

华为云安全白皮书

版本

3.1

发布日期

2019 年 7 月



华为技术有限公司



版权所有 © 华为技术有限公司 2019。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： 华为 – <https://www.huawei.com/cn/>
 华为云 – <https://www.huaweicloud.com/>

电子邮箱： support@huawei.com



目 录

导读.....	iv
1 云安全战略	1
2 责任共担模型	5
2.1 华为云的安全责任	6
2.2 租户的安全责任	7
3 安全合规与隐私保护	9
3.1 安全合规与标准遵从	9
3.2 隐私保护	11
4 安全组织和人员	12
4.1 安全组织	12
4.2 安全与隐私保护人员	12
4.3 内部审计人员	13
4.4 人力资源管理	13
4.5 安全违规问责	15
5 基础设施安全	17
5.1 物理与环境安全	17
5.2 网络安全	19
5.3 平台安全	22
5.4 API 应用安全	23
5.5 数据安全	25
6 租户服务与租户安全	30
6.1 计算服务	30
6.2 网络服务	33
6.3 存储服务	39
6.4 数据库服务	44
6.5 数据分析服务	47
6.6 应用服务	48
6.7 管理服务	51



6.8 安全服务	55
7 工程安全	65
7.1 DevOps 和 DevSecOps 流程	65
7.2 安全设计	67
7.3 安全编码和测试	67
7.4 第三方软件安全管理	68
7.5 配置与变更管理	68
7.6 上线安全审批	69
8 运维运营安全	70
8.1 O&M 账号运营安全	70
8.2 漏洞管理	72
8.3 安全日志和事件管理	73
8.4 业务连续与灾难恢复	75
9 安全生态	77

导读

过去几年中，华为云与所有云服务供应商（CSP – Cloud Service Provider）和客户一样，面临着层出不穷的云安全挑战，不断探索，收获颇多。2017 年初，华为云部（Cloud Business Unit, aka Cloud BU）正式成立，重新启程，开启华为云新时代。华为云迎难而上，视挑战为机遇，恪守业务边界，携手生态伙伴，共同打造安全、可信的云服务，为客户业务赋能增值、保驾护航。

华为云通过结合业界先进的云安全理念、世界领先的 CSP 优秀安全实践、华为长年积累的网络安全经验和优势以及在云安全领域的技术积累与运营实践，摸索出了一整套行之有效的云安全战略和实践。华为云已经构建起多维立体、纵深防御和合规遵从的基础设施架构，用以支撑并不断完善涵盖了 IaaS、PaaS 和 SaaS 等一百六十余项具有优良安全功能的常用云服务。在这背后，是华为云高度自治的扁平化组织，具备高度安全意识和能力的研发运维运营团队，先进的云服务 DevOps/DevSecOps¹ 流程，以及日益繁荣的云安全生态圈。华为云将一如既往，本着租户业务优先的原则，携手生态伙伴，不断发布高质量的云服务增值安全功能、高级云安全服务和安全咨询服务，切实保护租户利益，帮助租户持续扩大业务，提升华为云市场竞争力，实现用户、合作伙伴、华为云三者的长期共赢。

藉此，华为云隆重推出《华为云安全白皮书》（简称“白皮书”），将华为云对云安全的丰

¹ DevOps 和 DevSecOps 目前尚没有很好的统一中文译名。DevOps 是随着云服务发展而由高科技公司的实践派而非理论派创造并逐渐成熟的从研发到运营的全线工程流程和工具链实践。由于 DevOps 需要支撑云服务和其他线上功能的持续集成持续部署（CI/CD – Continuous Integration/Continuous Deployment），传统的瀑布流程和敏捷流程下的安全周期管理（SDL – Security Development Lifecycle）已大部分不适应新的节奏。安全必须无缝嵌入并实现高度自动化，这也就自然而然地形成了名为 DevSecOps 的全新安全周期管理。通过华为对国内外业界主流云服务和线上服务公司的调研，一个不争的事实是这些公司已经越来越普遍地大范围采用 DevOps/DevSecOps 工程流程和工具链实践。并且，采用 DevOps/DevSecOps 的结果也显示了传统 IT 安全人员源于直觉的担忧是杞人忧天。将安全无缝嵌入的 DevOps/DevSecOps 非但不会削弱安全，反而通过高度自动化对安全有高效的提升。

富经验，分享给用户，分享给业界，以求相互了解，相互借鉴，共同推动云行业、云安全行业的开放与发展。

本白皮书面向各行业、各地区的广大读者群：

- 从租户、生态伙伴和社区到互联网用户
- 从大中小型企业客户到个人用户
- 从决策层、管理层到 IT、安全和隐私保护等云服务相关的技术岗位人员，以及其他相关岗位人员（主要包括营销、采购/合同、合规审计等云服务相关人员）。

1 云安全战略

随着电信网络和信息技术，尤其是云服务相关技术的不断演进与发展，网络安全和云安全面临的威胁和挑战将日益严重。网络安全和云安全已经成为多维度的全球性挑战，只有通过全球范围内技术厂商，供应商，客户，标准、政策与法律制定者之间的合作，才能在应对该挑战上取得积极显著的成效。我们必须共享知识和经验，务实合作，共同努力，减少技术被滥用所导致的不可预期风险。

作为全球领先的信息和通信技术（ICT – Information and Communication Technology）解决方案供应商，华为技术有限公司（以下简称“华为”）充分理解网络安全和云安全的重要性，并充分理解各国政府及客户对此的担忧与高度关注。

针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击²，华为对安全问题的忧患意识也日益紧迫，高度重视在网络安全和云安全技术能力、合规及生态上的投入，并采取切实有效的措施，加速开发云安全技术和服务，提升公司云产品和云服务的安全性，提升云安全合规和生态建设，帮助客户规避和减少云安全风险，以赢得各利益相关方的信赖。华为认为，构建一个开放、透明、可视的多维全栈云安全框架，将有助于整个云服务产业健康持续发展，并将促进云技术创新。

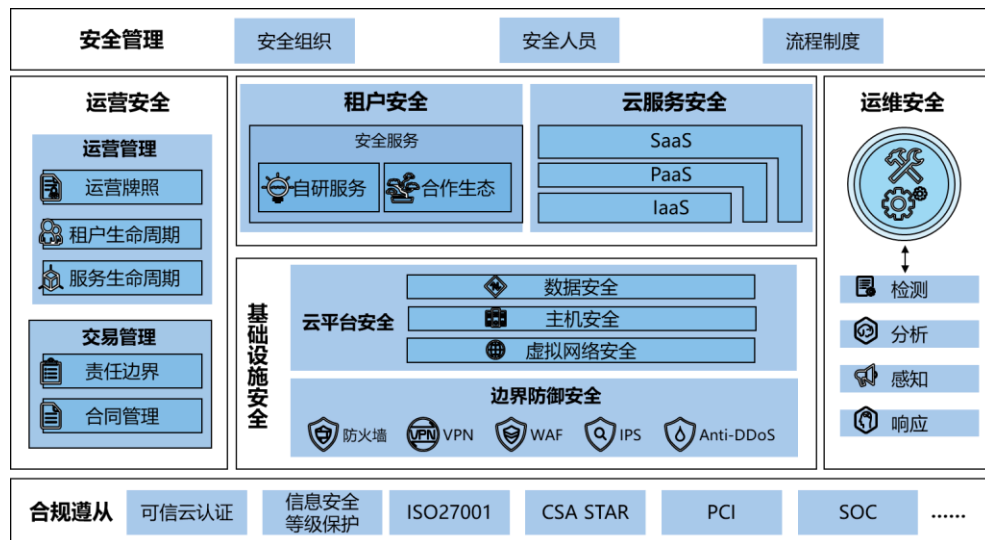
华为云秉承华为公司创始人、CEO 任正非先生提出的“**将公司对网络和业务安全性保障的责任置于公司的商业利益之上**”。在安全至上的企业文化氛围中，华为云不断汲取公司安全养分，脚踏实地，不断前行。华为云安全的历史可追溯到 2000 年华为安全测试实验室成立。从那时起，近 20 年来，华为持续不懈地构建自身安全能力，这些能力

² 云安全联盟（CSA – Cloud Security Alliance）对云安全挑战、威胁与攻击进行了系统而持续的梳理，请参考云安全联盟之云安全威胁排行榜（https://cloudsecurityalliance.org/group/top-threats/#_overview），在此不赘述。

积累，渗透到了云安全服务研发的每个毛细血管中，构筑了华为云多维立体、全栈防护的安全体系：2003 年，推出业界首款基于网络处理器（NP—Network Processor）的防火墙；2008 年，与赛门铁克（Symantec）合资成立华赛公司（Huawei-Symantec）安全产品线，专注安全领域；2011 年，成立安全能力中心，专攻研发安全能力；2012 年，华为网络安全产品国内市场占有率第一；2015 年，云安全解决方案及服务全面上线；2016 年，云安全全球化布局，密钥管理服务（KMS）和防 DDoS 攻击服务（Anti-DDoS）在德国、西班牙上线；2017 年，推出 DDoS 高流量防护（高防）、数据库防火墙等系列高增值安全服务；2018 年，推出专属加密服务（DHSM）。

网络安全和隐私保护是华为的最高纲领。华为云在此承诺：华为云以数据保护为核心，以云安全能力为基石，以法律法规业界标准遵从为城墙，以安全生态圈为护城河，依托华为独有的软、硬件优势，打造业界领先的竞争力，构建起面向不同区域、不同行业的完善云服务安全保障体系，并将其作为华为云的重要发展战略之一。华为云在遵从所有适用的国家和地区的安全法规政策、国际网络安全和云安全标准，参考行业最佳实践的基础上，从组织、流程、规范、技术、合规、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足云服务用户的安全需求。

图1-1 华为云安全防护框架



- 在组织方面，全球网络安全与隐私保护委员会（GSPC – Global Security & Privacy Committee）作为华为公司的最高网络安全管理机构，负责决策和批准公司总体网络安全战略。全球网络安全与用户隐私保护官（GSPO – Global Security & Privacy Officer）是 GSPC 的重要成员，负责领导团队制定安全战略，统一规划、管理和监

督研发、供应链、市场与销售、工程交付及技术服务等相关体系的安全组织和业务，确保网络安全保障体系在各体系、各区域、全流程的实施，积极推动与政府、客户、合作伙伴、员工等各利益相关方的沟通。华为云建立并完善其适合云服务持续集成、持续部署的扁平化组织。

- **在业务流程方面**，安全保障活动融入研发、供应链、市场与销售、工程交付及技术服务等各主业务流程中。安全作为质量管理体系的基本要求，通过管理制度和技术规范来确保其有效实施。华为通过内部审计和接受各国政府安全部门、第三方独立机构的安全认证和审计等来监督和改进各项业务流程。2004 年起，华为的安全管理体系通过了 BS7799-2/ ISO27001 认证。华为云在公司级的业务流程基础上，大胆地将已在华为全面采用的安全周期管理（SDL – Security Development Lifecycle）集成于当前适合云服务的 DevOps 工程流程和技术能力，形成有华为特色的 DevSecOps 方法论和工具链，既支撑云业务的敏捷上线，又确保研发部署的全线安全质量。
- **在人员管理方面**，华为云严格执行华为长期以来行之有效的人事和人员管理机制。华为全体员工、合作伙伴及外部顾问都必须遵从公司相关安全政策，接受安全培训，使安全理念融入整个组织之中。华为对积极执行网络安全保障政策的员工给予奖励，对违反的员工给予处罚，违反相关法律法规的员工，还将依法承担法律责任。
- **在云安全技术能力方面**，依托华为自身强大的安全研发能力，以数据保护为核心，开发并采用世界领先的云安全技术，致力于实现高可靠、智能化的云安全防护和自动化的云安全运维运营体系。同时，通过对现网安全态势的大数据分析，有目的地识别出华为云存在的重要安全风险、威胁和攻击，并采取防范、削减和解决措施；通过多维、立体、完善的云安全防御、监控、分析和响应等技术体系支撑云服务运维运营安全，实现对云安全风险、威胁和攻击的快速发现、快速隔离和快速恢复，让租户受益于华为云先进技术带来的便捷、安全与业务增值。
- **在云安全合规方面**，面向提供云服务的地区，华为云积极与监管机构对话，理解他们的担忧和要求，贡献华为云的知识 and 经验，不断巩固华为在云技术、云服务和云安全方面与相关法律法规的契合度。同时，华为也将法律法规的分析结果共享给租户，避免信息缺失导致的违规风险，通过合同明确双方的安全职责。华为一方面通过跨行业、跨区域的云安全认证满足监管机构要求，另一方面通过获得重点行业、重点区域所要求的安全认证，建立并巩固华为云业务的客户信赖度，最终在法律法规制定者、管理者、租户三者间共建安全的云环境。
- **在云安全生态方面**，华为云认识到单靠一个公司、一个组织的力量不足以应对日益

复杂的云安全威胁与风险。因此，华为云诚邀全球所有安全伙伴，携手共建云安全商业和技术生态体系，共同向租户提供安全保障与服务。华为云的云市场（Marketplace）欢迎具备技术竞争力的安全技术企业、组织和个人发布云安全服务；同时，华为云诚邀云业务商业合作伙伴，利用自身对云服务云安全行业的独到经验和见解，组合安全服务，形成行业级云安全解决方案。华为云愿意与所有志同道合的伙伴分享云安全市场。

同时，华为积极、持续地参与着国内外云安全组织和电信标准组织的安全标准制定，努力保障全球客户的安全，为行业的健康发展作出应有的贡献。

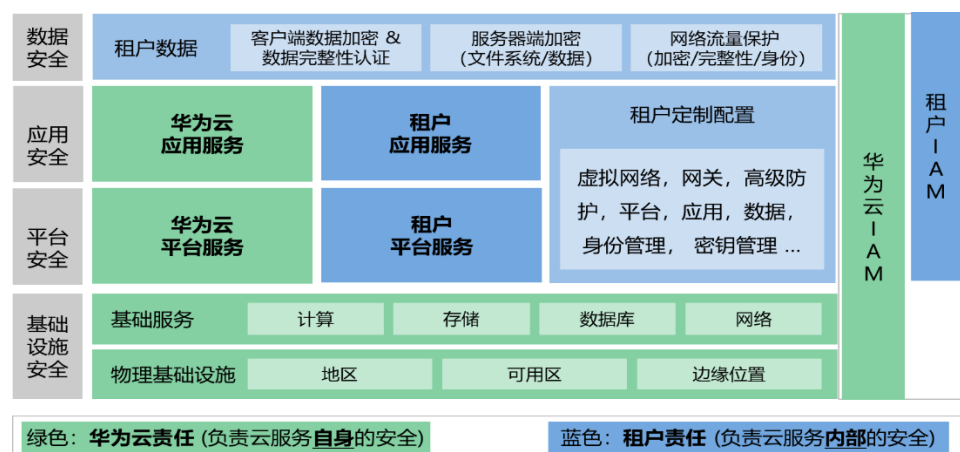
总之，华为愿意以开放透明的心态，与各国政府、客户、行业组织和行业伙伴开展各种形式的安全交流与合作，共同应对全球云安全的威胁与挑战！

2 责任共担模型

从传统数据中心的视角，云安全包括保护云服务本身在基础设施即服务（IaaS），平台即服务（PaaS）和软件即服务（SaaS）各类云服务以及云服务数据中心内部运维运营所需的技术资源，以确保各类应用和服务能够持续、高效、安全、稳定地运行。云服务与传统数据中心存在明显差异，前者对云安全整体设计和实践更侧重于为租户提供完善的、多维度的、按需要任意定制、组合的各种安全和隐私保护功能和配置，涵盖基础设施、平台、应用及数据安全等各个层面。同时，不同的云安全服务又进一步为租户提供了各类可自主配置的高级安全选项。这些云安全服务需要通过深度嵌入各层云服务的安全特性、安全配置和安全管控来实现，并通过可整合多点汇总分析的、日趋自动化的云安全运维运营能力来支撑。

我们在下面几章将讲述华为作为云服务供应商（CSP），如何实现如此复杂的云安全系统工程以及研发和运维运营的优秀安全实践。本章首先介绍华为云按业界常规做法定义的华为云服务安全责任共担模型，如下图：

图2-1 华为云安全责任共担模型



其中绿色部分为华为云负责，蓝色部分责任由租户承担。华为云负责云服务自身的安全，提供安全的云；租户负责云服务内部的安全，安全的使用云。

数据安全：指华为云中租户的业务数据自身的安全管理，包括数据完整性认证、加密、访问控制等。

应用安全：指在华为云中的支撑运维运营，以及支撑用户业务等应用系统的安全管理，包括应用的设计、开发、发布、配置和使用等。

平台安全：指在华为云中的微服务、管理、中间件等平台类的安全管理，包括平台的设计、开发、发布、配置和使用等。

基础服务安全：指华为云提供的计算、网络、存储等方面的安全管理，包括云计算、云存储、云数据库等服务的底层管理（如虚拟化控制层）和使用管理（如虚拟主机），以及虚拟网络、负载均衡、安全网关、VPN、专线链路等。

物理基础设施安全：华为云的区域、可用区和终端节点涉及机房、环境的安全管理，以及物理服务器和网络设备等设施的管理。

华为云的主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和 IAM 层的多维立体安全防护体系，并保障其运维运营安全。

租户的主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和 IAM 层的各项安全防护措施的定制配置，运维运营安全，以及用户身份的有效管理。

2.1 华为云的安全责任

华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 各类各项云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不但包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从（第 3.1 章节有专门介绍，在此不赘述）。

- 华为云一方面确保各项云技术的安全开发、配置和部署；另一方面，华为云负责所提供云服务的运维运营安全，例如，对安全事件实现快速发现、快速隔离、快速响应，确保云服务的快速恢复。同时采用适合云服务的漏洞管理机制，对云服务安全漏洞及时应急响应，保证适合 CSP 运维周期的快速发布和不影响租户服务的持续部署，包括不断优化云产品默认安全配置、补丁装载前置于研发阶段和灵活简化安全补丁部署周期等措施。另外，华为云的安全责任还表现在开发有强大市场竞争力、为华为云租户业务增值的云安全服务。
- 华为云将其基础设施的安全与隐私保护视为运维运营安全的重中之重。基础设施主要包括支撑云服务的物理环境，华为自研的软硬件，以及运维运营包括计算、存储、网络、数据库、平台、应用、身份管理和高级安全服务等各项云服务的系统设施。同时，华为云深度集成第三方安全技术或服务，并负责对其进行安全运维。
- 华为云还负责其支撑的各项云服务的自身安全配置和版本维护。
- 华为云对租户数据提供机密性、完整性、可用性、持久性、认证、授权、以及不可否认性等方面的全面数据保护功能，并对相关功能的安全性负责。但是，华为云只是租户数据托管者，租户对其数据拥有所有权和控制权。华为云绝不允许运维运营人员在未经授权的情况下访问租户数据。华为云关注内外部合规要求的变化，负责遵从华为云服务所必需的安全法律法规，开展所服务行业的安全标准评估，并且向租户分享我们的合规实践，保持应有的透明度。
- 华为云携手云安全商业合作伙伴向租户提供咨询服务，协助租户对虚拟网络，虚拟机（包括虚拟主机和访客虚拟机）的安全配置，系统和数据库安全补丁管理，虚拟网络的防火墙、API 网关（API GW – API Gateway）和高级安全服务的定制配置，DoS/DDoS 攻击防范，租户安全事件的应急响应以及灾难恢复。

2.2 租户的安全责任

华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类各项云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

- 租户的安全责任细节由最终所使用的云服务来决定，具体到租户负责执行什么默认和定制的安全配置。对于华为云的各项云服务，华为云只提供租户执行特定安全任务所需的资源、功能和性能，而租户需负责各项租户可控资源的安全配置工作。

- 租户负责部署配置其虚拟网络的防火墙，网关和高级安全服务等策略配置，租户空间的虚拟网络、虚拟主机和访客虚拟机等云服务所必需的安全配置和管理任务（包括更新和安全补丁）、容器安全管理、大数据分析等平台服务的租户配置，以及其他各项租户租用的云服务内部的安全配置等。租户也负责对其自行部署在华为云的任何应用程序软件或实用程序进行安全管理。
- 在配置云服务时，租户负责各项安全配置在部署到生产环境前做好充分测试，以免对其应用和业务造成负面影响。对大多数云服务的安全性而言，租户只需配置账户对资源的访问控制并妥善保管账户凭证。少数云服务需要执行其他任务，才能达到应有的安全性，例如使用数据库服务时，在华为云执行数据库整体安全配置的同时，租户还需设置用户账户和访问控制规则。各项监控管理服务和高级安全服务具有较多安全配置选项，租户可寻求华为云和其合作伙伴的技术支持，以确保安全性。
- 无论使用哪一项华为云服务，租户始终是其数据的所有者和控制者。租户负责各项具体的数据安全配置，对其保密性、完整性、可用性以及数据访问的身份验证和鉴权进行有效保障。在使用统一身份认证服务（IAM）和数据加密服务（DEW）时，租户负责妥善保管其自行配置的服务登录账户、密码和密钥，并负责执行密码密钥设定、更新和重设规则的业界优秀实践。租户负责设置个人账户和多因子验证（MFA），规范使用安全传输协议与华为云资源通信，并且设置用户活动日志记录用于监测和审计。

租户负责对其自行部署于华为云上、不属于华为云提供的各项应用和服务所必需的安全法律法规，并自行开展所服务行业的安全标准评估。

3 安全合规与隐私保护

华为云一贯高度重视并持续增加在提高客户信任方面的投入。而安全合规与标准遵从正是获得并维护客户信任的必由之路，同时也是防范“内鬼”破坏的重要手段。通过业界通用的安全合规与标准遵从的认证，既能提升华为云的整体安全能力和业务水平，也能帮助客户减少对合规和数据安全的担忧。同时，华为云始终秉持“以客户为中心”的核心价值观，充分理解客户个人数据安全的重要性，尊重和保护客户隐私权利，并将“尊重和保护隐私，让人们放心地享受万物互联的智能世界”作为隐私保护的愿景。华为云郑重对待并积极承担相应责任，把网络安全和隐私保护作为最高纲领，保证网络安全和隐私保护需求优先获得资源支持。

3.1 安全合规与标准遵从

华为云一如既往地确保其基础设施和云服务通过业界认可的独立第三方安全权威组织的测评以及安全认证机构的审核，并且只向客户提供运行于安全合规的基础设施之上的云服务。这些安全测评和认证向客户展示华为云在基础设施和云服务的技术研发和运维运营中对流程、组织、技术等多方面制定的安全策略和安全风险管控措施，使得客户能够深入了解华为云对用户数据保护和云上业务安全保障的有效管控能力。以华为云通过的云安全联盟 CSA STAR 金牌认证为例（CSA- Cloud Security Alliance, STAR- Security, Trust & Assurance Registry），该认证在 ISO/IEC 27001 的基础上，增加了云安全控制矩阵（CCM - Cloud Control Matrix）和其他安全要求，涵盖了风险治理、数据安全、应用安全、基础设施安全、开发和设计、身份和访问管理、数据中心安全、变更管理、配置管理、业务连续性管理、运营恢复能力、人力资源、供应链管理等方面的 16 个控制领域。

同时，基于华为云服务的安全责任共担模型，华为云通过主动构建并不断提升包括物理

环境、网络、平台等各层基础设施的安全合规能力，保障云租户所部署业务的安全与合规。

目前，华为云的安全测评及认证有：

- GB 50174《电子信息机房设计规范》A 类
- TIA 942《数据中心机房通信基础设施标准》T3+ 标准
- CSA STAR 金牌认证
- ISO/IEC 27001
- ISO/IEC 27017
- CC EAL3+（通用准则评估保证级 3+）³
- PCI DSS（支付卡行业数据安全标准）⁴
- BSIMM（软件安全构建成熟度模型）
- 中国公安部信息安全等级保护三级/四级⁵
- 中国数据中心联盟（DCA–Data Center Alliance）可信云服务认证、金牌运维，其中云主机获取最高级五星+认证
- 中国国家互联网信息办公室网络安全审查
- ITSS 云计算服务能力评估一级（增强级）
- SOC1 Type2 / SOC2 Type2
- ISO 27018
- ISO 20000
- ISO 22301
- MTCS Level 3（新加坡多层云安全认证最高评级）

另外，华为云主动识别并遵从业界优秀安全实践。例如，华为云参考互联网安全中心（CIS – Center of Internet Security）安全基线并将其融入华为云服务 DevSecOps 流程。CIS 安全基线是一套用于网络系统安全配置和操作的业界优秀实践，覆盖技术（软件、硬件）、

³ 华为云操作系统已获得 CC EAL3+ 认证证书，并在申请 CC EAL4+ 认证。

⁴ PCI DSS (Payment Card Industry Data Security Standard) 即支付卡行业数据安全标准，对使用主要支付卡品牌执行信用卡和现金卡收付功能的组织提供信息安全标准。

⁵ 华为云部分节点通过四级评测

流程（系统和网络管理）、人员（最终用户和管理行为），标志着华为云在安全合规与标准遵从上一如既往地与业界看齐。

3.2 隐私保护

华为云秉承公司以网络安全和隐私保护为最高纲领，以国内外隐私保护的法律法规为基石，依托于华为公司的隐私保护体系，借鉴业界广泛认可的优秀实践，已形成适合华为云的隐私保护体系。华为云投入大量的专业人员和资源支撑新技术的研究和应用以及保障隐私保护体系的有效运转，确保华为云的隐私保护处于行业领先的位置，实现华为云隐私保护的目标：遵守严格的服务边界，保护客户个人数据安全，助力客户实现隐私保护。

华为云建立完善、规范和统一隐私保护体系确保云平台的隐私保护得以实现，并帮助客户实施隐私保护。华为云制定隐私保护七大原则（合法、正当、透明，目的限制，数据最小化，准确性，存储期限最小化，完整性与保密性，可归责），同时采用业界认可和先进的理念 PbD⁶（Privacy by Design）作为指导，结合华为云实际情况形成华为云隐私保护理念。隐私保护理念广泛应用在华为云的组织和人员管理、云平台个人数据安全以及为客户提供的隐私服务等各个方面。同时，华为云使用 PIA⁷（Privacy Impact Assessment）识别隐私风险并采取恰当的方式消除或降低风险。华为云尊重用户的隐私权利，在官网明显处提供清晰的《隐私政策声明》以及客户反馈通道，帮助客户了解华为云隐私保护的信息。

华为云研究团队同时致力研发各类隐私增强技术（PET–Privacy Enhancing Technology），积累隐私保护工程技术能力，以满足客户不同需要实施隐私保护。华为云现已拥有的一系列 PET，包括等价类匿名、差分隐私、防跟踪技术、区块链私人支付以及隐私保存计算等。

更多关于华为云隐私保护的政策和表述，可以在华为云的官方网站找到。

⁶ 最早作为针对产品研发周期隐私保护的方法。经过近几年的发展，逐渐演变成隐私保护的管理理念。PbD 提倡全面、提前、主动将隐私保护融入业务和各项活动中，帮助组织在隐私保护中取得主动地位。

⁷ 隐私影响评估作为业界通用的隐私评估与设计工具被广泛使用和认可。PIA 帮助组织识别并减少业务的隐私风险，识别和最小化潜在隐私风险的过程

4 安全组织和人员

为了让所有员工不断提升安全意识，更好地保障客户利益和产品与服务信誉，华为在公司内部倡导“人人懂安全”的理念和实践，创造了一个无时不在，无处不在，充满活力和竞争力的安全文化。这种文化的影响贯穿在华为云招聘选才、员工入职、上岗培训、持续培训、内部调动和离职等各个环节。每位华为云的员工都积极参与建立并保持华为云安全，并按公司及华为云规定实施各项安全活动。

4.1 安全组织

华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。在组织方面，GSPC 作为最高网络安全管理机构，决策和批准公司总体网络安全战略。GSPO 及其办公室负责制定和执行华为端到端网络安全保障体系。GSPO 直接向公司 CEO 汇报。

秉承华为网络安全战略和规范，华为云安全团队对本领域安全工作进行自主规划和管理。全面实现云服务业务和云安全业务的研发运维运营组织合一，组织结构趋于扁平化，以便适应云服务必需的 DevOps/DevSecOps 流程。扁平化的组织结构和适应云服务的流程一方面满足云服务快速持续集成、交付与部署的进度要求，另一方面保证云服务达到必需的安全质量标准，有效控制安全风险。依托云服务安全工程能力、云安全服务与解决方案的设计和开发、云服务安全运维运营等职能，构建华为云服务的安全合规遵从和安全运维运营能力，切实保障华为云租户利益。基于云安全对华为云的特殊重要性，云安全团队直接向华为云总裁汇报。

4.2 安全与隐私保护人员

华为的安全技术团队包括全球各地业界优秀的信息安全、产品安全、应用安全、系统安

全、网络安全、云服务安全、运维运营安全、隐私保护等方面的专家专才。华为云安全团队的主要职责如下：

- 开发并执行云服务 DevOps/DevSecOps 流程和云安全审计流程，开发推广全流程安全工具链；
- 积极实施安全质量保证和安全评估，开展内部和第三方渗透测试和安全评估，监控、排查并解决安全威胁；
- 构建、开发、运维运营华为云基础设施安全防护体系，商务和 IT 应用以及对数据和知识产权的安全管控和隐私保护；
- 构建、开发、运维运营华为云的 IaaS、PaaS 和 SaaS 各类各项服务的安全功能和整体云安全解决方案；
- 遵从各行业、各区域、各国政府的数据隐私保护法律法规要求，倡导云技术、云服务的隐私保护最佳实践，推动发布符合隐私保护标准的云技术、云服务；
- 制定和发展可持续云安全技术及业务生态。

4.3 内部审计人员

华为内部审计团队直接向董事会和公司高层管理者汇报，严格的审计活动在推动网络安全流程和标准落地，保障结果交付上起着关键的作用。

华为建立了专门的安全审计团队，审查全球安全法律法规及公司内部安全要求的遵从情况。审计团队每年投入 10+ 人力对全球范围运营的华为云至少开展 1 次，为期 2 个月的审计，重点关注华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上的风险。

审计结果向董事会和公司高层管理者汇报，保证发现的问题得到解决并最终闭环。

4.4 人力资源管理

华为云安全的人力资源管理框架和公司的整体人力资源管理框架一致，都是建立在法律基础之上。云安全对 HR 的诉求主要是保证我们的员工背景和资历适合华为云业务的需要。员工行为符合所有法律、政策、流程以及华为商业行为准则的要求。员工有履行其职责必备的知识、技能和经验。整体模型如下：（此模型较为简明，故不赘述）

图4-1 华为云安全融入人力资源流程



4.4.2 安全意识教育

为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为从意识教育普及、宣传活动开展、BCG 及承诺书签署三个方面开展安全意识教育：

- **意识教育普及：**定期开展网络安全意识教育学习，要求员工持续学习网络安全知识，了解相关的政策和制度，知道哪些行为是可以接受，哪些是不能接受的，意识到即使主观上没有恶意，也要对自己的行为负责，并承诺按要求执行；
- **宣传活动开展：**面向全员开展形式多样的网络安全宣传活动，包括网络安全社区运营、网络安全典型案例宣传、网络安全活动周、网络安全动画宣传片等；
- **BCG 及承诺书签署：**将网络安全纳入《华为员工商业行为准则》（BCG – Business Conduct Guide），通过公司统一开展的年度例行 BCG 学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识。签署网络安全承诺书，承诺遵守公司各项网络安全政策和制度要求。

4.4.3 网络安全能力提升

参考业界优秀实践，华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，确保员工有能力向客户交付安全、合规的产品、解决方案与服务。

- **网络安全基础培训：**华为根据不同角色、岗位制定相应的安全基础能力培训计划。

新员工转正前必须通过有关网络安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试。管理者需参加网络安全必须的培训和研讨。

- **精准培训：**通过大数据分析识别产品研发过程中的典型安全问题和问题关联责任人，并向其精准推送安全典型培训方案（包括案例、培训课程、练习题等），持续改进安全质量。
- **实战演练：**引进业界优秀实践，开发网络安全实战演练平台，开展红蓝对抗，提供场景化的实战演练环境供员工练习和交流，提升员工的安全技能。
- **安全能力任职牵引：**为了让员工更加自觉、有效地进行网络安全学习，华为将网络安全要求融入到任职资格标准中。员工在任职晋升过程中需要学习相应的网络安全课程，通过相应的网络安全技能考试，提升自身网络安全能力。

4.4.4 重点岗位管理

为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，华为云对运维工程师等重点岗位实施专项管理。具体如下：

- **上岗安全审查：**针对新上岗人员，开展上岗人员安全审查，确保上岗人员背景和资历符合云安全业务要求。
- **在岗安全培训赋能：**围绕网络安全意识、客户网络服务的业务规范、用户数据及隐私保护要求进行网络安全学习和考试，并根据业务变化定期刷新学习和考试大纲。
- **上岗资格管理：**重点岗位员工必须通过网络安全上岗证的考试，并取得证书。通过证书管理平台对已通过安全上岗证考试的员工发放有效期不超过两年的电子证书，证书到期前提醒员工重新参加考试。
- **离岗安全审查：**按照调动、离职安全审查清单，对内部调离、离职人员进行离岗安全审查，包括离岗权限账号的清理或修改等。

4.5 安全违规问责

华为建立了严密的安全责任体系，贯彻违规问责机制。一方面，华为云恪守责任共担模型，履行华为云的各项责任，对华为云一方造成的安全违规，华为云对租户直接负责，最大限度控制对租户业务的影响。另一方面，华为云要求每个员工都对自己工作中的行为和结果负责，不仅要对技术和服务负责，也要承担法律的责任。华为云员工深知，安

全问题一旦发生，可能会对租户、公司带来极大影响。因此不管故意还是无意，华为云都会以行为和结果为主要依据对员工进行问责。根据华为云员工安全违规的性质，以及造成的后果确定问责处理等级，分级处理。对触犯法律法规的，移送司法机关处理。直接管理者和间接管理者存在管理不力或知情不作为的，须承担管理责任。违规事件处理根据违规个人态度与调查配合情况予以加重或减轻处理。

5 基础设施安全

华为云将基础设施安全视为构筑多维全栈的云安全防护体系的核心组成部分，没有安全合规与标准遵从的基础设施安全，云服务安全犹如在流沙上建楼，为租户业务赋能增值、为租户安全保驾护航即刻化作空谈。对于云服务租户而言，CSP 基础设施的透明度和开放度较低，直接影响 CSP 的云安全可信度。第三方评测机构的安全合规和标准遵从认证，能够反映 CSP 在基础设施安全和云服务安全方面做出的不懈努力。通过华为云构筑安全的基础设施底座，租户可以更放心地上云并利用安全的华为云服务更聚焦在业务发展上。本章介绍华为云安全防护体系中的物理环境、网络、平台、应用程序接口（API—Application Programming Interface）和数据等主要方面的安全设计和实践。

5.1 物理与环境安全

华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中的 T3+ 标准。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以确保华为云数据中心的物理和环境安全。

5.1.1 物理安全

- **机房选址：**华为云数据中心机房选址一定程度上决定面临的自然灾害以及可能的环境威胁。华为云数据中心选址一律避开自然灾害不利或危险的地区，减少周边环境对数据中心产生的干扰，如 400 米内无实验室、化工厂等危险区域。同时，选址上

保证了数据中心正常运营需要的配套资源，如市电、水、通信线路等。

- **访问控制：**华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了全天候（一天 24 小时、一周 7 天，即 7*24 小时）保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。
- **安保措施：**华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行 7*24 小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。

5.1.2 环境安全

- **电力保障：**华为云数据中心采用多级保护方案保障业务 7*24 小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源（UPS – Uninterrupted Power Supply），提供短期备用电力供应。在机房供电线路上配置了稳压器和过压防护设备。在供电设备及线路上还设置冗余或并行的电力电缆线路为计算机系统供电。
- **温湿度控制：**通过精密空调、集中加湿器自动调节，华为云数据中心机房温湿度保持在设备运行所允许的范围内，使设备元器件处于良好运行状态。机柜冷热通道有合理的布置，利用架空地板下空间作为静压箱来给机柜送风，并设置了冷通道密闭，以防止局部热点。
- **消防能力：**华为云数据中心建筑防火等级均按一级设计施工，使用了 A 级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统，得以控制火情。
- **例行监控：**华为云数据中心的电力、温湿度、消防等环境运行状态通过日常巡检制度得到例行监控，安全隐患能被及时发现并修复，确保设备稳定运行。

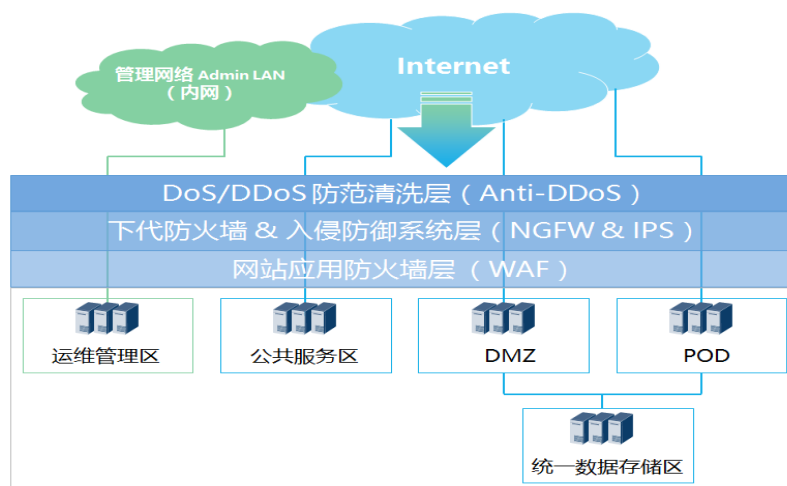
- **供水排水：**华为云数据中心的供水和排水系统均有合理规划，保证了总阀门正常可用，确保关键人员知晓阀门位置，以免信息系统受到漏水事故破坏。机房建筑和楼层均有抬高场地，在外围设置了绿化地排水沟，加速排水，以降低场地积水倒灌风险。建筑满足防水一级标准，保证了雨水不能通过屋顶、墙壁向机房渗透。数据中心也配备了及时排水的设施，供水灾时使用。
- **防静电：**华为云数据中心机房铺设了防静电地板，导线连接地板支架与接地网，机器接地以导走静电。在机房大楼顶部设置了避雷带，供电线路安装了多级避雷器，导走电流。

5.2 网络安全

华为云数据中心节点众多、功能区域复杂。为了简化网络安全设计，阻止网络攻击在华为云中的扩散，最小化攻击影响，华为云参考 ITU E.408 安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域、业务层面的划分和隔离。安全区域内的节点具有相同的安全等级。华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。

5.2.1 安全区域划分与隔离

图5-1 华为云平台安全域划分及网络边界保护



华为云根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力⁸。在这里介绍以下五个重要安全区域：

- **DMZ 区：**华为云 DMZ 区主要部署了面向外网和租户的前置部件，如负载均衡器、代理服务器等，以及服务部件，如服务控制台、API 网关等。租户对 DMZ 区的访问行为不可信，所以需要 DMZ 单独隔离，防止外部请求接触云服务后端部件。此区域部件面临极高安全风险，除部署了防火墙、防 DDoS 措施外，还部署了应用防火墙（WAF）及入侵检测与拦截设备（IDS/IPS）以保护基础网路、平台及应用。
- **公共服务区（Public Service）：**该区域主要部署 IaaS/PaaS/SaaS 服务化组件如级联层 OpenStack、IaaS/PaaS/SaaS 服务控制部件，以及一些基础设施服务部件如 DNS、NTP、补丁服务等。此区域内的部件根据业务需要受限开放给租户，且租户访问此区域部件和服务必须经过 DMZ 区。华为云管理员可以从内网区访问该区域进行操作和管理。
- **资源交付区（POD – Point of Delivery）：**此区域提供租户所需的基础设施资源，包括计算、存储、网络资源，如租户虚拟机、磁盘、虚拟网络。租户之间通过多层安全控制手段实现资源隔离，租户不能访问其它租户的资源；平台侧管理平面、数据存储平面隔离，且与租户数据平面隔离。该区域还可以支撑对进出互联网的租户流量做 DDoS 防护及入侵检测与防御，保障租户业务。
- **数据存储区（OBS – Object-Based Storage）：**此区域部署对象存储系统，提供对象存储服务，存储租户隐私数据，所以进行了分区隔离。在该区域边界由租户在华为云提供的安全组件上配置执行租户所需的访问控制规则，在任意租户空间访问该区域时就不需要绕道 DMZ。但从外网访问，因为安全风险高，所以必须通过 DMZ 的服务控制台或网关才能访问该区。
- **运维管理区（OM – Operations Management）：**该区域主要部署操作运维部件，华为云运维人员必须先通过虚拟专用网络（VPN – Virtual Private Network）接入该区域，再通过堡垒机访问被管理节点。管理员可从此区域访问所有区域的运维接口。此区域不向其他区域开放接口。

⁸ 华为云数据中心不同传统 IT 数据中心，因此在实现区域隔离上与传统手段不尽相同，不再是简单地使用防火墙实现，也会运用革新技术，如软件定义边界（SDP – Software Defined Perimeter）。并且，不止定义网络层区域边界，采用多层边界划分与隔离协防，从网络层、平台层、应用层一直到用户身份层，都有信任边界和相应的访问控制。这里介绍的网络层安全区域只是多维全栈防护体系的一部分。

除了上述网络分区，同时也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制。

5.2.2 业务平面划分与隔离

为保证租户业务不影响管理操作，确保设备、资源和流量不会脱离有效监管，华为云将其网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、BMC（Baseboard Management Controller）管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，便于实现职责分离。

- **租户数据平面**：作为租户提供业务通道和虚拟机之间通信平面，租户对其用户提供业务应用。
- **业务控制平面**：支撑云服务 API 的安全交互。
- **平台运维平面**：实现基础设施和平台（网络设备、服务器、存储）的后台运维管理。
- **BMC 管理平面**：作为云平台基础设施服务器的硬件后端管理平面，用于应急维护。
- **数据存储平面**：仅供 POD 区内计算节点与存储节点间的数据安全传输与存储。

在每个安全区域内，根据所承载业务的隔离要求划分不同网络平面，如 POD 区有租户数据平面、平台运维平面、业务控制平面、BMC 管理平面，而运维区只有平台运维平面和 BMC 管理平面。安全区域与业务平面并用形成更多层面的、既有物理又有逻辑控制的多维度隔离，而这还只是华为云全栈防护的一部分。

5.2.3 高级边界防护

华为云高效的多维全栈防护体系也包括多种边界防护措施，这不仅仅有上述主要通过传统网络技术和防火墙实现的安全区域和业务平面的划分与隔离，还包括了得益于华为自研的各项高级边界防护功能。华为云已将各项高级防护功能按需适配到华为云外网边界和内网的区域间的信任边界。对华为自研的几项主要高级边界防护功能⁹，简介如下：

⁹ 作为高级边界防护的主要技术之一，防火墙技术已经成熟，得到广泛使用，并且在白皮书第 6 章 6.1.1 弹性计算服务（ECS）和 6.2.1 虚拟私有云服务（VPC）中有具体介绍，在此不做赘述。

- **DDoS 异常和超大流量清洗：**在每个云数据中心边界部署华为专业的 Anti-DDoS 设备来完成对异常和超大流量攻击的检测及清洗。Anti-DDoS 设备还可以为租户提供精细化的 DDoS 防护服务，租户可以根据业务的应用类型，配置流量阈值参数，并查看攻击和防御状态。
- **网络入侵检测与拦截**（IDS/IPS – Intrusion Detection System / Intrusion Prevention System）：为了感知来自互联网以及租户虚拟网络之间东西向的攻击，并针对攻击实施阻断，华为云在网络边界部署了 IPS 设备，包括但不限于外网边界、安全区域边界和租户空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS 可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。
- **Web 安全防护：**华为云部署了 Web 应用防火墙应对 Web 攻击，如 Web 应用层的 DDoS 攻击、SQL 注入、跨站脚本攻击（XSS - Cross-Site Scripting）、跨站请求伪造（CSRF – Cross-Site Request Forgery）、组件漏洞攻击、身份伪造等，以保护部署在 DMZ 区、面向外网的 Web 应用服务和系统。

5.3 平台安全

作为华为云平台操作系统，华为统一虚拟化平台（UVP - Unified Virtualization Platform）通过对服务器物理资源的抽象，将 CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。在中国可信云认证中，华为云平台的云主机获得最高级的五星+认证。

为保证平台安全，华为云对主机操作系统进行最小化裁剪并对服务做安全加固。同时，对接入主机操作系统的华为云管理员执行严格的权限访问控制（PAM – Privilege Access Management），对其所执行的各项运维运营操作实行全面的日志审计。华为云管理员必须经过双因子认证后，才能通过堡垒机接入管理平面，所有操作都会记录日志并及时传送到集中日志审计系统。

UVP 直接运行于物理服务器之上，提供虚拟化能力，为虚拟机提供运行环境。UVP 需要保证虚拟机运行在合法的空间内，避免某个虚拟机对 UVP 或其他虚拟机发起攻击。

UVP 通过 CPU 隔离、内存隔离和 I/O 隔离等技术手段实现虚拟主机操作系统与访客虚拟机操作系统之间的隔离，并通过 Hypervisor 让虚拟主机操作系统与访客虚拟机操作系统使用不同的权限运行，来保证平台系统资源的安全。

以下分别从 CPU、内存和 I/O 隔离三个方面介绍 UVP 的资源安全隔离实现机制。

5.3.1 CPU 隔离

CPU 隔离主要是指虚拟化平台与虚拟机之间的隔离，虚拟机内部的权限分配和虚拟机与虚拟机之间的隔离。CPU 隔离是通过 Root 和 Non-Root 两种运行模式的切换、各运行模式下的运行权限分配以及以 VCPU（Virtual CPU）的形式呈现的虚拟计算资源的分配与切换等方式来实现的。通过 CPU 隔离机制，UVP 可以控制虚拟机对物理设备以及虚拟化运行环境的访问权限，从而实现虚拟化平台与虚拟机之间以及不同虚拟机之间在信息和资源上的隔离，也就是说，一个虚拟机无法获取到其他虚拟机或虚拟化平台的信息和资源。

5.3.2 内存隔离

虚拟化平台还负责为虚拟机提供内存资源，保证每个虚拟机只能访问到其自身的内存。为实现这个目标，虚拟化平台管理虚拟机内存与真实物理内存之间的映射关系。保证虚拟机内存与物理内存之间形成一一映射关系。虚拟机对内存的访问都会经过虚拟化层的地址转换，保证每个虚拟机只能访问到分配给它的物理内存，无法访问属于其他虚拟机或虚拟化平台自身使用的内存。

5.3.3 I/O 隔离

虚拟化平台还给虚拟机提供了虚拟 I/O 设备，包括磁盘、网卡、鼠标、键盘等。虚拟化平台为每个虚拟机提供独立的设备，避免多个虚拟机共享设备造成的信息泄露。

每个虚拟磁盘对应虚拟化平台上的一个镜像文件或逻辑卷，虚拟化平台控制只有一个虚拟机的一个虚拟磁盘设备跟一个镜像文件关联。实现了虚拟机使用的虚拟设备与虚拟化平台 I/O 管理对象之间一一对应的关系，保证虚拟机之间无法相互访问 I/O 设备，实现 I/O 路径的隔离。

5.4 API 应用安全

华为云各服务可通过公开的 API 进行配置管理，对接企业已有的 IT 管理和审计系统。考虑到 API 对云服务承载的重要功能和其在 HTTP 应用层面面临的安全威胁，业界普遍把 API 视为云服务至关重要的安全边界，采用多重机制和措施进行重点保护。调用华为云开放的 API 是通过华为自研的 API 网关实现的。API 网关支持以下机制和场景使 API 得到有效保护：

- **身份认证及鉴权：**华为云对每个 API 请求通过与华为云 IAM 的集成进行身份验证，确保只有经过身份验证的用户才能访问和管理云监控信息，且传输通道通过 TLS 加密。

租户通过 API 命令接口来管理虚拟机，API 命令的权限管理直接关系到虚拟机的安全性。华为云 API 网关对用户命令支持二级权限管理。用户发出命令时，不仅需要 IAM 的身份登录和鉴权，而且命令也需要经过 API 网关的检查鉴权。用户有权限执行该命令时，命令才可以通过 API 网关并下发到平台层或应用层执行。平台层或应用层接到命令后，会再次对用户的权限进行检查判断，只有用户确实拥有当前 API 命令的执行权限，命令才允许执行。

所有的访问请求可以通过两种方式认证：

- **令牌 (token) 认证：**认证请求会包含一个认证的 token，该 token 由租户通过使用 IAM 注册的用户名及密码调用 IAM 接口获取。
- **访问密钥 ID / 访问密钥 (AK/SK – Access Key ID / Secret Access Key) 认证：**认证请求会包含 AK/SK 的鉴权信息，API 网关的 AK/SK 鉴权机制要求客户端在获取 AK/SK 信息后，通过 API 网关发布的官方 SDK 进行签名，将包含签名信息的请求发送到 API 网关，API 网关将对签名信息进行认证校验。
- **传输保护：**API 调用需使用 TLS 加密以保证传输的机密性。目前 API 网关所有对外网开放的 API 均使用 TLS 1.2 版本加密协议，并且支持 PFS (Perfect Forward Secrecy) 安全特性。
- **边界防护：**API 网关结合 Anti-DDoS、入侵防御系统 (IPS) 和 Web 应用防火墙 (WAF) 等多层高级边界防护机制针对不同的威胁和攻击进行有效防范。通过负载均衡器对 TLS 加密传输进行解密，多层高级边界防护机制可对 API 网关流量明文进行监控，对攻击执行阻断。在高级边界防护的基础上，API 网关作为云服务特有的安全边界还提供以下多种防护措施：
 - **API 注册：**只有在 API 网关上注册的 API 接口，才能被租户访问。

- **ACL 规则限制:** 该功能允许租户自行配置特定的租户信息和网段信息。租户可根据访问控制列表（ACL – Access Control List）配置信息，API 网关能有限开放 API 给特定租户访问，或者有限开放 API 从特定网段访问，同时 ACL 规则默认限定管理域账号（op_service）防止从外部网络调用管理域接口。
- **防重放攻击:** 当 API 网关接受过期请求时，将会执行拒绝措施防止重放攻击。
- **防暴力破解:** 当接受某个 AK/SK 请求时，API 网关的防暴力破解机制一旦监测到失败请求次数已超出 API 网关所设定允许次数，会拒绝该请求并执行限时锁定。
- **API 流量控制:** API 网关实现对用户调用 API 的频率的适当流量控制，确保基于 API 的访问的高可用性和连续性。API 网关提供针对 API 级别和租户级别的秒级流控配置。每个开放的 API 在 API 网关需要配置对应的流控信息，在单位时间内，每个 API 基于所有华为云租户调用该 API 次数的配额、每个华为云租户调用该 API 次数的配额分别进行流控。

5.5 数据安全

数据安全指对用户数据信息资产的机密性、完整性、可用性、持久性、以及可追溯性等方面的全面保护。华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为用户提供最切实有效的数据保护能力，保证租户对其数据的隐私权、所有权和控制权不受侵犯。

5.5.1 访问隔离

- **身份认证和访问控制:** 华为云的访问控制能力是通过统一身份认证服务（IAM – Identity and Access Management）提供的。IAM 是面向企业租户的安全管理服务，通过 IAM，租户可以集中管理用户、安全凭证（例如访问密钥），以及控制用户管理权限和用户可访问的云资源权限。

使用 IAM，租户管理员可以管理用户账号，并且可以控制这些用户账号对租户名下资源具有的操作权限。当租户企业存在多用户协同操作资源时，使用 IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全，从而降低租户的企业信

息安全风险。

- **数据隔离：**华为云对云端数据的隔离是通过虚拟私有云（VPC – Virtual Private Cloud）实施的，VPC 采用网络隔离技术，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN 或云专线，将 VPC 与租户内网的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足租户更细粒度的网络隔离需要。

5.5.2 传输安全

对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过如下方式提供：

- **虚拟专用网络（VPN）：**VPN 用于在远端网络和 VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云上，为租户提供端到端的数据传输机密性保障。通过 VPN 在传统数据中心与 VPC 之间建立通信隧道，租户可方便地使用华为云的云服务器、块存储等资源，通过将应用程序转移到云中、启动额外的 Web 服务器来增加网络的计算容量，实现了企业的混合云架构的同时，也降低了企业核心数据非法扩散的风险。

目前，华为云采用硬件实现的 IKE（密钥交换协议）和 IPSec VPN 结合的方法对数据传输通道进行加密，确保传输安全。

- **应用层 TLS 与证书管理：**华为云服务提供 REST 和 Highway 方式进行数据传输：REST 网络通道是将服务以标准 RESTful 的形式向外发布，调用端直接使用 HTTP 客户端，通过标准 RESTful 形式对 API 进行调用，实现数据传输；Highway 通道是高性能私有协议通道，在有特殊性能需求场景时可选用。上述两种数据传输方式均支持使用传输层安全协议（TLS – Transport Layer Security）1.2 版本进行加密传输，同时也支持基于 X.509 证书的目标网站身份认证。

证书管理服务（SSL Certificate Service）则是华为云联合全球知名数字证书服务机构，为租户提供的一站式 X.509 证书的全生命周期管理服务，实现目标网站的可信身份认证与安全数据传输。

5.5.3 存储安全

- **密钥保护与管理**

密钥管理服务（KMS – Key Management Service）是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM – Hardware Security Module），为租户创建和管理密钥，防止密钥明文暴露。HSM 之外，从而防止密钥泄露。HSM 是一种安全产生、存储、管理及使用密钥并提供加密处理服务的硬件设备。为保护租户密钥安全，减少密钥外泄风险，华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云 HSM 供租户选择，满足不同租户的实际需求，例如通过 FIPS140-2 国际权威认证的第三方 HSM。KMS 对密钥的所有操作都会进行访问控制及日志跟踪，满足审计和合规性要求。目前已对接 KMS 服务的华为云服务包括：云硬盘（Elastic Volume Service，简称 EVS）、对象存储（Object Storage Service，简称 OBS）、云硬盘备份（Volume Backup Service，简称 VBS）及镜像服务（Image Management Service，简称 IMS）等。

• 专属加密

专属加密满足租户更高合规性要求的加密场景，采用通过国家密码局认证或 FIPS 140-2 第 3 级验证的硬件加密机，对租户业务进行专属加密，默认双机架构以提高可靠性。

• 数据机密性及可靠性保证

华为云针对各存储服务提供数据保护功能和建议，具体见下表：

表5-1 华为云存储服务机密性与可靠性概览

存储类型	服务描述	机密性保证	可靠性保证
EVS	云硬盘是一种基于分布式架构的、可弹性扩展的虚拟块存储服务。	KMS 提供密钥。用户主密钥（CMK - Customer Master Key）由 KMS 生成、管理和销毁，用于加密和解密数据加密密钥。华为云提供整卷加密功能。	三副本冗余，数据持久性高达 99.9999999%。 通过 VBS 实现云硬盘的备份与恢复，且支持通过云硬盘备份创建新的云硬盘。
VBS	云硬盘备份为 EVS 创建备份，利用备份数据回滚 EVS 数据。	加密盘的备份数据自动加密，保证数据安全。	备份数据跨数据中心保存，数据持久性高达 99.999999999%。

存储类型	服务描述	机密性保证	可靠性保证
OBS	对象存储服务是一种基于对象的海量存储服务，为用户提供海量、低成本、高可靠、高安全的数据存储能力。	对于服务器端加密，OBS 提供两种密钥管理方式： 用户提供密钥（SSE¹⁰-C 方式）：OBS 使用用户提供的密钥和密钥的 MD5 值进行服务端加密。 KMS 托管密钥（SSE-KMS 方式）：由 KMS 提供密钥。用户向区域中的桶上传对象时，OBS 将自动创建用于加密和解密数据的 CMK。	数据持久性高达 99.999999999%，服务可用性达 99.995%。 数据检查：存储前和存储后通过 Hash 校验数据一致性，确保存入数据是上传数据。 分片冗余：数据分片后多份冗余存储在不同磁盘，后台自行检测一致性并及时修复受损数据。
RDS	关系型数据库服务（Relational Database Service，简称 RDS）是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线关系型数据库服务。	通过静态加密、表空间加密、同态加密对数据进行加密。华为云关系型数据库服务支持对存储到数据库中的数据加密后存储，加密密钥由 KMS 进行管理。	关系型数据库服务采用热备架构，故障系统 1 分钟自动切换。每天自动备份数据，上传到 OBS 桶，备份文件保留 732 天，支持一键式恢复。
IMS	镜像服务提供灵活的自助服务和完善的镜像管理能力，用户可以从丰富的公共镜像库中选择或创建私有镜像，快速创建或批量复制弹性云服务器。	由 KMS 提供密钥。CMK 由 KMS 生成、管理和销毁，用于加密和解密数据加密密钥。华为云提供两种方式创建加密镜像：通过加密弹性云服务器创建和通过外部镜像文件创建。	使用多份冗余存储私有镜像，数据持久性高达 99.999999999%。

5.5.4 数据删除与销毁

在用户确认删除数据后，华为云会彻底删除用户数据，确保数据不泄露：

- **内存删除：**华为云在云操作系统将内存重新分配给用户之前，会对分配的内存进行

¹⁰ SSE – Server-Side Encryption. C 在 SSE-C 中是指客户（customer）。

清零操作，即写“零”处理，防止通过物理内存恢复删除数据造成的数据泄露。

- **加密数据防泄露：**华为云建议租户对要上云的重要数据进行加密存储，数据需要删除时，通过直接删除相关数据加密密钥，防止数据在被彻底删除前被恢复为明文后造成泄露。
- **存储数据删除：**当租户删除数据时，数据和对应的元数据在系统中一并删除，底层存储区域被回收以供系统重新覆盖写入，数据无法再被读取。但是针对客户误删除的操作场景，通过 EVS 服务的回收站功能、OBS 服务的多版本控制功能，用户可以最终决定数据的恢复或彻底删除。
- **磁盘数据删除：**华为云对删除虚拟卷采用清零措施，确保数据不可恢复，有效防止被恶意租户使用数据恢复软件读出磁盘数据，杜绝信息泄漏风险。
- **物理磁盘报废：**当物理磁盘报废时，华为云通过对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保用户隐私和数据不受未经授权访问。

6 租户服务与租户安全

华为云拥有纵跨 IaaS、PaaS 和 SaaS 类多项直接面向租户的云服务。本章精选了对于方便租户上云，为租户业务赋能增值，为租户安全保驾护航均尤为重要的服务，涉及计算、网络、存储、数据库、数据分析、应用、管理和安全等方面。每项云服务的介绍包括其基本技术特性、安全功能以及给租户安全带来的益处。同时，考虑到绝大多数租户对一些大众化的安全服务已有多年理论和实践积累，例如虚拟专用网络服务（VPN），因此未收入此章，具体内容可登录华为云网站（<http://www.huaweicloud.com/>）查询，敬请理解。

6.1 计算服务

6.1.1 弹性计算服务（ECS）

弹性计算服务（ECS – Elastic Compute Service）是华为云为租户提供的一种可随时自助获取，按需租用虚拟计算资源的云服务。租户购买的云服务器实例是一个虚拟的计算环境，包含了 CPU、内存、操作系统、磁盘、带宽等最基础的服务器组件。一个实例就是一台虚拟机。对自己创建的实例，租户拥有管理员权限，可以进行多项基本操作，如挂载磁盘、添加网卡、创建镜像、部署环境等。

华为云 ECS 提供了多层次的安全防护和保障，包括主机操作系统安全、虚拟机隔离、安全组等。通过从虚拟机到主机再到整个组网的整体安全设计，为用户打造安全可靠、灵活高效的应用环境。

- **主机安全：**主机操作系统使用华为统一虚拟化平台（UVP），对 CPU，内存和 I/O 资源隔离管理。UVP 安全性能已在第 5 章 5.3 平台安全一节详细介绍，在此不再

赘述。

- **虚拟机安全**

- **镜像加固：**华为云通过镜像工厂，由专业安全团队对虚拟机操作系统公共镜像进行安全加固，并及时修复系统安全漏洞，最终生成安全更新的公共镜像，并通过镜像服务（IMS）持续提供给租户。同时提供相关加固和补丁信息以供用户对镜像进行测试、排除故障及其他运维活动时参考。由客户根据相关应用运行及安全运维策略，选择直接使用最新的公共镜像重新创建虚拟机或自行创建已安装安全补丁的私有镜像。
- **网络与平台隔离：**主机内由 Hypervisor 提供的虚拟交换机（vSwitch）通过设置 VLAN、VXLAN、ACL 等属性确保虚拟机在网络层的逻辑隔离。多台主机之间的网络依然使用传统的物理网络设备（路由器、交换机等）进行物理隔离。同时，UVP 支撑的 CPU、内存、I/O 隔离进一步实现虚拟机在平台层的逻辑隔离。
- **IP/MAC 仿冒控制：**为了避免由于租户任意修改虚拟机 IP 或 MAC 引起的网络混乱，通过 DHCP snooping 技术，增加 IP 与 MAC 之间的绑定关系，然后通过 IP 源侧防护（IP Source Guard）与动态 ARP 检测（DAI – Dynamic ARP Inspection）对非绑定关系的报文进行过滤，可以防止用户虚拟机 IP 和 MAC 地址的仿冒。
- **安全组：**UVP 还提供安全组功能，用于多台虚拟机之间的分组隔离。多台虚拟机之间如果要相互访问，可以建立安全组。同一个安全组内的多台虚拟机默认可相互访问，处于不同安全组的任何两台虚拟机默认禁止相互通信。但可定制配置为允许通信。第 6 章 6.2.1 虚拟私有云服务（VPC）一节对安全组做详尽的介绍，请参考。
- **远程访问认证：**租户可通过 SSH 远程访问虚拟机操作系统来进行系统维护。但是，开放的 SSH 接口也是虚拟机的一个较高安全风险。为保证远程访问控制安全，租户可选择使用账号口令或公/私钥对完成远程访问的接入认证，建议租户默认使用更为安全的公/私钥对认证方式。
- **资源管理认证：**租户通过 API 来管理华为云 ECS 计算资源。租户发出 API 接入请求后，必须先完成基于 IAM 的身份认证和鉴权，才能接入 API 对计算资源进行管理。
- **VNC 安全：**租户通过 VNC（Virtual Network Computing）方式远程访问虚拟机，使用账号口令进行身份认证，采用 TLS 1.2 版本进行加密传输，确保数据传输安全。

6.1.2 镜像服务 (IMS)

镜像是一个包含了软件及必要配置的云服务器或裸金属服务器模版，至少包含操作系统，还可以包含各种预装的应用软件（例如，数据库软件）。镜像分为公共镜像、私有镜像、共享镜像和市场镜像。公共镜像是华为云为操作系统提供的标准镜像；私有镜像是用户自行创建的镜像；共享镜像是用户自己定义并分享给其他用户的镜像，由用户社区在自愿基础上维护；市场镜像是提供预装操作系统、应用环境和各类软件的优质第三方镜像。

华为云镜像服务 (IMS – Image Management Service) 提供简单方便的镜像自助管理功能。客户可通过服务控制台或 API 对自己的镜像进行管理。华为云负责公共镜像的定期更新与维护，向用户提供安装安全补丁的公共镜像和相关安全加固和补丁信息，以便用户在部署测试、故障排除等运维活动时参考。用户可以直接使用公共镜像，或者通过已有的云服务器或使用外部镜像文件自行创建私有镜像，也可以参与创建和维护共享镜像。用户能灵活选择上述任何镜像申请弹性云服务器。

IMS 基于华为云统一身份认证服务 (IAM) 来进行认证，支持镜像的传输和存储加密以及完整性检测。IMS 的所有数据都存储于信任子网内的镜像仓库，并且采用对象存储分桶机制，也就是将公共镜像和私有镜像分别存放在不同的桶中。IMS 提供了安全的加密算法和功能，让用户选择对镜像进行加密存储。在基于镜像创建虚拟机时，系统会自动检查镜像完整性，以确保创建的虚拟机包含完整的镜像内容。

IMS 对租户的所有操作进行权限判断，只有符合权限要求才允许执行，并对所有关键操作进行审计记录。审计日志实现持久化，租户可以对其进行长期而且精确的追溯。

6.1.3 弹性伸缩服务 (AS)

弹性伸缩服务 (AS – Auto-Scaling) 是根据租户的业务需求，通过用户预先定义的策略自动按需调整资源的服务。AS 在运行中无需人工干预，就可使资源使用量符合业务当前的需求。在业务增长时实现应用系统自动扩容，业务下降时实现应用系统自动减容。从而既能帮助租户节约资源和人力成本，又能保证其业务平稳健康运行。AS 对执行资源调配和管控策略的自动化特性有助于避免资源争夺类攻击或租户管理人员在调配资源时人为操作失误所造成的安全风险。

AS 支持自动地将加入的实例添加到负载均衡监听器，访问流量将通过负载均衡监听器自动分发到伸缩组内的所有实例，相比直接访问单个后端服务器和服务具有更高的防 DDoS 攻击的能力。AS 可以实时检测实例的运行状况，并启动新实例以替换运行状况

不佳的实例。同时支持配置使用多个可用区（AZ – Availability Zone），在多个可用分区中平均分配实例，保证伸缩组中部署应用的容灾能力，提升系统可用性。

6.1.4 专属主机服务 (DeH)

专属主机服务（DeH – Dedicated Host Service）是在华为云 ECS 的基础上，提供了一种灵活的以主机为单位出租的弹性计算服务，它继承了 ECS 服务的所有功能以及安全特性。

DeH 由于以主机为单位出租，在安全上有物理层主机隔离的优势：单个租户拥有整个主机，可以避免其他租户对系统资源的抢占，防止恶意租户通过 Hypervisor 可能出现的漏洞对系统实施攻击。

6.1.5 裸金属服务 (BMS)

裸金属服务（BMS – Bare Metal Service）是华为云为租户提供了一种可随时自助获取，按需租用物理层计算资源的云服务。租户购买的裸金属服务器，即 BMS 实例，是一个物理的计算环境，包含了 CPU、内存、操作系统、磁盘、带宽等最基础的服务器组件，是 BMS 提供给每个租户的操作实体。一个实例就是一台物理机。对自己创建的实例，租户拥有管理员权限，可以执行多项基本操作，如开关机器，挂载磁盘、部署环境等。

BMS 提供了与华为云 ECS 类似的多层安全防护，包括主机系统和网络安全、远程访问认证、管理控制安全等技术手段，具体内容可参考第 6 章 6.1.1 弹性计算服务（ECS）一节。更重要的是，BMS 独享物理机隔离的安全优势。通过从主机到整个组网的安全设计为租户提供可靠的安全保障，进而帮助用户打造一个在独立物理计算环境中运行的，安全可靠、灵活高效的应用环境。

6.2 网络服务

6.2.1 虚拟私有云服务 (VPC)

虚拟私有云服务（VPC – Virtual Private Cloud）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。

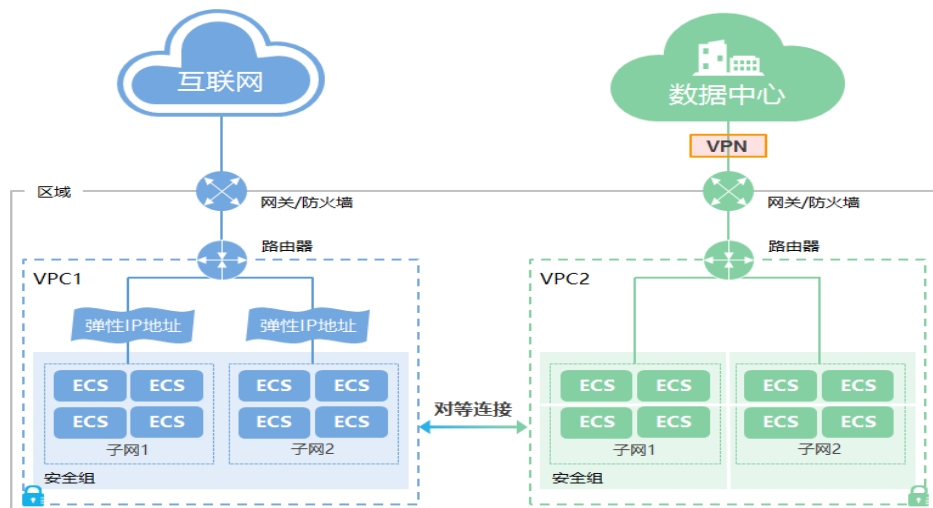
VPC 的优势如下：

- 可以完全掌控自己的虚拟网络，包括创建自己的网络。

- 可以通过在 VPC 中申请弹性 IP 地址¹¹，将弹性云服务器连接到公网。
- 可以使用 VPN 将 VPC 与传统数据中心互联，实现应用向云上的平滑迁移。
- 两个 VPC 可以通过对等连接功能互联。
- 可以通过 VPC 方便地创建、管理自己的网络，配置 DHCP，执行安全快捷的网络变更。
- 可以通过 VPC 多项网络安全防护功能提高网络安全性。

VPC 基本架构如下图：（请见下页）

图6-1 华为云 VPC 架构简图



VPC 提供了以下与租户网络安全强相关的网络功能：

- **子网**：子网是用来管理弹性云服务器网络平面的一个网络，可提供 IP 地址管理、DNS 服务。同一个 VPC 的所有子网内的弹性云服务器默认均可以相互通信，处于不同 VPC 中的任意两台弹性云服务器默认禁止通信。
- **VPN**：VPN 用于远端用户和 VPC 之间建立一条安全加密的通信管道，使远端用户通过 VPN 直接使用 VPC 中的业务资源。默认情况下，在 VPC 中的弹性云服务器无法与租户自己的数据中心或私有网络进行通信，如需通信，租户可启用 VPN 功能，配置 VPN 相关参数。

¹¹ 弹性 IP 是基于互联网上的静态 IP 地址，将弹性 IP 地址和子网中关联的弹性云服务器绑定和解绑，可以实现 VPC 中的弹性云服务器通过固定的公网 IP 地址与互联网互通。

- **云专线：**云专线服务是在租户自营的内网本地数据中心与华为云间建立连接的专线网络连接服务。租户可以利用云专线建立华为云与租户的数据中心、办公室或主机托管区域的专线连接，降低网络时延，获得比互联网线路更快速、更安全的网络体验。

VPC 还提供了多项不同 Open System Interconnection (OSI) 层的网络安全防护功能，租户可以根据其在华为云上的网络安全需求定制配置。其中，对整个华为云和每个租户的 VPC 的网络安全都至关重要的非网络 ACL 和安全组这两款安全功能莫属，先着重介绍：

- **网络 ACL：**网络 ACL 是对一个或多个子网的访问制定、维护并执行访问控制策略的系统，根据与子网关联的入站/出站规则，判断数据包是否被允许流入/流出关联子网。
- **安全组：**在 VPC 中，安全组是一组对弹性云服务器的访问规则的集合，为同一个 VPC 内具有相同安全保护需求并且相互信任的弹性云服务器提供访问策略。用户可以自行创建并定义安全组内与组间弹性云服务器的访问规则，将 VPC 中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。

每个安全组可以设定一组访问规则。安全组规则包括：协议、出/入方向、源 IP 地址段/子网或安全组、允许访问的端口范围。支持配置 TCP、UDP、ICMP 三种协议。

当虚拟机加入安全组后，即受到该访问规则组的保护。用户创建虚拟机时，通过选定要加入的安全组，来对虚拟机进行安全隔离和访问控制。同一个安全组内的多台虚拟机可以分布在物理位置分散的多台物理机上。同一个安全组内的多台虚拟机默认可相互访问，处于不同安全组的任何两台虚拟机默认禁止相互通信，但可定制配置为允许通信。

当安全组被成功创建，没有自定义规则的安全组即具备默认的访问规则。默认规则是在出方向上的数据报文全部放行，安全组内的云服务器无需添加规则即可互相访问。当默认访问规则可以满足需求时，则无需再为该安全组添加规则。

显而易见，网络 ACL 和安全组功能都是为了提升华为云 VPC 的网络安全性。因此，了解二者区别会对租户建立有效的 VPC 网络安全策略大有帮助。网络 ACL 和安全组的区别总结如下，仅供参考。

表6-1 安全组和网络 ACL 区别列表

安全组	网络 ACL
弹性云服务器实例级别操作 (第一层防护)	子网级别操作 (第二层防护)
支持允许策略	支持允许和拒绝策略
多个规则冲突, 取其并集生效	多个规则冲突, 靠前的规则优先生效
创建弹性云服务器实例默认必须 选择安全组, 默认安全组自动应 用到弹性云服务器实例	创建子网没有网络 ACL 选项, 必须创建网络 ACL、添加关联子网、添加出入规则, 并启用, 才 可应用到关联子网及子网下的弹性云服务器实例
支持报文三元组(即协议、端口和 对端地址)过滤	支持报文五元组(即协议、源端口、目的端口、源 地址和目的地址)过滤

另外, 为增强 VPC 网络隔离防护, 平台内也提供了其他网络安全功能, 总结如下:

- **虚拟局域网 (VLAN) 隔离:** VLAN 在 OSI 的第二层通过虚拟网桥支持 VLAN tagging 功能实现虚拟交换并确保虚拟机之间的安全隔离。
- **IP 和 MAC 绑定:** 防止虚拟机用户通过修改虚拟网卡的 IP、MAC 地址发起 IP、MAC 仿冒攻击, 避免网络混乱, 增强虚拟机网络的安全性。具体技术能力包括通过 DHCP snooping 生成 IP-MAC 的绑定关系, 然后通过 IP 源侧防护 (IP Source Guard) 与动态 ARP 检测对非绑定关系的报文进行过滤。
- **DHCP Server 隔离:** 禁止用户虚拟机启动 DHCP Server 服务, 防止用户无意识或恶意启动 DHCP Server 服务, 影响正常的虚拟机 IP 地址分配过程。
- **防 DoS/DDoS 攻击:** 系统通过限制虚拟端口的连接跟踪数来抵御来自云平台外部或平台内部其他虚拟机的大流量攻击¹²。

6.2.2 弹性负载均衡服务 (ELB)

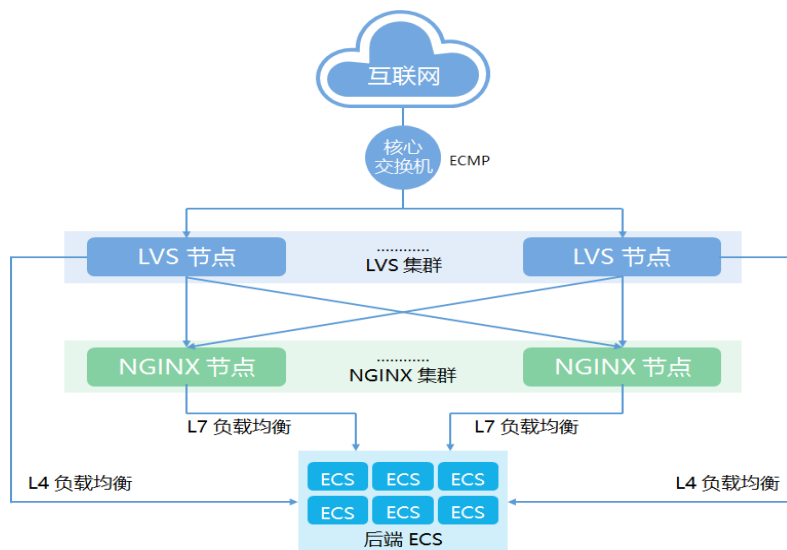
弹性负载均衡 (ELB – Elastic Load Balance) 将访问流量自动分发到多台弹性云服务器, 扩展应用系统对外的服务能力, 实现更高水平的应用程序容错性能。相比传统硬件负载均衡器, 弹性负载均衡具有如下优势:

¹² 大流量攻击会产生大量连接跟踪表项, 如果不做限制, 会耗尽连接跟踪表资源, 导致不能接受新的连接请求, 最终造成业务及管理流量中断。

- 冗余设计，自动移除异常节点，并将流量在正常节点之间重新路由，确保业务的可用性。
- 根据应用的流量，自动扩展处理能力，并可与弹性伸缩服务无缝集成，自动满足变化的流量需求。
- 支持最高 1 亿并发连接，满足用户的大流量需求；支持用户使用 OSI 四层（TCP 协议、UDP 协议）或七层（HTTP 协议、HTTPS 协议）的负载分发。

ELB 组网基本设计如下图：

图6-2 华为云 ELB 组网图



LVS: Linux Virtual Server
ECMP: Equal-Cost Multipath Protocol

弹性负载均衡服务提供如下安全防护：

- **隐藏内部真正的服务器地址和端口号：**ELB 仅对外暴露单个地址和相应服务端口，不暴露真实的后端地址和服务端口，防止网络信息泄露，减少攻击面。
- **根据流量状态，自动扩展处理能力：**ELB 可以配合弹性伸缩服务提供更加灵活的扩展收缩能力，相比直接访问单个后端和服务具有更高的防 DDoS 攻击能力。
- **内网 ELB 支持安全组配置：**建立内网 ELB 安全组可以确保租户实例只接收来自负载均衡器的流量。租户也可以定义允许的端口和协议，确保两个方向通过 ELB 的流量。
- **支持源地址透传：**ELB 在监听 HTTP 和 HTTPS 服务时支持源地址透传功能，租户可基于源地址进行溯源、连接统计、流量统计或者源地址白名单等进一步的安全

诉求，通过客户应用实现，更快速发现攻击并有效响应。

- **支持 SSL/TLS 卸载及证书管理：**ELB 支持 SSL/TLS 卸载。SSL/TLS 卸载将报文加解密的工作由租户的后端服务器转移到 ELB，可以有效降低租户后端服务器的性能压力。对于进入 ELB 的加密流量，由 ELB 负责将报文解密，然后分发到租户的后端服务器；对于流出 ELB 的流量，由 ELB 对报文进行加密后发送。使用 SSL/TLS 卸载功能时，需要租户上传所需证书及私密钥，由 ELB 进行管理。
- **支持加密协议和加密套件可配置：**租户使用 HTTPS 作为 ELB 的安全通信协议时，可以按需选择加密协议和相关配置。默认选择的加密协议是 TLS 1.2 版本。ELB 同时支持加密套件可选；对于有更多加密算法项选择的租户，ELB 提供扩展的加密套件；对有高安全需求的租户，提供严格的加密算法。

6.2.3 云解析服务（DNS）

云解析服务（DNS – Domain Name Service）提供高可用、高扩展的权威 DNS 服务和 DNS 管理服务，把人们常用的域名或应用资源转换成用于计算机连接的 IP 地址，从而将最终用户路由到相应的应用资源上。

通过 DNS 可以把域名解析到 ECS、OBS、RDS 等其他服务地址，便于通过域名直接访问不同服务资源。用户可以从 DNS 中获得其独有的内网域名解析服务，可以基于 VPC 任意定制域名和解析，解决了内部业务的域名注册和管理问题，降低了业务部署和维护的复杂度，同时也为业务高可用设计提供了可能。华为云 DNS 基于华为云高可用性和可靠性的基础架构构建，其服务器的分布式特性有助于提高可用性，确保将最终用户路由到应用程序。在单个业务节点发生故障时，可通过修改 DNS 解析记录进行故障转移，保障租户业务的可用性。

华为云 DNS 具有以下主要安全防护功能：

- 支持添加 IP 到域名映射的反向解析记录，通过反向解析可以降低垃圾邮件数量。
- 通过例行更新，缩短生存期（TTL – Time to Live）和频繁清除 DNS 缓存等措施防止 DNS 缓存中毒攻击。
- 提供 Anti-DDoS 功能，对访问流量进行特征模拟，清洗攻击流量，限流和屏蔽恶意 IP 访问，保障服务安全稳定运行。DNS 提供的七层防护算法，逐层对攻击流量进行清洗过滤，实现了对流量层攻击和应用层攻击的全面防护。例如，Anti-DDoS 功能可以阻断 DNS 放大攻击。

- 提供 HttpDNS 能力,允许客户端使用基于 HTTP/HTTPS 协议的 API 绕过传统 Local DNS Server 进行域名解析;可有效避免域名解析结果被劫持。

租户可以通过使用华为云 IAM 为租户成员分配云解析服务及操作权限,使用访问密钥,以 API 的方式访问华为云资源。

6.3 存储服务

6.3.1 云硬盘服务 (EVS)

云硬盘服务 (EVS – Elastic Volume Service) 是华为云提供的分布式存储服务,主要为 ECS、BMS 等计算服务提供硬盘。

EVS 基于 IAM 服务进行访问控制,采用 HTTPS+口令认证、会话管理、基于接口的权限控制、审计日志等措施来保证 web 操作的安全性;通过访问控制、网络平面隔离、自动告警等措施保证后台存储系统安全性和稳定性;通过对操作系统、数据库、web 应用组件等进行安全配置加固、开源组件及时补丁或升级,保障系统运行安全。

EVS 使用多副本的数据冗余保护机制,采用副本同步写、读修复等措施保证数据一致性,当检测到硬件故障能够自动后台修复,数据快速自动重建,数据持久性可达 99.9999999%。EVS 提供加密盘选项,用户自主管理密钥,满足用户不同安全场景的需求。

6.3.2 云备份服务 (CBR)

云备份 (CBR – Cloud Backup and Recovery) 提供对云硬盘 (Elastic Volume Service)、弹性云服务器 (Elastic Cloud Server) 和裸金属服务器 (Bare Metal Server) 的备份保护服务 (下文将云硬盘称为磁盘,弹性云服务器和裸金属服务器统称为服务器),支持基于快照技术的备份服务,并支持利用备份数据恢复服务器和磁盘的数据。同时云备份支持同步线下备份软件 BCManager 中的备份数据,可以在云上对备份数据进行管理,并支持将备份数据恢复至云上其他服务器中。

架构设计上, CBR 以微服务架构为基础,对业务进行抽象建模。做到业务数据与业务逻辑解耦,平台共有能力与产品能力解耦,各个微服务之间业务解耦。微服务设计遵循前后端分离,无状态服务,接口通信等设计原则。与外部交互,服务间交互充分考虑返回错误、重启、无响应、阻塞等异常情况,对故障进行隔离保证服务的可用性,当故障恢复后能够自动恢复服务。

CBR 基于 IAM 服务进行访问控制；通过 HTTPS 协议，对外接口基于 HTTPS 的 RESTful 架构，对 CBR 的访问通道进行安全保护；采用网络时间同步协议 NTP（NetWork Time Protocol）确保系统内各网元时间的一致性，对操作系统、数据库、web 应用组件等进行安全配置加固，保障系统运行安全。

CBR 支持对备份数据的完整性校验。在备份和恢复过程中，采用 CRC32C 校验备份数据的正确性，确保数据无损坏或被篡改。支持对加密卷的备份和恢复。通过华为云 KMS 服务获取密钥，将生产存储中的加密卷加密备份到备份存储中，同时可以将加密备份数据恢复至原卷或新卷中。不同租户的备份数据存储在不同的桶中，相互隔离，最大限度保障用户数据的安全。

6.3.3 内容分发网络（CDN）

内容分发网络（CDN – Content Delivery Network）是构建在现有互联网基础之上的一层智能虚拟网络，通过在网络各处部署节点服务器，实现将源站内容分发至所有 CDN 节点，提供媒体内容的预注入、回源、存储和缓存、分片、播放等功能，以及网页、文件的缓存和下载功能，使用户可以就近获得所需的内容。

CDN 采用口令认证、访问控制、最小授权、会话管理、输入校验、加密等安全手段确保整体系统安全性；通过对网络设备进行安全加固、网络平面隔离、安全区域划分及网络访问控制实现网络层面的安全；通过操作系统安全加固、防病毒等手段实现操作系统主机层面安全；通过数据库安全加固、数据库安全设计等手段确保数据库安全；通过对 Web 容器实施加固，对 Web 应用进行安全设计，使业务系统能够有效应对安全威胁；通过接口协议安全、敏感数据传输安全及敏感数据存储安全确保非 Web 应用安全；通过支持防盗链、防篡改等安全功能，保障 CDN 的内容安全；提供完善的通信矩阵和安全管理文档，指导安全运维人员部署和实施。

6.3.4 对象存储服务（OBS）

对象存储服务（OBS – Object Storage Service）是一个基于对象的海量存储服务，为租户提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删桶、上传、下载、删除对象等。OBS 为用户提供超大存储容量，可存放任意类型的文件，适合普通用户、网站、企业和开发者使用。由于 OBS 是一项面向互联网的服务，其提供的基于 HTTPS 协议的 Web 服务接口，让用户能在任意可连接至互联网的电脑上，通过 OBS 管理控制台或客户端随时随地访问和管理存储在 OBS 中的数据。

OBS 通过多种访问控制手段，如桶 ACL、桶策略、用户身份认证等安全手段，对租户请求的访问权限进行限制；同时，对租户数据，OBS 提供了一系列的安全手段，如通过访问日志功能进行审计，通过跨域资源共享限定访问来源及请求类型，通过防盗链确保链接来源可靠，通过服务端加密确保数据安全等，保障安全存储、安全访问租户数据。

- **访问控制：**OBS 支持通过 ACL、桶策略、用户签名验证等方式对用户的 OBS 请求进行访问控制。

- **访问控制列表 (ACL)：**OBS 提供基于帐户的 ACL，可授予指定帐户相应的访问权限。ACL 可以限制所有用户或特定用户对单个桶或对象的访问权限，例如只读权限、写入权限、完全控制权限。用户也可以设置其他访问策略，例如对某对象设置公开访问策略，赋予所有人只读权限。所有的桶和对象在默认情况下，只允许桶的创建者访问桶内的对象，其他人无法访问该桶及桶内的对象。

- **桶策略：**桶的所有者可以通过编写桶策略 (Bucket Policy)，限定桶的访问权限。桶策略可基于各种条件，如 OBS 操作、申请人、资源、请求的其他要素 (如 IP 地址) 提供对桶和对象的集中访问控制等。附加到某个桶上的权限适用于该桶内所有对象。在帐户制定策略上，可以按下面维度授予用户权限：

- 特定的桶
- 特定的用户

ACL 只能对单个对象进行权限的添加，而桶策略可对一个桶内的所有对象进行权限的添加和禁止。帐户可通过同一请求对某桶内任意数量的对象进行权限设置。此外，帐户还可以对资源名称及其他值添加通配符 (类似于正则表达式运算符)，从而实现对一组对象的访问控制。

设置桶策略后，OBS 将根据桶策略判断是接受还是拒绝对桶访问的请求。

- **用户签名验证：**帐户访问 OBS 时必须提供一对访问密钥，即 AK/SK。AK 和 SK 支持 IAM 的认证机制。OBS 通过用户帐户中的 AK 和 SK 进行认证鉴权，确保通过授权的帐户才能访问指定的 OBS 资源。当向 OBS 发送访问请求时，发送的消息头会包含由 SK、请求时间、请求类型等信息生成的鉴权信息。并且，在进行鉴权之前，OBS 需要对桶名、对象名单独进行 URL Encode 编码，再生成鉴权信息。只有经过签名鉴权验证通过的帐户，才能访问指定的 OBS 资源。

OBS 接口层面全面兼容亚马逊的 S3 (Simple Storage Service) 接口。租户可以使用亚马逊资源名称 (ARN – Amazon Resource Name)，亚马逊签名第 2 版和第 4 版

(Amazon Signature V2 / V4)¹³两种版本的签名认证流程以及认证接口，来完成从亚马逊的 S3 读取并迁移其数据到华为云上，确保租户数据迁移安全可靠。

- **数据可靠性和持久性：**OBS 通过支持对象数据的高可靠性，并通过业务节点的高可靠性网络和节点的多冗余设计，使系统设计可用性达 99.995%，完全满足对象存储服务高可用的需求。OBS 通过提供对象数据多份冗余和保证多份对象的数据一致性自动修复技术，来提供对象数据的高可靠性，系统设计数据持久性高达 99.9999999999%。

OBS 支持保存一个对象的多个版本，使用户更方便地检索和还原各个版本，在意外操作或应用程序故障时快速恢复数据。多版本控制为用户意外覆盖或删除对象场景提供了恢复手段。默认情况下，OBS 中新创建的桶不会开启多版本功能，向同一个桶上传同名的对象时，新上传的对象将覆盖原有对象。

- **访问日志记录：**OBS 支持对桶的访问请求，并保存访问日志记录，用于进行请求分析或日志审计。通过访问日志记录，桶的所有者可以深入分析访问该桶的租户请求性质、类型或趋势。当租户开启一个桶的日志管理功能后，OBS 会自动对该桶的访问请求进行日志记录，并生成日志文件，写入用户指定的桶（即目标桶）中。由于日志存储在 OBS 中也会占用租户的 OBS 存储空间，意味着将产生额外的存储费用，因此默认情况下 OBS 不会开启该功能。若出于分析或审计等目的，租户可开启该功能。
- **跨域资源共享 (CORS – Cross-Origin Resource Sharing)：**OBS 支持 CORS 规范，允许跨域请求访问 OBS 中的资源。CORS 是由 W3C (World Wide Web Consortium) 标准化组织提出的一种网络浏览器的规范机制，定义了一个域中加载的客户端 Web 应用程序与另一个域中的资源交互方式。OBS 支持静态网站托管，条件是只有在目标桶设置了合理的 CORS 配置时，OBS 中保存的静态网站才被响应另一个跨域网站的请求，不会由于同源安全策略 (SOP – Same Origin Policy) 的存在，而导致不同域之间的网站脚本和内容无法进行交互。
- **防盗链：**为了防止租户在 OBS 的数据被他人盗链，OBS 支持基于 HTTP 表头 (header) 中参照位址 (referer) 的防盗链方法，OBS 同时支持白名单和黑名单的访问设置。在 HTTP 协议中，通过表头字段，网站可以检测目标网页访问的来源网

¹³ 亚马逊签名认证第 4 版与第 2 版相比，除使用更加安全的 HMAC-SHA256 算法外，还会将用户数据纳入签名计算，并且计算签名时纳入签名计算的头域也可以由用户自行指定，由此极大提升了请求鉴权的安全性。因此，华为云建议租户使用第 4 版与亚马逊对接实现迁移。

页。有了跟踪来源，就可以通过技术手段进行处理，一旦检测到来源不是本站，即进行阻止或返回指定页面。防盗链还可以检测到请求来源是否与白名单或黑名单匹配，若与白名单匹配成功则允许请求访问，否则阻止或返回指定页面。

- **服务端加密：**用户可根据自身需求，采用不同的密钥管理方式来使用服务端加密功能。用户上传对象时，服务端会把数据加密成密文后进行存储。用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。目前，服务端加密功能支持两种方式：**KMS 托管密钥的服务端加密（SSE-KMS）**和**客户提供加密密钥的服务端加密（SSE-C）**。
 - **SSE-KMS** 是指 **OBS** 使用 **KMS** 提供的密钥进行服务端加密。用户首先需要在 **KMS** 中创建密钥（或使用 **KMS** 提供的默认密钥），然后在上传对象时使用该密钥进行服务端加密。
 - **SSE-C** 是指 **OBS** 使用用户提供的密钥和密钥的哈希值进行服务端加密。用户在上传对象的接口中携带密钥，**OBS** 使用该密钥进行服务端加密。**OBS** 不存储用户提供的加密密钥，因此若没有该密钥，用户则无法解密获取该对象。

6.3.5 数据快递服务（DES）

数据快递服务（DES – Data Express Service）是一种线下海量数据传输服务，它使用物理存储介质（例如：**eSATA** 硬盘驱动器）向华为云传输大量数据。使用数据快递服务可解决海量数据传输的难题，如高昂的网络成本、较长传输时间等。

在开通 **DES** 服务后，登录管理控制台创建服务单，将数据按 **DES** 要求加密存放入待邮寄磁盘中后，即可将磁盘邮寄快递至华为云数据中心。

为了保护数据安全，在邮寄前，建议用户对磁盘数据进行加密。**DES** 支持第三方加密工具使用业界通用的 **AES-256** 加密算法对数据进行客户端加密。**DES** 支持的客户端是 **Windows**、**Mac OS X**、**Linux** 等操作系统。工具不需要生成任何文件即可在硬盘上建立虚拟磁盘。用户可以按照盘符进行访问，所有虚拟磁盘上的文件都被自动加密，必须使用密码来进行访问。

华为云数据中心收到磁盘后，会将磁盘挂载至服务器并通知用户尽快启动上传任务。此时用户可再次登录管理控制台填写 **AK/SK** 和用户加密磁盘的密钥，启动数据上传。数据传输完成后用户还可以查看数据传输报表，确认无误后华为云数据中心将回邮磁盘。华为云人员全程不接触租户密钥及租户数据，确保数据传输安全。

6.4 数据库服务

6.4.1 关系型数据库服务（RDS）

关系型数据库服务（RDS – Relational Database Service）是华为云提供的一款允许租户快速发放不同类型数据库，并可根据业务需要对计算资源和存储资源进行弹性扩容的数据库服务。其提供自动备份、数据库快照、数据库恢复等功能，以防止数据丢失。参数组功能，则允许租户根据业务需要进行数据库调优。

RDS 还提供多个特性来保障租户数据库的可靠性和安全性，例如 VPC、安全组、权限设置、SSL 连接、自动备份、数据库快照、时间点恢复（PITR – Point In Time Recovery）、跨可用区部署等。

- **网络隔离：**VPC 允许租户通过配置 VPC 入站 IP 范围来控制连接数据库的 IP 地址段。RDS 实例运行在租户独立的 VPC 内。租户可以创建一个跨可用区的子网组，之后可以根据业务需要，将部署 RDS 的高可用实例选择此子网完成，RDS 在创建完实例后会为租户分配此子网的 IP 地址，用于连接数据库。RDS 实例部署在租户 VPC 后，租户可通过 VPN 使其它 VPC 能够访问实例所在 VPC，也可以在 VPC 内部创建 ECS，通过私有 IP 连接数据库。租户可以综合运用子网和安全组的配置，来完成 RDS 实例的隔离，提升 RDS 实例的安全性。
- **访问控制：**租户创建 RDS 实例时，RDS 会为租户同步创建一个数据库主帐户，主帐户的密码由租户指定。此主帐户允许租户操作自己创建的 RDS 实例数据库。租户可以使用数据库主帐户连接 RDS 实例数据库，并根据需要创建数据库实例和数据库子帐户，并根据自身业务规划，将数据库对象赋予数据库子帐户，以达到权限分离的目的。租户创建数据库实例时，可以选择安全组，将 RDS 实例业务网卡部署在对应的安全组中。租户可以通过 VPC 对 RDS 实例所在的安全组入站、出站规则进行限制，从而控制可以连接数据库的网络范围。数据库安全组仅允许数据库监听端口接受连接。配置安全组不需要重启 RDS 实例。
- **传输加密：**RDS 实例支持数据库客户端与服务端 TLS 加密传输。RDS 在发放实例时，指定的 CA 会为每个实例生成唯一的服务证书。客户端可以使用从服务控制台上下载的 CA 根证书，并在连接数据库时提供该证书，对数据库服务端进行认证并达到加密传输的目的。
- **存储加密：**支持对存储到数据库中的数据加密后存储，加密密钥由 KMS 管理。

- **自动备份和快照：**RDS 提供两种备份恢复方法，即自动备份和数据库快照。自动备份默认开启，备份存储期限最多 35 天，同时开启自动备份后允许对数据库执行时间点恢复。RDS 自动备份会进行全量数据备份，且每 5 分钟会增量备份事务日志，这就允许租户将数据恢复到最后一次增量备份前任何一秒的状态。快照是租户手动触发的数据库全量备份，这些备份数据存储在华为 OBS 桶中，当租户删除实例时，会同步删除 OBS 桶中的快照。租户也可以从已有的快照恢复到新实例中。
- **数据复制：**RDS 支持部署高可用实例。租户可选择在单可用区或多可用区中部署高可用实例。当租户选择高可用实例时，RDS 会主动建立和维护数据库同步复制，在主实例故障的情况下，RDS 会自动将从实例升为主实例，从而达到高可用的目的。如果租户使用 MySQL 数据库时，业务中读取数据比例大的话，可以对 RDS 单实例创建只读实例，RDS 维护主实例和只读实例间的数据同步关系，租户可以根据业务需要连接不同的实例进行读写分离。
- **数据删除：**租户删除 RDS 实例时，存储在此实例中的数据以及在 OBS 中相应的备份数据都会被自动删除，实例中的数据无法被查看及恢复。

6.4.2 文档型数据库服务（DDS）

文档型数据库服务（DDS – Document Database Service）是华为云提供的一款允许租户快速发放不同类型数据库，并可根据业务需要对计算资源和存储资源进行弹性扩容的数据库服务。其提供自动备份、数据库快照、数据库恢复、时间点恢复等功能，以防止数据丢失。参数组功能，则允许租户根据业务需要进行数据库调优。

DDS 还提供多个特性来保障租户数据库的可靠性和安全性，例如 VPC、安全组、权限设置、SSL 连接、自动备份、数据库快照、时间点恢复、跨可用区部署等。

- **网络隔离：**VPC 允许租户通过配置 VPC 入站 IP 范围来控制连接数据库的 IP 地址段。DDS 实例运行在租户独立的 VPC 内。租户可以创建一个跨可用区的子网组，之后可以根据业务需要，将部署 DDS 的高可用实例选择此子网完成，DDS 在创建完实例后会为租户分配此子网的 IP 地址，用于连接数据库。DDS 实例部署在租户 VPC 后，租户可通过 VPN 使其它 VPC 能够访问实例所在 VPC，也可以在 VPC 内部创建 ECS，通过私有 IP 连接数据库。租户可以综合运用子网和安全组的配置，来完成 DDS 实例的隔离，提升 DDS 实例的安全性
- **访问控制：**租户创建 DDS 实例时，DDS 会为租户同步创建一个数据库主帐户，主帐户的密码由租户指定。此主帐户允许租户操作自己创建的 DDS 实例数据库。租

户可以使用数据库主帐户连接 DDS 实例数据库，并根据需要创建数据库实例和数据库子帐户，并根据自身业务规划，将数据库对象赋予数据库子帐户，以达到权限分离的目的。租户创建数据库实例时，可以选择安全组，将 DDS 实例业务网卡部署在对应的安全组中。租户可以通过 VPC 对 DDS 实例所在的安全组入站、出站规则进行限制，从而控制可以连接数据库的网络范围。数据库安全组仅允许数据库监听端口接受连接。配置安全组不需要重启 DDS 实例。

- **传输加密：**DDS 实例支持数据库客户端与服务端 TLS 加密传输。DDS 在发放实例时，指定的 CA 会为每个实例生成唯一的服务证书。客户端可以使用从服务控制台上下载的 CA 根证书，并在连接数据库时提供该证书，对数据库服务端进行认证并达到加密传输的目的。
- **存储加密：**支持对存储到数据库中的数据加密后存储，加密密钥由 KMS 管理。
- **自动备份和快照：**DDS 提供两种备份恢复方法，即自动备份和数据库快照。自动备份默认开启，备份存储期限最多 35 天，同时开启自动备份后允许对数据库执行时间点恢复。DDS 自动备份会进行全量数据备份，且每 5 分钟会增量备份事务日志，这就允许租户将数据恢复到最后一次增量备份前任何一秒的状态。快照是租户手动触发的数据库全量备份，这些备份数据存储在华为 OBS 桶中，当租户删除实例时，会同步删除 OBS 桶中的快照。租户也可以从已有的快照恢复到新实例中。
- **数据复制：**DDS 支持集群、副本集高可用实例，也支持单节点实例。租户可选择在单可用区或多可用区中部署高可用实例。当租户选择高可用实例时，DDS 集群、副本集之间会自动同步数据，在集群/副本集的单节点故障时，DDS 会自动将业务路由到其他节点，从而达到高可用的目的。
- **数据删除：**租户删除 DDS 实例时，存储在此实例中的数据以及在 OBS 中相应的备份数据都会被自动删除，实例中的数据无法被查看及恢复。

6.4.3 分布式缓存服务（DCS）

分布式缓存服务（DCS – Distributed Cache Service）是以 Redis 为基础的分布式缓存中间件集群服务，在安全、性能、可靠性方面进行了增强。DCS 是基于内存的数据结构存储系统，它可以用作数据库、缓存或简单消息队列。它支持多种类型的数据结构，如字符串（strings）、散列（hashes）、列表（lists）、集合（sets）、有序集合（sorted sets）、位图（bitmaps）、hyperloglogs 和地理空间（geospatial）索引半径查询等。DCS 内置了复制，Lua 脚本功能，支持最近最少使用（LRU – Least Recently Used）等缓存挤出策略，

支持简单事务和持久化功能。

DCS 利用华为云统一的角色访问控制（RBAC – Role-Based Access Control）模型进行权限控制，每个租户只能操作属于自己的资源，如自己的缓存实例。不同 DCS 实例之间是物理隔离，不同的租户实例之间通过 VPC 隔离。DCS 对所有租户的操作进行权限判断，只有授权的操作才允许执行，并在审计日志中记录所有关键操作。审计日志可保留到指定的时间，以便必要时进行审计回溯。

DCS 管理面数据保存在信任子网里，通过多副本机制实现数据冗余，保证数据可靠性。

6.5 数据分析服务

6.5.1 MapReduce 服务（MRS）

MapReduce 服务（MRS – MapReduce Service）在华为云上提供高可靠性、高扩展性、高容错性、易运维的高效托管大数据分析集群服务。MRS 集群作为一个云上托管的数据管理和分析平台，其集群内所有节点都分布在租户同一个虚拟局域网中，同时集群内 OMS（Operation & Maintenance Service）的主、备节点和其他节点间采用双向互信。

MRS 支持用户使用浏览器、组件客户端的方式登录集群。MRS 提供了基于 CAS（Central Authentication Service）的单点登录（SSO – Single Sign-On），用户在任意 Web 页面登录后，即可访问大数据平台其他组件的 Web 页面，无需再次输入用户口令进行认证。

- **用户口令管理：**MRS 系统通过 IAM (Kerberos/LDAP) 进行用户口令管理。其中 Kerberos 负责用户口令的加密处理并将加密用户口令在保存 LDAP 数据库。
- **权限控制：**MRS 提供 RBAC 权限控制，用户的角色决定了用户的权限。通过指定用户特定的角色，赋予其相应的权限。每种角色具有的权限，可根据其需要访问的组件资源进行配置。
- **数据加密：**MRS 的 HBase 支持按列簇加密存储。在建表时，客户可选择对哪些数据进行加密存储。
- **数据完整性：**MRS 的用户数据保存在 HDFS 上，HDFS 默认采用 CRC32C 校验数据的正确性，也支持校验速度慢于 CRC32C 的 CRC32 校验方式。HDFS 的数据节点（DN – DataNode）负责存储校验数据，如果发现客户端传递过来的数据有异常（不完整）就将异常上报至客户端，让客户端重新写入数据。客户端从 DN 读

数据的时候会检查数据是否完整，如发现数据不完整，则会尝试从其他的 DN 节点上读取数据。

- **数据备份：**MRS HBase 集群支持将主集群数据异步实时备份至备集群。它对外提供了基础的运维工具，包含主备集群关系维护、数据重建、数据校验、数据同步进展查看等功能。

6.6 应用服务

6.6.1 消息通知服务（SMN）

消息通知服务（SMN – Simple Message Notification）是一个简单、灵活、海量、托管的消息推送服务。通过该服务，用户可以高效且经济的方式将消息推送给电子邮箱、手机号码、HTTPS 应用程序以及移动推送。通过 SMN，用户可以单独发送消息也可群发消息。用户还可以轻松地集成其它云服务(例如 CES、OBS、AS 等)，并接受它们的事件通知。

租户可通过服务控制台或 SMN API 来使用消息通知服务。SMN 采用基于租户的权限模型、严格参数校验、安全通讯协议、敏感信息保护、审计日志等安全措施，保护管理系统免受上述攻击的危害。

为保证业务灵活性，SMN 还提供非常灵活的授权访问机制：访问 SMN 服务的账户包括华为云账户、基于 IAM 服务创建并被授权 SMN 访问权限的用户，以及租户授权的云服务等。华为云账户可以访问 SMN 的所有操作；基于 IAM 服务创建并被授权 SMN 管理员访问权限的用户，可以访问 SMN 的所有操作；基于 IAM 服务创建并被授权租户访问权限的用户，只能做 SMN 服务的查询类操作。

SMN 服务只支持使用 HTTPS 协议访问 SMN API 接口，默认支持 TLS 1.2 协议和 PFS 安全特性。对所有租户的接口调用都会做严格的参数校验，以确保服务不会受恶意攻击的影响。对于租户的敏感数据，如通知的手机号码、邮件地址等，使用可靠的加密算法加密存储。同时，所有的接口调用都会进行审计记录，并可进行精确回溯。

6.6.2 分布式消息服务（DMS）

分布式消息服务（DMS – Distributed Message Service）是基于高可用分布式集群技术构建的消息中间件服务，提供可靠且可扩展的托管消息队列，用于收发消息和存储消息。

DMS 可应用在不同领域，包括异步通信解耦、企业解决方案、金融支付、电信、电子商务、快递物流、广告营销、社交、即时通信、手游、视频、物联网、车联网等。可以应用于以下业务场景：

- **业务解耦：**将业务中依赖其他系统同时属于非核心或不重要的部分使用消息通知即可，无需同步等待其他系统的处理结果。如电商网站在促销期间的抢购订单，抢到的手机订单信息放入消息队列，出库、发货等后续会从队列里读取任务信息然后执行。
- **最终一致性：**在交易或支付系统中，不同的子系统/模块的状态需要最终保持一致，或都成功或都失败。子系统/模块之间传递的数据不丢失，保证业务的连续性。DMS 可以用于子系统/模块间的高可靠数据传递，实现两者之间的事务最终一致，降低实现难度和成本。
- **错峰流控：**在电子商务系统或大型网站中，上下游系统处理能力存在差异，处理能力高的上游系统的突发流量可能会对处理能力低的某些下游系统造成冲击，需要提高系统的可用性的同时降低系统实现的复杂性。电商大促销等流量洪流突然来袭时，可以通过队列服务堆积缓存订单等信息，在下游系统有能力处理消息的时候再处理，避免下游订阅系统因突发流量崩溃。消息队列提供亿级消息堆积能力，3 天保留时长，消息消费系统可以错峰进行消息处理。
- **日志同步：**应用通过可靠异步方式将日志消息同步到消息服务，再通过其他组件对日志做实时或离线分析，也可用于关键日志信息收集进行应用监控。

DMS 的访问认证和鉴权基于 IAM 来进行控制。通过身份验证后，账户可以完全拥有访问自己队列资源的所有操作权限；同时，通过策略控制可以授予其他服务或 IAM 用户访问和操作指定队列的权限。默认情况下，账户仅能访问自己所创建的队列。

此外，DMS 服务只支持使用 HTTPS 协议访问 DMS API 接口，默认支持 TLS 1.2 协议和 PFS 安全特性。基于安全性上的考虑，DMS 为用户提供数据进行加密后存储的选项，即服务端加密（SSE）。用户可以选择采用 DMS 提供的通用密钥进行服务端加密存储，也可以使用 KMS 服务创建的密钥进行加密存储。另外，用户在将消息数据发送至 DMS 之前也可以进行数据加密，可防止未授权人员访问敏感数据。

6.6.3 云桌面服务（Workspace）

云桌面服务（Workspace）是由华为云提供基于 Windows 的虚拟桌面基础架构（VDI – Virtual Desktop Infrastructure）与虚拟应用服务，用户可通过瘦客户端（硬件盒子）随时

随地接入云桌面办公。相较传统 PC 应用，云桌面使用防火墙对用户使用界面和用户数据界面进行隔离，数据存储和处理集中化，有效防患数据泄露。

云桌面的瘦客户端不保存数据，只运行客户端程序；客户端和云桌面之间采用华为自研的具有高安全性的 HDP（Huawei Desktop Protocol）协议转换消息，对于本地外设的 USB、多媒体、flash、键盘鼠标重新定向；界面只进行图像重绘，不传输业务数据。

用户在一个用户域内或通过网络专线，可以随时随地通过瘦客户端登录自己的云桌面。与过去携带电脑、移动存储设备相比，云桌面提高了工作效率，增加了灵活性。

云桌面集中管理用户使用的密码复杂度策略、会话超时、桌面发布、外设使用、补丁升级等，大幅提高管理员的维护效率。

所有硬件采用虚拟化管理，客户可以根据需要调整虚拟化资源的分配情况，有效延长桌面的使用寿命，并且有效降低硬件升级换代带来的成本投入。

云桌面具有以下安全功能：

- **用户身份识别：**系统为管理员和最终用户提供唯一的身份标识。同时将身份标识与所有可审计事件相关联。每次请求访问虚拟桌面前，系统会进行用户身份鉴别，身份鉴别机制使用的口令须达到一定的复杂度要求，例如长度要求、数字字母及特殊字符组合要求等。在设定的时限内，如用户没有任何操作，系统会自动断开会话或重新鉴别用户，系统提供默认的时限值。系统还提供鉴别失败的处理功能，当用户鉴别尝试不成功次数在一定时间段内超过指定值后，系统会锁定一段时间，以阻止用户在限定时间内更多的鉴别请求。
- **访问控制：**访问控制的覆盖范围包括与资源访问相关的主体、客体及它们之间的操作。访问控制主体为用户、业务系统等。授权用户对受保护资源进行访问的内容、操作权限不能超出预定义的范围。用户鉴权的相关数据以加密的方式存储。
- **传输安全：**采用 HDP 协议进行桌面访问，确保传输数据的保密性和完整性。支持对单个桌面的多重会话进行限制。支持网络传输 TLS 1.2 协议建立加密通道。
- **镜像安全：**支持对虚拟机镜像文件进行完整性、机密性保护，并确保虚拟机的镜像、快照的剩余信息得到完全清除。
- **备份与恢复机制：**提供 VDI 系统的管理数据备份机制，保障备份数据可以恢复。
- **安全监控：**支持对用户在线状态、用户使用状态、虚拟机运行状态、终端在线状态等的实时监控。

- **安全审计：**日志可记录所有对系统产生影响的用户活动、操作指令，用以支撑事后审计。审计日志包括登录类型、操作类型、日志级别、事件时间、事件主体、IP 地址、事件描述和事件结果等字段，经过授权的用户才能对系统日志进行审计。审计日志存储在掉电非遗失性存储介质中。当存储空间将要耗尽时，提供转储机制，保证审计日志不丢失。保护审计日志不被未授权的访问、修改和破坏。

6.7 管理服务

6.7.1 云监控服务（CES）

云监控服务（CES – Cloud Eye Service）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。CES 提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。需要强调的是，CES 的监控对象是基础设施的资源使用数据，不监控或触碰租户数据。

CES 目前可以监控下列云服务的相关指标：弹性计算服务（ECS）、云硬盘服务（EVS）、虚拟私有云服务（VPC）、关系型数据库服务（RDS）、分布式缓存服务（DCS）、分布式消息服务（DMS）、弹性负载均衡（ELB）、弹性伸缩服务（AS）、网站应用防火墙（WAF）、主机漏洞检测服务（HVD）、云桌面服务（Workspace）、机器学习服务（MLS）、网页防篡改服务（WTP）、数据仓库服务（DWS）、人工智能服务（AIS）等¹⁴。用户可以通过这些指标，设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。

CES 服务器的分布式特性确保高可用性，资源使用监控及时有效，监控指标实时采样，告警通知可按设置规则及时准确触发。

只有通过华为云 IAM 认证的租户才能使用 CES 服务，使用方式包括服务控制台、开放接口、命令行和 SDK 等。CES 的数据以租户维度进行存储隔离，只有认证通过的租户才能访问其对应的监控数据。

¹⁴ 下列华为云服务未收入此白皮书：主机漏洞检测服务（HVD – Host Vulnerability Detection service）、机器学习服务（MLS – Machine Learning Service）、网页防篡改服务（WTP – Web Tampering Protection service）、数据仓库服务（DWS – Data Warehousing Service）、人工智能服务（AIS – Artificial Intelligence Service）。敬请登录 <https://www.huaweicloud.com/> 了解更多详情。

6.7.2 云审计服务（CTS）

云审计服务（CTS – Cloud Trace Service）为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的 API 执行的操作，以及华为云系统内部触发的操作。CTS 是满足用户专业认证以及 IT 合规性认证的不可或缺的支撑性服务，其具有以下功能：

- **资源变更审计：**华为云上的资源和系统配置变更，可通过 CTS，实时、系统地记录所有人员的操作，优越于传统企业 IT 环境中需要人为手工执行事后审计的各项 IT 变更。
- **访问安全审计系统性与实时性：**CTS 实时、系统地记录用户在管理界面上的所有操作和用户在华为云上的所有 API 操作，便于进行问题查询、分析与定位。
- **数据审计：**借助 CTS 中记录的对象级 API 事件，用户可以通过收集 OBS 对象上的活动数据来检测数据泄露情况。
- **低成本：**CTS 支持将操作记录合并，周期性地生成事件文件，实时同步转存至 OBS 存储桶，帮助用户实现操作记录高可用、低成本的长久保存。

CTS 作为华为云的管理服务之一，其安全设计是在华为云安全架构基础上构建的。主要涉及安全组网、网络边界安全防护、应用安全防护以及数据安全防护四个层面，确保向租户提供安全的云审计服务。这里重点介绍应用和数据安全层面，其他层面内容可参考第 5 章基础设施安全相关章节。

- **应用安全：**CTS 接收和处理合法用户发起的合规事件查询、追踪器操作请求，以及已与 CTS 完成对接的服务发来的合规事件。所有请求采用 HTTPS 协议传输，敏感数据进行加密，在与外部服务进行交互时有端口控制、白名单控制、请求发起方身份及请求内容多重验证等方式，保证应用安全。此外，CTS 的控制台节点的 Web 安全进行了安全加固，防范各种攻击。
- **数据安全：**CTS 所处理的用户日志数据，在生成阶段，会要求各服务内部进行脱敏，并会对各服务发送过来的日志数据进行检视，确保数据本身不含敏感信息；在传输阶段，通过身份认证、格式校验、白名单校验以及单向接收机制等手段，确保日志信息传输和保存的准确、全面；在保存阶段，采取多重备份，并根据华为网络安全规范要求，对数据库自身安全进行安全加固，杜绝仿冒、抵赖、篡改以及信息泄露等风险；最后，CTS 支持数据以加密的方式保存到 OBS 桶。

6.7.3 企业项目管理服务（EPS）

企业项目管理服务（EPS – Enterprise Project Service）是提供给企业客户的与多层级组织和项目结构相匹配的云资源管理服务。主要包括企业项目管理、财务管理和人员管理。企业项目管理提供统一的云资源按企业项目管理，以及企业项目内的资源管理、成员管理。财务管理提供多个华为云账号之间形成企业主子账号关联关系的能力，用户可以根据自己的企业结构创建组织、新建子账号或关联子账号，并使其从属于创建的组织，从而对这些子账号的财务进行管理。企业项目的用户归属于用户组，人员管理对这些用户和用户组进行管理，包括为用户设置凭证、创建、修改、删除用户和用户组等。

目前 EPS 已支持弹性云服务器(ECS)、弹性伸缩(AS)、镜像服务(IMS)、云硬盘(EVS)、虚拟私有云(VPC)、弹性公网 IP(EIP)、内容分发网络(CDN)、关系型数据库(RDS)、分布式缓存服务(DCS)、文档数据库服务(DDS)、云容器引擎服务(CCE)、DDoS 高防服务(AAD)、裸金属服务器(BMS)、专属主机(DeH)、微服务引擎(CSE)等服务的管理。

租户可通过服务控制台或 EPS API 来使用。EPS 采用基于租户的权限模型、严格参数校验、安全通讯协议、敏感信息保护、审计日志等安全措施，保护管理系统免受上述攻击的危害。为保证业务灵活性，EPS 还提供灵活的授权访问机制：访问 EPS 服务的账户包括华为云账户、基于 IAM 服务创建并被授权 EPS 访问权限的用户，以及租户授权的云服务等。华为云账户可以访问 EPS 的所有操作；基于 IAM 服务创建并被授权 EPS 管理员访问权限的用户，可以访问 EPS 的所有操作；基于 IAM 服务创建并被授权租户访问权限的用户，只能做 EPS 服务的查询类操作。

EPS 服务只支持使用 HTTPS 协议访问 EPS API 接口，默认支持 TLS 1.2 协议和 PFS 安全特性。对所有租户的接口调用都会做严格的参数校验，以确保服务不会受恶意攻击的影响。同时，所有的接口调用都会进行审计记录，并可进行精确回溯。

6.7.4 标签管理服务（TMS）

标签管理服务（TMS – Tag Management Service）是一种快速便捷将标签集中管理的可视化服务，提供跨区域、跨服务的集中标签管理和资源分类功能：

- 资源标签管理：通过给账户下资源添加标签，可以对资源进行自定义标记，实现资源的分类。标签管理服务为用户提供可视化表格操作资源标签，并支持对标签进行批量编辑。

- 资源标签搜索：用户可以跨服务、跨区域对资源进行按标签搜索，还可以多标签组合搜索。
- 预定义标签管理：用户可以创建或导入/导出预定义标签。通过标签的预定义操作，用户可以从自身业务角度规划标签，实现标签的高效管理。

TMS 不涉及用户隐私数据的存储，调用其他服务的接口，都是通过内部鉴权透传方式，统一由 IAM 鉴权。租户可通过服务控制台或 TMS API 来使用。TMS 采用基于租户的权限模型、严格参数校验、安全通讯协议、敏感信息保护、审计日志等安全措施，保护管理系统免受上述攻击的危害。TMS 还提供灵活的授权访问机制：访问 TMS 服务的账户包括华为云账户、基于 IAM 服务创建并被授权 TMS 访问权限的用户，以及租户授权的云服务。

TMS 服务只支持使用 HTTPS 协议访问 API 接口，默认支持 TLS 1.2 协议和 PFS 安全特性。对所有租户的接口调用都会做严格的参数校验，以确保服务不会受恶意攻击的影响。同时，所有的接口调用都会进行审计记录，并可进行精确回溯。

6.7.5 资源模板服务（RTS）

资源模板服务（RTS – Resource Template Service）帮助用户简化云计算资源管理和自动化运维工作。用户遵循资源模板服务定义的模板规范，编写模板文件，并在模板中定义云计算资源的集合以及资源间的依赖关系、资源配置等，资源模板服务通过编排引擎自动完成模板中所有资源的创建和配置，以达到自动化部署、简化运维的目的。资源模板服务支持原生 OpenStack Heat 组件的大部分 API 接口以及 HOT（Heat Orchestration Template）格式的模板。用户可通过调用 API 接口或管理控制台使用资源模板服务。管理控制台是资源模板服务的可视化用户界面，用户可通过管理控制台自动部署资源。

RTS 不涉及用户隐私数据的存储，调用其他服务的接口，都是用过内部鉴权透传方式，统一由 IAM 鉴权。租户可通过服务控制台或 RTS API 来使用。RTS 采用基于租户的权限模型、严格参数校验、安全通讯协议、敏感信息保护、审计日志等安全措施，保护管理系统免受上述攻击的危害。RTS 还提供灵活的授权访问机制：访问 RTS 服务的账户包括华为云账户、基于 IAM 服务创建并被授权 RTS 访问权限的用户，以及租户授权的云服务。

RTS 服务只支持使用 HTTPS 协议访问 API 接口，默认支持 TLS 1.2 协议和 PFS 安全特性。对所有租户的接口调用都会做严格的参数校验，以确保服务不会受恶意攻击的影响。同时，所有的接口调用都会进行审计记录，并可进行精确回溯。

6.8 安全服务

6.8.1 统一身份认证服务（IAM）

统一身份认证服务（IAM – Identity and Access Management）提供适合企业级组织结构的用户账号管理服务，为企业用户分配不同的资源及操作权限。用户通过使用访问密钥获得基于 IAM 的认证和鉴权后，以调用 API 的方式访问华为云资源。

IAM 可以按层次和细粒度授权，保证同一企业租户的不同用户在使用云资源上得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保租户业务的持续性。

- **密码认证：**密码是租户最初创建账户（注册或创建企业用户）时指定的。用户在登录华为云控制台时，需要使用密码。同时，该密码也可以用于 API 方式访问华为云资源。
 - **密码策略：**IAM 支持租户的安全管理员根据需求，设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码，导致账号泄露。
 - **登录策略：**IAM 支持租户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等，导致账号信息泄露。
 - **ACL：**IAM 通过提供基于 IP 的 ACL 可以限制企业用户只在安全的网络环境下访问华为云资源，避免企业用户因接入不安全网络环境导致的数据泄露。
- **多因子认证（MFA）：**多因子认证（MFA – Multi-Factor Authentication）是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信验证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。
- **访问密钥：**当企业管理员使用运维工具或 API 命令管理华为云上的资源时，访问密钥用于对 API 请求进行签名，API 网关则校验签名信息。数字签名和时间戳可以防止数据传输过程中请求被篡改，确保消息完整性，并防止潜在的重放攻击。

企业管理员可随时通过“我的凭证”页面创建和下载访问密钥，并且查看其状态。出于安全考虑，密钥一旦丢失或遗忘，则无法恢复或重新下载。此时，用户可创建新的密钥，然后禁用或删除旧的密钥。为避免滥用，密钥须妥善保存并定期更改，万勿嵌入代码中。

- **联邦认证：**如果租户有安全可靠的外部身份认证服务（如 LDAP 或 Kerberos）验证用户的身份并且该外部服务支持 SAML 2.0 协议（SAML – Security Assertion Markup Language），那么租户可以将该服务作为身份提供商（IdP – Identity Provider），将华为云配置为服务提供商（SP – Service Provider）。这样企业租户在不需要将其用户信息同步到华为云的情况下，租户就可以基于 SAML 协议登录华为云服务控制台，或者通过 API 方式访问云资源。

租户可以在有限时间内，通过联邦认证把外部用户映射成华为云的临时用户，并访问租户的华为云资源。出于安全考虑，需要创建合理的用户组（权限集合），将该临时用户映射并限定在对应的用户组权限内。

如果租户创建一个移动或基于 Web 的应用程序访问华为云资源，则应用程序中不应嵌入长期安全认证凭据。可以让用户登录到所需应用程序，然后使用其验证过的身份信息，通过联邦认证来获取临时安全凭据。

- **权限管理：**IAM 权限包括用户管理权限和云资源权限。用户管理权限可以管理用户、用户组及用户组的权限，实现用户及用户组的创建、删除、修改和为用户授予相应的权限。云资源权限包括对云资源的创建、删除、修改、设置等操作的权限。为用户组添加云资源权限，再将用户加入用户组，可以使用户继承用户组的权限。通过用户组来管理用户权限可以使权限管理更有条理，避免权限管理的混乱。另外，IAM 结合 PAM 功能还可以更有效地细化管理特权账户。

6.8.2 数据加密服务（DEW）

数据加密服务（DEW – Data Encryption Workshop）是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块（HSM）保护，并与许多华为云服务集成。用户也可以借此服务开发自己的加密应用。通过专属加密服务（DHSM – Dedicated HSM），用户可以选择基于国家密码局认证或 FIPS 140-2 第 3 级验证的硬件加密机，实现高性能、用户独享的加密能力，支持 SM1~SM4 的国产密钥加密算法，将硬件加密机托管到云上与用户应用放置在同一个 VPC 内，加密机机框、电源、带宽、接口资源全部归该租户独占使用，在应用加解密时，通过 API 接口实现最高每秒钟 10000TPS 以上的运算性能，从而满足海量用户并发使用的需求。加密的根密钥产生，通过邮寄 Ukey（物理介质）的方式，由用户的安全管理员导入自己定义的密钥材料，甚至可以多个用户联合生成密钥因子，生成的根密钥（Root Key）存储在 HSM 里，该加密机为经过国家密码局认证的第三方设备，包括加密机厂家、云服务提供商在内的任何人，都无法访问到根密钥。该根密钥来加密用户主密钥，用户主密钥再来加密用户

数据密钥。因此即使是云服务提供商，也无法得知用户主密钥和数据密钥的明文内容。

通过密钥管理（KMS – Key Management Service），用户能够方便地管理自己的密钥，并能随时使用数据加密密钥（DEK – Data Encryption Key）进行数据加密，确保关键业务数据的安全。DEK 使用保存在 KMS 中的用户主密钥（CMK – Customer Master Key）进行加密，CMK 使用保存在 HSM 中的根密钥（Root Key）进行加密，以密文的形式保存在密钥存储节点中，保证密钥不会泄露。HSM 作为信任根，构成完整的信任链。HSM 拥有 FIPS 140-2（2 级和 3 级）的主流国际安全认证，满足用户的数据合规性要求。

KMS 实现了同云存储服务，如云硬盘服务（EVS）、对象存储服务（OBS）的对接，用户配置存储服务时，仅需选择加密所需主密钥，即可实现云端数据加密存储。KMS 为各个云服务提供加密特性，对用户数据进行全方位的加密，满足用户对敏感数据的加密要求，让用户安心使用云服务，专注于核心业务的开发，而不是密钥管理。

为保障租户密钥的安全可靠，KMS 提供了多个安全特性：

- **密钥随机生成：**KMS 中所有密钥均由 HSM 的硬件真随机数生成器生成，保证密钥的随机性。
- **密钥安全存储：**KMS 的根密钥保存在 HSM 中，从来不会出现在 HSM 之外，确保根密钥不泄露。HSM 采用双机部署，保证 HSM 的高可靠性和高可用性。CMK 经过根密钥加密后，以密文的形式保存在密钥存储节点中。密钥存储节点采用经过安全加固的 MySQL 数据库保存经根密钥加密后的 CMK。MySQL 数据库以双机主备模式部署，用户密钥在保存到主 MySQL 的同时，会备份到备 MySQL 中，一旦主 MySQL 发生故障无法提供服务，备 MySQL 仍可正常工作和访问，保证服务不中断。HSM 作为信任根，与上述其他密钥保护设备一起，构成完整的信任链。
- **密钥延迟删除：**KMS 提供对 CMK 的全生命周期管理，包括 CMK 的启用、禁用、删除。其中，KMS 提供的密钥延迟删除功能，租户必须设置 CMK 延迟删除时间（7 天~3 年），在这个时间段内，租户都可以取消删除 CMK，避免误删。
- **KMS 灾备：**KMS 提供完善的密钥备份机制和灾备功能，保证用户的密钥不会因为不可抗力而丢失，确存储保存在 KMS 的密钥高可用。即使发生重大的灾难事故，通过 KMS 服务倒换操作，实现服务的连续性。保存在 HSM 中的根密钥，会备份在 HSM 专有备份工具中。保存 CMK 的密钥存储节点，定期频繁进行增量和全量备份，将密钥备份到指定的存储设备中。一旦发生特殊事件导致用户密钥丢失，KMS 可以通过备份数据将用户密钥恢复。

- **主机信任链接：**KMS 主机均使用标准的加密传输模式与 KMS 服务节点建立安全通信链接，保证 KMS 相关数据在节点间的传输安全。
- **访问控制：**KMS 基于 IAM 角色统一进行 RBAC 访问控制。对于用户，只有通过 IAM 身份验证及 KMS 鉴权，并设置了密钥操作权限的用户，才能操作 KMS 中存储的 CMK。仅设置了只读权限的用户只能查询 CMK 信息，不能对 CMK 进行操作。KMS 对 CMK 进行了租户隔离，每一个租户只能访问与管理属于自己的 CMK，无法操作其他租户的 CMK。此外，系统管理员仅有设备管理权限，没有任何访问 CMK 的权限。
- **操作日志审计：**对密钥的所有操作（例如创建用户主密钥、加密数据密钥等），都会产生日志并记录到云审计服务（CTS）中，便于后期审计 CMK 的操作活动等。

此外，KMS 服务还通过华为云自身的一系列技术，如安全的基础架构平台、安全组网、边界防护、区域划分、虚拟网络隔离、租户 KMS 实例隔离、API 接口安全等，增强其安全能力，保障 KMS 服务自身的业务安全。

6.8.3 防 DDoS 攻击服务（Anti-DDoS Service）

防 DDoS 攻击服务（Anti-DDoS Service）通过专业的防 DDoS 设备，精准有效地实现对流量型攻击和应用层攻击的全面防护；快速响应，为大中小型企业、互联网初创公司等提供安全防护能力，保障企业门户及网站安全，并极大地节约用户投资。Anti-DDoS 服务提供精细化的抵御 DDoS 攻击的功能，包括但不限于 Ping Flood、SYN Flood、UDP Flood、Challenge Collapsar（CC）、HTTP Flood、DNS Flood。用户只需根据租用带宽及业务模型自助配置防护阈值，系统检测到攻击后，就会实时通知用户，并进行有效防御。

目前 Anti-DDoS 服务提供如下功能：

- **自助设置防护策略：**用户可根据租用带宽及业务模型自助选择防护模板。
- **流量检测和清洗：**用户开启服务后，实时进行流量检测，对于满足阈值条件的攻击流量，进行清洗。
- **便捷管理：**配套提供高度管控、灵活使用的管理平台，用户可通过报表功能实时了解流量曲线，配置简单、服务资源监控方便。
- **报表监控：**提供查看单个公网 IP 的监控功能，包括当前防护状态、当前防护配置参数、24 小时以前直到现在的流量情况、24 小时以内的异常事件（清洗和黑洞）；提供安全报告查看功能。查看区间为一周，支持查询前四周统计数据，包括防护流

量、攻击次数、攻击 Top 10 排名等。

- **日志分析：**提供 Anti-DDoS 设备日志接收、分析和上报等功能，通过界面将结果呈现给用户。

Anti-DDoS 服务还通过华为云自身的一系列技术，如安全的基础架构平台、安全组网及边界防护、虚拟机网络隔离、API 接口安全与日志审计等，增强其安全能力，保障 Anti-DDoS 服务自身的业务安全。

6.8.4 企业主机安全服务（HSS）

企业主机安全（HSS – Host Security Service）是服务器的贴身安全管家，提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为，以及满足等保合规的要求。

华为云企业主机安全服务提供以下主要功能：

- **资产管理：**提供账号、端口、进程、Web目录和软件等安全资产信息的管理和分析。
- **漏洞管理：**检测Windows/Linux操作系统与SSH、OpenSSL、Apache、Mysql等软件存在的漏洞，并给出修复建议。
- **基线检查：**检测系统口令复杂度策略、经典弱口令、风险账号，以及常用系统与中间件的配置，识别不安全项目，预防安全风险。
- **账户破解防护：**检测SSH、RDP、FTP、SQL Server、MySQL等账户遭受的口令破解攻击，对识别出的攻击源IP封锁24小时，禁止其再次登录，防止主机因账户破解被入侵。
- **双因子认证：**结合短信/邮箱验证码，对云服务器登录行为进行二次认证，极大地增强云服务器账户安全性。
- **关键文件变更检测：**对于系统关键文件（例如：ls、ps、login、top等）进行监控，一旦文件被修改就进行告警，提醒用户关键文件存在被篡改的可能。
- **恶意程序检测：**通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，并提供一键隔离查杀能力。
- **网站后门检测：**检测云服务器上Web目录中的文件，判断是否为 WebShell 木马文件，支持检测常见的PHP、JSP等后门文件类型。
- **网页防篡改：**保护网站的网页、电子文档、图片等文件不被黑客篡改和破坏。

华为云企业主机安全服务主要有以下优点：

- **主机风险预防效果好：**通过资产管理、漏洞管理和基线检查功能，能够发现与预防主机的漏洞、弱密码及不安全配置，帮助用户主机减少 90% 的被攻击面。
- **账户破解防护能力强：**通过主机登录双因子认证功能，结合先进的防护算法，能够有效预防暴力破解攻击。
- **恶意程序检出率高：**通过行为分析与基于 AI 的图像指纹算法，能够有效检测与查杀未知与变种的恶意程序，检出率业界领先。
- **网页防篡改效果佳：**网页防篡改版本提供 Web 文件目录锁定、篡改检测自动恢复和远端备份恢复的三重防护能力，彻底杜绝黑客网页篡改行为，是政府、教育行业与大企业官网的必备安全服务。
- **等保测评必备服务：**企业主机安全的入侵检测功能满足主机入侵防范，恶意代码防范条款；漏洞管理功能满足主机漏洞扫描条款；网页防篡改功能满足数据完整性条款。

6.8.5 容器安全服务（CGS）

容器安全服务（CGS – Container Guard Service）能够扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题；同时提供容器进程白名单、文件只读保护和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。

华为云容器安全服务提供以下主要功能：

- **镜像漏洞管理：**可扫描华为云容器镜像服务中的私有镜像、官方镜像以及节点中所有正在运行的镜像，发现镜像中的漏洞并给出修复建议，帮助用户得到一个安全的镜像。
- **容器安全策略管理：**通过配置安全策略，帮助企业制定容器进程白名单和文件保护列表，从而提高容器运行时系统和应用的安全性。
- **容器进程白名单：**提供的进程白名单功能，能有效阻止异常进程、提权攻击、违规操作等安全风险事件的发生。
- **文件保护：**容器中关键的应用目录（例如：bin, lib, usr 等系统目录）应该设置只读保护以防止黑客进行篡改和攻击。容器安全服务提供的文件保护功能，可以将这些目录限制为只读目录，有效阻止文件篡改等安全风险事件的发生。

- **容器逃逸检测:** 扫描所有正在运行的容器,发现容器中的异常(包括逃逸漏洞攻击、逃逸文件访问等)并给出解决方案。

6.8.6 云 Web 应用防火墙服务 (WAF)

华为云 WAF 是结合了华为多年攻防经验和一系列针对性优化算法的高级 Web 应用防火墙。采用正则规则和语义分析的双引擎架构,对 SQL 注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意 bot、webshell、CC 等攻击实现实时的高性能防护。

华为云 WAF 给用户提供了简便的管理界面,用户可根据自身业务需要进行相关防护设置,亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。

华为云 WAF 服务具有如下功能:

- **常见 Web 攻击海量过滤:** 华为云 WAF 可识别 99% 的 Web 攻击,包括 SQL 注入、XSS、命令注入、代码注入、目录遍历、敏感文件获取等常见 (OWASP Top 10) 攻击类型,并能检测在网址、参数、头字段等位置的恶意攻击有效载荷。
- **强大的编码还原功能:** 能够对 url_encode, Unicode 编码, xml 编码, C-OCT 编码, 十六进制编码, html 转义编码, base64 编码, 大小写混淆, javascript、shell、php 等拼接混淆进行还原等。
- **CC 攻击防护:** CC 攻击 (应用层 DDoS 的一种) 会占用大量业务资源,影响正常业务体验。华为云 WAF 可基于 IP、cookie 和 Referer 信息对用户进行标识,并通过灵活的配置阈值,执行访问限速,对超过阈值的访问者,可阻断其请求,避免对业务造成压力;也可发起验证码挑战,进行人机识别,更精准地将攻击者甄别出来,并进行阻断。
- **Webshell 防范:** 华为云 WAF 通过对 HTTP(S) 传输通道的内容检测,对各种类型的 Web shell 进行检测和阻断,防止其给业务带来后续危害。用户可以一键启用该功能,对业务进行防护。

同时,华为云 WAF 服务使用简便、易于管理:

- **自定义精准控制:** 用户可以通过华为云 WAF 提供的接口,设置自定义的检测规则。包括自定义的黑白 IP 名单、用户代理黑名单及其他更复杂的检测规则。
- **隐私过滤:** 可避免在 WAF 的事件日志中出现涉及用户隐私的用户名密码等信息。用户可灵活自定义过滤规则,实现隐私过滤。

- **集中管理：**在后端对 WAF 节点集中管理，如策略下发、事件日志的查看处理等。

6.8.7 数据库安全服务（DBSS）

数据库安全服务（DBSS – Database Security Service），包括数据库安全审计和数据库安全防护两大功能模块，提供数据库审计、数据泄露保护、数据库防火墙三大功能，可以全面保障云上数据库安全和资产安全。

1、数据库安全审计

数据库安全审计提供的旁路模式数据库审计功能，可以对风险行为进行实时告警，并对攻击行为进行阻断。同时，通过生成满足数据安全标准的合规报告，可以对数据库的内部违规和不正当操作进行定位追责，有效检测并阻断外部入侵，保障数据资产安全。提供用户行为发现审计、多维度分析、实时告警和报表功能：

- **用户行为发现审计：**关联应用层和数据库层的访问操作，支持协助用户溯源到应用者的身份和行为。
- **多维度线索分析：**（1）风险线索：支持从高中低的风险等级、SQL 注入、黑名单语句、违反授权策略等 SQL 行为进行分析。（2）会话线索：支持根据时间、用户、IP 地址、客户端等多角度进行分析。（3）详细语句线索：提供用户、客户端 IP、访问时间、操作对象、操作类型等多种检索条件。
- **异常操作、SQL 注入、黑白名单实时告警：**（1）异常操作风险：支持通过客户端 IP、数据库 IP、数据库用户、风险等级等多种元素细粒度定义要求监控的风险访问行为。（2）SQL 注入：提供系统性的 SQL 注入库，以及基于正则表达式或语法抽象的 SQL 注入描述，发现数据库异常行为立即告警。（3）黑白名单：通过准确而抽象的方式，对系统中的特定访问 SQL 语句进行描述，并在 SQL 语句出现时实时告警。
- **针对各种异常行为提供精细化报表：**（1）会话行为：提供登录失败报表、会话分析报表。（2）SQL 行为：提供新型 SQL 报表、SQL 语句执行历史报表、失败 SQL 报表。（3）风险行为：提供告警报表、通知报表、SQL 注入报表、批量数据访问行为报表。（4）合规报表：提供满足数据安全标准（例如 Sarbanes-Oxley）的合规报告。

华为云数据库安全审计具备如下优势：

- **部署简单：**采用数据库旁路部署方式，操作简单，快速上手。
- **全量审计：**支持对华为云上的 RDS、ECS/BMS 自建的数据库进行审计。

- **快速识别：**实现 99%+ 的应用关联审计、完整的 SQL 解析、精确的协议分析。
- **高效分析：**每秒万次入库、海量存储、亿级数据秒级响应。
- **多种合规：**满足等保三级数据库审计需求，满足网络安全法，SOX¹⁵等国内外法案。
- **三权分立：**系统管理员，安全管理员，审计管理员权限分离，满足审计安全需求。

2、数据库安全防护

数据库安全防护主要提供如下功能：

- **数据库防火墙：**支持用户自定义配置防火墙策略、自动学习策略及基于异常检测的 IDS/IPS 策略，当请求到达数据库防火墙且违反策略时，DBSS 会根据用户需求选择实时告警或阻断。DBSS 还可通过机器学习，建立用户访问行为基线，生成查询模式组并可应用至数据库防火墙策略中。
- **权责分离机制：**通过细粒度的帐户管理和权限控制，可以按照角色类型、表、视图对象、列等进行权限控制。
- **SQL 注入检测和防御：**DBSS 内置了 SQL 注入特性库、基于上下文的学习模型和评分机制，对 SQL 注入进行综合诊断，并实时阻断，从而确保用户数据库免受 SQL 注入攻击。
- **动态数据脱敏：**用户可以设置脱敏规则来对指定数据库表/列以及来自特定源 IP、用户和应用的查询进行脱敏。通过精确的脱敏引擎，对用户的敏感数据实施实时脱敏，不会对应用产生性能损耗，也不会改变数据在数据库中的存储。
- **敏感数据发现：**DBSS 内置 PCI、HIPAA¹⁶、SOX、GDPR 等合规知识库，用户也可以自定义敏感数据的规则知识库，并通过配置相应敏感数据发现策略来发现数据库中的敏感数据。一旦识别了敏感数据，可以一键自动生成脱敏规则和审计规则。
- **数据库防拖库：**用户可以设置防拖库规则来对未授权用户、IP 地址和应用在数据库特定表中的数据操作进行检测，当操作数据量超过规则设定的阈值后，DBSS 将会向管理员发出告警，并将该事件记录至防拖库日志中，协助用户避免数据泄露。

数据库活动监控：DBSS 提供数据库的库级、表级和列级的视图监控，可独立监控和分

¹⁵ SOX 即 Sarbanes-Oxley Act，是于 2002 年美国国会通过的美国联邦法律，为所有美国上市公司董事会，管理层和公共会计师事务所设定了更新更广的监管要求。

¹⁶ HIPAA 即 Health Insurance Portability and Accountability Act of 1996，是于 1996 年美国国会通过的美国联邦法律，建立起了美国健康保险的便携性和问责制度，为保护医疗信息提供数据隐私和安全规定。

析数据库活动，并对未授权的活动进行监控和告警。提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访问时间、请求的数据库、原 SQL 语句、操作、成功与否、耗时和返回内容等，协助用户溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。

7 工程安全

在传统 ICT 领域，华为持续向客户交付安全、优质的产品和服务。在这个过程中积累了大量的产品安全开发能力、工具和经验。华为进入云服务市场后，这些知识和经验同样也在帮助华为云构筑多维全栈的安全防护体系和高可用、高可信的云服务。同时，云服务特有的持续集成，持续交付，持续部署需要全新思维、方法论、流程和工具链。通过结合华为在安全上的长期积累和华为云的现状，华为云不仅积极推行快速迭代的全新 DevOps 流程，还将华为的安全生命周期（SDL）无缝嵌入，DevOps 逐步形成高度自动化的 DevSecOps 全新安全生命周期管理流程，以及确保全新流程顺利而灵活执行的云安全工程能力和工具链。本章除了对 DevOps/DevSecOps 流程的介绍，还会重点描述华为云安全流程中尤为重要的安全设计、安全编码和测试、第三方软件管理、配置与变更管理、上线安全审批等方面的具体实践。

7.1 DevOps 和 DevSecOps 流程

由于华为云服务商业模式的变化，华为云已经建立起新的组织结构、管理体系并采用更适合云服务的 DevOps 模式进行开发、部署和运营。相较于适合传统 ICT 业务的研发流程，DevOps 有如下典型变化：

- **商业决策：**从基于 Gate（DCP/TR）的决策向基于业务用例（business case）的定期审视转变。
- **产品开发和交付模式：**交付的对象为线上业务或服务，而 DevOps 的定位就是在华为云管理体系中负责云服务业务快速上线的新型研发和运维模式。
- **营销模式：**引进互联网的营销模式。
- **产业链和生态：**在新的运营模式下建立联盟合作、合作伙伴管理及价值分配机制。

- **供应链**：对用户提供服务，但资产还属于华为。
- **财务**：系统需适应互联网交易模式。

运营驱动开发、小步快跑、频繁部署是 DevOps 的关键特征。因此，在 DevOps 模式下，各项安全活动也融入新的流程活动中。华为云已经采用全新的持续集成、持续交付、持续部署、快速迭代 DevOps 流程。并且，华为云将高可靠、高稳定的安全研发和运维运营要求结合在 DevOps 流程中，形成适合华为云的 DevSecOps 流程。

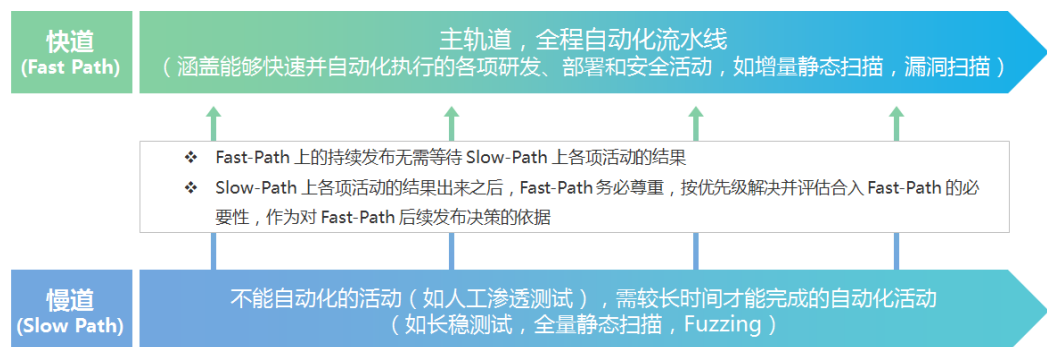
DevSecOps 聚焦于实现以下两个关键目标：

- **安全质量**：在 DevOps 模式下始终确保各项云服务达到其所需安全活动的质量标准。
- **进度**：保证云服务安全活动不影响 DevOps 的快速持续集成、发布与部署。

7.1.1 双轨制（Dual Path）机制

针对云服务需要快速持续集成、发布与部署，但部分研发运维中必需的安全活动很耗时的矛盾，华为云采用双轨制平衡进度与质量。双轨制的本质是将快速活动、慢速活动分轨道开展，避免慢速活动延迟云服务的快速持续交付与部署。

图7-1 华为云 DevOps/DevSecOps 双轨制流程



双轨制的活动定义：

- **快速（Fast Path）**：完全自动化流水线，其中包含能够快速自动化执行的各种安全活动，如增量静态扫描、动态扫描、攻击面分析等。
- **慢速（Slow Path）**：半自动或手动流水线，包含不能完全自动化的安全活动，如需要人工执行的渗透测试，以及需要很长时间才能完成的自动化安全活动，如静态扫描、长稳测试、渗透测试、业务连续性测试、模糊测试、动态程序分析、威胁和脆弱性测试等。

弱性分析、容量测试等。

双轨制的协作关系如下：

- 快道是 DevOps 流程的主航道，对于已完全自动化的安全活动一旦达到安全质量门限，则开发和运维运营活动快速执行通过。快道不需要等待慢道上各项安全活动的结果。消除高风险的云服务安全活动优先自动化，放在快道上执行。
- 慢道上安全活动的结果需要作为后续发布的决策依据，快道也必须遵从。例如，慢道发现的严重安全隐患可叫停快道，并在严重问题得到优先解决之后才可重启快道。

7.2 安全设计

华为云秉承华为一贯坚持的安全源自优秀设计的理念，这与采用 DevOps/DevSecOps 流程没有矛盾。华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。威胁分析使用的引导分析威胁库、消减库、安全设计方案库来源于包括传统领域产品和新的云领域所有产品的安全积累和业界优秀实践。当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。

7.3 安全编码和测试

华为云严格遵从华为对内发布的安全编码规范。华为云服务研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了静态代码扫描工具每日检查，其结果数据进入云服务持续集成和持续部署（CI/CD – Continuous Integration, Continuous Deployment）工具链，通过质量门限进行控制，以评估云服务产品的质量。所有云产品、云服务在发布前，均需完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。

所有云服务发布前都经过了多轮安全测试，包括但不限于 Alpha 阶段的认证、鉴权、会话安全等微服务级功能和接口安全测试，Beta 阶段通过对 API 和协议的 fuzzing 测试验证服务集成，Gamma 阶段的数据库安全等安全专项测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。同时，华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如 SecureCat 可以对业界主流的 OS 和 DB 的安全配置进行检查。除了一次融入、多次使用的优点外，

这样做还能带来另一个明显的好处，即发布的云服务通过测试后可同时满足不同区域、客户的安全要求。

7.4 第三方软件安全管理

华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。在使用中，须将第三方软件作为服务或解决方案的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或解决方案中使用独立的第三方软件是否引入新的安全问题。

华为云将网络安全能力前置到社区，在出现开源漏洞问题时，依托华为云对开源社区的影响力，第一时间发现漏洞并修复。漏洞响应时，须将开源及第三方软件作为服务和解决方案的一部分开展测试，验证开源及第三方软件已知漏洞是否修复，并在服务的 **Release notes** 里体现开源及第三方软件的漏洞修复列表。

7.5 配置与变更管理

华为云配置和变更管理对保障华为云安全起着重要作用。华为云设置配置经理对所有业务单元进行配置管理，包括提取配置模型(配置项类型、各类配置项属性、配置项间的关系等)，记录配置信息等。并通过专业的配置管理数据库工具（**CMDB – Configuration Management Database**）对配置项、配置项的属性和配置项之间的关系进行管理。

华为云的各项变更都是影响云服务运行的因素。生产环境的各要素，如机房设施、网络、系统平台软硬件和应用等的更改，包括设备增减、架构调整、系统软件更新（含网络系统，操作系统镜像和应用容器）、配置改变等发生变更，都需要通过有序的活动进行变更管理。所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。

7.6 上线安全审批

为确保华为云以及华为开发的云服务满足各区域法律法规、客户安全需求，华为的全球网络安全与用户隐私保护官（GSPO）和首席法务官（CLO – Chief Legal Officer）也参与到云服务的上线活动中。云平台版本、重要云服务上线前，GSPO 和 CLO 的团队和开发团队合作，共同分析、判断其相关版本或服务是否符合所服务区域的安全隐私合规要求。

同时，简化的华为云上线安全审批流程确保中低安全风险的云服务可以快速上线。GSPO 和 CLO 制定并发布安全与隐私合规的自检清单，该清单包含所有主要区域、行业的合规要求。云服务团队在开发、部署、上线过程中需进行自检，对于中低风险的云服务，自检通过后即可上线。自检结果也同步提交给 GSPO 和 CLO 执行审计。对高风险的云服务，通过更多的投入、在短时间内执行更严格的上线检测和审批，确保其及时并安全上线，保障租户利益。

8 运维运营安全

在上一章介绍的 DevOps/DevSecOps 云服务流程中，运维运营与研发同等重要，相辅相成，混然一体。华为云对运维运营尤为重视，更聚焦运维运营安全并给与高度优先和重点投入。本章主要介绍华为云在运维安全、漏洞管理、安全事件管理和业务连续与灾难恢复管理等方面的具体实践。

8.1 O&M 账号运营安全

运维工作对华为云至关重要，涉及到安全的方方面面。针对运维安全，华为云有专门的设计、规范和流程。运维安全包括统一帐号、权限和接入管理等。

8.1.1 账号认证

运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证，如 USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。

特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。

8.1.2 权限管理

系统帐号/权限管理分两个维度：帐号生命周期管理和授权管理。

- **帐号的生命周期管理：**包括帐号的开销户管理、帐号责任人/使用人管理、口令管理、开销户监控管理等，帐号一旦建立，立即纳入帐号管理员的日常维护管理工作。所有运维帐号，所有设备及应用的帐号均实现统一管理，并通过统一审计平台集中监

控，并且进行自动审计。以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。

- **帐号授权流程：**如果帐号使用人要使用帐号，帐号管理员可启动授权流程，通过口令或者提升帐号的权限等方式进行授权；帐号的申请人和审批人不能是同一个人。
- **权限管理：**根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。登录权限分为：核心网络、接入网络、安全设备、业务系统、数据库系统、硬件维护、监控维护等。不同岗位不同职责人员限定只能访问本角色所管辖的设备，其他设备无权访问。

华为云运维人员在开展日常工作时，严格遵守下述权限管理相关规定：

- 不得尝试绕开系统的安全审计措施，不得修改、删除、销毁系统日志。
- 不得用个人存储介质连接服务器。
- 未经授权，不得私自使用任何存储介质连接服务器。
- 未经授权，不得改变生产环境中设施、设备、系统的用途，不得在其上从事与其原本功能定义不符的活动和操作。

8.1.3 接入安全

为了保证云服务数据中心的持续稳定运行，华为云建立了一支强大的运维队伍。通过在华为云数据中心部署的 VPN 和堡垒机，实现运维管理平台的统一运维管理和审计。数据中心外网运维人员和内网运维人员对网络、服务器等设备的本地及远程操作，全部集中管理，实现用户对设备资源操作管理的统一接入、统一认证、统一授权、统一审计。

- **外网远程运维接入：**为实现对华为云的远程管理，不论是从互联网还是办公网接入，都要首先访问资源池堡垒机，再从堡垒机访问相关资源。归纳为以下两种远程访问路径：
 - **路径 1：运维人员从互联网访问。**运维人员从互联网执行运维时，需要先通过 SSL VPN 建立从互联网进入云运维网络的连接，限定只可以访问堡垒机，保证从互联网接入访问的权限最小化。
 - **路径 2：运维人员从华为内网访问。**使用华为已有跳转系统从其办公内网接入华为云运维内网（通常用 MPLS VPN 连接两种内网），进入运维内网后限定只能访问堡垒机，实现访问权限最小化。
- 运维接入认证安全：

- 。 改变使用者的认证方式，使用独立的账号体系来对使用者进行授权，使用用户名、密码等信息更统一、简单、安全、有效。
- 。 设备密码的自动更改方式，可以设定每周期（天、周、月）内自动改变设备密码。设备密码更改后，只有超级权限账号才能查看密码，对其余使用者的密码区则为不可见状态。密码策略，类似于 Windows 的密码策略，主要是位数，复杂度的定义。

8.2 漏洞管理

华为产品安全事件响应团队（PSIRT – Product Security Incident Response Team）于 2010 年正式成为国际应急响应论坛 FIRST 成员之一，通过该组织可实现与 471 个成员交流业界最佳实践和安全信息；华为 PSIRT 已经建立成熟的漏洞¹⁷响应机制，针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。

同时，华为 PSIRT 和华为云安全运维团队已经建立了完善的漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。

8.2.1 漏洞感知

华为 PSIRT 已建立完善的漏洞感知与收集渠道。在华为官网 PSIRT 公开了漏洞收集邮箱 psirt@huawei.com 及漏洞奖励计划 <https://bugbounty.huawei.com/hbp>，鼓励全球漏洞协调组织、供应商、安全公司、组织、安全研究者和华为员工等提交华为产品或解决方案的漏洞。同时，华为 PSIRT 会主动监控业界知名漏洞库、安全论坛、邮件列表、安全会议等渠道，以保证第一时间感知到包括云在内的华为相关漏洞信息。通过建立包括云业务在内的所有产品和解决方案的公司级漏洞库，以保证有效记录、追踪和闭环每个漏洞。同时，华为云设立了专有漏洞收集邮箱 hws_security@huawei.com，华为云自己的安全运维团队通过自研及商业在线安全扫描工具，定期执行漏洞扫描任务（扫描不包括租户实例），让华为云环境下的漏洞“无处可躲”，实现漏洞的“可视化”。

¹⁷ “漏洞指系统设计、实施、运营和管理中，可被利用于违反系统安全策略的缺陷或弱点。”（RFC4949）。

8.2.2 漏洞响应和处理

与华为传统 ICT 业务相比，华为云拥有更完整的网络配置信息和设备操作权。再结合华为云采用的 DevOps/DevSecOps 流程，使得华为云在漏洞修复上能做到更快速、更直接的持续集成、持续部署。

华为云基于业界最佳实践 CVSS（Common Vulnerability Scoring System）对漏洞进行严重级别的评估，并结合漏洞在华为云中被利用的风险评估结果决定处理优先等级。同时考虑到华为云直接面向最终用户提供服务，面临着更大的互联网攻击风险，因此在漏洞评估严重级别时增加了服务是否面向互联网（ETI – Exposed to Internet）的判断依据。综合考量，最终制定漏洞修复的 SLA 要求。

华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，此系统会自动接收来自 PSIRT、在线扫描工具等众多漏洞收集渠道提交的漏洞，并自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复 SLA 要求。对于重大安全漏洞，安全运维团队可通过自研工具，对现网进行扫描，实现分钟级的受影响服务和模块的范围界定；同时安全运维团队会根据现网情况，采取必要的漏洞缓解措施，例如限制端口访问、实施 WAF 漏洞规则等方式对受影响的服务进行防护或隔离，以降低漏洞被利用的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对租户业务造成影响。同时，华为云还持续更新操作系统及容器镜像，通过镜像和容器的滚动升级完成系统漏洞修复，不会对租户业务造成影响。

8.2.3 漏洞披露

为保护最终用户和租户，华为云秉承负责任的披露原则，对于涉及云平台、租户服务等漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，向最终用户/租户及时推送漏洞规避和修复方案和建议，与租户共同面对安全漏洞带来的挑战。

8.3 安全日志和事件管理

云安全事件指由可疑网络攻击或者破坏，可能或已经造成云服务系统信息泄露、数据被篡改、系统入侵、服务不可用及其他已经核实即可能影响云服务品牌的安全事件。这些攻击行为主要包括基础设施、平台和应用攻击（如后门攻击、漏洞攻击、网络扫描窃听、钓鱼攻击、DDoS 攻击，OWASP Top 10 等），信息破坏（如信息篡改、假冒、泄漏、窃取、丢失等）。

鉴于安全事件处理的专业性、紧迫性和可回溯性，华为云拥有完善的安全日志管理要求、安全事件定级处置流程和 7*24 小时的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。

8.3.1 日志管理和审计

华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，日志包含资源 ID(如：源 IP、主机 ID、用户 ID 等)、事件类型、日期时间、受影响的数据/组件/资源的 ID(如目的 IP、主机 ID、服务 ID 等)、成功或失败等信息，以确保支撑网络安全事件回溯和合规。该日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间超过 180 天，90 天内可以实时查询。华为云有专门的内审部门，定期对运维流程各项活动进行审计。

华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM – Security Information and Event Management）系统如 ArcSight、Splunk 对接。

8.3.2 快速发现与快速定界

华为云建立了稳固、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；Anti-DDoS 快速发现和防护 DDoS 攻击；WAF 实时检测和防御 Web 攻击；IDS/IPS 实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。

针对公有云攻击的手段多样、流量巨大的特点，华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。

- 区别传统的运维流程（没有自动化工具，安全事件主要靠人工经验分析，效率低），大数据安全分析平台从海量的原始告警日志中，实时检测威胁行为，通过可视化界面展示，极大减少人工分析时间，将攻击的发现和定界缩短至秒级。
- 支持众多威胁分析模型和算法，结合威胁情报和安全咨询，精准识别攻击，包括最常见的云攻击威胁：暴力破解、端口扫描、肉鸡、Web 攻击、Web 未授权访问、APT 攻击等。并且该系统实时评估华为云安全状态，分析潜在风险，并结合威胁情

报进行预警，做好预防工作。

- 针对日常多样化的攻击告警事件，华为云有专业的安全事件管理系统对安全事件进行端到端的跟踪闭环，整个处置过程可回溯。

8.3.3 快速隔离与快速恢复

- 当华为云受到攻击时，边界安全设备成为快速隔离、快速恢复的第一道防线。例如，Anti-DDoS 逐层对攻击流量进行清洗过滤，实时对流量型攻击和应用层攻击进行全面防护；WAF 实时检测 Web 攻击，对高危攻击进行告警并立刻自动阻断；IPS 同时防御对平台和租户的攻击。
- 大数据安全分析平台与各类安全设备联动以及时发现并阻断攻击，是快速隔离、快速恢复的第二道防线。大数据安全分析平台可以快速识别出入侵行为并且精准识别攻击源，智能联动安全设备进行自动阻断，将阻断时间缩短至秒级。
- 华为云与电信运营商联动，自动封堵大流量 DDoS 攻击是快速隔离、快速恢复的第三道防线。当大流量 DDoS 攻击影响到华为云实际吞吐量时，DDoS 自动封堵系统会自动联动运营商封堵系统，在运营商骨干路由器丢弃攻击流量，保证华为云的带宽不受影响，保证租户业务正常运行，整个过程不超过两分钟。
- 基于云面临环境下存在复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，以确保在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。

8.4 业务连续与灾难恢复

华为云基础设施具备高可用性，将系统故障给客户带来的影响降到最低。

8.4.1 基础设施高可用

- 华为云依赖数据中心集群的二地三中心架构实现数据中心本身的容灾和备份，数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。同时，两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一数据中心故障的情况下，也可以将流量负载均衡到其他中心。

- 华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。
- 用户可充分利用这些地域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下（包括自然灾害和系统故障）系统都能连续运行。

8.4.2 可用区之间灾备复制

为了减小由硬件故障、自然灾害或其他灾难带来的服务中断，华为云为所有数据中心提供灾难恢复计划：

- 华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统做到自动检测和自愈。
- 单个区域内不同可用区之间，通过高速光纤实现数据中心互联（DCI – Data Center Interconnect），满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。

8.4.3 业务连续性计划和测试

- 华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划，并定期对其进行测试。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行，保障客户的业务和数据安全。
- 华为云还制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。

9 安全生态

面对网络空间变化多端、发展快速、危害巨大的安全威胁，开放、协同的快速检测、深度防御、及时恢复已经成为业界共识。公有云服务商为海量租户提供服务，面对不同层次的安全需求，很难完全依靠自身的技术和服务能力保护云租户的数据和业务安全。因此，华为云聚集广泛而全面的安全合作伙伴的力量，共同为租户提供安全保障。

华为云致力于构建开放、协作、共赢的安全生态体系，与业界领先的安全产品与服务供应商一起，基于责任共担模式，为云租户提供易部署、易管理、完善的安全解决方案，应对已知、未知的安全威胁，保障租户的数据和业务安全。

- 在安全技术合作方面，华为云致力于与业界优秀的安全产品与服务合作伙伴合作，为用户提供主机安全、网络安全、数据安全、应用安全、安全管理等各领域的产品和服务。华为云已与合作伙伴联合推出了主机入侵检测、Web 应用防火墙、主机漏洞检测、网页防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力。截止目前，华为云已与 50 多家国内外安全伙伴展开深度合作，在华为云上提供 160 多项安全产品及服务。
- 在安全咨询服务方面，华为云寻求与各行业优秀厂商开展深度合作，为金融、政务、交通、制造等行业开发安全解决方案，同时，华为云与全球 400 多家解决方案伙伴合作，帮助用户设计行业安全解决方案及商业模式，加速行业数字化转型。
- 在云安全生态建设方面，华为云除开展安全技术与咨询服务合作外，还在云安全标准、开源社区积极参与、主动贡献，为云计算产业健康发展贡献力量。此外，华为云还开放各种基础能力及安全服务，为软件及应用开发者提供安全服务。
- 在市场机会方面，华为云将为安全生态合作伙伴提供丰富的市场机会和多种方式的技术支持。首先，华为云安全生态合作伙伴可以使用华为云 Marketplace 平台展现

自己的产品、解决方案和服务，与华为云共享云上潜在客户和销售机会。借助于华为云 Marketplace 和华为云的技术能力，还可以提升销售、交付和维护环节的效率，降低业务经营成本；其次，合作伙伴可以借助华为遍布全球的云服务资源网络，将业务部署到全球。特别优秀的合作伙伴，还将有机会获得华为云在全球业务拓展中的市场线索分享和解决方案推荐；再次，华为已经同政府、教育、医疗、交通、制造、能源及大企业等市场建立了广泛、全面的合作关系，华为云将开放这些市场资源给合作伙伴，帮助合作伙伴创建新的安全产品和安全解决方案，在保障行业客户数字化转型的同时，实现客户、合作伙伴和华为的共赢；最后，华为云安全合作伙伴将有机会参加华为公司的各种线上及线下的品牌营销活动，展示产品解决方案、传播成功案例；随着合作的深入，还将有机会与华为云进行联合品牌营销活动、面向客户的联合解决方案发布等。

- 在技术支持方面，首先，华为云将赋能合作伙伴，帮助伙伴实现自己的云化战略转型，实现产品云化和服务上云；其次，华为云将向合作伙伴开放云服务技术接口，支持合作伙伴开发面向各行业客户的安全方案，华为将帮助和支持这些方案走向市场，为客户带来价值，并助力合作伙伴商业成功；再次，华为云也将逐步开放自己的安全技术能力和安全工程能力，输出安全经验，共享安全资源，通过培训、认证、开发接口、技术文档、安全标准、流程规范、安全测试等多种方式赋能给合作伙伴，从而帮助合作伙伴提升自身的安全能力；最后，华为云将在法律法规和客户许可的前提下，促进合作伙伴间的安全情报共享和互通。当然，通过认证的合作伙伴还可获得相应的免费测试资源支持、培训支持、商务优惠政策等。

面对未来智能社会的安全威胁，华为云将积极联合全球安全伙伴打造一个开放、协作、共赢的安全生态圈。在持续提供云安全增值服务，提升用户信任的同时，不遗余力地推动行业和社会进步。



版本历史

日期	版本	描述
2014 年 7 月	2.0	在华为迈入云服务领域一两年之际，为了帮助用户了解华为在云环境中的安全实践，发布了第一版（2.0 版）公开发布的白皮书。注：1.0 版只对华为内部发布。
2017 年 9 月	3.0	随着华为云的安全技术能力迅速成熟，合规遵从日益完备，生态环境不断成长，业务范围日益壮大，2.0 版华为云计算安全技术白皮书已经不能反映当前华为云的安全战略、组织人员结构、合规和生态，也没有提供华为云安全防御体系、租户服务安全、云安全服务以及支撑其良性发展的研发运营管理的内容。因此发布全新白皮书来涵盖上述各方面的内容至关重要，有利于推介华为云的安全可信品牌，提升客户信任，增强华为云在市场和业界的透明度。3.0 版华为云安全白皮书全文结构和范围在主创团队经过大量业界调研后进行了重新策划、组织；素材收集后，主创团队对全部内容进行了重写、编辑。经多层集体评审，合入大量反馈后定稿。
2019 年 6 月	3.1	在 3.0 版本上新增 EVS、CBR、CDN、EPS、TMS、RTS、DEW、DDS、HSS、CGS 等服务内容，同时刷新部分内容原有服务的描述。