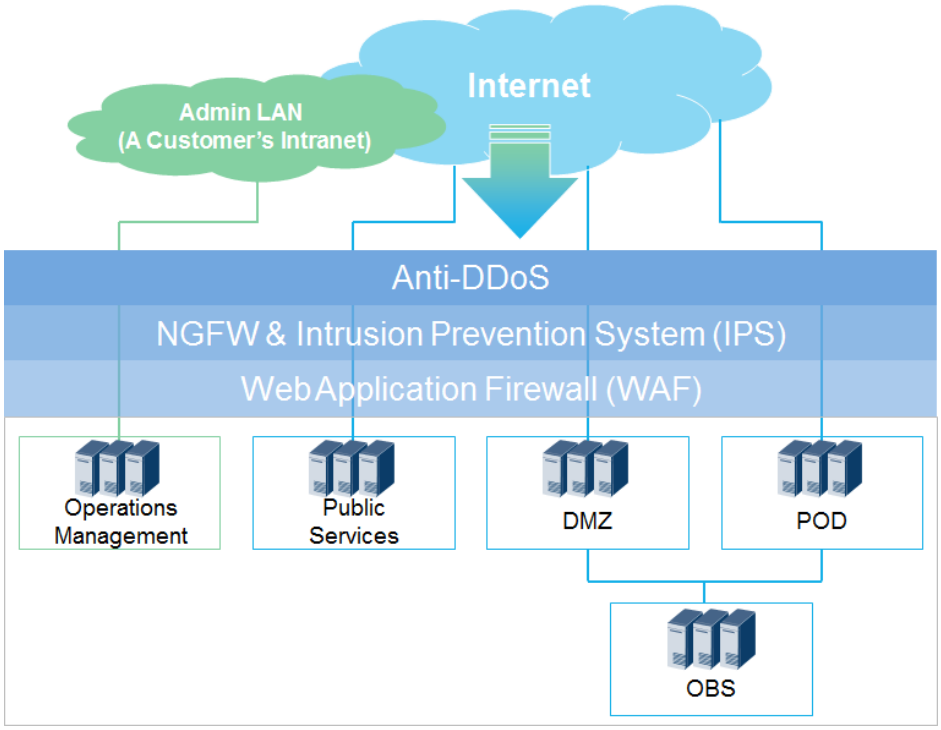
5.2 Network Security

Every Huawei Cloud data center has numerous nodes and complex functional zones. To simplify its network security design, prevent the propagation of network attacks in Huawei Cloud, and minimize the potential impact of attacks, Huawei Cloud defines both security zones and service planes, and implements a network segregation strategy in Huawei Cloud by referencing and adopting the security zoning principle of ITU E.408 and industry best practices on network security. Nodes in the same security zone are at the same security level. Huawei Cloud always takes into full consideration a wide variety of network security aspects ranging from network architecture design to device selection and configuration, as well as O&M. As a result, Huawei Cloud has adopted a set of network security mechanisms to enforce stringent controls and ensure cloud security. Some key examples of these network security mechanisms are multi-layered security isolation, access control, and perimeter protection for physical and virtual

networks, which will be covered in more detail throughout the rest of this chapter and the following chapters of the white paper.

5.2.1 Security Zone Planning and Isolation

Figure 5-1 Huawei Cloud platform security zones and network border protection



Based on business functions and network security risks, the Huawei Cloud data center network is mapped into different security zones to achieve network isolation using both physical and logical controls, which boosts the network immunity and fault tolerance[1] in Huawei Cloud in response to attacks from external threat actors and malicious insiders. The following list describes the five key security zones:

- **DMZ zone** mainly hosts public-facing cloud service frontend components (for example infrastructure components such as load balancer and proxy server, service components such as the service console, and the API Gateway). Tenants' access behavior (through the Internet or their own VMs on the public cloud) is untrusted, hence the need for a dedicated DMZ zone to isolate external requests and keep them from reaching cloud service backend components. Components in the DMZ zone are faced with more serious security threats and risks than other zones. Therefore, in addition to deploying firewalls and anti-DDoS appliances, Huawei Cloud also has deployed technologies such as web application firewall (WAF) and intrusion detection/prevention system (IDS/IPS) in order to further bolster infrastructure, platform, and application security.
- **Public Services zone** primarily hosts IaaS, PaaS, and SaaS service components (for example, OpenStack at the cascading layer), IaaS, PaaS, and SaaS service control components, and some infrastructure service components (for example, DNS, NTP, and patch management service). Components in the

 Copyright © Huawei Technologies Co., Ltd.

public service zone support restricted access by tenants based on business needs only. Tenants' requests to access components and services in this security zone must go through the DMZ zone. Huawei Cloud administrator-level personnel are allowed to access this security zone from the internal network for O&M purposes.

- **Point of Delivery (POD) zone** provides infrastructure resources as needed by tenants, including compute, storage, database and network resources, for example, tenants' VMs, disks, and virtual networks. Resources are isolated between tenants through multi-layered security controls to ensure that one tenant cannot access another's resources. In this security zone, the platform management plane and data storage plane are isolated from each other and also from the tenant data plane. This security zone may also host anti-DDoS and IDS/IPS appliances or services to inspect tenants' ingress and egress traffic, fend off attacks, and protect tenants' business.
- **Object-based Storage (OBS) zone** hosts object-based storage systems that provide the object-based storage service, which stores tenants' confidential data, necessitating this dedicated security zone, isolated from others. At the trust boundary of this security zone, tenants need to utilize and configure access control policies by utilizing and configuring Huawei Cloud's built-in security components based on their own requirements. This way, tenants' access requests from any tenant space to this security zone do not need to go through the DMZ zone. However, tenants' access requests from the Internet to this security zone must go through the service console or the Application Gateway in the DMZ zone due to the higher security risks involved.
- **Operations Management (OM) zone** hosts OM components. Huawei Cloud OM personnel must first log onto the Virtual Private Network (VPN) to connect to this security zone and then log onto managed nodes through bastion hosts. Huawei Cloud administrator-level personnel can access OM interfaces of all security zones from this security zone. This security zone does not expose its interfaces to any other security zone.

In addition to the above-mentioned security zoning for every Huawei Cloud data center's network, distinct security levels within different security zones are also defined for Huawei Cloud. Attack surfaces and security risks are determined based on different business functions. For example, security zones that are directly exposed to the Internet have the highest security risks, whereas the OM zone that exposes no interface to the Internet therefore has a much smaller attack surface, lower security risks, and less challenging to manage.

Note:

1. A Huawei Cloud data center, unlike a traditional IT data center, requires different mechanisms to achieve security zoning and network segregation. Just firewalls alone are inadequate. The adoption of newer, more innovative technologies such as software-defined perimeter (SDP) is inevitable. Furthermore, trust boundaries and perimeters are everywhere, and are no longer defined at the network layer only. Instead, they have moved up from network layer to the platform layer and application layer, and even all the way up to the user and identity layer, all of which require proper access control. Network security zoning as covered in this segment is at best an integral component of the Huawei Cloud multi-layered full stack security framework.

 Copyright © Huawei Technologies Co., Ltd.

5.2.2 Service Plane Planning and Isolation

To ensure that services run by tenants do not affect Huawei Cloud administrative operations and that devices, resources, and traffic are properly monitored and managed, different communication planes have been designed and built into Huawei Cloud's network based on their different business functions, security risk levels, and access privileges. They include the tenant data plane, service control plane, platform OM plane, Baseboard Management Controller (BMC) management plane, and data storage plane. This ensures that network traffic for different business purposes is reasonably and securely kept in separate lanes, which helps achieve separation of duties, roles, and responsibilities.

- **Tenant data plane** functions as the communication interface between tenant business service channels and VMs within a tenant space, and provides business applications to a tenant's users.
- **Service control plane** supports secure data exchange through APIs for cloud services.
- **Platform OM plane** supports the backend O&M management of the cloud infrastructure and platform (including network, compute, and storage devices).
- **Baseboard Management Controller (BMC) management plane** functions as the backend management plane for the hardware of the cloud infrastructure servers, used for emergency maintenance.
- **Data storage plane** supports secure data transmission and storage between the compute and storage nodes in the POD zone only.

In addition, different service planes are designed in each security zone on an as-needed basis as per the specific isolation requirements of the services that the security zone hosts. For example, the POD zone has a tenant data plane, platform OM plane, service control plane and BMC management plane. But the OM zone has only a platform OM plane and BMC management plane. The combined implementation of both security zones and service planes contributes to a network security isolation design that has more layers and more dimensions, also including both physical and logical controls, all of which form a mere portion of Huawei Cloud's full stack protection framework.

5.2.3 Advanced Perimeter Protection

The highly effective multi-layered full stack security protection framework of Huawei Cloud also includes a number of perimeter protection mechanisms, which include various in-house-developed advanced perimeter protection functions in addition to the aforementioned security zoning and business service plane planning and isolation as implemented through conventional network technologies and firewalls. Huawei Cloud has deployed and configured its various advanced perimeter protection capabilities at the public-facing cloud edge perimeter and the trust boundaries in between security zones internally. The following list provides details on three such flagship advanced perimeter protection capabilities[1] that have been developed by Huawei:

- **DDoS scrubbing under abnormal traffic and/or extreme load**: Huawei in-house-developed enterprise-grade anti-DDoS appliances, which are deployed at the perimeter of each cloud data center network, detect and scrub abnormal traffic and mega load attacks. Anti-DDoS appliances also provide

 Copyright © Huawei Technologies Co., Ltd.

tenants with the ability to fine-tune the anti-DDoS service. A tenant can customize traffic threshold parameters to fit its business application types and check attack and protection status.

- **Network intrusion detection and prevention system (IDS/IPS)**: In order to detect and intercept attacks from the Internet as well as east-west attacks between tenants' virtual networks, network IPS appliances are deployed on Huawei Cloud's network, including but not limited to the public-facing network perimeter, trust boundaries of security zones, and tenant space perimeter. IPS in Huawei Cloud can analyze real-time network traffic and trigger blocking on various intrusions such as protocol attacks, brute force attacks, port and vulnerability scanning, virus and Trojan horse attacks, and attacks targeting specific vulnerabilities. Based on network traffic, IPS can also provide information needed to help locate and troubleshoot network issues, assign direction-specific load throttling policies, and apply customized detection rules accordingly in order to protect application and infrastructure security in the production environment.
  - **Web application security**: Huawei Cloud has deployed web application firewalls (WAFs) to fend off web attacks such as layer 7 DDoS, SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), attacks targeting component-specific vulnerabilities, and identity impersonation. The WAF primarily protects public-facing web-based application services and systems in the DMZ zone.

Note

1. Firewalls, as an important technology for advanced perimeter protection, have reached technology maturity, with its functions and features well understood and widely adopted, hence not covered in this section. For further details, refer to section 6.1.1 ECS and section 6.2.1 VPC.

5.3 Platform Security

Huawei Cloud's Unified Virtualization Platform (UVP) abstracts physical server resources such as CPU, memory, and input/output (I/O) resources, and converts them into a pool of logical resources that can be centrally managed, flexibly scheduled, and dynamically assigned. Based on the logical resources, the UVP provisions on a single physical server a number of VM execution environments, which run concurrently but are isolated from each other. Huawei Cloud's UVP OS has been awarded the highest rating Five Star Plus Certification as part of Huawei Cloud's China DCA Trusted Cloud Certification.

To ensure Huawei Cloud platform security, Huawei Cloud has taken a minimalist approach in building an extremely stripped-down host OS and also performs security hardening on all its services. In addition, Huawei Cloud enforces stringent privilege access management (PAM) on Huawei Cloud administrators who have host OS access and enables comprehensive logging and centralized log management of all administrator-level O&M activities. Huawei Cloud administrators must pass two-factor authentication in order to access the management plane through bastion hosts.

The UVP, which directly runs on physical servers, supports virtualization capabilities and provides execution environments for VMs. The UVP ensures that

 Copyright © Huawei Technologies Co., Ltd.

each VM runs in its own properly assigned space such that it prevents a VM from attacking the UVP or other VMs.

The UVP uses technologies such as CPU isolation, memory isolation, and I/O isolation to isolate the virtual host OS from the guest VM OS. In addition, the UVP uses the Hypervisor to make the virtual host OS and the guest VM OS run with different sets of permissions, ensuring platform resource security.

UVP resource isolation mechanisms in the three areas of CPU, memory, and I/O are described in further detail in the following subsections.

5.3.1 CPU Isolation

CPU isolation mainly refers to the isolation between the virtualization platform and VMs, the permission allocation inside VMs, and the isolation between VMs themselves. CPU isolation is implemented in various modes such as running mode switching between root and non-root modes, permission allocation in each running mode, and allocation of virtual computing resource in the form of virtual CPU (VCPU). Through CPU isolation, the UVP is able to control the permissions for VMs to access physical resources and virtualized environment. Consequently, it achieves information and resource isolation between the virtualization platform and VMs as well as between different VMs, which prevents one VM from unauthorized access to information and resources belonging to another VM or the virtualization platform.

5.3.2 Memory Isolation

The virtualization platform is also responsible for providing memory resources for VMs and ensuring that each VM can only access its own memory. To achieve this objective, the virtualization platform manages and enforces the one-to-one mapping between VM memory resources and physical memory resources. VMs' access to memory resources entails address translation at the virtualization layer, which ensures that each VM can access only the physical memory resources to which it has been assigned and cannot access the memory resources belonging to other VMs or the virtualization platform.

5.3.3 I/O Isolation

The virtualization platform also provides each VM with its dedicated virtual I/O devices, including storage disks, network adapters, mouse and keyboard, which prevents unauthorized information disclosure due to I/O device sharing between VMs.

Each virtual disk corresponds to an image file or a logical volume on the virtualization platform. The virtualization platform ensures one-to-one mapping between a virtual I/O device used by a VM and its corresponding I/O management object on the virtualization platform such that, for example, only one virtual disk of a specific VM is associated with one unique image file. This also prevents I/O device sharing between VMs and achieves I/O access path isolation.

5.4 API Security

Huawei Cloud services support their published APIs for configuration management and integration with enterprise customers' IT management and audit systems.

 Copyright © Huawei Technologies Co., Ltd.

Considering the important functions that APIs support in cloud services and security threats that APIs face at the HTTP application layer, the industry generally regards APIs as crucial security perimeters of cloud services and employs multi-layered protection mechanisms and measures to safeguard API security. APIs of Huawei Cloud can be invoked through the API Gateway developed by Huawei, which supports the following API protection mechanisms and scenarios:

- **Identity authentication and authorization**: Huawei Cloud performs identity authentication on each API request through Huawei Cloud IAM integration. Only users who pass identity authentication are allowed to access and manage cloud monitoring information. The data transmission channel is encrypted using TLS.

  Tenants use API command interfaces to manage VMs. Therefore, API command privilege management can directly impact VM security. The Huawei Cloud API Gateway supports 2-step privilege management for user commands. When a user issues a command, not only is the user identity authenticated and authorized through the IAM service but also the command is inspected by the API gateway for authorization. Only when a user has the privilege to execute the command, the command is let through the API Gateway and delivered to the platform or application layer for execution. Upon receiving the command, the platform or application layer checks the user privilege again and executes the command only after confirming that the user does have the privilege to execute the API command.

  Each access request can be authenticated in either of the following modes:

  - **Token authentication**: Such an authentication request contains an authentication token, which is obtained by a tenant through the IAM interface upon authentication using their IAM username and password.
  - **Access Key ID/Secret Access Key (AK/SK) authentication**: Such an authentication request contains AK/SK authorization information. The AK/SK authentication mechanism of the API gateway requires that the client side, after obtaining AK/SK authentication information, must use the official SDK released by the API Gateway to sign the request and then send the request containing the signature to the API Gateway. The API Gateway validates the signature and authenticates the request.
- **Transmission protection**: API calls must use TLS-based encryption to ensure the confidentiality of data during transit. As of this writing, all public APIs supported by the API gateway use TLS 1.2 for encryption and support Perfect Forward Secrecy (PFS) security feature.
- **Perimeter protection**: Coupled with multi-layered advanced perimeter protection mechanism including anti-DDoS, IPS and WAF, the API Gateway can effectively protect against various threats and attacks. By offloading the decryption of TLS encrypted traffic to the load balancer, the multi-layered advanced perimeter security mechanism is able to monitor plaintext traffic inbound or outbound through the API Gateway and block attacks as needed. Built upon the advanced perimeter protection mechanism, the API Gateway being a unique security perimeter for cloud services also provides the following protection measures:
  - **API registration**: Only APIs registered with the API Gateway can be accessed by tenants.
  - **ACL rule-based access restriction**: Tenants can configure tenant-specific and network segment-specific information. Based on the ACL information

that tenants have configured, the API Gateway restricts access to APIs by specified tenants or from specified network segments. Furthermore, every ACL rule by default restricts its administration domain to the domain name op_service, preventing access to management domain interfaces from external networks.

  - **Replay attack prevention**: When the API Gateway receives an expired request, it rejects the request to prevent replay attacks.
  - **Brute force attack prevention**: Upon receiving an AK/SK request, if the brute force attack prevention mechanism of the API Gateway detects that the number of failed request attempts exceeds the maximum number allowed, the API Gateway rejects the request, and the AK/SK lockout timer is triggered.

- **API traffic flow control**: The API Gateway controls the frequency of each user's API access in order to ensure the availability and continuity of API-based access. The API Gateway supports the configuration of requests per second for flow control on a per-API and per-tenant basis. Flow control information must be configured on the API gateway for each public API. The API Gateway achieves separate flow control for each setting according to the maximum API access count by all Huawei Cloud tenants within one time measurement unit and the maximum API access count by each Huawei Cloud tenant within one time measurement unit.

5.5 Data Security

Data security refers to the comprehensive protection of users' data and information assets through security measures spanning many aspects such as confidentiality, integrity, availability, durability, and traceability. Huawei Cloud attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. Huawei Cloud will continue to embrace industry-leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, Huawei Cloud will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business.

5.5.1 Access Isolation

- **Identity authentication and access control**: The access control capabilities of Huawei Cloud are facilitated through its Identity and Access Management (IAM) service. The IAM service is a security management service optimized for enterprise tenants. Through the IAM service, tenants can manage users and security credentials (such as access keys) in a centralized manner and control users' administrative privileges and cloud resource access permissions.

  The IAM service allows tenant administrators to manage user accounts and privileges to access resources within the corresponding tenant space. If an enterprise tenant requires resource access by multiple users for collaborative purposes, the IAM service can be used to prevent users from sharing account and password information, as well as assign permissions to users based on

 Copyright © Huawei Technologies Co., Ltd.

the least privilege principle. In addition, the IAM service supports security policy configuration for login authentication, passwords, and access control lists (ACL) to ensure user account and access security. In summary, the IAM service helps mitigate the security risks associated with enterprise tenant information.

- **Data isolation**: Huawei Cloud facilitates data isolation in the cloud through the Virtual Private Cloud (VPC) service, the VPC uses the network isolation technology to isolate tenants at Layer 3. Tenants can control their own virtual network construction and configuration. On the one hand, a tenant's VPC can be connected to the tenant's enterprise network traditional data center using VPN or Direct Connect service such that tenant's applications and data residing in its internal network can be seamlessly migrated to the tenant's VPC. On the other hand, the ACL and security group function of the VPC can be used to configure network security and access rules as per the tenant's specific requirements for finer-grained network segregation.

5.5.2 Transport Security

In the scenario where data is transmitted between clients and servers and between servers of the Huawei Cloud via common information channels, data in transit is protected as follows:

- **VPN**: The Virtual Private Network (VPN) service is used to establish a secure encrypted communication channel that complies with industry standards between a remote network and a tenant VPC such that a tenant's existing traditional data center seamlessly extends to Huawei Cloud while ensuring end-to-end data confidentiality. With a VPN-based communication channel established between the traditional data center and the VPC, a tenant can utilize Huawei Cloud resources such as cloud servers and block storage at one's convenience. Applications can be migrated to the cloud, additional web servers can be launched, and the compute capacity within a tenant space can be expanded so as to establish enterprise hybrid cloud architecture and also lower risks of unauthorized dissemination of a tenant's core business data.

  Currently, Huawei Cloud uses IPSec VPN together with Internet Key Exchange (IKE) to encrypt the data transport channel and ensure transport security.
- **Application-layer security: TLS and certificate management**: Huawei Cloud supports data transmission in REST and Highway modes. In REST mode, a service is published to the public as a RESTful service and the initiating party directly uses an HTTP client to initiate the RESTful API for data transmission. In Highway mode, a communication channel is established using a high-performing Huawei-proprietary protocol, which is best suited for scenarios requiring especially high performance. Both REST and Highway modes support TLS 1.2 for data in transit encryption and X.509 certificate-based identity authentication of destination websites.

  The SSL Certificate Management service is a one-stop-shop type of X.509 certificate full lifecycle management service provided to our tenants by Huawei Cloud together with world-renowned public certificate authorities (CA). It ensures the identity authentication of destination websites and secure data transmission.

 Copyright © Huawei Technologies Co., Ltd.

5.5.3 Storage Security

- **Key protection and management**

  Key Management Service (KMS) is a secure, reliable, and easy-to-use key escrow service that facilitates centralized key management in order for users to achieve better key security. The KMS employs Hardware Security Module (HSM) technology for key generation and management, preventing the disclosure of plaintext keys outside HSM. HSM is a hardware device that provides cryptographic capability and securely generates, stores, manages, and uses crypto keys. To protect tenants' crypto keys and mitigate the risks of crypto key leakage to the public, Huawei Cloud provides cloud HSM service using different HSM vendors in different specifications (such as industry standard encryption algorithms, and country-specific encryption algorithms) and cipher suite strengths, which allows tenants to select the options suitable for their real-world requirements, for example, third-party HSM certified by FIPS140-2.

  KMS enforces access control of all crypto key-related operations with logging enabled, which meets audit and compliance requirements. Currently, the following Huawei Cloud services have been interconnected with the KMS service:

  - Elastic Volume Service (EVS)
  - Object Storage Service (OBS)
  - Volume Backup Service (VBS)
  - Image Management Service (IMS)

- **DHSM**

  DHSM meets tenants' higher compliance requirements. Dedicated encryption is implemented for tenant services by using a hardware encryptor certified by the Office of the State Commercial Cryptography Administration (OSCCA) or FIPS 140-2 Level 3. The default two-node cluster architecture is used to improve reliability.

- **Data confidentiality and reliability assurance**

  Huawei Cloud offers data protection functions and recommendations for each cloud storage service. See **Table 5-1** for details.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-1 Confidentiality and reliability of Huawei Cloud storage services

Storage Service	Description	Confidentiality	Reliability
EVS	The EVS is a virtual block storage service that is based on a distributed architecture and can scale flexibly.	KMS provides crypto keys as needed. It supports the management of Customer Master Keys (CMKs) from generation to erasure. CMKs are used to encrypt and decrypt data encryption keys. The volume encryption function is also supported.	Three-copy data backup with data durability up to 99.9999999%. The VBS can be used to implement volume backup and restore and supports volume creation based on a volume backup.
VBS	The VBS supports data backup for the EVS services, which use VBS backups to roll back or restore EVS data.	The backup data on the encrypted disk is automatically encrypted for data security.	Backup data is stored across data centers, data durability up to 99.999999999%.
OBS	The OBS is an object-based mass storage service, which provides users with massive, low-cost, highly reliable, and secure data storage capabilities.	For server-side encryption, the OBS provides the following key management modes: **SSE-C mode**[1]: A user provides a key, and the OBS uses the key provided by the user and the MD5 value of the key for server-side encryption. **SSE-KMS mode**: The KMS provides and manages keys. When a user uploads an object to the bucket in the zone, the OBS automatically creates the CMK for data encryption and decryption.	Data durability up to 99.9999999999% and service availability up to 99.995%. Data integrity is checked using the hash before and after data storage, ensuring that the data to be stored matches the uploaded data. Slice redundancy is achieved by storing multiple slice copies on different disks after data slicing. The service backend automatically checks the slice integrity and promptly repairs damaged data

Storage Service	Description	Confidentiality	Reliability
RDS	The Relational Database Service (RDS) is an online relational database service that is based on the cloud computing platform. It is turnkey upon subscription and is stable, reliable, readily scalable, and easy to manage.	Data can be encrypted in static, tablespace, or homomorphic mode. The Huawei Cloud RDS encrypts data before storing it in the database. Encryption keys are managed by the KMS.	The RDS uses the hot standby architecture. If a fault occurs, the system automatically switches services to the standby node within 1 minute. Data is automatically backed up every day and uploaded to OBS buckets. Backup files are stored for 732 days. One-click restoration is supported.
IMS	The IMS provides user-friendly self-service and complete image management capabilities. Users can select images from the rich public image library and create private images in order to quickly create or bulk copy of Elastic Cloud servers.	Same as EVS above. In addition, Huawei Cloud supports two ways for encrypted image creation: setting up encrypted Elastic Cloud Servers and creating external image files.	Ensures private image redundancy by storing multiple copies. Data durability up to 99.999999999%.

Note:

1. SSE-C refers to server side encryption with customer-provided key.

5.5.4 Data Deletion & Destruction

After a user confirms data deletion, Huawei Cloud deletes the user data permanently to prevent data leakage.

- **Memory deletion**: Before the cloud operating system reallocates memory to users, Huawei Cloud clears (zeros out) the memory to prevent data leakage caused by data restoration using physical memory.
- **Data leakage prevention through encryption**: Huawei Cloud advises tenants to encrypt important data to be uploaded to the cloud for storage. If data needs to be deleted, tenants can directly delete related data encryption keys

to prevent data from being restored to plaintext before being completely deleted.

- **Deletion of stored data**: When a tenant deletes data, the data and corresponding metadata are both deleted from the system. The underlying storage area is reclaimed for the system to write other data, so that the original data cannot be read again. However, if data is deleted by mistake, tenants can use the recycle bin function of the EVS and multi-version control function of the OBS to determine whether to restore or permanently delete the data.
- **Disk data deletion**: Huawei Cloud zeros out the deleted virtual volume to ensure that data cannot be restored, thereby preventing malicious users from using data restoration software to retrieve the deleted user data and preventing information leakage.
- **Physical disk destruction**: When a physical disk needs to be decommissioned, Huawei Cloud permanently deletes the data present on the disk by means of physical disk degaussing and/or shredding as needed to ensure user privacy and avoid unauthorized data access. In addition, Huawei Cloud adheres industry standard practices and keeps a complete data deletion activity log for chain of custody and audit purposes.

 Copyright © Huawei Technologies Co., Ltd.

6 Tenant Services and Security

Huawei Cloud offers our tenants a range of cloud services including IaaS, SaaS, and PaaS. This chapter describes the services selected for their importance in helping tenants move to the cloud, protecting their security, and creating value for their business. The following categories of cloud services are included: compute, network, storage, database, data analytics, application, management, and security. For each of the cloud services covered, the basic technical features and security functions are introduced, as well as the security-related benefits that they bring to tenants. Note that because the vast majority of tenants are already familiar with rather commoditized security services such as virtual private network (VPN) services, which are not included in this chapter. Details about such services are available at **https://www.huaweicloud.com/en-us/**.

6.1 Compute Services

6.1.1 ECS

Elastic Compute Service (ECS) provides self-service virtual computing resources that tenants can subscribe on demand. Its cloud server instances, each of which is a VM, are virtual computing environments that include basic server components: CPUs, memory, an operating system, hard disks, and bandwidth. Tenants have administrator permissions for the instances that they create, and can mount hard disks, add NICs, create images, deploy environments, and perform other basic operations.

ECS provides multiple layers of protection and assurance, including host operating system security, VM isolation, and security groups. With its comprehensive security design covering virtual machines, hosts, and the networks that connect them, the service offers users a secure, reliable, user-friendly, and high-performing application environment.

- **Host security**: Huawei's Unified Virtual Platform (UVP) is used as the host operating system, which enforces isolation of CPU, memory, and I/O resources. For a detailed description of UVP security, see section 5.3 Platform Security.
- **VM security:**

 Copyright © Huawei Technologies Co., Ltd.

  - **Image hardening**: Huawei Cloud's professional security team performs security hardening on public images and patches any system vulnerabilities that may occur. Secure, updated public images are created with the help of an image factory and provided to users through Image Management Service (IMS). Pertinent hardening and patch information is also provided to tenants for reference during image testing, troubleshooting, and other O&M activities. When creating VMs, tenants can decide based on their applications and security policies whether to use an up-to-date public image or create a private image that has the required security patches installed.
  - **Network and platform isolation**: On the network layer, a virtual switch provided by the hypervisor on each host is used to configure VLAN, VXLAN, and ACL settings to ensure that the VMs on that host are logically isolated. Conventional physical devices, mainly routers and switches, are still used to physically isolate different hosts. On the platform layer, CPUs, memory, and I/O resources are logically isolated using UVP.
  - **IP/MAC address spoofing protection**: To avoid network issues that may occur if users change their IP or MAC addresses at will, IP and MAC addresses are bound together using DHCP snooping. Spoofing is further prevented by using IP Source Guard and dynamic ARP inspection (DAI) to filter out packets from unbound addresses.
  - **Security groups**: UVP supports the configuration of security groups to isolate VMs by group. Tenants can create security groups containing multiple VMs to enable those VMs to access each other while maintaining isolation from other VMs. By default, VMs in the same security group can access each other but any two VMs in different security groups cannot access each other. That said, access and communication between any two VMs in different security groups can also be customized by the tenant. For a detailed description of security groups, see section 6.2.1 VPC.
- **Remote access control**: Tenants can log in to their VMs over SSH to perform system maintenance. However, leaving the SSH port open is a relatively high security risk. For security purposes, tenants can enable access authentication by username/password or crypto key (public and private key pair). It is recommended that crypto key-based authentication be selected.
- **Resource management**: Tenants can manage ECS computing resources through API. API access requests must be authenticated and authorized through IAM before resources can be managed.
- **VNC security**: Tenants remotely access VMs in Virtual Network Computing (VNC) mode, use accounts and passwords for identity authentication, and use TLS 1.2 for encrypted transmission to ensure data transmission security.

6.1.2 IMS

An image is a template containing software and configurations for a cloud virtual server or bare metal server. Each image must contain an operating system and may additionally contain preinstalled applications such as database software. Huawei Cloud classifies images into public, private, shared and market images:

- Public images are standard operating system images provided by Huawei Cloud.

 Copyright © Huawei Technologies Co., Ltd.

- Private images are created by users for their own use.
- Shared images are custom images created by any user, maintained on a voluntary basis by the user community and provided for all users to use.
- Market images are high-quality third-party images that provide pre-installed operating systems, application environments, and various software.

Image Management Service (IMS) provides simple and convenient self-service management functions for images. Tenants can manage their images through the IMS API or the management console. Huawei Cloud staff periodically update and maintain public images, including applying security patches on them as required. The staff also provide security-related information for users to reference in deployment testing, troubleshooting, and other O&M activities. Users can deploy their ECS servers by selecting one of the public images provided, creating a private image from an existing cloud server deployment or an external image file, or using a shared image and participating in its development and maintenance.

IMS performs authentication based on the unified identity authentication service (IAM) of Huawei Cloud, and supports encryption and integrity verification for the transmission and storage of images. All data is stored in an image database on a trusted subnet, and public and private images are stored in different buckets using Object-based Storage (OBS). IMS comes with secure cryptographic algorithms and functions that enable users to select to encrypt their image files for storage. When a VM is created using an image, the integrity of the image is verified automatically to ensure that it is complete.

IMS requires tenants to have sufficient permissions to perform any operation, and keeps audit logs of major operations. Audit logs are retained indefinitely so that tenants can accurately trace operations performed over a long period of time.

6.1.3 AS

Auto-Scaling (AS) automatically adjusts resources in accordance with pre-defined policies to meet the requirements of tenant services. AS ensures that resource usage satisfies current service requirements without any manual intervention, scaling application systems out as service utilization grows with tenant business and scaling in as it declines. This helps reduce resource and labor costs and ensures that services operate in a stable and sound manner. By automating the allocation of resources and the enforcement of management and control policies, AS helps avoid the impact of resource exhaustion-type attacks as well as security risks resulting from human errors during manual allocation of resources.

AS can automatically add managed instances to an ELB listener, which delivers access traffic to all instances in a scaling group. This offers a higher level of protection against DDoS attacks than the traditional method of directly accessing a single backend server and service. AS can detect instance status in real time and launch new instances to replace those that are not operating properly. AS can also deploy the instances in a scaling group evenly across multiple availability zones (AZs) to improve system availability and support disaster recovery of applications deployed in the scaling group.

6.1.4 DeH

Dedicated Host Service (DeH) provides another form of elastic compute service through flexible leasing by host. It has all the functions and security features of ECS.

 Copyright © Huawei Technologies Co., Ltd.

DeH has the advantage of physical isolation because each host is leased by a single tenant. The system resources on each host cannot be preempted by other tenants, nor can a malicious tenant exploit vulnerabilities that may be found in hypervisor and attack the system.

6.1.5 BMS

Bare Metal Service (BMS) provides compute resources at the physical layer that tenants can lease on demand in a self-service manner. BMS instances, each of which is a physical server, are physical computing environments that include basic server components: CPUs, memory, an operating system, hard disks, and bandwidth. Tenants have administrator permissions for the instances that they create and can turn their servers on or off, mount hard disks, deploy environments, and perform other basic operations.

Like ECS, BMS also provides multiple layers of protection, including host and network security, remote access control, and other security management controls. For details, see section 6.1.1 ECS. More importantly, BMS has the unique security advantage of physical isolation. With its comprehensive security design covering hosts and networks, it ensures tenant security and offers a reliable, flexible, and high-performing application environment running on an isolated physical-layer compute environment.

6.2 Network Services

6.2.1 VPC

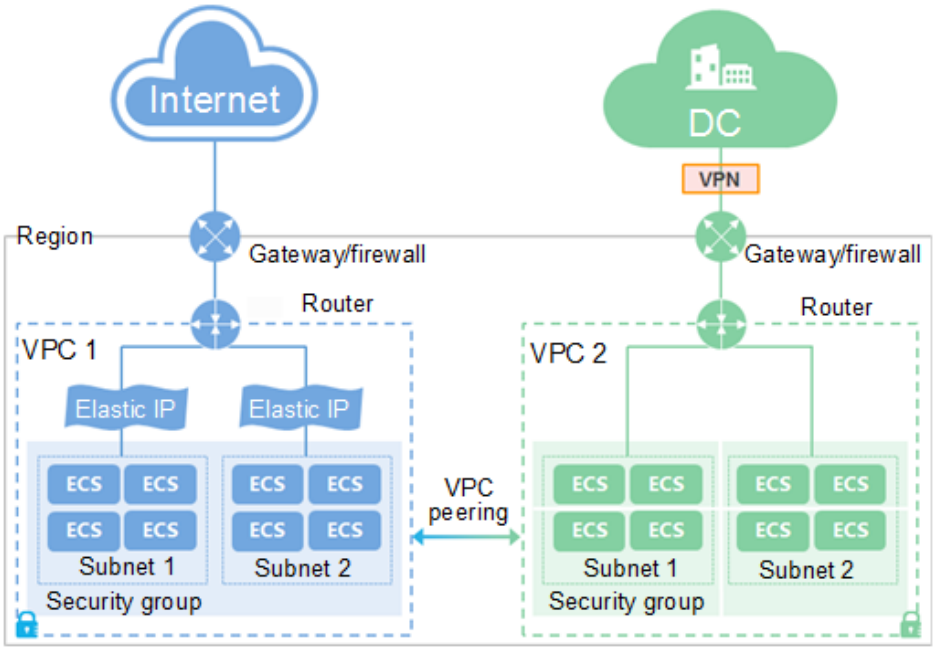
Virtual Private Cloud (VPC) creates an isolated, virtual network environment for Elastic Cloud Servers that users can configure and manage on their own. This enhances the security of user resources in the cloud and makes network deployment easier.

The advantages of VPC are as follows:

- Users can create their own virtual networks and have complete control of them.
- Users can apply for elastic IP addresses[1] to connect their Elastic Cloud Servers to public networks.
- VPNs can be used to connect VPCs with traditional data centers so that applications can be smoothly migrated to the cloud.
- Two VPCs can be interconnected using VPC peering.
- Users can configure DHCP and create, manage, and modify their networks conveniently and securely.
- VPC's network protection functions improve overall tenant cybersecurity.

Figure 6-1 illustrates the basic architecture of VPC.

Figure 6-1 Huawei Cloud VPC architecture



The following VPC functions are closely related to tenant network security:

- **IP subnets** are commonly used to provision IP addresses, DNS service, and other network functions for Elastic Cloud Servers. The Elastic Cloud Servers within a single VPC can communicate with each other by default regardless of subnet, but servers in different VPCs cannot by default.
- **VPN** is used to establish encrypted communication channels between remote users and their VPCs for direct access to the service resources located in the VPCs. The Elastic Cloud Servers deployed in VPCs cannot communicate with tenants' own traditional data centers or private networks by default. But tenants can configure and enable VPN to support such communication if required.
- **Direct Connect** establishes dedicated network connections between Huawei Cloud and tenants' operated private networks located in local data centers. These connections can be used to interconnect Huawei Cloud with tenants' own data centers, offices, and hosting colocations. Compared with connecting over the Internet, Direct Connect lowers network latency and offers a faster and more secure network experience for tenants.

VPC provides security functions at lower-stack layers of the Open System Interconnection (OSI). Tenants can configure these functions as needed based on their network security requirements. Network ACLs and security groups are without a doubt the most important security functions for Huawei Cloud as a whole and for the VPC(s) of every tenant. These two functions are described in detail as follows:

- **Network ACLs** are systems that specify, maintain, and enforce access control policies for one or more subnets. They determine whether to permit packets to enter or leave a subnet based on the inbound or outbound rules associated with that subnet.
- **Security groups** are sets of access rules for specified Elastic Cloud Servers. They provide unified access policies for servers within a VPC that trust each

 Copyright © Huawei Technologies Co., Ltd.

other and have the same security requirements. To enhance access security, users can place Elastic Cloud Servers in different security groups, thus being defined as different security zones, and create access rules for communication within and between security groups.

One set of access rules can be configured per security group. These rules include protocols, direction (inbound or outbound), sources (IP address segments, subnets, or security groups), and port numbers or port ranges that can be used to access servers in the security group. The protocols currently supported are TCP, UDP, and ICMP.

VMs are protected by the configured access rules as soon as they are added into a security group. Users can specify a security group during the VM creation process to immediately provide the new VM with the isolation and access control corresponding to that group. Each security group can contain VMs that are deployed on different physical servers. The VMs within the same security group can communicate with each other by default, but those in different security groups cannot. Note that communication between VMs in different security groups can be configured using custom rules if required.

Upon the creation of security groups, the default access rules are used by security groups that have no configured rules. The default rules permit all outbound packets and allow VMs in the same security group to access each other. If these rules are sufficient, it is not necessary to configure any custom rules.

As network ACLs and security groups are both major factors in enhancing the cybersecurity of Huawei Cloud VPCs, understanding the differences between them is important for creating effective network security policies for VPCs. These differences are summarized in **Table 6-1** for your reference.

Table 6-1 Differences between security groups and network ACLs

Security Groups	Network ACLs
Work on the Elastic Cloud Server instance level (first layer of protection).	Work on the subnet level (second layer of protection).
Support permit policies.	Support permit and deny policies.
If rules conflict with each other, only the parts in agreement take effect.	If rules conflict with each other, only the first of the conflicting rules takes effect.
Must be selected when an Elastic Cloud Server instance is created; take effect automatically on Elastic Cloud Server instances.	Cannot be selected during subnet creation. At a tenant's discretion if to set up a network ACL, add associated subnets and inbound/outbound rules, and then enable the network ACL in order for the associated subnets and the Elastic Cloud Server instances on those subnets to be protected.
Support packet filtering by 3-tuple (protocol, port, and destination IP address).	Support packet filtering by 5-tuple (protocol, source port, destination port, source IP address, and destination IP address).

 Copyright © Huawei Technologies Co., Ltd.

To enhance VPC network isolation, the platform also provides the following network security features:

- **VLAN isolation**: VLAN, which works on Layer 2, uses virtual bridging to support VLAN tagging and implement virtual switching to ensure secure isolation between VMs.
- **IP and MAC address binding**: This measure enhances the security of virtual networks by preventing VM users from spoofing IP or MAC addresses. DHCP snooping is used to bind IP addresses with corresponding MAC addresses. IP Source Guard and dynamic ARP inspection are also used to filter out packets from non-bound sources.
- **DHCP server isolation**: To ensure that IP addresses are allocated properly, users are not allowed to run DHCP servers.
- **DoS and DDoS mitigation**: The number of tracked connections to virtual ports is restricted so as to prevent traffic flooding attacks[2] from inside or outside the cloud platform.

Note:

1. Elastic IP addrsses are static public IP addresses. Binding an elastic IP address to an Elastic Cloud Server enables it to connect to the Internet.
2. Traffic flooding attacks interrupt service and management traffic by generating a large number of connection tracking entries, which exhausts connection tracking table resources and prevents legitimate connection requests from being received.

6.2.2 ELB

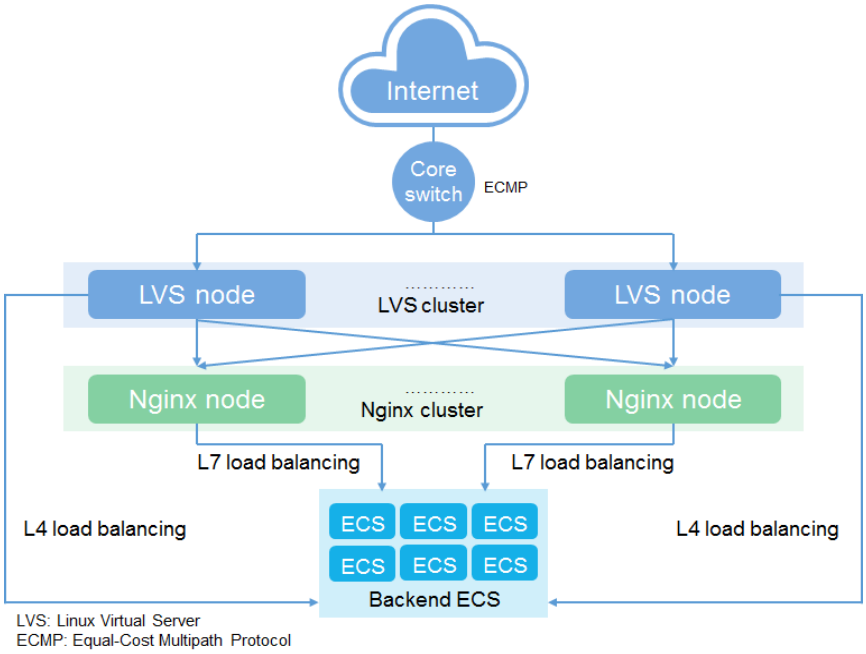
Elastic Load Balance (ELB) automatically distributes access traffic among multiple Elastic Cloud Servers, improving the ability of application systems to provide service and enhancing the fault tolerance of application programs. ELB has the following advantages over traditional load balancers:

- ELB ensures service availability with its redundant design. Faulty nodes are automatically removed, and traffic is rerouted to nodes that are operating normally.
- ELB is seamlessly integrated with AS to automatically scale processing capability as required by application traffic.
- A maximum of 100,000,000 concurrent connections are supported for applications with heavy traffic. Load balancing can be performed on Layer 4 (over TCP or UDP) or Layer 7 (over HTTP or HTTPS).

Figure 6-2 shows the basic networking design for ELB.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Huawei Cloud ELB networking diagram



ELB provides the following security functions:

- **IP address and port masking**: ELB allows external networks to see only a single IP address and service port(s); the actual IP address(es) and port(s) used by the backend are not exposed. This prevents the disclosure of network information and minimizes the attack surface.
- **Automatic scaling based on traffic status**: ELB can work with AS to provide more flexible scaling and better DDoS mitigation than the traditional method of directly connecting to single backend server(s) and service(s).
- **ELB Intranet security groups**: ELB security groups can be created on a tenant's intranet to ensure that tenant instances only receive traffic from the load balancer. Tenants can define allowed ports and protocols to ensure that traffic in both directions is sent through ELB.
- **Source IP address transparency**: ELB can transparently transmit source IP addresses when listening for HTTP and HTTPS services. This enables tenants to perform source tracing, collect connection or traffic statistics, enforce whitelisting for source IP addresses, and perform other tasks needed to meet enhanced security requirements. By implementing these through their applications, tenants can more quickly detect and respond to attacks.
- **SSL/TLS offloading and certificate management**: With SSL/TLS offloading, the SSL/TLS encryption and decryption of packets is performed on ELB, reducing the processing burden that these tasks place on the tenant's backend server. In this process, encrypted traffic is sent to ELB for decryption and then delivered to the tenant's backend server; likewise, outbound traffic is sent to ELB for encryption and then on to its destination. To use SSL/TLS offloading, tenants must upload any SSL/TLS certificates and private keys required to ELB for management.
- **Support for encryption protocols and cipher suites**: Tenants communicating with ELB over HTTPS can select an encryption protocol and configuration as required. TLS 1.2 is used by default. Tenants requiring higher security and

more robust encryption algorithms can select them from ELB's extended list of cipher suites.

6.2.3 DNS

Domain Name Service (DNS) provides a highly available and scalable DNS administration service running authoritative domain name servers. DNS translates human-friendly domain names and application resources into IP addresses, which are used to establish the network connections that give end users access to desired resources.

DNS can resolve domain names into ECS, OBS, RDS, and other service addresses for ease of access to service resources. Users can resolve their internal domain names using the DNS service. Domain names and their associated addresses can be customized using VPC. By resolving the challenge of registering and managing domain names for tenants' internal services, DNS reduces the complexity of service deployment and maintenance while also making high-availability design a possibility. DNS is built on Huawei Cloud's highly available and reliable infrastructure. The distributed nature of DNS servers helps to improve service availability and ensures that end users are routed to their desired applications. If a fault occurs on a service node, tenants can ensure service availability by modifying the domain name record to fail over to an operational node.

DNS provides the following key security functions:

- Reverse lookup records (IP address to domain name) can be used to reduce spam emails.
- The DNS cache is protected against viruses and attacks by regular updates, shortened time to live (TTL), and frequent cleansing.
- DNS includes DDoS mitigation to ensure that services can operate in a stable and secure manner. Behavioral profiling is performed on inbound traffic, attack traffic is scrubbed, and access from malicious IP addresses is restricted or blocked. The Layer 7 protection algorithm used by DNS scrubs and filters traffic layer by layer, offering complete protection against transport-layer and application-layer attacks. This anti-DDoS functionality also blocks DNS amplification attacks.
- DNS allows clients to use HTTP/HTTPS-based APIs to bypass traditional local DNS servers for domain name resolution. This effectively prevents domain name resolution results from being hijacked.

Tenants can use IAM to assign DNS service and permissions to their members. With access keys, resources can be accessed through API.

6.3 Storage Services

6.3.1 EVS

Elastic Volume Service (EVS) is a distributed storage service provided by Huawei Cloud. It provides hard disks for computing services such as ECS and BMS.

EVS implements access control based on the IAM service and ensures web operation security using measures such as HTTPS + password authentication,

 Copyright © Huawei Technologies Co., Ltd.

session management, interface-based permission control, and log auditing. It ensures the security and stability of the back-end storage system by means of access control, network plane isolation, and automatic alarms. In addition, it performs security hardening on the operating systems, databases, and web application components, and patches and upgrades open-source components in a timely manner to ensure system security.

EVS uses the multi-copy data redundancy protection mechanism and the synchronous write and read repair mechanism to ensure data consistency. If a hardware fault is detected, EVS automatically rectifies the fault in the background and quickly rebuilds data. The data durability reaches 99.9999999%. EVS provides the encryption option and allows users to manage keys, meeting requirements in different security scenarios.

6.3.2 CBR

Cloud Backup and Recovery (CBR) provides backup protection services for EVS, elastic cloud servers, and bare metal servers (EVS disks are referred to as disks, and elastic cloud servers and bare metal servers are referred to as servers in this document), supports snapshot-based backup services, and can use backup data to restore data on servers and disks. In addition, CBR supports the synchronization of backup data in the offline backup software BCManager, management of backup data on the cloud, and restoration of backup data to other servers on the cloud.

In terms of architecture design, CBR abstracts and models services based on the microservice architecture. It decouples service data and service logic, platform capabilities and product capabilities, as well as services between microservices. Microservices are designed based on the principles of separation between the frontend and backend, stateless services, and interface communication. When interacting with external systems and services, CBR takes into account the exceptions such as returned errors, restart, no response, and blocking, and isolates faults to ensure service availability. After faults are rectified, services can be automatically restored.

CBR controls access based on the IAM service, uses external interfaces based on the HTTPS-based RESTful architecture to protect access channels, uses the Network Time Protocol (NTP) to ensure time consistency between NEs in the system, and performs security hardening on the operating systems, databases, and web application components to ensure system security.

CBR supports integrity check of backup data. During backup and restoration, CBR uses CRC32C to verify the correctness of backup data to ensure that the data is not damaged or tampered with. CBR supports the backup and restoration of encrypted volumes. After obtaining keys through Huawei Cloud KMS, CBR encrypts and backs up encrypted volumes in the production storage to the backup storage, and restores encrypted backup data to the original or new volumes. Backup data of different tenants is stored in different buckets and isolated from each other, maximizing user data security.

6.3.3 CDN

Content Delivery Network (CDN) is an intelligent virtual network built on the existing Internet. Node servers are deployed on the network to distribute content from the origin server to all CDN nodes and provide functions such as content ingestion, retrieval, storage, caching, segmentation, play, and caching and

downloading web pages and files, enabling users to obtain the required content from the nearest server.

CDN uses security measures, such as password authentication, access control, minimum authorization, session management, input verification, and encryption, to ensure system security: Network layer security is ensured by means of security hardening, network plane isolation, security zone division, and network access control. Security of the operating system host layer is ensured by means of operating system security hardening and antivirus. Database security is ensured by means of database security hardening and database security design. Web containers are hardened and web applications are designed to ensure that service systems can effectively cope with security threats. Non-web application security is ensured by means of interface protocol security, sensitive data transmission security, and sensitive data storage security. CDN supports security functions such as anti-leeching and anti-tampering to ensure content security, and provides a complete communication matrix and security management documents to guide security O&M personnel through deployment and implementation.

6.3.4 OBS

Object Storage Service (OBS) provides tenants with object-based mass storage that is secure, reliable, and economical. Tenants can perform a variety of operations (creating, modifying, deleting, uploading, and downloading) to control their objects and buckets. OBS can be used by any type of users – regular users, websites, enterprises, and developers – to store any type of files. As an Internet-facing service, OBS can be accessed over its HTTPS web interface from any computer anywhere as long as it is connected to the Internet. Users can access and manage their stored data at any time over the OBS management console or client.

OBS offers a range of access controls, including ACLs and bucket policies, user authentication, and restrictions on tenant access requests. A series of mechanisms are also in place to protect tenant data: access log auditing, source and request type restrictions on access to resources shared across domains, URL anti-spoofing and validation, and server-side encryption. These ensure that data can be securely stored and accessed.

- **Access controls**: Requests to access OBS can be controlled through ACLs, bucket policies, and user signature verification.
  - **Access control list (ACL)**: OBS access permissions can be assigned to accounts by using an ACL. The ACL can grant all or certain accounts read, write, or full permissions on a per-bucket or per-object basis. Other access policies can also be configured, such as public access to a specified object (allowing all users read permissions only). By default, a bucket and the object(s) in the bucket can be accessed only by the creator of the bucket.
  - **Bucket policy**: The owner of a bucket can create a bucket policy to restrict access to the bucket. Bucket policies restrict access in a centralized fashion based on many conditions: OBS operation, applicant, resource, and other request information (such as IP address). Permissions can be assigned for specific buckets and specific accounts.

    Unlike ACLs, which only control permissions for single objects, bucket policies can affect multiple or all objects within buckets. Permissions for any number of objects in a bucket can be configured with a single

 Copyright © Huawei Technologies Co., Ltd.

request. Multiple objects can be specified by using wildcard characters in resource names and other fields, similar to regular expression operators, which allows the configuration of permissions for groups of objects.

OBS determines whether to accept or deny requests to access a bucket based on the policy configured for that bucket.

- **User signature verification**: To access OBS, users must provide an access key ID (AK) and secret access key (SK), which are authenticated by IAM. Therefore, OBS authenticates and authorizes user accounts with the AK and SK to ensure that OBS resources cannot be accessed without proper authorization. The headers of access requests sent to OBS contain authentication information generated based on the SK, request timestamp, and request type. OBS also independently performs URL encoding on bucket and object names before generating authorization information. Only accounts that pass crypto-based authentication and authorization can access OBS resources.

  The OBS API is fully compatible with Amazon's Simple Storage Service (S3) interface. Tenants can securely and reliably migrate their AWS data from AWS locations, specified by Amazon Resource Name (ARN), to Huawei Cloud using the AWS interface and Amazon Signature Version 2 or Version 4 Signing Process[1].

- **Data reliability and durability**: OBS provides highly reliable storage. With redundant node design and highly reliable networks connecting service nodes, it offers 99.99% availability. In addition, by using automated recovery technology that provides data redundancy and ensures consistency, OBS offers data durability of 99.9999999999%.

  OBS can retain multiple versions of an object so that users can conveniently retrieve or restore previous versions and quickly recover data in the event of an accidental operation or application failure. Version control provides users with a way to recover objects that were unintentionally deleted or overwritten. Note that version control is not enabled by default for new OBS objects. Unless version control is enabled, an object uploaded to a bucket that contains another object with the same name will replace the original object.

- **Access logs**: OBS can log bucket access requests for use in analysis or auditing. These access logs allow the owner of a bucket to comprehensively analyze the nature and type of requests to access the bucket and identify trends. Once logging is enabled for a bucket, OBS automatically records all access requests into a log file that is written to a user-specified bucket. Note that because these logs occupy tenants' OBS space and may cause additional storage fees to be incurred, logging is disabled by default. Tenants can enable it manually if required for analysis or auditing purposes.

- **Cross-Origin Resource Sharing (CORS)**: OBS supports standard CORS, allowing access to OBS resources across domain boundaries. CORS is a World Wide Web Consortium (W3C) standard for web browsers that defines interactions between web applications in one domain and resources in another. This enables static websites hosted on OBS to respond to requests from websites in other domains, provided that CORS is configured properly on the corresponding bucket. Website scripts and content can then interact across domains even when a same-origin policy (SOP) is in place.

- **URL anti-spoofing and validation**: To prevent URL spoofing for OBS tenants, URL validation based on HTTP header and referer as well as access whitelists and blacklists are supported. The source website from which a user is linked

to a destination website can be determined based on the header of the HTTP request. Requests that originate from an external website can then be denied or redirected to a specified web page. URL anti-spoofing and validation mechanism can also check requests against a blacklist or whitelist; access is granted when a match with a whitelist entry, otherwise denied or redirected to a specified web page.

- **Server-side encryption (SSE)**: Objects uploaded by users are encrypted on the server side into ciphertext before being stored. When an encrypted object is downloaded, the ciphertext is decrypted on the server side and then transmitted as plaintext. Keys managed by KMS (SSE-KMS) or provided by the client (SSE-C) can both be used for SSE:
  - In SSE-KMS, OBS uses keys provided by KMS to perform encryption. Users must create a key on KMS (or use the default KMS key) and then select that key for SSE when uploading objects.
  - In SSE-C, OBS uses keys provided by the user and the corresponding hash values to perform encryption. The interface used to upload objects can transmit keys, which OBS can use for server-side encryption. Note that OBS does not store user-provided key information, therefore users will be unable to decrypt their objects without the proper keys.

Note

1. Version 4 uses the more secure HMAC-SHA256 algorithm and includes user data in signature computation. The header used during computation can be user-defined, greatly improving the security of authentication requests. It is therefore recommended that Amazon Signature Version 4 be used during migration.

6.3.5 DES

Data Express Service (DES) enables offline mass data transmissions to Huawei Cloud using physical storage media such as eSATA hard disks. DES addresses the high cost and extended timeframe issues associated with moving massive amounts of data to the cloud.

To use DES, users log in to the management interface and create work orders. They then encrypt data according to DES requirements and store it on hard disks that are shipped to a Huawei Cloud data center.

For data security purposes, it is strongly recommended that users encrypt data before shipping. DES supports client-side encryption by a designated third-party encryption utility that uses the industry-standard AES-256 algorithm, and runs on Windows, Mac OS X, and Linux. The utility can create virtual drives on hard disks without generating any files. Users can access their data by drive letter. All files on the virtual drives are automatically encrypted and require a proper key for access.

Once hard disks are received by a Huawei Cloud data center, they are mounted on data center servers, and users are notified that their data is ready for them to upload. To upload data to the cloud, users need to log in to the management console and enter their AK, SK, and the key that was used to encrypt the hard disk. Users are then presented with a report of uploaded data for confirmation. After the uploaded data has been confirmed, the hard disks are shipped back to the tenant. To ensure the security of data transmissions, Huawei Cloud staff do

 Copyright © Huawei Technologies Co., Ltd.

not come into contact with keys or data belonging to tenants at any time during this process.

6.4 Database Services

6.4.1 RDS

Relational Database Service (RDS) allows tenants to rapidly provision different types of databases whose compute and storage resources can flexibly scale to meet tenants' service requirements. Automatic backup, database snapshot, and restoration functions are provided to prevent data loss. In addition, RDS parameter groups allow tenants to optimize their databases as needed by their business.

RDS provides many features to ensure the reliability and security of tenant databases, including VPCs, security groups, permissions settings, SSL-encrypted connections, automatic backup, database snapshots and point-in-time recovery (PITR), and deployment across AZs.

- **Network isolation**: RDS instances run in independent tenant VPCs and can also be deployed in subnet groups that span multiple AZs to provide high availability. After an RDS instance is created, the tenant is allocated an IP address in the subnet group for that instance to enable connection to the database. To control access to their databases, tenants can configure a range of IP addresses that are allowed to access their VPC(s) designated for database instance(s). After deploying an RDS instance on a VPC, tenants can configure a VPN to allow other VPCs to access it. Alternatively, tenants can deploy an Elastic Cloud Server in a VPC and connect to the database through a private IP address. Subnet groups and security groups can be configured in combination to isolate RDS instances and enhance instance security.
- **Access control**: Creating an RDS instance also creates a primary account for the instance that its creator can use to perform operations on it. The password of this account can be set by the creator. The primary account can be used to connect to the instance, create sub-accounts, and assign database objects to those sub-accounts based on service planning. This provides a certain degree of security isolation. Furthermore, during database instance creation, a security group can be selected in which to deploy the NICs for the instance. VPC can be used to set inbound and outbound rules for the RDS instance and thereby control the scope of access to it. Only the database listening port is allowed to accept connections. Once configured, a security group immediately take effect without the need to restart an RDS instance.
- **Transmission encryption**: The connections between database clients and servers can be encrypted with TLS. A specified certificate authority generates a unique service certificate for each RDS instance upon provisioning. Database clients can download a root certificate from the management console and provide this certificate when connecting to the database to authenticate the server and enable encrypted transmissions.
- **Storage encryption**: RDS can encrypt data before storage. Encryption keys are managed by KMS.
- **Automatic backup and snapshot**: These features help recover RDS databases in the event of a fault. Automatic backup is enabled by default, and backups can be stored for a maximum of 35 days. Automatic backup allows tenants to

perform point-in-time recovery (PITR) on their databases. Automatic backup performs a complete backup of all data and then incremental backups of transaction logs every 5 minutes so that a tenant can restore data to its status at any second before the previous incremental backup. Tenants can also manually create a complete backup, known as a snapshot. Database snapshots are stored in OBS buckets and removed upon deletion of the corresponding database instance. New instances can be created based on existing snapshots.

- **Data replication**: RDS instances can be deployed in a single AZ or across multiple AZs for high availability. When the latter option is chosen, RDS initiates and maintains data replication for database synchronization. High availability is achieved by having a secondary instance take over in the event that a failure occurs on the primary instance. It is also possible to create read-only MySQL database instances when operations are read-heavy. RDS maintains data synchronization between those read-only instances and primary instances, and tenants can connect to either type of instances as required by business to isolate read and write operations.
- **Data deletion**: When a tenant deletes an RDS instance, the data stored in the instance and the corresponding backup data in OBS are automatically deleted. The data in the instance cannot be viewed or restored.

6.4.2 DDS

Document Database Service (DDS) is a database service provided by Huawei Cloud to allow tenants to quickly provision different types of databases and support auto scaling of computing and storage resources based on service requirements. DDS provides functions such as automatic backup, database snapshot, database restoration, and Point-In-Time Recovery (PITR) to prevent data loss. In addition, DDS parameter groups allow tenants to optimize their databases as needed by their services.

DDS also provides multiple features such as VPC, security group, permission setting, SSL connection, automatic backup, database snapshot, PITR, and cross-AZ deployment to ensure the reliability and security of tenants' databases.

- **Network isolation:** To control access to their databases, tenants can configure a range of IP addresses that are allowed to access their VPCs. DDS instances run in independent tenant VPCs. Tenants can also deploy high-availability DDS instances in subnet groups that span multiple AZs. After a DDS instance is created, the tenant is allocated an IP address in the subnet group for that instance to enable connection to the database. After deploying a DDS instance on a VPC, tenants can configure a VPN to allow other VPCs to access it. Alternatively, tenants can deploy an Elastic Cloud Server in a VPC and connect to the database through a private IP address. Subnet groups and security groups can be configured in combination to isolate DDS instances and enhance instance security.
- **Access control:** Creating a DDS instance also creates a primary account for the instance. The password to this account can be set by the tenant. This primary account allows the tenant to operate the DDS instance database created by themselves. The primary account can be used to connect to the DDS instance database, create database instances and sub-accounts, and assign database objects to those sub-accounts based on service planning. This provides a certain degree of security isolation. A security group can be

 Copyright © Huawei Technologies Co., Ltd.

selected during database instance creation in which to deploy the NICs for the instance. VPCs can be used to set inbound and outbound rules for the DDS instance to control the scope of access to it. Only the database listening port is allowed to accept connections. It is not necessary to restart a DDS instance after configuring a security group for it.

- **Transmission encryption:** The connections between database clients and servers can be encrypted with TLS. A specified certificate authority generates a unique service certificate for each DDS instance upon provisioning. Database clients can download a root certificate from the management console and provide this certificate when connecting to the database to authenticate the server and enable encrypted transmissions.
- **Storage encryption:** DDS can encrypt data before storage. Encryption keys are managed by KMS.
- **Automatic backup and snapshot:** These features enable backup and snapshot for databases. Automatic backup is enabled by default, and backups can be stored for a maximum of 35 days. Automatic backup allows tenants to perform PITR on their databases. Automatic backup performs a complete backup of all data and then incremental backups of transaction logs every 5 minutes so that a tenant can restore data to its status at any second before the previous incremental backup. Tenants can also manually create a complete backup, known as a snapshot. Database snapshots are stored in OBS buckets and removed upon deletion of the corresponding database instance. Tenants can also restore data from an existing snapshot to a new instance.
- **Data replication:** DDS supports cluster and copy set high availability (HA) instances as well as single-node instances. Tenants can deploy HA instances in a single AZ or multiple AZs. When a tenant selects an HA instance, data is automatically synchronized between the DDS cluster and copy set. If a single node in the cluster or copy set is faulty, DDS automatically routes services to other nodes for HA.
- **Data deletion:** When a tenant deletes a DDS instance, the data stored in the instance and the corresponding backup data in OBS are automatically deleted. The data in the instance cannot be viewed or restored.

6.4.3 DCS

Distributed Cache Service (DCS) is a Redis-based distributed caching middleware service that enhances security, performance, and reliability. DCS is a storage system based on the data structure in memory and can be used as a database, cache, or simple message queue. It enables radius querying of geospatial indexes and supports data structures of multiple types: strings, hashes, lists, sets, sorted sets, bitmaps, and hyperloglogs. With built-in replication and Lua scripting, DCS supports simple transactions, data persistency, and cache replacement policies such as Least Recently Used (LRU).

DCS controls permissions using Huawei Cloud's unified role-based access control (RBAC) model, and tenants can perform operations only on their own resources, in this case, their own DCS instances. DCS instances are physically isolated, and tenant instances are isolated by VPC. DCS checks tenant permissions before allowing any operation. Only authorized operations can be performed, and all key operations are recorded in audit logs. Audit logs can be stored for a specified time for auditing and tracing purposes.

 Copyright © Huawei Technologies Co., Ltd.

DCS management plane data is stored on trusted subnets, and redundant copies are made to ensure data durability.

6.5 Data Analytics Services

6.5.1 MRS

MapReduce Service (MRS) provides high-performing hosted Big Data clusters that are reliable, scalable, fault-tolerant, and easy to operate and maintain. MRS clusters provide a Big Data management and analytics platform hosted in the cloud. All cluster nodes are deployed on the same tenant VLAN, and mutual trust relationships are established between the active/standby Operations and Maintenance Service (OMS) nodes and other nodes in the cluster.

Users can log in to MRS using its client or a web browser. The MRS supports single sign-on (SSO) based on central authentication service (CAS) so that users can conveniently access the web pages of other Big Data platform components without being prompted for authentication again.

- **User password management**: MRS uses IAM (Kerberos and LDAP) to manage user passwords. Kerberos encrypts user passwords and saves them to the LDAP database.
- **Permissions control**: MRS uses RBAC. Assigning a role to a user grants that user the permissions associated with the role. The permissions of each role can be configured based on the component resources that the role is required to access.
- **Data encryption**: The HBase function of MRS supports column family-based storage encryption. When creating a table, users can choose which data to store under encryption.
- **Data integrity**: MRS user data is stored in Hadoop Distributed File System (HDFS), which uses CRC32C to verify data integrity. Note that the default setting of CRC32C can be changed to the slower CRC32 if desired. Verification data is stored on the HDFS DataNode (DN). If the DN detects that data transmitted from a client is abnormal (i.e. incomplete), the DN reports an exception to the client and asks it to write the data again. Data integrity is also verified by the client when reading data from the DN. If the client detects that the data is incomplete, it attempts to read the data from another DN.
- **Data backup**: MRS Hbase cluster supports asynchronous real-time data backup from the active cluster to the standby cluster. It provides a basic O&M tool for external systems that can set active and standby nodes, rebuild and verify data, and check the progress of data synchronization.

6.6 Application Services

6.6.1 SMN

Simple Message Notification (SMN) is a hosted notification service for messages that is simple, flexible, and massive in scale. With SMN, users can efficiently and economically push messages to email addresses, mobile phone numbers, HTTPS

applications, and mobile clients one by one or in groups. The service can also be readily integrated with and receive event notifications from other cloud services, such as CES, OBS, and AS.

SMN can be used through its API or the management console. The service features a wide range of security measures to protect the management system from attack. It employs a tenant-based permissions model, strict parameter verification, secure communications protocols, and measures for protecting sensitive information and auditing logs.

SMN offers exceptionally flexible access authorization: Huawei Cloud accounts, users created by IAM, and other cloud services are all able to access the service. There are different levels of permissions. Huawei Cloud accounts as well as accounts created by IAM and assigned SMN administrator permissions can perform all SMN operations. Users created by IAM but assigned tenant permissions can only perform query operations.

The SMN API can be accessed only through HTTPS, with TLS 1.2 and PFS enabled by default. The parameters of all tenant API calls are strictly verified to ensure that they are not malicious, and all API calls are recorded and audited for accurate backtracking. Mobile phone numbers, email addresses, and other sensitive tenant data is stored under encryption using reliable algorithms.

6.6.2 DMS

Distributed Message Service (DMS) is a messaging middleware service built on highly available distributed clustering technology that provides reliable and scalable hosted queueing for sending, receiving, and storing messages.

DMS can be used in a wide range of scenarios including asynchronous communication for service decoupling, enterprise solutions, financial transactions, e-commerce, logistics, marketing, the Internet of Things (IoT), and the Internet of Vehicles (IoV), and so on. Some key usage scenarios are described as follows:

- **Service decoupling**: Non-essential or unimportant service components that rely on other systems can send notifications asynchronously instead of waiting for those systems to finish processing. Information about orders placed during a sales event at an online marketplace, for example, can be queued and later obtained from the queue during packaging and delivery.
- **Eventual consistency**: The status of the different subsystems or modules on transaction or payment systems must be consistent in the end, and data transmitted between subsystems or modules cannot be lost. DMS can guarantee the reliable transmission of data between subsystems or modules to ensure that their transactions are eventually consistent while reducing the difficulty and cost of operations.
- **Off-peak traffic control**: On e-commerce systems or large-scale websites, traffic bursts that are handled by powerful upstream systems may have a major impact on less powerful downstream systems. Burst traffic during shopping holidays, for example, can be cached using DMS so that downstream systems can process it according to their ability and are not overloaded. DMS can cache hundreds of millions of messages for up to three days so that they can be processed during off-peak hours.
- **Log synchronization**: Applications can synchronize log information with the information server in an asynchronous manner and then analyze those logs

offline or in real time using other system components. Applications can also be monitored by collecting key log information.

Authentication and authorization for DMS access are controlled by IAM. After authentication, users can perform all operations on their own queue resources. By default, users can only access queues that they have created, but policy controls can also be configured to allow other services or IAM users to perform operations on specified queues.

The DMS API can be accessed only through HTTPS, with TLS 1.2 and PFS enabled by default. For security purposes, users can enable SSE, setting DMS to encrypt all user-provided data before storage. SSE can use a common key provided by DMS or a key created with KMS. Users can also choose to encrypt messages before sending them to DMS if required in order to prevent unauthorized access to sensitive data.

6.6.3 Workspace

Workspace provides virtual application services and Windows clients using Virtual Desktop Infrastructure (VDI). It enables users to access their cloud desktop over thin client hardware from anywhere at any time. Workspace provides a higher level of security than traditional PCs by isolating users' interfaces and data and thereby prevents data leakage by centrally storing and processing that data.

No data is stored on the thin clients used with Workspace; they are used for running the Workspace client program only. Desktop user interface is regenerated as graphics on the client side but the actual business data is not transmitted. Information transmitted to and from Workspace is sent over the highly secure Huawei Desktop Protocol (HDP), and input from local peripherals (USB devices, multimedia devices, flash storage, keyboards, and mouse devices) is recalibrated for security.

Users can log in to their Workspace accounts at any time from thin clients in a tenant space or over Direct Connect. With these capabilities, Workspace offers greater efficiency and flexibility than the laptop computers and external storage devices of the past.

Workspace greatly improves maintenance efficiency by centrally managing password policies, session timeout, desktop delivery, peripheral devices, patches, and upgrades.

With virtualized management of all hardware, virtualized resources can be allocated to users as needed. This lengthens the service life of user desktops and reduces costs associated with replacing and upgrading hardware.

Workspace offers the following security functions:

- **User identification:**
  - Administrators and end users are assigned unique identifiers, which are linked to all auditable events.
  - All users must be authenticated using a password that meets predefined complexity requirements (such as password length or types of characters included).
  - A default timeout value is provided. If a user does not perform any action within a specified time, Workspace will automatically terminate the session or require reauthentication of the user.

 Copyright © Huawei Technologies Co., Ltd.

  - Any user who unsuccessfully attempts to log in too many times within a specified interval will be locked out. This ensures user security and has the added benefit of limiting the number of authentication requests sent.
- **Access control**: The subjects (such as users and services) and objects involved in resource access along with any operations between subject and object are all within the scope of access control. Authorized users' permissions to access content and perform operations on protected resources are not allowed to exceed the preset scope. For added security, data related to user authentication is stored under encryption.
- **Transport security**: Desktop access is performed over HDP to ensure the security and integrity of data transmissions. The number of sessions to a single desktop can be limited, and TLS 1.2 can be used to establish encrypted communication channels.
- **Image security**: The integrity and confidentiality of VM image files are protected, and residual data from VM images and snapshots is completely erased.
- **Backup and restoration**: A backup management mechanism for VDI ensures that backed-up data can be restored.
- **Security monitoring**: Workspace can monitor in real time the online status and usage status of users, the operating status of VMs, and the online status of terminals.
- **Security auditing**: All user activities, operations, and commands that affect the system can be logged to support subsequent auditing. Log data includes the following: login type, operation type, log level, event time, event subject, IP address, event description, and event outcome. To ensure that audit logs are not lost, they are stored on non-volatile storage media and can be migrated if storage space becomes insufficient. Only authorized users can access and review system logs; logs cannot be accessed, modified, or damaged by unauthorized users.

6.7 Management Services

6.7.1 CES

Cloud Eye Service (CES) is a comprehensive monitoring platform for Elastic Cloud Servers, bandwidth, and other resources. CES monitors alarms, notifications, and custom reports and diagrams in real time, giving the user a precise understanding of the status of service resources. It must be emphasized that CES does not come into contact with tenant data. It monitors only the data related to the utilization of infrastructure resources.

The purpose of CES is to monitor indicators from other cloud services, which currently include but are not limited to ECS, EVS, VPC, RDS, DCS, DMS, ELB, AS, WAF, HVD, Workspace, MLS, WTP, DWS, and AIS[1]. Alarm rules and notification policies can be set based on these indicators to help the user understand the usage and performance status of the instance resources used by each and every service.

CES servers are deployed in a distributed manner to ensure high availability. Resource usage monitoring is timely and effective, indicators are sampled in real

 Copyright © Huawei Technologies Co., Ltd.

time, and alarms and notifications are triggered accurately based on pre-configured rules and policies.

CES can be used through the management console, API, command line, or SDK. The CES data belonging to different tenants is isolated. Tenants must be authenticated through IAM before they can use CES and access the corresponding monitoring data.

Note:

1. The following Huawei Cloud services are not covered in the White Paper: HVD – Host Vulnerability Detection service, MLS – Machine Learning Service, WTP – Web Tampering Protection service, DWS – Data Warehousing Service, and AIS – Artificial Intelligence Service. For further details, go to **https://www.huaweicloud.com/en-us/**.

6.7.2 CTS

Cloud Trace Service (CTS) records operations on cloud service resources so that they can be queried, audited, and traced. It records operations performed on the management console, executed through an API, and internally triggered on the Huawei Cloud system. CTS is an essential support system for tenant-specific industry certification and IT compliance certification. It provides the following functions:

- **Resource change auditability**: Changes to Huawei Cloud resource and system configurations performed by all users are recorded systematically and in real time. This is superior to the traditional method in enterprise IT environments of manually auditing each change.
- **Access security monitoring and auditability**: All management console operations and API calls are recorded systematically and in real time to help query, analyze, and locate issues closer to real time or after fact.
- **Data auditability**: Users can verify whether data has been disclosed by collecting activity data about OBS objects and object-level API events recorded by CTS for audit purposes.
- **Low cost**: CTS can merge records into event files on a regular basis and move these to an OBS bucket for storage, making logs highly available over a long period of time and at a low cost.

The security design for CTS is based on the Huawei Cloud security framework. The security of the cloud computing services provided to tenants is ensured through secure network architecture and through the implementation of network perimeter, application, and data protection. Application and data security are described as follows. See chapter 5 for details on secure network architecture and network perimeter protection.

- **Application security**: Valid requests for compliance event queries and tracker operations sent by legitimate users and also valid compliance events from interconnected services are accepted and processed by CTS. All requests must be transmitted over HTTPS. Sensitive data is encrypted, and a number of measures are taken to ensure security when interacting with external services: interface control, whitelist control, requestor authentication, and multiple rounds of verification. Furthermore, the web security of CTS control nodes has been hardened to defend against a wide range of attacks.

 Copyright © Huawei Technologies Co., Ltd.

- **Data security**: The security requirements for user log data processed by CTS differ as the data is generated, transmitted, and stored. When generated, log data must be desensitized within each service and verified to contain no sensitive data. When transmitted, the accuracy and completeness of log data transmission and storage must be ensured through identity authentication, format validation, whitelist inspection, and unidirectional reception. When stored, log data must have multiple backup copies stored in a distributed manner, and databases must be hardened in accordance with Huawei security requirements to prevent data security threats such as spoofing, repudiation, tampering, and leakage. For additional security, CTS can be configured for encryption of log data when saved in an OBS bucket.

6.7.3 EPS

Enterprise Project Service (EPS) is a cloud resource management service provided for enterprise customers. It matches the hierarchical organization and project structure. EPS mainly includes enterprise project management, financial management, and personnel management. EPS provides unified cloud resource management by enterprise project, and resource management and member management in enterprise projects. Financial management allows multiple Huawei Cloud accounts to become the primary accounts and sub-accounts of an enterprise. Users can create organizations and sub-accounts, or associate sub-accounts based on the enterprise structure and make the sub-accounts subject to the created organizations. Users of enterprise projects belong to user groups. Personnel management manages these users and user groups, including setting credentials for users, and creating, modifying, and deleting users and user groups.

Currently, EPS can manage the following services: Elastic Cloud Servers, auto scaling, IMS, EVS, VPC, Elastic IP (EIP), CDN, RDS, DCS, DDS, Cloud Container Engine (CCE), Advanced Anti-DDoS (AAD), bare metal servers, DeH, and Cloud Service Engine (CSE).

Tenants can use EPS through the service console or EPS API. EPS features a wide range of security measures to protect the management system from attack. It uses a tenant-based permissions model and secure communications protocols, strictly verifies parameters, and provides measures for protecting sensitive information and auditing logs. EPS offers flexible access: Huawei Cloud accounts, accounts created by IAM and granted the EPS access, and other cloud services authorized by tenants are all able to access EPS. There are different levels of permissions. Huawei Cloud accounts as well as accounts created by IAM and assigned EPS administrator permissions can perform all EPS operations. Accounts created by IAM but assigned tenant permissions can perform only query operations.

The EPS API can be accessed only through HTTPS, and EPS supports TLS 1.2 and PFS by default. The parameters of all tenant API calls are strictly verified to prevent attacks. In addition, all interface calls are logged for audit and accurate backtracking.

6.7.4 TMS

Tag Management Service (TMS) is a visualized service that can quickly and conveniently manage tags in a centralized manner. It provides the following functions:

- Resource tag management: Tags can be added to resources under an account to mark and classify the resources. TMS allows users to operate resource tags in a visualized table and edit tags in batches.
- Resource tag search: Users can search for resources by tag across services and regions or by a combination of tags
- Predefined tag management: Users can create, import, and export predefined tags. By predefining tags, users can plan tags from the service perspective for efficient tag management.

TMS does not store user privacy data. It calls interfaces of other services through internal authentication and transparent transmission, and IAM performs authentication. Tenants can use TMS through the service console or TMS API. TMS features a wide range of security measures to protect the management system from attack. It uses a tenant-based permissions model and secure communications protocols, strictly verifies parameters, and provides measures for protecting sensitive information and auditing logs. TMS offers flexible access: Huawei Cloud accounts, accounts created by IAM and granted the TMS access, and other cloud services authorized by tenants are all able to access TMS.

The TMS API can be accessed only through HTTPS, and TMS supports TLS 1.2 and PFS by default. The parameters of all tenant API calls are strictly verified to prevent attacks. In addition, all interface calls are logged for audit and accurate backtracking.

6.7.5 RTS

Resource Template Service (RTS) helps users simplify cloud computing resource management and automatic O&M. Users develop template files based on the template specifications defined by RTS and define cloud computing resource sets, resource dependencies, and resource configurations in the templates. RTS automatically creates and configures all resources in the templates through the orchestration engine. In this way, automated deployment and simplified O&M are achieved. RTS supports most APIs of the native OpenStack Heat component and templates in the Heat Orchestration Template (HOT) format. Users can call APIs or the management console to use RTS. The management console is a visualized user interface of RTS. Users can use the management console to automatically deploy resources.

RTS does not store user privacy data. It calls interfaces of other services through internal authentication and transparent transmission, and IAM performs authentication. Tenants can use RTS through the service console or RTS API. RTS features a wide range of security measures to protect the management system from attack. It uses a tenant-based permissions model and secure communications protocols, strictly verifies parameters, and provides measures for protecting sensitive information and auditing logs. RTS offers flexible access: Huawei Cloud accounts, accounts created by IAM and granted the RTS access, and other cloud services authorized by tenants are all able to access RTS.

The RTS API can be accessed only through HTTPS, and RTS supports TLS 1.2 and PFS by default. The parameters of all tenant API calls are strictly verified to prevent attacks. In addition, all interface calls are logged for audit and accurate backtracking.

6.8 Security Services

6.8.1 IAM

IAM is a user account management service designed for enterprises that allocates resources and operation permissions to enterprise users in a differentiated manner. Once IAM has authenticated and authorized these users, they can use an access key to access Huawei Cloud resources through APIs.

IAM supports hierarchical fine-grained authorization to ensure that the various users who are part of an enterprise tenant use cloud resources as authorized. This authorization scheme prevents users from exceeding the scope of their permissions and ensures the continuity of tenant services.

- **Password-based authentication**: A password is specified when a user account is registered or created. The password is required to log in to the Huawei Cloud console and can also be used to access Huawei Cloud resources using APIs.
  - **Password policy**: IAM allows the security administrator for each tenant to set a policy for user passwords to reduce the likelihood that user accounts can be exploited. Password policies include rules such as password length, complexity and expiration interval.
  - **Login policy**: IAM also allows security administrators to create account lockout policy for user login to prevent user passwords from brute force and phishing attacks.
  - **ACL**: Tenants can configure an IP address-based ACL to ensure that enterprise users can access Huawei Cloud resources only from a secure network environment, greatly mitigating the risk of data leakage that would be rampant otherwise.
- **Multi-factor authentication (MFA)**: MFA is an optional security measure that enhances account security. If MFA is enabled, users who have completed password authentication will receive a one-time SMS authentication code that they must use for secondary authentication. MFA is used by default for changing important or sensitive account information such as passwords or mobile phone numbers.
- **Access key**: API requests must be signed with an access key to manage Huawei Cloud resources using O&M tools or API commands. Signature information is verified by the API gateway. Digital signatures and timestamps prevent requests from being tampered with and protect against replay attacks.

  Enterprise administrators can create and download an access key on the My Credentials page at any time and view the status of the key. However, for security purposes, the access key cannot be recovered or re-downloaded in the event that the access key is lost or forgotten. The administrator must create an access key and then disable or delete the old one. The access key must be stored in a safe location and changed regularly. Under no circumstances should it be hardcoded.
- **Identity Federation**: Secure and reliable external services for identity authentication that support Security Assertion Markup Language (SAML) 2.0,

 Copyright © Huawei Technologies Co., Ltd.

such as LDAP and Kerberos, can be used for user authentication. To enable authentication by an external service, tenants must configure the service as an identity provider (IdP) and Huawei Cloud as the service provider (SP). Enterprise tenants can then log in to the Huawei Cloud console over SAML or use APIs to access cloud resources without synchronizing user information to Huawei Cloud.

Tenants can use federated identity authentication to map external users to temporary Huawei Cloud users and allow those users to access Huawei Cloud resources for a specified time period. An appropriate user group (i.e. set of permissions) must be created for these temporary users to restrict their permissions.

Long-term security credentials should not be hardcoded into mobile or web applications that access Huawei Cloud resources. Instead, such applications should prompt users to first log in, then use already authenticated identity information to obtain temporary credentials through identity federation.

- **Permissions management**: IAM includes user administration permissions and cloud resource permissions. User administration permissions deal with creating, deleting, modifying, and assigning permissions to users and user groups, while cloud resource permissions have to do with creating, deleting, modifying, and configuring cloud resources. Users inherit the cloud resource permissions assigned to their user group. Managing user permissions by user groups therefore makes the process more organized. IAM can also work with PAM to implement fine-grained management of privileged accounts.

6.8.2 DEW

Data Encryption Workshop (DEW) is a comprehensive cloud data encryption service. It provides functions such as dedicated encryption, key management, and key pair management. It uses HSMs to protect the security of keys. DEW can be integrated with other Huawei Cloud services to meet your needs for various encryption scenarios. Users can also use this service to develop their own encryption applications.

With DHSM, users can select the hardware encryptor certified by the OSCCA or FIPS 140-2 Level 3 to implement high-performance and user-exclusive encryption capabilities. DEW supports SM1 to SM4 key encryption algorithms developed in China. The hardware encryptor can be hosted on the cloud and placed in the same VPC as the user application. The encryptor subrack, power supply, bandwidth, and interface resources are exclusively used by the tenant. During application encryption and decryption, the API can achieve computing performance of over 10000 TPS to meet a large number of concurrent requirements. After DEW generates an encryption root key, the Ukey (physical medium) containing the root key is sent to a user. The user imports the key material defined by himself/herself or generates key factors together with other users. The generated root key is stored in the HSM, which is a third-party device certified by the OSCCA. No one, including the encryptor vendor and cloud service provider, can access the root key. The root key is used to encrypt the user's master key, and the master key is used to encrypt the user's data key. Therefore, even the cloud service provider cannot obtain the user's plaintext master key and data key.

KMS enables users to manage their keys conveniently and ensures the security of critical business data by supporting data encryption using a data encryption key (DEK) at any time. The DEK is encrypted using the customer master key (CMK)

that is stored in KMS. The CMK, in turn, is encrypted by the root key, which is stored in the HSM, and saved as ciphertext on the key storage node. The chain of trust in KMS is rooted in the HSM, which is FIPS 140-2 (Level 2 and Level 3) certified to meet users' data security compliance requirements.

The KMS interconnects with cloud storage services such as EVS and OBS so that users can encrypt data stored in Huawei Cloud simply by selecting the required CMK. It provides a convenient way for other cloud services to support full encryption of user data, especially sensitive data. Users can focus on their business and rest assured that the encryption keys for their data in Huawei Cloud are properly managed.

To ensure the security and reliability of tenants' keys, KMS provides the following security features:

- **Random number generation**: All keys in the KMS are generated by the HSM's hardware true random number generator (TRNG) to ensure key randomization.
- **Secure key storage**: Key disclosure is prevented by storing the root key of the KMS in the HSM. The root key at no time appears outside the HSM. In addition, at least two HSM devices are deployed as a pair to ensure reliability and availability. The CMKs are encrypted using the root key and saved as ciphertext on the key storage nodes, which store them in a security-hardened MySQL database. The MySQL database is deployed in a cluster of two nodes, one active and the other standby. When a user key is saved to the active MySQL database, it is also backed up to the standby MySQL database so that the standby database can take over and continue to provide service in the event of a failure on the active node. The HSM is the root of trust in the KMS, and in combination with the other keys forms a complete chain of trust.
- **Postponed key deletion**: KMS is used to manage CMKs throughout their lifecycle, enabling, disabling, and deleting them. KMS also offers postponed key deletion. This function allows tenants to set a time (7 days to 3 years) during which CMK deletions can be canceled, avoiding CMK deletion by mistake.
- **KMS disaster recovery**: KMS provides a full range of backup and disaster recovery functions to ensure that keys are available and not lost. In the event of a disaster, KMS is switched over to a server at a secondary location to ensure service continuity. The root key stored in the HSM is backed up through its dedicated backup tool. The key storage node that stores CMKs backs up keys (incremental and full) on a regular basis to the specified storage device. If an error causes user keys to be lost, the KMS can recover the keys using the backup data.
- **Trusted links**: To ensure the security of KMS data, KMS hosts use a standard encrypted transmission mode to establish secure communication with the KMS service node.
- **Access control**: KMS performs centralized RBAC based on IAM roles. Operations on the CMKs stored in KMS can be performed only by users who have been authenticated by IAM and KMS and have the appropriate permissions. Users with read-only permissions can query information about CMKs but cannot perform other operations. In addition, KMS isolates the CMKs of different tenants so that tenants can access and manage their own CMKs only. Although system administrators have permissions to manage devices, they cannot access CMKs.

 Copyright © Huawei Technologies Co., Ltd.

- **Operations** log auditing: Logs are generated for all major operations (such as creating a CMK or encrypting a DEK) and recorded to CTS so that CMK operations can be audited.

KMS also leverages other Huawei Cloud technologies to enhance its security capabilities: namely, the secure infrastructure and platform, secure network architecture, perimeter protection, zone division, virtual network isolation, tenant KMS instance isolation, and API security.

6.8.3 Anti-DDoS

The Anti-DDoS service uses specialized anti-DDoS devices to implement precise and efficient defense against a range of traffic attacks and application-layer attacks. Its quick response to attacks ensures portal and website security for enterprises of all sizes and maximizes return on investment. Anti-DDoS provides fine-grained DDoS mitigation capabilities to deal with the likes of Challenge Collapsar (CC) attacks and ping, SYN, UDP, HTTP, and DNS floods. Once a protection threshold is configured (based on the leased bandwidth and the business model), Anti-DDoS will notify the affected tenant and activate protection in the event of a DDoS attack.

Anti-DDoS provides the following functions:

- **Self-service protection policy**: Users can select the defense template that best meets the needs of their bandwidth and business model.
- **Traffic inspection and scrubbing**: Anti-DDoS checks traffic in real time and performs scrubbing on attack traffic when it reaches pre-defined threshold(s).
- **Ease of administration**: Users can view traffic trends and reports in real time on a management platform that is flexible and easy to use. The platform makes it simple to configure the service, set up stringent controls, and monitor service resources.
- **Report monitoring**: Users can query DDoS protection-related information about specific public IP addresses. This information includes current protection status, protection parameters, and the last 24 hours of information about traffic, scrubbing operations, and black holes. Security reports are available for review, displaying DDoS protection information generated by week. Users can query the past four weeks of DDoS protection information, including but not limited to scrubbed traffic, number of intercepted DDoS attacks, and top 10 frequently attacked Elastic Cloud Servers.
- **Log analysis**: Anti-DDoS receives and analyzes logs reported by DDoS mitigation devices and displays the results on the management console.

Anti-DDoS also leverages other Huawei Cloud technologies to enhance its security capabilities: namely, the secure infrastructure and platform, secure network architecture, perimeter protection, virtual network isolation, API security, and log auditing.

6.8.4 HSS

Host Security Service (HSS) is a security manager for servers. It provides asset management, vulnerability management, baseline check, and intrusion detection functions to help enterprises better manage host security risks, detect and prevent hacker intrusion in real time, and meet graded security protection compliance requirements.

 Copyright © Huawei Technologies Co., Ltd.

Huawei Cloud HSS provides the following functions:

- **Asset management:** manages and analyzes security asset information, such as accounts, ports, processes, web directories, and software.
- **Vulnerability management:** detects vulnerabilities in the Windows and Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provides fixing suggestions.
- **Baseline check:** checks system password complexity policies, typical weak passwords, risky accounts, and common system and middleware configurations to identify insecure items and prevent security risks.
- **Account cracking prevention:** detects password cracking attacks on accounts such as SSH, RDP, FTP, SQL Server, and MySQL, blocks the identified attack source IP addresses for 24 hours, and forbids them to log in again to prevent hosts from being intruded due to account cracking.
- **Two-factor authentication:** HSS authenticates login attempts to Elastic Cloud Servers twice by SMS messages and emails. This significantly improves account security.
- **Key file tampering detection**: HSS monitors key files (such as **ls**, **ps**, **login**, and **top** files) and prompts users about possibility of tampering once the files are modified.
- **Detection of malicious programs**: By detecting program features and behaviors and using the AI image fingerprint algorithm and cloud-based virus scanning and removal, the system can effectively identify malicious programs, such as viruses, Trojan horses, backdoors, worms, and mining software, and provide one-click isolation and virus removal capabilities.
- **Website backdoor detection**: HSS checks files in web directories to help identify webshells (such as php and jsp) in Elastic Cloud Servers.
- **Web page anti-tamper**: HSS protects web pages, electronic documents, images, and other files of websites from tampering or sabotage by hackers.

Huawei Cloud HSS has the following advantages:

- **Effective host risk prevention**: The asset management, vulnerability management, and baseline check functions can detect and prevent host vulnerabilities, weak passwords, and insecure configurations, reducing the attack surface by 90%.
- **Strong account cracking defense capability**: Two-factor authentication upon host login and advanced protection algorithms can effectively prevent brute-force cracking attacks.
- **High detection rate of malicious programs**: The behavior analysis and AI-based image fingerprint algorithm can effectively detect and remove unknown and variant malicious programs, providing an industry-leading detection rate.
- **Effective web page anti-tamper**: The web page anti-tamper function provides three protection capabilities: web file directory locking, automatic restoration upon tampering detection, and web page restoration based on remote backup. This prevents web page tampering and has become a mandatory security service for government, education, and large enterprise websites.
- **Mandatory services for graded security protection assessment**: The intrusion detection function meets host intrusion prevention and malicious

code prevention requirements. The vulnerability management function meets host vulnerability scanning requirements. The web page anti-tamper function meets data integrity requirements.

6.8.5 CGS

Container Guard Service (CGS) can scan vulnerabilities and configuration information in images, helping enterprises resolve container environment problems that cannot be detected by traditional security software. In addition, CGS provides the container process whitelist, read-only file protection, and container escape detection functions to prevent security risks during container running.

Huawei Cloud CGS mainly provides the following functions:

- **Image vulnerability management**: CGS can scan private, official, and all running images in Huawei Cloud to detect vulnerabilities in the images and provide fixing suggestions, helping users obtain secure images.
- **Container security policy management**: CGS supports the configuration of security policies to help enterprises define the container process whitelist and file protection list, improving system and application security during container running.
- **Container process whitelist**: Defining such a whitelist can effectively prevent security risks such as abnormal processes, privilege escalation attacks, and non-compliant operations.
- **File protection**: Read-only protection must be configured for key application directories (such as **bin**, **lib**, and **usr** system directories) in containers to prevent tampering and hacker attacks. This function can restrict the access (set to read-only) to these directories to prevent security risks such as file tampering.
- **Container escape detection**: This function scans all running containers, detects exceptions (including escape vulnerability attacks and escape file access) in the containers, and provides solutions.

6.8.6 Cloud WAF

Cloud Web Application Firewall (WAF) is an advanced web application firewall service featuring a series of targeted optimization algorithms that give full play to Huawei's extensive experience in network attacks and defense mechanisms. Cloud WAF runs on the dual-engine architecture of regular expression rule and semantic analysis to ensure high-performance protection against SQL injections, cross-site scripting (XSS) attacks, command and code injections, directory traversals, scanners, malicious bots, web shells, and CC attacks.

Cloud WAF provides a user-friendly and centralized management interface on which users can configure protection settings based on their service and business requirements, view WAF logs, and resolve false positive events.

Cloud WAF provides the following functions:

- **Web attack filtering**: Cloud WAF can detect 99% of web attacks (including all OWASP Top 10 attacks) and can detect malicious payloads in parameters, headers, and web addresses.

 Copyright © Huawei Technologies Co., Ltd.

- **Powerful decoding**: Cloud WAF can restore url_encode, Unicode, XML, C-OCT, hexadecimal, HTML escape, and base64 code, case confusion, as well as JavaScript, shell, and PHP concatenation confusion.
- **Protection against CC attacks**: CC attacks, a type of application-layer DDoS attack, occupy a large number of service resources and affect service experience. Cloud WAF can identify users based on IP address, cookie, and Referer information and limit their access rates based on a flexibly configured threshold to prevent services from being overloaded. Cloud WAF can also employ a verification code-based challenge/response mechanism to verify that the requester is a real user rather than a bot. This mechanism can more accurately identify attackers and stop their attacks.
- **Web shell defense**: Cloud WAF checks the content in HTTP or HTTPS transmission channels to detect and block various web shell attacks. This function can be enabled with a single click to protect tenant services.

Cloud WAF is easy to use and manage, and features the following:

- **Precise customized control**: The Cloud WAF API can be used to create custom detection rules, including IP address blacklists and whitelists, user agent blacklists, and other more complex and precise rules.
- **Privacy filtering**: Private user information such as user names and passwords can be filtered out of WAF event logs. Privacy filtering rules can be flexibly customized.
- **Centralized management**: WAF nodes are managed and operations such as policy deployment and event log processing are performed in a centralized manner on the backend.

6.8.7 DBSS

Database Security Service (DBSS) includes two functional modules: database security audit and database security protection. It provides three functions: database audit, data leakage prevention, and database firewall, ensuring database and asset security on the cloud.

(1) Database security audit

This function in bypass mode can generate alarms for risky behaviors in real time and block attacks. In addition, this function can generate compliance reports that meet data security standards to locate and punish internal database violations and inappropriate operations, effectively detecting and blocking external intrusions and ensuring data asset security. Detailed functions are as follows:

- **User behavior discovery and audit**: Access operations at the application layer and database layer can be associated to help customers trace the identities and behaviors of users.
- **Multi-dimensional lead analysis**: (a) Risk leads: This function can analyze SQL behaviors such as SQL injection, blacklist statements, and authorization violation at high, medium, and low risk levels. (b) Session leads: This function supports analysis from multiple dimensions, including time, user, IP address, and client. (c) Detailed statement leads: This function supports search by user, client IP address, access time, operation object, and operation type.
- **Abnormal operations, SQL injection, and real-time blacklist and whitelist alarms**: (a) Risks of abnormal operations: This function supports the

 Copyright © Huawei Technologies Co., Ltd.

definition of risky access behaviors to be monitored based on client IP addresses, database IP addresses, database users, and risk levels. (b) SQL injection: This function provides a systematic SQL injection database and SQL injection description based on regular expressions or syntax abstraction, and generates alarms when detecting database exceptions. (c) Blacklist and whitelist: SQL statements for accessing the system are described accurately and abstractly, and alarms are generated in real time when the SQL statements appear.

- **Refined reports for various abnormal behaviors**: (a) Session behavior: login failure and session analysis reports. (b) SQL behavior: new SQL, SQL statement execution history, and SQL failure reports. (c) Risky behaviors: alarm, notification, SQL injection, and batch data access behavior reports. (4) Compliance reports: compliance reports that meet data security standards (such as Sarbanes-Oxley).

Huawei Cloud database security audit has the following advantages:

- **Easy deployment**: database deployment in bypass mode, which is easy to use.
- **Full audit**: audit on RDS and ECS/BMS databases on Huawei Cloud.
- **Quick identification**: associated audit of more than 99% of applications, complete SQL parsing, and accurate protocol analysis.
- **Efficient analysis**: tens of thousands of data records imported to the database per second, mass data stored, and retrieval response in hundreds of millions of data records within seconds.
- **Compliance with multiple standards**: meeting the database audit requirements of graded protection Level-3 and complying with China's Cybersecurity Law and Sarbanes-Oxley Act (SOX[1]).
- **Separation of rights**: separated rights of system, security, and audit administrators to meet audit security requirements.

(2) Database security protection

Database security protection provides the following functions:

- **Database firewall**: Users can configure firewall policies, automatic learning policies, and IDS/IPS policies based on anomaly detection. When a request violating a specified policy reaches the database firewall, DBSS either generates an alarm or denies the request, depending on configuration. DBSS can also establish user access behavior baselines through machine learning, generate query pattern groups, and apply the query pattern groups to database firewall policies.
- **Separation of rights and responsibilities**: With fine-grained account management and rights control, rights can be controlled by role type, table, view object, and column.
- **SQL injection detection and defense**: An SQL injection signature database and a context-based learning model and rating mechanism are built into DBSS to comprehensively identify and block SQL injections in real time.
- **Sensitive data discovery**: DBSS has built-in knowledge bases for PCI, HIPAA[2], SOX, and GDPR compliance. Users can also customize a knowledge base for sensitive data rules and configure sensitive data discovery policies to discover

 Copyright © Huawei Technologies Co., Ltd.

sensitive data in databases. Once sensitive data is identified, anonymization and audit rules can be generated through one click.

- **Dynamic data anonymization**: Users can set anonymization rules for specified database tables or columns and queries from specific source IP addresses, users, and applications. A precise anonymization engine is used to anonymize sensitive data in real time without affecting application performance or changing data stored in the database.
- **Database data reduction**: Users can set data reduction rules to detect data operation on specific database tables from unauthorized users, IP addresses, or applications. When the amount of operated data exceeds the specified threshold, DBSS alerts administrators and records this event in a data reduction log to protect user data from leakage.
- **Database activity monitoring**: DBSS provides visualized monitoring on the database, table, and column levels. It independently monitors and analyzes database activities and provides alarms about unauthorized activities. DBSS provides database auditing trails to help trace attackers. Tracing can be performed based on the following: source IP address, user identity, application, access time, database requested for access, original SQL statement, operation, operation result, time taken, and content returned. Audit records are remotely stored to ensure compliance.

Note:

1. As a federal law passed by the United States Congress in 2002, SOX sets more regulatory requirements for all US-listed companies' boards, management, and public accounting firms.
2. HIPAA (Health Insurance Portability and Accountability Act of 1996), a federal law passed by the United States Congress in 1996, establishes a portability and accountability system for health insurance in the US, providing data privacy and security regulations for the protection of medical information.

 Copyright © Huawei Technologies Co., Ltd.

7 Engineering Security

In the traditional ICT field, Huawei continues to deliver secure and high-quality products and services to our customers. Huawei has accumulated expansive capabilities, a wide variety of tools, and a wealth of experience in product security development during the process. After Huawei entered the cloud service market, this knowledge and experience also helped Huawei Cloud to establish and mature its multi-faceted full-stack security protection framework and high-availability, high-reliability cloud services. At the same time, the continuous integration, delivery, and deployment practices, which are characteristic of online and cloud services development and operations, require entirely new mindset, methodologies, and processes, as well as an all-new tool chain. By leveraging Huawei's wealth of experience and far-reaching capabilities in the field of security, Huawei Cloud has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result, DevOps is gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. In addition to introducing the DevOps and DevSecOps processes, this chapter focuses on specific practices in the Huawei Cloud security process, including security design, secure coding and testing, third-party software management, configuration and change management, and pre-release security approval.

7.1 DevOps and DevSecOps Processes

As the business model of Huawei Cloud services has changed, Huawei Cloud has established a new organizational and management structure and adopted DevOps practices, which are more suitable for cloud service development, deployment, and operation than traditional ICT products and services. DevOps has the following differences from traditional ICT R&D processes:

- **Business decision-making**: Periodic reviews based on business cases replace decisions based on gate (DCP/TR).
- **Product development and delivery mode**: Online services become the delivery objectives. The positioning of DevOps in the Huawei Cloud management framework is a new R&D and O&M hybrid mode that enables cloud services to go online quickly.

 Copyright © Huawei Technologies Co., Ltd.

- **Marketing mode**: An Internet marketing mode is introduced.
- **Industry chain and ecosystem**: A new business model featuring alliance, collaboration, partnership management, and value distribution mechanisms.
- **Supply chain**: Services are provided for customers, but assets still belong to Huawei.
- **Finance**: The system is required to adapt to the Internet-based transaction mode.

Operation-driven development, incremental improvements, rapid-fire sprints, and frequent deployments are key features of DevOps. Therefore, in the DevOps mode, security activities must also be incorporated into the new process. Huawei Cloud has adopted the new and rapidly iterative DevOps process, which supports continuous integration, delivery, and deployment. In addition, Huawei Cloud has incorporated the R&D and O&M security requirements of high reliability and stability into the DevOps process to form the DevSecOps process, which suits the needs and characteristics of Huawei Cloud.

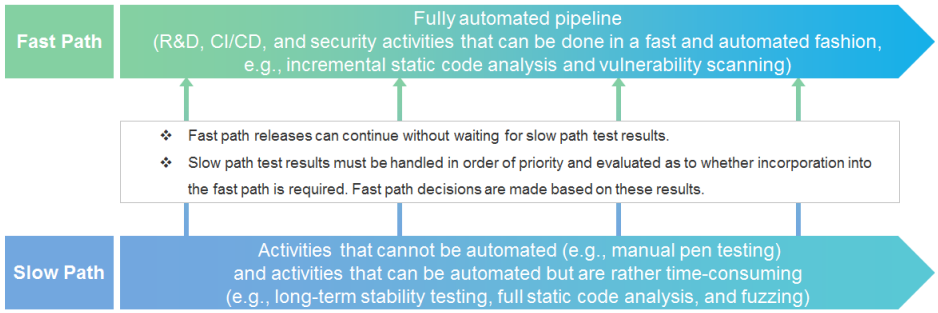
DevSecOps focuses on the following key objectives:

- **Security quality**: Ensuring that cloud services reach the quality standards of security activities in the DevOps mode.
- **Progress**: Ensuring that cloud service security activities do not affect the rapid and continuous integration, delivery, and deployment of DevOps.

7.1.1 Dual Path Mechanism

Cloud services require rapid and continuous integration, delivery, and deployment, but some security activities required in R&D and O&M are time-consuming. To resolve this challenge, Huawei Cloud adopts the Dual Path mechanism to balance progress and quality. In essence, the Dual Path mechanism separates fast activities from slow activities, preventing slow activities from delaying the rapid and continuous integration, delivery and deployment of cloud services.

Figure 7-1 Huawei Cloud DevOps/DevSecOps Dual Path mechanism process



The Dual Path mechanism provides a different path for each of its activity classifications:

- **Fast path**: A fully automated pipeline for a variety of security activities that can be performed quickly and automatically, such as incremental static code analysis, dynamic run-time scanning, and attack surface analysis.
- **Slow path**: A semi-automatic or manual pipeline for security activities that cannot be completely automated, such as manual penetration testing, and

 Copyright © Huawei Technologies Co., Ltd.

automatic security activities that require a significant amount of time to be completed, such as static code analysis, long-term stability test, penetration test, business continuity test, fuzzing, dynamic program analysis, threat and vulnerability analysis, and capacity test.

The Dual Path mechanism's two paths work together in the following ways:

- The Fast Path is the primary path used by the DevOps/DevSecOps process. Once completely automated security activities reach security quality thresholds, development and O&M activities can be executed and completed without further delay. Activities on the Fast Path do not need to wait for the results of security activities on the Slow Path. Security activities that eliminate the most serious risks to cloud services are prioritized and executed on the Fast Path.
- Results of security activities on the Slow Path function as the basis for follow-up decision-making, which the Fast Path must follow as well. For example, when a critical security concern is identified on the Slow Path, the Fast Path may be suspended and only able to restart after the critical concern is resolved.

7.2 Security Design

Huawei has always believed that security fundamentally stems from excellence in design. This idea is in perfect harmony with the concepts behind the DevOps and DevSecOps processes, and is something that Huawei Cloud steadfastly adheres to. Huawei Cloud and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, Huawei Cloud runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. The threat analysis library, threat mitigation library, and security design solution library used to guide Huawei Cloud threat analysis draws from security accumulation and industry best practices in traditional products and new cloud domain products. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure the ultimate security of products and services.

7.3 Secure Coding and Security Testing

Huawei Cloud strictly complies with the secure coding specifications released by Huawei. Before they are onboarded, Huawei Cloud service development and test personnel are all required to learn corresponding specifications and prove they have learned these by passing examinations on them. In addition, we introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code-related issues that can extend rollout time coding.

 Copyright © Huawei Technologies Co., Ltd.

All cloud services pass multiple security tests before release, including but not limited to micro service-level functions and interface security tests such as authentication, authorization, and session security in the alpha phase; API and protocol fuzzing type of testing incorporated in the beta phase; and database security validation testing in the gamma phase. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. In addition, Huawei Cloud leverages its in-depth understanding of customers' security requirements and industry standards and develops matching security test tools. One such tool is SecureCAT, which can be used to check security configurations of mainstream OS and database systems. Once integrated, such security capabilities, controls and tools can be used and reused many times. But there is also another, more obvious advantage: these integrated security capabilities, controls and tools render cloud services that are deployed into production after passing security testing automatically in compliance with the security requirements of different regions and customers.

7.4 Third-Party Software Security Management

Huawei Cloud ensures the secure introduction and use of open source and third-party software based on the principle of strict entry and wide use. Huawei Cloud has formulated clear security requirements and complete process control solutions for introduced open source and third-party software, and strictly controls the selection analysis, security test, code security, risk scanning, legal review, software application, and software exit. For example, cybersecurity assessment requirements are added to open source software selection in the selection analysis phase to strictly control the selection. During the use of third-party software, carry out related activities by taking the third-party software as part of services or solutions, and focus on the assessment of the integration of open source, third-party, and Huawei-developed software, or whether new security issues are introduced when independent third-party software is used in solutions.

Huawei Cloud extends cybersecurity capabilities to open source communities. Once an open source vulnerability occurs, Huawei Cloud can discover and fix the vulnerability in a timely manner with the help of its influence on the open source community. During response to vulnerabilities, test open source and third-party software as part of services and solutions to verify whether known vulnerabilities of open source software and third-party software have been fixed. The list of fixed vulnerabilities of open source and third-party software must be included in the *Release Notes* of services.

7.5 Configuration and Change Management

Configuration and change management plays a key role in assuring Huawei Cloud security. In Huawei Cloud, configuration managers are assigned to manage the configuration of all services, including extracting configuration models (configuration item types, attributes, and relationships) and recording configurations. Additionally, an industry-grade Configuration Management Database (CMDB) tool is utilized to manage configuration items and their relationships with configuration item attributes.

Changes to environments include but are not limited to data center equipment, networks, system hardware and software, and applications, whether those are

 Copyright © Huawei Technologies Co., Ltd.

changes in the equipment used, architectural changes, system software updates (including network device software, OS image, and application container software), or changes in configuration. All changes must be performed in an organized and priority-driven fashion. After all change requests are generated, they are submitted to the Huawei Cloud Change Committee by the change manager team with change classification assigned. After the committee has reviewed and approved the requests, the planned changes can be implemented on the production network. Before submitting a change request, the change must undergo a testing process that includes production-like environment testing, pilot release, and/or blue/green deployment. This ensures that the change committee clearly understands the change activities involved, duration, failure rollback procedure, and all potential impacts.

7.6 Pre-Release Security Approval

To ensure that Huawei Cloud infrastructure and cloud services comply with the laws and regulations and customer security requirements in every region in which they operate, Huawei Global Security & Privacy Officer (GSPO) and Chief Legal Officer (CLO) both participate in the release of cloud services. Before releasing new cloud platform versions and key cloud services, the GSPO, CLO, and development teams work together to analyze and determine whether the versions and services to be released meet the security and privacy requirements of the service regions.

In addition, a much simplified security approval process for Huawei Cloud release ensures the rapid release of medium- and low-risk cloud services. The GSPO and CLO have defined and released a security and privacy compliance checklist that contains all compliance requirements in main regions and industries. Huawei Cloud service teams must conduct self-checking during development, deployment, and release. Medium- and low-risk cloud services can be directly released after the self-check. The self-check results are simultaneously submitted to the GSPO and CLO for auditing purposes. For high-risk cloud services, Huawei invests more resources to conduct more stringent verification and review within a short time window in order to ensure timely and secure release while protecting tenants' business.

 Copyright © Huawei Technologies Co., Ltd.

8 Operational Security

In the previous chapter, DevOps/DevSecOps is described as a cloud service process with R&D and O&M deemed equally important and treated as an inseverable continuum. Huawei Cloud O&M operations are particularly valued. A strong focus is placed on O&M operational security, which has been made a top priority and received increased resource investment as a result. This chapter describes Huawei Cloud's specific practices for security administration, vulnerability management, and security log and event management, as well as business continuity and disaster recovery management.

8.1 O&M Account Security Administration

O&M is critical to Huawei Cloud, and security is involved in every aspect of O&M. Huawei Cloud comes with its own designs, standards, and processes for O&M security, Security administration, an essential aspect of O&M security, primarily includes centralized management of accounts, permissions and, access.

8.1.1 Account Authentication

Huawei employee accounts and two-factor authentication, such as USB token or smart card, are required for O&M personnel to access the Huawei Cloud management network from which systems are centrally managed. Employee accounts are used to connect securely to jump servers over remote access VPN. Both VPN gateways and bastion servers support detailed auditing of user login and access operations.

The privileged account management system binds functional and technical accounts for daily and emergency O&M to O&M teams or individuals. Low-level logging is supported on bastion servers to ensure that all operations on the target host can be traced to any O&M personnel.

8.1.2 Permissions Management

System account and permission management includes account lifecycle management and permissions management, which are described as follows:

- **Account lifecycle management**: It includes the administration of account registration and deletion, account owners and users, passwords, and the monitoring and auditing of account registration and deletion. Once created,

 Copyright © Huawei Technologies Co., Ltd.

new accounts are immediately scoped in for daily O&M by security administrators. All O&M, device, and application accounts are centrally managed. All accounts are centrally monitored and automatically audited through the unified audit platform. Therefore, the entire account lifecycle is well managed, from account creation, permissions granting, permissions verification and access granting, and account and permissions deletion.

- **Account permissions-granting process**: When a user requests the use of an account, the account security administrator must start the permissions-granting procedure and modify permissions after approval, providing the requestor with a new passphrase when needed. An account cannot be approved for permission changes nor granted permissions by the account owner.
- **Permissions management**: Based on different business roles and responsibilities, access permissions management applies RBAC and includes the following basic roles: core network, access network, security devices, service systems, database systems, hardware maintenance, and monitoring maintenance. Any O&M personnel is restricted to access only devices within the administrative scope of his/her role and is not granted permissions to access other devices.

  During daily operations, Huawei Cloud O&M personnel are strictly prohibited from the following:

  - Bypass security auditing measures or modify, delete, or destroy system logs.
  - Connect any personal storage device to a server.
  - Secretly connect any storage device to a server without proper approval.
  - Modify the usage of facilities, equipment, or systems in the production environment, or engage in activities or operations that are inconsistent with the functions as per their specifications.

8.1.3 Access Security

Huawei Cloud boasts a large team of high-caliber O&M personnel to ensure the continuous and stable operations of Huawei Cloud data centers and services. Centralized O&M management and auditing is achieved through VPNs and bastion hosts that are deployed in Huawei Cloud data centers. External and internal network O&M personnel perform all local and remote O&M operations on networks and devices such as servers in a centralized manner, which ensures unified management of O&M account authentication, authorization, access and auditing.

- **Remote O&M access from external networks**: For remote management of Huawei Cloud, whether from the Internet or Huawei corporate network, one must first connect to Huawei Cloud's bastion server environment, and then access target resources from a bastion server. Below sum up the two approved remote access paths:

  - **Path 1: Access over the Internet**. When performing O&M over the Internet, O&M personnel must first establish an SSL VPN tunnel to connect to Huawei Cloud O&M network, where they are restricted to access only the bastion servers, from which they can access their targeted systems for O&M operations. This process minimizes O&M access exposure to the Internet.

 Copyright © Huawei Technologies Co., Ltd.

  - **Path 2: Access over Huawei intranet**. O&M personnel uses Huawei's existing bastion server environment to connect from Huawei corporate network into Huawei Cloud O&M network (usually using the MPLS VPN to connect these two types of internal networks). Once inside Huawei Cloud O&M network, O&M personnel are restricted to access only the jump servers, from which they can access their targeted systems for O&M operations. This process also minimizes O&M access exposure to Huawei corporate intranet.
- **O&M access authentication:**
  - Access authentication can be configured to use an independent account system to centrally manage user accounts/passwords and grant permissions, keeping access management simple and secure.
  - Device password automatic rotation can be enabled with an interval in days, weeks or months, by which the corresponding devices automatically reset their passwords. Only superuser administrator accounts can be used to look up the changed device passwords but other users' passwords remain invisible. O&M account password policy settings resemble those of Windows OS, that is, primarily password length and complexity.

8.2 Vulnerability Management

The Huawei Product Security Incident Response Team (PSIRT) has a reasonably mature vulnerability[1] response program. The nature of Huawei Cloud's self-service model makes it necessary for PSIRT to continuously optimize the security vulnerability management process and technical means. It will ensure rapid patching of vulnerabilities found on in-house-developed and third party technologies for Huawei Cloud infrastructure, IaaS, PaaS and SaaS services, mitigating risks to tenants' business operations.

In addition, Huawei PSIRT and Huawei Cloud's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. Huawei Cloud relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in Huawei Cloud infrastructure and cloud services, and O&M tools, regardless whether they are found in Huawei's or third party technologies, are handled and resolved within SLAs. Huawei Cloud strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers.

Note:

1. "A vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy" (RFC 4949).

8.2.1 Vulnerability Identification

Huawei PSIRT has well-established vulnerability detection, identification and collection channels. Huawei's official website includes PSIRT email address psirt@huawei.com for vulnerability submission and Huawei Bug Bounty Program (https://bugbounty.huawei.com/hbp). PSIRT welcomes international vulnerability response coordination organizations, service providers, security companies, other organizations, security researchers, and Huawei employees to submit

vulnerabilities on Huawei products, services and solutions. In addition, Huawei PSIRT closely monitors industry-reputable vulnerability databases, security forums, email distribution lists, industry security conferences and other channels to identify Huawei- and Huawei Cloud-related vulnerabilities close to real time. A corporate-level vulnerability database covering all Huawei products, services and solutions, Huawei Cloud included, has been created to ensure the effective logging, tracking, resolution and closure of each and every vulnerability. Moreover, Huawei Cloud has provided a mailbox hws_security@huawei.com to collect vulnerability information, and Huawei Cloud's security O&M team has also used commercial and self-developed online security scanning tools to regularly perform vulnerability scanning tasks (tenant instances are not scanned) in the entire Huawei Cloud, leaving no blind spots for our vulnerability management.

8.2.2 Vulnerability Response & Resolution

Unlike Huawei's traditional ICT business models, Huawei Cloud has more complete network configuration information and more privileged device operation permissions. That combined with the DevOps and DevSecOps processes that Huawei Cloud has adopted, Huawei Cloud is capable of much more rapid vulnerability response and patch management, which is directly built into the CI/CD pipeline.

Huawei Cloud uses the industry best practice Common Vulnerability Scoring System (CVSS) to assess the severity of vulnerabilities, and determines the handling priorities based on the rating of vulnerability exploitation risks on Huawei Cloud. As Huawei Cloud directly provides services for end users and faces greater Internet attack risks, Huawei Cloud determines whether a service is exposed to Internet (ETI) when assessing the vulnerability severity. Then, the final SLA requirements for vulnerability fixing are determined based on comprehensive consideration.

Huawei Cloud has set up an end-to-end vulnerability response work order system covering every step of the process, from vulnerability detection, identification to hotfix and patch management. This system automatically collects vulnerabilities from various channels such as PSIRT and online scanning tools, and then automatically assigns priority ratings based on criticality and maps with vulnerability resolution SLAs. In the case of a major vulnerability, the security O&M team uses in-house tools to scan Huawei Cloud network, maps out the scope of affected services, systems and components within minutes. In addition, the security O&M team takes necessary vulnerability mitigation measures based on the live network situation, for example, restricting port access and implementing WAF vulnerability rules to protect or isolate affected services, reducing the risk of vulnerability exploitation. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the impact on tenant services. In addition, Huawei Cloud continuously updates operating system and container images, and rectifies system vulnerabilities by rolling upgrade of the images and containers. This does not affect tenant services.

8.2.3 Vulnerability Disclosure

To protect end users and tenants, Huawei Cloud upholds the principle of responsible disclosure. While ensuring no undue risks of potential exploitation and attacks will result from the disclosure of any vulnerability, Huawei Cloud continues

to proactively make recommendations on platform-layer and tenant service-specific vulnerabilities, and offer our end users and tenants vulnerability mitigation solutions, standing shoulder to shoulder with our customers in tackling security challenges caused by endless vulnerabilities.

8.3 Security Logging & Event Management

A cloud security event is a suspected cloud network, system, application attack or sabotage or a suspected account or data breach that may cause or has caused data leakage, data tampering, system or account compromise, and service interruption. Such events, once confirmed, usually have a negative impact on the CSP reputation and brand. Cloud attacks primarily include infrastructure-, platform-, and application-layer attacks (such as backdoors, vulnerability exploitation, network scanning, eavesdropping, phishing, DoS/DDoS, OWASP Top 10), data breaches (such as data tampering, spoofing, leakage, theft, and loss).

To ensure the professionalism, urgency, and traceability of security event handling, Huawei Cloud has comprehensive security log management requirements, security event rating and handling processes, a 24/7 professional security event response team, and a corresponding security expert resource pool. Huawei Cloud strives to achieve rapid security incident response in terms of incident detection, impact scoping, damage isolation, and service recovery. In addition, Huawei Cloud keeps our security event rating criteria, time to response, and time to resolution up to date by taking into account the impact of a security event or incident on our entire network and customers.

8.3.1 Log Management and Auditing

Huawei Cloud uses a centralized and comprehensive log system based on big data analytics. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as threat detection logs of security products and components. The logs support for cybersecurity event backtracking and compliance and include the following information: resource IDs (such as source IP addresses, host IDs, and user IDs), event types, date and time, IDs of the affected data/components/resources (such as destination IP addresses, host IDs, and service IDs), and success or failure information. This log analysis system supports massive data storage and powerful search and query features, which can store all logs for over 180 days and support real time queries within 90 days. Huawei Cloud also has a dedicated internal audit department that performs periodic audits on O&M activities.

Huawei Cloud log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third-party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk.

8.3.2 Rapid Detection and Impact Scoping

Huawei Cloud is built upon a solid, multi-layered full stack security framework with comprehensive perimeter defense. For example, layers of firewalls isolate networks by security zone, anti-DDoS quickly detects and protects against DDoS attacks, WAF detects and fends off web attacks close to real time, and IDS/IPS detects and blocks network attacks from the Internet in the real time while also monitoring for behavioral anomalies on the host.

 Copyright © Huawei Technologies Co., Ltd.

Given that a public cloud usually needs to process huge amounts of traffic while also exposed to a wide variety of attacks, Huawei Cloud employs its situation awareness analysis system, which correlates security alerts and logs from myriad security appliances, and performs centralized analysis to ensure rapid and thorough detection of ongoing attacks and forecast potential threats.

- Unlike traditional O&M processes (which lack tool-based automation and mostly rely on inefficient manual operations and experience-based analysis of security events), Huawei Cloud's Big Data security analytics platform detects threats in real time or close to real time from large volumes of original alerts and logs, and displays detected threats visually on the security O&M console dashboard. This technology greatly reduces the manual labor required for data analysis, and shortens attack detection and impact scoping to a matter of seconds.
- The Big Data security analytics system incorporates a number of threat analytics models and algorithms, processes threat intelligence and security advisories, and accurately identifies attacks, including the most common cloud attacks such as brute force attacks, port scanning, zombie attacks, web attacks, unauthorized web access, and APT attacks. In addition, the system performs real-time evaluation of the security posture of Huawei Cloud, analyzes potential risks, and provides warnings by combining known risks, potential risks with threat intelligence, helping Huawei Cloud take necessary security precautions.

8.3.3 Rapid Isolation and Recovery

- When Huawei Cloud is under attack, perimeter security appliances become the first line of defense for rapid isolation and recovery. For example, Huawei Cloud's built-in anti-DDoS protection scrubs the attack traffic layer by layer and fends off both volumetric DDoS and application-layer DDoS attacks in real time. WAF also detects web attacks in real time, sends out an alert for each high-risk attack, and instantly activates automatic blocking of the attack. IPS protects both the platform and tenant spaces against attacks.
- The Big Data security analytics platform integrates with a variety of security appliances to detect and block attacks, forming a second line of defense for rapid isolation and recovery. The platform can instantly detect intrusions, accurately identify attack sources, and intelligently activate automatic blocking of detected intrusions through its integration with security appliances, shortening time-to-block to merely seconds.
- Huawei Cloud also partners with telecom carriers to automatically block volumetric DDoS attacks. This forms the third line of defense for rapid isolation and recovery. When a volumetric DDoS attack impacts Huawei Cloud's actual throughput, its built-in anti-DDoS capability automatically communicates and correlates with the carrier's anti-DDoS system, which drops the attack traffic on the carrier's backbone routers, restoring Huawei Cloud's throughput and its tenant services, and ensuring normal tenant business operations. The entire execution, start to finish, does not exceed 2 minutes.
- Huawei Cloud has formulated various specific contingency plans to deal with complex security risks in the cloud environment. Each year, Huawei Cloud conducts contingency plan drills for major security risk scenarios to quickly reduce potential security risks and ensure cyber resilience.

 Copyright © Huawei Technologies Co., Ltd.

8.4 Disaster Recovery and Business Continuity

Huawei Cloud infrastructure is highly available and thereby minimizes the impact of system failures on our customers.

8.4.1 High Availability of Infrastructure

- Huawei Cloud implements a disaster recovery (DR) and data backup solution that is based on the "two sites, three data centers" data center clustering architecture. Data centers are located throughout the world with proper site surveys as per regulations. All of them are operating normally and serving customers. In terms of the "two sites, three data centers" architecture, the two sites serve as each other's DR site and keeps each other backed up. In the event of failure in a data center at one site, the system can automatically migrate customer applications and data from the affected site to the unaffected site on the premise of compliance, ensuring business continuity. Huawei Cloud has also deployed a global load balancing (GLB) scheduling center, and customers' applications are deployed in N+1 mode across data centers, which enables load balancing of customers' application traffic to other unaffected data centers if one data center experiences failure.
- Compute instances and data stored in Huawei Cloud can be flexibly exchanged among multiple regions or multiple AZ within the same region. Each AZ is an independent, physically isolated fault maintenance domain, has its own UPS and on-site backup power generator, and also connects to a power grid different than any other AZ. All AZs connect to multiple tier-1 telecom providers for redundancy, eliminating the risk of single point of failure.
- Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in Huawei Cloud. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures).

8.4.2 DR Among AZs

To minimize service interruption caused by hardware failures, natural disasters, or other disastrous events, Huawei Cloud has prepared DR plans for all data centers.

- User data can be replicated and stored on multiple nodes in a data center. If a single node fails, user data will not be lost. The system supports automatic failure detection and data recovery.
- Different AZs within a single region have implemented Data Center Interconnection (DCI), connecting them through high-speed fiber and supporting the essential requirement of cross-AZ data replication. Users can also leverage our DR replication service and solution based on their business needs.

 Copyright © Huawei Technologies Co., Ltd.

8.4.3 Business Continuity Plan and Testing

- In addition to the high availability infrastructure, data redundancy and backup, and DR among AZs, Huawei Cloud also has a formal business continuity plan (BCP) and conducts BCP drills periodically. This plan, which applies to major disasters such as earthquakes or public health crises, ensures continued operations of Huawei Cloud services and safeguards customers' service and data security.
- Huawei Cloud has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first, bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP.

 Copyright © Huawei Technologies Co., Ltd.

9 Security Ecosystem

Faced with radically evolving, rapidly growing, and highly damaging security threats, open, well-orchestrated and rapid threat detection, defense in depth, and timely service recovery has nowadays become a widely-accepted absolute necessity in the security industry. CSPs provide services for vast numbers of tenants with differing levels of security requirements. This makes it extremely difficult to rely solely on their own technical and service capabilities to protect tenant data and service security. As a result, Huawei Cloud has gathered a broad, comprehensive group of security partners who can share their capabilities and thereby jointly provide security assurance for tenants.

Committed to building an open, collaborative, and mutually beneficial security ecosystem. Huawei Cloud is cooperating with industry-leading security products and service suppliers, based on a shared responsibility model. This helps Huawei and its partners to provide cloud tenants with a comprehensive, easy-to-deploy, easy-to-manage security solution to address known and unknown security threats, safeguarding tenant data and ensuring service security.

- **Security technologies**: Huawei Cloud partner with leading security product and service vendors to provide products and services in various fields such as host security, network security, data security, application security, and security management. Together with partners, Huawei Cloud has launched host intrusion detection, web application firewall, host vulnerability scanning, web page anti-tampering, and penetration test services, which enhance the security detection, correlation, and protection capabilities of Huawei Cloud.
- **Security consulting services**: Huawei Cloud seeks close partnership with leading vendors in every major industry, striving to develop security solutions for industries such as finance, government, transportation, and manufacturing. In addition, Huawei Cloud works with solution partners throughout the world, helping users design industry-specific security solutions and business models and accelerate industry-wide digital transformation.
- **Security ecosystem**: Huawei Cloud is devoted to the healthy development of the cloud computing industry. Huawei Cloud not only establishes close partnerships in the fields of security technologies and consulting services, but also actively participates in and contributes to cloud security standards and open source communities. In addition, Huawei Cloud openly offers free of charge various infrastructure capabilities and security services to software and application developers.

 Copyright © Huawei Technologies Co., Ltd.

- **Market opportunities**: Huawei Cloud provides abundant opportunities and many types of technical support for security ecosystem partners. Firstly, Huawei Cloud's security ecosystem partners can use Huawei Cloud's Marketplace to offer their products, solutions, and services, sharing the existing customer base and potential sales opportunities with Huawei Cloud. Utilizing the Marketplace and technical capabilities of Huawei Cloud, partners can also become more effective with their sales, service delivery, and maintenance, and thereby reduce their operating expenses. Secondly, partners can deploy their services all over the world by riding on Huawei Cloud network that spans the entire world. Those outstanding partners also have the opportunity to obtain the market leads shared and solutions recommended by Huawei Cloud during global business expansion. Thirdly, Huawei has established broad and comprehensive partnership with market sectors such as government, education, healthcare, transportation, manufacturing, energy, and large enterprise. Huawei Cloud will soon open up these market resources to partners and help them develop new security products and solutions, achieving win-win for customers, partners, and Huawei Cloud while assuring customers' digital transformation. Last but not least, Huawei Cloud security partners will have the opportunity to participate in myriad brand promotion events both online and in person, present products and solutions, and share customer success stories. As our partnership strengthens further, partners will also have the opportunity to participate in joint brand promotion events and release joint solutions to customers with Huawei Cloud.
- **Technical support**: Huawei Cloud provides several types of technical support for security partners. Firstly, Huawei Cloud enables partners to carry out their cloud transformation strategies, helping them migrate their products and services to the cloud. Secondly, Huawei Cloud opens up cloud service interfaces to partners so that they can develop and integrate security solutions for a much broader customer base, helping translate these solutions to customer value and partner success. Thirdly, Huawei Cloud will gradually offer up its security technology and security engineering capabilities to the community, sharing security experience and resources such as technical documentation, security standards, methodologies and workflows, and security testing, and further enabling partners through security training, certification, open interfaces for development and integration. Last but not least, Huawei Cloud promotes security intelligence sharing under the umbrella of laws and regulations and also consent by customers and partners. Authorized partners can also receive free testing resources and trainings, and benefit from preferential business policies.

As security threats from an increasingly intelligent society emerge, Huawei Cloud will more actively engage with our security partners worldwide and work closer with them to create an open, collaborative, and win-win security ecosystem. Huawei Cloud will continue to deliver cloud security value-added services and bolster customer trust, sparing no effort to make progress in the cloud and cloud security industry, and effect positive changes in society as a whole.

 Copyright © Huawei Technologies Co., Ltd.