Huawei Cloud Security White Paper

Issue	**3.4**
Date	**2023-12-26**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com/

Website: https://www.huawei.com/

Email: support@huawei.com

Contents

1 Introduction

In early 2017, Cloud Business Unit (Cloud BU) was formally established, raising the curtain on a new era for Huawei Cloud.

Recent years have seen the rapid evolution of threats to cloud security, with new threats emerging at an alarming and increasing rate. Huawei Cloud, like most Cloud Service Providers (CSPs) and cloud customers, has risen to the challenge by continuing to learn, explore, and mature, largely benefiting from this process. It faces these emerging security challenges in stride and sees opportunities to offer secure and trustworthy cloud services by collaborating with ecosystem partners in accordance with its committed lines of business, furthering its objective to both safeguard and add value to customer business.

A comprehensive set of highly effective cloud security strategies and practices has emerged through integrating industry-wide leading cloud security concepts and the best security practices of 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 a multi-layered security architecture that provides in-depth defense and complies with all relevant regulations. Furthermore, Huawei Cloud continues to improve the security of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) services. This is all supported by 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 its ecosystem partners, continue to prioritize customers 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 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, customers, and partners.

Within this context, Huawei Cloud releases the *Huawei Cloud Security White Paper* ("this White Paper"), which shares Huawei Cloud's extensive cloud security experience with users and the industry at large, helping each party 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:

- From tenants, ecosystem partners, and communities to general Internet users
- From small, medium-sized, and large enterprise customers to individual users
- From the decision-making executive level and the management level to cloud service related technical personnel in IT, security, and privacy and personnel in other cloud service related positions, including marketing, procurement and contracting, and compliance audit.

Note

DevOps is a set of practices that combines software development and IT operations. The concept was created by high-tech industry practitioners, as opposed to theorists, and it has matured along with the development of cloud services. Cloud services and other online features entail Continuous Integration/Continuous Delivery (CI/CD) supported by DevOps, as opposed to the Security Development Lifecycle (SDL) in traditional waterfall and agile processes, which is not suited for new demands. Security must be seamlessly embedded into and highly automated throughout the engineering process. As a result, a new security lifecycle management process called DevSecOps was created. Based on Huawei's study on the practices of world-leading CSPs and major online service companies around the world, it is evident that DevOps/DevSecOps and corresponding tool chains are being fully adopted by these companies at an accelerating rate. With security seamlessly embedded into DevOps, DevSecOps will not weaken security; instead, it will be effectively elevated through a high degree of automation.

2 Cloud Security Strategy

Increasingly complex cybersecurity threats and challenges are emerging at an alarming rate, as cloud service related technologies and Information and Communications Technology (ICT) as a whole continue to evolve and progress. Cloud security threats in particular are becoming increasingly difficult to handle. In fact, cybersecurity has become a multi-faceted challenge for cloud technology vendors and security companies across the globe. Only through global collaboration between vendors, service providers, and customers, as well as industry standards bodies, and 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 can successfully handle unforeseen cloud security risks rooted in the misuse and abuse of technologies.

As a leading provider of ICT solutions worldwide, Huawei fully understands the importance of cybersecurity and cloud security, which are emphasized by governments and customers worldwide.

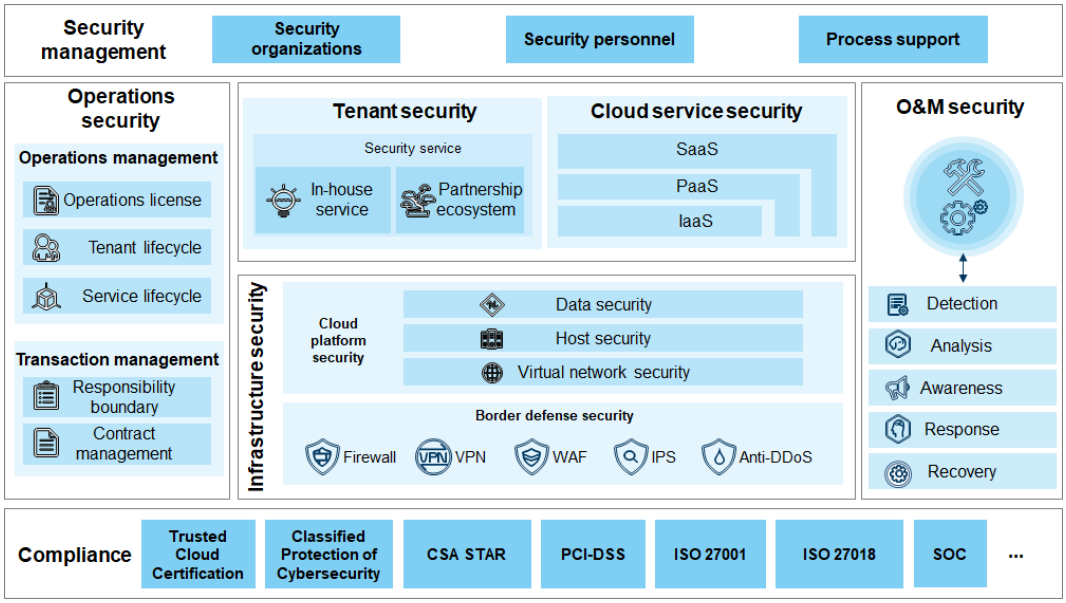
The cloud era is accompanied by an endless variety of new security challenges, pervasive threats, and persistent attacks[1]. Huawei is increasingly cognizant of these security concerns and prioritizes — through heavy investment — technological competency, regulatory compliance, and ecosystem growth in cybersecurity 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 mitigate their cloud security risks. Huawei asserts that the establishment of an open, transparent framework for cloud security solutions featuring visualization is instrumental to sustainable progress across the entire cloud service industry, and it is especially crucial 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 efforts. Cloud security at Huawei dates back to the establishment of Huawei Security Test Lab in 2000. Since then, Huawei has spared no effort in strengthening its security capabilities, striving to enhance the R&D and O&M of its 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, which was based on a Network Processor (NP) architecture.
- 2008: together with Symantec Corporation, established a joint venture named Huawei-Symantec Technologies Co. Ltd., focusing on security.
- 2011: opened Security Competence Center to specialize in the R&D of security capabilities.
- 2012: held the largest share of the cybersecurity product market in China.
- 2015: launched cloud 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 Advanced Anti-DDoS (AAD) and Database Security Service (DBSS).
- 2018: launched the Dedicated Hardware Security Module (DHSM).

Cybersecurity and privacy protection are Huawei's top priorities. Moving forward, Huawei Cloud 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 the industry's best security practices, but also complies with all applicable country- and region-specific security policies and regulations, as well as international cybersecurity and cloud security standards. This forms our security baseline. Moreover, Huawei Cloud continues to build and mature in areas such as security-related organizations, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction. The aim is to provide highly trustworthy and sustainable security infrastructure and services to our customers. We also openly and transparently address cloud security challenges with our customers and partners, as well as the relevant governments, to meet the security requirements of our cloud users.

Figure 2-1 Huawei Cloud security protection framework



- **Organization:** The Global Security and Privacy Committee (GSPC), as the highest cybersecurity management organization at Huawei, is responsible for company-level security policy decisions and the authorization of overall security strategies. As a key member of the GSPC, the Global Security and Privacy Officer (GSPO) is responsible for leading and guiding the team to develop 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 also ensures that cybersecurity is systematically practiced in each applicable function, area, and process and actively enhances communication with governments, customers, partners, employees, and other stakeholders. Additionally, Huawei Cloud continues to fine-tune its flat organization that befits the CI/CD of cloud services.
- **Processes:** Security activities are fully integrated into key business processes at Huawei, including 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 its business processes by conducting internal audits and subjecting them to security accreditation and attestation by different nations' government agencies for cybersecurity and independent third-party audit/test agencies. For example, Huawei's security management system obtained BS7799-2/ISO27001 certification in 2004 and has maintained it ever since. By leveraging existing company-level business processes, Huawei Cloud has integrated the SDL — which 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. They not only support the increasingly agile online releases of Huawei Cloud services, but also ensure E2E security from R&D to deployment.
- **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 (including legal actions) against employees who violate the policies.

- **Technical capabilities:** Huawei Cloud focuses on data protection, leverages the company's 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, through big data analysis of network security posture, Huawei Cloud identifies, prevents, mitigates, and resolves major risks, threats, and attacks. It employs a robust multi-layered technological framework for cloud security protection, monitoring, analysis, and response to ensure cloud service O&M security, thereby supporting rapid detection, isolation, and recovery when faced with security risks, threats, and attacks. Huawei Cloud's advanced technologies bring tenants convenience, security, and business value.
- **Compliance:** In regions within our cloud service coverage, Huawei Cloud actively facilitates dialogue with local regulators 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. Additionally, Huawei Cloud shares its legal and regulatory insights with customers, avoiding violations caused by inadequate information disclosure. While ensuring that tenant contracts accurately specify the security responsibilities of both sides, Huawei Cloud continuously complies with regulatory requirements by obtaining cross-industry, cross-region cloud security certifications. It continues to foster and strengthen customer trust by gaining security certifications that target key industries and regions, striving toward a secure cloud environment built by law-makers, cloud platform administrators, and tenants.
- **Ecosystem:** Huawei believes that no single organization or company has sufficient resources to address the increasingly complex risks and threats to cloud security. Therefore, we call on all our security partners worldwide to join forces and develop a cloud security business and technology ecosystem, where security services are provided to tenants. Huawei Cloud Marketplace welcomes security technology vendors, as well as organizations and individuals, with competitive advantages, to provide cloud security services. We also invite our cloud business partners to leverage their unique experiences and insight into cloud services and the cloud security industry and package their security services into optimal 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 and outside China. Huawei strives to ensure the security of customers worldwide and contribute to the industry.

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

NOTE

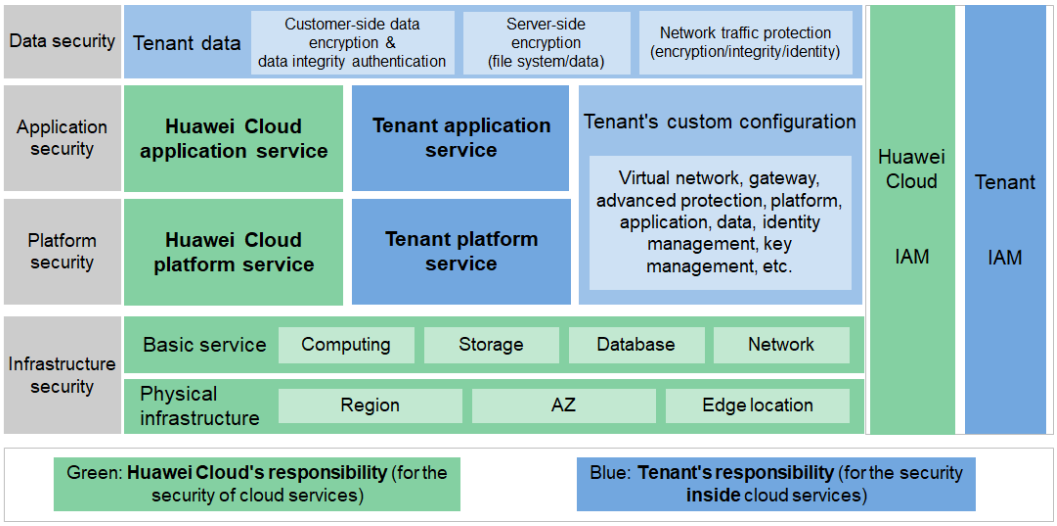
Cloud Security Alliance (CSA) has an ongoing project and work group that focuses on covering the latest cloud security challenges, threats and attacks in an organized manner. For details, refer to CSA Cloud Security Top Threats.

3 Shared Responsibility Model

Cloud security focuses on ensuring the high performance, stability, and security of all applications and services, without the risk of outage. This ranges from internal data center O&M to customer-facing IaaS, PaaS, and SaaS. However, data centers that run cloud services are considerably different from those geared toward traditional IT. In terms of overall security design and practices, data centers with cloud services attach more priority than traditional IT data centers to providing tenants with comprehensive, multi-dimensional, customized, and combined security and privacy protection functions and configurations, covering infrastructure, platform, application, and data security. In addition, Huawei Cloud security services support the customization of various advanced security settings according to 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 multiple silo technologies, along with the increasingly automated cloud security O&M.

In the following chapters, we describe how Huawei Cloud makes advanced cloud security systems a reality, while adhering to the best practices in security during both R&D and O&M. This chapter introduces the shared responsibility model for Huawei Cloud services. Huawei Cloud has defined the model according to widespread practices across the industry, as shown in the following figure.

Figure 3-1 Shared responsibility model for Huawei Cloud services



Huawei Cloud is responsible for the green part, while tenants are responsible for the blue part. Huawei Cloud is responsible for providing secure cloud services, while tenants are responsible for the internal security and secure use of 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 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, storage, and database services, and the management of virtual networks, load balancing, security gateways, Virtual Private Networks (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.

Huawei Cloud is primarily responsible for developing and operating the physical infrastructure of its data centers; the IaaS, PaaS, and SaaS services it provides; and the built-in security functions of various services. Huawei Cloud is also responsible for building a multi-layered protection system with defense in depth, which spans the physical, infrastructure, platform, application, and data layers, in addition to the cross-layer Identity and Access Management (IAM) function. Additionally, it ensures secure O&M.

Tenants are primarily responsible for customizing configurations and operating the virtual network, platform, application, data, management, security, and other cloud services that they subscribe to on Huawei Cloud. This includes the customization of Huawei Cloud services as well as the O&M of any platform, application, and IAM services that tenants deploy on Huawei Cloud. Tenants are also responsible for customizing the security settings at the virtual network layer, platform layer, application layer, data layer, and cross-layer IAM function, as well as their O&M security and effective user identity management.

3.1 Huawei Cloud's Security Responsibilities

Huawei Cloud is responsible for the security of its IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers that these services operate on. Huawei Cloud is also responsible for the security functions and performance of its infrastructure, cloud services, and technologies, as well as the overall cloud O&M security and, in an even broader sense, the security compliance of its infrastructure and services. (Refer to section 4.1 "Security Compliance and Standards Compliance" for details on security compliance.)

- From one perspective, Huawei Cloud works to ensure the secure development, configuration, and deployment of its cloud technologies. From another perspective, Huawei Cloud is responsible for the O&M security of its cloud services, for instance, the rapid detection, isolation, and response to security

incidents, ensuring fast recovery. In addition, Huawei Cloud adopts a vulnerability management mechanism befitting cloud services to not only ensure prompt response to vulnerabilities, but also support rapid release and continuous deployment of tenant-facing services. To support CSP O&M lifecycle management and avoid impacting 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 is responsible for developing highly competitive value-added cloud security services for tenants.

- Of all aspects of O&M security, Huawei Cloud attaches the highest priority to infrastructure security and privacy protection. Infrastructure primarily consists of the physical environment supporting cloud services, in-house 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 their O&M security when they operate within Huawei Cloud.
- Huawei Cloud supports the secure configuration and version upkeep of its cloud services.
- Regarding tenant data, Huawei Cloud provides comprehensive data protection functions to achieve confidentiality, integrity, availability, durability, authentication, authorization, and non-repudiation, and it is also responsible for the security of the related functions. However, Huawei Cloud is merely the trustee of tenant data, meaning tenants retain sole ownership of their data and control how it is used. It prohibits all 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 the legal and regulatory compliance of its services. Huawei Cloud shares its compliance practices with tenants and conducts internal and independent evaluations of its compliance posture for security standards specific to the industries that Huawei Cloud serves, with evaluation results kept reasonably transparent to tenants.
- Huawei Cloud engages 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 database-level security patch management, but also custom configurations of virtual firewalls, API gateways, and advanced security services. Additionally, Huawei Cloud helps tenants in anti-DoS/DDoS exercises, security incident response, and disaster recovery.

3.2 Tenants' Security Responsibilities

Tenants of Huawei Cloud are responsible for security inside the IaaS, PaaS, and SaaS services that they subscribe to. Specifically, they are responsible for securely and effectively managing their customization of cloud service configurations. This includes 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 the cloud services that tenants subscribe to. These responsibilities are tied to the specific default or customized security configurations that tenants implement. As for each

Huawei Cloud service, tenants are solely responsible for the security configurations of all the cloud service resources they manage, whereas Huawei Cloud is only responsible for providing tenants with the cloud resources, functions, and performance capabilities required to execute specific security tasks.

- Tenants are responsible for the following:
  (1) Policy configurations of tenant-managed virtual firewalls, gateways, and advanced security services
  (2) Security configurations and management (for example, software version and security patch management) for tenants' virtual networks, virtual hosts, containers, and guest VMs; and security configurations of platform-level services such as container security management (including cluster, node, and container security configurations, and access control security configurations) and big data analytics
  (3) Security configurations inside any services that tenants subscribe to
  (4) Security management of any application software or utility that tenants deploy on Huawei Cloud
- When configuring cloud services, tenants are responsible for conducting adequate pre-production testing of security configurations to prevent adverse effects on their applications and minimize business impact. For the security of the majority of cloud services, tenants need to configure only accounts, and grant them the necessary permissions to access resources, and properly manage account credentials. Tenants need to set additional security configurations for a few cloud services to achieve desired security. In addition, because monitoring and management services, as well as advanced security services, feature numerous security configurations, tenants may seek technical support and professional services from Huawei Cloud and its partners to ensure optimal security.
- When using MapReduce Service (MRS), tenants are responsible for the following:
  (1) Managing the policy configurations (such as elastic IP addresses and virtual network firewalls) of purchased MRS big data clusters
  (2) Configuring access control policies. For example, ports bound to elastic IP addresses are open only to trusted networks or hosts, preventing big data clusters from being directly exposed to the Internet
  (3) Managing users of the big data clusters, setting security configurations of big data components, and properly maintaining relevant account credentials
  (4) Managing the security of applications deployed on big data clusters
- When using database services, tenants are responsible for database engine lifecycle management and database security management, including the following:
  (1) Using the latest instance version by default and updating versions as prompted by the Huawei Cloud official website and vulnerability notices
  (2) Reviewing asset categories and formulating database instance protection policies, such as database active/standby and cluster design, data disaster recovery and restoration policies, VPC and security group configuration, Internet access configuration, access channel encryption configuration, database authentication and authorization configuration, database audit configuration, and other security configurations

- Regardless of the Huawei Cloud service, tenants always own and have full control of their data. They are responsible for the security configurations necessary to ensure data confidentiality, integrity, and availability, as well as authenticating and authorizing data access. When using IAM and Data Encryption Workshop (DEW), tenants are responsible for properly managing their own service accounts, passwords, and keys. They are also responsible for adhering to the best security practices in the industry for password and key creation, reset, and renewal; 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.

  Tenants are solely responsible for the legal and regulatory security compliance of any application and service not included in Huawei Cloud's service offerings but deployed and operated on Huawei Cloud by the tenants.

4 Security Compliance and Privacy Protection

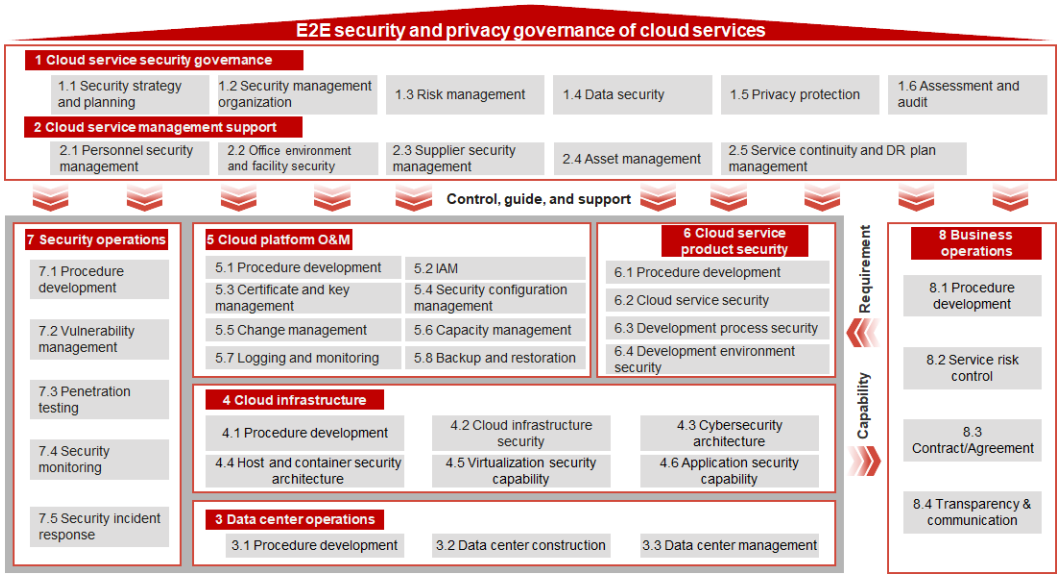
Huawei Cloud has always been committed to and is continuously increasing its investment in improving customer trust. Compliance with security standards and regulations is the only way to earn and maintain customer trust and also an important method of defending against malicious insiders. On top of that, obtaining certification for compliance with industry security standards and regulations helps improve the overall security capabilities and service level of Huawei Cloud, while also alleviating any customer concerns about compliance and data security. Strictly adhering to customer-centric core values, Huawei Cloud fully understands the importance of customers' personal data security, respects and protects customers' right of privacy, and follows 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, views cybersecurity and privacy protection as top priorities, and ensures that cybersecurity and privacy protection requirements are preferentially supported.

4.1 Security Compliance and Standards Compliance

To implement comprehensive and efficient security and privacy compliance governance, Huawei Cloud developed a cloud-native security governance framework – Cloud Service Cybersecurity & Compliance Standard (3CS) — based on 16 mainstream global security standards in the industry and Huawei's 30 years of experience in security operations management and technical accumulation. The basic concept of the 3CS system is to divide security control domains based on the processes of each cloud service module, enabling security control requirements to be embedded into the cloud service management process, which in turn ensures that security management responsibilities are clear, measurable, and traceable.

The 3CS system helps Huawei Cloud fully utilize its global compliance governance experience. This significantly cuts the time required to obtain regulatory and industry standards certifications, implements comprehensive and efficient security governance, and continuously improves the trustworthiness of cloud services.

Figure 4-1 3CS framework



Huawei Cloud leverages its compliance governance capabilities through 3CS and continues to ensure that its infrastructure and cloud services pass evaluation and certification by independent, industry-recognized third-party security organizations. Huawei Cloud provides customers with secure and compliant infrastructure and services. Up to now, Huawei Cloud has obtained over 100 authoritative security compliance certifications from both in and outside China. Industry security evaluations and certifications demonstrate Huawei Cloud's security risk controls in terms of policies, processes, organizations, technologies, and other aspects, enabling customers to fully understand Huawei Cloud's investment and effective control capabilities in ensuring cloud service and user data security.

One example is the Cloud Security Alliance - Security, Trust & Assurance Registry (CSA STAR) Gold Certification, which is based on ISO/IEC 27001 and also includes the Cloud Control Matrix (CCM) and other security requirements, covering 16 control domains such as risk governance, data/application/infrastructure security, development, and design. The CSA STAR Gold Certification demonstrates that Huawei Cloud's operational security management and technical capabilities are recognized by international authorities, and its security compliance is world-class.

Based on the shared responsibility model, Huawei Cloud continues to build and enhance its security compliance capabilities in its infrastructure (across the physical environment, network, and platform layers) and cloud services to ensure the security and compliance of its services and data.

To date, Example of Huawei Cloud Partial Standard Certification：

- ISO27001:2022
- ISO27017:2015
- ISO27018:2019
- TL 9000& ISO 9001
- ISO20000-1:2018
- ISO22301:2019
- CSA STAR Certification

- ISO27701:2019
- BS 10012:2017
- ISO 29151:2017
- PCI DSS[1]
- PCI 3DS
- ISO 27799:2016
- ISO 27034
- SOC Audit Report

For more information on HUAWEI CLOUD security compliance and downloading relevant compliance Certification please refer to the official website of HUAWEI CLOUD "Trust Center - Compliance"

In addition, Huawei Cloud proactively seeks out and adopts the industry's best security practices. For example, it 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, covering 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

- 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.

4.2 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 numerous professionals and resources to support the research and application of new technologies and ensure the privacy protection system operates effectively, ensuring Huawei Cloud leads the industry in privacy protection and achieving the corresponding 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 system to enable the privacy protection of the cloud platform and help customers implement it. Huawei Cloud formulates seven privacy protection principles (lawfulness, fairness and transparency; purpose limitation; data minimization; 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 its specific 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, which are then eliminated or reduced through appropriate measures. Huawei Cloud respects users' right of privacy. It provides a clear Privacy Statement and customer feedback channels in

prominent positions on the Huawei Cloud official website, helping customers understand the corresponding privacy protection information.

The Huawei Cloud research team is committed to developing Privacy Enhancing Technologies (PETs) to accumulate privacy protection engineering capabilities, meeting 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 on Huawei Cloud privacy protection policies and statements, see the *White Paper for Huawei Cloud Privacy Protection* or visit the Huawei Cloud official website.

NOTE

- First privacy protection method for product R&D cycles. After recent years of development, it has gradually evolved into the management concept for 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.
- PIA is a widely used and recognized privacy assessment and design tool in the industry. It helps organizations identify and reduce business privacy risks.

5 Security Organization and Personnel

To continuously improve employees' security awareness, protect customer interests, and boost product and service reputation, Huawei advocates a company-wide mindset and practice where "everyone understands security", cultivating a 24/7 security culture that is dynamic and competitive throughout the company. The impact of such a culture runs through talent recruitment, employee orientation, initial and ongoing training, and internal transfer, 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.

5.1 Security Organization

Huawei prioritizes cybersecurity as a key strategy, and therefore implements it from 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 GSPO Office are responsible for formulating and executing Huawei's E2E cybersecurity framework, with the GSPO reporting directly to the company 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, accommodating the DevOps and DevSecOps processes best suited for cloud services. This flat organizational structure and cloud service oriented processes meet the requirements of the rapid and continuous integration, delivery, and deployment of cloud services. They also ensure that cloud services meet the necessary security standards to effectively manage security risks. Through functions such as cloud security engineering, cloud service and solution design and development, and O&M, Huawei Cloud develops its service security compliance and security O&M and effectively protects the interests of tenants. Due to the unique importance of cloud security to Huawei Cloud, the cloud security group reports directly to the president of Huawei Cloud.

5.2 Security & Privacy Protection Personnel

Huawei's technical security personnel include 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 the cloud service DevOps/DevSecOps workflow and cloud security audit process; develop and promote the corresponding security tool chain
- Actively participate in security Quality Assurance (QA) activities and evaluations; conduct internal and third-party penetration testing and security evaluations; track, investigate, and resolve identified security threats
- Design, develop, maintain, and operate the Huawei Cloud infrastructure security protection system and its security and privacy protection controls for business and IT applications, data, and intellectual property
- Design, develop, maintain, and operate myriad security features for the IaaS, PaaS, and SaaS services of Huawei Cloud and its overall cloud security solutions
- Ensure compliance with data and privacy protection laws and regulations in each industry, region, and country where Huawei Cloud operates; advocate the best practices in privacy protection for 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

5.3 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 established a dedicated security audit team to review compliance with security laws and regulations worldwide and internal security requirements. The team assigns over 10 members to perform at least one two-month annual audit on Huawei Cloud operations worldwide, focusing on aspects such as legal and procedural compliance; accomplishment of business objectives; reliability of decision-making information; and security O&M risks.

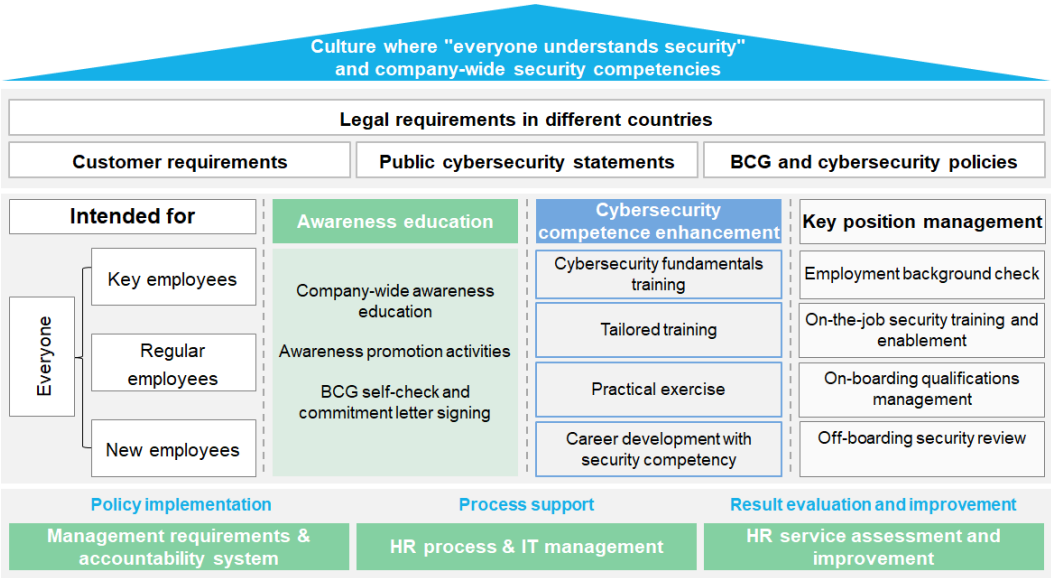
Audit results are reported to the Board of Directors and executive management, who ensure that identified issues are properly resolved and closed.

5.4 Human Resource Management

Huawei Cloud's HR management framework, like that of the entire company, was established on the basis of applicable laws. Cloud security requires HR to ensure employees' backgrounds and qualifications meet the requirements of Huawei Cloud services. Each Huawei Cloud employee must comply with applicable laws, policies,

processes, and the Huawei Business Conduct Guidelines (BCG). They must consistently demonstrate the required knowledge, skills, and experience. The overall model is as follows:

Figure 5-1 Huawei Cloud's security integration into the HR process



5.4.1 Security Awareness Education

To raise company-wide cybersecurity awareness, avoid non-compliance risks, and ensure normal business operations, Huawei provides security awareness education in three ways: company-wide awareness education, awareness promotion events, and BCG self-check and commitment letter signing.

- **Company-wide awareness education:** Cybersecurity awareness courses are held periodically for employees to continually refresh their knowledge and understand relevant policies and systems. This enables them to distinguish acceptable behavior from unacceptable behavior, assume responsibilities for any wrongdoing regardless of intent, and abide by all corporate rules and legal requirements.
- **Awareness promotion events:** Events in various formats are held to promote company-wide cybersecurity awareness. This includes cybersecurity community events, classic case study presentations, Cybersecurity Week, and animated films promoting security.
- **BCG self-check and commitment letter 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.

5.4.2 Security Competency

By utilizing industry best practices, Huawei has established a comprehensive cybersecurity training program, which implements security competency trainings for new, existing, and recently promoted employees. This program boosts security

competencies and ensures that employees deliver secure products, services, and solutions that comply with all relevant laws and regulations.

- **Cybersecurity fundamentals training:** Huawei offers security fundamentals training plans tailored to different roles and positions. All new employees must take and pass the cybersecurity and privacy protection on-boarding course by the end of their probation period to become full-time employees. Existing employees must also take and pass regular courses befitting their roles and responsibilities. Additionally, managers need to attend cybersecurity trainings and seminars.
- **Tailored trainings:** Through big data analytics, typical security issues in product R&D are detected, and the responsible parties are identified. Tailor-made security trainings, including relevant case studies, training classes, and practice questions, are delivered to the responsible parties, enabling them to continuously improve the quality of security.
- **Practical exercises:** By adopting 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 exchanges. This platform helps improve employees' security skills and response capabilities.
- **Career development with security competency:** To help employees raise their security awareness and competency and benefit more from cybersecurity trainings, Huawei integrates cybersecurity into its Competency and Qualification (C&Q) criteria. Employees must attend and pass cybersecurity courses when they are promoted.

5.4.3 Key Position Management

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

- **On-boarding security review:** New employees must pass a security review to ensure that their background and qualifications meet cloud security requirements.
- **On-the-job security training and enablement:** Employees must take and pass cybersecurity trainings on topics such as cybersecurity awareness, code of conduct for customer network services, and customer data and privacy protection. Additionally, they must periodically adjust their training plans and take refresher courses/exams to keep up with changes in services, security threats, and regulations.
- **On-boarding qualifications management:** Personnel in key positions must pass the cybersecurity on-boarding exam. The certification administration system issues an electronic certificate valid for no more than two years to any key position employee who passes the exam. Before the certificate expires, the system reminds the employees to retake the exam.
- **Off-boarding security review:** A security clearance checklist is used to conduct the off-boarding security review for employee transfer or termination. This includes modifying or revoking accounts and privileges.

5.5 Security Violation Accountability

Huawei has established a rigorous security responsibility system and implemented accountability measures against security violations. From one perspective, Huawei Cloud carries out its responsibilities in accordance with the shared responsibility model and takes full responsibility for any security violation caused by Huawei Cloud to minimize the impact on tenants. From a different perspective, Huawei Cloud mandates that every employee be responsible for their actions and results, including the technologies and services of concern and the legal responsibility. Huawei Cloud employees are made well aware that customers and the company as a whole may face grave consequences if a security issue arises due to a security violation. Therefore, Huawei Cloud always holds employees accountable for their behavior and results, regardless of intent. Huawei Cloud will determine the nature of an employee's security violation and the level of accountability based on the consequences and take disciplinary actions accordingly. Cases will be handed over to law enforcement agencies if legal violations are involved. Direct and indirect management must also bear responsibility for negligence, substandard management, and condonation of security violations. Huawei Cloud also factors in the perpetrator's attitude and cooperation during investigation and adjusts the punishment severity accordingly.

6 Infrastructure Security

6.1 Physical and Environmental Security

Huawei Cloud has established and implemented comprehensive physical and environmental security protection strategies, procedures, and measures that comply with Class A standards of *GB 50174 Code for Design of Electronic Information System Room* and T3+ standards of *TIA-942 Telecommunications Infrastructure Standard for Data Centers*. Huawei Cloud data centers are located on suitable physical sites, as determined by high-quality site surveys. During the design, construction, and operations of data centers, physical zoning in equipment rooms as well as the appropriate placement of information system components helps prevent potential physical and environmental risks (for example, fire or electromagnetic leakage) as well as unauthorized access. Furthermore, sufficient physical space and electric power, network, and cooling capacities are provided in order to meet the requirements of rapid infrastructure expansion. The Huawei Cloud O&M team strictly implements access control, security protection, regular monitoring and auditing, and emergency response measures to ensure the physical and environmental security of Huawei Cloud data centers.

6.1.1 Physical Security

- **Data center site selection:** When choosing a location for a Huawei Cloud data center, factors such as potential natural disaster risks and environmental threats are considered. Huawei Cloud data centers avoid hazardous and disaster-prone regions and minimize any peripheral interference. For example, Huawei Cloud data centers are always located in areas where there are no potentially hazard-causing laboratories, chemical plants, or other hazardous areas within a 400-meter radius. Comprehensive site selection also ensures that there are ample resources for data center operations, such as utility power, water, and communication lines.
- **Physical access control:** Huawei Cloud enforces stringent data center access control for both personnel and equipment. Security guards are stationed round the clock at every entrance to each data center campus, as well as at the entrance of each building on a campus. They are responsible for registering and vetting visitors, and monitoring and restricting their access within the authorized scope. Different security strategies are applied to different zones of the data center campus, ensuring optimal physical access control. Vital parts of a data center are stored in designated safes, with crypto-based electronic access control, in a warehouse. The safes can only be operated by designated personnel. Work orders must be filled out before any parts can be taken away

from the data center, and the corresponding information must be registered in a warehouse management system. As an additional step in security management, data center administrators perform regular safety checks and audit data center visitor logs. Regular safety checks are also carried out by dedicated personnel to review physical access devices and warehouse system materials.

- **Security measures:** Huawei Cloud data centers employ industry standard equipment room security technologies to monitor and eliminate potential physical hazards. CCTV monitoring is enabled 24/7 for data centers' physical perimeters, entrances, exits, hallways, elevators, and equipment rooms. CCTV is also integrated with infrared sensors and physical access control systems. Security guards regularly patrol data centers and set up online patrol systems, so that unauthorized access and other physical security incidents promptly trigger sound and light alarms.

6.1.2 Environmental Security

- **Power supply assurance:** Huawei Cloud data centers employ a multi-level protection solution to ensure 24/7 service continuity. Dual utility power supplies from different substations are used for routine power supply. Data centers are equipped with diesel generators and Uninterruptible Power Supply (UPS) apparatus, which are engaged in the event of a power outage. Voltage regulators and overvoltage protection devices are installed on data center power lines. Power supply equipment is also configured with redundancy and power lines that run in parallel, ensuring stable power supply to data center computer systems.
- **Temperature and humidity control:** Equipment rooms of Huawei Cloud data centers are fitted with high precision air conditioning and automatically adjustable centralized humidifiers to ensure that equipment components operate well within the equipment's specified temperature and humidity range. Hot and cold air channels for cabinets are properly positioned. Cold air channels are sealed to prevent isolated hot spots. The space beneath the raised floor is used as a plenum chamber to supply air to cabinets.
- **Fire control:** Huawei Cloud data centers adopt a top level of design and fireproof materials 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 systems are deployed to quickly and accurately detect and report fires. These systems are integrated into power supply, monitoring, and ventilation facilities so that the systems can be activated even when unattended, autonomously keeping potential fires under control.
- **Routine monitoring:** Power, temperature, humidity, and fire controls in all Huawei Cloud data centers are monitored through routine inspections, which allows for the timely discovery and correction of safety hazards. This in turn, ensures stable operation.
- **Water supply and drainage:** The water supply and drainage system at each Huawei Cloud data center is properly planned, ensuring that main valves function well and key personnel are aware of valve locations. This prevents water damage to information systems. Data center buildings reside on elevated ground with peripheral green drains, and each floor inside 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 in through roofs or walls. The buildings also have proper drainage.

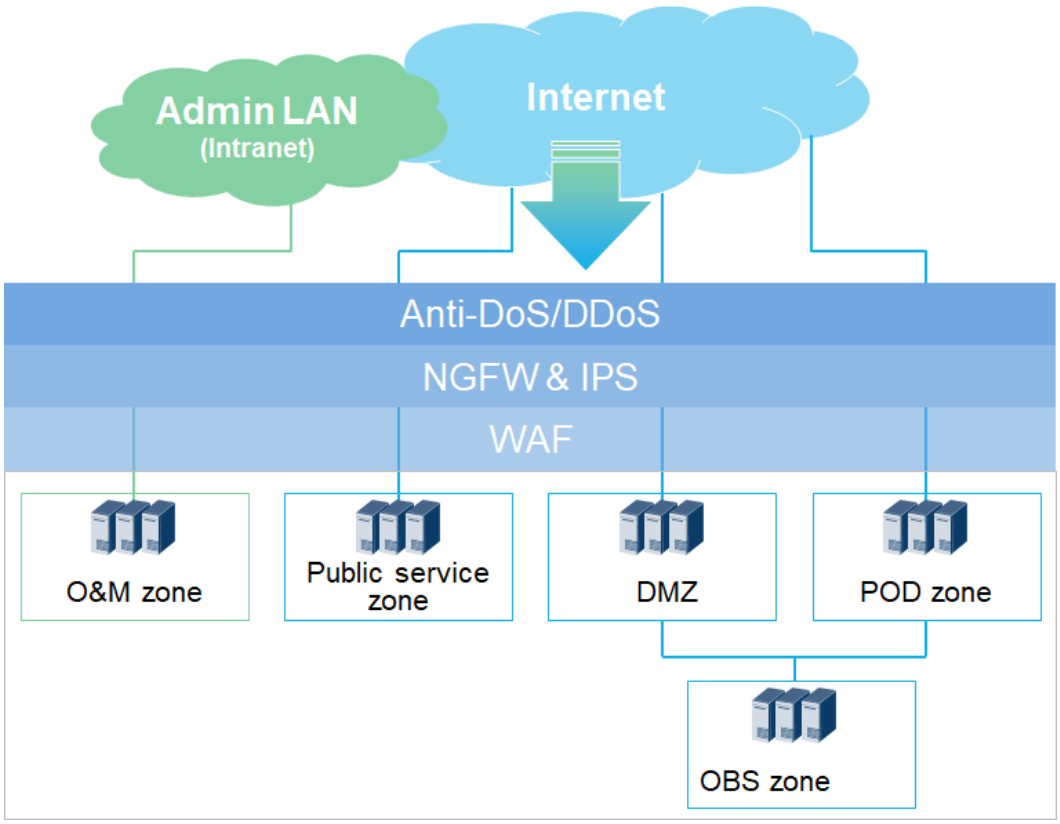
- **Electrostatic Discharge (ESD):** Huawei Cloud data centers use ESD floors in equipment rooms and use conducting wires to connect the floor support to grounding networks, discharging static electricity from equipment. Data center roofs are fitted with lightning belts, and power lines are fitted with multiple-level lighting arresters, diverting the current safely to grounding networks.

6.2 Network Security

Every Huawei Cloud data center has numerous nodes and complex functional zones. To simplify its network security design and prevent the escalation of network attacks, Huawei Cloud defines both security zones and service planes. This allows attacks to be minimized. Furthermore, a network isolation strategy is implemented 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 on the same security level. Huawei Cloud adopts multi-layer security isolation, access control, and border protection technologies for physical and logical networks on its bearer network, and performs required management and control measures to ensure security, by taking network architecture design, device selection and configuration, and O&M into consideration.

6.2.1 Security Zone Planning and Isolation

Figure 6-1 Huawei Cloud platform security zones and network border protection



Based on service functions and network security risks, Huawei Cloud divides a data center into multiple security zones for isolation purposes, using both physical and logical controls. This boosts the network's self-protection and fault tolerance[1] in response to both external and internal threats. The following describes the five key security zones:

- **Demilitarized Zone (DMZ)** mainly hosts Internet- and tenant-oriented frontend components (such as load balancers and proxy servers) and service components (such as the service console and API Gateway). Tenants' access to the DMZ is untrusted. Therefore, the DMZ must be isolated to prevent any external requests from reaching backend components of cloud services. Components in the DMZ are challenged with high security risks. Therefore, in addition to firewalls and anti-DDoS measures, the Web Application Firewall (WAF) and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) are deployed to protect the infrastructure network, platform, and applications.
- **Public service zone** primarily hosts IaaS, PaaS, and SaaS components (for example, OpenStack at the cascading layer), IaaS, PaaS, and SaaS control components, and some infrastructure service components, for example, Domain Name Service (DNS), Network Time Protocol (NTP), and patch service components. Components in the public service zone support restricted access by tenants based on business needs. Tenants must access components and services in this zone through the DMZ. Huawei Cloud administrators can access the public service zone from the intranet for operation and management purposes.
- **Point of Delivery (POD) zone** provides infrastructure resources as needed by tenants, including compute, storage, and network resources (for example, tenants' VMs, disks, and virtual networks). Resources are isolated between tenants through multi-layered security controls to prevent mutual access. In this zone, the management plane and data storage plane on the platform side are isolated from each other and also from the tenant data plane. In addition, this zone provides anti-DDoS and intrusion detection/prevention for tenant traffic to and from the Internet, safeguarding tenant services.
- **Object-Based Storage (OBS) zone** hosts OBS systems that store tenants' privacy data. Therefore, this zone is isolated. At the border of the OBS zone, tenants configure and execute desired access control rules on the security component provided by Huawei Cloud. In this way, access to the OBS zone from any tenant space does not need to pass through the DMZ. However, the security risk is high if customers access this zone from the Internet. In this case, external requests must go through the service console or application gateway in the DMZ.
- **Operations and Maintenance (O&M) zone** hosts O&M components. Huawei Cloud O&M personnel must access this zone through a VPN and then access managed nodes through a bastion host. From this zone, administrators can access O&M interfaces of all the zones. This zone does not expose its interfaces to any other zone.

In addition to the aforementioned security zoning for every Huawei Cloud data center network, distinct security levels within different security zones are also defined. Attack surfaces and security risks are determined based on different service functions. For example, security zones that are directly exposed to the Internet have the highest security risks. In contrast, the O&M zone which does not expose any interface to the Internet or other zones has the smallest attack surface. In this sense, it is easy to mitigate security risks in comparison with other zones.

NOTE

A Huawei Cloud data center, unlike a traditional IT data center, requires different mechanisms to achieve security zoning and network isolation. Deploying firewalls alone is inadequate. The adoption of innovative technologies such as Software-Defined Perimeter (SDP) is inevitable. Furthermore, trust boundaries are everywhere, and are no longer defined at the network layer only. Instead, they have moved up from the network layer to the platform layer and application layer, and even all the way up to the user identity layer, all of which require proper access control. Network layer security zoning, as covered in this section, is only part of the Huawei Cloud multi-layered full-stack protection system.

6.2.2 Service Plane Planning and Isolation

Huawei Cloud classifies its communication planes into the tenant data plane, service control plane, platform O&M plane, Baseboard Management Controller (BMC) management plane, and data storage plane based on their service functions, security risk levels, and permissions, so that services run by tenants do not affect management operations, and that devices, resources and traffic are properly monitored and managed. This ensures that network traffic for different services is reasonably and securely kept in separate planes, helping achieve a separation of duties.

- **Tenant data plane** provides service channels and functions as the communications plane between VMs, through which tenants provide service applications to users.
- **Service control plane** supports secure interaction of cloud service APIs.
- **Platform O&M plane** implements backend O&M management for infrastructure and platforms (network devices, servers, and storage devices).
- **BMC management plane** serves as the backend management plane for the hardware of cloud platform infrastructure servers, and is used for emergency maintenance.
- **Data storage plane** supports secure data transmission and storage between compute and storage nodes in the POD zone only.

In addition, different network planes are designed in each security zone according to the specific isolation requirements of the services that the security zone hosts. For example, the POD zone has the tenant data plane, platform O&M plane, service control plane, and BMC management plane, whereas the O&M zone has only the platform O&M plane and BMC management plane. The combined implementation of both security zones and service planes contributes to multi-layered and multi-dimensional network security isolation (including both physical and logical controls), which is a mere portion of Huawei Cloud's full-stack protection system.

6.2.3 Advanced Border Protection

The highly effective multi-layered full-stack protection system of Huawei Cloud also includes a number of border protection mechanisms. These include various in-house advanced border protection functions, in addition to the aforementioned security zoning and service plane planning and isolation (as implemented through conventional network technologies and firewalls). Huawei Cloud has adapted advanced protection functions to the external network border and the trust boundaries between zones on the intranet. The following describes the major advanced border protection functions[1]:

- **Scrubbing of abnormal and heavy DDoS traffic:** Huawei anti-DDoS devices are deployed at the border of each cloud data center to detect and scrub DDoS

traffic. Anti-DDoS devices also enable tenants to fine-tune the anti-DDoS service. A tenant can customize traffic threshold parameters to fit its service application types and check attack and protection status.

- **Network intrusion detection and prevention** (IDS/IPS): To detect and block attacks from the Internet as well as east-west attacks between tenants' virtual networks, Huawei Cloud deploys the IPS on network borders, including external network borders, security zone borders, and tenant space borders. The IPS provides real-time network traffic analysis and blocking capabilities to defend against intrusions such as abnormal protocol attacks, brute force attacks, port and vulnerability scanning, viruses and Trojan horses, and attacks targeting specific vulnerabilities. Based on network traffic, the IPS can also provide information needed to help locate and investigate network exceptions, assign direction-specific flow throttling policies, and apply customized detection rules accordingly. These measures protect application and infrastructure security in the production environment.
- **Web security protection:** Huawei Cloud has deployed WAFs to fend off web attacks such as DDoS attacks, Structured Query Language (SQL) injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), attacks targeting component-specific vulnerabilities, and identity theft. This protects the web application services and systems oriented for external networks and deployed in the DMZ.

NOTE

Firewall technologies play an important part towards advanced border protection and have already reached their peak maturity, hence their widespread use. For further details, see sections 7.1.1 "ECS" and 7.2.1 "VPC."

6.3 Platform Security

As the OS of Huawei Cloud, Huawei Unified Virtualization Platform (UVP) abstracts physical server resources such as CPU, memory, and Input/Output (I/O) resources, and converts them into a group of logical resources that can be centrally managed, flexibly scheduled, and dynamically allocated. Dependent on logical resources, the UVP provisions on a single physical server a number of VM execution environments, which run concurrently, however, are isolated from each other. Huawei Cloud hosts have been awarded the highest rating Five Star Plus Certification in China's Trusted Cloud Services (TRUCS) certification.

To ensure platform security, Huawei Cloud has taken a minimalist approach in building a stripped-down host OS and also performs security hardening on its services. In addition, Huawei Cloud enforces stringent Privilege Access Management (PAM) on its administrators who have host OS access, and enables comprehensive log audits for all administrator-level O&M operations. Huawei Cloud administrators must pass a two-factor authentication in order to access the management plane through bastion hosts. All operations are recorded in logs and sent to the centralized log audit system in a timely manner.

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

The UVP uses technologies such as CPU, memory, 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 guest VM OS run with different permissions, ensuring platform resource security.

The following sections describe secure resource isolation of the UVP in terms of CPU, memory, and I/O isolation.

6.3.1 CPU Isolation

CPU isolation mainly refers to the isolation between the UVP and VMs, permission allocation in VMs, and isolation between VMs. CPU isolation is implemented by switching between root and non-root modes, allocating permissions in each running mode, and allocating and switching virtual compute resources in the form of Virtual CPUs (vCPUs). Through CPU isolation, the UVP is able to control the permissions for VMs to access physical devices and virtualized running environments. Consequently, it achieves information and resource isolation between the UVP and VMs, as well as between different VMs. This prevents one VM from accessing information and resources belonging to another VM or the UVP.

6.3.2 Memory Isolation

The UVP also provides memory resources for VMs and ensures that each VM can only access its own memory. To achieve this objective, the UVP manages and enforces a 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 that have been assigned to it and cannot access the memory resources belonging to other VMs or the UVP.

6.3.3 I/O Isolation

The UVP also provides each VM with its dedicated virtual I/O devices, including disks, Network Interface Cards (NICs), mouse, and keyboard. This prevents information leakage due to I/O device sharing between VMs.

Each virtual disk corresponds to an image file or logical volume on the UVP. The UVP ensures that only one virtual disk of a VM is associated with an image file. This implements a one-to-one mapping between virtual devices used by VMs and I/O management objects on the UVP, and ensures that VMs cannot access the I/O devices of each other, thereby implementing I/O path isolation.

6.4 API Application Security

Huawei Cloud services can be configured and managed through open APIs and connected to existing IT management and audit systems. Considering the vital 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 borders of cloud services and employs multi-layered protection mechanisms and measures to safeguard APIs. Open APIs of Huawei Cloud can be invoked through the Huawei-developed API Gateway, which supports the following API protection mechanisms and scenarios:

- **Identity authentication and authorization:** Huawei Cloud integrates the IAM service to perform identity authentication on each API request. Only authenticated users are allowed to access and manage cloud monitoring information. The transmission channel uses Transport Layer Security (TLS).

  Tenants run commands through API calls to manage VMs, and permission management for these commands determines the security of VMs. API Gateway

supports two-level permission management for user commands. When a user issues a command, not only is the user authenticated and authorized through the IAM service, but also the command is inspected by API Gateway for authorization. Only if the user is authorized to run the command will this command be delivered to the platform or application layer through API Gateway. Upon receiving the command, the platform or application layer checks the user's permission again and executes the command, only after confirming that the user has the permission to execute the command.

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

- **Token-based authentication:** An authentication request contains a token. A tenant obtains a token by calling the IAM API using the registered IAM username and password.
- **AK/SK-based authentication:** An authentication request contains Access Key ID/Secret Access Key (AK/SK) authentication information. The AK/SK authentication mechanism of API Gateway requires that the client (after obtaining AK/SK information) must use the official SDK released by API Gateway to sign the request and then send the request containing the signature to API Gateway, which then validates the signature and authenticates the request.

- **Transmission protection:** API calls must use TLS to ensure confidentiality of data in transit. Currently, all open APIs supported by API Gateway use TLS 1.2 for encryption and support Perfect Forward Secrecy (PFS).
- **Border protection:** Coupled with a multi-layered advanced border protection mechanism that includes anti-DDoS, IPS, and WAF, API Gateway can effectively defend against various threats and attacks. By leveraging the load balancer to decrypt TLS traffic, the multi-layered advanced border protection mechanism monitors plaintext traffic over API Gateway and blocks attacks. Developed on an advanced border protection mechanism, API Gateway (as a security border unique to cloud services) also provides the following protection measures:
  - **API registration:** Only APIs registered with API Gateway can be accessed by tenants.
  - **Access Control List (ACL):** This function enables tenants to configure their information and network segment information. Depending on the ACL information that tenants have configured, API Gateway allows access to APIs by specified tenants or from specified network segments.
  - **Replay attack prevention:** When API Gateway receives an expired request, it rejects the request to prevent replay attacks.
  - **Brute force attack defense:** Upon receiving an AK/SK request, if API Gateway detects that the number of failed requests exceeds the maximum number allowed, it rejects the request and locks the user account for a specified period to defend against brute force attacks.
- **API request throttling:** API Gateway controls the frequency of API calls to ensure highly available and continuous API-based access. API Gateway supports the configuration of requests per second on a per-API and per-tenant basis. Request throttling information must be configured on API Gateway for each open API. API Gateway limits the number of calls per second for each API, and the number of calls per second for an API by each tenant.

6.5 Data Security

Data security refers to the comprehensive protection of users' data assets with respect to confidentiality, integrity, availability, durability, and traceability. Huawei Cloud prioritizes users' data assets, and considers data protection inherent to its security policies. Huawei Cloud will continue to embrace industry-leading standards for data security lifecycle management and adopt leading security technologies, practices, and processes across a variety of aspects, including identity authentication, permission management, access control, data isolation, transmission, storage, data deletion, and physical destruction. Ultimately, Huawei Cloud always strives toward the most practical and effective data protection in order to best safeguard tenants' privacy, ownership, and control over their data.

6.5.1 Access Isolation

- **Authentication and access control:** They are facilitated through IAM. IAM is a security management service that enables enterprise tenants to manage users and security credentials (such as AK/SK) and control users' management and cloud resource access permissions in a centralized manner.

  The IAM service allows tenant administrators to manage user accounts and control user accounts' operation permissions for resources used by the tenants. If an enterprise tenant has resources that require multi-user collaboration, the IAM service can be used to prevent users from sharing account keys and assign permissions to users based on the least privilege principle. In addition, login authentication policies, password policies, and ACLs can be configured to secure user accounts. This reduces the security risks of enterprise information regarding tenants.
- **Data isolation:** Huawei Cloud implements data isolation on the cloud through the Virtual Private Cloud (VPC), and the VPC uses network isolation technology to isolate tenants at Layer 3. Tenants can control the construction and configuration of their own virtual networks. A tenant's VPC can be connected to a traditional data center on the tenant's intranet through a VPN or Direct Connect. This allows the tenant's applications and data residing on its intranet to be seamlessly migrated to the tenant's VPC. Furthermore, the ACL and security group functions of the VPC can be used to configure security and access rules according to the tenant's specific requirements for finer-grained network isolation.

6.5.2 Transmission Security

In scenarios where data is transmitted between clients and servers and between servers on the Huawei Cloud platform through common information channels, data in transit is protected as follows:

- **VPN:** A VPN establishes a secure encrypted communication channel that complies with industry standards between the remote network and VPC, so that a tenant's existing traditional data center seamlessly extends to Huawei Cloud, while ensuring E2E data confidentiality. When a VPN channel is established between a traditional data center and a VPC, a tenant can utilize Huawei Cloud resources such as cloud servers and block storage conveniently. Applications can be migrated to the cloud and additional web servers can be enabled to increase the compute capacity on the network so as to establish a hybrid cloud architecture. This also lowers the risk of unauthorized dissemination of a tenant's core data.

Currently, Huawei Cloud encrypts data transmission channels using the hardware assisted Internet Key Exchange (IKE) and Internet Protocol Security (IPsec) VPN to ensure transmission security.

- **Application layer TLS and certificate management:** Huawei Cloud services support data transmission in Representational State Transfer (REST) or Highway mode. The REST network channel publishes services in standard RESTful mode. Standard RESTful APIs can be directly called by the HTTP client to implement data transmission. The Highway channel is a high-performance proprietary protocol channel that can be selected in scenarios with special performance requirements. The two data transmission modes support encrypted transmission using TLS 1.2 and target websites authentication based on X.509 certificates.

  The SSL Certificate Service (SCS) is jointly provided by Huawei Cloud and world-renowned Certificate Authorities (CAs). It provides tenants with fully inclusive management of X.509 certificates throughout their lifecycle to ensure trusted authentication and secure data transmission for target websites.

6.5.3 Storage Security

- **Key protection and management**

  Key Management Service (KMS) is a secure, reliable, and easy-to-use key hosting service that allows users to centrally manage keys. KMS uses the Hardware Security Module (HSM) to create and manage keys for tenants and prevents the disclosure of plaintext keys outside the HSM. This ensures no data is leaked. The HSM is a hardware device that securely produces, stores, manages, and uses keys and provides encryption services. To protect tenants' keys and mitigate the risk of key leakage, Huawei Cloud provides cloud HSMs from different vendors and with different cryptographic algorithms (such as industry standard encryption algorithms and Chinese cryptographic algorithm) and algorithm strengths. This allows tenants to select an option suitable for their real-world requirements, for example, third-party HSM certified by Federal Information Processing Standards (FIPS) 140-2. KMS implements access control of all key-related operations with logging enabled, which meets audit and compliance requirements. Currently the KMS is interconnected with the following Huawei Cloud services:

  - Elastic Volume Service (EVS)
  - Object Storage Service (OBS)
  - Cloud Backup and Recovery (CBR)
  - Image Management Service (IMS)

- **Dedicated Hardware Security Module (DHSM)**

  The DHSM meets tenants' higher compliance requirements. It is implemented for tenant services by using a hardware encryptor certified by FIPS 140-2 Level 3 or China's Office of the State Commercial Cryptography Administration (OSCCA). 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 cloud storage services, as described in the following table.

Table 6-1 Confidentiality and reliability of Huawei Cloud storage services

Storage Type	Service Description	Confidentiality	Reliability
EVS	EVS is a virtual block storage service that builds on a distributed architecture and supports elastic scalability.	The KMS provides keys. It generates, manages, and destroys Customer Master Keys (CMKs), which are used to encrypt and decrypt data. The volume encryption function is also supported.	Three data replicas are provided for redundancy, which ensures a data durability of up to 99.9999999%. CBR can be used to implement EVS backup and restoration, and supports EVS creation based on an EVS backup.
CBR	Cloud Backup and Recovery (CBR) provides easy-to-use backup services for elastic cloud servers, bare metal servers, EVS, and on-premises VMware environments. If there is a virus intrusion, accidental deletion, or software or hardware fault, data can be restored to any point when the data was backed up.	The backup data on encrypted disks is automatically encrypted for data security.	Backup data is stored across data centers, and the data durability reaches 99.999999999%.
OBS	OBS is an object-based mass storage service, which provides users with significant, low-cost, highly reliable, and secure data storage capabilities.	For server-side encryption, the OBS provides two key management modes: • **SSE-C mode**[1]**:** OBS uses the user-provided key and the key's MD5 value for server-side encryption. • **SSE-KMS mode:** The KMS provides keys. When a user uploads an object to the bucket in	The data durability is up to 99.9999999999%, and the service availability is up to 99.995%. Data consistency is checked using the hash before and after data storage to verify that the data stored is that uploaded. After data is sliced, multiple replicas are stored on different disks. Data consistency is

Storage Type	Service Description	Confidentiality	Reliability
		the zone, the OBS automatically creates a CMK for data encryption and decryption.	checked at the backend, and damaged data will be automatically repaired in a timely manner.
SFS	Scalable File Service (SFS) is a file-based storage service.	The KMS provides keys. It generates, manages, and destroys CMKs, which are used to encrypt and decrypt data.	The data durability is up to 99.9999999%, and the service availability is up to 99.95%. CBR is used to back up and restore file storage.
RDS	Relational Database Service (RDS) is an online service that builds on the cloud compute platform. It is available upon provisioning and is stable, reliable, elastically scalable, and easy to manage.	Data can be encrypted in static, tablespace, or homomorphic mode. RDS encrypts data before storing it in the database. Encryption keys are managed by KMS.	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	IMS provides flexible self-service and comprehensive image management capabilities. Users can select images from the public image repository or create private images for quick creation or batch replication of elastic cloud servers.	The KMS provides keys. It generates, manages, and destroys CMKs, which are used to encrypt and decrypt data. Huawei Cloud allows users to create an encrypted image using an encrypted elastic cloud server or an external image file.	Private images are stored in multiple replicas, achieving a data durability of up to 99.999999999%.

NOTE

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

6.5.4 Data Deletion and Destruction

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

- **Memory clearance:** Before the cloud OS reallocates memory to users, Huawei Cloud clears (zeros out) the memory to prevent data leakage that might result from restoring data in physical memory.
- **Data leakage prevention through encryption:** Huawei Cloud advises tenants to encrypt important data that they upload to the cloud for storage. If such data needs to be deleted, tenants can directly delete related data encryption keys to prevent data from being restored to plaintext before it is permanently deleted.
- **Deletion of stored data:** When a tenant deletes stored data, both the data and the corresponding metadata are deleted from the system. The underlying storage area is reclaimed, and other data is written to prevent the deleted data from being read again. When a tenant deletes a storage resource, the corresponding metadata is immediately marked for deletion so that data in the storage resource cannot be accessed. In addition, a backend task is started to permanently delete the data and corresponding metadata in the storage resource and to reclaim the physical space of the storage resource. The physical space is reallocated only after it is cleared. Before data is written for the first time into the physical space allocated to a new storage resource, the system returns only zero for all read requests. If data is deleted by mistake, tenants can use the recycle bin function of the EVS and versioning function of the OBS 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. This prevents malicious tenants from using data restoration software to retrieve data deleted from the disk, thereby avoiding information leakage.
- **Physical disk scraping:** When a physical disk needs to be scrapped, Huawei Cloud degausses or physically destroys the storage medium to clear data and keeps a record of the operation. This meets industry standards and prevents unauthorized access to user privacy and data.

7 Tenant Services and Security

Huawei Cloud offers tenants a range of cloud services, such as IaaS, SaaS, and PaaS. This chapter describes important services that help tenants move to the cloud, protect their security, and create value for their own services. The following categories of cloud services are included: compute, network, storage, database, data analysis, application, management, and security. The basic technical features, security functions, and benefits to tenant security are introduced for each cloud service. Common security services are not described in this chapter. For details about such services, visit http://www.huaweicloud.com/.

7.1 Compute

7.1.1 ECS

Elastic Compute Service (ECS) delivers self-service virtual compute resources that tenants can subscribe to on demand. Its cloud server instances, each of which is a VM, are virtual computing environments that include basic server components: CPUs, memory, an OS, 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 multi-layered security protection and assurance, including host OS security, VM isolation, and security groups. With its comprehensive security design covering VMs, hosts, and the networks that connect them, the service offers users a secure, reliable, flexible, and efficient application environment.

- **Host security:** Host OSs use Huawei UVP to isolate and manage CPUs, memory, and I/O resources. For details about UVP's security performance, see section 6.3 "Platform Security."
- **VM security**
  - **Image security hardening:** Huawei Cloud provides a Marketplace for images. A dedicated security team hardens public images on VM OSs, promptly fixes OS security vulnerabilities, and provides secure, updated public images for tenants through IMS. In addition, this team provides hardening and patch information as a reference for tenants when they test images, rectify faults, or perform O&M operations. When creating VMs, tenants can decide based on application running and security O&M 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, Virtual Extensible LAN (VXLAN), and ACL settings to ensure that VMs on that host are logically isolated. To physically isolate different hosts, traditional physical devices, such as switches and routers, are used. On the platform layer, CPU, memory, and I/O resources are logically isolated using UVP.
- **IP or MAC address anti-spoofing:** To prevent network disorder caused by tenant-instigated VM IP or MAC address changes, DHCP snooping is used to bind an IP address and a MAC address. IP Source Guard (IPSG) and Dynamic ARP Inspection (DAI) are used to filter out packets from addresses that are not bound, preventing VM IP and MAC address spoofing.
- **Security group:** UVP provides security groups to isolate VMs. Tenants can create a security group 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 communicate with each other but any two VMs in different security groups cannot. However, communication between two VMs in different security groups can be customized. For details about security groups, see section 7.2.1 "VPC."

- **Remote access authentication:** Tenants can use Secure Shell (SSH) to remotely access VM OSs for maintenance. Nevertheless, leaving the SSH port open is a relatively high security risk. For security purposes, tenants can enable remote access authentication using a key pair (public and private keys) or a username and password. It is recommended that key pair authentication be used because it is more secure.
- **Resource management authentication:** Tenants use APIs to manage Huawei Cloud ECS resources. After calling an API, tenants must be authenticated and authorized by IAM before they can use the API.
- **VNC security:** Tenants remotely access VMs in Virtual Network Computing (VNC) mode, use accounts and passwords for authentication, and use TLS 1.2 to ensure data transmission security.

7.1.2 IMS

An image is a template that contains software and necessary configurations for an elastic cloud server or bare metal server. Each image contains at least an OS and may also contain preinstalled application software, such as database software. Huawei Cloud classifies images into public, private, shared, and Marketplace images:

- Public images are standard OS images provided by Huawei Cloud.
- 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 other users to use.
- Marketplace images are high-quality third-party images that provide preinstalled OSs, application environments, and various software.

Image Management Service (IMS) provides simple and convenient self-service management functions for images, enabling tenants to manage their images through the IMS console or API. Huawei Cloud periodically provides users with public images that have security patches installed, as well as relevant security hardening and patch information as a reference for users during O&M activities, such as deployment, testing, and troubleshooting. Users can directly use a public image, create a private

image through an existing elastic cloud server or an external image file, or participate in the development and maintenance of a shared image. They can apply for an elastic cloud server by using any of these images.

IMS uses IAM for authentication, and can encrypt images in transit or at rest and check image integrity. All IMS data is stored in an image repository on a trusted subnet, and public and private images are stored in different buckets using OBS. IMS comes with secure cryptographic algorithms and functions that allow users to encrypt images for storage. When a VM is created using an image, the integrity of the image is verified automatically.

IMS checks tenants' permissions of all operations and allows only operations with required permissions. It also keeps audit logs of all key operations. Audit logs are retained indefinitely so that tenants can accurately trace historical operations.

7.1.3 AS

Auto-Scaling (AS) automatically adjusts resources in accordance with predefined policies to meet tenants' service requirements. AS ensures that required service resources are available without manual intervention, scaling application systems in and out as service use fluctuates. This helps tenants reduce resource and labor costs and ensures that their services operate in a stable and healthy manner. By automating resource allocation and policy enforcement, AS helps avoid the impact of resource exhaustion-type attacks as well as security risks resulting from human errors during resource allocation by tenants' management personnel.

AS can automatically add instances to a load balancer listener, which distributes access traffic to all instances in an AS group. This offers a higher level of protection against DDoS attacks than that offered by direct access to single backend servers and services. AS can detect instance status in real time and launch new instances to replace those that are not operating properly. Multiple AZs can be configured and instances can be evenly distributed among the AZs to ensure DR for applications deployed in the AS group, thereby improving system availability.

7.1.4 DCC

Dedicated Computing Cluster (DCC) is a physically isolated cloud computing resource pool based on Huawei Cloud ECS. It inherits all functions and security features of ECS.

DCC has the advantage of host isolation at the physical layer because each compute resource pool is leased by only a single tenant and is physically isolated from other tenants' resources and the VPC network. This eliminates the potential impact on resources and prevents mutual network access.

7.1.5 DeH

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

DeH has the advantage of host isolation at the physical layer because each host is leased by only 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 the Hypervisor and attack the system.

7.1.6 BMS

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

Like ECS, BMS also provides multi-layered protection, including host OS and network security, remote access authentication, and management and control security. For details, see section 7.1.1 "ECS." More importantly, BMS has the security advantage of physical machine isolation. With its comprehensive security design covering hosts and networks, BMS ensures tenant security and offers a secure, reliable, flexible, and efficient application environment running on an independent physical computing environment.

7.2 Network

7.2.1 VPC

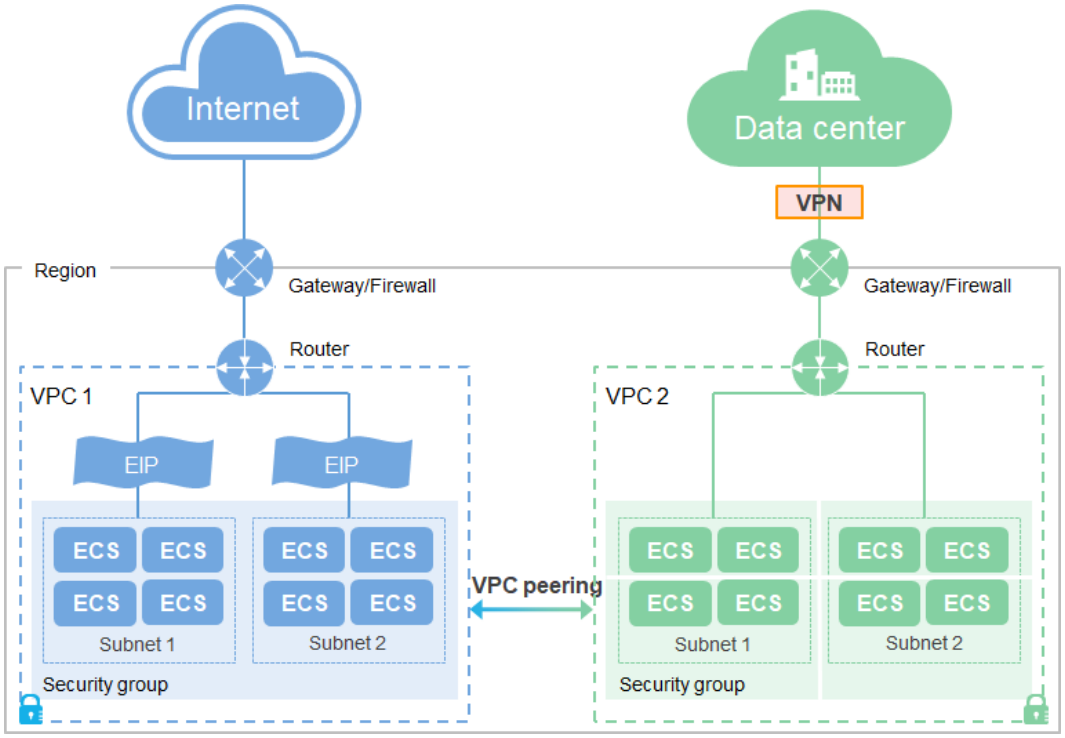
Virtual Private Cloud (VPC) creates an isolated, virtual network environment that users can configure and manage on their own for elastic cloud servers. This enhances the security of user resources on the cloud and makes network deployment easier.

The advantages of VPC are as follows:

- Users can create their own virtual networks and have complete control over them.
- Users can apply for elastic IP addresses[1] in VPC 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 security.

The following figure shows the basic architecture of VPC.

Figure 7-1 Huawei Cloud VPC architecture



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

- **Subnets** facilitate network plane management of elastic cloud servers, as well as IP address management and DNS. By default, the elastic cloud servers on all subnets within a VPC can communicate with each other, but servers in different VPCs cannot.
- A **VPN** establishes an encrypted tunnel between a remote user and a VPC, thereby enabling the remote user to use service resources in the VPC. Elastic cloud servers deployed in VPCs cannot communicate with tenants' data centers or private networks by default, but tenants can configure and enable VPN to permit such communication if required.

VPC provides network security functions on different Open System Interconnection (OSI) layers. Tenants can configure these functions as needed based on their network security requirements. Among these functions, network ACLs and security groups are the most important security functions both for Huawei Cloud as a whole and for the VPCs 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 elastic cloud servers that have the same security requirements and are mutually trusted in a VPC. To enhance access security, users can place elastic cloud servers in different security groups and create access rules for communication of elastic cloud servers within and between security groups.

One set of access rules can be configured per security group. These rules cover protocols, direction (inbound or outbound), source IP address segment/subnet or security group, and port numbers that can be used to access servers. The protocols supported are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

VMs added to a security group are protected by access rules configured for the security group. Users can specify a security group during VM creation for VM security isolation and access control. Each security group can contain VMs that are deployed on different physical servers. By default, VMs in the same security group can communicate with each other but any two VMs in different security groups cannot. However, communication between two VMs in different security groups can be customized.

Upon the creation of security groups, the default access rules are used by security groups that are not configured with any access rules. The default rules permit all outbound packets and allow elastic cloud servers in the same security group to access each other. Custom rules need to be configured only if the default rules are insufficient.

Both the network ACL and security group functions are adopted to improve the network security of Huawei Cloud VPC. Understanding the differences between them is important for creating effective network security policies for VPCs. The following table summarizes the differences.

Table 7-1 Differences between network ACLs and security groups

Network ACLs	Security Groups
Operations at the subnet level (second line of defense).	Operations at the elastic cloud server instance level (first line of defense).
Support for permit and deny policies.	Support for permit policies.
If rules conflict with each other, the rule with the smallest index value takes precedence over others.	If rules conflict with each other, only the common parts take effect.
Not available during subnet creation. To apply a network ACL to the associated subnets and the elastic cloud server instances on the subnets, create a network ACL, associate it with subnets, add inbound and outbound rules, and enable the ACL.	Mandatory by default when an elastic cloud server instance is created. The default security group applies automatically on elastic cloud server instances.
Support for packet filtering by 5-tuple (protocol, source port, destination port, source IP address, and destination IP address).	Support for packet filtering by 3-tuple (protocol, port, and destination IP address).

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

- **VLAN isolation:** A VLAN, which works on OSI Layer 2, uses virtual bridges that support VLAN tagging to implement virtual switching and ensure secure isolation between VMs.
- **IP and MAC address binding:** This function prevents IP or MAC address spoofing initiated by changing the IP or MAC address of a VM NIC, and therefore enhances VM network security. Specifically, DHCP snooping is used to bind an IP address and a MAC address. IPSG and DAI are used to filter out packets from addresses that are not bound.
- **DHCP server isolation:** DHCP servers are disabled on VMs to prevent unintentional and malicious operations on the DHCP servers, thereby ensuring VM IP address allocation.
- **Anti-DoS/DDoS:** The number of tracked connections to virtual ports is restricted to prevent large-scale attacks[2] from inside or outside the cloud platform.

NOTE

- An Elastic IP (EIP) address is a static, public IP address. You can bind an EIP to an elastic cloud server on your subnet to enable the elastic cloud server in your VPC to communicate with the Internet through a fixed public IP address. Unbinding is also supported.
- Large-scale attacks interrupt service and management traffic by generating a large number of connection tracking entries. Excessive entries, if not limited, will exhaust connection tracking table resources and prevent new connection requests from being accepted.

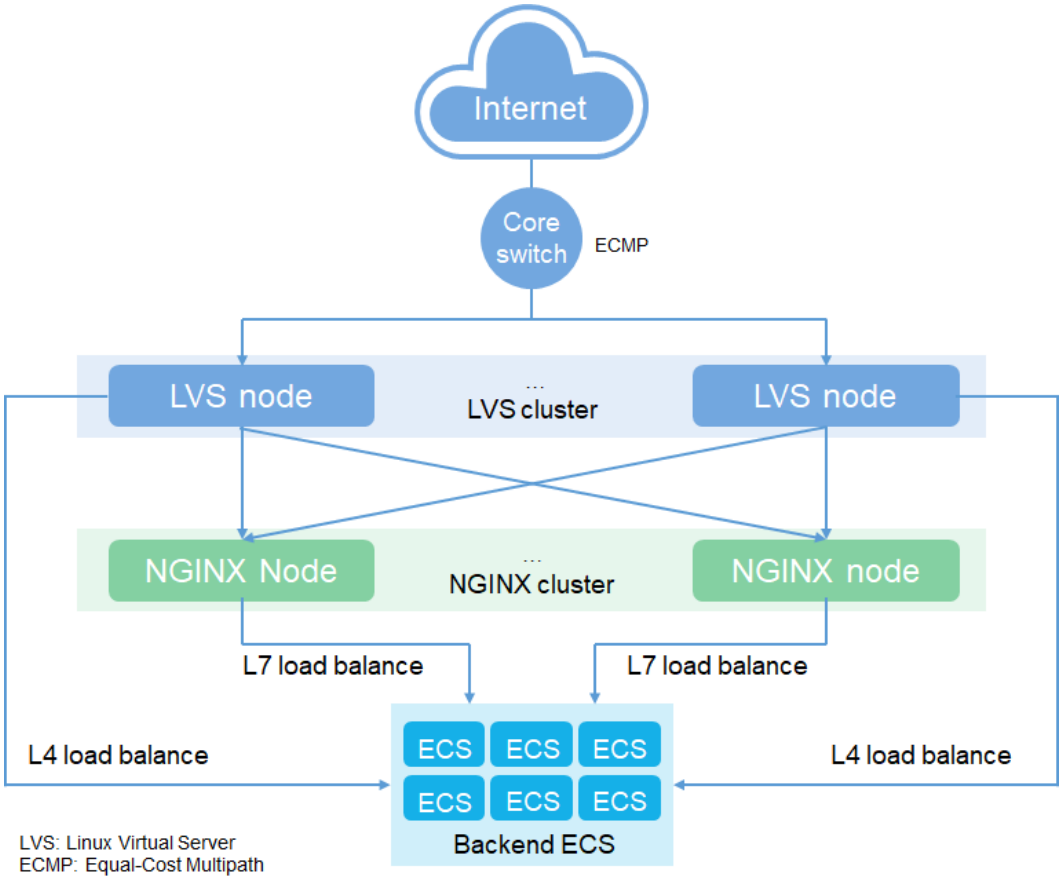
7.2.2 ELB

Elastic Load Balance (ELB) automatically distributes access traffic among multiple elastic cloud servers and enables application systems to provide services, enhancing system fault tolerance. ELB has the following advantages over traditional hardware load balancers:

- ELB ensures service availability with its redundancy 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 capabilities as required by application traffic.
- Up to 100 million concurrent connections are supported. Load balancing can be performed on Layer 4 (over TCP or UDP) or Layer 7 (over HTTP or HTTPS).

The following figure shows the ELB networking diagram.

Figure 7-2 Huawei Cloud ELB networking diagram



ELB provides the following security functions:

- **Server IP address and port masking:** ELB exposes only one IP address and the corresponding service port and does not expose backend IP addresses and ports. This prevents network information leakage and reduces the attack surface.
- **Automatic scaling based on traffic status:** ELB can work with AS to provide more flexible scaling and higher anti-DDoS capabilities than the traditional method of direct access to single backend servers and services.
- **ELB security groups on intranets:** 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 specified traffic is sent and received through ELB.
- **Source IP address transparency:** ELB can pass source IP addresses to servers when routing HTTP and HTTPS requests. This enables tenants to perform source tracing, collect connection or traffic statistics, trustlist source IP addresses, and perform other tasks needed to meet enhanced security requirements, helping detect and respond to attacks more quickly.
- **SSL/TLS offloading and certificate management:** ELB takes over the tenant's backend server to encrypt and decrypt the SSL/TLS packets, reducing the server's processing burden. In this process, ELB decrypts the inbound traffic before delivering it to the tenant's backend server; likewise, it encrypts outbound

traffic before sending it to the destination. To use SSL/TLS offloading, tenants must upload the SSL/TLS certificates and private keys to ELB for management.

- **Support for encryption protocols and cipher suites:** Tenants communicating with ELB over HTTPS can select an encryption protocol and related configurations as required. TLS 1.2 is used by default. For tenants who have more encryption algorithm options, ELB provides extended cipher suites. For tenants with high security requirements, ELB also provides strict encryption algorithms.

7.2.3 DNS

Domain Name Service (DNS) is a highly available and scalable authoritative domain name resolution service that provides domain name management. It translates common domain names or application resources into IP addresses used for computer connections.

DNS can resolve domain names into ECS, OBS, RDS, and other service addresses for ease of access to different service resources. It provides intranet users custom domain name resolution services based on VPCs. By addressing the challenge of registering and managing domain names for tenants' internal services, DNS reduces the complexity of service deployment and maintenance while also facilitating high-availability design. DNS is built on Huawei Cloud's highly available and reliable infrastructure. The distributed nature of DNS servers helps improve service availability and ensures that end users are routed to target applications. To ensure failovers between nodes for service availability, tenants can modify DNS records.

DNS mainly provides the following security functions:

- Reverse lookup records (IP address to domain name) can be used to reduce spam emails.
- Regular updates, shortened Time to Live (TTL), and frequent cleaning are typical methods to protect the DNS cache from viruses and attacks.
- DNS provides anti-DDoS to ensure stable and secure services by performing behavioral profiling on inbound traffic, scrubbing attack traffic, limiting access traffic, and blocking access from malicious IP addresses. The seven-layer protection algorithm provided by DNS scrubs and filters traffic layer by layer, offering comprehensive protection against network- and application-layer attacks. For example, the anti-DDoS function blocks DNS amplification attacks.
- DNS allows clients to use HTTP/HTTPS APIs to bypass traditional local DNS servers for domain name resolution. This effectively prevents hijacking of domain name resolution results.

Tenants can use IAM to assign DNS service and operation permissions to their members. With the AK/SK, Huawei Cloud resources can be accessed through APIs.

7.2.4 NAT Gateway

A Network Address Translation (NAT) gateway provides network address translation for compute instances in a VPC. It enables multiple compute instances to share an EIP for network access through IP address mapping or port mapping. NAT gateways are classified into public and private NAT gateways.

A public NAT gateway translates private IP addresses into public IP addresses. This enables cloud resources to securely access the public network or provide services

externally. It also prevents direct exposure of private network information to the public network.

A private NAT gateway provides private address translation for cloud hosts (elastic cloud servers and bare metal servers) in a VPC. Users can configure Source Network Address Translation (SNAT) and Destination Network Address Translation (DNAT) rules to translate the source and destination IP addresses into transit IP addresses, so that cloud hosts in the VPC can communicate with other VPCs or Internet Data Centers (IDCs).

The NAT gateway has the following advantages:

- Flexible deployment: A NAT gateway can be deployed across subnets and AZs. The fault of a NAT gateway in a single AZ does not affect the NAT gateway's service continuity. The type and EIP of a NAT gateway can be adjusted at any time.
- Diversity and ease of use: Multiple types of NAT gateways can be flexibly selected. Only simple configuration is necessary to ensure NAT gateways run stably, and O&M is also simple.
- Lower cost: Multiple cloud hosts share an EIP. When users send data through a private IP address or provide services accessible from the Internet using a NAT gateway, the NAT gateway translates the private IP address into a public IP address. In this case, users do not need to purchase additional EIPs or bandwidth resources, effectively reducing costs.

The NAT gateway provides the following security functions:

- **Server IP address and port masking:** NAT allows multiple hosts to share an EIP, and the real addresses and service ports used by backend servers are not exposed. This prevents EIP exposure and network information leakage and reduces the attack surface.
- **Anti-DoS/DDoS:** The system uses QoS rate limiting to prevent large-scale DoS/DDoS attacks from inside or outside the cloud platform.

7.2.5 Direct Connect

Direct Connect allows tenants to establish stable, high-speed, low-latency, secure dedicated network connections between their local data center and a VPC on Huawei Cloud. It leverages Huawei Cloud services and existing IT facilities to build a flexible, scalable hybrid cloud computing environment.

These connections can be used to interconnect Huawei Cloud with tenants' data centers, offices, and hosting centers with lower latency. Compared with a public Internet connection, Direct Connect offers a faster, more secure network experience for tenants.

Direct Connect has the following advantages:

- With Direct Connect, a dedicated channel that is isolated from other networks is used for communication, ensuring high security.
- A dedicated network is used for data transmission, achieving high network performance, low latency, and better user experience.
- A Direct Connect connection supports up to 100 Gbit/s bandwidth.
- By connecting local data centers to resources on the cloud, users can gain access to huge cloud resources on a flexible, scalable hybrid cloud.

DC mainly provides the following security functions:

- **Network isolation:** Direct Connect connects to Huawei Cloud VPCs through physical private lines that are exclusively used by tenants, thereby implementing network isolation.
- **Encrypted transmission:** Direct Connect establishes a TLS channel between the client and server, reducing data leakage risks.

7.2.6 VPCEP

VPC Endpoint (VPCEP) connects a VPC to endpoint services (including cloud services and users' private services), enabling cloud resources in the VPC to access the VPCEP service without needing an EIP. This improves access efficiency and provides a flexible and secure networking mode. VPCEP has the following advantages:

- Excellent performance: Each gateway node provides millions of sessions to meet the requirements of various application scenarios.
- Ready for use upon creation: VPCEP can be created in seconds and takes effect promptly.
- Flexible usage: VPCEP enables direct access to the intranet without having to use EIPs.
- High security: Users can access the VPCEP service over an endpoint without exposing server information, thereby avoiding unknown risks.

VPCEP provides the following security functions:

- **Access control:** Each user can control their access permissions through VPCEP. Only specified users can access their services.
- **Connection configuration:** Users can determine whether to accept connection requests from other services, manage the connection status, and reduce the possibility of attacks through trustlists.
- **No need to use EIP:** VPCEPs establish connections through private channels without using EIPs. This avoids the risk of scanning attacks on EIPs, reducing the attack surface.

7.2.7 VPN

Virtual Private Network (VPN) provides convenient, flexible, and provision-and-play IPsec connections between users' local data centers and Huawei Cloud VPCs, helping build a flexible and scalable hybrid cloud computing environment.

A VPN establishes an encrypted, Internet communications tunnel between a remote user and a VPC. By default, elastic cloud servers on a VPC cannot communicate with the user's data center or private network. The VPN function can be enabled so that they can communicate.

A VPN consists of a VPN gateway and one or more VPN connections. A VPN gateway provides an Internet egress for a VPC and works together with the remote gateway in a local data center. A VPN connection encrypts the communications line between the VPN gateway and the remote gateway and enables communication between the local data center and VPC, quickly establishing a secure hybrid cloud environment.

VPN provides the following security functions:

- **Secure tunnel:** A VPN connects a VPC to the local network through an encrypted connection, which routes data between the VPC and local network to protect the confidentiality and integrity of data in transit.
- **Infrastructure security:** Dedicated Huawei devices encrypt data in transit using IKE and IPsec and provide carrier-class reliability to ensure the stable running of VPN services from the hardware, software, and link perspectives.

7.3 Container

7.3.1 CCE

Cloud Container Engine (CCE) provides highly scalable, high-performance, enterprise-class Kubernetes clusters and supports Docker containers. It enables tenants to easily deploy, manage, and scale containerized applications on Huawei Cloud. After purchasing a Kubernetes cluster through CCE, a tenant obtains a managed Kubernetes controller node and several on-demand worker nodes. The controller node is hardened in accordance with the baseline during creation, and VMs (functioning as worker nodes) are added to the cluster. The tenant has administrator permissions and can perform service operations and security configurations as required.

CCE provides systematic cloud-native security capabilities. At the infrastructure level, it inherits security capabilities provided by Huawei Cloud and ECS. At the cluster level, it supports fine-grained permission management, quota management, network isolation, sensitive information protection, and various security mechanisms offered by the Kubernetes community. And at the container level, CCE supports Kata containers, and together with Container Guard Service (CGS), it provides high-level runtime detection capabilities such as container escape detection. In terms of cloud-native application development and image management, CCE has released a raft of best security practices on the Huawei Cloud website, and in conjunction with SoftWare Repository for Container (SWR), it also supports image vulnerability scanning and container image signature. Leveraging the Kubernetes extension mechanism, tenants can build and manage more security plug-ins based on the Huawei Cloud CCE template.

- **Fine-grained permission management:** CCE provides fine-grained permission management based on Huawei Cloud IAM and Kubernetes Role-Based Access Control (RBAC), enabling IAM-based permission control, IAM token-based authentication, and cluster- and namespace-level authorization for user groups or users.
- **Quota management:** A total resource quota can be set for Kubernetes resources in namespaces in a cluster, and resource quotas can also be set for specific containers in a namespace.
- **Network isolation:** When a cluster is created, CCE creates a VPC security group for controller and worker nodes by default, and tenants can harden security based on service requirements. In addition, CCE supports the configuration of network policies (container tunnel network) and container security group policies (on the cloud-native 2.0 network) for mutual access traffic between application containers on worker nodes. This is equivalent to building a container network firewall at the application layer.
- **Sensitive information protection:** Sensitive information can be stored in secret resources in a cluster. CCE encrypts this information when flushing data to

disks. To decouple sensitive configuration information from service data in a cluster, tenants can host sensitive configuration information using Cloud Secret Management Service (CSMS). CCE allows tenants to mount CSMS credentials to containers, and also allows them to mount external storage volumes encrypted using KMS, including file storage and object storage.

- **Secure container:** Compared with common containers, each secure container runs on an independent micro-VM, has an independent OS kernel, and is securely isolated at the virtualization layer. If application containers in a cluster require strong security isolation, secure containers are recommended.
- **Cloud-native application deployment security:** Tenants can use SecurityContext, PodSecurityPolicy, AdmissionWebhook, and other mechanisms to set container startup and running policies. In this way, CCE can prevent containers from running in privileged mode or obtaining unnecessary permissions during running.
- **Runtime detection:** For details, see section 7.10.4 "CGS."

7.3.2 SWR

SoftWare Repository for Container (SWR) provides easy-to-use, secure, and reliable management of container images throughout their lifecycle, facilitating the deployment of containerized services. SWR allows tenants to securely host and efficiently distribute images on the cloud without building or maintaining image repositories. In addition, it can be used together with CCE and Cloud Container Instance (CCI) for smooth migration of containers to the cloud.

SWR uses Huawei Cloud IAM for authentication and grants image access permissions to users by organization, implementing security isolation between tenants and between users within a tenant. HTTPS is used to upload and download container images, image integrity is checked in accordance with Open Container Initiative (OCI) specifications on the repository, and images are hosted in the OBS repository on a trusted subnet, ensuring security and reliability. In addition to repository security capabilities, SWR integrates with CGS to provide image security scanning.

- **Image security scanning:** Tenants can scan uploaded images with one click to identify vulnerabilities in the images, and obtain remediation suggestions. This helps users obtain secure images.

7.4 Storage

7.4.1 EVS

Elastic Volume Service (EVS) offers highly reliable, high-performance, scalable block device services with varying specifications for cloud servers. It is ideal for scenarios such as distributed file systems, development/testing, data warehouses, and High-Performance Computing (HPC). EVS is built based on underlying distributed block storage devices. Tenants can create EVS disks each up to 32 TB in size and mount them to ECS, BMS, CCI, and other instances as block devices.

- **Resource management authentication:** EVS uses Huawei Cloud IAM for authentication. It checks the permissions of tenants before they perform any operations and allows only authorized operations. By doing so, EVS denies other tenants and unauthorized users from accessing EVS disks. EVS logs all

critical operations for auditing by interconnecting with CTS so that tenants can accurately trace operations.

- **Data reliability and durability:** EVS provides highly reliable block storage. With redundant node design and highly reliable networks connecting service nodes, it offers an availability of 99.95%, meeting the requirements of block storage services. As a standard service without additional charge, EVS stores data replicas in multiple physical locations using the multi-replica data redundancy mechanism. In addition, EVS uses the synchronous write and read mechanism for replicas to ensure data consistency. This mechanism enables EVS to automatically rectify hardware faults at the backend and quickly rebuild data, providing a data durability of up to 99.9999999%. EVS data is redundantly stored in the same AZ instead of across multiple AZs. Therefore, tenants are advised to periodically back up EVS disks to ensure long-term data durability.
- **Storage encryption:** EVS provides a secure encryption algorithm (AES-256) and secure encryption functions. It allows users to choose encrypted storage of EVS data and select a CMK, which is managed by Data Encryption Workshop (DEW). EVS encrypts data written to EVS disks by a user application, and decrypts and provides it to the user application when requested.
- **Data deletion:** When a tenant deletes an EVS disk, the underlying distributed block storage devices immediately delete the metadata tag of the EVS disk to ensure that data cannot be accessed. In addition, a backend task is started to permanently delete the metadata and corresponding data blocks and to reclaim the physical space of the EVS disk. The physical space is reallocated only after it is cleared. Before data is written for the first time into the physical space allocated to a new EVS disk, the system returns only zero for all read requests.
- **Note:** EVS disks behave like raw, unformatted block devices which have block device names and interfaces. Tenants can create a file system on top of the EVS disks, or use them in any way tenants would use block devices (such as hard disks). When a tenant deletes files from the file system, the file system usually deletes only file indexes, meaning that the EVS disk still contains the data. As such, when creating a backup or image of the EVS disk and sharing it with other tenants, a tenant should exercise caution. If sensitive data is stored in the EVS disk or files have been deleted from the EVS disk, the tenant should create another EVS disk, copy the files to be shared, and then create a backup or image and share it with other tenants.

7.4.2 SFS

Scalable File Service (SFS) is a network-attached storage (NAS) service that provides scalable, high-performance file storage. With SFS, shared access can be achieved among multiple elastic cloud servers, bare metal servers, and containers created on CCE and CCI. SFS Capacity-Oriented provides up to petabytes of shared file storage hosted on the cloud. It features high availability and durability and supports data- and bandwidth-intensive applications. SFS Capacity-Oriented is suitable for multiple scenarios, including HPC, media processing, file sharing, content management, and web services. SFS Turbo is expandable to 320 TB and provides shared file storage hosted on the cloud. It features high availability and durability, and supports massive quantities of small files, as well as applications requiring low latency and high Input/Output Operations per Second (IOPS). SFS Turbo is mainly suitable for high-performance websites, log storage, compression and decompression, DevOps, enterprise offices, and containerized applications.

- **Resource management authentication:** SFS uses Huawei Cloud IAM for authentication. It checks the permissions of tenants before they perform any operations and allows only authorized operations. By doing so, SFS denies other tenants and unauthorized users from accessing file storage. SFS logs all critical operations for auditing by interconnecting with CTS so that tenants can accurately trace operations.
- **Data reliability and durability:** SFS provides highly reliable file storage. With redundant node design and highly reliable networks connecting service nodes, it offers an availability of 99.95%, meeting the requirements of file storage. Tenants are advised to periodically back up SFS data for long-term data durability, which reaches up to 99.9999999%.
- **Network isolation:** To control the range of IP addresses that can access file storage, tenants can configure VPC network segments. SFS Turbo instances run in an independent VPC. In a VPC, tenants can create a subnet that spans multiple AZs. This subnet can be selected for creating an SFS Turbo instance as required by services, and tenants will be allocated an IP address on the subnet for access to the file storage. After an SFS Turbo instance is deployed in a VPC, the tenant can use VPC peering to enable other VPCs to access this VPC. The tenant can also create an elastic cloud server in the VPC and connect the server to the file storage using a private IP address. Subnets and security groups can be configured in combination to isolate SFS Turbo instances and thereby enhance instance security.
- **Access control:** When creating an SFS Turbo instance, tenants can select a security group and deploy service-plane NICs of the instance in it. A VPC allows tenants to configure inbound and outbound rules for security groups hosting the SFS Turbo instances, thereby controlling the range of IP addresses that can connect to databases. File storage security groups allow only file storage listening ports to be connected. Tenants do not need to reboot SFS Turbo instances when configuring security groups.
- **Storage encryption:** SFS Capacity-Oriented and SFS Turbo both allow users to choose encrypted storage of data in the file system and select a CMK, which is managed by DEW. SFS encrypts data written to the file storage by a user application, and decrypts and provides it to the user application when requested.
- **Data deletion:** When a tenant deletes an SFS instance, data stored in the instance is automatically deleted, and cannot be viewed or restored.

7.4.3 CBR

Cloud Backup and Recovery (CBR) provides backup protection services for EVS disks, elastic cloud servers, and bare metal servers (EVS disks will be referred to as disks, and elastic cloud servers and bare metal servers will be referred to as servers in subsequent text). It also supports snapshot-based backup services, and can use backup data to restore data on servers and disks. In addition, CBR can synchronize backup data in the offline backup software BCManager, manage backup data on the cloud, and restore backup data to other servers on the cloud.

CBR adopts a microservice architecture, based on which it abstracts and models services. It decouples service data and service logic, platform capabilities and product capabilities, and 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 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 HTTPS RESTful APIs to protect access channels, uses NTP to ensure time consistency among NEs in the system, and hardens the OS, database, and web application configurations to ensure system security.

CBR supports integrity check of backup data. During backup and restoration, CBR uses CRC32C to verify that backup data is not damaged or tampered with. CBR also supports the backup and restoration of encrypted volumes. After obtaining keys through Huawei Cloud KMS, CBR 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, protecting user data security to the maximum extent.

7.4.4 OBS

Object Storage Service (OBS) provides tenants with massive, secure, reliable, and cost-effective data storage capabilities, such as bucket creation, modification, and deletion as well as object upload, download, and deletion. It can store any type of file and is suitable for websites, enterprises, developers, and common users. As an Internet-oriented service, OBS provides web service interfaces over HTTPS. This enables users to access and manage data stored in OBS anytime and anywhere by using OBS Console or OBS Browser+ on any computer with an Internet connection.

OBS offers a range of access controls — including bucket ACLs, bucket policies, and identity authentication — to restrict access permissions requested by tenants. To keep data storage and access secure, OBS also adopts a series of security measures, such as using access logs for auditing, Cross-Origin Resource Sharing (CORS) for restricting access sources and request types, URL validation to ensure that URLs are from trusted sources, and server-side encryption for keeping data secure.

- **Access control:** Access requests sent to OBS can be controlled using ACLs, bucket policies, and signature verification.
  - **ACL:** OBS access permissions can be granted to specified accounts by using an ACL, which restricts access (including read-only, write, and full control access) of all users or a specific user to a single bucket or object. Users can also configure other access policies, for example, setting a public access policy for an object to assign all users the read-only permission. By default, objects in a bucket can be accessed only by the creator of the bucket.
  - **Bucket policy:** A bucket owner can configure a bucket policy to control access to the bucket. Bucket policies control access to buckets and objects in a centralized fashion based on various conditions: OBS operation, applicant, resource, and other request elements (such as IP address). The permissions attached to a bucket apply to all objects in that bucket. A bucket policy can grant permissions on a per-bucket or per-user basis.

    Unlike ACLs, which can grant permissions only for single objects, bucket policies can allow or deny permissions for all objects in a bucket. Permissions can be configured for any number of objects in a bucket with a single request. Multiple objects can be specified by using wildcard characters in resource names and other fields (similar to regular expression operators), enabling access control for a group of objects.

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

- **User signature verification:** An account must use a pair of access keys (AK/SK) when accessing OBS. OBS uses AKs and SKs for IAM authentication and authorization to ensure that only authorized accounts have access to specified OBS resources. The headers of access requests sent to OBS contain authorization information generated based on the SK, request time, and request type. OBS also independently performs URL encoding on bucket and object names before generating authorization information. Only accounts that pass signature verification can access specified OBS resources.

  OBS interfaces are fully compatible with Amazon's Simple Storage Service (S3) interface. Tenants can securely and reliably migrate their data from Amazon S3, specified by an 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 an availability of 99.995%, meeting the requirements of object storage services. In addition, by using automated restoration technology that provides data redundancy and ensures consistency, OBS offers a data durability of up to 99.9999999999%.

  OBS can retain multiple versions of an object so that users can conveniently retrieve or restore previous versions and quickly restore data in the event of an accidental operation or application failure. Versioning enables users to recover objects that were unintentionally deleted or overwritten. By default, versioning is disabled for new OBS buckets. As such, a new object uploaded to a bucket that contains another object with the same name will overwrite the existing object.

- **Access log:** OBS logs bucket access requests for analysis and audit. These access logs allow a bucket owner to comprehensively analyze the nature and type of the access requests and identify trends. After log management is enabled for a bucket, OBS automatically logs access requests to this bucket, generates a log file, and writes it to a specified bucket (target bucket). Log management is disabled by default, because storing access logs consumes tenants' OBS space and may cause additional storage fees. Tenants can enable this function for analysis or audit purposes.

- **CORS:** OBS supports CORS that allows cross-origin requests to access resources in OBS. CORS, a World Wide Web Consortium (W3C) standard for web browsers, defines how client web applications in one origin interact with resources in another origin. This enables static websites hosted on OBS to respond to requests from websites in another origin, provided that CORS is configured properly in the target bucket. Website scripts and content can then interact across origins even when a Same Origin Policy (SOP) is in place.

- **URL validation:** To prevent URL spoofing, OBS supports URL validation based on the referer in HTTP headers, as well as access trustlists and blocklists. The source website page from which a user is linked to a destination web page can be determined. Requests that originate from an external website can then be denied or redirected to a specified web page. URL validation also checks requests against the blocklist or trustlist. Access is granted if the trustlist is matched, and denied or redirected to a specified web page if the blocklist is matched.

- **Server-side encryption:** Objects uploaded for storage are encrypted by the server, which also decrypts those objects when tenants download them. Keys managed by KMS (SSE-KMS) and keys provided by customers (SSE-C) can both be used for server-side encryption.

- SSE-KMS: OBS uses keys provided by KMS to encrypt objects. Users must create a key on KMS (or use the default KMS key) and then select that key for server-side encryption when uploading objects.
- SSE-C: OBS uses user-provided keys and the corresponding hash values to perform encryption. The interface used to upload objects can transmit a key, which can be used by OBS for server-side encryption. OBS does not store user-provided key information; therefore, users will be unable to decrypt objects without the key.

NOTE

Compared with Amazon Signature Version 2, Amazon Signature Version 4 uses the more secure HMAC-SHA256 algorithm, includes user data in signature calculation, and allows users to specify the header field used in signature calculation, greatly improving the security of request authentication. It is therefore recommended that Amazon Signature Version 4 be used during migration.

7.4.5 DES

Data Express Service (DES) enables offline massive data transmission to Huawei Cloud using physical storage media such as External Serial Advanced Technology Attachment (eSATA) hard disks. DES helps addresses issues facing massive data transmission, such as high network costs and long transmission time.

To use DES, users log in to the management console and create service tickets. 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 recommended that users encrypt the data on hard disks before shipping. DES supports client-side encryption by a third-party encryption utility that uses the industry-standard AES-256 algorithm, and runs on Windows, Mac OS X, and Linux. This utility must be able to 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 can be accessed only with a password.

Once hard disks are received by a Huawei Cloud data center, drives are mounted on data center servers, and users are notified to start upload. Users log in to the management console, enter their AK/SK and the key that was used to encrypt the drives, and then start to upload data. After the data is uploaded, users are presented with a report of uploaded data. After they confirm the uploaded data, the Huawei Cloud data center ships the hard disks back to them. During the process, Huawei Cloud staff have no access to users' keys or data, thereby ensuring the security of data transmission.

7.5 CDN and Intelligent Edge

7.5.1 CDN

Content Delivery Network (CDN) is an intelligent virtual network built on the Internet. Node servers are deployed on the network to distribute content from origin servers to all CDN nodes and provide functions such as media content pre-ingestion, retrieval, storage, caching, segmentation, and playback, as well as caching and download of web pages and files. These functions enable users to obtain required content from nearby servers.

CDN uses security measures such as password authentication, access control, minimum authorization, session management, input validation, and encryption to safeguard the system. Specifically:

- Network device security hardening, network plane isolation, security zoning, and network access control are provided to implement network-level security.
- OS security hardening and antivirus measures are used to implement host-level security on the OS.
- Database security hardening and database security design are used to ensure database security.
- Security hardening for web containers and security design for web applications enable the service system to effectively cope with security threats.
- The security of interface protocols, sensitive data transmission, and sensitive data storage ensure the security of non-web applications.
- Security functions such as URL validation and anti-tampering are supported to ensure CDN content security
- Comprehensive communication matrix and security management documents are provided to guide security O&M personnel in deployment and implementation.

In addition, CDN is deeply integrated with Edge Security Acceleration (ESA) to provide security acceleration services with intelligent defense, effectively defending against live-network attacks.

ESA is deployed on edge nodes to accelerate security and build near-end protection capabilities so that attacks can be terminated in the shortest path. ESA uses big data, behavior analysis, human-machine identification, and threat detection technologies to implement security capabilities such as precise access control, Challenge Collapsar (CC) attack defense, and DDoS attack defense.

- **Precise access control:** ESA allows flexible combinations of user-defined conditions (such as the request method, request domain name, and request header field) and logical conditions (such as equal to, including, and containing prefixes) and supports multiple access control technologies, enabling precise access control.
- **CC attack defense on the edge:** It effectively mitigates CC attacks on tenant domain names. ESA can restrict requests for access to protected websites based on a single IP address, cookie, or referer through flexible combinations of user-defined conditions (such as the request method, request domain name, request header field, and URL) and logical conditions (such as equal to, including, and containing prefixes), providing precise protection against CC attacks.
- **DDoS attack defense on the edge:** ESA monitors service traffic from the Internet to EIPs in real time, detects abnormal DDoS attack traffic promptly, and implements intelligent scheduling and defense to eliminate the impact of attacks on users.

7.6 Database

7.6.1 Relational Database Services

7.6.1.1 RDS

Relational Database Service (RDS) allows tenants to rapidly provision different types of databases whose storage resources can flexibly scale to meet tenants' service requirements. It also provides parameter groups that allow tenants to optimize their databases as required.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

RDS provides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshots, Point-in-Time Recovery (PITR), and deployment across AZs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each RDS instance runs in an independent VPC. Tenants can create a subnet group that spans multiple AZs and deploy high-availability RDS instances on a subnet. After an instance is created, RDS allocates an IP address of the subnet to the tenant for connection to the database. After deploying an RDS instance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be configured in combination to isolate RDS instances and thereby enhance instance security.
- **Access control:** When a tenant creates an RDS instance, a master database account is also created, with the password specified by the tenant. This account allows tenants to connect to and operate the RDS instance that they have created. Tenants can create database instances and sub-accounts as required, and assign database objects to those sub-accounts based on service plans to separate permissions. When creating an RDS instance, tenants can select a security group and deploy service-plane NICs of the instance in it. A VPC allows tenants to configure inbound and outbound rules for security groups hosting the RDS instances, thereby controlling the range of IP addresses that can connect to databases. Database security groups allow only database listening ports to be connected. Tenants do not need to reboot RDS instances when configuring security groups.
- **Transmission encryption:** RDS instances support TLS transmission between the database client and server. When RDS provisions instances, the specified Certificate Authority (CA) will generate a unique service certificate for each instance. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.
- **Storage encryption:** RDS can encrypt data before it is stored in a database. Encryption keys are managed by KMS.

- **Automatic backup and snapshot:** RDS supports automatic backup and snapshot for backup and restoration. Automated backups are created during the backup time window for DB instances. RDS saves automated backups based on a retention period tenants specify. Automatic backup is enabled by default. It stores backups for up to 2 years, allowing 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 any point in time 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 instance. Tenants can also restore data from an existing snapshot to a new instance.
- **Data replication:** RDS supports the deployment of high-availability instances. Tenants can deploy such instances in a single AZ or across AZs. If tenants use high-availability instances, RDS creates and maintains replicas for database synchronization. If the master instance fails, RDS will automatically instruct the standby instance to take over from the master instance in order to achieve high availability. If services are running on a read-heavy MySQL database, tenants can create a read-only instance. RDS maintains data synchronization between the master instance and read-only instance, and tenants can connect to either type of instance as required to split read and write operations.
- **Data deletion:** If a tenant deletes an RDS instance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.1.2 GaussDB(for MySQL)

GaussDB(for MySQL) is a high-performance, enterprise-class distributed relational database compatible with MySQL. It uses a decoupled compute and storage architecture and Huawei's latest generation of Data Function Virtualization (DFV) storage that auto-scales up to 128 TB. GaussDB(for MySQL) supports millions of Queries Per Second (QPS) and cross-AZ deployment to prevent data loss, combining the performance and reliability of commercial databases with the flexibility of open source ones.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

GaussDB(for MySQL) provides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshots, PITR, and deployment across AZs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each GaussDB(for MySQL) instance runs in an independent VPC. After an instance is created, GaussDB(for MySQL) allocates an IP address of the subnet to the tenant for connection to the database. After deploying a GaussDB(for MySQL) instance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be

configured in combination to isolate GaussDB(for MySQL) instances and thereby enhance instance security.

- **Storage isolation:** Storage resources are allocated by tenant, and containers are independently allocated to instances.
- **Access control:** When a tenant creates a GaussDB(for MySQL) instance, a master database account is also created, with the password specified by the tenant. This account allows tenants to connect to and operate the GaussDB(for MySQL) instance that they have created. Tenants can create database instances and sub-accounts as required, and assign database objects to those sub-accounts based on service plans to separate permissions. When creating a GaussDB(for MySQL) instance, tenants can select a security group and deploy service-plane NICs of the instance in it. Database security groups allow only database listening ports to be connected. Tenants do not need to reboot GaussDB(for MySQL) instances when configuring security groups.
- **Transmission encryption:** GaussDB(for MySQL) instances support TLS transmission between the database client and server. When GaussDB(for MySQL) provisions instances, the specified CA will generate a unique service certificate for each instance. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.
- **Automatic backup and snapshot:** GaussDB(for MySQL) supports automatic backup and snapshot for backup and restoration.Automatic backup is enabled by default. It stores backups for up to 2 years, allowing tenants to perform PITR on their databases. Once the automated backup policy is enabled, a full backup is triggered immediately. After that, full backups will be created based on the backup window and backup cycle tenants specified. When a DB instance is being backed up, data is copied and uploaded to OBS. Tenants do not need to set incremental backups because the system automatically performs an incremental backup every 5 minutes. The generated incremental backup can be used to restore the database and table data to a specified point in time. 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 instance. Tenants can also restore data from an existing snapshot to a new instance.
- **High availability:** GaussDB(for MySQL) supports high-availability cluster instances. Tenants can deploy such instances in a single AZ or across AZs. If tenants use cluster instances and a node fails, GaussDB(for MySQL) will automatically route services to another node in order to achieve high availability.
- **Data deletion:** If a tenant deletes a GaussDB(for MySQL) instance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.1.3 GaussDB

GaussDB is an enterprise-grade distributed relational database from Huawei. It uses a distributed architecture and features Hybrid Transactional/Analytical Processing (HTAP) capabilities. GaussDBsupports intra-city deployment across AZs for zero data loss, petabytes of data storage, and scale-up to more than 1000 nodes per instance. It is highly available, reliable, secure, and scalable, and provides key capabilities including one-click deployment, fast backup and restoration, monitoring, and alarm reporting for enterprises.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

GaussDBprovides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshots, PITR, and deployment across AZs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each GaussDB instance runs in an independent VPC. After an instance is created, GaussDBallocates an IP address of the subnet to the tenant for connection to the database. After deploying a GaussDBinstance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be configured in combination to isolate GaussDBinstances and thereby enhance instance security.
- **Storage isolation:** Storage resources are allocated by tenant, and containers are independently allocated to instances.
- **Access control:** When a tenant creates a GaussDBinstance, a master database account is also created, with the password specified by the tenant. This account allows tenants to connect to and operate the GaussDB instance that they have created. Tenants can create database instances and sub-accounts as required, and assign database objects to those sub-accounts based on service plans to separate permissions. When creating a GaussDBinstance, tenants can select a security group and deploy service-plane NICs of the instance in it. Database security groups allow only database listening ports to be connected. Tenants do not need to reboot GaussDB instances when configuring security groups.
- **Transmission encryption:** GaussDB instances support TLS transmission between the database client and server. When GaussDBprovisions instances, the specified CA will generate a unique service certificate for each instance. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.
- **Automatic backup and snapshot:** GaussDBsupports automatic backup and snapshot for backup and restoration. Automatic backup is enabled by default. It stores backups for up to 2 years, allowing tenants to perform PITR on their databases. Automatic backup performs a complete backup of all data so that a tenant can restore data to any point in time before the previous incremental backup. By default, the system automatically differential backs up the updated data every 30 minutes since the last automated backup. The backup period can be changed from 15 minutes to 1,440 minutes. 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 instance. Tenants can also restore data from an existing snapshot to a new instance.
- **High availability:** GaussDBsupports high-availability cluster instances. Tenants can deploy such instances in a single AZ or across AZs. If tenants use cluster

instances and a node fails, GaussDBwill automatically route services to another node in order to achieve high availability.

- **Data deletion:** If a tenant deletes a GaussDBinstance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.2 Non-relational Database Services

7.6.2.1 DDS

Document Database Service (DDS) allows tenants to quickly provision different types of databases. It supports auto scaling of compute and storage resources based on service requirements, and provides parameter groups that allow tenants to optimize their databases as required.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

DDS complies with the *Huawei MongoDB Security Configuration Specifications*. It provides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshots, PITR, and deployment across AZs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each DDS instance runs in an independent VPC. Tenants can create a subnet group that spans multiple AZs and deploy high-availability DDS instances on a subnet. After an instance is created, DDS allocates an IP address of the subnet to the tenant for connection to the database. After deploying a DDS instance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be configured in combination to isolate DDS instances and thereby enhance instance security. A VPC allows tenants to configure inbound and outbound rules for security groups hosting the DDS instances, thereby controlling the range of IP addresses that can connect to databases. During rule configuration, the GaussDB(for DDS) instance does not need to be restarted. Database security groups allow only database listening ports to be connected.
- **Storage isolation:** Storage resources are allocated by tenant, and VMs are independently allocated to instances.
- **Access control:** When a tenant creates a DDS instance, a master database account is also created, with the password specified by the tenant. This account allows tenants to connect to and operate the DDS instance that they have created. Tenants can create database instances and sub-accounts as required, and assign database objects to those sub-accounts based on service plans to separate permissions. When creating a DDS instance, tenants can select a security group and deploy service-plane NICs of the instance in it.
- **Transmission encryption:** DDS instances support TLS transmission between the database client and server. When DDS provisions instances, the specified

CA will generate a unique service certificate for each instance. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.

- **Storage encryption:** RDS can encrypt data before it is stored in a database. Encryption keys are managed by KMS.
- **Automatic backup and snapshot:** DDS supports automatic backup and snapshot for backup and restoration. Automatic backup is enabled by default. Once the automated backup policy is enabled, a full backup is triggered immediately. After that, full backups will be created based on the backup window and backup cycle tenants specify. It stores backups for up to 2 years, allowing tenants to perform PITR on their databases. After the automated backup policy is enabled, an incremental backup is automatically performed every 5 minutes for replica set instances to ensure data reliability. . When an instance is being backed up, data is copied and then compressed and uploaded to OBS.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 instance. Tenants can also restore data from an existing snapshot to a new instance.
- **Data replication:** DDS supports high-availability cluster/replica set instances as well as single-node instances. Tenants can deploy such instances in a single AZ or across AZs. If tenants use cluster/replica set instances, DDS automatically synchronizes data among nodes in a cluster/replica set. This means that, if a node fails, DDS can automatically route services to another node in the cluster/replica set in order to achieve high availability.
- **Data deletion:** If a tenant deletes a DDS instance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.2.2 GaussDB(for Mongo)

GaussDB(for Mongo) allows tenants to quickly provision different types of databases. It supports auto scaling of compute and storage resources based on service requirements, and provides functions such as automatic backup, database snapshot, and database restoration to prevent data loss. It also provides parameter groups that allow tenants to optimize their databases as required.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

GaussDB(for Mongo) complies with the *Huawei MongoDB Security Configuration Specifications*. It provides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshot, deployment across AZs, monitoring and alarming, audit logs, and slow logs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each GaussDB(for Mongo) instance runs in an independent VPC. Tenants can create a subnet group that spans multiple AZs and deploy high-availability GaussDB(for Mongo) instances

on a subnet. After an instance is created, GaussDB(for Mongo) allocates an IP address of the subnet to the tenant for connection to the database. After deploying a GaussDB(for Mongo) instance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be configured in combination to isolate GaussDB(for Mongo) instances and thereby enhance instance security. A VPC allows tenants to configure inbound and outbound rules for security groups hosting the GaussDB(for Mongo) instances, thereby controlling the range of IP addresses that can connect to databases. During rule configuration, the GaussDB(for Mongo) instance does not need to be restarted. Database security groups allow only database listening ports to be connected.

- **Storage isolation:** Storage resources are allocated by tenant, and containers are independently allocated to instances.
- **Access control:** When a tenant creates a GaussDB(for Mongo) instance, a master database account is also created, with the password specified by the tenant. This account allows tenants to connect to and operate the GaussDB(for Mongo) instance that they have created. Tenants can create database instances and sub-accounts as required, and assign database objects to those sub-accounts based on service plans to separate permissions. When creating a GaussDB(for Mongo) instance, tenants can select a security group and deploy service-plane NICs of the instance in it.
- **Transmission encryption:** GaussDB(for Mongo) instances support TLS transmission between the database client and server. When GaussDB(for Mongo) provisions instances, the specified CA will generate a unique service certificate for each instance. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.
- **Automatic backup and snapshot:** GaussDB(for Mongo) supports automatic backup and snapshot for backup and restoration. Automatic backup is enabled by default, and backups can be stored for a maximum of 35 days. Automated backups are generated according to a backup policy and saved as packages in OBS buckets to ensure data confidentiality and durability. Automatic backup performs a complete backup of all data. 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 instance. Tenants can also restore data from an existing snapshot to a new instance.
- **Data deletion:** If a tenant deletes a GaussDB(for Mongo) instance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.2.3 GaussDB(for Redis)

GaussDB(for Redis) is a cloud-native distributed database that is compatible with Redis.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

GaussDB(for Redis) complies with Huawei's *Redis 5.0 Security Configuration Baseline*. It provides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshots, and deployment across AZs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each GaussDB(for Redis) instance runs in an independent VPC. Tenants can create a subnet group that spans multiple AZs and deploy high-availability GaussDB(for Redis) instances on a subnet. After an instance is created, GaussDB(for Redis) allocates an IP address of the subnet to the tenant for connection to the database. After deploying a GaussDB(for Redis) instance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be configured in combination to isolate GaussDB(for Redis) instances and thereby enhance instance security. A VPC allows tenants to configure inbound and outbound rules for security groups hosting the GaussDB(for Redis) instances, thereby controlling the range of IP addresses that can connect to databases. During rule configuration, the GaussDB(for Redis) instance does not need to be restarted. Database security groups allow only database listening ports to be connected.
- **Storage isolation:** Storage resources are allocated by tenant, and containers are independently allocated to instances.
- **Access control:** When a tenant creates a GaussDB(for Redis) instance, a master database account is also created, with the password specified by the tenant. This account allows tenants to operate the GaussDB(for Redis) instance that they have created. When creating a GaussDB(for Redis) instance, tenants can select a security group and deploy service-plane NICs of the instance in it.
- **Transmission encryption:** GaussDB(for Redis) instances allow tenants to enable SSL-encrypted transmission. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.
- **Backup and restoration:** GaussDB(for Redis) supports automatic and manual backup as well as restoration. Automatic backup is enabled by default, and backups can be stored for a maximum of 35 days. Automated backups are generated according to a backup policy and saved as packages in OBS buckets to ensure data confidentiality and durability.The backup data is stored in OBS buckets and removed upon deletion of the corresponding instance. Tenants can also restore data from an existing backup to a new instance.
- **High availability:** GaussDB(for Redis) supports high-availability cluster instances. Tenants can deploy such instances in a single AZ or across AZs. If tenants use cluster instances and a node fails, GaussDB(for Redis) will automatically route services to another node in order to achieve high availability.
- **Data deletion:** If a tenant deletes a GaussDB(for Redis) instance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.2.4 GaussDB(for Influx)

GaussDB(for Influx) allows tenants to quickly provision different types of databases. It supports auto scaling of compute and storage resources based on service

requirements, and provides functions such as automatic backup, database snapshot, database restoration, and PITR to prevent data loss. It also provides parameter groups that allow tenants to optimize their databases as required.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

GaussDB(for Influx) provides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshots, PITR, and deployment across AZs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each GaussDB(for Influx) instance runs in an independent VPC. Tenants can create a subnet group that spans multiple AZs and deploy high-availability GaussDB(for Influx) instances on a subnet. After an instance is created, GaussDB(for Influx) allocates an IP address of the subnet to the tenant for connection to the database. After deploying a GaussDB(for Influx) instance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be configured in combination to isolate GaussDB(for Influx) instances and thereby enhance instance security. A VPC allows tenants to configure inbound and outbound rules for security groups hosting the GaussDB(for Influx) instances, thereby controlling the range of IP addresses that can connect to databases. During rule configuration, the GaussDB(for Influx) instance does not need to be restarted. Database security groups allow only database listening ports to be connected.
- **Storage isolation:** Storage resources are allocated by tenant, and containers are independently allocated to instances.
- **Access control:** When a tenant creates a GaussDB(for Influx) instance, a master database account is also created, with the password specified by the tenant. This account allows tenants to connect to and operate the GaussDB(for Influx) instance that they have created. Tenants can create database instances and sub-accounts as required, and assign database objects to those sub-accounts based on service plans to separate permissions. When creating a GaussDB(for Influx) instance, tenants can select a security group and deploy service-plane NICs of the instance in it.
- **Transmission encryption:** GaussDB(for Influx) instances support TLS transmission between the database client and server. When GaussDB(for Influx) provisions instances, the specified CA will generate a unique service certificate for each instance. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.
- **Automatic backup and snapshot:** GaussDB(for Influx) supports automatic backup and snapshot for backup and restoration. Automatic backup is enabled by default. It stores backups for up to 35 days, allowing tenants to perform PITR on their databases. Automated backups are generated according to a backup policy and saved as packages in OBS buckets to ensure data confidentiality and durability. Automatic backup performs a complete backup of all data and then

incremental backups every 15 minutes so that a tenant can restore data to any point in time 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 instance. Tenants can also restore data from an existing snapshot to a new instance.

- **Data deletion:** If a tenant deletes a GaussDB(for Influx) instance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.2.5 GaussDB(for Cassandra)

GaussDB(for Cassandra) allows tenants to quickly provision different types of databases. It supports auto scaling of compute and storage resources based on service requirements, and provides functions such as automatic backup, database snapshot, database restoration, and PITR to prevent data loss. It also provides parameter groups that allow tenants to optimize their databases as required.

To ensure the security of operations, data, and services and support customers' secure and orderly service activities, Huawei Cloud requires O&M personnel to strictly comply with the *Live-Network O&M Specifications for Database Services*. For example, they shall not delete instances or backup data when deleting resources, nor shall they access customers' database instances or process/transfer customer data without customers' written authorization.

GaussDB(for Cassandra) provides a wealth of security features to ensure the reliability and security of tenant databases. These features include VPCs, security groups, permission settings, SSL connections, automatic backup, database snapshots, PITR, and deployment across AZs.

- **Network isolation:** A VPC allows tenants to configure a range of source IP addresses that are permitted to access databases. Each GaussDB(for Cassandra) instance runs in an independent VPC. Tenants can create a subnet group that spans multiple AZs and deploy high-availability GaussDB(for Cassandra) instances on a subnet. After an instance is created, GaussDB(for Cassandra) allocates an IP address of the subnet to the tenant for connection to the database. After deploying a GaussDB(for Cassandra) instance in a VPC, tenants can configure a VPC interconnection 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. Subnets and security groups can be configured in combination to isolate GaussDB(for Cassandra) instances and thereby enhance instance security. A VPC allows tenants to configure inbound and outbound rules for security groups hosting the GaussDB(for Cassandra) instances, thereby controlling the range of IP addresses that can connect to databases. During rule configuration, the GaussDB(for Cassandra) instance does not need to be restarted. Database security groups allow only database listening ports to be connected.
- **Storage isolation:** Storage resources are allocated by tenant, and containers are independently allocated to instances.
- **Access control:** When a tenant creates a GaussDB(for Cassandra) instance, a master database account is also created, with the password specified by the tenant. This account allows tenants to connect to and operate the GaussDB(for Cassandra) instance that they have created. Tenants can create database instances and sub-accounts as required, and assign database objects to those sub-accounts based on service plans to separate permissions. When creating a

GaussDB(for Cassandra) instance, tenants can select a security group and deploy service-plane NICs of the instance in it.

- **Transmission encryption:** GaussDB(for Cassandra) instances support TLS transmission between the database client and server. When GaussDB(for Cassandra) provisions instances, the specified CA will generate a unique service certificate for each instance. Tenants can use the database client to download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data in transit.
- **Automatic backup and snapshot:** GaussDB(for Cassandra) supports automatic backup and snapshot for backup and restoration. Automatic backup is enabled by default. It stores backups for up to 35 days, allowing tenants to perform PITR on their databases. Automatic backup performs a complete backup of all data and then incremental backups every 15 minutes so that a tenant can restore data to any point in time 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 instance. Tenants can also restore data from an existing snapshot to a new instance.
- **Data replication:** GaussDB(for Cassandra) supports high-availability cluster/replica set instances as well as single-node instances. Tenants can deploy such instances in a single AZ or across AZs. If tenants use cluster/replica set instances, GaussDB(for Cassandra) automatically synchronizes data among nodes in a cluster/replica set. This means that, if a node fails, GaussDB(for Cassandra) can automatically route services to another node in the cluster/replica set in order to achieve high availability.
- **Data deletion:** If a tenant deletes a GaussDB(for Cassandra) instance, the data stored in the instance and the corresponding backup data in OBS will be automatically deleted. Once the data in the instance is deleted, it cannot be viewed or restored.

7.6.3 DRS

Data Replication Service (DRS) is an easy-to-use, stable, and efficient service that enables real-time database migration and synchronization. It provides a variety of functions for cloud databases, such as real-time migration, backup migration, real-time synchronization, data subscription, and real-time DR. This simplifies data flow between databases and helps users reduce data transmission costs.

DRS also provides security features such as IAM fine-grained authentication, network isolation, high availability, and encrypted transmission to ensure the security and high availability of data during replication.

- **Fine-grained authentication:** Tenants can create IAM accounts for users of different functional departments in their enterprises and assign access permissions based on users' functions. In this way, DRS operation permissions of users are isolated.
- **Network isolation:** DRS can specify subnets for network isolation from the source or target database. DRS can additionally implement network isolation by controlling network connectivity using the source database, target database, or DRS security group.
- **Host security of DRS instances:** DRS instances use ECS as compute resources. An ECS OS uses Huawei UVP to isolate and manage CPUs,

memory, and I/O resources. For details about UVP, see section 6.3 "Platform Security."

- **Data reliability and durability of DRS instances:** The storage resources of DRS instances are provided by Huawei Cloud EVS, which enables equivalent data reliability and durability. For details, see the introduction to data reliability and durability in section 7.4.1 "EVS."
- **High availability of DRS instances:** DRS provides high availability within an AZ. If a DRS instance fails, services can be switched to a new DRS instance in order to ensure continuous and stable services. DRS also provides high availability across AZs. As such, if the underlying compute resources of DRS instances in AZ 1 fail, the DRS instances in AZ 2 will be used to provide DRS for tenants.
- **Encrypted transmission:** DRS supports SSL encryption for data in transit over a public network, VPN, Direct Connect, or VPC, thereby enhancing the security of real-time migration, backup migration, real-time synchronization, and other data activities.
- **Data deletion:** DRS compute and storage resources are reclaimed after a tenant completes a DRS task. This means that all logs and running data on DRS instances are deleted and cannot be restored.

7.7 Big Data

7.7.1 MRS

MapReduce Service (MRS) is a data management and analysis platform featuring high reliability, scalability, and fault tolerance along with easy O&M. It hosts big data analytics clusters on Huawei Cloud. All nodes in an MRS cluster are distributed on the same VLAN of a tenant, and mutual trust is adopted between the active and standby Operation and Maintenance Service (OMS) nodes and other nodes in the cluster.

MRS allows users to log in to a cluster from a web browser or a component client. MRS provides Single Sign-On (SSO) based on Central Authentication Service (CAS). After users log in to a web page, they can access web pages of other components without entering the user name and password again.

MRS clusters in safe mode use the Kerberos protocol for authentication, and users can configure Kerberos authentication as required. The Kerberos system adopts the client-server model and encryption technologies such as AES. In addition, the client and server can authenticate each other to prevent unauthorized access, eavesdropping, and replay attacks. For details about the principles and user guide, visit https://support.huaweicloud.com/intl/en-us/usermanual-mrs/mrs_07_020001.html.

MRS supports data access control over big data components through Ranger. Apache Ranger is a centralized security management framework that provides unified authorization and audit. It implements fine-grained data access control over Hadoop and related components, such as the Hadoop Distributed File System (HDFS), Hive, HBase, Kafka, and Storm. Users can use the web UI console provided by Ranger to configure policies for controlling access permissions to these components. For details about the principles and user guide, visit:

1. https://support.huaweicloud.com/intl/en-us/productdesc-mrs/mrs_08_00411.html

2. https://support.huaweicloud.com/intl/en-us/cmpntguide-mrs/mrs_01_2393.html

- **User password management:** The MRS system uses IAM (Kerberos/LDAP) to manage user passwords. Kerberos encrypts user passwords and stores them in an LDAP database.
- **Permission control:** MRS provides RBAC. Assigning a role to a user will grant that user the permissions of the role. Such permissions are configured based on the component resources to be accessed.
- **Data encryption:** MRS HBase supports encrypted storage by column family. When creating a table, customers can determine which data is to be encrypted.
- **Data integrity:** User data is stored in HDFS DataNodes, which use CRC32C to verify data by default (CRC32 is also supported but it is slower). If the data transmitted from a client is incomplete, the DataNode reports the exception to the client and requests the client to rewrite data. The client checks data integrity when reading data from a DataNode. If the data is incomplete, the client will read data from another DataNode.
- **Data backup:** Data can be backed up from the active MRS HBase cluster to the standby MRS HBase cluster in an asynchronous real-time manner. The clusters provide basic O&M functions, including maintaining the relationship between active and standby clusters, rebuilding data, verifying data, and displaying the data synchronization progress.

7.8 Application Middleware

7.8.1 DMS

Distributed Message Service (DMS) is a message 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 variety of fields, such as enterprise solutions, financial payment, telecommunications, e-commerce, logistics, marketing/advertising, social networking, Instant Messaging (IM), mobile gaming, video, Internet of Things (IoT), and Internet of Vehicles (IoV). Its application scenarios include:

- **Service decoupling:** DMS can be used to provide message notifications for non-essential service components that rely on other systems, without needing to wait for those systems to finish processing. For example, the Order Processing (OP) system of an e-commerce website puts order information in DMS queues, and the inventory and delivery management systems will read the order information from the queues later.
- **Eventual consistency:** In a transaction or payment system, different subsystems/modules must eventually converge on the same state, either successful or failed. To ensure service continuity, reliable data transmission is required between subsystems and between modules. DMS meets this requirement, ensuring that the transactions of subsystems and modules are eventually consistent while also reducing the difficulty and cost of operations.
- **Coordinated traffic control:** On an e-commerce system or a large website, upstream and downstream systems have disparate processing capabilities. Traffic bursts that are handled by powerful upstream systems may have a significant impact on less powerful downstream systems. To address this issue, DMS can cache burst traffic (including order information) so that downstream

systems can process it when they have available capacity, thereby preventing them from being overloaded. DMS can cache hundreds of millions of messages for up to three days, enabling them to be processed during off-peak hours.

- **Log synchronization:** Applications can send log messages to DMS over reliable asynchronous channels. Other components can read log messages from DMS for further analysis, either in real time or offline. In addition, DMS can also be used to collect key log information required for monitoring.

Authentication and authorization for DMS access are controlled by IAM. After authentication is successful, users can perform all operations on their own queue resources. In addition, other services or IAM users can be assigned permissions to access and operate specified queues through policy-based control. By default, users can only access queues created by themselves.

DMS supports TLS 1.2 and PFS by default, and its API can be accessed only through HTTPS. For security purposes, DMS provides users with data encryption and storage functions, that is, server-side encryption (SSE). Users can use the common DMS-provided key or the KMS-generated key to encrypt and store data. In addition, messages can be encrypted before they are sent to DMS to prevent unauthorized access to sensitive data.

7.8.2 DCS

Distributed Cache Service (DCS) is a Redis-based distributed in-memory cache middleware service, featuring enhanced security, performance, and reliability. It can be used as a database, cache, or simple message queue. It supports multiple types of data structures, such as strings, hashes, lists, sets, sorted sets with range queries, bitmaps, hyperloglogs, and geospatial index radius queries. With built-in replication and Lua scripting, DCS also supports simple transactions, persistence, and cache replacement policies such as Least Recently Used (LRU).

DCS controls permissions using Huawei Cloud's RBAC, ensuring tenants can perform operations only on their own resources. For example, tenants can operate only their own DCS instances (DCS instances are physically isolated, and tenant instances are isolated by VPC). DCS checks tenant permissions and allows only authorized operations to be performed, with all key operations recorded in audit logs. Such logs can be retained for a specified period of time for auditing and backtracking if necessary.

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

7.8.3 API Gateway

API Gateway is a high-performance, highly available, and secure API hosting service that helps enterprise developers and partners build, manage, and deploy APIs at any scale. It facilitates internal system integration, service capability exposure, and service capability monetization in a simple, fast, and cost-effective manner with minimal risk.

API Gateway has the following security functions:

- **Access control:** It controls access to APIs based on IP addresses and accounts. Users can create a blocklist or trustlist to deny or allow access to APIs according to IP addresses and accounts.

- **Alarm monitoring:** It provides real-time and visualized monitoring of API events, including the number of API requests, API call delay, and API error information. The monitoring panel helps you understand the API call status and identify potentially service-affecting risks.
- **Signature key:** The signature key is used by the backend service to verify the identity of API Gateway, securing the backend services requested by API Gateway. A signature key, which consists of a pair of AK/SK, takes effect only after it is bound to an API. After this key is bound to an API, API Gateway adds the signature information when sending an API request to the backend service. The backend service then signs the API request in the same way, and verifies the API by checking whether the signature is consistent with that carried in the Authorization header sent by API Gateway.
- **Traffic control:** The frequency of API, user, application, and source IP address requests can be controlled based on service levels and user levels to ensure stable running of backend services.
- **Log audit:** Log Tank Service (LTS) can be used to analyze API call request logs of API Gateway to locate issues. Cloud Trace Service (CTS) can collect, store, and query all tenant configuration operation records of API Gateway for security analysis, compliance audit, resource tracing, and fault locating.

7.8.4 Workspace

Workspace is a Windows-based Virtual Desktop Infrastructure (VDI) and virtual application service provided by Huawei Cloud. It enables users to access their cloud desktop over Thin Client (TC) hardware from anywhere at any time. Workspace provides a higher level of security than traditional PCs by isolating user interfaces from data interfaces and effectively prevents data leakage by centrally storing and processing data.

No user data is stored on the TCs used with Workspace; they are used for running the Workspace client program only. Messages are transmitted between the TCs and Workspace over the highly secure Huawei Desktop Protocol (HDP), and input from local peripheral devices (USB devices, multimedia devices, flash storage, keyboards, and mouse devices) is redirected for security. Graphics rendering is performed on the client side, and no service data is transmitted.

Workspace enables users to log in to their Workspace accounts at any time from TCs in a tenant domain or over a private network line, making it more efficient and flexible than traditional computers and mobile storage devices.

It also improves maintenance efficiency by centrally managing password complexity policies, session timeout, desktop release, peripheral devices, patches, and upgrades.

And because Workspace employs virtualized management of all hardware, virtualized resources can be allocated to users as needed, lengthening the service life of user desktops and reducing costs associated with hardware upgrade.

Workspace provides the following security functions:

- **User identification:** Administrators and end users are assigned unique identities, which are linked with 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). In addition, Workspace automatically disconnects the session or requires user re-authentication if the user does not perform any action within a specified time.

And any user who fails to log in too many times within a specified interval is locked out. This not only ensures user security, but also has the added benefit of limiting the number of authentication requests sent.

- **Access control:** The scope of access control covers all subjects (such as users and service systems) and objects involved in resource access, as well as any operations between subjects and objects. Authorized users' permissions to access content and perform operations on protected resources are not allowed to exceed the preset scope. And for security purposes, data related to user authentication is stored in encrypted format.
- **Transmission security:** Desktop access is performed over HDP to ensure the confidentiality and integrity of data in transit. The number of sessions to a single desktop can be limited, and TLS 1.2 can be used to establish encrypted 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. Audit 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 the audit logs are not lost, they are stored on non-volatile storage media and can be dumped if storage space becomes insufficient. Logs are protected from unauthorized access, modification, and destruction, and only authorized users are permitted to access them.

7.9 Management and Monitoring

7.9.1 IAM

IAM is a user account management service designed for enterprises that allocate 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 employs a hierarchical fine-grained authorization mechanism to ensure that the users who are part of an enterprise tenant use cloud resources as authorized. This mechanism 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 security administrators of tenants to set different password policies, helping to protect user accounts from being exploited. Password policies include password complexity and validity period.

  - **Login policy:** IAM allows security administrators of tenants to set login policies to protect user passwords from brute force and phishing attacks, thereby preventing account leakage.
  - **ACL:** IAM provides IP address-based ACL to ensure that enterprise users can access Huawei Cloud resources only from a secure network environment, mitigating the risk of data leakage.
- **MFA:** It is an optional security measure that enhances account security and is used in conjunction with password-based authentication when users log in to the console. If MFA is enabled, users who have completed password-based authentication will receive a one-time SMS authentication code that they must use for secondary authentication. MFA is used by default for changing sensitive information such as passwords or mobile phone numbers.
- **Access key:** API requests must be signed with an access key for enterprise administrators to manage Huawei Cloud resources using O&M tools or API commands. Signature information is verified by API Gateway. Digital signatures and timestamps prevent requests in transit from being tampered with and protect against potential 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. For security purposes, the access key cannot be recovered or re-downloaded if it is lost or forgotten. After creating a new access key, the administrator must disable or delete the old one. The access key must be stored in a safe location and changed regularly, and under no circumstances should it be hardcoded.
- **Federated authentication:** If a tenant uses a secure and reliable external authentication service (for example, LDAP or Kerberos) and the service supports the Security Assertion Markup Language (SAML) 2.0 protocol, the tenant can configure the service as the 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 authentication to map external users to temporary Huawei Cloud users and allow those external users to access Huawei Cloud resources for a specified time period. For security purposes, a user group with a restrictive set of permissions must be created for these temporary users.

  Security credentials must not be hardcoded into mobile or web applications that access Huawei Cloud resources. Instead, such applications should prompt users to first log in, and then use already authenticated identity information to obtain temporary security credentials through federated authentication.
- **Permission 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, whereas cloud resource permissions deal with creating, deleting, modifying, and configuring cloud resources. Users inherit the cloud resource permissions assigned to their user group. As such, managing user permissions by user group facilitates systematic management. IAM can also work with PAM to implement fine-grained management of privileged accounts.

7.9.2 OneAccess

OneAccess provides centralized identity management, authentication, and authorization capabilities to ensure that authorized enterprise users can access trusted cloud and local application systems based on their permissions. In addition, it

can effectively track and audit abnormal user access behavior by managing audit logs in a centralized manner. OneAccess provides an E2E identity and access control mechanism that covers pre-event prevention, in-event control, and post-event tracing, improving user identity management efficiency and protecting information resource security. Its main functions include:

- **Unified identity management:** It manages and sets users, organizations, user groups, applications, accounts, and credentials in a unified manner. It also provides data synchronization, password policies, and self-service for enterprises and administrators to manage user identities throughout the lifecycle.
- **Unified permission management:** It manages and configures internal application permissions and platform permissions, and uses flexible policies that combine authorization modes with permission compliance rules to meet most permission requirements.
- **Unified authentication management:** It supports SSO and single sign-off and provides multiple built-in authentication modes, such as static passwords, SMS verification codes, dynamic passwords, and QR codes. Users can flexibly configure MFA policies and select multiple authentication modes to implement trusted authentication and improve information security.
- **Intelligent access control:** It provides adaptive access control capabilities. Based on the access context information (access time, location, and device) and user behavior data, users can use preset rules to identify risks during user access in real time. When a risk is detected, the authentication mode is adjusted in real time to enhance verification and implement adaptive access control.
- **Process compliance audit:** It provides multiple types of logs, including authentication, access, operation, synchronization, and system logs. The platform centrally manages user and administrator logs, and displays logs on a GUI to help enterprise administrators query, trace, and audit logs in real time.

7.9.3 CES

Cloud Eye Service (CES) is a comprehensive monitoring platform for elastic cloud servers, bandwidth, and other resources. It accurately monitors resource usage, samples indicators in real time, and accurately triggers alarms and notifications based on preconfigured rules. By monitoring alarms, notifications, and custom reports and diagrams in real time, CES enables users to precisely understand the status of service resources. Only tenants that have been authenticated by Huawei Cloud IAM have access to CES, which can be used through the service console, API, command line, or Software Development Kit (SDK). Note that CES does not obtain any tenant data; instead, it monitors only the data related to the utilization of infrastructure resources and such data is isolated by tenant. CES monitors indicators from other cloud services, including ECS, EVS, VPC, RDS, DCS, DMS, ELB, AS, WAF, Host Vulnerability Detection (HVD), Workspace, Machine Learning Service (MLS), Web Tampering Protection (WTP), Data Warehousing Service (DWS), Artificial Intelligence Service (AIS)[1], and more. Alarm rules and notification policies can be set based on these indicators to help users understand the usage and performance status of the instance resources used by each service. CES servers are deployed in a distributed manner to ensure high availability.

NOTE

The following Huawei Cloud services are not covered in the White Paper: HVD, MLS, WTP, DWS, and AIS. For more information, visit https://www.huaweicloud.com/.

7.9.4 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 service for tenant-specific industry certification and IT compliance certification. It provides the following functions:

- **Resource change auditability:** Changes to Huawei Cloud resources and system configurations performed by all users are recorded and audited systematically in real time. This is more efficient than manual auditing in traditional enterprise IT environments.
- **Real-time and systematical access security:** All management console operations and API calls are recorded systematically and in real time to help query, analyze, and locate issues.
- **Data auditability:** With the help of object-level API events recorded by CTS, users can detect data leakage by collecting active data of OBS objects.
- **Cost-effectiveness:** CTS can merge records into event files on a regular basis and move these to an OBS bucket for storage, making logs highly available, persistent, and cost-effective.

The security design for CTS is based on the Huawei Cloud security framework. Secure cloud auditing services are provided to tenants by ensuring secure networking, network border security, application security, and data security. Chapter 5 discusses infrastructure security in greater detail, including secure networking and network border security. Application security and data security are described as follows.

- **Application security:** CTS receives and processes the requests for compliance event queries and tracker operations sent by legitimate users and also the requests for compliance events from interconnected services. All requests are transmitted over HTTPS, and sensitive data is encrypted. Numerous measures, including interface control, trustlist control, requestor authentication, and content verification, are taken to ensure application security when CTS interacts with external services. Furthermore, the web security of CTS control nodes has been hardened to defend against a wide range of attacks.
- **Data security:** The security requirements for user log data processed by CTS differ according to whether the data is being generated, transmitted, or stored. During generation, log data must be masked within each service and verified to contain no sensitive data. During transmission, the accuracy and completeness of log data transmission and storage must be ensured through identity authentication, format validation, trustlist-based validation, and unidirectional reception. And during storage, log data must be backed up as multiple replicas, 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 to encrypt log data saved in an OBS bucket.

7.9.5 EPS

Enterprise Project Service (EPS) is a cloud resource management service provided for enterprise customers. Matching the hierarchical organization and project structure, it provides unified cloud resource management by enterprise project, and resource management and member management in enterprise projects. EPS mainly

includes enterprise project management, financial management, and personnel management. 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 Server (ECS), Auto Scaling (AS), Image Management Service (IMS), Elastic Volume Service (EVS), Virtual Private Cloud (VPC), Elastic IP (EIP), Content Delivery Network (CDN), Relational Database Service (RDS), Distributed Cache Service (DCS), Document Database Service (DDS), Cloud Container Engine (CCE), Advanced Anti-DDoS (AAD), Elastic Load Balance (ELB), Bare Metal Server (BMS), Dedicated Host (DeH), Cloud Service Engine (CSE), DLV Instance, PrivateNumber, Simple Message Notification (SMN), Application Performance Management (APM), Recommendation System (RES), DevCloud, DNS, Graph Engine Service (GES), Data Ingestion Service (DIS), Blockchain Service (BCS), Cloud Backup and Recovery (CBR), Distributed Database Middleware (DDM), Web Application Firewall (WAF), Cloud Search Service (CSS), Data Warehouse Service (DWS), MapReduce Service (MRS), Scalable File Service (SFS), Application Operations Management (AOM), Data Lake Insight (DLI), Cloud Data Migration (CDM), Object Storage Service (OBS), NAT Gateway, Distributed Message Service (DMS), AI development platform (ModelArts), CloudTable Service, Cloud Container Instance (CCI), Host Security Service (HSS), SupportPlan, API Gateway, Key Management Service (KMS), FunctionGraph, ROMA, Cloud Database (GaussDB), Gene Container Service (GCS), Cloud Eye Service (CES), Log Tank Service (LTS), Cloud Connection (CC), and Data Replication Service (DRS).

Tenants can use EPS through the service console or EPS API, which can be accessed only through HTTPS. EPS adopts a wide range of security measures to protect the management system from attacks. It uses a tenant-based permission model and secure communications protocols, strictly verifies parameters, and provides measures for protecting sensitive information and audit logs. It also supports TLS 1.2 and PFS by default. Furthermore, the parameters of all tenant API calls are strictly verified to prevent attacks, and all API calls are logged for auditing and accurate backtracking. EPS offers flexible access: Huawei Cloud accounts, accounts created by IAM and granted the EPS access, and other cloud services authorized by tenants. Different levels of permissions can be granted to users. Huawei Cloud accounts and IAM-created accounts that are assigned EPS administrator permissions can perform all EPS operations. Accounts created by IAM but assigned tenant permissions can perform only query operations.

7.9.6 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 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.

Tenants can use TMS through the service console or TMS API, which can be accessed only through HTTPS. TMS adopts a wide range of security measures to protect the management system from attacks. It uses a tenant-based permission model and secure communications protocols, strictly verifies parameters, and provides measures for protecting sensitive information and audit logs. It also supports TLS 1.2 and PFS by default. Furthermore, the parameters of all tenant API calls are strictly verified to prevent attacks, and all API calls are logged for auditing and accurate backtracking. TMS offers flexible access: Huawei Cloud accounts, accounts created by IAM and granted the TMS access, and other cloud services authorized by tenants. It does not store user privacy data. It calls interfaces of other services through internal authentication and transparent transmission, and IAM performs authentication.

7.9.7 SMN

Simple Message Notification (SMN) is a simple, flexible, and large-scale hosted notification service for messages. With SMN, users can efficiently and economically push messages to email addresses, mobile phone numbers, HTTPS applications, and mobile clients individually or in batches. The service can be readily integrated with and receive event notifications from other cloud services, such as CES, OBS, and AS.

Tenants can use SMN through the service console or SMN API, which can be accessed only through HTTPS. SMN adopts a wide range of security measures to protect the management system from attacks. It uses a tenant-based permission model and secure communications protocols, strictly verifies parameters, and provides measures for protecting sensitive information and audit logs. It also supports TLS 1.2 and PFS by default. Furthermore, the parameters of all tenant API calls are strictly verified to prevent attacks, and all API calls are logged for auditing and accurate backtracking. Mobile phone numbers, email addresses, and other sensitive tenant data are stored under encryption using reliable algorithms. SMN offers flexible access: Huawei Cloud accounts, accounts created by IAM and granted the SMN access, and other cloud services authorized by tenants. Different levels of permissions can be granted to users. Huawei Cloud accounts and IAM-created accounts that are assigned SMN administrator permissions can perform all SMN operations. Accounts created by IAM but assigned tenant permissions can perform only query operations.

7.10 Security and Compliance

7.10.1 DEW

Data Encryption Workshop (DEW) is a comprehensive cloud data encryption service that helps address issues in data security, key security, and complex key management. It provides functions such as dedicated encryption, key management, credential management, and key pair management, using the Hardware Security Module (HSM) to protect the security of keys. DEW is integrated with other Huawei Cloud services. Users can use DEW to develop their own encryption applications.

Key Management Service (KMS) is a secure, reliable, and easy-to-use key escrow service that helps create, manage, and protect keys. KMS uses the HSM to protect keys. All user keys are protected by the root key in the HSM to prevent key leakage.

Cloud Secret Management Service (CSMS) is a secure, reliable, and easy-to-use credential management service that enables users and applications to create, retrieve, update, and delete credentials. This service implements unified management of sensitive credentials throughout the lifecycle, effectively prevents sensitive information leakage caused by hardcoding or plaintext configuration, and prevents service risks resulting from ineffective permission control.

Key Pair Service (KPS) is a secure, reliable, and easy-to-use service that manages SSH key pairs in a centralized manner and protects their security.

KPS uses HSM-generated true random numbers to generate key pairs. It provides a comprehensive and reliable key pair management solution, helping users easily create, import, and manage SSH key pairs. The public key file of the generated SSH key pair is stored in KPS, and the private key file is downloaded and stored locally by users, ensuring the privacy and security of the SSH key pair.

Dedicated HSM is a cloud data encryption service. It provides encryption and decryption, signature signing, signature verification, key generation, and secure key storage.

Dedicated HSM provides exclusive resources to ensure concurrent high-speed computing performance under different encryption protocols including RSA, DSA, ECDSA, and others. It also provides industry-standard and application-integrated APIs, including PKCS #11, JCE, CNG, and more. Tenants can use the exclusive subrack, power supply, bandwidth, and interface resources, meeting their strict security requirements.

7.10.2 Anti-DDoS

The Anti-DDoS service uses specialized devices to implement precise and effective defense against a wide range of traffic attacks and application-layer attacks. It provides security protection capabilities for large, medium-sized, and small enterprises, Internet startups, and other businesses, protecting portal and website security and greatly reducing investment costs. The types of DDoS attacks protected against include Ping flood, SYN flood, UDP flood, CC attack, HTTP flood, and DNS flood. Once a protection threshold is configured (based on the leased bandwidth and service model), the system will notify affected users and perform effective protection immediately after a DDoS attack is detected.

The service provides the following functions:

- **Self-service protection policy:** Users can select a protection template based on their leased bandwidth and service model.
- **Traffic detection and scrubbing:** Anti-DDoS checks traffic in real time and performs scrubbing on attack traffic when it reaches the pre-defined threshold.
- **Ease of administration:** Real-time traffic trends are provided in reports on the flexible and easy-to-use management platform. The platform makes it simple to configure services, set up stringent controls, and monitor service resources.
- **Report monitoring:** It allows users to query defense information about individual public IP addresses. This information includes current protection status, protection parameters, traffic information, and abnormal events (countermeasures about traffic scrubbing and blackhole routing). Security reports are available, and users can query the previous four weeks of anti-DDoS

information, including scrubbed traffic, number of intercepted DDoS attacks, and top 10 frequently attacked IP addresses.

- **Log analysis:** Anti-DDoS receives and analyzes logs from anti-DDoS devices, reports alarms, and displays the results on a user-friendly interface.

Anti-DDoS also leverages other Huawei Cloud technologies to enhance its security capabilities, specifically, the secure infrastructure platform, secure networking, border protection, VM network isolation, API security, and log auditing.

7.10.3 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 multi-level security compliance requirements.

The service provides the following functions:

- **Asset management:** It manages and analyzes security asset information, such as accounts, ports, processes, web directories, and software.
- **Vulnerability management:** It detects vulnerabilities in the Windows and Linux OSs and software such as SSH, OpenSSL, Apache, and MySQL, and provides fixing suggestions.
- **Baseline check:** It checks system password complexity policies, typical weak passwords, risky accounts, and common system and middleware configurations to identify insecurities and prevent security risks.
- **Account cracking prevention:** It detects password cracking attacks on accounts such as SSH, RDP, FTP, SQL server, and MySQL, and blocks the identified attack source IP addresses for 24 hours to prevent hosts from being intruded due to account cracking.
- **Two-factor authentication:** It uses the verification codes in SMS messages and emails for secondary authentication of login attempts to ECS. This significantly improves account security.
- **Key file tampering detection:** It monitors key files (such as **ls**, **ps**, **login**, and **top** files) and prompts users about the risk of tampering once the files are modified.
- **Detection of malicious programs:** By detecting program features and behavior, and by using the AI-based fingerprint image 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:** It checks files in web directories to help identify webshells (written in languages such as PHP and JSP) in ECS.
- **Web page anti-tamper:** It protects web pages, electronic documents, images, and other files on websites from tampering or sabotage by hackers.

The service offers the following benefits:

- **Effective host risk prevention:** The asset management, vulnerability management, and baseline check functions can detect 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 fingerprint image 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.
- **Compliance with MLPS requirements:** The intrusion detection, vulnerability management, and web page anti-tamper functions meet the requirements of MLPS in China, such as host intrusion prevention, malicious code prevention, host vulnerability scanning, and data integrity.

7.10.4 CGS

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

The service provides the following functions:

- **Image vulnerability management:** CGS can scan private, official, and all running images in Huawei Cloud for vulnerabilities and provide fixing suggestions, ensuring image security.
- **Container security policy management:** CGS supports the configuration of security policies to help enterprises define the container process trustlist and file protection list, improving system and application security during container running.
- **Container process trustlist:** The container process trustlist can effectively prevent security risks, such as abnormal processes, privilege escalation attacks, and non-compliant operations.
- **File protection:** It can set important application directories (for example, **bin**, **lib**, and **usr** system directories) in containers to read-only to prevent tampering.
- **Container escape detection:** It scans all running containers for exceptions (including escape vulnerability attacks and escape file access), and provides mitigations for issues identified.

7.10.5 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 attack and defense mechanisms. Cloud WAF adopts a dual-engine architecture based on regular expressions 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, webshells, and CC attacks.

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

The service provides the following functions:

- **Web attack filtering:** Cloud WAF can detect 99% of web attacks (including all OWASP top 10 attacks, ranging from SQL injections, XSS attacks, command and code injections, and directory traversals to sensitive file access) and can detect malicious payloads in parameters, headers, and web addresses.
- **Powerful decoding:** Cloud WAF can restore url_encode, Unicode, XML, C-OCT, hexadecimal, HTML escape, and base64 code, case obfuscation, and JavaScript, shell, and PHP concatenation obfuscation.
- **Protection against CC attacks:** 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 function can more accurately identify attackers and stop CC attacks, a type of application-layer DDoS attack that consumes many service resources and affects service experience.
- **Webshell defense:** Cloud WAF checks the content in HTTP or HTTPS transmission channels to detect and block webshell attacks. This function can be enabled with a single click to protect services.
- **Precise customized control:** The Cloud WAF API can be used to create custom detection rules, including IP address blocklists and trustlists, user agent blocklists, and other more complex and precise rules.
- **Privacy filtering:** Private information such as user names and passwords can be removed from WAF event logs. Privacy filtering rules can be flexibly customized.
- **Centralized management:** WAF nodes are managed and operations (such as policy delivery and event log access) are performed in a centralized manner on the backend.

7.10.6 DBSS

Database Security Service (DBSS) leverages the machine learning mechanism and big data analytics technology to provide functions that ensure database security on the cloud, including database audit, SQL injection attack detection, and risk operation identification. It also provides user behavior discovery and audit, multi-dimensional analysis, real-time alarming, refined reporting, sensitive data protection, and audit log backup.

Database security audit provides the database audit function in bypass mode, enabling the system to generate real-time alarms for risky operations and perform audits. DBSS also generates compliance reports that meet data security standards. In this way, it locates internal violations and improper operations, holding relevant parties accountable.

The service provides the following functions:

- **User behavior discovery and audit**
  - Performs correlation analysis of access operations at the application and database layers.
  - Provides built-in or user-defined privacy data protection rules to prevent privacy data (such as accounts and passwords) in audit logs from being displayed in plaintext on the console.
- **Multi-dimensional analysis**

  - **Behavior statistics:** analysis from multiple dimensions, including audit duration, statement quantity, risk quantity, risk distribution, session statistics, and SQL distribution
  - **Session statistics:** analysis from multiple dimensions, including time, database user, and client
  - **Statement statistics:** analysis based on a variety of search criteria, including time, risk level, data user, client IP address, database IP address, operation type, and rule
- **Real-time alarms for risky operations and SQL injection**
  - **Risky operations:** You can define risky operations based on multiple fine-grained elements, including operation type, operation object, and risk level.
  - **SQL injection:** Database security audit provides an SQL injection library. It helps generate alarms immediately when detecting abnormal database behavior based on SQL command characteristics or risk levels.
  - **System resources:** An alarm is generated when the usage of system resources (CPU, memory, and disk) reaches the preset alarm threshold.
- **Refined reports for different abnormal behavior**
  - **Session behavior:** Analysis reports on client and database user sessions are provided.
  - **Risky operation:** Risk distribution analysis reports are provided.
  - **Compliance reports:** Compliance reports that meet data security standards, such as the Sarbanes-Oxley (SOX) Act[1], are provided.

NOTE

As a federal law passed by the United States Congress in 2002, the SOX Act sets more regulatory requirements for all US-listed companies' boards and management, as well as public accounting firms.

7.10.7 CFW

Cloud Firewall (CFW) is a next-generation cloud-native firewall that protects the Internet and VPC borders on the cloud and supports on-demand elastic scaling. It is fundamental for cloud-based network security protection. It provides the following functions:

- **Global unified access control:** It manages access control policies from the Internet to cloud services (Internet border) and between services (VPC border) in a unified manner, and provides access control and real-time intrusion prevention functions to comprehensively protect the network security of cloud services.
- **IPS:** For assets that are publicly accessible, the IPS can automatically identify the exposed threat surface and enable protection with one click. In addition, the IPS integrates Huawei's threat and vulnerability database for intelligent and precise protection.
- **Active external connection detection and interception:** It analyzes all active external connection behavior, assesses host compromise risks, blocks malicious connection behavior in real time based on the threat intelligence library, and records related logs to ensure asset security.
- **Full traffic analysis and visualization:** It analyzes all inbound and outbound traffic at the Internet border and between VPCs and displays the analysis report in a visualized manner.

- **Log audit and source tracing analysis:** It analyzes and records all service access logs, including access control logs, attack event logs, traffic logs, and operation logs, for auditing and advanced source tracing analysis.
- **On-demand elastic scaling:** Based on service development, users can dynamically scale in or out the number of protected EIPs, bandwidth of protected traffic, disk storage space, and more.
- **Ecosystem:** Third-party firewall engines are supported and can be configured using the same method as used for cloud-native firewall engines, delivering the same user experience.

Based on the preceding architecture and functions, cloud-native firewalls provide security protection for all traffic of cloud services.

7.10.8 DSC

Data Security Center (DSC) is a next-generation cloud-based data security platform that provides basic data security capabilities, including data classification, data security risk identification, data watermarking for source tracing, and static data masking. DSC integrates the status of each phase of the data security lifecycle in the data security overview to display the overall data security status on the cloud, helping users implement data security management throughout the lifecycle.

The service provides the following functions:

- **Sensitive data identification:** Leveraging both AI and an expert knowledge base, sensitive data and files can be accurately identified, covering both structured (RDS) and unstructured (OBS) data across all cloud scenarios.
- **Abnormal user behavior analysis:** DSC establishes a user behavior library through deep learning of user behavior. Any behavior not found in the library is deemed abnormal and an alarm will be reported in real time. You can then trace user behavior and correlate the events with the users to identify who performed the risky operations.
- **Data masking:** DSC supports both static and dynamic data masking.
- **Data watermarking:** DSC can add watermarks to and extract watermarks from PDF, PPT, Word, and Excel files.

The service offers the following benefits:

- **No impact on user data:** Data is read from the original database, and sensitive data is statically masked using the precise data masking engine. Masked data is stored separately, without affecting the original user data.
- **Various data sources:** Data of various sources on the cloud, such as RDS, self-built databases on ECSs, or big data, can be masked to meet security requirements.
- **Multiple masking requirements:** Users can mask specified database tables using more than 20 preset masking rules or user-defined masking rules. For details about the masking algorithms supported by DSC, see the Huawei Cloud official website.
- **One-click compliance:** Masking compliance suggestions are automatically provided based on the scanning result, and masking rules can be configured in one-click mode.

7.10.9 SA

Situation Awareness (SA) is a Huawei Cloud security management and situation analysis platform. It can detect more than 20 types of cloud security threats, including DDoS attacks, brute force cracking, web attacks, backdoors/Trojan horses, zombie hosts, abnormal behavior, vulnerability attacks, and command-and-control attacks. SA can collect statistics on attack events, threat alarms, and attack sources by category and comprehensively analyze them using big data analytics to present the global security landscape for users.

The service provides the following functions:

- **Security overview:** The security overview displays the overall security assessment status on the cloud, including security scores, security monitoring, security trends, and threat detection data. It can work with other cloud security services to centrally demonstrate cloud security.
- **Resource management:** It can synchronize the security status statistics of all resources under the current account and allows users to view resource names, services, regions, and security status, helping them quickly locate security risks and providing solutions accordingly.
- **Service analysis:** It comprehensively analyzes the service environment and displays the security status of the assets on the cloud. Service analysis includes HSS, WAF, and DBSS analysis.
- **Threat alarming:** Based on big data analytics and a highly accurate threat intelligence library, the system monitors threats on the cloud in real time, analyzes threat attacks, provides alarm notifications in a timely manner, and preconfigures response policies for typical threat events. The database stores event alarm details of the past 180 days.
- **Vulnerability management:** It helps users gain a comprehensive understanding of cloud asset vulnerability risks by obtaining the latest information about security vulnerabilities and synchronizing host and website vulnerability scanning results. Furthermore, it provides vulnerability remediation suggestions.
- **Baseline check:** It scans cloud services based on baseline configurations to identify risky settings, reports alarms for configurations with security risks, and provides hardening suggestions accordingly.

7.10.10 MTD

Managed Threat Detection (MTD) intelligently checks for potentially malicious activities and unauthorized behavior in IAM, DNS, CTS, OBS, and VPC logs generated when users perform operations on Huawei Cloud in the target region. It then promptly generates an alarm if any exception is detected. With MTD, users can handle alarms based on the alarm description, address potential threats, and harden service security quickly to prevent major losses such as information leakage, ensuring accounts and services remain secure and stable.

The service provides the following functions:

- **Checking logs of global services:** MTD accesses logs from IAM, VPC, DNS, CTS, and OBS and uses an AI engine, threat intelligence, and detection policies to continuously detect potential threats, malicious activities, and unauthorized behavior, such as brute-force cracking, penetration attacks, and mining attacks. It displays identified threats and generated alarms on a graphical dashboard.

- **Identifying distributed brute-force attacks:** MTD uses an industry-leading AI engine (also used for IAM) to detect known and unknown threats, improving the detection efficiency and accuracy. MTD uses an elastic profile model, unsupervised model, and supervised model to detect abnormal behavior in seven high-risk scenarios, including risky passwords, credential leakage, token exploitation, abnormal delegation, remote logins, unknown threats, and brute-force cracking. MTD can detect distributed brute-force attacks even if they occur with low frequency.
- **Capturing botnets and Trojan horses:** Based on the Bidirectional Encoder Representations from Transformers (BERT) model, MTD divides DNS into three channels (Bigram, Segment, and Position) and constructs a three-channel CNN model to detect known and unknown DGA and tunnel domain names, scanning behavior, and mining behavior. Leveraging BERT, MTD can effectively detect the Linux.Ngioweb botnet, SystemdMiner Trojan, WatchBog Trojan, and Bad Rabbit ransomware.
- **Data linkage:** Third-party threat intelligence in STIX/CSV format and IP address trustlists can be imported into OBS and asynchronously synchronized to MTD. MTD then preferentially detects the IP addresses and domain names in the list library, and identifies activities related to those in the imported intelligence or ignores activities related to those in the imported trustlists. This not only makes the detection response faster, but also reduces the service workload. In addition, detection results can be stored in OBS, meeting MLPS requirements.

7.10.11 AAD

Advanced Anti-DDoS (AAD) protects servers against large-scale DDoS attacks to ensure reliable and stable services. AAD changes the IP address of a protected server to a high-defense IP address, diverting malicious attack traffic to the high-defense IP address for scrubbing and thereby protecting mission-critical services. It is used to protect Huawei Cloud, non-Huawei Cloud, and IDC Internet hosts.

The service offers the following benefits:

- **Massive bandwidth:** It provides terabyte-level protection, defending against different DDoS attacks at the network and application layers. For details, see the Huawei Cloud official website.
- **High availability:** It automates attack detection and implements adaptive defense policies for real-time protection to ensure high availability. Service traffic is distributed in clusters, which feature high performance, low latency, and high stability.
- **Elastic protection:** It offers both basic bandwidth and elastic bandwidth services. The anti-DDoS threshold can be flexibly adjusted at any time to meet service requirements.
- **Professional operations team:** It provides 24/7 services to address threats to service continuity.

8 Huawei Cloud Engineering Security

In the traditional ICT field, Huawei continuously delivers secure and high-quality products and services to 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 help Huawei Cloud establish its multi-faceted full-stack security protection system and provide highly available, trusted cloud services. In addition, the continuous integration, delivery, and deployment practices, which are characteristics of cloud services, require entirely new mindsets, methodologies, and processes, as well as an all-new tool chain. By leveraging Huawei's wealth of experience and far-reaching capabilities in the security field, Huawei Cloud has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei SDL. As a result, DevOps is gradually taking shape as a highly automated new management process for the security lifecycle, called DevSecOps, alongside the cloud security engineering capabilities and tool chain that together ensure smooth and flexible DevSecOps implementation. In addition to the DevOps and DevSecOps processes, this chapter focuses on specific practices in Huawei Cloud security processes, including security design, secure coding, security testing, third-party software management, configuration and change management, and security approval for rollout.

8.1 DevOps and DevSecOps

Due to the changed business model of Huawei Cloud services, Huawei Cloud has established a new organizational structure and management system and adopted the DevOps process, which is more suitable for cloud service development, deployment, and operations. DevOps is different from traditional ICT R&D processes in the following ways:

- **Business decision-making:** Periodic reviews based on business cases replace decisions based on gates, that is, Decision Checkpoint (DCP)/Technical Review (TR).
- **Product development and delivery method:** Online services are delivered. DevOps in the Huawei Cloud management system is positioned as a new hybrid between R&D and O&M, enabling cloud services to go online quickly.
- **Marketing method:** An Internet marketing method is introduced.

- **Industry chain and ecosystem:** A new operations model featuring alliance collaboration, partnership management, and value distribution mechanisms is established.
- **Supply chain:** Services are provided to customers, but assets still belong to Huawei.
- **Finance:** The system needs to adapt to the Internet-based transaction method.

Operations-driven development, incremental improvements, rapid-fire sprints, and frequent deployments are key features of DevOps; therefore, in DevOps, 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.

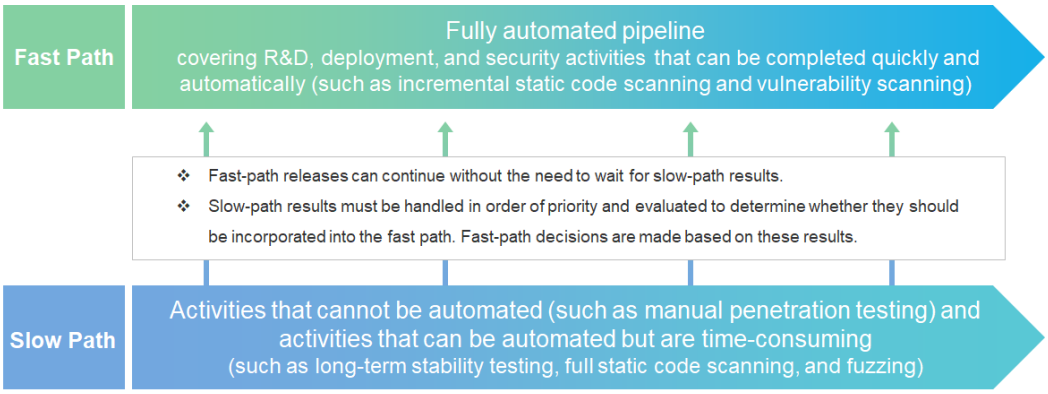
DevSecOps focuses on the following key goals:

- **Security quality:** ensuring that cloud services meet the quality standards of DevOps security activities.
- **Progress:** ensuring that cloud service security activities do not affect rapid and continuous integration, release, and deployment of DevOps.

8.1.1 Dual Path Mechanism

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

Figure 8-1 Dual Path mechanism



Definition of activities in the Dual Path mechanism:

- **Fast Path:** A fully automated pipeline for various security activities that can be performed quickly and automatically, such as incremental static code scanning, dynamic code 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 automated security activities that require a significant amount of time, such as

static code scanning, long-term stability testing, penetration testing, service continuity testing, fuzzing, dynamic program analysis, threat and vulnerability analysis, and capacity testing.

The two paths work together in the following ways:

- The Fast Path is the primary path of the DevOps/DevSecOps process. Once completely automated security activities reach security quality thresholds, R&D and O&M activities can be executed and completed immediately. Activities on the Fast Path do not need to wait for the results of security activities on the Slow Path. Security activities that eliminate high risks to cloud services are prioritized and executed on the Fast Path.
- The results of security activities on the Slow Path provide the basis for release decision-making, which the Fast Path must follow as well. For example, when a serious security risk is identified on the Slow Path, the Fast Path may be suspended and only able to restart after the risk is addressed.

8.2 Security Design

Huawei has always believed that security fundamentally stems from excellent design. This idea is in perfect harmony with the concepts behind the DevOps and DevSecOps processes. Huawei Cloud and the related cloud services comply with security and privacy design principles and specifications, as well as the legal and regulatory 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 that guide the threat analysis are drawn from the security accumulation and industry best practices in traditional products and new cloud domain products. After identifying a threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then they implement the corresponding security solution design. All threat mitigation measures eventually become security requirements and functions. Additionally, the design of security test cases is completed according to the company's security test case library and then implemented to ensure products and services with optimal security.

8.3 Secure Coding and Security Testing

Huawei Cloud strictly complies with Huawei's secure coding standards. Before taking up positions, Huawei Cloud service development and testing personnel are all required to learn the corresponding standards and pass examinations. In addition, Huawei Cloud introduces static code scanning tools for daily checks, with the resulting data fed into the cloud service CI/CD tool chain to control code quality via thresholds and assess the quality of cloud services and products. All alarms generated during static code scanning must be cleared before any cloud service is released, thereby preventing code-related security issues before service rollout.

To ensure the security of Huawei Cloud services, service testing teams test cloud services multiple times before release. This includes the microservice-level functions and interface security testing (such as authentication, authorization, and session security) in the alpha phase; API and protocol fuzzing in the beta phase; and database security testing in the gamma phase. The test cases cover the security

requirements identified in the security design phase and penetration test cases from an attacker's perspective. In addition, Huawei Cloud leverages its in-depth understanding of customers' security requirements and industry standards to design security check items and develop security testing tools. One such in-house tool is SecureCAT, which can be used to check the security configurations of mainstream OSs and database systems. This ensures that, after passing security testing, released cloud services comply with the security requirements of different regions and customers.

In addition, for cloud services sold or operated in specific countries and regions, the Internal Cyber Security Lab (ICSL), which is independent of the R&D system, conducts an independent security testing audit process. ICSL conducts security testing on cloud services from the customer perspective, performs in-depth security evaluation, and verifies compliance with Huawei's cybersecurity standards, baselines, and specifications. As the cybersecurity gatekeeper of customers, ICSL uses various attack methods, such as fuzzing, DoS testing, SQL injection, and XSS injection, as well as strict testing standards. ICSL does not allow services that fail the security testing to go live, thereby minimizing the cyber security risks facing Huawei Cloud service users.

8.4 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. In this regard, Huawei Cloud has formulated clear security requirements and comprehensive process control solutions for open-source and third-party software, and strictly controls software sourcing analysis, security testing, code security, risk scanning, legal review, software application, software exit, and more. For example, cybersecurity evaluation requirements are added to the open-source software sourcing phase to strictly control the sourcing. Third-party software in use is viewed as part of the services or solutions in the related activities. On top of that, considerable attention is given to the integration of open-source and third-party software and in-house software, or whether the use of independent third-party software in solutions creates new security issues.

Huawei Cloud extends its cybersecurity capabilities to open source communities. Once a vulnerability occurs in open-source software, Huawei Cloud can promptly discover and fix it with help gained through influence in open source communities. During response to vulnerabilities, open-source and third-party software is viewed as part of the services and solutions to verify whether known software vulnerabilities have been fixed. The list of fixed vulnerabilities in open-source and third-party software must be included in the Release Notes of the services.

8.5 Configuration and Change Management

Configuration and change management plays an important role in ensuring Huawei Cloud security. In Huawei Cloud, configuration managers are assigned to manage the configurations of all service units, 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, their attributes, and the relationships between them.

Any change to Huawei Cloud affects how cloud services run. Environment changes include changes to data center equipment, networks, system hardware and software, and applications. They involve the equipment used, architecture, system software updates (including network device software, OS image, and application container), and configurations. All changes must be managed in an organized fashion. After a change request is generated, the change manager assigns the change classification and submits the request to the Huawei Cloud Change Committee. After the Committee reviews and approves the request, the change can be implemented on the live network as planned. Before the change request is submitted, the change must undergo a testing process that includes production-like environment testing, gray release, and/or blue-green deployment. This ensures that the Committee fully understands the change activities, duration, rollback procedure, and all potential impacts.

8.6 Security Approval for Rollout

To ensure that Huawei Cloud and its cloud services comply with the laws and regulations and customer security requirements in every region in which they operate to minimize cybersecurity and privacy compliance risks, the Huawei GSPO and Chief Legal Officer (CLO) both participate in the release of cloud services. Before cloud platform versions and important cloud services are rolled out, the GSPO and CLO teams collaborate with development teams to analyze and determine whether the related versions or services meet local security and privacy compliance requirements.

To ensure that cloud services with medium and low security and privacy compliance risks go live quickly, the GSPO and CLO release a security and privacy compliance checklist, which contains the compliance requirements of all major regions and industries. Cloud service teams must perform self-check against the checklist during development, deployment, and rollout. And low- and medium-risk cloud services can be rolled out after passing the check. The results are submitted to both the GSPO and CLO for audit. Regarding high-risk cloud services, Huawei invests additional resources to quickly conduct more stringent verification and reviews, ensuring prompt and secure releases while also protecting tenants' interests.

9 Huawei Cloud O&M 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 highly values O&M. It places a strong emphasis on O&M security, which has become a top priority with increased resource investments. This chapter describes Huawei Cloud's practices in O&M security, vulnerability management, security event management, service continuity, and DR management.

9.1 O&M Account Operations Security

O&M involves all aspects of security. Huawei Cloud has established O&M security designs as well as specifications and processes. O&M security includes unified account, permission, and access management.

9.1.1 Account Authentication

When O&M personnel access the Huawei Cloud management network to centrally manage the system, they need to use employee identity accounts and MFA using two or more factors, such as something you know, something you have, and something you are. Employee accounts are used to log in to the VPN and bastion host for in-depth audits on user login.

Privileged accounts of assets such as OS hosts, network devices, and security devices are centrally managed by the privileged account management system and their passwords are automatically changed. When using privileged accounts, O&M personnel need to submit service tickets and perform routine audits to ensure the security of privileged accounts.

9.1.2 Permission Management

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

- **Account lifecycle management:** includes creating, reclaiming, authorizing, using, deregistering, and monitoring accounts. When O&M personnel receive O&M permissions, they need to raise their security awareness and pass the on-the-job exam to qualify. Once an account is created, it is immediately added to the account management system to ensure the E2E management from account creation, authorization, and authentication to permission reclaiming.

- **Account authorization process:** complies with the principles of separation of duties as well as checks and balances. The applicant and approver of an account must not be the same person. If O&M personnel need to use an account, they must submit a request in the account management system, and then obtain authorization using different service tickets, including event, alarm, and change tickets.
- **Permission management:** complies with the principles of work relevance, least privilege, and controlled approval and can be audited and traced. Attribute-Based Access Control (ABAC) and domain-based, hierarchical permission management are implemented on the basis of the different services and responsibilities of the same service. Login permissions are classified by core network, access network, security device, service system, database system, hardware maintenance, monitoring, maintenance, and other factors. Additionally, professional teams conduct regular reviews to determine if the account permissions are appropriate. This includes clearing the permissions of employees who leave or change positions, and checking for non-compliant use of accounts.

  Huawei Cloud O&M personnel must strictly comply with the following permission management rules during daily work:
  - Do not bypass security audit measures designed for systems, and do not modify, delete, or destroy system logs.
  - Do not use personal storage media to connect to servers.
  - Do not use any storage medium to connect to servers without authorization.
  - Without authorization, do not change the usage of facilities, equipment, and systems in the production environment, and do not perform activities or operations inconsistent with the originally-defined basic functions.

9.1.3 Access Security

Huawei Cloud boasts a large team of high-caliber O&M personnel to ensure its services and data centers operate continuously and stably. Centralized O&M management and auditing are achieved through VPNs and bastion hosts 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, ensuring access, authentication, authorization, and audits are managed in unison.

- **Remote O&M access from external networks:**

  To remotely manage Huawei Cloud, O&M personnel need to use an encrypted VPN channel to access the cloud platform O&M network or office network, and then log in to the cloud O&M management platform. To access resources such as OS hosts, network devices, and security devices from the Internet or office network, the personnel must apply for access permissions through the bastion host to implement authentication, authorization, and audit.
- **O&M access authentication security:**
  - The privileged accounts of users are centrally managed and authorized, making user name and password management more unified, simple, secure and effective.
  - Device passwords can be automatically changed every day, week, or month. After the device password expires, the account management system generates a strong password that complies with the password policy and automatically completes the password change.

9.2 Vulnerability Management

Huawei Product Security Incident Response Team (PSIRT) has established a mature vulnerability[1] response mechanism. For the self-operated cloud, PSIRT continuously optimizes the security vulnerability management process and technical means to ensure rapid remediation of vulnerabilities found in in-house and third-party software used by Huawei Cloud IaaS, PaaS, and SaaS services as well as O&M tools, reducing the risks to tenant services.

PSIRT and Huawei Cloud's security O&M team have established a comprehensive mechanism for vulnerability awareness, handling, and disclosure. Huawei Cloud manages vulnerabilities based on its vulnerability management system. It ensures that the vulnerabilities found in the in-house and third-party software are addressed and remediated within the SLA-specified period, thereby preventing vulnerability exploitation from potentially affecting tenant services.

NOTE

Vulnerabilities indicate defects or weaknesses in system design, deployment, operations, and management and can be used to violate system security policies. (RFC 4949)

9.2.1 Vulnerability Awareness

Huawei PSIRT has properly established vulnerability awareness and collection channels. The vulnerability collection mailbox (psirt@huawei.com) and bug bounty program (https://bugbounty.huawei.com/hbp) have been released on Huawei official website. Huawei PSIRT welcomes global vulnerability coordination organizations, suppliers, security companies, security researchers, Huawei employees, and other parties to report vulnerabilities in Huawei products or solutions. Additionally, Huawei PSIRT closely follows the industry's well-known vulnerability databases, security forums, mailing lists, security conferences, and other channels to ensure that Huawei PSIRT is promptly aware of Huawei-related vulnerabilities, including those in Huawei Cloud. A corporate-level vulnerability database that covers all Huawei products and solutions, including cloud services, is established to ensure that each vulnerability is effectively recorded, tracked, and addressed. Moreover, Huawei Cloud has provided a mailbox hws_security@huawei.com to collect vulnerability information, and Huawei Cloud's security O&M team uses commercial and self-developed online security scanning tools to perform regular vulnerability scanning tasks (tenant instances are not scanned), leaving no blind spots.

9.2.2 Vulnerability Response and Handling

Compared with Huawei's traditional ICT services, Huawei Cloud features more comprehensive network configuration information and more device operation permissions. Backed by the DevOps/DevSecOps process, Huawei Cloud is outstanding in continuous integration and deployment, with rapid remediation of vulnerabilities.

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 given to vulnerability exploitation risks on Huawei Cloud. As Huawei Cloud directly provides services for end users and faces greater Internet attack risks, it determines whether a service is Exposed to Internet (ETI) when assessing the vulnerability severity. The vulnerability remediation SLA requirements are finalized based on comprehensive considerations.

Huawei Cloud has established an E2E vulnerability response service ticket system from vulnerability awareness to live-network remediation. This system automatically receives vulnerabilities from multiple channels, such as PSIRT and online scanning tools, automatically determines the handling priority based on the severity of vulnerabilities, and specifies the remediation SLA. As for major vulnerabilities, the security O&M team uses in-house tools to scan live networks, mapping out the scope of affected services and modules within minutes. In addition, the security O&M team takes necessary mitigation measures based on live network situations, for example, restricting port access and implementing WAF rules on vulnerabilities to protect or isolate affected services, reducing the risk of vulnerability exploitation. If a vulnerability needs to be fixed by installing a patch or version, gray release or blue-green deployment is used to minimize the impact on tenant services. On top of that, Huawei Cloud continuously updates OS and container images, and rectifies system vulnerabilities through rolling upgrade of the images and containers, without affecting tenant services.

9.2.3 Vulnerability Disclosure

To protect the security of tenants, Huawei Cloud upholds the principle of responsible disclosure. For vulnerabilities related to cloud platforms and tenant services, Huawei Cloud offers tenants vulnerability workarounds, remediations, and recommendations on the premise that proactive vulnerability disclosure does not lead to greater attack risks, collaborating with tenants to address security challenges.

9.3 Security Logging & Event Management

A cloud security event refers to a suspected cyber attack or damage that has caused or may cause information leakage, data tampering, system intrusion, and service unavailability, as well as any confirmed security event that compromises the cloud service brand. The cloud attacks mainly include infrastructure-, platform-, and application-layer attacks (such as backdoors, vulnerability exploits, network scanning and eavesdropping, phishing, DDoS, and OWASP top 10 attacks) and information compromises (such as tampering, spoofing, leakage, theft, and loss).

To ensure the professionalism, urgency, and traceability of security event handling, Huawei Cloud has implemented comprehensive security log management requirements, rating and handling processes for security events, a 24/7 professional response team for security events, and a corresponding security expert resource pool. Huawei Cloud adheres to the principles of quick detection, scoping, isolation, and restoration to settle security events. In addition, Huawei Cloud keeps its event rating criteria, response time limit, and resolution time limit up to date by considering the impacts on the entire network and customers.

9.3.1 Log Management and Auditing

Huawei Cloud uses a centralized and comprehensive log system based on big data analytics, namely, Cloud Security Brain (CSB). CSB collects the management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems as well as the threat detection logs of security products and components. The logs support 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. CSB provides massive data storage and

powerful query capabilities. Specifically, it can store logs for over 180 days and support real-time queries within 90 days. Huawei Cloud also has a dedicated internal audit department that performs regular audits on O&M activities.

CSB can quickly collect, process, and analyze massive logs in real time. It uses in-house analysis engines and AI models to automate log analysis, threat identification, alarming, and handling.

9.3.2 Rapid Detection and Impact Scoping

Huawei Cloud has established a solid, multi-layered security protection system with comprehensive border defense. For example, firewalls are deployed hierarchically to isolate networks by security zones; anti-DDoS rapidly detects and defends against DDoS attacks; WAF detects and defends against web attacks in real time; IDS/IPS detects and blocks network attacks from the Internet and monitors abnormal host behavior in real time.

To handle different public cloud attacks with heavy traffic, Huawei Cloud uses CSB to associate the alarm logs of different security devices and then analyze them in a unified manner, quickly identifying existing attacks and predicting potential threats.

- Unlike the traditional O&M process (which lacks automation tools and relies on inefficient manual operations and experience-based analysis of security events), the CSB platform detects and displays threats in real time based on the massive data in original alarm logs. This platform significantly reduces the manual analysis time, shortening attack detection and impact scoping to just seconds.
- The SA analysis system supports various threat analysis models and algorithms and accurately identifies typical cloud attacks, including brute-force cracking, port scanning, zombies, web attacks, unauthorized web access, and APTs, based on threat intelligence and security consulting. Additionally, the system assesses Huawei Cloud's security posture in real time, analyzes potential risks, and provides warnings based on threat intelligence.
- Huawei Cloud has a professional security event management system for tracing and closing attack alarm events in an E2E manner. The entire handling process can be traced.

9.3.3 Rapid Isolation and Recovery

- When Huawei Cloud is under attack, border security devices become the first line of defense for rapid isolation and recovery. For example, Huawei Cloud's anti-DDoS protection scrubs the attack traffic layer by layer and fends off both large-scale DDoS and application-layer DDoS attacks in real time. WAF detects web attacks in real time, generates alarms for high-risk attacks, and blocks them immediately, and IPS defends against attacks on the platform and tenants.
- The CSB platform works with different security devices to detect and block attacks within seconds, forming a second line of defense for rapid isolation and recovery. It quickly identifies intrusions and accurately identifies attack sources.
- Huawei Cloud also partners with telecom carriers to automatically block large-scale DDoS attacks. This forms the third line of defense for rapid isolation and recovery. When a large-scale DDoS attack impacts Huawei Cloud's actual throughput, the anti-DDoS systems of Huawei Cloud and the carrier automatically collaborate to drop the attack traffic on the carrier's backbone routers. This ensures Huawei Cloud's bandwidth and tenant services that run normally. The entire defense process can be completed within minutes.

- Huawei Cloud has formulated various specific contingency plans to address complex security risks in the cloud environment. Each year, Huawei Cloud conducts contingency plan exercises for scenarios with major security risks, quickly reducing potential risks and ensuring cyber resilience.

9.4 Service Continuity and DR

Huawei Cloud infrastructure is highly available, thereby minimizing the impact of system failures on customers.

9.4.1 High Availability of Infrastructure

- Using the data center cluster architecture with "two sites, three data centers", Huawei Cloud implements DR and data backup. Properly operating data centers are deployed worldwide, and the two sites serve as each other's DR sites. If a failure occurs at one site, the system can automatically migrate customer applications and data to the unaffected site on the premise of compliance, ensuring service 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 unaffected data centers if one data center experiences a failure.
- Compute instances and data stored in Huawei Cloud can be flexibly switched between multiple regions or multiple AZs within the same region. Each AZ is an independent, physically isolated fault maintenance domain with its own UPS, on-site backup power generator, and power grid. All AZs connect to multiple tier-1 telecom providers for redundancy, eliminating the risk of a single point of failure.
- Users can fully utilize these regions and AZs to plan the deployment and running of application systems on the cloud. Distributed deployment of applications across multiple AZs ensures system running in most cases (including natural disasters and system failures).

9.4.2 DR Replication Between 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 cloud platform supports automatic failure detection and self-healing.
- Different AZs within a single region implement Data Center Interconnection (DCI) via high-speed fibers, meeting the basic requirement of cross-AZ data replication. Users can use the DR replication service as needed.

9.4.3 Service Continuity Planning and Testing

- In addition to providing high-availability infrastructure, data redundancy and backup, and DR between AZs, Huawei Cloud also formulates a service continuity plan, which it uses to perform regular testing. The plan, which applies to major disasters (such as earthquakes or public health crises), ensures Huawei Cloud services operate continuously and safeguards customers' service and data security.

- Huawei Cloud also develops a DR plan, which it uses to perform regular testing. For example, Huawei Cloud first brings the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, performs system operations and migration as specified in the DR plan, and then verifies the services and operations functions in the region presumably impacted by the disaster. Testing results are then annotated and archived to continuously improve the DR plan.

10 Security Ecosystem

In the face of ever-changing and increasingly serious security threats in cyberspace, the industry has reached consensus on working together to achieve open, collaborative, comprehensive detection, in-depth defense, emergency response, and rapid mitigation. Cloud service providers provide many different professional services for numerous tenants. To meet different levels of security requirements for various services in different scenarios, cloud service providers need to leverage the advantages of cloud native security while driving professional security product and service partners to jointly protect the data and service security of cloud tenants. As a result, Huawei Cloud has gathered a broad, comprehensive group of partners to provide security for tenants.

10.1 Security Ecosystem

Leveraging the global best practices in compliance and over 20 years of product and service experience, Huawei Cloud builds the security system foundation and provides a secure cloud platform and cloud security services to safeguard the digital transformation and intelligent innovation of governments and enterprises. Huawei Cloud is committed to building an "innovative, convergent, and win-win" security ecosystem. In 2021, Huawei Cloud launched the "Canghai campaign (together for a better ecosystem)" plan to gather seven types of security ecosystem partners and take three initiatives: ecosystem building, partnership, and federation. Working with global security partners to build a security ecosystem that meets the different security requirements of customers, Huawei Cloud aims to deliver cloud security products, services, and solutions that comply with global security regulations, providing more professional and comprehensive security capabilities.

The actions of the Huawei Cloud security ecosystem are guided by the "win-win" idea, which centers on meeting the different security requirements of customers/industries to gradually build a collaborative ecosystem with complementary capabilities. Huawei Cloud selects and regulates security ecosystem partners based on the principles of "consistent security capabilities", "unified security solutions", and "consistent security experience". These partners provide secure and trusted services that support cloud-cloud collaboration based on industry-recommended technologies. There are over 300 security services, such as SSL VPN, cloud firewall, mobile application hardening, bastion host, and unified identity authentication, fully meeting customers' security requirements for data, hosts, networks, applications, compliance, etc. For details on the security services provided

by Huawei Cloud ecosystem partners, visit https://marketplace.huaweicloud.com/search/security/.

Figure 10-1 Three initiatives of Huawei Cloud security ecosystem

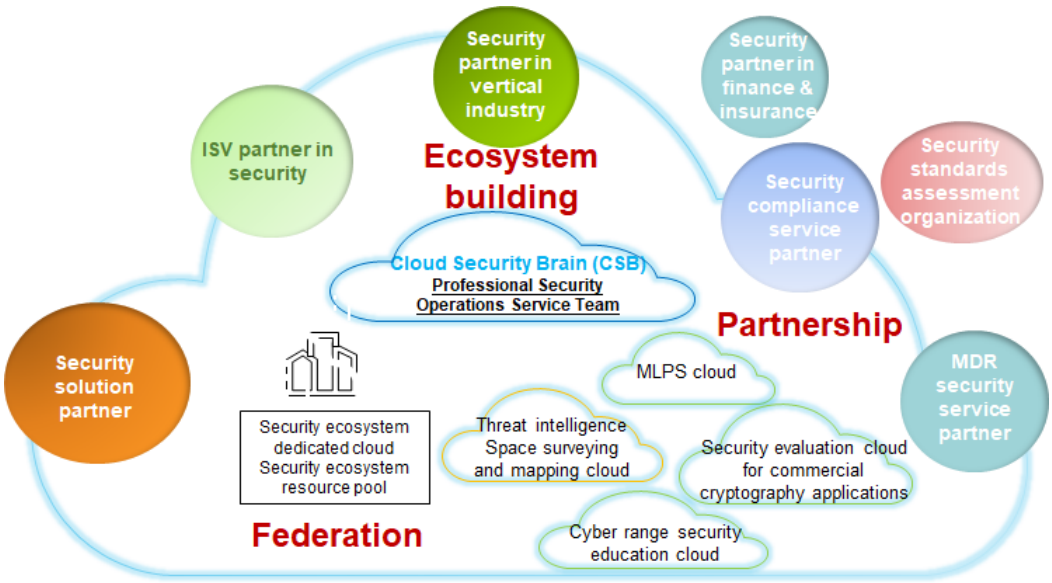
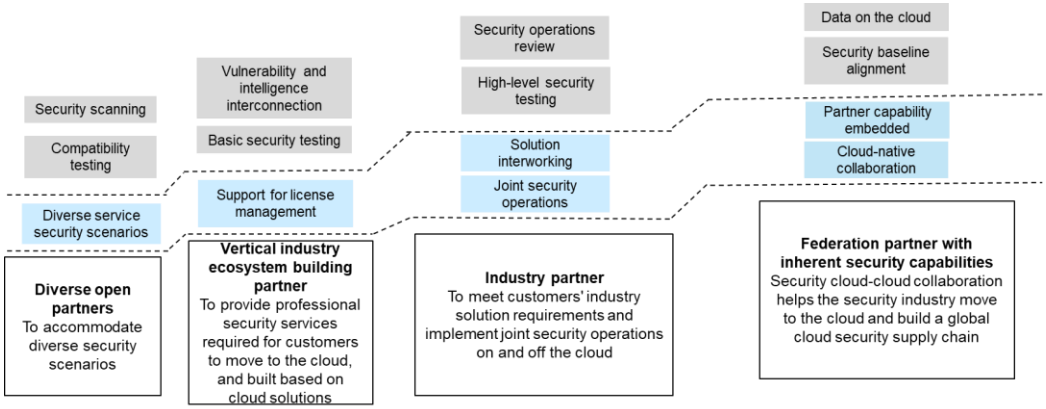


Figure 10-2 Different types of Huawei Cloud security ecosystem partners

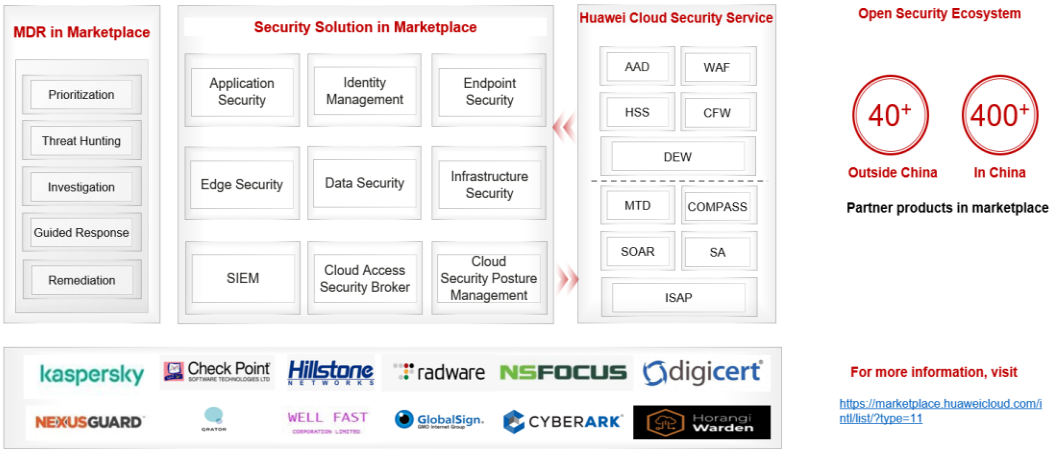


Seven types of Huawei Cloud security ecosystem partners

The Huawei Cloud security ecosystem consists of seven types of partners: security solution partner, security standards assessment organization, Independent Software Vendor (ISV) partner in security, security partner in vertical industry, security partner in finance & insurance, security compliance service partner, and MDR security service partner. These partners contribute to Huawei Cloud's native security solution, which can meet customers' security requirements for cloud migration in different scenarios, assure security operations capabilities, and maximize investment value. The seven types of Huawei Cloud security ecosystem partners are described as follows:

- **Security solution partner:** refers to the top vendors providing a comprehensive suite of security solutions, value-added security integration service providers, and solution service providers in the security industry.
- **ISV partner in security:** refers to the partners focusing on product/service solutions in segmented security scenarios, such as Cyber Trusted Identity (CTID) and industrial Internet security.
- **Security partner in vertical industry:** refers to professional security product/service providers (such as providers in honeypots, spatial surveying and mapping, or CSPM) in the vertical industry.
- **Security compliance service partner:** refers to partners in MLPS security and commercial cryptography application security evaluation in China and security (certification) partners outside China.
- **MDR security service partner:** refers to partners that closely work with Huawei Cloud to provide security and emergency response services for tenants.
- **Security partner in finance & insurance:** refers to the institutions that can invest in/finance major security projects and security innovation partners of Huawei Cloud customers, and professional partners (reinsurance companies, insurance companies, or security insurance service providers) that provide cybersecurity cloud insurance for Huawei Cloud security services.
- **Security standards assessment organization:** refers to professional security standards organizations, third-party security certification and assessment organizations, etc.

Figure 10-3 Huawei Cloud security ecosystem partners and solutions



Three initiatives for enabling ecosystem partners

Huawei Cloud enables security ecosystem partners for joint innovation through three initiatives: ecosystem building, partnership, and federation. Partners can volunteer to build secure and reliable cloud security solutions for Huawei Cloud customers after passing the corresponding assessment.

- **Ecosystem building**

  Leveraging cloud native security, Huawei Cloud introduces security ecosystem partners in vertical industries to quickly improve the basic security service capabilities required by tenants and meet their security requirements.

- **Partnership**

  Huawei Cloud works with the ecosystem partners to launch security solutions that meet customers' industry and scenario-specific service requirements, and develop typical cases in different industries, including governments and enterprises, finance, energy, transportation, and industrial Internet, to help customers migrate services to the cloud.

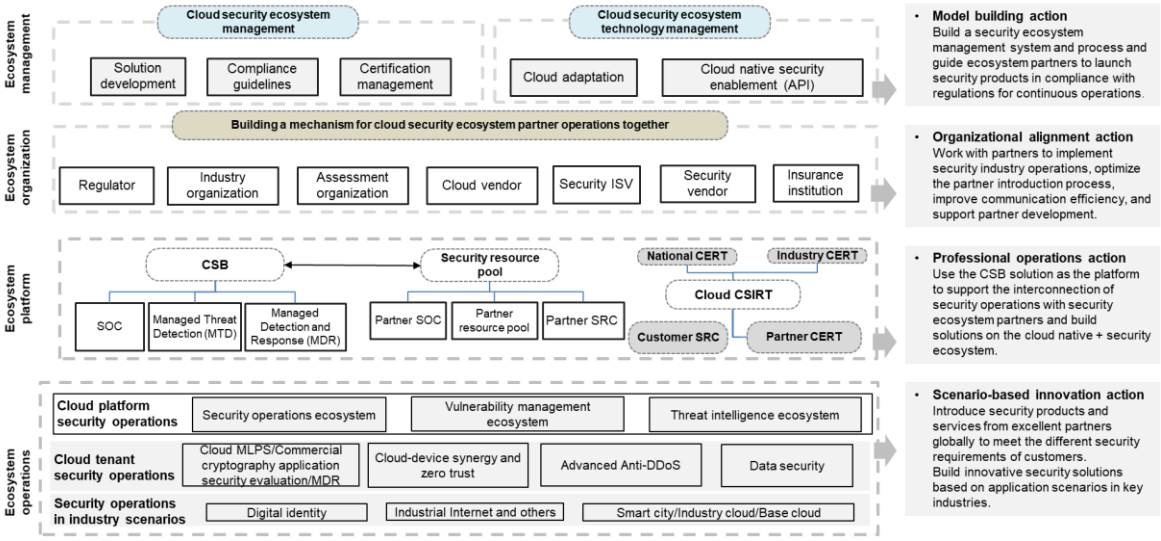
- **Federation**

  Security ecosystem partners are encouraged to establish dedicated regions, dedicated clouds, and resource pools on Huawei Cloud for comprehensive collaboration. Huawei Cloud enables partners with cloud native security capabilities and implements security ecosystem operations in important industries to build the security industry cloud, allowing partners to grow on Huawei Cloud while sharing responsibilities and developing capabilities together.

Four actions for building a new security ecosystem

Huawei Cloud takes four actions to build a new security ecosystem with partners, creating value for tenants, the partners, and the security industry.

Figure 10-4 Four actions for Huawei Cloud security ecosystem



- **Model building action**

  Build a security ecosystem management system and process and guide ecosystem partners to launch security products in compliance with regulations for continuous operations.

- **Organizational alignment action**

  Work with partners to implement security industry operations, optimize the partner introduction process, improve communication efficiency, and support partner development.

- **Professional operations action**

  Use the CSB solution as the platform to support the interconnection of security operations with security ecosystem partners and build solutions on the cloud native + security ecosystem.

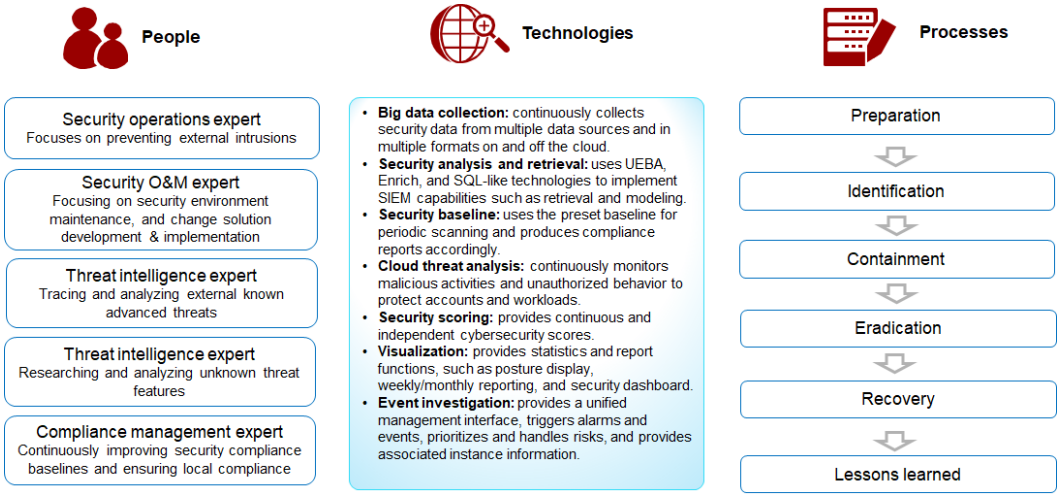
- **Scenario-based innovation action**

  Introduce security products and services from excellent partners globally to meet the different security requirements of customers. Build innovative security solutions based on application scenarios in key industries.

10.2 Technical Architecture of the Security Ecosystem

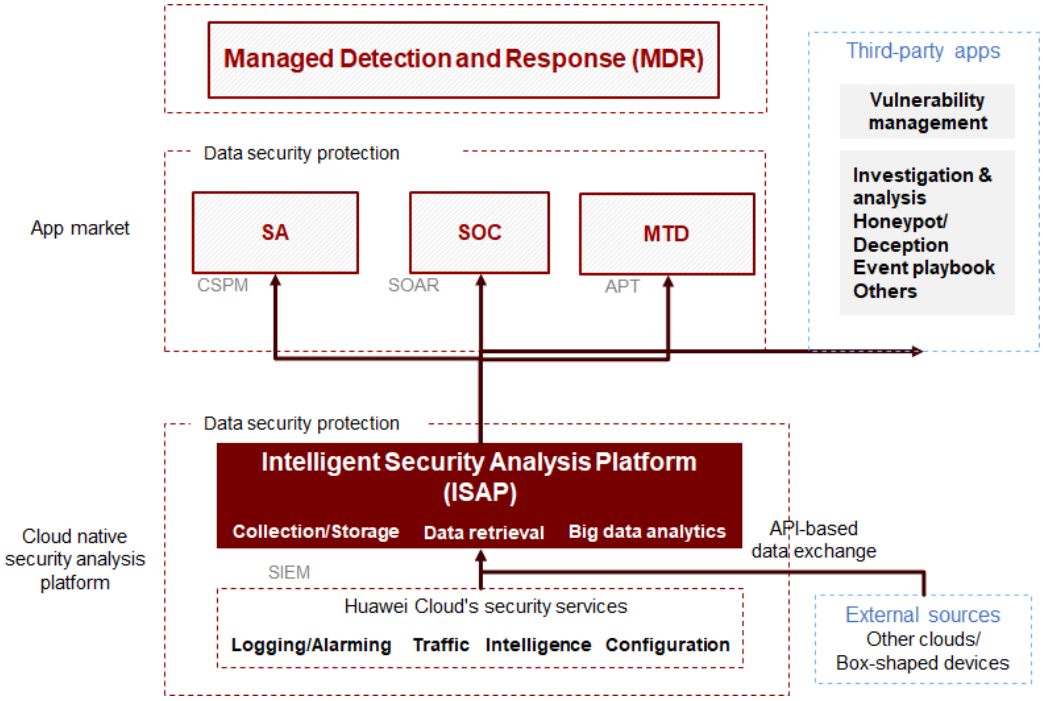
The Huawei Cloud security ecosystem is a modern cloud security management and operations platform that uses Huawei Cloud CSB as the cloud computing environment. It is an ideal combination of people, processes, and technologies. The CSB solution is designed to meet customers' security requirements and hybrid cloud requirements in the future and in on- and off-cloud collaboration scenarios. It provides a unified security management plane for Huawei Cloud tenants, supports centralized management and control of global security in the hybrid cloud environment, and enables tenants to monitor and respond to overall security in real time. CSB effectively overcomes the following shortcomings: various security capabilities of different enterprises, separate security management across multiple tenants using different accounts, and lack of overall security posture display and centralized emergency response capabilities for security products and services from different vendors.

Figure 10-5 Huawei Cloud CSB



As for the solution architecture, CSB is a comprehensive big data security solution based on the Intelligent Security Analysis Platform (ISAP). It provides a wide variety of in-house services (including SA, the security operations center, and the threat detection service) and third-party ecosystem services. The following figure shows the overall logical architecture of this solution.

Figure 10-6 CSB architecture



Partners and cloud users can benefit from the CSB ecosystem.

- **Integrated entry: simplified operations, saving 80% of operating time**

  Centralized access: The secure application ecosystem, on-demand purchase of services, and one-click installation significantly shorten the procurement process

  Centralized threat alarms: The alarms of each service are aggregated, and security events are automatically analyzed, considerably reducing O&M costs.

  Centralized policies: The security policies of each service can be quickly and conveniently adjusted and optimized on demand, significantly improving O&M efficiency.

- **Integrated capabilities: integrated security capabilities for intelligent security operations**

  Huawei Cloud removes obstacles to cloud migration for ecosystem partners and enables them to build secure and easy-to-use cloud environments for end users.

  Huawei Cloud provides easy-to-use security products, helping customers improve the efficiency of their security operations.

- **Integrated data: unified standards, data confined to the cloud, and security and trustworthiness**

  Cloud native data collection, governance, and lifecycle management ensure the data privacy and trustworthiness of platforms and tenants, facilitating migration of ecosystem products to the cloud.

  Unified resource models, data standards, and access specifications, along with shared security data, help ecosystem partners explore the value of security big data and implement more efficient cloud migration.

  Traditional SA products are widely used offline, and the related projects may involve different security management software on and off the cloud. Therefore,

Huawei Cloud's in-house security products and non-Huawei Cloud security products need to be interconnected using one of the following:

- **Connect mode:** This can be used if customers have purchased typical Security Information and Event Management (SIEM), SOC, and SA products. The alarms of off-cloud products are sent to the ISAP or SA platform on the cloud through unified APIs. In this mode, vendors' products and the related components of CSB must be adapted and verified in advance.
- **Add-on mode:** This can be the SaaS software capability integration, threat intelligence integration, or MDR integration mode. Details are as follows:
  - **SaaS software capability integration:** If customers require additional security management capabilities, ecosystem partners can contact Huawei Cloud ecosystem representatives to introduce the ecosystem products to the Huawei Cloud product system; alternatively, the customers can engage agents or integrators to purchase third-party products in a centralized manner to meet their requirements.
  - **Threat intelligence integration:** Some customers need to call threat intelligence data to better discover security risks. For example, they need to conduct an intelligence investigation on suspected IP addresses that are exposed. In this case, threat intelligence partners can contact Huawei Cloud to feed intelligence data to the CSB data platform and negotiate the cooperation mode.
  - **MDR:** If customers want to establish O&M teams or enhance their O&M security capabilities to assure major events and support important conferences, the capable partners can contact Huawei Cloud and get certified as MDR expert service providers after passing the appraisal and training so that they can leverage the CSB platform to help Huawei Cloud users utilize the various cloud security tools better.

Huawei Cloud has released corresponding technical interface guides. It is committed to working with industry-leading security ecosystem partners to continuously build security linkage solutions and provide professional security operations services through openness, convergence, and win-win cooperation, facilitating service innovation on the cloud.

10.3 Security Ecosystem Features

We are building the Huawei Cloud security ecosystem through collaborative innovation and win-win convergence. So far, Huawei Cloud has developed over 200 professional security products and services with partners worldwide. Huawei Cloud and its partners will leverage their respective strengths to address the threats to the cloud, incubate and deliver better security products and services, build long-term trust and partnerships, and promote the cloud-based upgrades of the security industry.

- **Collaborate to Address Threats**

  The Huawei Cloud security ecosystem is not a traditional interlock between two parties. Instead, it combines cloud native security and the security ecosystem to support cloud-based upgrades of security partners, overcome the weaknesses of the security bucket, and accelerate convergence of the security industry. Together with ecosystem partners, Huawei Cloud addresses the increasingly serious security threats and challenges in the global cyberspace.
- **Serve Users Together**

The Huawei Cloud security ecosystem is not a traditional security distribution channel. Instead, it aims to grow the security industry, facilitate business model innovation, and improve professional security operations services through solution coupling, in-depth exploration of industry scenarios, and collaborative development of defense capabilities.

- **Build Trust and Collaboration**

  The Huawei Cloud security ecosystem does not involve a short-term market behavior. Instead, Huawei Cloud enables its ecosystem partners with cloud native security and shares threats to build a high starting point for compliance. Through technical measures such as business and security interface interconnection in the global cloud market (joint operations), Huawei Cloud works with partners to flourish the global security market, support the upgrade of the security industry, and optimize the global cloud security supply chain.

11 Change History

Year	Version	Description
2023	3.4	Regular update
2022	3.3	Regular update
2021	3.2	Regular update
2020	3.1	Regular update
2019	3.0	Regular update
2018	2.0	Regular update
2017	1.0	First release

