云计算基础

HUAWEI

前言

- 随着ICT技术的高速发展，企业架构对计算、存储、网络资源的需求更高，急需一种新的架构来承载业务，以获得持续，高速，高效的发展，云计算应运而生。
- 本章，我们将带领大家揭开云计算的面纱。

目标

- 学完本课程后，您将能够：
  - 对云计算有清晰的认识，包括云上有什么，云能做什么。
  - 了解云计算领域的一些热门前沿技术与发展趋势，以及云计算在各行业领域的应用场景和案例。
  - 了解云计算技术能够给用户带来哪些价值，未来云计算还会在哪些领域有所突破。

目录

信息大爆炸正在加速到来

- 随着移动互联网、全联接时代的到来，越来越多的终端设备被投入使用，每天都会有大量的数据产生，传统的ICT基础设施也在面临着前所未有的挑战。

PC时代
x86架构电脑

Windows/Linux

移动互联网时代
ARM架构手机

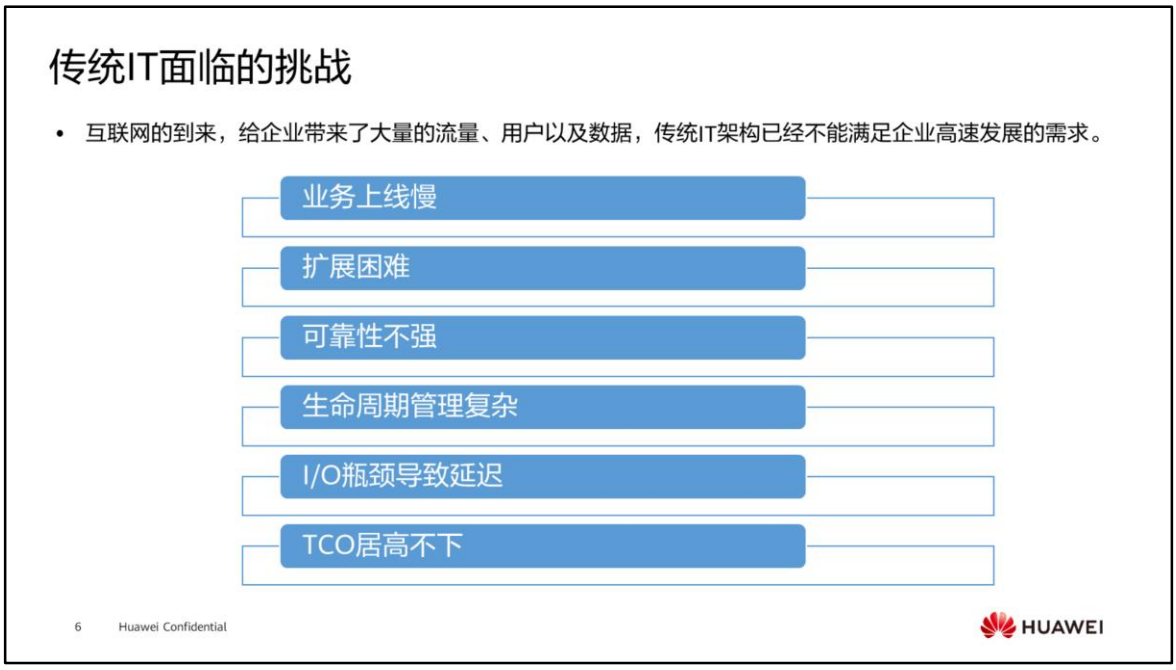
Android/iOS

物联网时代
x86/ARM/DSP/MIPS/FPGA... 各种终端

物联网操作系统

HUAWEI

- PC时代从本质上讲是计算机和计算机的联网，个人的电脑通过服务器彼此相连。现在，我们正处于移动时代，大家通过手机就可以互相联网。随着5G网络将要到来，所有的电脑，手机，智能终端，都能连接到一起，将会进去万物互联的时代。
- 万物互联到来后，整个产业的布局和竞争是生态的竞争。从过去的经验看，PC时代到了移动时代，再到万物互联时代，每个时代形成之后，生态一开始是高速变化的，然后趋于稳态，当稳态的时候很难再改变它。PC时代是Windows、Intel芯片和X86架构，上面有许许多多的应用，互联网来了之后又有了浏览器。到了移动时代，这个时候的ARM上面有IOS、安卓系统，它们上面又有各种各样的应用。
- 互联网经历了两代，现在正在开启第三代，也就是万物互联。每一代互联网相比上一代，从设备的数量和市场的规模，都会有巨大的增长，这是未来的机会所在。 每一代互联网都有掌握产业链的龙头公司，从PC时代的英特尔和微软，到今天的ARM和Google，而未来谁能掌握核心芯片和操作系统，就会成为新的产业链霸主。



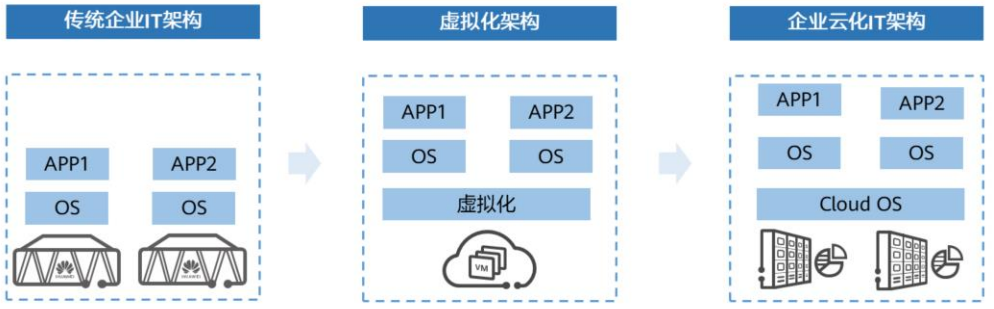
- 互联网的到来，给企业带来了大量的流量，用户以及数据，为了能够匹配企业高速发展的进度，就需要不断地采购传统IT设备，时间一长，传统IT设备的弊端就逐渐显示出来：
  - 采购周期长等原因，导致新业务系统上线慢；
  - 集中式架构扩展性差，纵向扩展只能增加单机处理性能；
  - 传统硬件设备孤立存在，可靠性只能依赖软件侧；
  - 设备种类多，厂商多，导致管理十分复杂；
  - 单个设备性能有限；
  - 设备整体利用率不高，企业总成本支出居高不下。

问题研讨：

- 企业IT架构该如何应对这些挑战？
  - IT基础架构整合
  - 资源整合以及综合利用
  - 业务协同和持续优化

- 研讨环节
  - 这些痛点该如何解决（学员可通过对云计算的熟悉程度来发散，思考云计算哪些优点和现在痛点可一一对应，以便更好理解知识点）。

企业IT基础设施架构开始走向云化



HUAWEI

- 传统IT 基础架构由通常的硬件和软件组件组成：设施、数据中心、服务器、网络硬件台式计算机和企业应用软件解决方案。 与其他基础架构类型相比，这种基础架构设置通常需要更多的电力、物理空间和资金。 传统基础架构往往安装在本地，仅供企业或专有使用。
- 虚拟化是指计算机元件在虚拟的基础上而不是真实的基础上运行。虚拟化技术可以扩大硬件的容量，简化软件的重新配置过程。
- 企业数据中心“云化”转型的要点：1.从资源孤岛到真正资源池化；2.从集中式向分布式架构转型； 3：从专用硬件向开放的软件定义模式转型；4：从人工处理向自助、自动服务转型；5：从分散统计到统一计量转型。

目录

云计算的定义

- Cloud computing is a model for enabling ubiquitous, convenient, **on-demand network access** to a **shared pool** of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be **rapidly provisioned** and released with **minimal management** effort or service provider interaction.

——美国国家技术和标准研究院（NIST）

- 通俗地讲，“云”是网络、互联网的一种比喻说法，即互联网与建立互联网所需要的底层基础设施的抽象体。“计算”指的是一台足够强大的计算机提供的计算服务（包括各种功能、资源、存储）。“云计算”可以理解为：通过互联网可以使用足够强大的计算机为用户提供的服务，这种服务的使用量可以使用统一的单位来描述。

- 中文翻译：云计算是一种模型，它可以实现随时随地、便捷地、随需应变地从可配置计算资源共享池中获取所需的资源（例如，网络、服务器、存储、应用及服务），资源能够快速供应并释放，使管理资源的工作量和与服务提供商的交互减小到最低限度。
- 云计算的特性：
  - 广泛的网络接入
  - 快速弹性伸缩
  - 按需自助服务
  - 资源池化
  - 可计量服务

目录

从身边的云服务、云应用认识云计算（个人用户）

HUAWEI

- 生活中，云计算的数据具体来源有哪些?
  - 云相册：百度云，苹果云相册
  - 云音乐：网易云音乐，酷狗，酷我，虾米
  - 云视频：百度云，腾讯云视频
  - 云文档：有道云笔记，石墨文档
- 通过生活中我们使用的应用就可以发现，云计算让我们的生活更加方便。企业也通过云计算的方式，让自己的产品能够提供更好的体验，从而收获更多的用户。

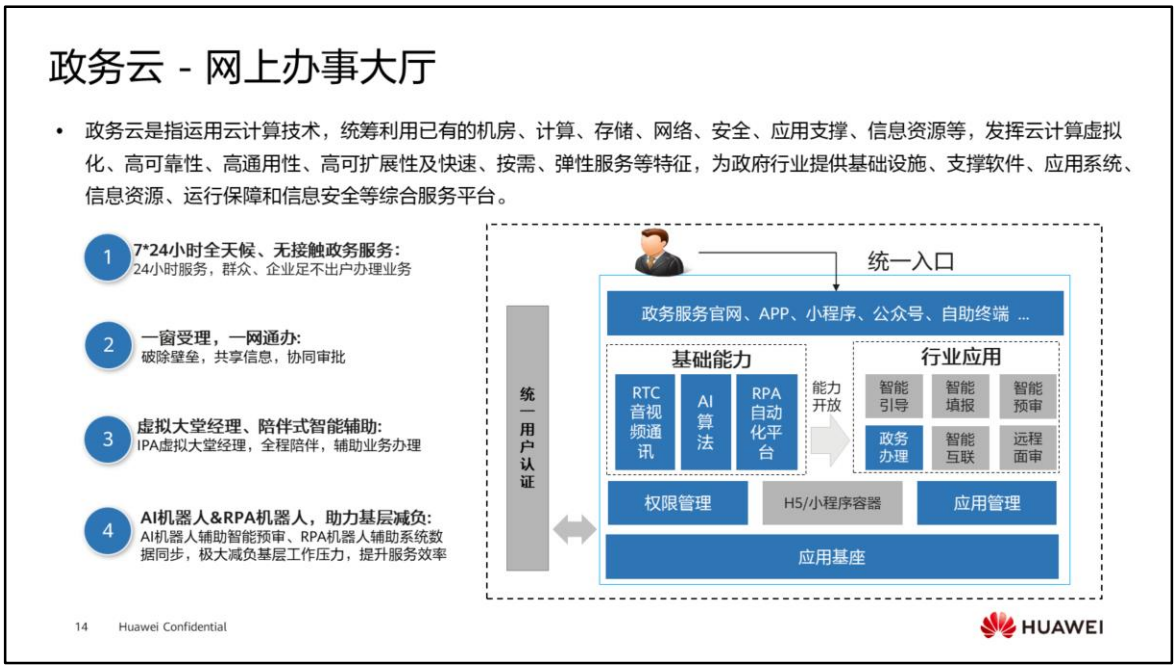
从身边的云服务、云应用认识云计算（企业用户）

- 云会议为用户提供全场景、端云协同的视频会议体验，满足跨地区、跨企业、跨终端的智能沟通协作需求。

视频会议

网络直播

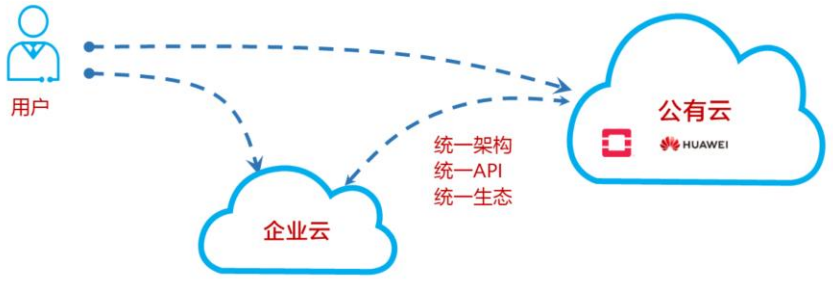
- 在政府、交通、电力、医疗、教育、金融、军队等行业领域及企业需求的共同带动下，我国的视频会议市场呈现稳定的增长趋势，平均年增长在20%以上。考虑到中国现阶段只有仅不到 5% 的企业拥有视频会议室，而且越来越多的企业开始意识到高效协作的重要性，视频会议系统已逐渐成为企业高效办公的“标配”。
- 云会议的应用场景：企业办公、远程医疗、智慧教育、企业组织建设等。



- 网上办事大厅是目前电子政务资源融合中最典型的应用，各地都有建设。通过网上办事大厅，申办人可以在网上填写申报内容、提交相关证明材料，行政审批中心可以通过网络收集申办人的业务申请，并通过拉通跨部门数据，实现并联审批，实现一窗式行政审批。通过上云，政务大大降低了支出，云服务提供商有了新的发展收益，而民众处理事情也越来越方便了，可以说是一举三得。
  - 导：所有政策/公告/办理流程都通过信息指引发布，群众/企业办事流程指引一目了然；依托IPA（Intelligent Process Automation，智能流程自动化）智能机器人为客户提供智能指引
  - 办：依托大数据和人工智能技术，可以实现资料自动完善和智能填报，自动填报
  - 审：依托AI技术实现资料预审，提升资料审查效率和质量，降低工作人员压力；依托RTC（Real-Time Communication）音视频技术，实现无接触线上远程预审
  - 同：依托RPA（Robotic Process Automation，机器人流程自动化）技术，所有工作项都能够通过工作台由RPA辅助处理，高效协同各个职能部门工作。所有应用/服务的入口都能够通过网上政务大厅进行统一管理

公有云

- 简单来讲，就是要由云服务提供商自行建设，然后将云资源面向所有用户销售，用户可以通过互联网像使用水电一样租用IT服务，如：华为云等。



HUAWEI

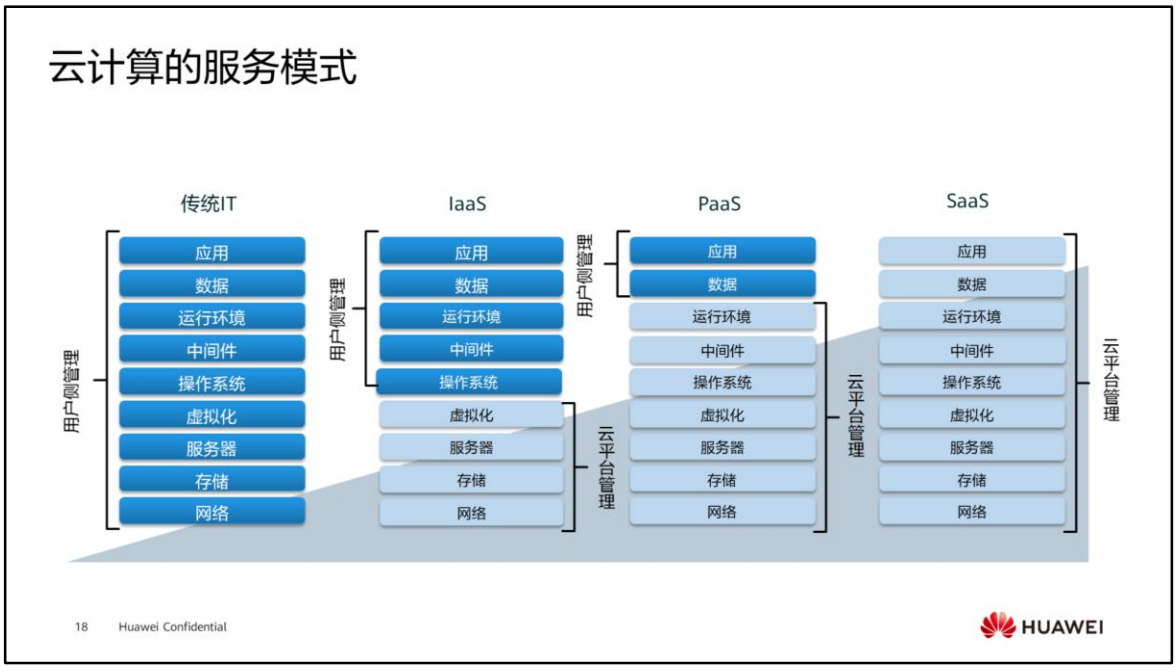
- 公有云被认为是云计算的主要形态。在国内发展如火如荼，根据市场参与者类型分类，可以分为五类：
  - 传统电信基础设施运营商，包括中国移动、中国联通和中国电信；
  - 政府主导下的地方云计算平台，如各地如火如荼的各种“XX云”项目；
  - 互联网巨头打造的公有云平台，如阿里云、腾讯云；
  - 部分原IDC运营商，如世纪互联；
  - 具有国外技术背景或引进国外云计算技术的国内企业，如风起亚洲云。

目录

云计算的部署模式

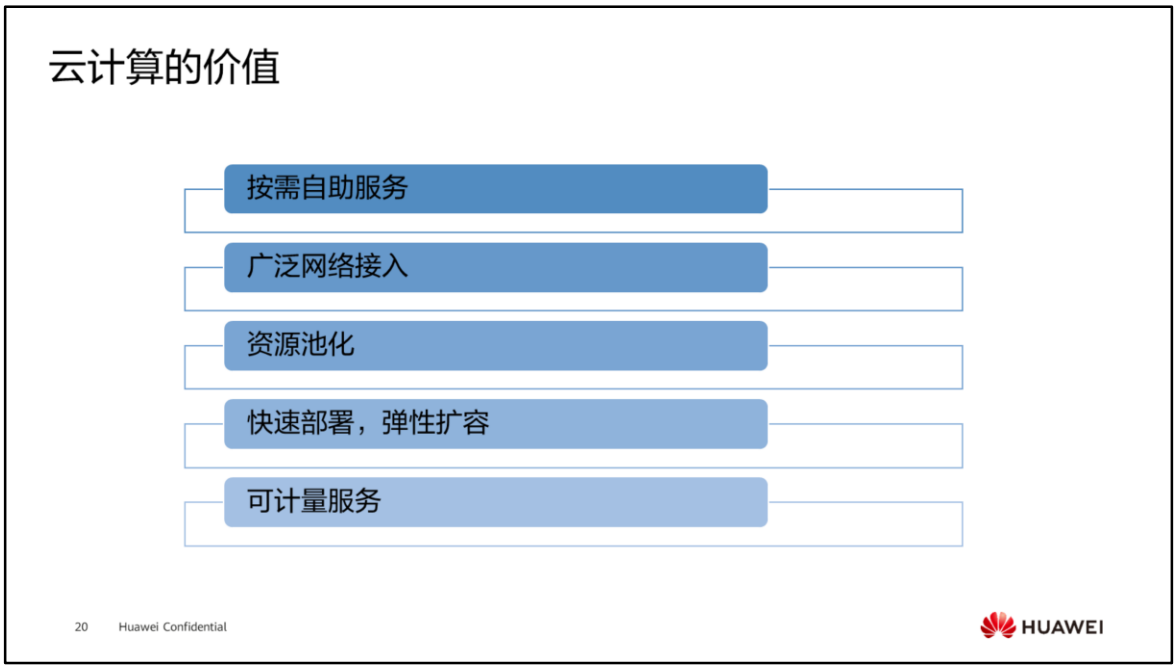
私有云（Private cloud）：云计算的基础设施由单一的组织拥有，并且仅仅为该组织运营。
公有云（Public cloud）：云服务运营商拥有云基础设施，并且为公众或者企业用户提供云服务。云计算基础设施由一个组织拥有并且向公众或者大型的工业团体销售云计算服务。
混合云（Hybrid cloud）：云计算基础设施由两种或者多种云组成，对外仍然表现为一个整体。

- 私有云：私有云通常部署在企业或单位内部，运行在私有云上的数据全部保存在企业自有的数据中心内，如果需要访问这些数据，就需要经过部署在数据中心入口的防火墙，这样可以在最大程度上保护数据。
- 公有云：云服务运营商拥有云基础设施，并且为公众或者企业用户提供云服务。云计算基础设施由一个组织拥有并且向公众或者大型的工业团体销售云计算服务，用户可以通过互联网像使用水电一样使用IT服务。
- 混合云：混合云是一种比较灵活的云计算模式，它可能包含了公有云、私有云或者后面要讲的行业云中的两种或两种以上的云，用户的业务可以根据需求在这几种云上切换。



- IaaS：Infrastructure as a Service（基础设施即服务），就是由云平台提供基础设施（如：服务器、存储、网络、虚拟化资源）以及负责相关资源的维护，用户只需要关注系统和应用层面的部分即可。
- PaaS：Platform as a Service（平台即服务），就是由云平台提供基础设施（如：服务器、存储、网络、虚拟化资源）+应用部署环境（如：操作系统、中间件、软件运行环境）以及负责相关资源的维护，用户只需要关注应用和数据本身即可。
- SaaS：Software as a Service（软件即服务），就是由云平台提供全部资源服务以及维护，用户只管使用应用即可。
- 相比于传统IT全流程全设备采购的方式，云服务模式将IT设备服务化地销售，让客户按需选择，在使用灵活性和成本上比传统IT更有优势。

目录



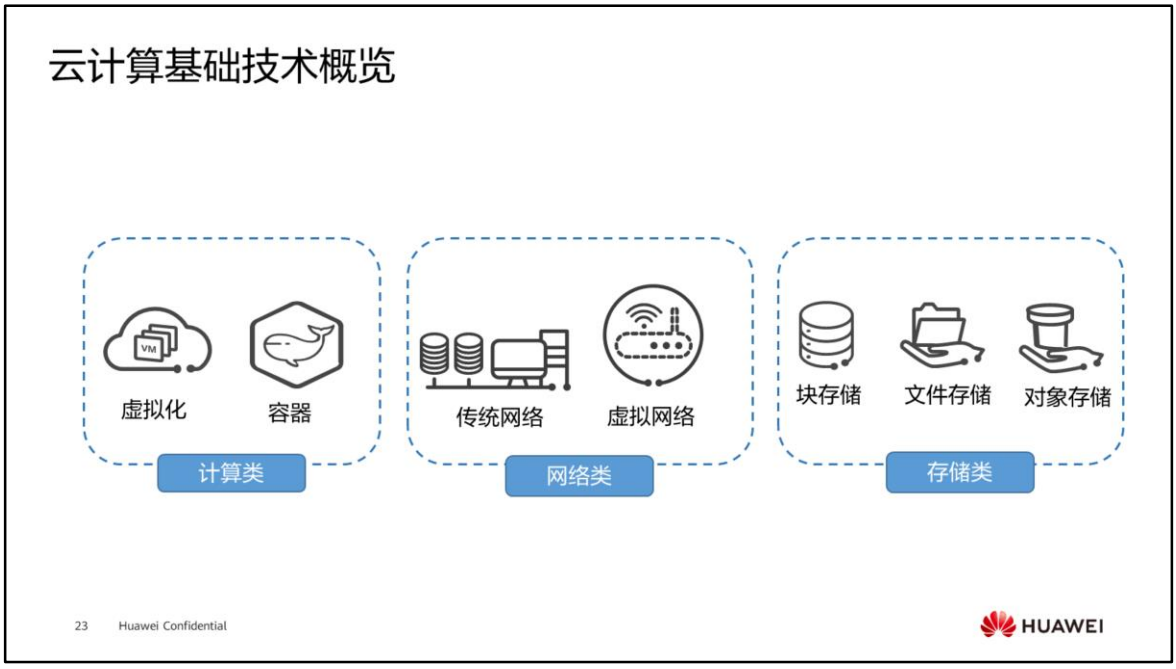
- 云计算通过将硬件资源以软件的方式整合为一个整体，然后再以软件的方式动态分配给应用，大大地提高了资源的使用率，并且还能够弹性扩容，极大地优化了工作效率。通过建设高规格的云数据中心，引入自动化调度技术，让数据存储更加集中，数据资产也就能够更加有效利用，也更加节能减排和易于维护。从各个维度都起到了降本增效的作用。
- 五个主要价值点：
  - 按需自助服务：消费者可以按需部署处理能力，如服务器时间和网络存储，而不需要与每个服务供应商进行人工交互
  - 广泛网络接入：可以通过互联网获取各种能力, 并可以通过标准方式访问，通过各种客户端接入使用。例如移动电话，笔记本电脑，PAD等
  - 资源池化：供应商的计算资源被集中起来，以便以多用户租用模式服务所有客户，同时不同的物理和虚拟资源可根据客户需求动态分配和重新分配。客户一般无法控制或知道资源的确切位置。这些资源包括存储、处理器、内存、网络带宽和虚拟机等
  - 快速部署，弹性扩容：云计算可以迅速、弹性地提供能力，能快速扩展，也可以快速释放实现快速缩小。对客户来说，可以租用的资源看起来似乎是无限的，并且可在任何时间购买任何数量的资源
  - 可计量服务：云服务的收费是基于用户实际使用的资源进行计量，比如云主机的CPU、内存、存储容量，网络带宽的消耗，按小时计费或者包年包月

云计算的8个通用点

- 大规模（Massive Scale）
- 同质化（Homogeneity）
- 虚拟化（Virtualization）
- 弹性计算（Resilient Computing）
- 低成本软件（Low Cost Software）
- 先进安全技术（Advanced Security Technologies）
- 地理分布（Geographic Distribution）
- 面向服务（Service Orientation）

- 大规模，因为云计算服务把IT的资源供应集中化了，自然规模很大。也正因为如此，量变导致质变，使得云计算与传统IT有了众多的区别。
- 同质化，也可以理解成标准化，这点倒是和用电很类似，大家要保持相同电压、插座接口，这样人们的电器和各种设备才能被广泛使用。
- 虚拟化，有两层含义，一个是计算单元的精细化，一块蛋糕太大，一个人吃不了，那最好切成小块，大家分着吃，也就是让每个计算单元更小，这样可以充分利用IT资源；另外一层含义是软硬件的分离，虚拟化之前软件和指定硬件是绑在一起的，虚拟化之后软件在所有硬件上可以自由的迁移，这跟人们由买房变成租房是一样的，既然北上广深的房价太高，很多人便租房住了，拎个箱子想住哪就住哪。
- 弹性计算，指的是IT资源供给可弹性伸缩。
- 低成本软件，是从竞争与市场需求发展的角度说的。云计算降低了人们使用IT的门槛，不仅仅在个人技术能力上，而且在资金能力上，很多小微的初创企业，希望能够用最少的钱使用最多的IT服务，要想打开这部分市场，自然需要低成本的软件，通过薄利多销的形式赚到更多的钱。
- 地理分布，前文提到的泛在接入，也就是能够在任意时间任意地点提供IT服务。从使用者的角度看，就是地理分散的，由于各地网络带宽的优劣差异，那么IT提供者，也就是云计算数据中心的部署，自然也是呈现出地理分布式特征的。大的公有云厂商都有几十个甚至数百个数据中心或服务节点，面向全球提供云计算服务。
- 面向服务，因为云计算是一种服务模式，整体的设计也就是面向服务的。
- 先进安全技术，林子大了，什么鸟都有，公有云大了，什么用户也都有，包括好的坏的，自然先进的安全技术保障是一个云计算必须的条件了。

目录



- 计算类产品主要提供算力，支持业务运行，例如网站、办公软件、数据分析等计算能力，目前典型的产品主要是虚拟化和容器，在公有云上的云主机本质也是虚拟机。
- 网络类产品主要满足资源的网络连通性和隔离，传统数据中心的网络，园区网络等场景，在云上的虚拟机也同样需要虚拟网络，例如虚拟私有云VPC，该逻辑拓扑与传统网络类似。
- 存储类产品一般分为三大类：
  - 块存储：具备高性能和低时延的特点，用各种高IO需求的场景
  - 文件存储 ： 能满足多服务器间的文件共享，或者企业团队部门的文件共享
  - 对象存储：扁平化架构，横向扩展方便，适合做云存储池，用于海量数据存储、冷数据备份、软件仓库等场景

什么是虚拟化

- 虚拟化技术可将单台物理服务器虚拟为多台虚拟机使用，多台虚拟机共享该物理服务器的硬件资源。
  - 虚拟机本质上是由磁盘文件和描述文件组成，封装在同一个文件夹中。
  - 服务器上运行多个虚拟机，各自封装，互相隔离，即存在多个文件夹。
    - 这些文件夹又可以存放在底层存储提供的文件系统上，因此实现同一介质可以存放或运行多个虚拟机。

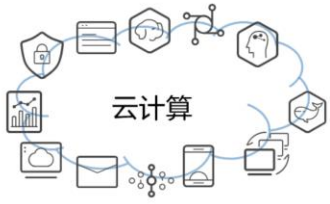
- 虚拟化的本质就是将原先的物理设备进行逻辑化，转化成一个文件夹或文件，实现软硬件的解耦。

HUAWEI

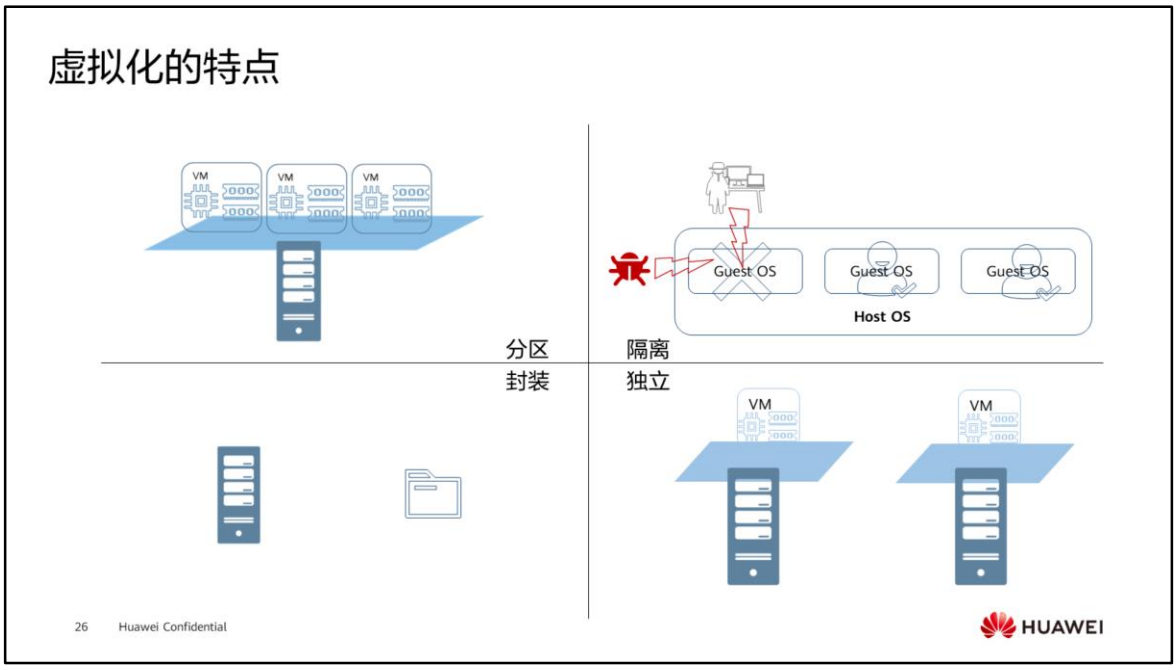
- 在计算机技术中，虚拟化（技术）一种资源管理技术，是将计算机的各种实体资源（CPU、内存、磁盘空间、网络适配器等），予以抽象、转换后呈现出来并可供分割、组合为一个或多个电脑配置环境。由此，打破实体结构间的不可切割的障碍，使用户可以比原本的配置更好的方式来应用这些电脑硬件资源。
- 从图中我们可以了解到，通过虚拟化，原本的硬件服务器被分割成一个个文件，而这一个个文件也代表着一个个虚拟机。

虚拟化与云计算

- 虚拟化是实现云计算的核心技术，但不等同于云计算。云计算的内容维度要比虚拟化大得多。

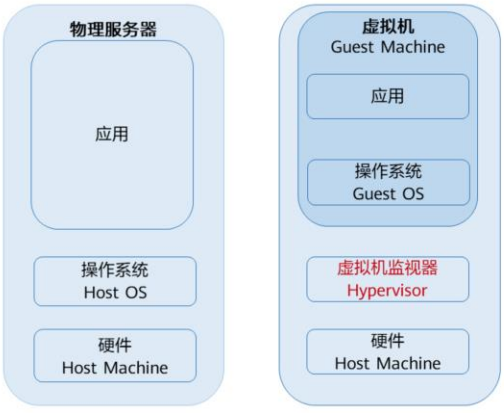


- 虚拟化是云计算的关键技术，旨在将物理资源抽象为逻辑资源，进而能够二次分配，特点是支撑资源池的弹性敏捷，灵活调度，同时也具备分布式调度、资源高可用的能力。
- 云计算是一种服务，突出其按需的商业模式，使得用户能像用水用电一样地使用云资源。其敏捷的特点又依赖虚拟化技术实现。



- 虚拟机的特点：
  - 分区：同一台物理服务器上可以同时运行多台虚拟机，也意味着虚拟化层拥有为虚拟机划分底层服务器资源的能力。我们把这个能力叫做分区。
  - 隔离：同一服务器上的虚拟机若有一台故障或者中病毒，不会影响到其他虚拟机的使用。这就要求虚拟机具备最基本的隔离能力。
  - 封装：虚拟机的本质是以文件的形式存在于虚拟化系统中，可以通过移动文件或者复制粘贴的形式对虚拟机进行迁移。
  - 独立：在迁移虚拟机后无需对服务器做任何修改即可运行虚拟机（相当于上层操作系统与硬件解耦合），所以这里的独立主要指的是独立于硬件。

计算虚拟化中的重要概念



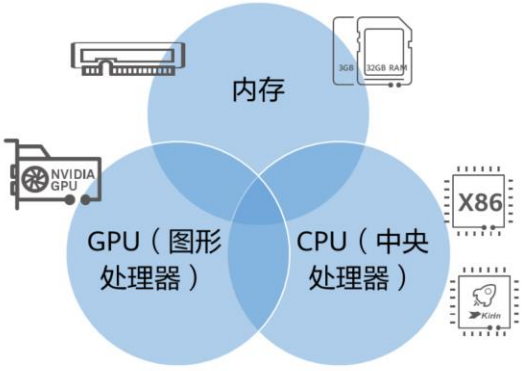
- **Guest OS**：虚拟机操作系统
- **Guest Machine**：虚拟出来的虚拟机
- **Hypervisor**：虚拟化软件层/虚拟机监视器（Virtual Machine Monitor，VMM）
- **Host OS**：运行在物理机之上的OS
- **Host Machine**：物理机

HUAWEI

- Hypervisor：我们经常把它称之为虚拟化软件层或者虚拟机监视器；通过Hypervisor，我们可以实现按需使用物理机硬件资源的目的。目前主流的几个开源的虚拟化技术有：Xen、KVM等。

计算资源就在我们身边

- 计算的本质是获得信息的一种过程。在ICT行业中，我们需要借助很多计算资源，来将数据做运算处理，从而得到对应的信息。



HUAWEI

- 计算机程序运行时所需的CPU资源、内存资源、硬盘资源和网络资源， 指计算中所需的各种资源。一般地，计算资源包括CPU，GPU，内存。
- CPU（Central Processing Unit，中央处理器）作为计算机系统的运算和控制核心，是信息处理、程序运行的最终执行单元。
- 内存（Memory）是计算机的重要部件之一，也称内存储器和主存储器，它用于暂时存放CPU中的运算数据，与硬盘等外部存储器交换的数据。
- GPU（Graphics Processing Unit，图形处理器），又称显示核心、视觉处理器、显示芯片，是一种专门在个人电脑、工作站、游戏机和一些移动设备（如平板电脑、智能手机等）上做图像和图形相关运算工作的微处理器。

计算在云计算中的服务形态

HUAWEI

- 弹性云服务器（Elastic Cloud Server，ECS）是由CPU、内存、操作系统、云硬盘组成的基础的计算组件。弹性云服务器创建成功后，用户就可以像使用自己的本地PC或物理服务器一样，在云上使用弹性云服务器。
- 弹性伸缩（Auto Scaling）可根据用户的业务需求和预设策略，自动调整计算资源，使云服务器数量自动随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行。
- 镜像（Image Service）是用于创建服务器或磁盘的模板。镜像服务提供镜像生命周期管理能力。可以通过服务器或外部文件创建系统盘镜像或数据盘镜像，也可以使用弹性云服务器或云服务器备份创建带数据盘的整机镜像。

什么是容器

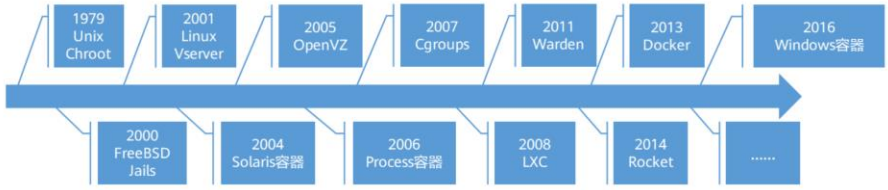
- 容器是一个标准化的单元，是一个轻量级、可移植的软件打包技术。它将软件代码及其相关依赖打包，使应用程序可以在任何计算介质中运行。简单来讲，容器就像一个标准化的盒子，能够装很多不同类型的东西，并且装完后能够塞进很多不同类型的柜子里。

HUAWEI

- 容器的特性：
  - 打包：将软件打包成标准化单元以进行开发、迁移和部署
  - 隔离性：计算、存储、网络等资源彼此隔离
  - 高效性：轻量、快速启停、快速部署与迁移
  - 职责分工明确：开发专心写代码，运维专注基础环境配置

容器技术发展历史

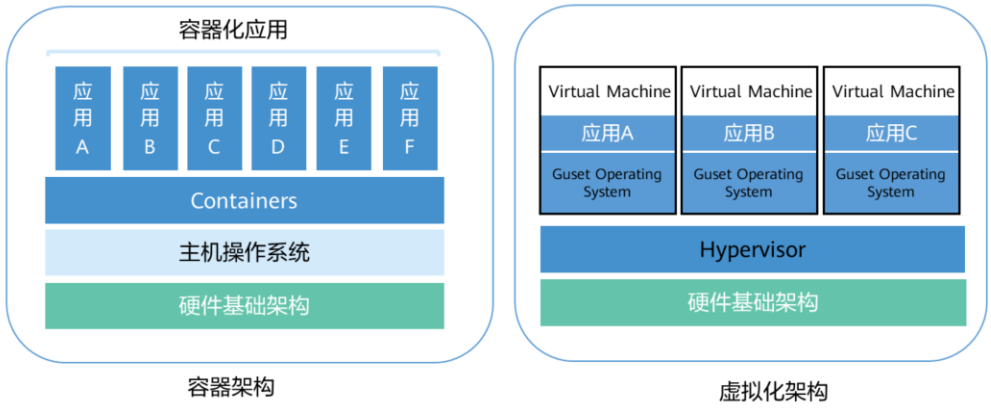
- 容器发展全景图，容器虚拟化在推广应用中面临的两大难题逐渐被攻破：
  - 统一平台
  - 易用性



HUAWEI

- 容器技术最早可以追溯到1979年UNIX系统中的chroot，最初是为了方便切换root目录，为每个进程提供了文件系统资源的隔离，这也是OS虚拟化思想的起源。
- 2000年，BSD吸收并改进了chroot技术，发布了FreeBSD Jails。FreeBSD Jails除文件系统隔离外，还添加了用户和网络资源等的隔离，每个Jail还能分配一个独立IP，进行一些相对独立的软件安装和配置。
- 2005年SWsoft公司发布了OpenVZ，OpenVZ和Solaris Containers非常类似，通过打了补丁的Linux内核来提供虚拟化、隔离、资源管理和检查点。OpenVZ 标志着内核级别的虚拟化真正成为主流，之后不断有相关的技术被加入。
- 2006年Google发布了Process Containers，Process Containers记录和隔离每个进程的资源使用（包括CPU、内存、硬盘I/O、网络等），后改名为Cgroups（Control Groups），并在2007年被加入Linux内核2.6.24版本中。
- 2008年出现了第一个比较完善的LXC容器技术，基于已经被加入内核的Cgroups和Linux namespaces实现。不需要打补丁，LXC就能运行在任意vanila内核的Linux上。
- 2013年Docker诞生，Docker最早是dotCloud（Docker公司的前身，是一家PaaS公司）内部的项目，和Warden类似，Docker最初也用了LXC，后来才自己写了libcontainer替换了LXC。和其它容器技术不同的是，Docker围绕容器构建了一套完整的生态，包括容器镜像标准、容器Registry、REST API、CLI、容器集群管理工具Docker Swarm等。
- 2014年CoreOS创建了rkt，为了改进Docker在安全方面的缺陷，重写的一个容器引擎，相关容器工具产品包括：服务发现工具etcd和网络工具flannel等。
- 2016年微软公司发布基于Windows的容器技术Hyper-V Container，Hyper-V Container原理和Linux下的容器技术类似，可以保证在某个容器里运行的进程与外界是隔离的，兼顾虚拟机的安全性和容器的轻量级。

容器和虚拟化的架构对比



HUAWEI

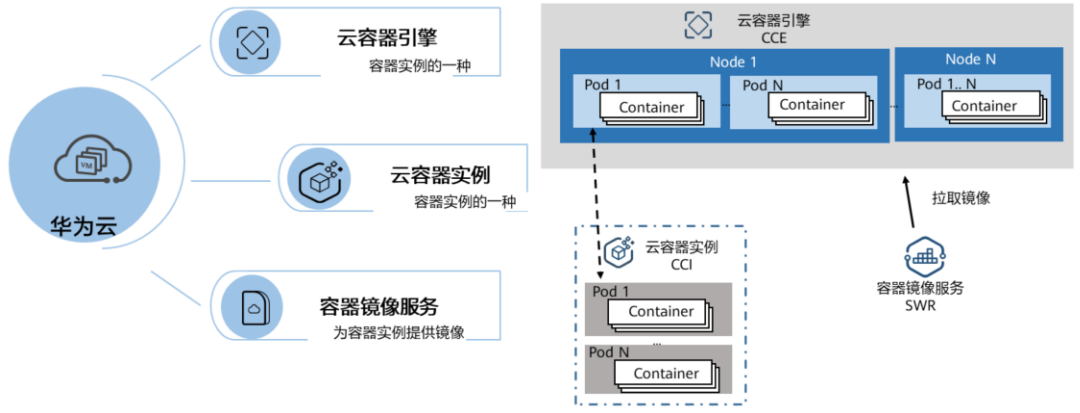
- 容器和虚拟机具有相似的资源隔离和分配优势，但功能不同，因为容器虚拟的是操作系统而不是硬件，容器更便携，更高效。
- 从容器和虚拟化的架构图可以看出，容器是没有虚拟化层的，这也是为什么我们通常把容器称为轻量级虚拟化技术的原因。也正因为没有虚拟化层，使得运行在容器中的应用比运行在虚拟机中的应用性能更强。
- 容器因具有许多优势而变得流行起来。下面列出的是容器的一些好处：
  - 敏捷应用程序的创建和部署：与使用 VM 镜像相比，提高了容器镜像创建的简便性和效率
  - 持续开发、集成和部署：通过快速简单的回滚（由于镜像不可变性），支持可靠且频繁的容器镜像构建和部署
  - 跨云和操作系统发行版本的可移植性：可在 Ubuntu、RHEL、CoreOS、本地、Google Kubernetes Engine和其他任何地方运行
  - 以应用程序为中心的管理：提高抽象级别，从在虚拟硬件上运行 OS 到使用逻辑资源在 OS 上运行应用程序
  - 松散耦合、分布式、弹性、解放的微服务：应用程序被分解成较小的独立部分，并且可以动态部署和管理，而不是在一台大型单机上整体运行
  - 资源隔离：可预测的应用程序性能
  - 资源利用：高效率和高密度

容器和虚拟机的区别

特性	容器	虚拟机
启动时间	秒级	分钟级
虚拟化类型	操作系统虚拟化	硬件级虚拟化
操作系统依赖	所有容器共享主机操作系统	每个VM都在自己的OS中运行
安全性	进程级隔离，可能不太安全	完全隔离，因此更安全
隔离策略	Namespace、CGroups	Hypervisor
镜像大小	KB - MB	GB - TB
性能优势	本机性能	性能有限
系统支持量	单机（物理机）可支持上千个容器	一般几十个

- 容器是应用层的抽象，将代码和依赖项打包在一起。多个容器可以在同一台机器上运行，并与其他容器共享操作系统内核，每个容器作为用户空间中的独立进程运行。容器占用的空间比虚拟机少，可以处理更多应用程序，并且需要更少的CPU和内存资源。
- 虚拟机（VM）是将一台服务器变成多台服务器的物理硬件的抽象。管理程序允许多个VM在一台机器上运行。每个VM都包含操作系统、应用程序、必要的二进制文件和库的完整副本，占用几十GB。VM的启动速度也可能很慢。
- 容器镜像：专用于运行特定服务，通常只包含运行该服务所需的上下文内容，许多广泛使用的镜像都只有几十MB，甚至几MB大小。虚拟机镜像：需要提供包括内核在内的通用进程运行环境，它的镜像偏向于大而完整的全功能集合，即使一个最小的精简镜像的体积也有几百MB。

容器在云计算中的服务形态

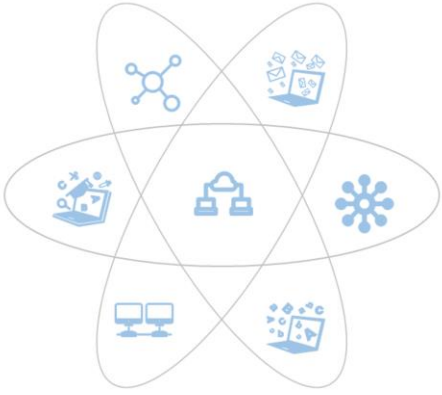


HUAWEI

- 云容器引擎（Cloud Container Engine）提供高可靠高性能的企业级容器应用管理服务，支持Kubernetes社区原生应用和工具，简化云上自动化容器运行环境搭建，面向云原生2.0打造CCE Turbo容器集群，计算、网络、调度全面加速。
- 云容器实例（Cloud Container Instance，CCI）服务提供 Serverless Container（无服务器容器）引擎，让用户无需创建和管理服务器集群即可直接运行容器。
- 容器镜像服务（Software Repository for Container，简称SWR）是一种支持镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，帮助用户快速部署容器化服务。用户可以通过界面、社区CLI和原生API上传、下载和管理容器镜像。
- 容器镜像服务可配合云容器引擎CCE、云容器实例CCI使用，也可单独作为容器镜像仓库使用。

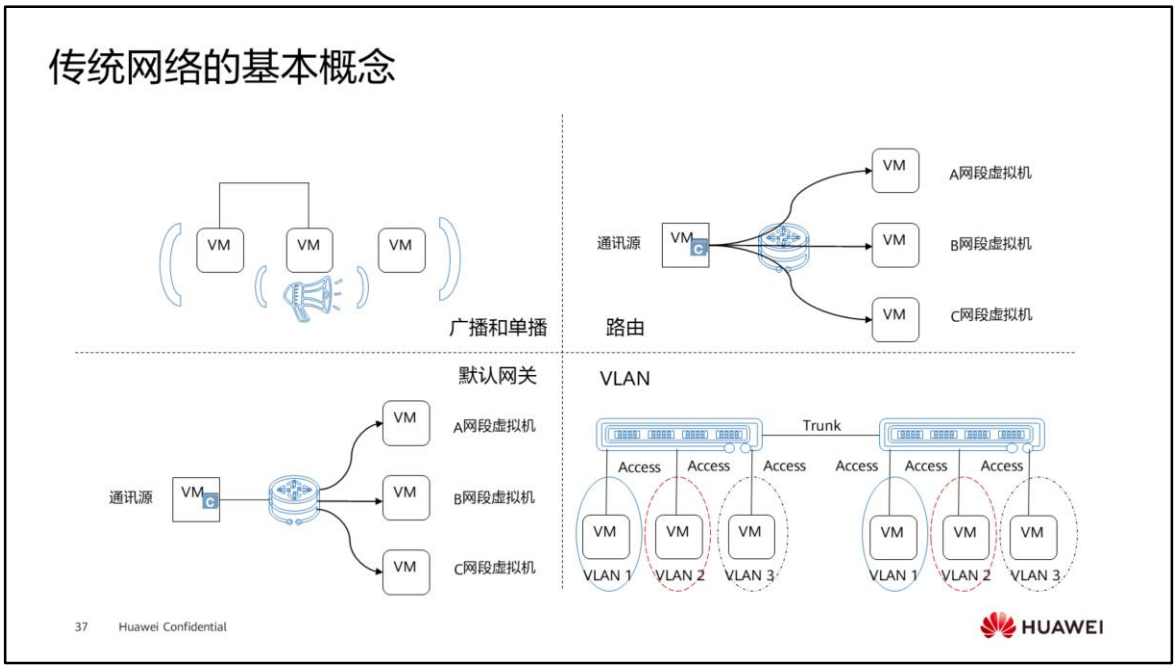
目录

网络的作用



HUAWEI

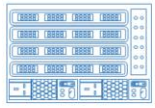
- 网络是设备间、虚拟机之间通信的桥梁。因此，在ICT基础设施中，网络是必不可少的。



- 广播和单播：两个设备通信就好像是人们之间的对话一样。如果一个人对另外一个人说话，那么用网络技术的术语来描述就是单播，此时信息的接收和传递只在两个节点之间进行。广播可以理解为一个人通过广播喇叭对在场的全体说话，这样做的好处是通话效率高，信息一下子就可以传递到全体。
- 路由：路由，即路由器，是连接两个或多个网络的硬件设备，在网络间起网关的作用，是读取每一个数据包中的地址然后决定如何传送的专用智能性的网络设备。
- 默认网关：要了解默认网关，首先要了解网关。网关是子网与外网连接的设备，当一台设备发送信息时，根据发送信息的目标地址，通过子网掩码来判定目标主机是否在本地子网中，如果目标主机在本地子网中，则直接发送即可。如果目标不在本地子网中则将该信息送到默认网关/路由器，由路由器将其转发到其他网络中，进一步寻找目标主机。
- VLAN：即虚拟局域网，是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样。通过VLAN，我们可以将不同的业务进行分隔。

传统网络包含的设备

路由器



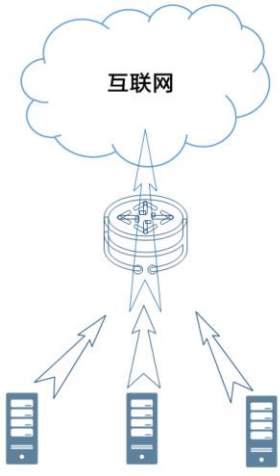
三层交换机

二层交换机

服务器网卡

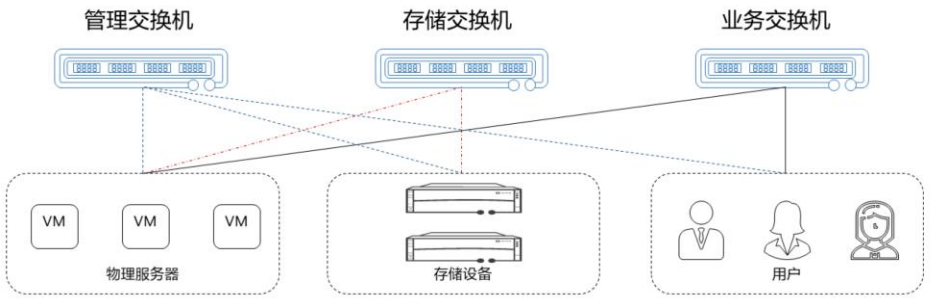
HUAWEI

路由器的作用



- 例如我们家庭电脑通过路由器出外网一样，服务器也可以借助路由器实现访问互联网的功能。
- 路由器又被称为网关设备。路由器就是在OSI参考模型中完成的网络层中继以及第三层中继任务，对不同网络之间的数据包进行存储、分组转发处理。数据在一个子网中传输到另一个子网中，可以通过路由器的路由功能进行处理。在网络通信中，路由器具有判断网络地址以及选择IP路径的作用，可以在多个网络环境中，构建灵活的链接系统，通过不同的数据分组以及介质访问方式对各个子网进行链接。路由器在操作中仅接受源站或者其他相关路由器传递的信息，是一种基于网络层的互联设备。

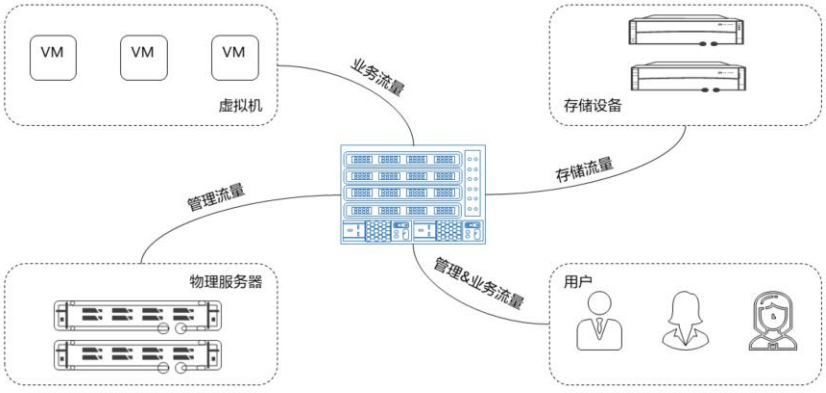
二层交换机的作用



HUAWEI

- 交换机是一种用于电信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。交换是按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术的统称。交换机有多个端口，每个端口都具有桥接功能，可以连接一个局域网或一台高性能服务器或工作站。
- 在传统网络中，二层交换机主要通过VLAN来做网络平面的隔离。

三层交换机的作用

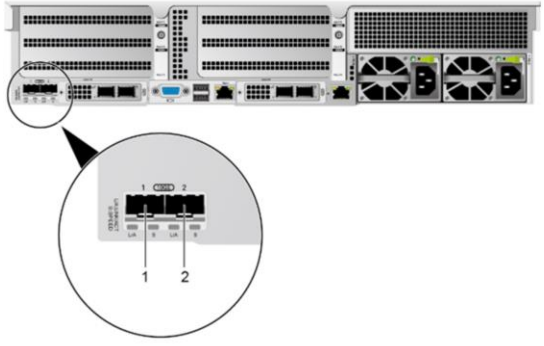


HUAWEI

- 出于安全和管理方便的考虑，主要是为了减小广播风暴的危害，必须把大型局域网按功能或地域等因素划成一个个小的局域网，这就使VLAN技术在网络中得以大量应用，而各个不同VLAN间的通信都要经过路由器来完成转发。随着网间互访的不断增加，单纯使用路由器来实现网间访问，由于端口数量有限且路由速度较慢，限制了网络的规模和访问速度。基于这种情况三层交换机便应运而生，三层交换机是为IP设计的，接口类型简单，拥有很强二层包处理能力，非常适用于大型局域网内的数据路由与交换，它既可以工作在协议第三层替代或部分完成传统路由器的功能，同时又具有几乎第二层交换的速度，且价格相对便宜些。

网卡的作用

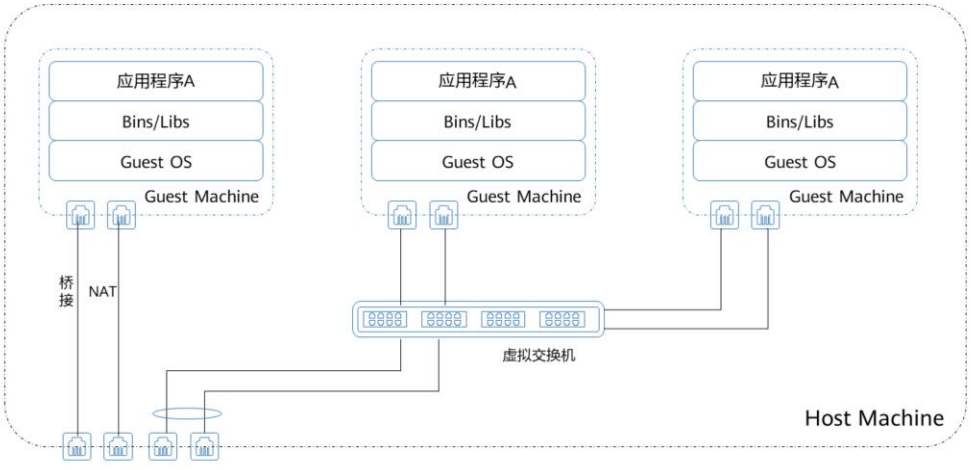
- 网卡的主要作用就是用来连接不同设备的介质。因为有了网卡，设备之间才有了通信的可能，就如同电话卡一般。除此之外，还可以通过绑定网卡，来提高网卡的可靠性、网络的性能等。



HUAWEI

- 板载网卡提供网络扩展能力。能让服务器的数据通过网卡传输到其他设备，是对外提供应用服务的通道。
- 常见网卡支持的速率：100 M/1 G/10 G。

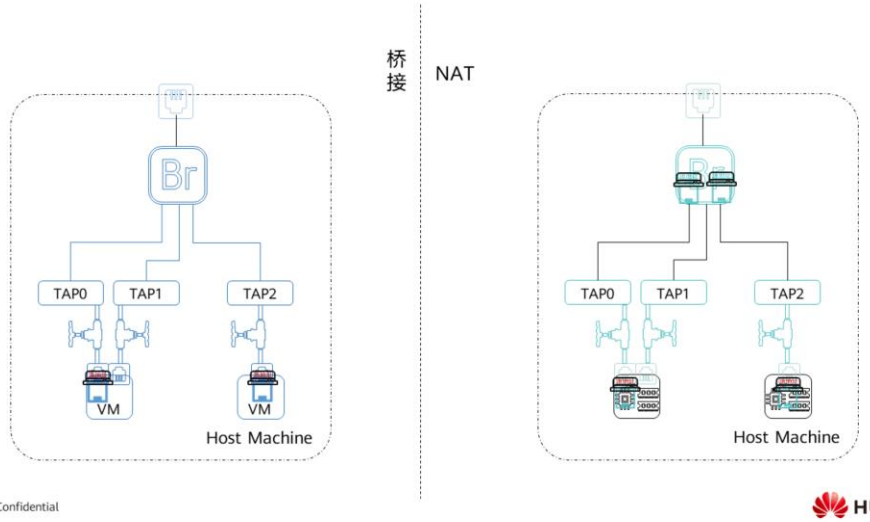
虚拟网络的基本概念



HUAWEI

- 为什么需要虚拟网络?
  - 由于在服务器中需要允许多台虚拟机，并且这些虚拟机的网段可能不同，因此在服务器内部需要有隔离机制，使得虚拟机像传统服务器一样有二层VLAN隔离技术，并且这些虚拟网卡需要共用服务器的物理网卡通向外部网络。因此在服务器内部引入了虚拟交换机，构建虚拟网络。
- 在网络虚拟化中，首先要解决的问题就是虚拟机的虚拟网卡如何能够映射到所在物理服务器的物理网卡上。如图所示，我们可以通过桥接、NAT或者虚拟交换机来实现。

桥接和NAT的作用

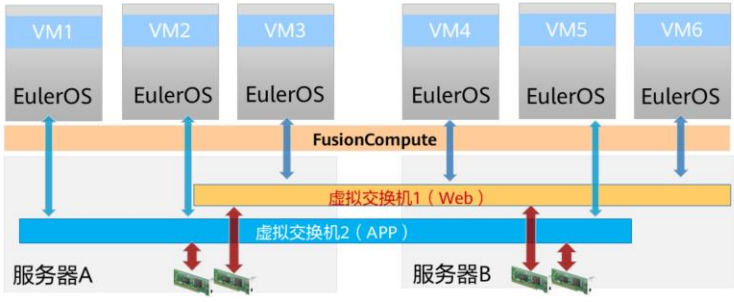


HUAWEI

- 桥接和NAT都可以将不同虚拟机的流量转发到物理网卡上，使得数据报文从服务器通往物理交换机，实现不同虚拟机之间和虚拟机与外部的通信。
- 虚拟交换机就有桥接作用，就交换机来说，本身有一个端口与mac的映射表，用于隔离冲突域。 简单来说就是通过网桥可以把两个不同的物理局域网连接起来，是一种在链路层实现局域网互连的设备。
- NAT是通过网络地址转换来完成流量通往外部的。NAT不仅能解决IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

虚拟交换机的作用

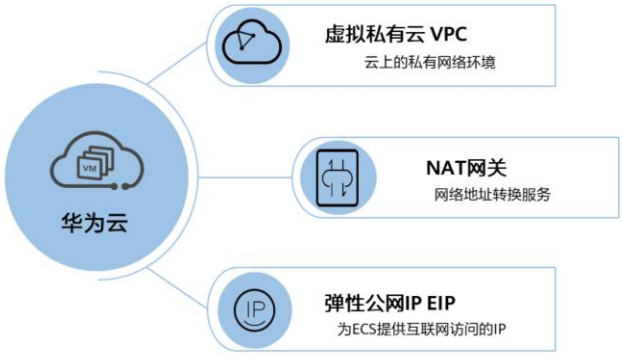
- 同桥接和NAT不同，前者是Linux操作系统自身的功能，而虚拟交换机是经过虚拟化技术处理之后产生的网络模型。但同桥接和NAT一样，虚拟交换机也是为了解决虚拟机内部流量如何从所在物理服务器的物理网口出去的问题。常见的虚拟交换机模型有OVS、EVS等。



HUAWEI

- OVS：Open vSwitch，一款基于软件实现的开源虚拟交换机。能够支持多种标准的管理接口和协议，提供了对OpenFlow协议的支持，并且能够与众多开源的虚拟化平台相整合。主要有两个作用：传递虚拟机VM之间的流量，以及实现VM和外界网络的通信。
- EVS：Enhance vSwitch，增强型虚拟交换机，基于OVS转发技术，提升了其IO性能的一种弹性化虚拟交换，仍然符合OpenFlow协议标准。其中IO性能提升使用了Intel DPDK技术，通过用户态进程接管网卡数据收发，因而IO性能方面有显著提升。
- OVS和EVS的主要区别在于对流量处理的流程差异，OVS对于流量的接收和发送在内核态完成，而EVS则在用户态完成。
- DVS（Distributed Virtual Switch）是分布式虚拟交换机，与物理交换机一样，构建起虚拟机之间的网络，并提供与外部网络互通的能力。
- 虚拟机的虚拟网卡连接到DVS，再经过DVS的上行链路连接到其所在主机的物理网卡，从而实现与外部网络环境的通信。
- 与传统交换机相比，虚拟交换机能够对网络设备数量进行缩减，简化网络架构，以此缓解系统管理维护的压力。

网络在云计算中的服务形态



HUAWEI

- 虚拟私有云（Virtual Private Cloud）是用户在华为云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性IP搭建业务系统。
- NAT网关（NAT Gateway）提供公网NAT网关和私网NAT网关。公网NAT网关为VPC内的云主机提供SNAT和DNAT功能，可轻松构建VPC的公网出入口。私网NAT网关为VPC内的云主机提供网络地址转换服务。
- 弹性公网IP（Elastic IP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。拥有多种灵活的计费方式，可以满足各种业务场景的需要，使多个云主机可以共享私网IP访问用户本地数据中心或其他VPC，并支持云主机面向私网提供服务。

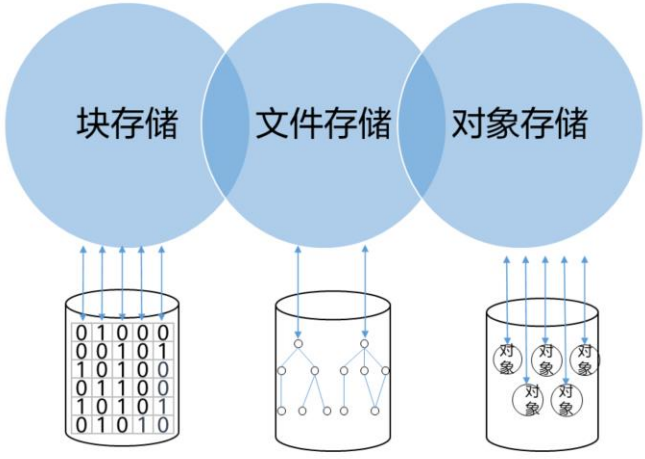
目录

云上数据如何存储

HUAWEI

- 存储介质的作用：数据存储是数据流在加工过程中产生的临时文件或加工过程中需要查找的信息。数据以某种格式记录在计算机内部或外部存储媒介上。
- 为什么会出现云存储?
  - 在解决数据存储问题上，现有的云存储产品已经能够做到在效率和成本上的同步降低，所以，摒弃原始的存储方式，选择云存储会将是个人、企业的必然选择。

主流存储类型



HUAWEI

- 最初的服务器是计算存储合一的，使用服务器本地存储存放数据，这就是块存储的始祖，通过服务器内部总线连接磁盘，可以达到很低的时延，但是服务器可以承载的磁盘数量有限，在容量、带宽以及可靠性上有所欠缺。随着IT的发展，数据越来越多，对数据可靠性的要求越来越高，就有了计算、存储分离的需求，这时就有了存储阵列。传统的磁盘阵列采用控制器+磁盘框的架构，控制器采用双机头或者多机头设计，可靠性更高，通过扩展磁盘框，存储容量相比服务器本地磁盘，有了成百上千倍的提高，独立地通过FC交换机或者IP交换机与服务器相连，这就是现代的块存储。
- 随着IT系统的进一步发展，企业内的协同办公诉求出现，需要将同一个目录/文件夹共享给多个主机访问，这时便出现了共享文件系统，将目录/文件夹共享给多个主机访问，这就是共享文件存储。文件存储还是在一个数据中心/机房内共享数据。
- 随着互联网的兴起，许多互联网应用需要通过终端设备由公网访问数据，这时支持HTTP/HTTPS协议的对象存储就开始大规模使用了。对象存储支持应用端通过API调用的方式存取数据，并且采用分布式的架构设计，具备大容量、高可靠的特点。

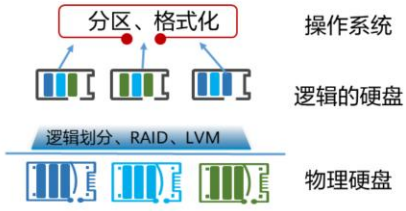
块存储简介

定义

- 块存储是将裸磁盘空间整个映射给服务器使用，比如磁盘阵列里有5块硬盘，可通过划分成N个逻辑盘，然后再映射给服务器，服务器侧完成分区、格式化、挂载后，就可以直接存放数据了。

使用场景

- 块存储通用性强，使用十分广泛，可用于大部分通用业务场景下的数据存储。



HUAWEI

- 块存储是无法直接在操作系统中使用的，必须对块存储进行格式化、创建文件系统后才能使用，操作系统中的数据都是按照文件的格式存放的。
- 块存储适用于数据库、ERP等企业核心应用的存储，具有三大存储中最低的时延。

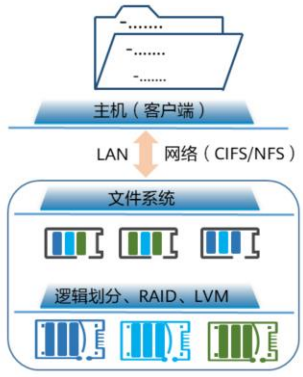
文件存储简介

定义

- 简单来讲，文件存储就好像是一个共享文件夹，文件系统已经存在，用户可以通过共享文件访问协议，直接将自己的数据存放在文件存储上。常见的文件共享协议有NFS、CIFS等。

使用场景

- 由于自带文件系统，并且可以直接存储用户的数据。所以文件存储广泛用于数据备份归档，图片视频类数据存储，文件共享等场景。



HUAWEI

- NFS：Network File System，网络文件系统，Unix系统之间共享文件的一种协议，NFS的客户端主要为Linux。
- CIFS：Common Internet File System，通用网络文件系统，是一个新提出的协议，它使程序可以访问远程Internet计算机上的文件并要求此计算机提供服务。CIFS的客户端主要为Windows。
- 文件存储适用于HPC、企业OA等需要存储数据被多个计算机点共享的场景，具备PB级别的容量，ms级别的时延。

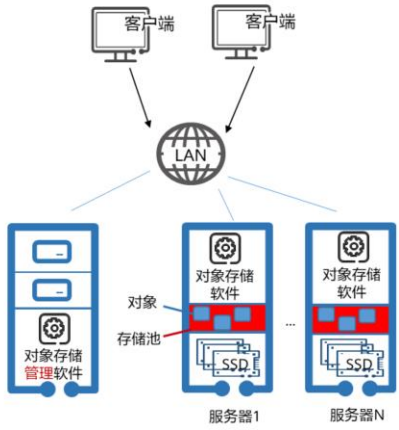
对象存储简介

定义

- 对象存储采用全新的存储架构设计，使其同时兼具块存储高速直接访问磁盘的特点和文件存储的分布式共享特点。因此，它能够像文件存储那样，直接存放用户的数据，而性能却要好过文件存储。

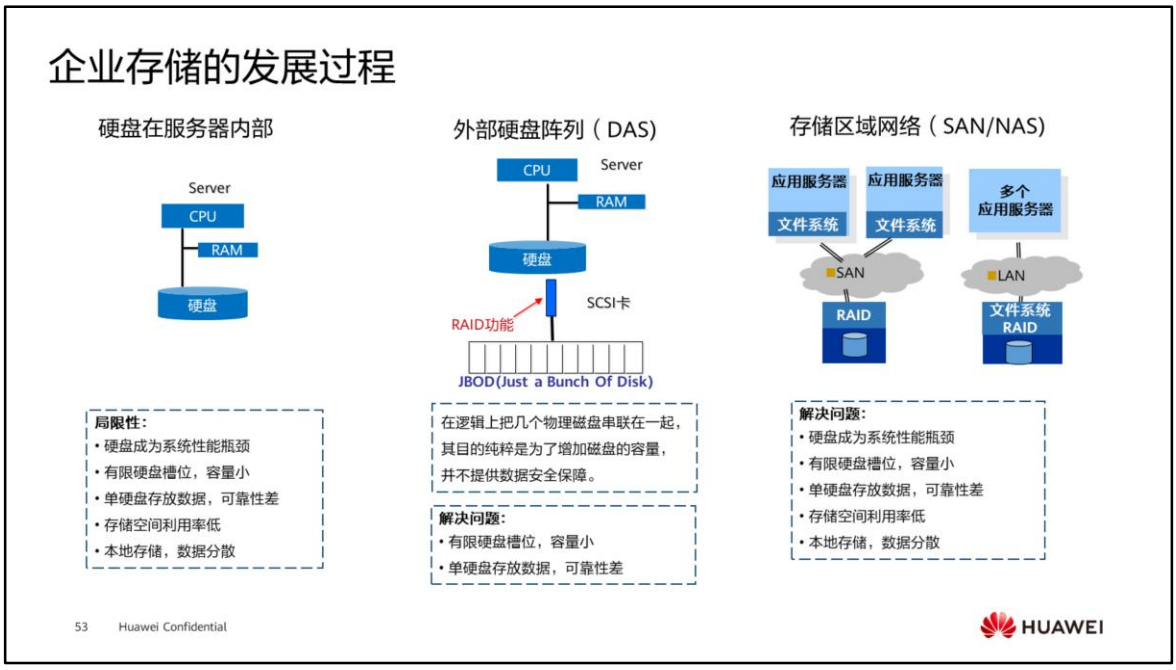
使用场景

- 同文件存储一样，对象存储被广泛使用于数据备份，图片视频类数据存储，网站托管等场景。



HUAWEI

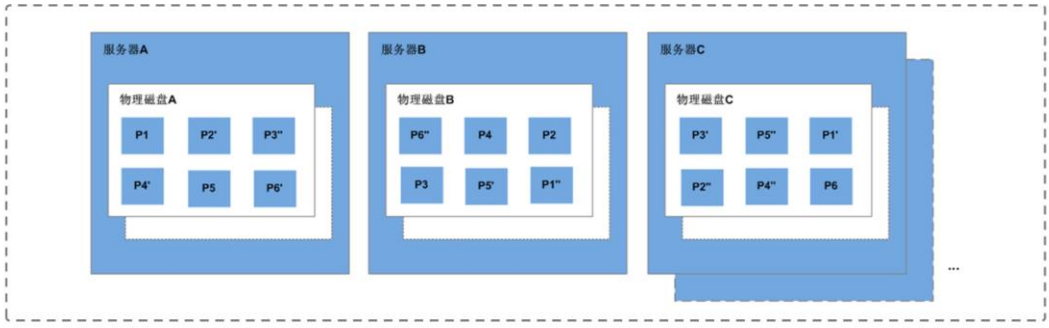
- 超大规模数据管理能力是对象存储相对于文件存储的最大优势。File Storage采用了树形结构对所有文件和目录进行管理，当文件或目录过多时，文件或目录的检索性能就会极大下降。Object Storage只有目录和对象两层结构，这种扁平化的结构即使对象数量达到百亿级别，对象的检索速度依然不会有大的变化。但对象存储接口是应用级接口，而不是系统级接口，因此传统应用迁移到对象存储时需要重新开发，这是对象存储规模应用的最大困难。
- 对象存储适用于大数据、IOT、备份归档等场景，具有EB级别的容量和3大存储中最高的数据可靠性。



- DAS即直接连接存储（Direct Attached Storage），DAS是指将外置存储设备通过SCSI或FC接口直接连接到应用服务器上，存储设备是整个服务器结构的一部分。在这种情况下，数据和操作系统往往都未分离。
- NAS即网络接入存储（Network Attached Storage），NAS采用网络技术（TCP/IP、ATM、FDDI），通过网络交换机连接存储系统和服务器主机来建立存储私网。其主要特征是把存储设备、网络接口和以太网技术集成在一起，直接通过以太网网络存取数据。也就是把存储功能从通用文件服务器中分离出来。
- SAN即存储区域网络（Storage Area Network），SAN是通过交换机连接存储阵列和服务器，建立专用数据存储的存储私网。

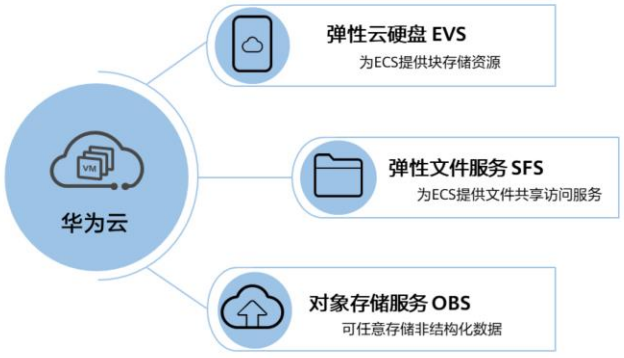
什么是分布式存储技术

- 分布式存储是一种数据存储技术，通过网络使用企业中的每台机器上的磁盘空间，并将这些分散的存储资源构成一个虚拟的存储设备，数据分散地存储在企业的各个角落。提高了系统的可靠性、可用性和存取效率等。



- 实际上，使用分布式存储是“被迫”的，因为随着互联网的飞速发展、应用越来越丰富、用户数量越来越多、数据也成几何级增长，海量数据的存储给本地存储带了巨大压力，存储系统已经不堪重负，处于崩溃的边缘，因此，必须通过其他手段分散存储系统压力，分布式存储和分布式文件系统应运而生。
- 如何保证分布式存储的高性能与高可用?
  - 除了传统架构里面的备份、双活、多活这种架构之外，为了保证分布式存储系统的高可靠和高可用，数据在系统中一般存储多个副本。当某个存储节点出故障时，系统能够自动将服务切换到其他的副本，从而实现自动容错。分布式存储系统通过复制协议将数据同步到多个存储节点，并确保多个副本之间的数据一致性。同一份数据有多个副本，仅有一个为主副本，其他的副本为备份副本，数据从主副本复制到备份副本，采用最终一致性来保证数据完整。

存储在云计算中的服务形态



HUAWEI

- 云硬盘（Elastic Volume Service）是一种为ECS、BMS等计算服务提供持久性块存储的服务，通过数据冗余和缓存加速等多项技术，提供高可用性和持久性，以及稳定的低时延性能。用户可以对云硬盘做格式化、创建文件系统等操作，并对数据做持久化存储。
- 提供按需扩展的高性能文件存储（NAS），可为云上多个弹性云服务器（Elastic Cloud Server，ECS），容器（CCE&CCI），裸金属服务器（BMS）提供共享访问。
- 对象存储服务（Object Storage Service）是一款稳定、安全、高效、易用的云存储服务，具备标准Restful API接口，可存储任意数量和形式的非结构化数据。

思考题

1. （判断题）桥接和NAT的实现原理是相同的。

   正确

   错误

2. （单选题）以下哪一个不是当前主流的存储类型?

   A. 块存储

   B. 对象存储

   C. 磁带库

   D. 文件存储

HUAWEI

- 错误。桥接只是将虚拟机的网口接到了物理网口上，从而出物理服务器。而NAT是通过网络地址转换，来实现虚拟机的流量从物理网口出去的目的。
- C。当前主流的存储类型主要有3个：块、文件、对象。磁带也算一个存储介质，但是已经被逐步淘汰了，只出现在一些备份归档的场景中。

本章总结

- 本章主要介绍了云计算的一些基本知识以及计算类、网络类、存储类的一些基础技术。通过这些知识和技术，我们对云计算有了比较好的认识，也对云服务有了初步的印象。在后面的章节中，我们将继续了解相关的云服务。

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为云技术支持网站
  - https://support.huaweicloud.com/help-novice.html
- 华为云学院
  - https://edu.huaweicloud.com/

术语和缩略语

APP：Application，应用

AS：Auto Scaling，弹性伸缩

CPU：Central Processing Unit，中央处理器

CCE：Cloud Container Engine，云容器引擎

CCI：Cloud Container Instance，云容器实例

CIFS：Common Internet File System，通用网络文件系统

ECS：Elastic Cloud Server，弹性云服务器

EIP：Elastic IP，弹性IP

EVS：Elastic Volume Service，弹性云硬盘

术语和缩略语

GPU：Graphics Processing Unit，图形处理器

ICT：Information and Communications Technology，信息通信技术

I/O：Input/Output，输入/输出

IaaS：Infrastructure as a Service，基础设施即服务

IBM：International Business Machines Corporation，国际商业机器公司

KVM：Kernel-based Virtual Machine，开源虚拟机

IMS：Image Management Service，镜像管理服务

LXC：Linux Container，Linux容器

LVM：Logical Volume Manager，逻辑卷管理

术语和缩略语

NAT：Network Address Translation，网络地址转换

NFS：Network File System，网络文件系统

NIST：National Institute of Standards and Technology，美国国家标准与技术研究院

OS：Operation System，操作系统

OBS：Object Storage Service，对象存储服务

PC：Personal Computer，个人电脑

PaaS：Platform as a Service，平台即服务

RAID：Redundant Arrays of Independent Disks，独立磁盘冗余阵列

SFS：Scalable File Service，弹性文件服务

术语和缩略语

SWR：SoftWare Repository for Container，容器镜像服务

SaaS：Software as a Service，软件即服务

TCO：Total Cost of Ownership，总拥有成本

TAP：Test Access Point，分路器

VM：Virtual Machine，虚拟机

VLAN：Virtual Local Area Network，虚拟局域网

VPC：Virtual Private Cloud，虚拟私有云

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

华为云介绍

HUAWEI

前言

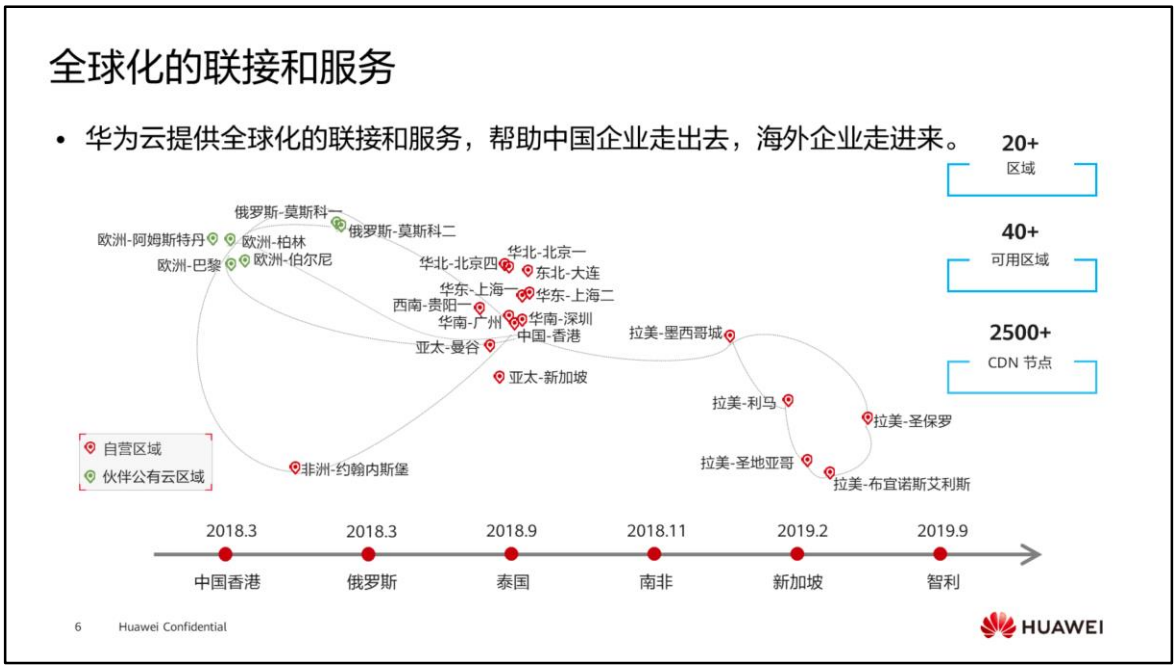
- 华为云是华为的云服务品牌，将华为30多年在ICT领域的技术积累和产品解决方案开放给客户，致力于提供稳定可靠、安全可信、可持续创新的云服务，赋能应用、使能数据、做智能世界的“黑土地”，推进实现“用得起、用得好、用得放心”的普惠AI。
- 本章，我们将带领大家了解华为云。

目标

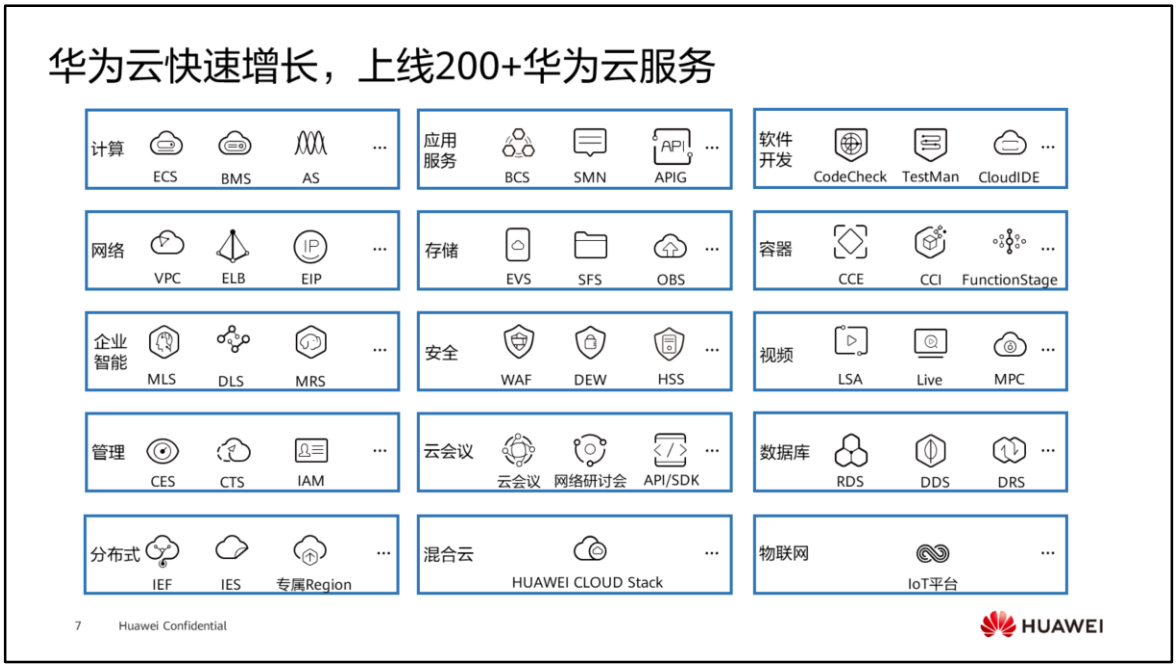
- 学完本课程后，您将能够：
  - 了解华为云的定位、应用场景。
  - 了解华为云的交付模式、技术支持和华为生态。
  - 了解华为云相关概念。

目录

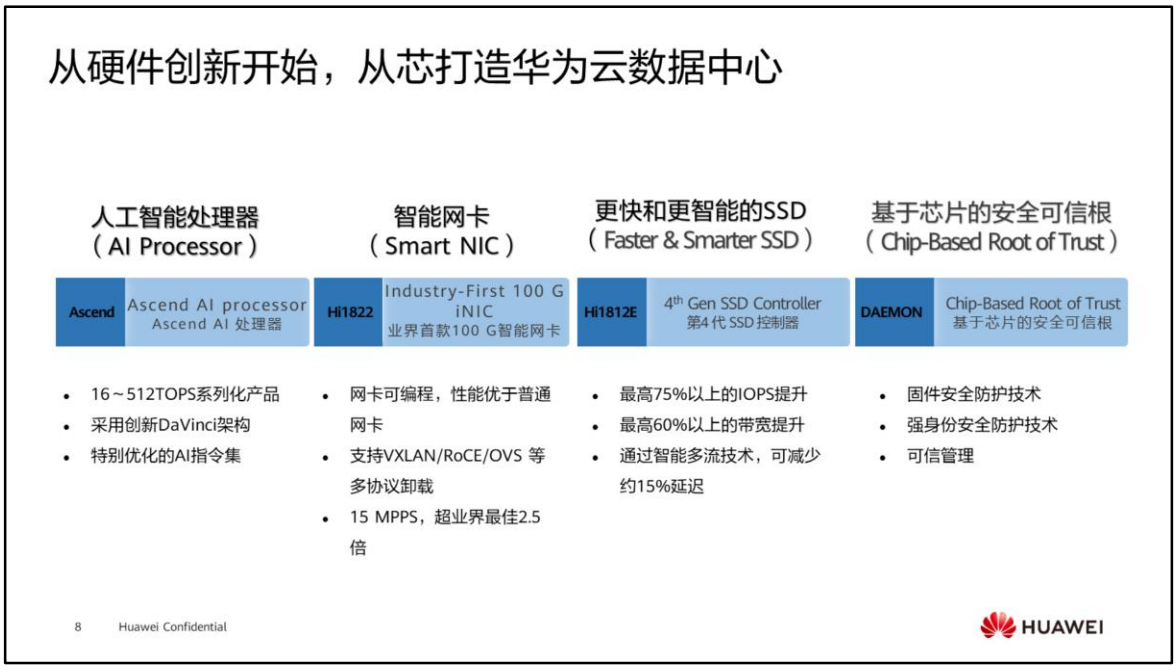
- 华为云是华为面向所有用户发布的一款云服务品牌，定位于公有云，凭借华为三十多年ICT基础设施领域积累沉淀，为客户提供各种云与AI协同创新、中立安全可信的云服务。
- 华为云平台形象视频：https://bbs-video.huaweicloud.com/video/media/20200720/20200720115105_10194/%E5%8D%8E%E4%B8%BA%E4%BA%91%E5%93%81%E7%89%8C%E5%BD%A2%E8%B1%A1%E8%A7%86%E9%A2%91.mp4 。



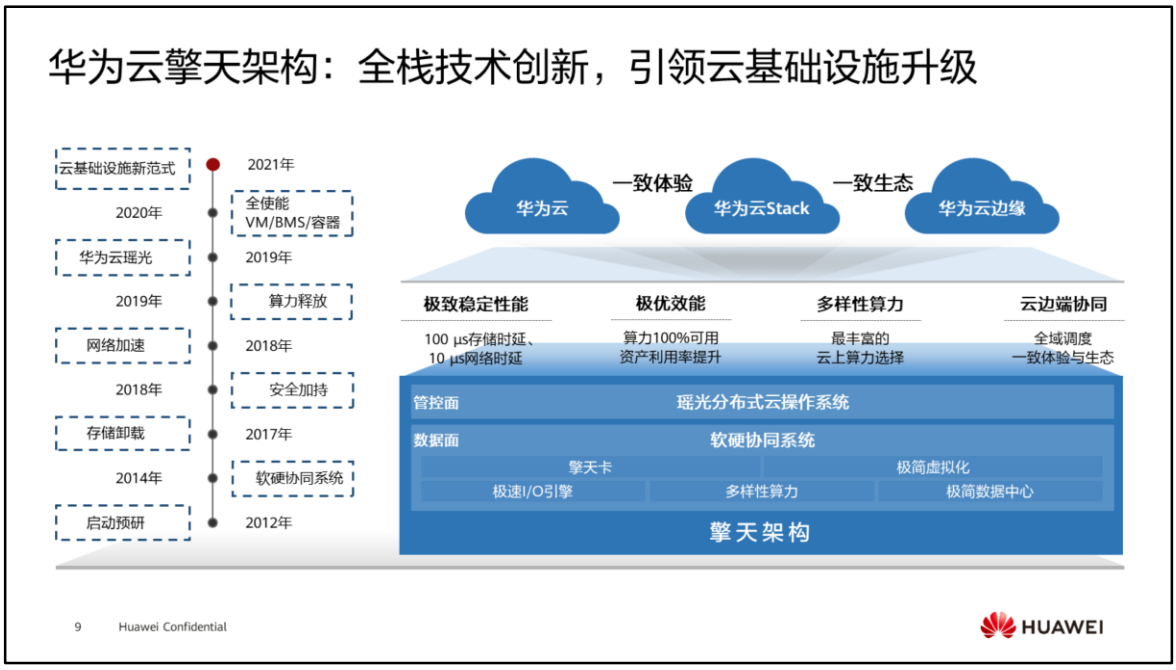
- 在海外，华为云的新加坡、智利、巴西、墨西哥、秘鲁大区陆续开服，与伙伴在全球20+个地理区域运营40+个可用区，能够为跨国企业提供全球化的公有云服务，能全力支持中国企业走向海外，海外企业进入中国市场。华为云为亚太地区用户提供安全可靠的云服务，并在十多个亚太国家设有本地服务团队。在拉美，华为云已成为在拉美建设本地数据中心最多的云服务商。2019年华为在南非正式上线华为云，是全球第一个在南非运营本地数据中心的云服务提供商，发展迅速，目前为非洲12个国家提供云服务，包括安哥拉、博茨瓦纳、加纳、肯尼亚、毛里求斯、莫桑比克、纳米比亚、尼日利亚、南非、坦桑尼亚、赞比亚及津巴布韦。华为云在非洲已发展伙伴200+，覆盖非洲30+个国家。



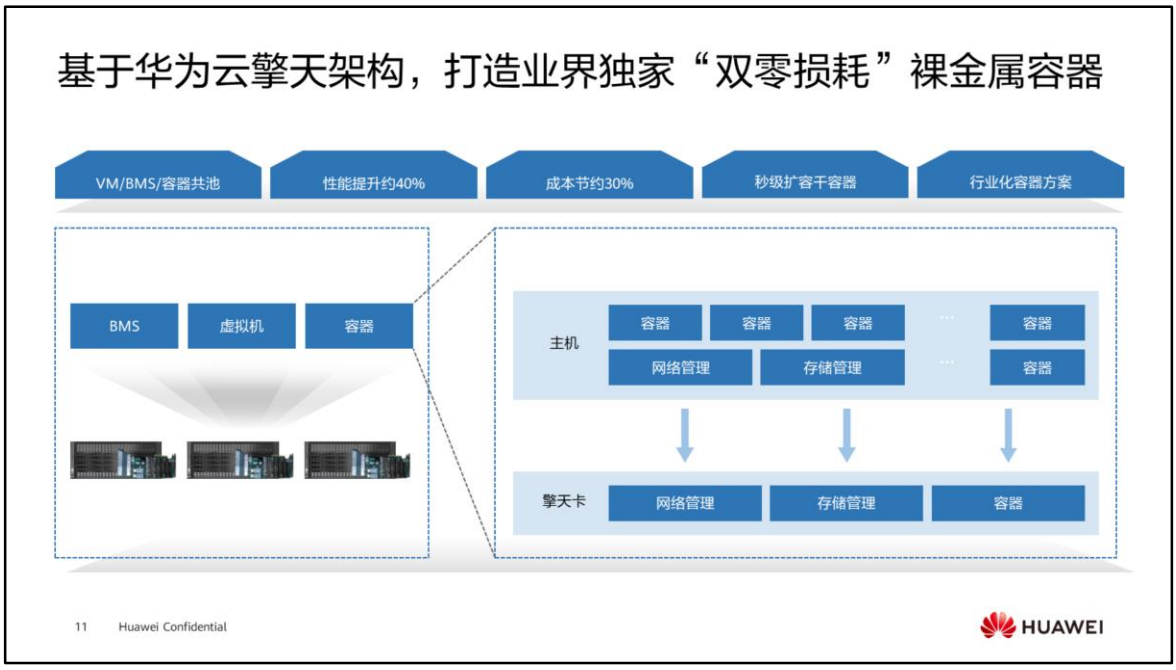
- 华为云对全栈云原生技术能力，进行了持续的创新升级，我们已经上线了220多个云服务和210多个解决方案。



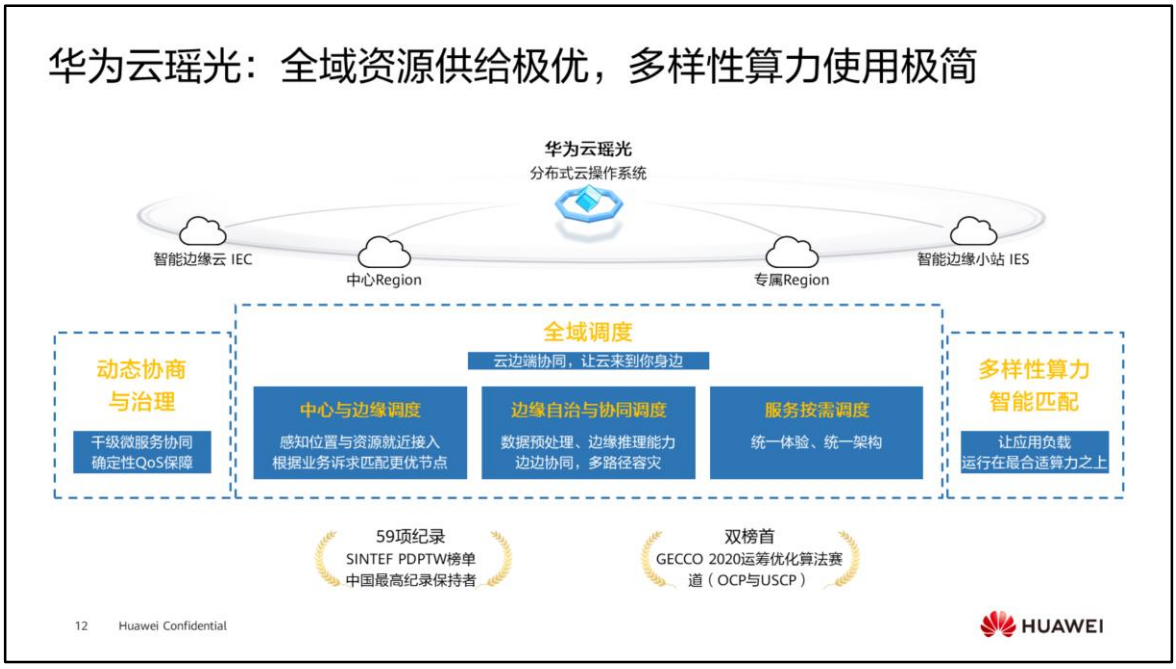
- 芯片是IT产业的压舱石，是IT产业研发的最核心、最难点，需要长期专注的投入。
- 华为秉承过去20多年在芯片上的长期积累，持续在Cloud 2.0时代进行芯片的创新，目前已经推出新一代的云数据中心全系列芯片。
  - 计算芯片：全系列AI处理器
  - 网络芯片：华为新一代网络芯片Hi822，基于类NP可编程架构，支持多种协议的Offloading
  - 存储芯片：已经发展到第四代，75%以上的性能提升，60%以上的带宽提升，基于智能多流技术，减少约15%时延
  - 安全芯片：华为将安全可信根植于芯片之中，从而基于可信的管理，将固件、身份、软件系统、数据置于全面的保护之中



- 华为云提供1个基于擎天架构的云基础设施底座，为企业构筑硬核性能、极致稳定、多样性算力、云边端协同的云基础设施。历时八年打造的擎天架构，为华为云、华为云Stack、华为云边缘提供一致架构、一致体验和一致生态。



- 华为云擎天架构在业界首家实现了裸机、虚拟机、容器共主机、共资源池，使得资源100%可用，企业资产利用率达到极致。
- 华为云擎天架构还推出了业界首个双零损耗容器，将容器引擎整体卸载到擎天卡上，可以提升40%的网络性能，同时帮客户节省30%的成本，在容器领域持续领先。

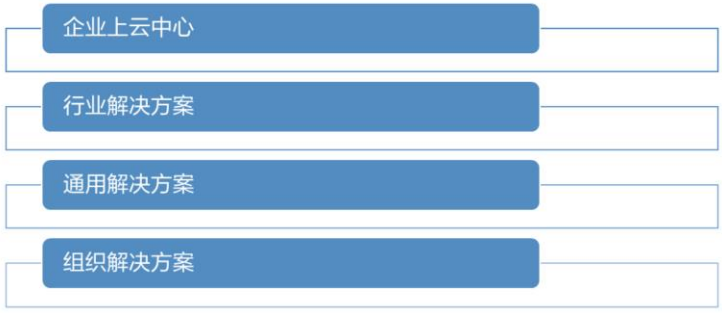


- 同擎天架构不同，擎天架构主要是数据面的软硬协同架构系统，而瑶光则是管控面的分布式云操作系统。我们可以把擎天理解为华为云的基础设施底座，而瑶光则是在擎天架构之上运行的分布式云操作系统。
- 瑶光分布式云操作系统通过三大关键能力，实现“极优、极简”的云上体验：
  - 全域调度：支撑未来10万级分布式站点间复杂的调度协同，实现全域资源供给极优。主要有三个维度：
    - 中心与边缘的调度：实现就近接入，可根据业务诉求匹配最优节点
    - 边缘自治与协同调度：如车路协同，边缘可独立进行数据预处理、推理
    - 服务按需调度：同享180+云服务、40+算子按需推送

目录

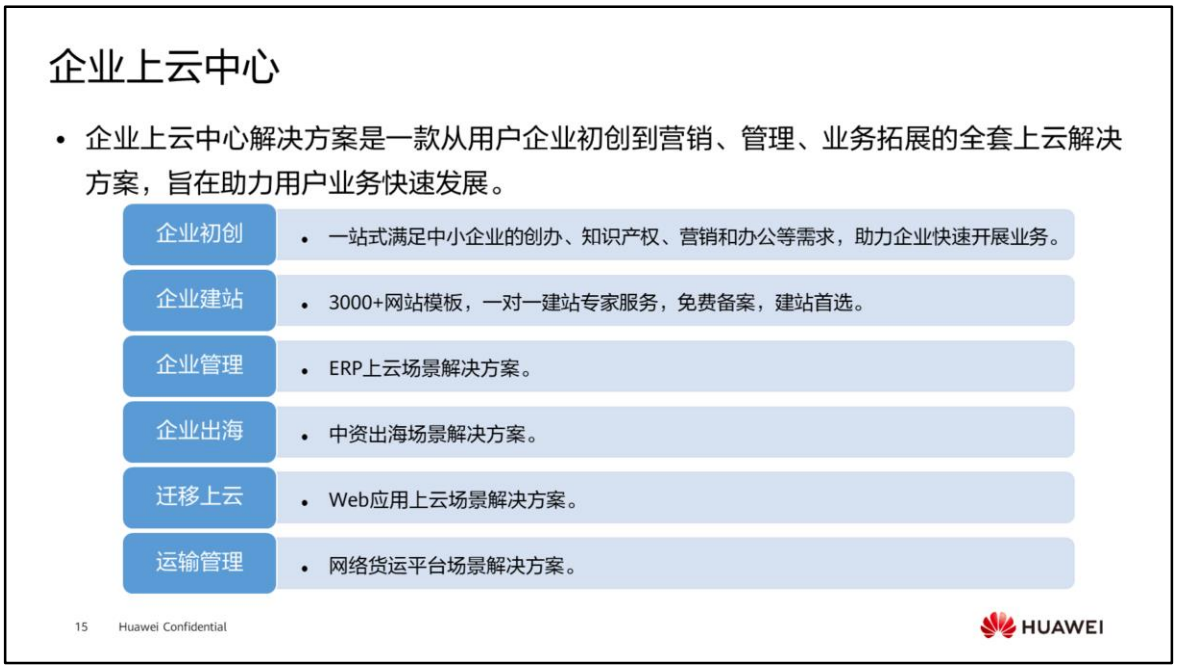
华为云应用场景概览

- 华为云针对于千行百业不同用户的场景，推出了四种解决方案供用户参考，方便用户更快更好地找到属于自己需求的云服务。



HUAWEI

- 四种解决方案的应用场景，后文将逐一展开。



- 企业上云中心是华为云针对企业上云所提供的各种解决方案的集合，为客户提供企业迁移上云、企业初创、企业管理、企业出海、运输管理等各类云解决方案：
  - 迁移上云方面提供Web应用上云场景、云上网络互联场景、华为云灾备场景、华为云容器上云等解决方案
  - 企业初创方面提供企业初创场景解决方案
  - 企业管理方面提供ERP上云场景、企业管理通用场景、华为云会议全场景等解决方案
  - 企业出海方面提供跨境电商场景、游戏出海场景、SaaS出海场景等解决方案
  - 运输管理方面提供网络货运平台场景解决方案

- 华为云行业解决方案如下（最新分类请参考华为云官网）：
  - 金融：金融专区，虚拟银行，保险全业务上云，证券行业资讯等。
  - 零售电商：自建电商，智慧零售，智慧门店，电商鞋服等。
  - 媒体文娱：渲染，VR视频，融合媒体等。
  - 交通物流：智慧高速，智慧机场，智慧物流，智慧停车等。
  - 农业及环保：智慧气象，遥感行业解决方案等。
  - 游戏：云游戏，游戏云端部署，游戏运营分析，游戏安全等。
  - 政府及公共事业：遥感，智慧气象，智慧财政，交通智能体等。
  - 制造：云MES，云仿真，智能配煤，预测性维护等。
  - 工业互联网：为工业转型升级提供增量的智能化平台。
  - 能源：光伏云网，智慧充电，油气勘探开发，电力数据中台等。
  - 汽车：车联网，汽车仿真，数字化营销，自动驾驶开发平台等。
  - 智慧城市：政务云，政务大数据，城市智能运营中心等。
  - 医疗健康：医联体，基因测序，医药云，医疗影像等。
  - 教育：随时学，区域教育云，人才培养云，高教云中校园等。

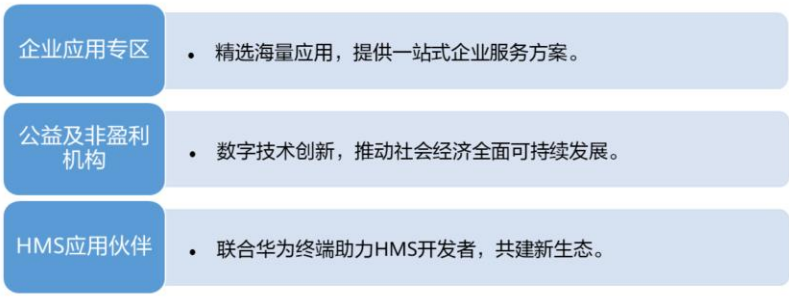
通用解决方案

- 华为云通用解决方案是华为基于丰富的云基础服务，提供适用于各行业的、预集成的产品与能力的组合，以满足企业ICT业务上云的需求。

- 华为云通用解决方案如下（最新分类请参考华为云官网）：
  - 视频：视频直播，视频点播，视频转码，5G超高清制播，云展会等。
  - 安全：上云安全建设实践，等保合规，网站安全，云主机防暴力破解，通用安全等。
  - 科学计算：量子计算，高性能计算等。
  - 数据平台：数据使能DAYU，智能空管数据使能等。
  - 商业应用：ERP上云解决方案，核心大数据上云，微软应用上云等。
  - 智慧园区：产业园区，办公园区，物流园区，教育园区，智慧社区，智慧工地，化工园区等。
  - 基础方案：IPv6，云VR，应用性能调优，KYON企业级云网络，BigData Pro大数据等。
  - 区块链：政务服务，金融创新，其他领域等。
  - 容灾与备份：云容灾，备份与归档。
  - 应用平台：应用平台ROMA等。
  - SAP上云：专属云，全系统上云，灾备系统上云，开发测试系统上云等。
  - 边云协同：智慧高速，智慧物流，园区智慧安防，高教数据治理等。
  - 移动互联：网站，移动APP等。
  - DevOps：软件实训，游戏开发，电商双交付等。
  - 企业办公：企业云盘等。

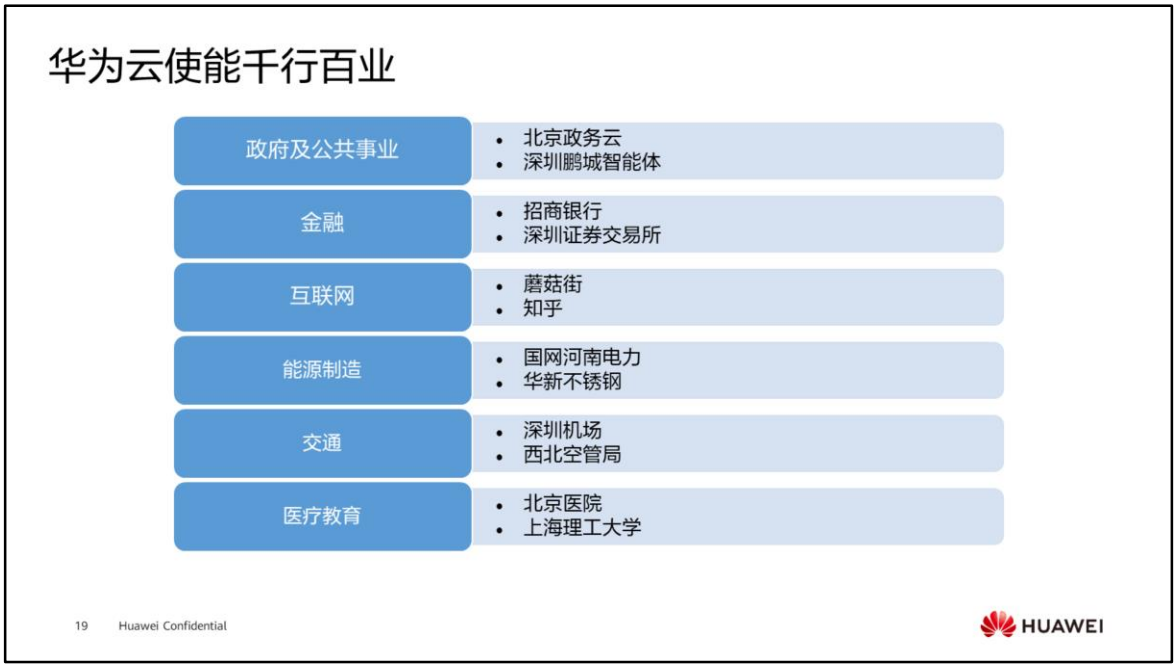
组织解决方案

- 华为云针对企业、公益及非盈利机构、HMS生态伙伴也提供了定向的方案专区，助力其更加方便、快捷地上云。



HUAWEI

- 想要更多了解，可移步华为云：https://www.huaweicloud.com/solution/。

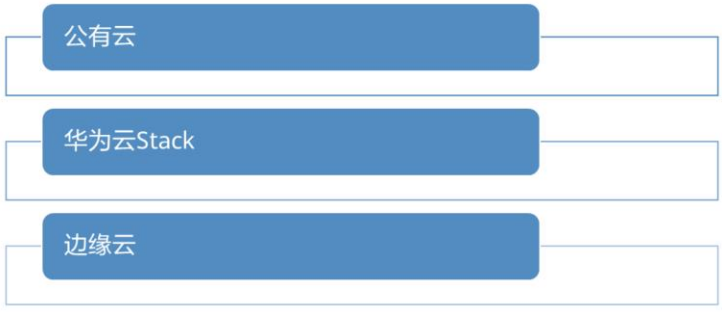


- 华为凭借30+年ICT基础设施建设经验，通过华为云使能千行百业，目前已经与不少行业客户建立了合作。想了解更多优秀案例，可访问华为云官网：https://www.huaweicloud.com/cases.html

目录

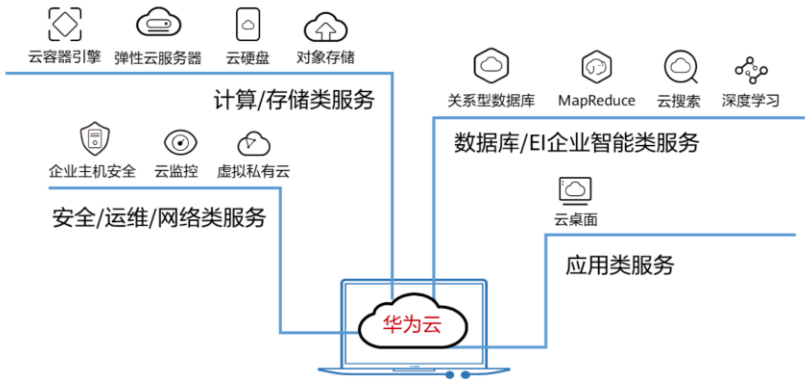
华为云交付模式概览

- 用户由于自身或者企业属性的原因，对于使用云服务的要求也会有所不同。因此，华为云针对于不同用户的不同要求，提供了以下三种交付模式供用户选择。



- 三种交付模式，后文将逐一展开。

公有云模式



HUAWEI

- 公有云的核心属性是共享资源服务华为公有云为个人和企业用户提供IT基础设施服务，使得企业不需要再花费高昂成本自建数据中心，在数据库，企业智能平台等领域也一直深耕，公有云服务商也持续跟进客户需求，补齐云产品。如此一来，客户的基础设施可快速获取，常用平台可轻松构建，软件商城琳琅满目。公有云上为用户提供网络安全、系统安全、数据安全等能力，为客户IT上云保驾护航。
- 用户只需要通过Internet连接到公有云的服务器、存储、平台等资源，对于安全要求较高的场景，还可以通过运营商专线或者VPN连接，使用成本低廉。

华为云Stack模式

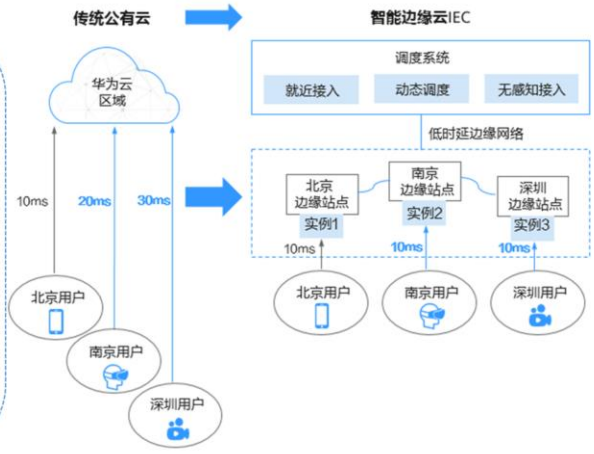
- 华为云Stack是华为云为政企客户提供的，部署在客户本地数据中心的云基础设施。

HUAWEI

- 采用华为云Stack模式交付，既可以兼顾公有云的快速创新能力和私有云的可管可控，同时又能匹配政企组织架构和业务流程，实现用户视角一朵云。
- 华为云Stack交付模式提供了协同、统一、安全的混合云模式，适用于数据要求本地化存储或者有规定设备必须物理隔离的中大型企业。
- 华为云Stack应用场景涵盖业务云化&云原生、大数据分析、AI应用、行业云、城市云。
- 产品优势：三大使能（AI使能、数据使能、应用使能）-公有云能力，本地化部署；多级云管-匹配政企治理架构，云联邦、多级架构、智能运维；云边协同-将智能延伸到边缘，统一边缘框架、视频AI/IoT接入、开箱即用；安全可信-功能/性能领先，全栈可信、一云双池、丰富生态。

边缘云模式

智能边缘云（Intelligent EdgeCloud）部署在距离企业和热点用户区域更近的位置，具有与中心云一致的体验，能够为时延敏感型业务如互动娱乐、在线教育、媒体创作等提供低于10 ms的时延体验，并支持全局智能管理及调度。主要面向互动直播、在线教育、应用加速和自建CDN等应用场景。



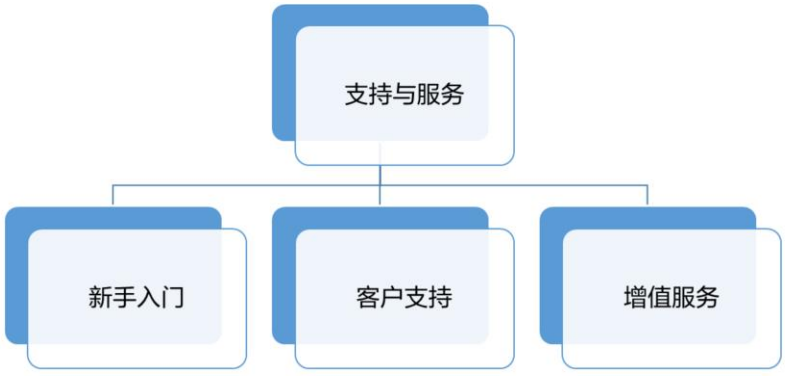
HUAWEI

- 从广义上讲，云计算囊括边缘计算。迈入5G和AI时代，新型业务如互动直播、自动驾驶、智能制造等业务场景对时延和网络带宽有着强烈诉求，而在传统的集中式云计算场景中，所有数据都集中存储在大型数据中心。由于地理位置和网络传输的限制，无法满足新型业务的低时延、高带宽等要求。边缘计算通过在靠近终端应用的位置建立站点，最大限度地将集中式云计算的能力延伸到边缘侧，有效解决以上的时延和带宽问题。
- 华为云边缘云基于覆盖中国大陆主要省市和主流运营商的优质节点资源进行部署，用户可以将时延敏感业务就近接入部署，保证确定性时延，提升业务体验。

目录

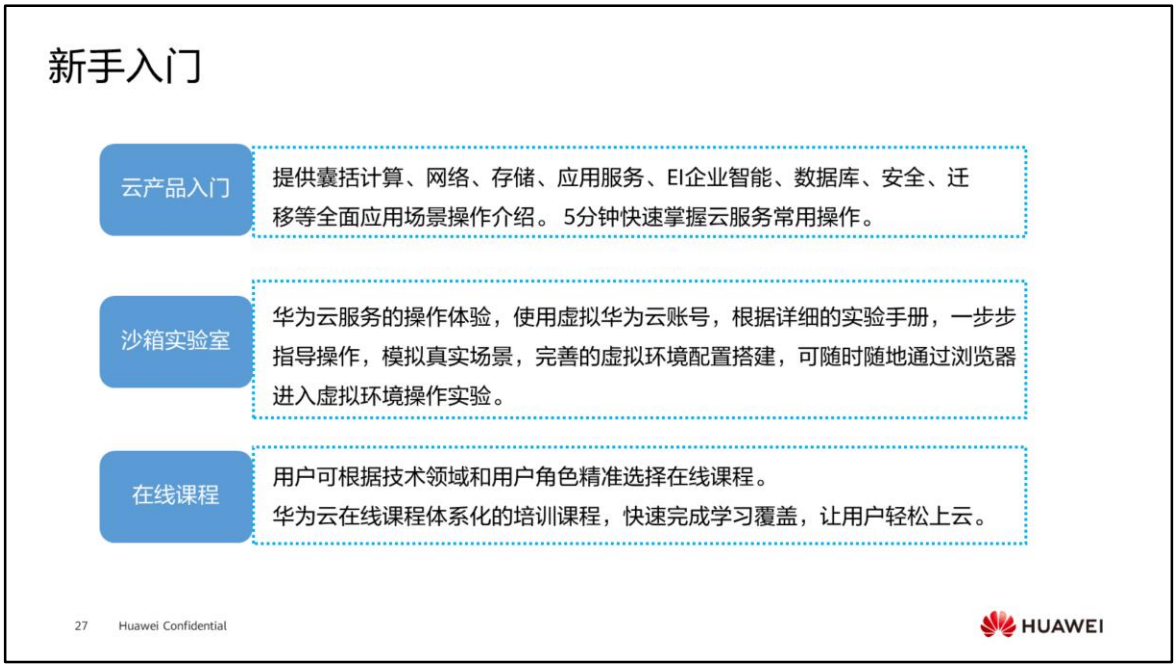
华为云技术支持

- 为用户提供高效的服务保障、多样化的服务支持计划，以及支撑上云前、中、后全流程的专业技术服务，让用户云上业务更便捷、更安心。



HUAWEI

- 华为云的支持与服务体系主要包含新手入门，客户支持，增值服务三大类，接下来我们将一一介绍这三大类的应用。

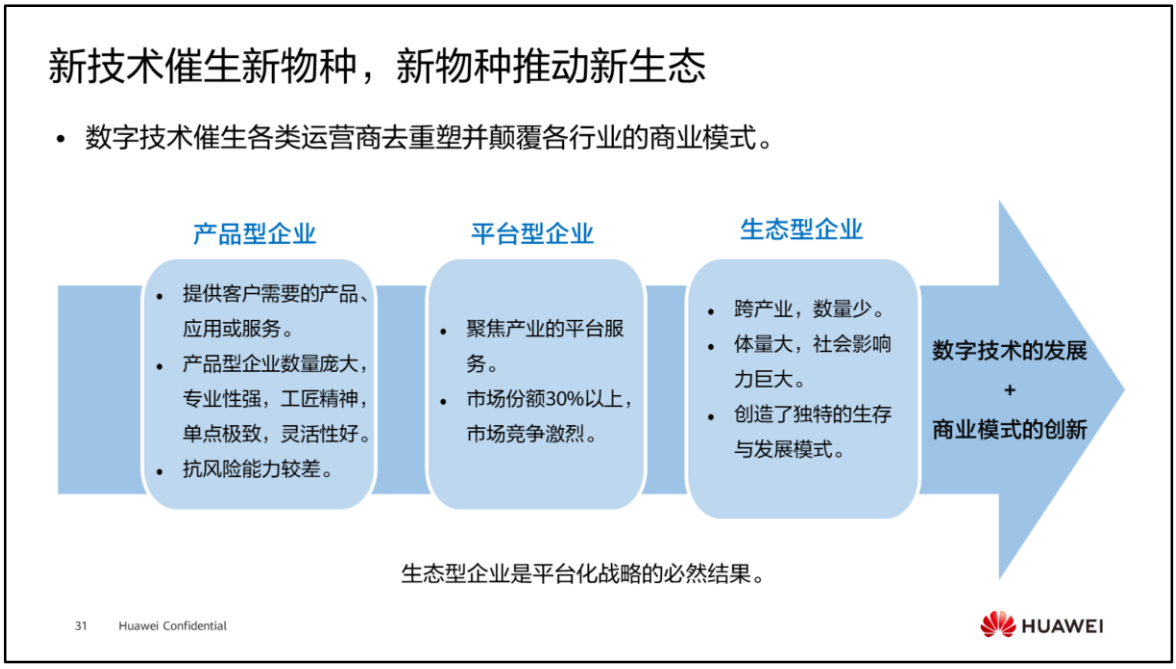


- 从图说云服务、初学者课程、典型场景最佳实践到专家技术汇，全方位地帮用户了解华为云服务器。想了解更多，请移步华为云官网：https://support.huaweicloud.com/help-novice.html。

- 提供多种咨询沟通通道，为客户响应需求。想了解更多，请移步华为云官网：https://support.huaweicloud.com。
- 自助服务为客户提供费用中心、伙伴中心、实名认证、网站备案、统一身份认证等多种自助服务：
  - 费用中心：提供查询欠费详情、消费明细、申请发票、退订等服务
  - 伙伴中心：提供关联与解除关联、设置伙伴折扣等服务
  - 实名认证：提供企业认证和个人认证
  - 网站备案：支持多种备案类型，提供详细备案流程
  - 统一身份认证：创建IAM用户，为IAM用户授权

- 为不同需求的用户提供各种专业的服务支持，全栈的培训认证服务等。
- 华为云专业服务提供上云实施、云上管理、专家服务、培训等服务。
- 华为云培训服务全方位覆盖云服务培训、人工智能培训、智能数据&数据仓库培训、物联网培训、鲲鹏培训、敏捷与DevOps培训、WeLink数字人才等多方面培训。
- 计算增值服务基于计算产品和解决方案，各领域专家使用专业工具，提供卓越的全流程专业服务，加速实现用户的业务价值；资深讲师面授，使能计算人才培养，助力企业数字化转型。

目录



- 从业务层面看，企业始终如一的目标是业务增长和持续盈利，围绕这些目标衍生出提质、增效、降本、安全、创新和合规的业务诉求，注意这些是业务诉求，不是ICT需求，例如这里的降成本不仅仅是指降低ICT的TCO，更是希望通过数字化转型实现整体生产运营成本的降低。
- 企业历经千辛万苦才得以从小到大，最后发现开始有些不堪重负，如何才能做到“大而强”？只有进化为生态型企业才能实现。互联网时代，集团企业多数将选择平台化战略，而平台化战略将是生态型企业的前奏，集团企业进化成为生态型企业是市场适者生存作用的结果。小规模企业则将进化为小型生态企业，只不过生态系统中的物种不再是企业组织，而是一个个团队，是团队的生态系统。

华为云秉承共创、共享、共赢的生态理念，以华为云为底座，构筑生态发展的黑土地，同事携手伙伴，助力行业数字化转型、智能化升级。

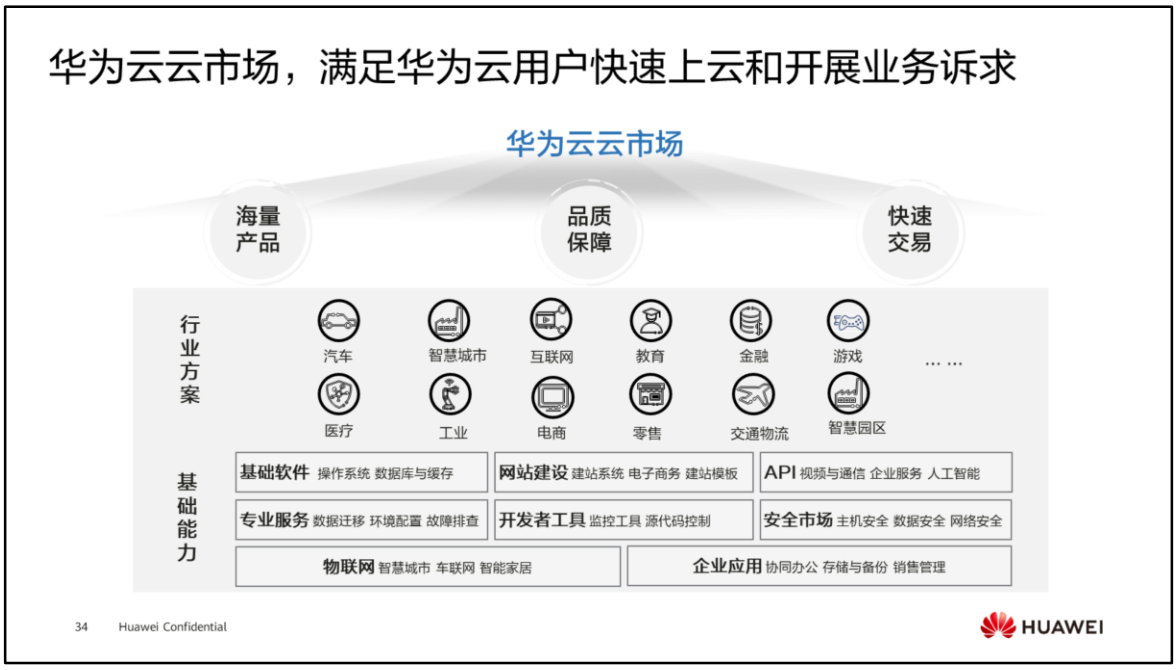
共创：持续不断的技术创新才能使能行业创新，华为云通过构建应用使能、数据使能、AI使能三个使能平台，帮助生态伙伴实现应用的云化、SaaS化及智能化；

共享：行业应用正向云边端协同的场景演进，华为云通过擎天架构打通公有云、混合云、边缘云，构建起统一的应用生态，实现多行业、多应用场景、多部署形态的创新能力共享。

共赢：华为云致力于与伙伴共同为客户创造价值，让优秀软件服务更多的企业，与客户、伙伴共赢数字时代。

- 目前，我们已经聚合了1800000开发者、13000+咨询伙伴、7000+技术伙伴、超过100000付费用户，云市场上架应用4000+，年度交易流水超过10亿元，付费用户数超过10万个，我们诚邀更多的优秀企业加入华为云的生态体系。

- 华为云的合作伙伴体系包括咨询类伙伴、技术类伙伴两类。
- 咨询合作伙伴指专业的服务公司，帮助客户设计、架构、搭建、迁移和管理其工作负载和应用程序，包括咨询公司、经销商、SI等。
- 技术类伙伴指帮助客户搭建基于云服务的平台或提供集成软件解决方案的商用软件公司。包括：独立应用软件开发厂商 (ISV)、SaaS、PaaS、开发工具、管理和安全供应商等。
- 我们为伙伴提供全方位的支持，提供从培训赋能、技术认证、方案上架、商机共享等端到端资源和支撑。
- 2020年，华为云合作伙伴体系新增发布了面向国内的华为云Stack技术伙伴计划、面向海外的SaaS伙伴计划、HMS生态扶持计划等，2021年发布沃土云创伙伴计划，为合作伙伴提供更全面的权益与激励支持。



华为云云市场是企业值得信赖的软件及服务交易交付平台，在云服务的生态系统中，云市场与合作伙伴致力于为用户提供优质、便捷的基于云计算、大数据业务的软件、服务和解决方案，满足华为云用户快速上云和快速开展业务的诉求。
云市场分别提供行业、基础能力等类别的商品目录，从而帮助伙伴的优秀方案更高效地触达行业客户。
服务商基于华为云云市场，可以借助华为全球化的销售和服务能力，扩宽商品的销售通路，提升服务体验，从而更好的服务于最终客户，并获得更多的商业收益。

- 华为云致力于成为最佳应用构建平台！
- 具体来说，华为云提供一系列的极简工具和模板，来提升开发效率。同时，提供应用、数据、AI三个使能服务，内置多种行业知识与资产模型，灵活响应市场需求变化。
- 更重要的是，华为云要帮助开发者实现商业变现！ 华为云提供强大的应用分发能力，和最具潜力的商业扶持计划，让开发者可以获取丰富的云资源和流量支持，并有机会与顶级的企业加速器、孵化器进行交流合作。希望开发者可以在华为云上成长、成功、成就！
- 华为云Marketplace是我们面向政企用户提供的应用分发平台。两年来，我们飞速发展，目前华为云Marketplace年交易额已超过10亿，订单数量超过10万，有30家伙伴的销售额已经超过1000万。
- 大家熟悉的华为终端应用分发平台AppGallery目前已经是全球第三大应用市场，全球活跃用户达5.3亿，应用累计分发量已突破3844亿。华为云联手AppGallery Connect，打造移动应用一站式解决方案，为集成HMS Core的创新应用提供更多技术及资源支持。
- 华为云希望两大应用分发平台，可以帮助开发者加速商业价值转化。

目录

如何使用华为云

- 我们如何使用华为云?
- 需要关注哪些方面?

HUAWEI

- 创建个人/企业账号
- 查看服务菜单
- 进入控制台
- 如何买
- 资源模型

弹性云服务器的购买流程

HUAWEI

- 弹性云服务器的详细购买过程，我们会在后面的课程内容和实验练习中重点讲解。
- 注意事项：
  - 由于弹性云服务器购买需要花钱，因此注册完账号后需充值才能完成购买流程
  - 如果购买的云资源已结束使用，一定要记得删除并释放资源，以免产生多余费用

如何注册一个企业账号

- 登录华为云网站，华为云网站地址：https://www.huaweicloud.com/
- 华为云企业账号注册
- 华为云企业账号认证
  1. 完成注册后，使用注册账号登录华为云，界面提示需完成企业认证或激活邮箱，单击“确认”
  2. 选择“实名认证 > 企业账号”，根据界面提示，在“银行对公账户认证”或“企业证件认证”中任选一种认证方式完成认证
- 绑定注册邮箱

HUAWEI

- 个人账号和企业账号的区别：
  - 选择个人帐号类型，完成实名认证后的帐号归属个人
  - 选择企业帐号类型，完成实名认证后的帐号归属企业
  - 帐号类型的选择对帐号归属有很大影响，例如，企业帐号做个人实名认证后，发生帐号责任人变动、帐号欠费或归属纠纷时，可能会对使用产生不便或带来经济损失

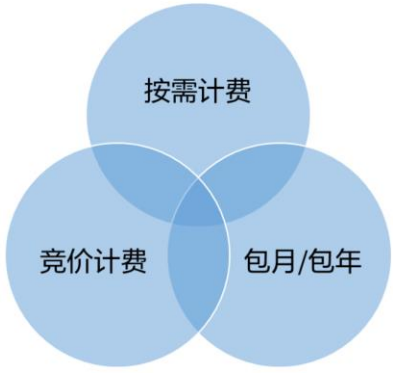
什么是控制台

- 控制台是每个用户申请和管理云服务资源的后台，通过云服务的控制台，我们能够更好地管控自己的资源。

HUAWEI

华为云的计费模式

- 由于不同云服务的计费模式可能存在不同，所以我们以购买弹性云服务器为例，主要包含如图三种计费模式：



- 按需计费：按需计费是后付费模式，按弹性云服务器的实际使用时长计费，可以随时开通/删除弹性云服务器。
- 包月/包年：包年包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。
- 竞价计费：竞价计费是后付费模式，相较于按需计费模式，以更低的折扣按实际使用时长计费。

什么是Region

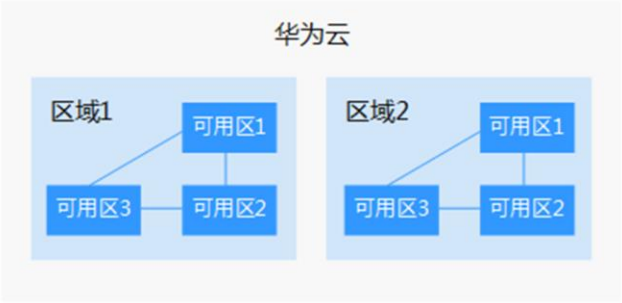
- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。
- Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

HUAWEI

- Region就是一个独立的物理上的数据中心。在华为云上，当用户购买某种云服务时，界面会提供给用户不同的Region选择，如：华北-北京一，华东-上海一等，所以，Region指的是地域，其实就是物理的数据中心。
- 在国内，华为云遵循了“2+7+N”架构、在全国范围内部署高速互联，提供覆盖全国的云服务。
- 乌兰察布与贵阳的数据中心属于“2+7+N”中的“2”，是公司构建的两个一级中心之一。一级中心的建设每个地方要有三个AZ，三个点之间相隔30-50公里，形成三AZ的高可靠架构。
- “2+7+N”中的“7”是华为云的区域中心，包括华北、华东、华南，香港等，是华为云的主力Region。
- “N”是指华为云的卫星节点，每个卫星节点有两个用途：一是作为服务于当地政府的政务云；二是作为华为公有云的一个节点。目前有的N有五个：乌兰察布、襄阳、玉溪、克拉玛依等。
- 选择区域时，需要考虑以下几个因素：
    - 地理位置：一般情况下，建议就近选择靠近用户，目标用户的区域，这样可以减少网络时延，提高访问速度。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果用户或者目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题；
    - 资源的价格：不同区域的资源价格可能有差异。

什么是AZ

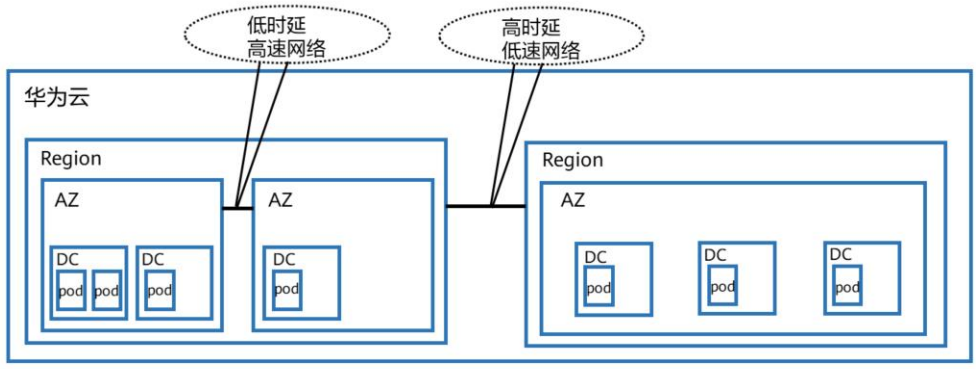
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。



- 风火水电指的是数据中心的制冷，消防，湿度，电力等基础设施的集合。
- 如何选择可用区？是否将资源放在同一可用区内，主要取决于用户对容灾能力和网络时延的要求：
  - 如果应用需要较高的容灾能力，建议用户将资源部署在同一区域的不同可用区内；
  - 如果应用要求实例之间的网络延时较低，则建议用户将资源创建在同一可用区内。

Region和AZ的区别

- 从图中，可用区AZ比区域Region范围小，可用区AZ属于区域Region。一个区域Region可以包含多个可用区AZ。



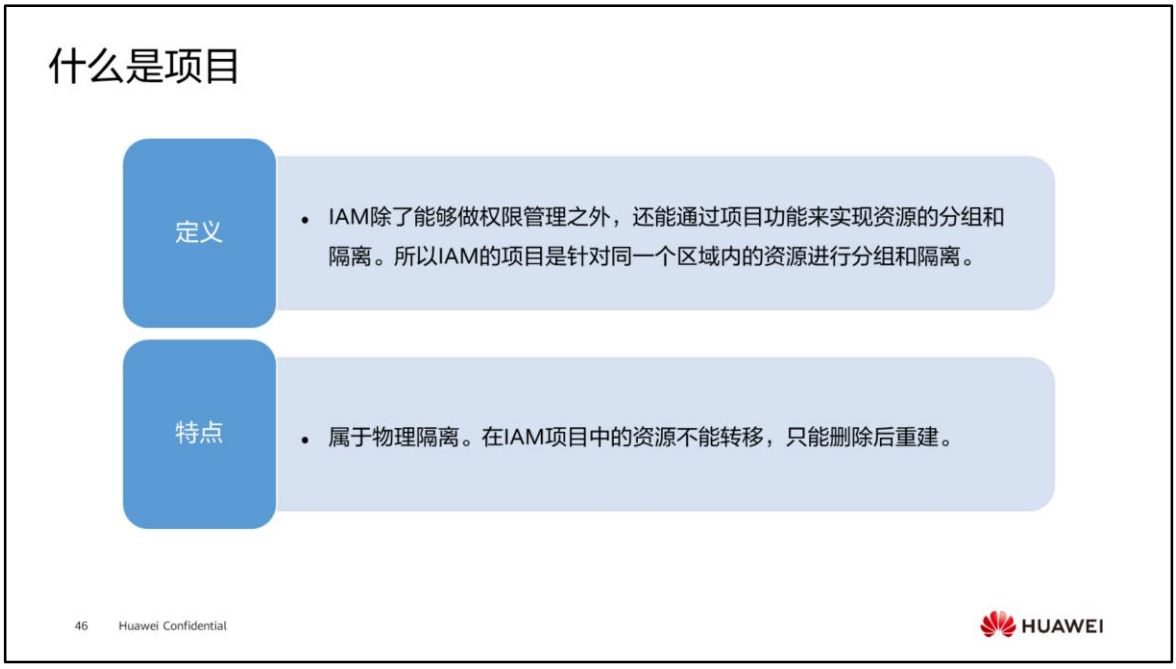
HUAWEI

- 关于图中其他概念的解读：DC指的是物理位置概念的数据中心，或者不同的机房；pod是虚拟化平台管理的资源池或者独立的云平台软件实例，网络时延等效于 AZ。
- 用户可以根据自己的所在地，就近选择靠近自己的Region，从而获得更低的时延，需要注意的是，资源创建成功后不能更换Region，且如果需要考虑同城或者异地备份或容灾，则应考虑跨Region做业务部署。
- 如果用户业务要求较高可用性，可将业务做跨AZ部署。

什么是IAM

- IAM(Identity and Access Management)，又叫统一身份认证管理服务，是提供给用户的一种用户资源管控服务。当用户想要共享资源给其他人，但又不想共享自己的账号和密码时，可以通过创建IAM用户来实现。

- IAM是一种统一身份认证服务，能够帮助用户更安全地控制云服务和资源的访问权限。IAM用户的作用是多用户协同操作同一帐号时，避免分享帐号的密码。关于IAM的详细介绍会在后续章节中展开，本页只做简单介绍。



- 项目的详细介绍可参考：https://support.huaweicloud.com/productdesc-ecs/ecs_01_0058.html。

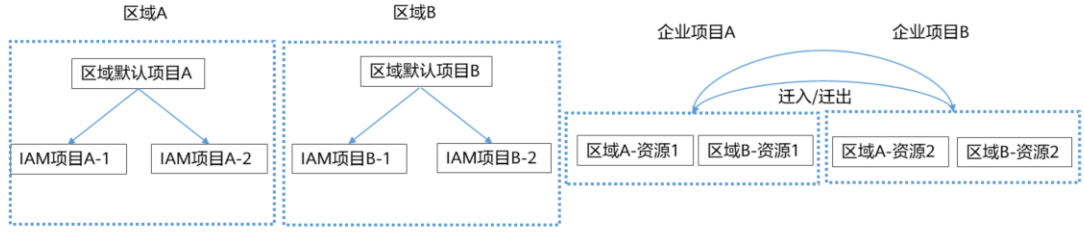
什么是企业项目

定义	• 除了IAM的项目之外，在企业管理服务中，也有项目的概念，我们把它称为企业项目。企业项目是IAM项目的升级版，是针对企业不同项目间资源的分组和管理。
特点	• 企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。如果用户开通了企业管理服务，将不能创建新的IAM项目（只能管理已有项目）。

- 未来IAM项目将逐渐被企业项目所替代，推荐使用更为灵活的企业项目。
- 企业项目的详细介绍可参考：https://support.huaweicloud.com/productdesc-ecs/ecs_01_0058.html。

项目和企业项目的区别

- 项目，也就是IAM项目，主要是针对同一个区域内的资源进行分组和隔离，是物理隔离。在IAM项目中的资源不能转移，只能删除后重建。
- 而企业项目是IAM项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。企业项目可以实现对特定云资源的授权。



HUAWEI

- 项目及企业项目会根据实际场景需求进行变更，以官网描述为准。

思考题

1. （判断题）华为云中购买的服务可以按分钟计费。

   正确

   错误

2. （单选题）以下哪一项不是华为云提供的服务支持?

   A. 自助服务

   B. 智能客服

   C. 云声-建议

   D. 贴身管家

- 错误。当前只有按需计费、包月/包年、竞价计费三种模式。
- D。没有贴身管家这一项

本章总结

- 回顾本章，我们对华为云做了整体性介绍，包括华为云的节点优势、云产品优势、解决方案优势、生态优势、技术支持体系优势等，对于华为云的定位有了清晰的认识且能更好地使用华为云。

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为云技术支持网站
  - https://support.huaweicloud.com/help-novice.html
- 华为云学院
  - https://edu.huaweicloud.com/

本章缩略语

AI：Artificial Intelligence，人工智能

AS：Auto Scaling，弹性伸缩

APM：Application Performance Management，应用性能管理

AOM：Application Operations Management，应用运维管理

AZ：Availability Zone，可用分区

API：Application Programming Interface，应用程序接口

BMS：Bare Metal Server，裸金属服务器

BCS：Hyperledger Fabric，区块链服务

CCE：Cloud Container Engine，云容器引擎

CDN：Content Delivery Network，内容分发网络

本章缩略语

CBH：Cloud Bastion Host，云堡垒机服务

CPTS：Cloud Performance Test Service，云性能测试服务

CAE：Computer Aided Engineering，计算辅助工程

CES：Cloud Eye Service，云监控服务

CTS：Cloud Trace Service，云审计服务

CCS：Cloud Catalog Service，云目录服务

CRS：Cloud Record Service，云报表服务

CDM：Cloud Data Migration，云数据迁移

CMC：Cloud Migration Center，云迁移中心

DES：Data Express Service，数据快递服务

本章缩略语

DNS：Domain Name Service，域名解析服务

DDS：Document Database Service，文档数据库服务

DDM：Distributed Database Middleware，分布式数据库中间件

DAS：Data Admin Service，数据管理服务

DBSS：Database Security Service，数据库安全服务

DMS：Distributed Message Service，分布式消息服务

DWS：Data Warehouse Service，数据仓库服务

DevOps：Development and Operations，开发即运营

ECS：Elastic Cloud Server，弹性云服务器

EVS：Elastic Volume Service，弹性云硬盘服务

本章缩略语

ELB：Elastic Load Balance，弹性负载均衡

EI：Enterprise Intelligence，企业智能

ERP：Enterprise Resource Planning，企业资源计划

GES：Graph Engine Service，图引擎服务

HMS：Huawei Mobile Service，华为移动服务

HSS：Host Security Service，主机安全服务

ICT：Information and Communications Technology，信息通信技术

IMS：Image Management Service，镜像管理服务

IAM：Identity and Access Management，统一身份认证服务

IOPS：Input/Output Operations Per Second，每秒的读写次数

本章缩略语

I/O：Input/Output，输入/输出

LTS：Log Tank Service，云日志服务

MVP：Most Valuable Player，最有价值选手

MRS：MapReduce Service，MapReduce服务

NIC：Network Interface Controller，网络接口控制器

OBS：Object Storage Service，对象存储服务

OCR：Optical Character Recognition，光学字符识别

OMS：Object Storage Migration Service，对象存储迁移服务

OVS：Open Virtual Switch，开源虚拟交换机

QoS：Quality of Service，服务质量

本章缩略语

RoCE：RDMA over Converged Ethernet，允许通过以太网使用远程直接内存访问（RDMA）的网络协议

RDS：Relational Database Service，关系型数据库服务

SDK：Software Development Kit，软件开发工具包

SFS：Scalable File Service，弹性文件服务

SA：Situation Awareness，态势感知

SMN：Simple Message Notification，消息通知服务

SWR：SoftWare Repository for Container，容器镜像服务

SMS：Server Migration Service，主机迁移服务

SSD：Solid State Disk，固态硬盘

本章缩略语

SAP：System Applications and Products，德国的一家企业管理软件公司

TMS：Tag Management Service，标签管理服务

TTS：Text-To-Speech，语音合成

VBS：Volume Backup Service，云硬盘备份服务

VPC：Virtual Private Cloud，虚拟私有云

VPN：Virtual Private Network，虚拟私有网络

VxLAN：Virtual Extensible Local Area Network，虚拟扩展局域网

WAF：Web Application Firewall，web防火墙

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

计算云服务

HUAWEI

前言

- 一直以来，计算资源都是整个企业业务系统发展所需的大动脉，没有计算资源，企业业务就无法正常运行。在云计算的时代里，计算服务也是云服务中的第一大类服务，计算资源的重要性由此可见。
- 本章，我们将带领大家了解华为云上的计算服务。

目标

- 学完本课程后，您将能够：
  - 掌握华为云上常见的计算服务。
  - 掌握这些计算服务的定位、原理以及使用方法等。

计算服务总览


弹性云服务器
ECS


裸金属服务器
BMS


弹性伸缩
AS


云容器引擎
CCE


GPU加速云服务器
GACS


云手机
CPH


镜像服务
IMS


FPGA加速云服务器
FACS

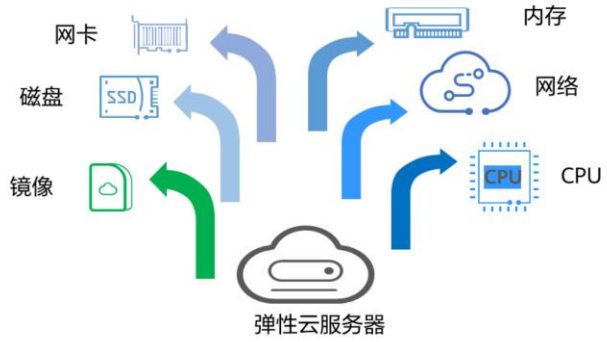

专属主机
DeH


函数工作流服务
FGS

目录

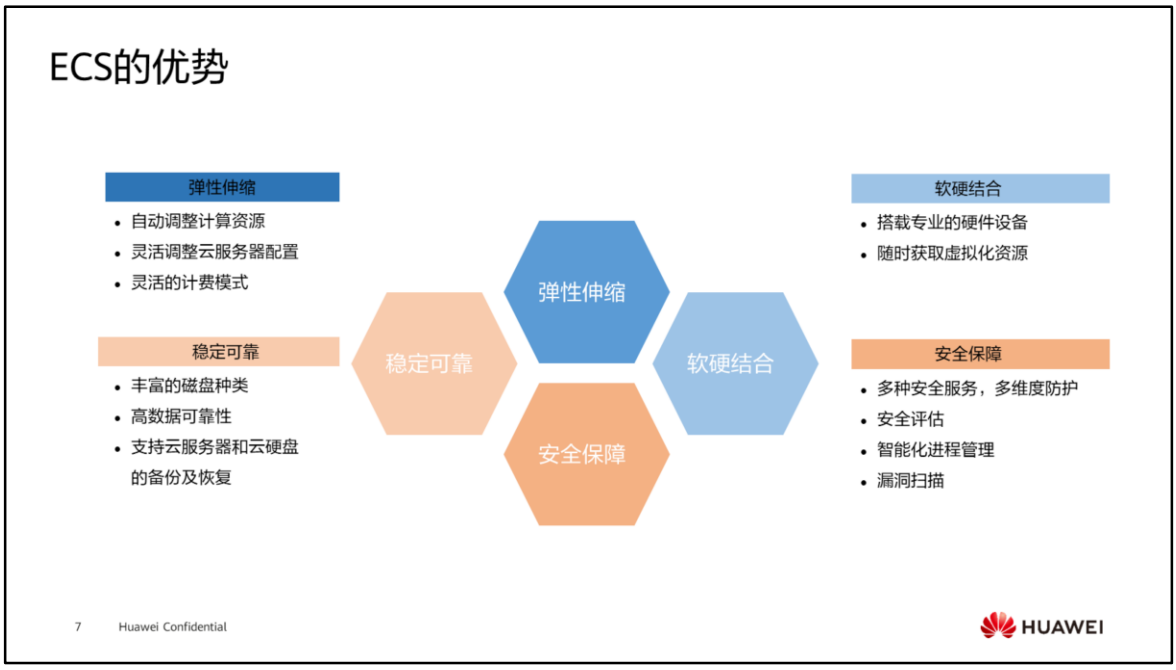
什么是弹性云服务器（ECS）

- 弹性云服务器（Elastic Cloud Server，ECS）是由CPU、内存、操作系统、云硬盘组成的基础计算组件。弹性云服务器创建成功后，可以像使用自己的本地C或物理P服务器一样，在云上使用弹性云服务器。



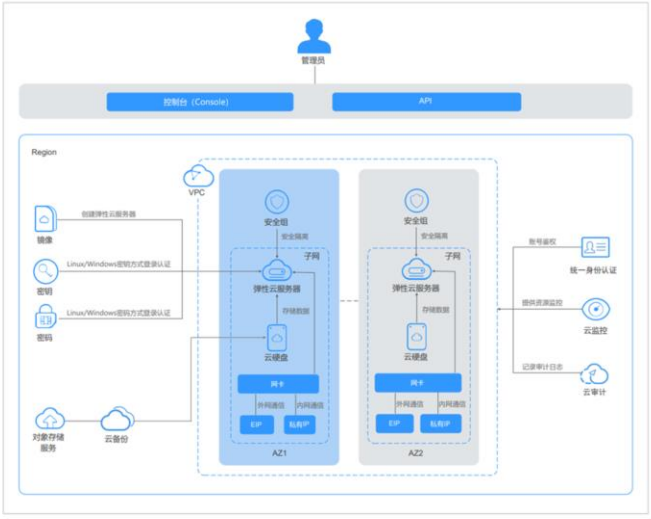
HUAWEI

- 为什么选择弹性云服务器?
  - 丰富的规格类型：提供多种类型的弹性云服务器，可满足不同的使用场景，每种类型的弹性云服务器包含多种规格，同时支持规格变更。
  - 丰富的镜像类型：可以灵活便捷地使用公共镜像、私有镜像或共享镜像申请弹性云服务器。
  - 丰富的磁盘种类：提供普通IO、高IO、通用型SSD、超高IO性能的硬盘，满足不同业务场景需求。
  - 灵活的计费模式：支持包年/包月或按需计费模式购买云服务器，满足不同应用场景，根据业务波动随时购买和释放资源。
  - 数据可靠：基于分布式架构的，可弹性扩展的虚拟块存储服务；具有高数据可靠性，高I/O吞吐能力。
  - 安全防护：支持网络隔离，安全组规则保护，远离病毒攻击和木马威胁；Anti-DDoS流量清洗、Web应用防火墙、漏洞扫描等多种安全服务提供多维度防护。
  - 弹性易用：根据业务需求和策略，自动调整弹性计算资源，高效匹配业务要求。
  - 高效运维：提供控制台、远程终端和API等多种管理方式，给用户完全管理权限。
  - 云端监控：实时采样监控指标，提供及时有效的资源信息监控告警，通知随时触发随时响应。
  - 负载均衡：弹性负载均衡将访问流量自动分发到多台云服务器，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。



- 稳定可靠
  - 丰富的磁盘种类：提供普通IO、高IO、通用型SSD、超高IO、极速型SSD类型的云硬盘，可以支持云服务器不同业务场景需求。
  - 高数据可靠性：基于分布式架构，可弹性扩展的虚拟块存储服务；具有高数据可靠性，高I/O吞吐能力，能够保证任何一个副本故障时快速进行数据迁移恢复，避免单一硬件故障造成数据丢失。
  - 支持云服务器和云硬盘的备份及恢复：可预先设置好自动备份策略，实现在线自动备份。也可以根据需要随时通过控制台或API，备份云服务器和云硬盘指定时间点的数据。
- 安全保障
  - 多种安全服务，多维度防护：Web应用防火墙、漏洞扫描等多种安全服务提供多维度防护。
  - 安全评估：提供对用户云环境的安全评估，帮助用户快速发现安全弱点和威胁，同时提供安全配置检查，并给出安全实践建议，有效减少或避免由于网络中病毒和恶意攻击带来的损失。
  - 智能化进程管理：提供智能的进程管理服务，基于可定制的白名单机制，自动禁止非法程序的执行，保障弹性云服务器的安全性。
  - 漏洞扫描：支持通用Web漏洞检测、第三方应用漏洞检测、端口检测、指纹识别等多项扫描服务。

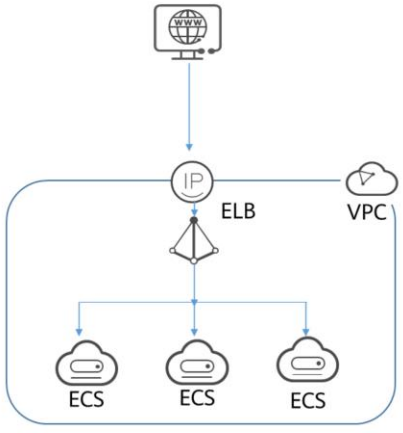
ECS的产品架构



HUAWEI

- 通过和其他产品、服务组合，弹性云服务器可以实现计算、存储、网络、镜像安装等功能：
  - 弹性云服务器在不同可用区中部署（可用区之间通过内网连接），部分可用区发生故障后不会影响同一区域内的其它可用区
  - 可以通过虚拟私有云建立专属的网络环境，设置子网、安全组，并通过弹性公网IP实现外网链接（需带宽支持）
  - 通过镜像服务，可以对弹性云服务器安装镜像，也可以通过私有镜像批量创建弹性云服务器，实现快速的业务部署
  - 通过云硬盘服务实现数据存储，并通过云硬盘备份服务实现数据的备份和恢复
  - 云监控是保持弹性云服务器可靠性、可用性和性能的重要部分，通过云监控，用户可以观察弹性云服务器资源
  - 云备份（Cloud Backup and Recovery，CBR）提供对云硬盘和弹性云服务器的备份保护服务，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

应用场景 - 网站应用



适用场景

- 网站开发测试环境、小型数据库应用

推荐使用

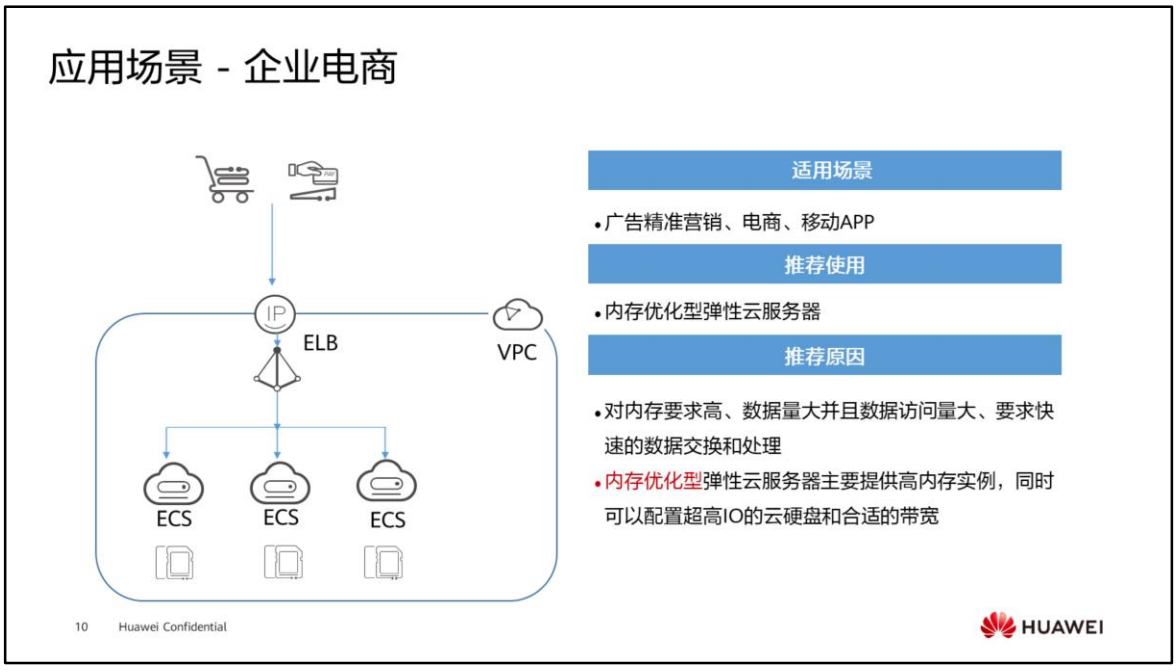
- 通用型弹性云服务器

推荐原因

- 对CPU、内存、硬盘空间和带宽无特殊要求，对安全性、可靠性要求高，服务一般只需要部署在一台或少量的服务器上，一次投入成本少，后期维护成本低
- 通用型弹性云服务器，主要提供均衡的计算、内存和网络资源，适用于业务负载压力适中的应用场景，满足企业或个人普通业务搬迁上云需求

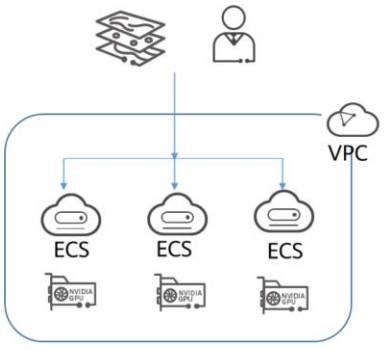
HUAWEI

- 通用计算型弹性云服务器主要提供基本水平的vCPU性能、平衡的计算、内存和网络资源，同时可根据工作负载的需要实现性能的突增，具有短期发挥更高性能的能力。适用于那些不会经常（或始终）用尽vCPU性能，但会偶尔使用的场景，特别适合通用工作负载，如Web服务器、开发人员环境和小型数据库等，是很多应用程序的最佳选择。



- 内存优化型云服务器擅长应对大型内存数据集和高网络场景。适用于内存要求高，数据量大并且数据访问量大，同时要求快速的数据交换和处理。例如广告精准营销、电商、车联网等大数据分析场景。
- 企业电商行业背景：
  - 应对业务浪涌风险高：促销、秒杀、爆款等电商业务场景，瞬间访问量达到平常的几十至数百倍，导致服务器负载高，系统响应慢；瞬间的访问流量暴增，导致带宽占满、数据库瘫痪等，以致整个系统服务不可用
  - 用户体验差：电商业务涉及大量的静态数据，如产品图片，产品视频等，这些数据按照传统的方式放在服务器中，加载速度慢、耗时费钱，不同网络用户访问电商网站出现网页打开慢、网络延时等问题
  - 商业决策缺乏数据支撑：由于缺乏大数据平台及分析工具，无法对已有用户、商品、交易数据进行有效分析，导致电商网站存在推广投入高，用户二次下单率低等问题
  - 安全性难以保证：电商在站外引流、注册登录、浏览比较、获取优惠、下单、支付、交付及评价等环节存在撞库爆破、薅羊毛、黄牛倒卖、网页篡改、DDoS攻击、账号泄露、木马植入等一系列风险

应用场景 - 图形渲染



适用场景

- 图形渲染、工程制图

推荐使用

- GPU图形加速型弹性云服务器

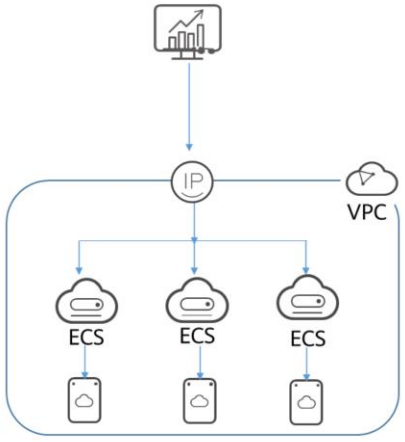
推荐原因

- 对图像视频质量要求高、大内存，大量数据处理，I/O并发能力，可以完成快速的数据处理交换以及大量的GPU计算能力
- 使用GPU图形加速型弹性云服务器，提供较为经济的图形加速能力

HUAWEI

- GPU加速型云服务器（GPU Accelerated Cloud Server，GACS）能够提供强大的浮点计算能力，从容应对高实时、高并发的海量计算场景。
- GPU加速型云服务器包括G系列和P系列两类。其中：
  - G系列：图形加速型弹性云服务器，适合于3D动画渲染、CAD等
  - P系列：计算加速型或推理加速型弹性云服务器，适合于深度学习、科学计算、CAE等

应用场景 - 数据分析



适用场景

- MapReduce、Hadoop计算密集型

推荐使用

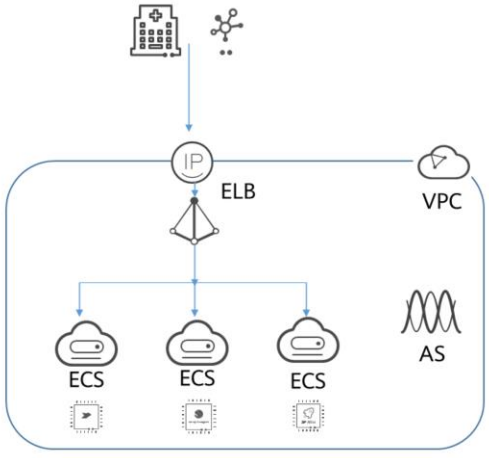
- 磁盘增强型弹性云服务器

推荐原因

- 处理大容量数据，需要高I/O能力和快速的数据交换处理能力的场景
- 磁盘增强型弹性云服务器，主要适用于需要对本地存储上的极大型数据集进行高性能顺序读写访问的工作负载

- 磁盘增强型弹性云服务器自带高存储带宽和IOPS的本地盘，具有高存储IOPS以及读写带宽的优势。同时，本地盘的价格更加低廉，在海量数据存储场景下，具备更高的性价比。磁盘增强型弹性云服务器具备如下特点：本地磁盘提供更高顺序读写性能和更低时延，提升文件读写性能。
- 提供强大而稳定的计算能力，保障计算作业的高效处理效率。
- 提供更高的内网性能，包括高内网带宽和PPS（ Packet per Second ），满足业务高峰期弹性云服务器间数据交互需求。
- 场景举例：Hadoop分布式计算，大规模的并行数据处理和日志处理应用。主要的数据存储是基于HDD的存储实例，默认配置最高10 GE网络能力，提供较高的PPS性能和网络低延迟。最大可支持24个本地磁盘、48个vCPU和384 GB内存。

应用场景 - 高性能计算



适用场景

- 科学计算、基因工程、游戏动画、生物制药等

推荐使用

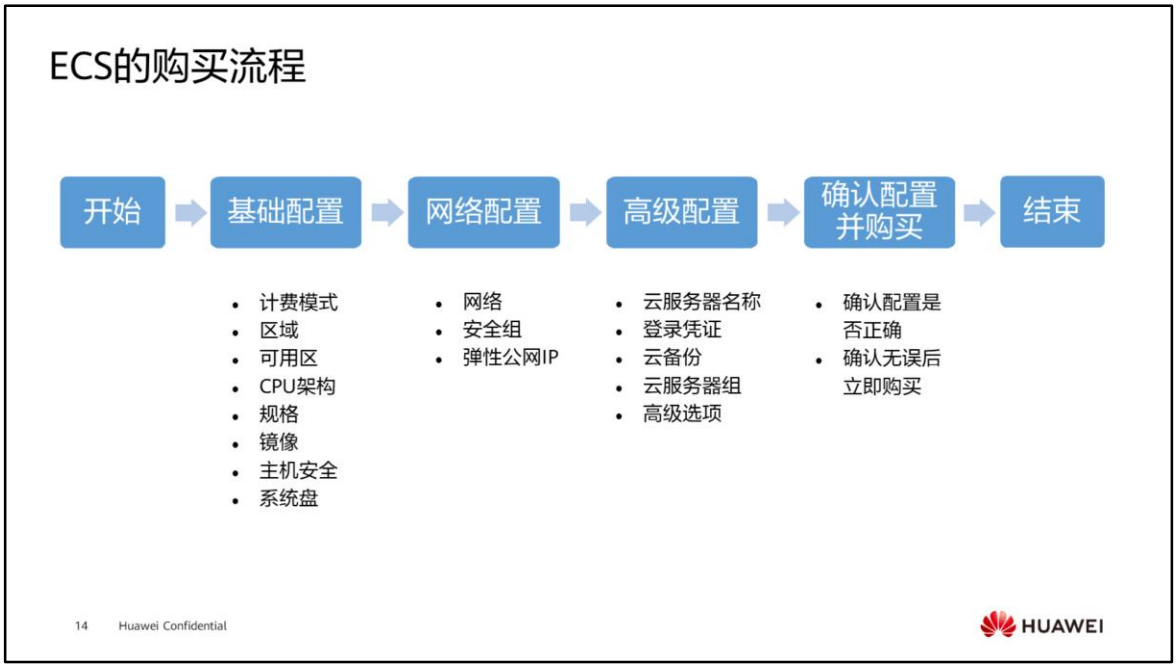
- 高性能计算型弹性云服务器

推荐原因

- 使用高性能计算型弹性云服务器，主要使用在受计算限制的高性能处理器的应用程序上，适合要求提供海量并行计算资源、高性能的基础设施服务，需要达到高性能计算和海量存储，对渲染的效率有一定保障的场景

HUAWEI

- 高性能计算型实例每一个vCPU都对应一个英特尔® 至强® 可扩展处理器核心的超线程，主要适用于高性能计算业务场景，能够提供海量并行计算资源和高性能的基础设施服务，达到高性能计算和海量存储的要求，保障渲染效率。



- 选择“计费模式”——“包年/包月”或“按需付费”：
  - 包年/包月：用户选购完云服务器配置后，可以根据需要设置购买时长，系统会一次性按照购买价格对账户余额进行扣费
  - 按需付费：用户选购完云服务器配置后，无需设置购买时长，系统会根据消费时长对账户余额进行扣费
- 选择“规格”：公有云提供了多种类型的弹性云服务器供用户选择，针对不同的应用场景，可以选择不同规格的弹性云服务器。可以在列表中查看已上线的弹性云服务器类型与规格，或输入规格名称（如c3），或根据vCPU、内存大小搜索目标规格。
- 设置“网络”：在下拉列表中选择可用的虚拟私有云、子网，并设置私有IP地址的分配方式。弹性云服务器网络使用虚拟私有云（VPC）提供的网络，包括子网、安全组等。用户可以选择使用已有的虚拟私有云网络，或者创建新的虚拟私有云。
- 设置“弹性公网IP”：弹性公网IP是指将公网IP地址和路由网络中关联的弹性云服务器绑定，以实现虚拟私有云内的弹性云服务器通过固定的公网IP地址对外提供访问服务。
- 设置“登录凭证”：“密钥对”方式创建的弹性云服务器安全性更高，建议选择“密钥对”方式。

ECS的基础配置

- ECS的基础配置包含计费模式，区域和可用区，CPU架构，规格/镜像。

- ECS的基础配置包含：
  - 计费模式：提供按需、包周期（按月、按年）、竞价共3种计费方式，使用越久越便宜。
  - 区域和可用区：不同区域的云服务产品之间内网互不相通。请就近选择靠近业务的区域，可减少网络时延，提高访问速度。
  - CPU架构：X86 CPU架构采用复杂指令集（CISC）；鲲鹏CPU架构采用精简指令集（RISC）。
  - 规格/镜像：针对不同的应用场景，选择不同规格、不同镜像的弹性云服务器。
- 规格选型：
  - 通用计算增强型：适用于对自主研发、安全隐私要求较高的政企金融场景，对网络性能要求较高的互联网场景，对核数要求较多的大数据、HPC场景，对成本比较敏感的建站、电商等场景。
  - 内存优化型：适用于大数据分析，如广告精准营销、电商、车联网等大数据分析场景。
  - 超高I/O型：适用于高性能关系型数据库，NoSQL数据库（Cassandra、MongoDB等）以及ElasticSearch搜索等场景。
  - GPU加速型：适用于高实时、高并发的海量计算场景。
  - FPGA加速型：适用于视频处理、机器学习、基因组学研究、金融风险分析等场景。
  - AI加速型：适用于机器视觉、语音识别、自然语言处理通用技术，支撑智能零售、智能园区、机器人云大脑、平安城市等场景。

ECS的网络配置

- ECS网络使用VPC提供的网络，包括子网、安全组等。

HUAWEI

- ECS的网络配置包含：
  - 子网：子网是用来管理弹性云服务器网络平面的一个网络，可以提供IP地址管理、DNS服务，子网内的弹性云服务器IP地址都属于该子网。
  - 安全组：安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的弹性云服务器提供访问策略。用于加强弹性云服务器的安全保护。
  - 添加扩展网卡：可选配置。

ECS的高级配置

- ECS的高级配置包含云服务器名称、登录凭证、云备份、云服务器组和高级选项。

- ECS的高级配置包含：
  - 云服务器名称：名称可自定义，但需符合命名规则，如果同时购买多台弹性云服务器，系统会自动按序增加后缀。
  - 登录凭证：“密钥对” 指使用密钥作为弹性云服务器的鉴权方式；“密码” 指使用设置初始密码作为弹性云服务器的鉴权方式。Linux操作系统为root用户的初始密码，Windows操作系统为Administrator用户的初始密码。
  - 云备份：云备份提供对云硬盘和弹性云服务器的备份保护，并支持利用备份数据恢复云服务器和云硬盘的数据。
  - 云服务器组：设置云服务器组，可选配置，云服务器组内的弹性云服务器将遵循反亲和策略，尽量分散地创建在不同主机上。
  - 高级选项：高级配置，可选配置等。

ECS的访问方式

- 公有云提供了Web化的服务管理平台，即管理控制台和基于HTTPS请求的REST API管理方式。

API 方式

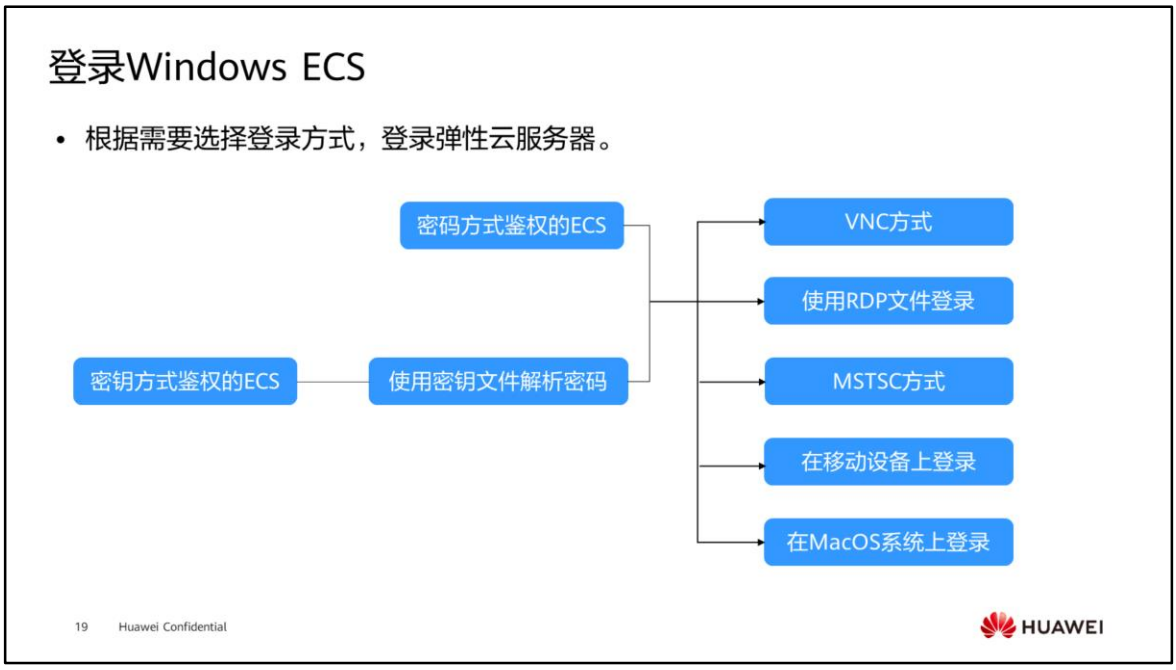
如果用户需要将公有云平台上的弹性云服务器集成到第三方系统，用于二次开发，请使用API方式访问弹性云服务器。

控制台方式

如果用户已注册公有云，可直接登录管理控制台，从主页选择“弹性云服务器”。

HUAWEI

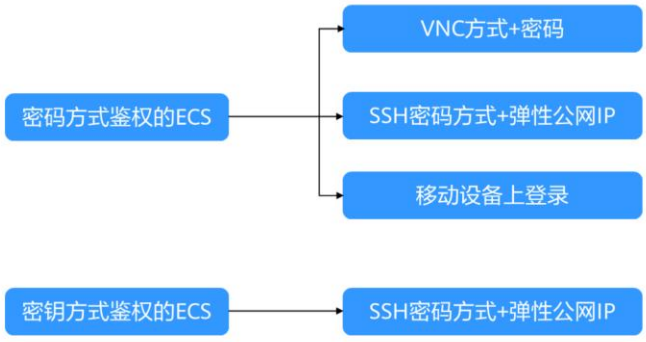
- ECS也支持SDK对接的管理方式，用户也可以通过SDK的管理方式来访问ECS。



- 根据需要选择登录方式，登录弹性云服务器：
  - 在用户个人便携设备上，通过管理控制台远程登录（VNC方式）：登录用户名“Administrator”
  - 在用户个人便携设备上，使用管理控制台提供的RDP文件登录Windows云服务器：登录用户名为“Administrator”，且弹性云服务器必须绑定弹性公网IP
  - 在用户个人便携设备上，通过远程桌面连接（MSTSC方式）：登录用户名为“Administrator”，且弹性云服务器必须绑定弹性公网IP
  - 在用户移动设备上登录Windows云服务器：登录用户名为“Administrator”，且弹性云服务器必须绑定弹性公网IP
  - 在Mac OS系统上登录Windows云服务器：登录用户名为“Administrator”，且弹性云服务器必须绑定弹性公网IP
- 更多关于Windows弹性云服务器的登录方式，请参见：https://support.huaweicloud.com/usermanual-ecs/zh-cn_topic_0092494943.html。

登录Linux ECS

- 购买弹性云服务器时设置的登录鉴权方式不同，登录弹性云服务器的方法也存在差异。



HUAWEI

- 首次登录密码方式鉴权的弹性云服务器时，可以使用以下方法登录弹性云服务器：
  - 管理控制台远程登录（VNC方式），登录用户名为“root”
  - SSH密码方式，登录用户名为“root”，且弹性云服务器必须绑定弹性公网IP
  - 在移动设备上登录Linux云服务器，登录用户名为“root”，且弹性云服务器必须绑定弹性公网IP

ECS的使用 - 重装/切换操作系统

- 操作场景：弹性云服务器操作系统无法正常启动或云服务器系统运行正常，但需要对系统进行优化，使其在最优状态下工作时，用户可以使用重装或切换操作系统的功能。

说明：

- 重装操作系统只支持使用原镜像进行系统重装，不支持使用新的系统镜像；
- 切换操作系统是为您的弹性云服务器重新切换一个系统盘。切换完成后弹性云服务器的系统盘ID会发生改变，并删除原有系统盘。

HUAWEI

- 操作步骤：
  - 登录管理控制台
  - 单击管理控制台左上角的图标，选择区域和项目
  - 选择“计算 > 弹性云服务器”
  - 在待重装操作系统的弹性云服务器的“操作”列下，单击“更多 > 镜像/磁盘 > 重装操作系统”，重装操作系统前请先将云服务器关机，或根据页面提示勾选“系统自动关机后重装操作系统”
  - 设置登录方式，如果待重装操作系统的弹性云服务器是使用密钥登录方式创建的，此时可以更换使用新密钥

ECS的使用 - 变更规格

- 当用户购买的弹性云服务器规格无法满足业务需要时，可以随时变更弹性云服务器的规格，升级vCPU、内存。
- 说明：
  - “包年/包月”计费模式的弹性云服务器，选择要变更的目标云服务器规格后，需补齐差价（多退少补），重启弹性云服务器即可变更成功。
  - “按需计费”模式的弹性云服务器变更规格时不需要补齐差额。

ECS的使用 - 重置密码

- 使用场景：ECS密码丢失、密码过期。
- 前提条件：ECS已提前安装一键式重置密码插件。
- 说明：使用公共镜像的云服务器，默认已安装一键式重置密码插件。

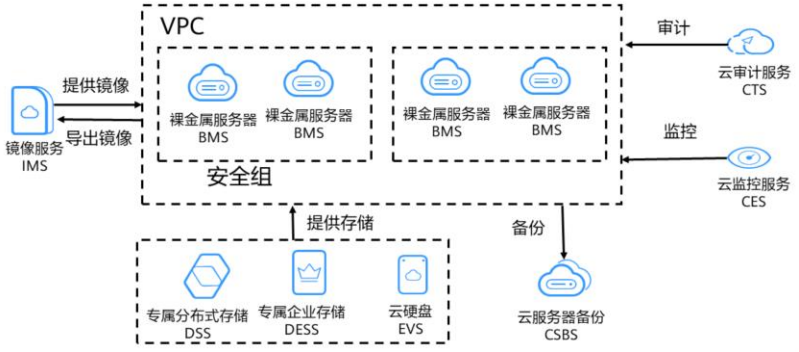
HUAWEI

- 插件名称：CloudResetPwdAgent和CloudResetPwdUpdateAgent。
- 一键式重置密码插件安装成功后，请勿删除重置密码进程CloudResetPwdAgent和CloudResetPwdUpdateAgent，否则，会导致一键式重装密码功能不可用。

目录

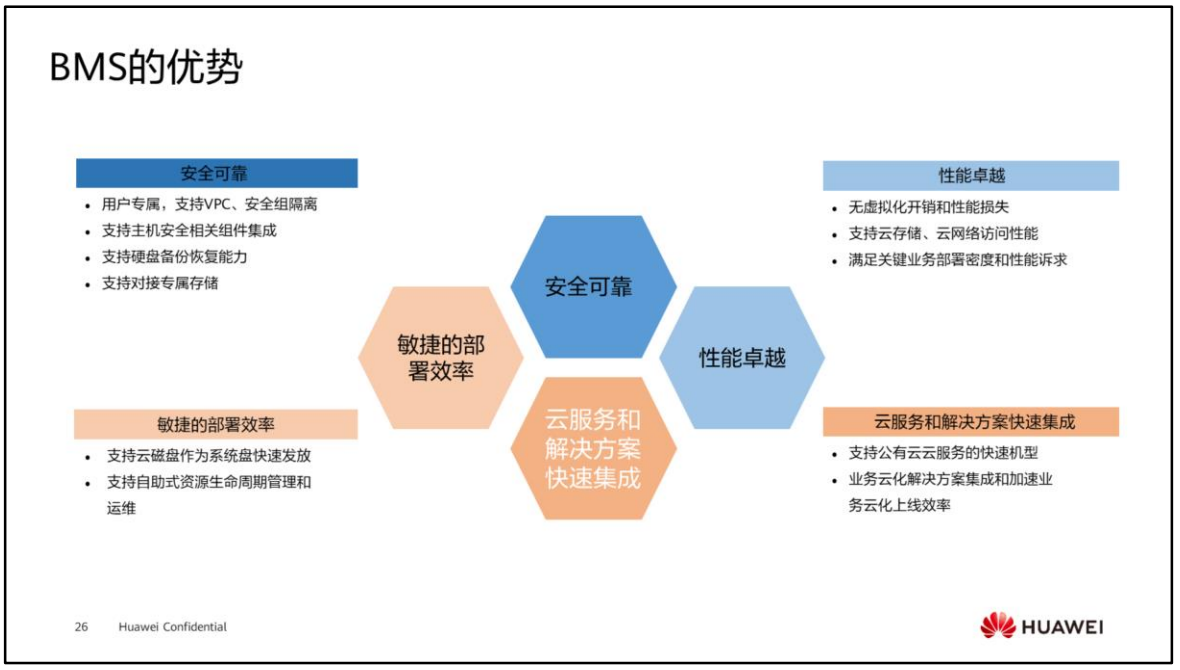
什么是裸金属服务器（BMS）

- 裸金属服务器（Bare Metal Server，BMS）是一款兼具虚拟机弹性和物理机性能的计算类服务，为用户以及相关企业提供专属的云上物理服务器，为核心数据库、关键应用系统、高性能计算、大数据等业务提供卓越的计算性能以及数据安全。用户可灵活申请，按需使用。



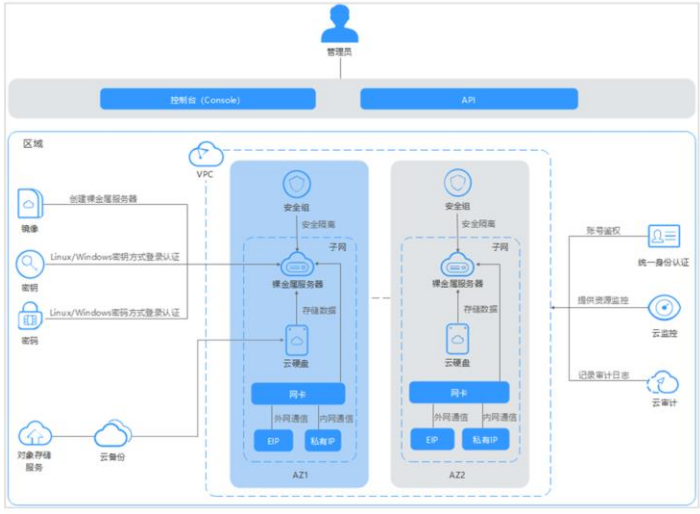
HUAWEI

- 裸金属服务器BMS和传统物理机本质上都是一台物理设备，但是它们最大的区别是裸金属服务器BMS能够将物理机接入到云平台，从而实现自动化配置和自服务化购买。而传统物理机只能人工手动配置和走线下采购。
- 裸金属服务器BMS，让传统物理机具有了自动发放、自动运维、VPC互联、支撑对接共享存储等云的能力。BMS可以像虚拟机一样灵活地发放和使用，同时又具备了优秀的计算、存储、网络能力。



- BMS的优势：
  - 安全可靠：裸金属服务器是用户专属的计算资源，支持VPC、安全组隔离；支持主机安全相关组件集成；基于擎天架构的裸金属服务器支持云磁盘作为系统盘和数据盘，支持硬盘备份恢复能力；支持对接专属存储，满足企业数据安全和监管的业务安全和可靠性诉求
  - 性能卓越：裸金属服务器继承物理服务器特征，无虚拟化开销和性能损失，100%释放算力资源。结合华为自研擎天软硬协同架构，支持高带宽、低时延云存储、云网络访问性能；满足企业数据库、大数据、容器、HPC、AI等关键业务部署密度和性能诉求
  - 敏捷的部署效率：裸金属服务器基于擎天加速硬件，支持云磁盘作为系统盘快速发放；分钟级资源发放，基于统一console控制台、开放API和SDK，支持自助式资源生命周期管理和运维
  - 云服务和解决方案快速集成：裸金属服务器基于统一的VPC模型，支持公有云云服务的快速机型；帮助企业客户实现数据库、大数据、容器、HPC、AI等关键业务云化解决方案集成和加速业务云化上线效率

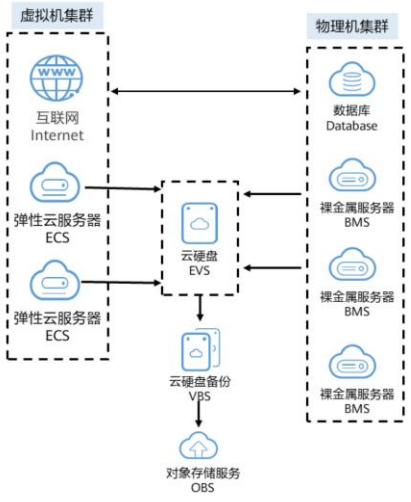
BMS的产品架构



HUAWEI

- 通过和其他服务组合，裸金属服务器可以实现计算、存储、网络、镜像安装等功能：
  - 裸金属服务器在不同可用区中部署（可用区之间通过内网连接），部分可用区发生故障后不会影响同一区域内的其他可用区。
  - 可以通过虚拟私有云建立专属的网络环境，设置子网、安全组，并通过弹性公网IP实现外网链接（需带宽支持）。
  - 通过镜像服务，可以对裸金属服务器安装镜像，也可以通过私有镜像批量创建裸金属服务器，实现快速的业务部署。
  - 通过云硬盘服务实现数据存储，并通过云硬盘备份服务实现数据的备份和恢复。
  - 云监控是保持裸金属服务器可靠性、可用性和性能的重要部分，通过云监控，用户可以观察裸金属服务器资源。
  - 云备份提供对云硬盘和裸金属服务器的备份保护服务，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。

应用场景 - 核心数据库



适用场景

- 核心数据库场景。满足核心数据库对性能和安全有较高的要求，华为云BMS提供多种规格的服务器，并支持自动化挂载共享云硬盘。

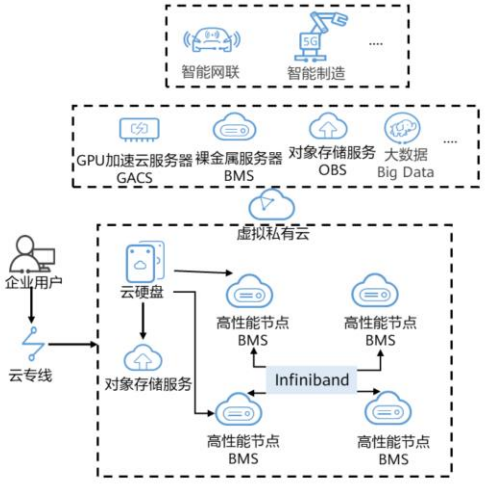
推荐原因

- 某些关键的数据库业务不能部署在虚拟机上，必须通过资源专享、网络隔离、性能有保障的物理服务器承载。
- 裸金属服务器为用户提供独享的高性能物理服务器，可以满足此种场景下的业务需求。

HUAWEI

- 安全高效：独享物理服务器，提供超高计算性能，无虚拟化性能损失，同时提供三副本备份，保障数据安全可靠。
- 快速发放：在管理控制台自助申请，无需人工介入，只需数分钟即可获得一台物理服务器；同时实现自动化镜像安装、网络配置、云硬盘挂载功能。
- 支持RAC模式：自动化挂载共享云硬盘，解决了传统物理服务器受限于本地硬盘容量的问题，满足企业核心系统集群部署数据库RAC模式的需求。
- 灵活部署：弹性云服务器互联，物理服务器通过VPC与外部资源互通，与弹性云服务器混合部署、灵活组网，同时支持弹性IP，满足多种复杂场景的组网诉求。

应用场景 - 高性能计算



适用场景

- 超算中心、基因测序等场景。针对高计算，高吞吐的场景特点，BMS支持最新CPU的计算实例，结合100 GB网络，带来低时延的性能体验。

推荐原因

- 超算中心、基因测序等高性能计算场景，处理的数据量大，对服务器的计算性能、稳定性、实时性等要求很高。
- 低时延：100 GB网络自动化、安全隔离，微秒级时延。
- 高性能：支持Intel最新CPU，性能强劲。
- 易扩展：支持开放API，便于生态集成。

HUAWEI

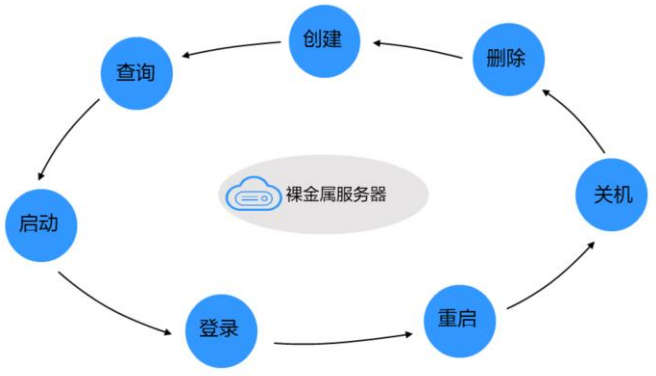
- 高性能弹性云服务器：提供C6（通用计算增强型）、M6（内存优化型）等计算密集型ECS实例，搭载第二代英特尔® 至强® 可扩展处理器 ，多项技术优化，计算性能强劲稳定，配套华为自研智能高速网卡，提供超高带宽和超低时延的网络体验。
- 卓越性能的裸金属服务器：提供H2高性能裸金属服务器，配置100 GB EDR Infiniband网络，按照专属物理服务器方式提供卓越的计算性能，无虚拟化损耗，具备良好的性能优势，用户可通过管理控制台实现裸金属服务器的自动化发放，满足HPC业务按需灵活弹性的需求。
- 卓越的网络性能：为HPC用户在公有云上构建安全隔离的虚拟网络环境，HPC计算网络通过智能高速网卡或专线互连，为用户提供高带宽的网络环境。

BMS vs ECS vs 物理服务器

对比维度	BMS	ECS	物理机
物理资源	用户独享	用户共享	用户独享
使用场景	关键类应用或性能要求较高的业务	通用型、特定业务	传统业务
使用方式	灵活	灵活	固化
高级能力	自动发放、自动运维、VPC互联、支撑对接共享存储等	自动发放、自动运维、VPC互联、支撑对接共享存储等	传统能力

- 缺少灵活性，是传统物理机的最大弊端。尽管云计算发展如火如荼，但有些企业为追求极致的性能，仍然可能选择使用笨重的物理机。他们选择的唯一理由是相对虚拟机而言，物理机没有虚拟化损耗，性能更强大。
- 但在实际部署过程中，周期长、运维复杂、架构僵化等弊端一一凸显。一些云上物理机运维交付都涉及大量人工操作，费事费时，人工成本极高，无法自动化运维，而一旦物理机出现宕机，那就可能导致“灾难性”的损失。
- 如果转身选用虚拟机，又考虑到性能不能完全满足企业核心数据库的业务要求而望而却步。企业原有的核心应用不想基于虚拟机进行过多的调整，同时对于性能、稳定性又有较高要求，以至于用户进入两难境地，物理机缺少灵活，虚拟机又无法满足性能。
- 而此时，弹性裸金属服务器应势而生。裸金属服务器用户独享物理资源，而虚拟机环境由多个租户共享物理资源。对于关键类应用或对性能要求较高的业务以及对安全性的要求，裸金属服务器具备物理机级别的性能和隔离性，是这类企业的不二之选。
- 相较物理机而言，裸金属服务器让传统物理机具有了在线交付、自动化无人运维、VPC互联、支撑对接共享存储等云的能力。用户可以像管理虚拟机一样灵活使用，同时又具备了优秀的计算、存储、网络能力。
- 裸金属服务器产品解决了由于公有云虚拟云主机架构限制所不能实现的一些功能部署问题，例如，虚拟化业务、高性能计算业务、对IO性能有极高要求的业务，以及对核心数据要求高度掌控、安全隔离的业务。另外，提供裸金属服务的厂商也会提供运维服务，响应速度也很快，这样节省了您自有运维人员的成本支出。

裸金属服务器管理



自助申请，意见Console操作，分钟级发放，服务器全生命周期管理。

HUAWEI

- BMS的创建方式有如下几种，此课程以创建裸金属服务器为例：
  - 创建裸金属服务器
  - 创建快速发放型裸金属服务器
  - 创建专属裸金属服务器
  - 通过私有镜像创建裸金属服务器

创建裸金属服务器 - 基础配置

- BMS的基础配置包含、区域、可用区、规格和镜像。

HUAWEI

- BMS的基础配置包含：
  - 区域、可用区：不同区域的云服务产品之间内网互不相通。就近选择靠近业务的区域，可减少网络时延，提高访问速度。
  - 规格/镜像：针对不同的应用场景，选择不同规格、不同镜像的裸金属云服务器。

创建裸金属服务器 - 网络配置

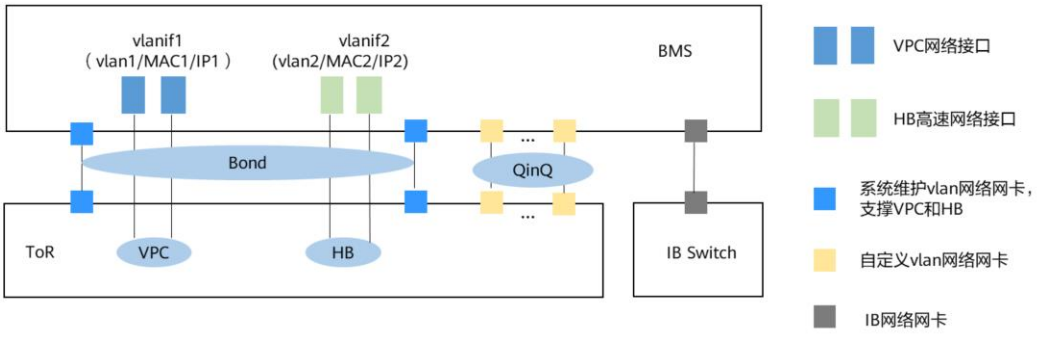
- BMS的网络配置包含VPC、网卡、增强高速网卡、安全组和弹性公网IP。

HUAWEI

- 第一次使用云服务时，系统将自动创建一个默认的虚拟私有云，包括安全组、网卡，并为子网开启DHCP功能。
- 安全组用来实现安全组内和安全组间裸金属服务器的访问控制，加强裸金属服务器的安全保护。用户可以在安全组中定义各种访问规则，当裸金属服务器加入该安全组后，即受到这些访问规则的保护。
- 创建裸金属服务器时，仅支持选择一个安全组。但是裸金属服务器创建成功后，可以为裸金属服务器关联多个安全组。

BMS的网络

- 裸金属服务有五种网络类型，分别是虚拟私有云、高速网络、增强高速网络、自定义VLAN网络和IB网络，五种网络之间相互隔离不互通。

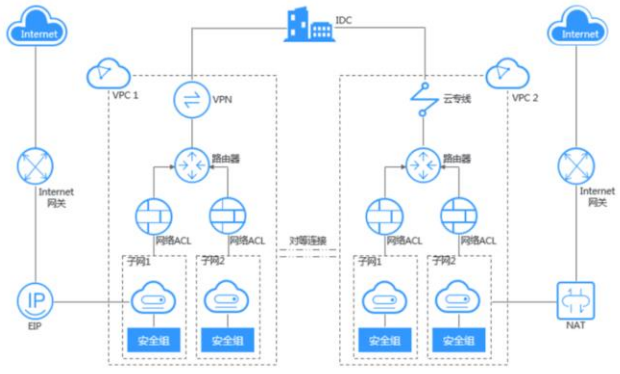


HUAWEI

- 图中的ToR表示服务器机柜的布线方式，接入交换机放在机架顶部，服务器放在下方。HB表示高速网络。QinQ表示802.1Q隧道。
- VPC网络接口和HB高速网络接口由系统生成，租户不可修改。这两个网络接口属于同一个网卡Bond。
- 弹性云服务器和裸金属服务器之间可以通过虚拟私有云通信，也可以通过IB网络通信（如果存在）。
- 只有虚拟私有云支持安全组、弹性公网IP和弹性负载均衡能力。
- 对于高速网络和自定义VLAN网络，同一网络中的裸金属服务器实例之间仅提供L2连接。

BMS网络 - 虚拟私有云

- 虚拟私有云（Virtual Private Cloud，VPC），为裸金属服务器构建隔离的、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。

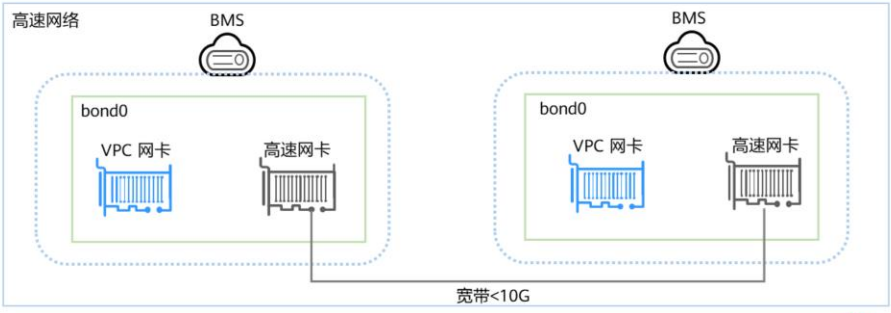


HUAWEI

- VPC部署优势：
  - 灵活配置：用户可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性。
  - 安全可靠：VPC之间通过隧道技术进行100%逻辑隔离，不同VPC之间默认不能通信。网络ACL对子网进行防护，安全组对弹性云服务器进行防护
  - 互联互通：默认情况下，VPC与公网是不能通信访问的，依靠了弹性公网IP、弹性负载均衡、NAT网关、虚拟专用网络、云专线等多种方式连接公网。默认情况下，两个VPC之间也是不能通信访问的，依靠对等连接的方式，使用私有IP地址在两个VPC之间进行通信
  - 高速访问：使用全动态BGP协议接入多个运营商，支持20多条线路。可以根据设定的寻路协议实时自动故障切换，保证网络稳定，网络时延低，云上业务访问更流畅

BMS网络 - 高速网络

- 属于裸金属服务器的内部网络，为同一可用区内的裸金属服务器之间提供带宽不受限制的网络。如果用户需要部署高吞吐量或要求低时延的服务，可以创建高速网络。
- 高速网络与VPC共享一个物理平面。高速网络只有东西流量，没有三层路由功能，用于节点间内部二层通信。

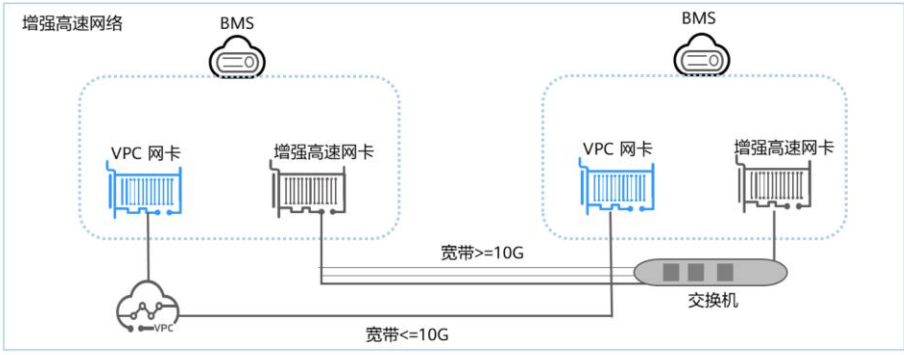


HUAWEI

- 高速网络使用限制：
  - 创建裸金属服务器时，普通网卡子网的网段与高速网络的网段不能存在交集。
  - 高速网络不支持安全组、EIP、DNS、VPN、专线等功能。
  - 同一裸金属服务器的多个高速网卡，其所在的高速网络不能重复。
  - 裸金属服务器下发成功后不能再配置高速网络。

BMS网络 - 增强高速网络

- 增强高速网络通过云数据中心实现内网互通互连，可以提供高质量、高速度、低时延的内网环境。

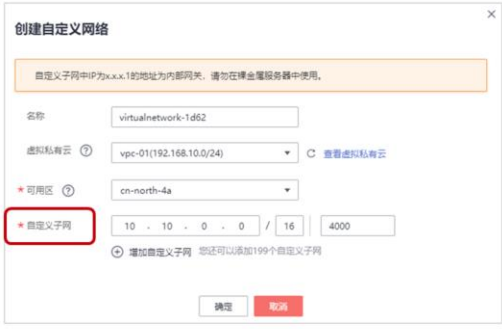


HUAWEI

- 增强高速网络基于上一代高速网络进行了软硬件的优化升级，使租户的裸金属服务器可以跨POD互通。相比上一代高速网络，增强高速网络具有如下三大优势：
  - 带宽提升至10 GE及以上；
  - 租户自定义网络平面数量，最多支持4 K个子网；
  - 支持裸金属服务器虚拟化访问外网。

BMS网络 - 自定义VLAN网络

- 用户能够自由划分所需的VLAN子网来分隔流量，适用于SAP HANA、虚拟化等场景。自定义VLAN网络的网卡是成对出现的，用户可以通过配置bond实现高可用。

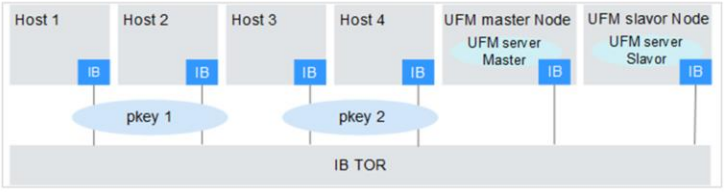


HUAWEI

- 自定义VLAN网络当前不支持跨AZ互通。

BMS网络 - IB网络

- IB网络因其低延迟、高带宽的网络特性被用于很多高性能计算（High Performance Computing，HPC）项目。在BMS场景，IB网络支持RDMA和IPoIB通信。
- 裸金属服务器IB网络的发放是通过在创建BMS时选择支持IB网络的flavor实现的，即可动态创建IB网络。



HUAWEI

- IB网络发放完成后，即可在裸金属服务器上通过RDMA方式实现高速通信。在IPoIB通信模式下，需要在IB网口上配置IP地址，有静态配置和DHCP动态分配两种方式。
- InfiniBand技术不是用于一般网络连接的，它的主要设计目的针对服务器端的连接问题。被应用于服务器与服务器（比如复制、分布式工作等）、服务器和存储设备（比如SAN和直接存储附件）以及服务器和网络之间（比如LAN、 WANs和the Internet）的通信。
- InfiniBand的特点:
  - 基于标准协议
  - 高带宽，低时延
  - 远程直接内存存取功能
  - 传输卸载

创建裸金属服务器 - 高级配置

- BMS的高级配置包含裸金属服务名称，登录凭证和高级配置。

HUAWEI

- 登录凭证可选择“密钥对”或“密码”，如果用户使用的是Linux裸金属服务器，建议使用密钥对（Key Pair）进行远程登录身份验证。用户可以新建一个密钥对，并下载私钥，私钥用于远程登录身份认证，为保证裸金属服务器安全，私钥只能下载一次，请妥善保管。也可以把已有密钥对（Key Pair）的公钥导入系统，使用对应的私钥进行远程登录身份验证。

BMS的使用 - 重装操作系统

- 裸金属服务器操作系统无法正常启动，操作系统中毒或裸金属服务器系统运行正常，但需要对系统进行优化，使其在最优状态下工作时，用户可以使用重装裸金属服务器的操作系统功能。

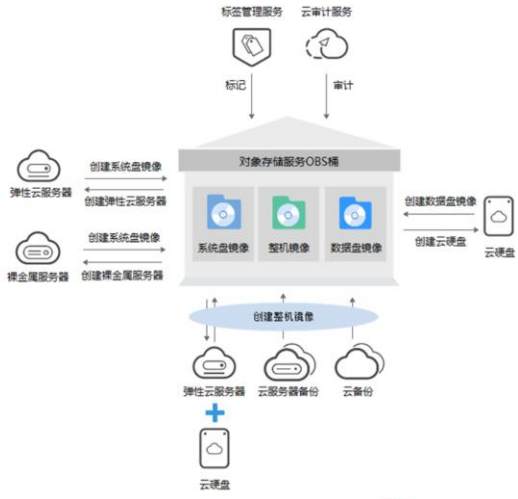
HUAWEI

- 重装操作系统注意事项：
  - 重装操作系统需要停止裸金属服务器，因此会中断业务。
  - 重装操作系统会清除系统盘数据，包括系统盘上的系统分区和所有其他分区，需要做好数据备份。
  - 重装过程中禁止对裸金属服务器进行关机或重启等操作，否则可能重装失败。
  - 重装系统后，当前操作系统内的个性化设置（如DNS、主机名等）将被重置，需重新配置。

目录

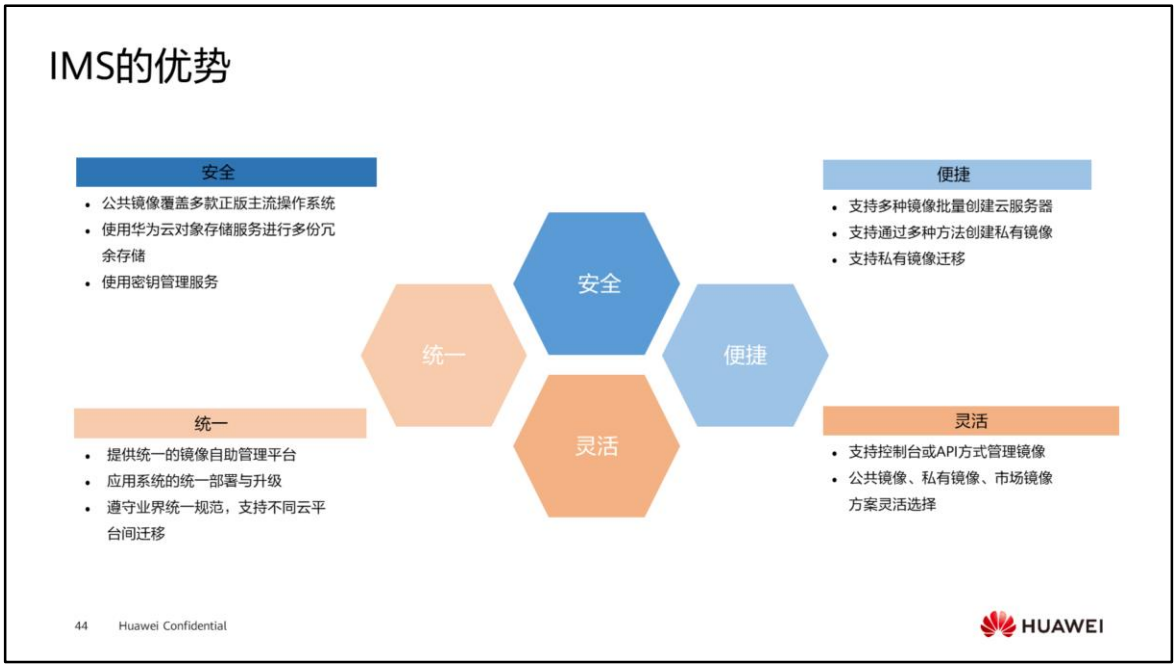
什么是镜像服务（IMS）

- 镜像服务（Image Management Service，IMS）提供镜像的生命周期管理能力。用户可以灵活地使用公共镜像、私有镜像或共享镜像申请弹性云服务器和裸金属服务器。同时，用户还能通过已有的云服务器或使用外部镜像文件创建私有镜像，实现业务上云或云上迁移。



HUAWEI

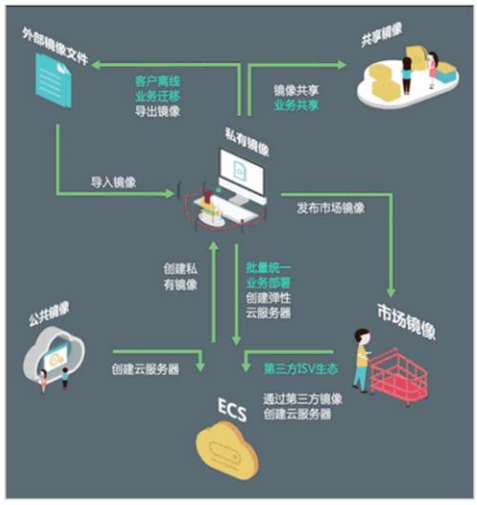
- 镜像是一个包含了软件及必要配置的服务器或磁盘模版，包含操作系统或业务数据，还可以包含应用软件（例如，数据库软件）和私有软件。镜像分为公共镜像、私有镜像、共享镜像、市场镜像。



- 便捷：通过弹性云服务器和外部镜像文件均可创建私有镜像；支持通过镜像批量创建云服务器。
- 灵活：通过管理控制台或API方式均能完成镜像的生命周期管理，用户可以按照需求灵活选择。
- 统一：镜像服务提供统一的镜像自助管理平台，简化维护的复杂度。
- 安全：公共镜像覆盖多款主流操作系统，皆以正版授权，均经过严格测试，能够保证镜像安全、稳定。

IMS的产品类型

- 公共镜像：所有用户可见，包括操作系统以及预装的公共应用。
- 私有镜像：用户基于弹性云服务器创建的个人镜像，仅用户自己可见。
- 共享镜像：接受其他用户共享的私有镜像，作为自己的镜像进行使用。
- 市场镜像：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。



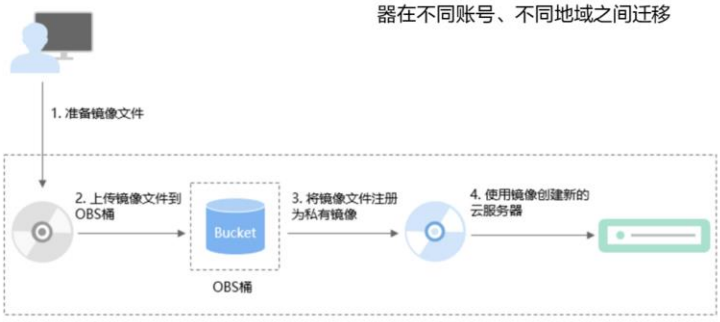
HUAWEI

- 公共镜像：包含常见的标准操作系统镜像，所有用户可见，包括操作系统以及预装的公共应用。请根据用户的实际情况自助配置应用环境或相关软件。官方公共镜像支持的操作系统类型包括：Windows，CentOS，Debian，openSUSE，Fedora，Ubuntu，EulerOS，CoreOS。选择部分操作系统的公共镜像时，系统推荐配套使用公有云提供的企业主机安全服务（Host Security Service，HSS）。企业主机安全提供双因子认证登录，帐户破解防护、弱口令检测等功能，保护云服务器免遭暴力破解攻击。
- 私有镜像：包含操作系统或业务数据、预装的公共应用以及用户的私有应用的镜像，仅用户个人可见。私有镜像包含：
  - 系统盘镜像：包含用户运行业务所需的操作系统、应用软件的镜像。系统镜像可以用于创建云服务器，迁移用户业务到云。
  - 数据盘镜像：只包含用户业务数据的镜像。数据镜像可以用于创建云硬盘，将用户的业务数据迁移到云上。
  - 整机镜像：包含用户运行业务所需的操作系统、应用软件和业务数据的镜像。
- 共享镜像：用户将接受云平台其他用户共享的私有镜像，作为自己的镜像进行使用。
- 市场镜像：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。无需配置，可一键部署，满足建站、应用开发、可视化管理等个性化需求。市场镜像通常由具有丰富云服务器维护和配置经验的服务商提供，并且经过华为云的严格测试和审核，可保证镜像的安全性。

应用场景 - 服务器上云或云上迁移

推荐原因

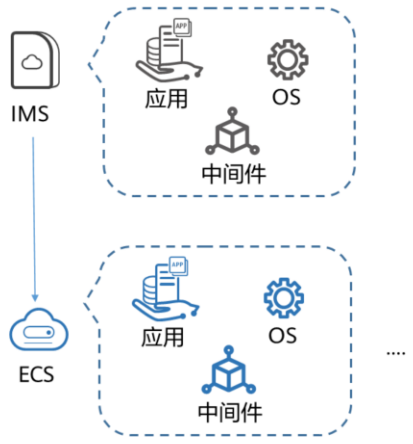
- 利用镜像导入功能，将已有的业务服务器制作成镜像后导入到云平台，方便企业业务上云。使用镜像共享和镜像跨区域复制功能，实现云服务器在不同账号、不同地域之间迁移



HUAWEI

- 华为云支持导入VMDK、VHD、QCOW2、RAW、VHDX、QED、VDI、QCOW、ZVHD2和ZVHD格式的镜像文件。其他镜像文件，需要转换格式后再导入。用户可以使用开源qemu-img工具或自研qemu-img-hw工具转换镜像格式。

应用场景 - 部署特定软件环境



适用场景

- 部署特定软件环境

推荐原因

- 使用共享镜像或者应用超市的市场镜像均可帮助企业快速搭建特定的软件环境，免去了自行配置环境、安装软件等耗时费力的工作，特别适合互联网初创型公司使用

HUAWEI

- 传统的批量业务部署需要经历评估业务场景，选择合适的操作系统、数据库、应用软件等，并且需要安装和调试，其复杂度较高，也依赖开发或运维人员的水平。
- 而如果使用私有镜像、应用超市的市场镜像，或者根据已使用过的方案均可快速创建符合要求的云服务器。除共享镜像需要用户自行甄别来源以外，公共镜像、私有镜像，及市场镜像均经过严格测试，能够保证镜像安全、稳定。

应用场景 - 服务器运行环境备份

适用场景

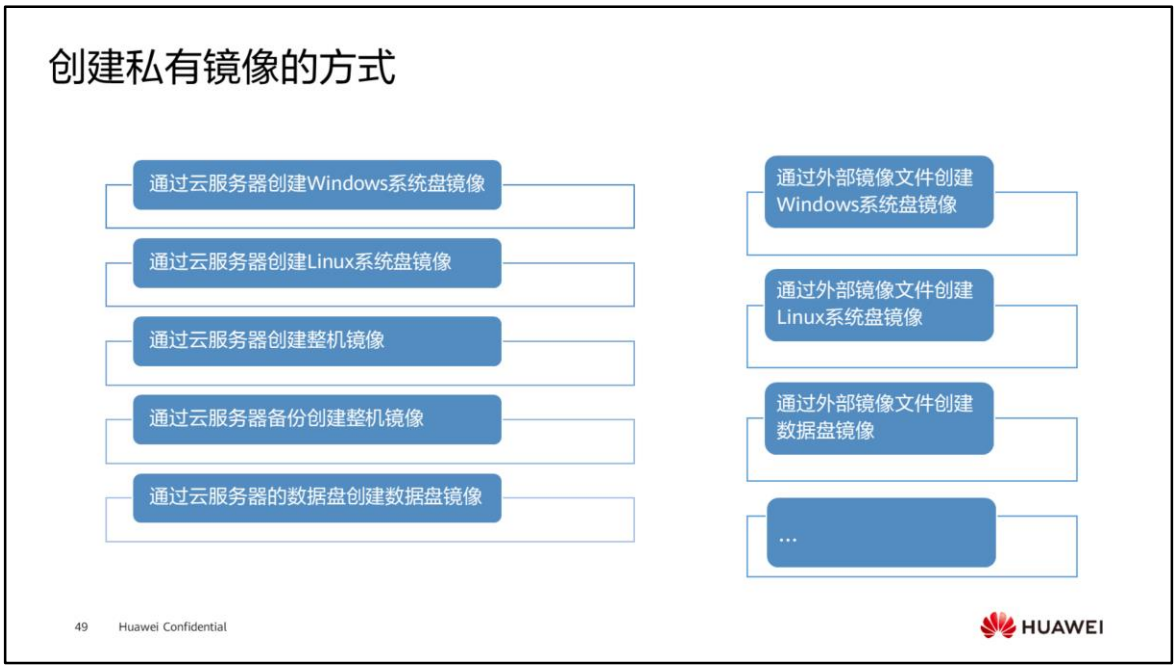
- 服务器运行环境备份

推荐原因

- 对一台云服务器实例制作镜像以备份环境。当该实例的软件环境出现故障而无法正常运行时，可以使用镜像进行恢复

HUAWEI

- 该场景类似我们以前个人电脑做GHOST系统还原点，假如出现病毒感染、系统奔溃等情况，可以恢复到曾经的还原点。
- 在公有云上，我们可以利用私有镜像功能对服务器的状态进行备份。但需要手工备份，如果需要定期执行备份，则推荐云主机备份/云硬盘备份等专业备份产品。



- 创建私有镜像的方式常用的包括2大类：通过云服务器和通过外部镜像文件。如果已有外部镜像文件，可以通过外部镜像文件的方式来创建私有镜像。如果想要通过已有的云服务器来创建镜像，可以选择通过云服务器的方式来创建私有镜像。
- 除了通过云服务器和外部镜像文件创建私有镜像外，还有些其他的创建镜像的方式：
  - 通过ISO文件创建Windows或Linux系统盘镜像；
  - 通过云备份创建整机镜像；
  - 通过裸金属服务器创建裸金属服务器系统盘镜像。

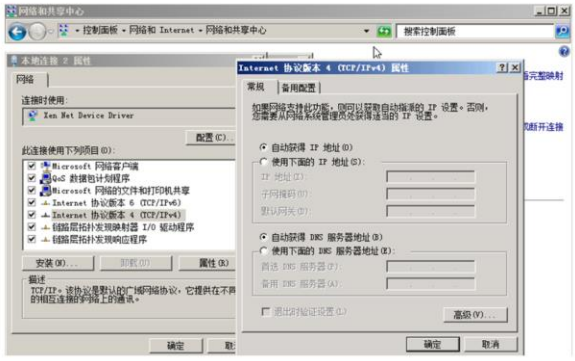
通过云服务器创建Windows系统盘镜像

HUAWEI

- 此课程以通过云服务器创建Windows系统盘镜像为例。

配置Windows云服务器

- 首先我们要准备一台Windows云服务器，检查该云服务器的网卡属性是否为修改为DHCP方式。

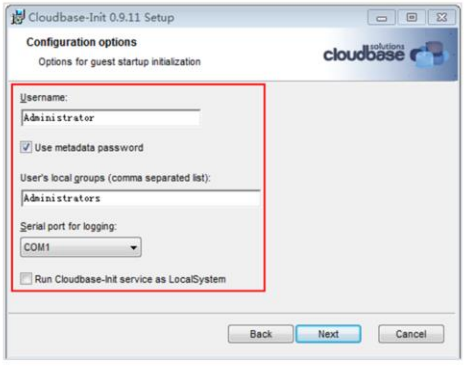


HUAWEI

- 如果创建Windows私有镜像所使用的云服务器网络配置是静态IP地址，用户需要登录Windows云服务器，将该云服务器的网卡属性修改为DHCP方式，再创建私有镜像。具体操作如下：
  - 登录Windows云服务器，“开始 > 控制面板 >网络和Internet >本地连接 >属性 >常规”。
  - 在“常规”页签中勾选“自动获得IP地址”和“自动获得DNS服务地址”，单击“确定”。

安装初始化工具

- 为了保证使用私有镜像创建的新云服务器可以自定义配置，建议用户在创建私有镜像前安装Cloud-init/Cloudbase-init工具。



HUAWEI

- Cloud-init/Cloudbase-init是云初始化程序，能够对新创建弹性云服务器中指定的自定义信息（主机名、密钥和用户数据等）进行初始化配置。如果是Windows操作系统，需下载并安装Cloudbase-init。如果是Linux操作系统，需下载并安装Cloud-init。因为需要从官网下载并安装，因此，需提前给云服务器配置弹性IP。

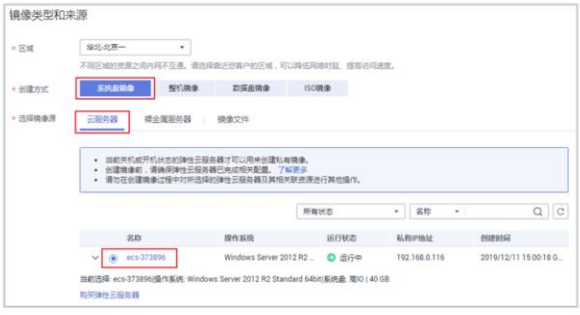
优化镜像（Windows）

- 云服务器的正常运行依赖于虚拟化的驱动程序，为了同时支持XEN虚拟化和KVM虚拟化，需要确保镜像安装了PV driver和UVP VMTools。

- XEN和KVM都是两种开源的虚拟化技术。而PV driver和UVP VMTools就是这两种虚拟化各自的驱动程序。

创建Windows系统盘镜像

- 在“镜像服务”列表页面，单击“创建私有镜像”。
- 在“镜像类型和来源”页面，选择镜像的创建方式为“系统盘镜像”。
- 镜像的源默认选择为“云服务器”，从列表中选择相应的云服务器即可。

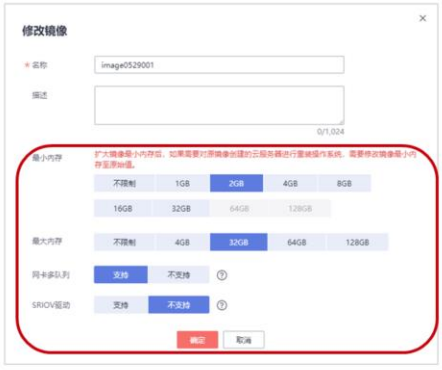


HUAWEI

- 华为云支持在线制作镜像，不需要关机，但是生产环境为了数据一致性，仍然建议关机制作。

IMS的使用 - 修改镜像属性

- 用户可以修改镜像名称、描述信息、最小最大内存或是否支持网卡多队列以及SRIOV驱动。



HUAWEI

- 只有“私有镜像”中状态是“正常”的镜像才允许用户修改镜像属性。
- 网卡多队列：开启网卡多队列功能可以将网卡中断分散给不同的CPU处理，实现负载均衡。
- SRIOV驱动：镜像安装SRIOV驱动后，可以极大提高云服务器的网络处理性能。

IMS的使用 - 删除镜像

- 删除镜像后：
  - 将无法找回该镜像，请谨慎操作。
  - 不能再使用该镜像创建云服务器或云硬盘。
  - 已使用该镜像创建的云服务器仍可正常使用，并会继续产生费用，但是无法重装操作系统，也不能创建相同配置的云服务器。
- 删除复制镜像的源镜像，对复制后的镜像没有影响；反之亦然。

IMS的使用 - 共享镜像

- 当用户将自己的私有镜像共享给云平台的其他用户使用时，可以使用镜像服务的共享镜像功能。

HUAWEI

- 当用户作为共享镜像的提供者时，可以共享指定镜像、取消共享镜像、添加或删除镜像的共享租户。
- 当用户作为共享镜像的接受者时，可以选择接受或者拒绝其他用户提供的共享镜像，也可以移除已经接受的共享镜像。

IMS的使用 - 加密镜像

- 用户可以采用加密方式创建私有镜像，确保镜像数据安全性。加密镜像不能共享给其他用户，不能发布到应用超市。对于加密镜像创建的云服务器，其系统盘只能为加密状态，且磁盘密钥与镜像密钥一致。如果云服务器的系统盘已加密，那么使用该云服务器创建的私有镜像也是加密的。

IMS的使用 - 区域内复制镜像

- 用户复制镜像的场景有以下三种：
  - 将加密镜像复制为非加密镜像
  - 将加密镜像复制为加密镜像
  - 将非加密镜像复制为加密镜像

HUAWEI

- 用户复制镜像的场景有以下三种：
  - 将加密镜像复制为非加密镜像：目前，加密镜像不允许共享和发布为市场镜像。如果用户需要将自己的加密镜像发布为市场镜像或者共享给某个租户，则可以通过镜像复制功能将加密的私有镜像复制为非加密私有镜像，再共享或者发布该非加密私有镜像。
  - 将加密镜像复制为加密镜像：目前，加密镜像不支持更换加密密钥。如果用户需要更换某个加密镜像的加密密钥，则可以通过镜像复制功能，选择新的加密密钥，将原来的加密镜像重新加密为新的私有镜像。
  - 将非加密镜像复制为加密镜像：如果用户需要将原来某个非加密的镜像采用加密方式进行保存，则可以通过镜像复制功能，指定加密密钥，将原有的非加密镜像复制为新的一个加密私有镜像。

IMS的使用 - 跨区域复制镜像

- 用户在一个区域制作的私有镜像，可以通过跨区域复制镜像，将镜像复制到其他区域，在其他区域发放相同类型的云服务器，帮助用户实现区域间的业务迁移。

HUAWEI

- 跨区域复制镜像的典型场景为系统环境多区域部署，以应对系统高可用及国际化的趋势。部署方式通常需要多区域+海外节点部署，快速实现跨区域复制云服务器的方法之一便是通过复制镜像将一个镜像复制到多个区域，然后使用私有镜像快速部署云服务器。
- 跨区域复制适用于跨区域部署服务器，或者跨区域备份数据，常和共享镜像结合使用，以达到跨区域跨帐号复制镜像的目的。
- 批量跨区域复制时，不允许复制ISO镜像、加密镜像、整机镜像以及状态为“创建中”或“已冻结”的镜像。

IMS的使用 - 导出镜像

- 应用场景：
  - 用户需要将私有镜像导出到指定存储设备
  - 将华为云平台的私有镜像导出到其他云平台，实现主机迁移

HUAWEI

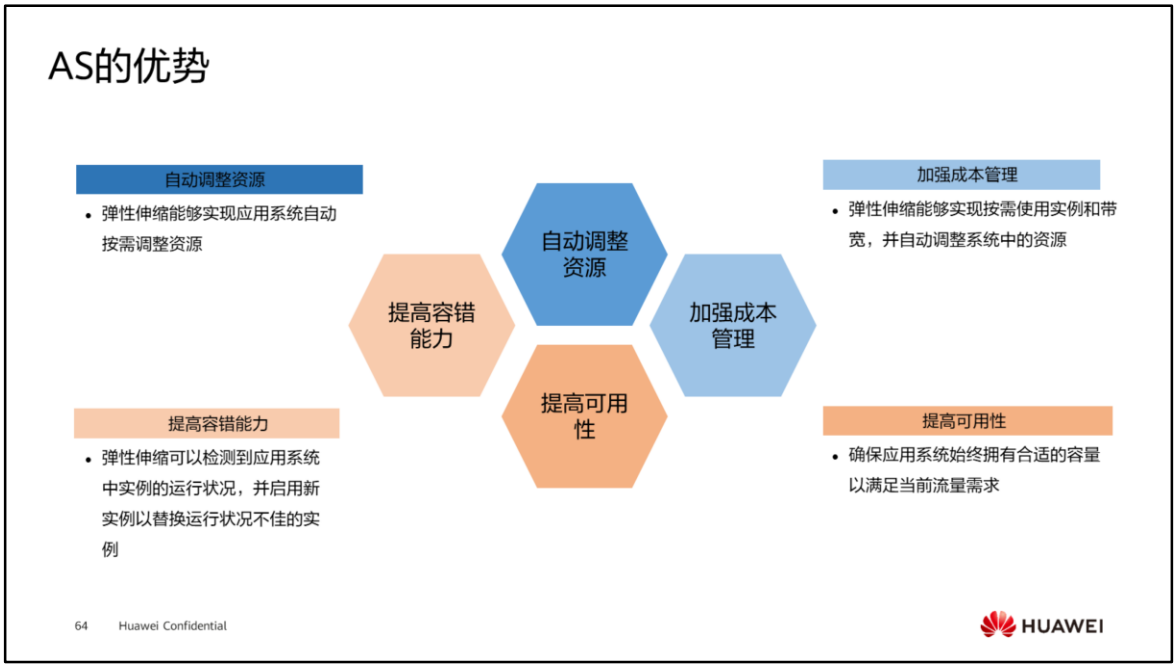
- 目前，支持用户将处在可用状态的私有镜像导出到OBS桶中并指定导出镜像的格式。用户可以通过对象存储服务将OBS桶中的镜像下载到指定存储。在镜像导出过程中，不同的导出格式会导致镜像的大小不同，导出的镜像所占用的OBS存储空间以实际导出的镜像大小为准，对象存储服务会根据实际导出的镜像大小收取存储费用。

目录

什么是弹性伸缩（AS）

- 弹性伸缩（Auto Scaling，AS）是根据用户的业务需求，通过策略自动调整其业务资源的服务。用户可以根据业务需求自行定义伸缩配置和伸缩策略，降低人为反复调整资源以应对业务变化和高峰压力的工作量，帮助用户节约资源和人力成本。

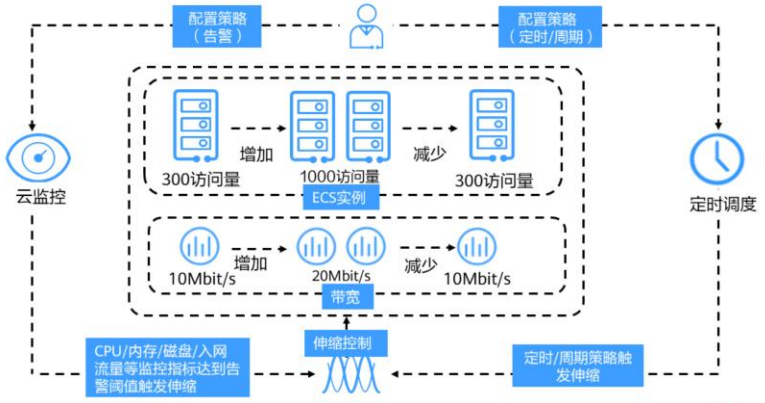
定义弹性伸缩组　　定义策略和配置　　系统自动添加云主机



- AS的优势：
  - 自动调整资源：弹性伸缩能够实现应用系统自动按需调整资源，即在业务增长时能够实现自动增加实例数量和带宽大小，以满足业务需求，业务下降时能够实现应用系统自动缩容，保障业务平稳运行。
  - 加强成本管理：弹性伸缩能够实现按需使用实例和带宽，并自动调整系统中的资源，节省了资源和人为调整资源带来的损耗，为用户最大程度节约了成本。
  - 提高可用性：弹性伸缩可确保应用系统始终拥有合适的容量以满足当前流量需求。当弹性伸缩和负载均衡器结合后，伸缩组会自动地为新加入的实例绑定负载均衡监听器。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。
  - 提高容错能力：弹性伸缩可以检测到应用系统中实例的运行状况，并启用新实例以替换运行状况不佳的实例。

AS的产品架构

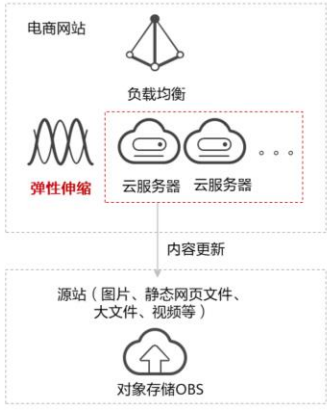
- 弹性伸缩服务（Auto Scaling）可根据用户的业务需求和策略，自动调整计算资源，使得云服务器数量可随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行。



HUAWEI

- 通过伸缩控制可以实现弹性云服务器（ECS）实例伸缩和带宽伸缩：
  - 伸缩控制：配置策略设置指标阈值/伸缩活动执行的时间，通过云监控，监控指标是否达到阈值，通过定时调度，实现伸缩控制。
  - 配置策略：可以根据业务需求，配置告警策略/定时策略/周期策略。
  - 配置告警策略：可配置CPU、内存、磁盘、入网流量等监控指标。
  - 配置定时策略：通过配置触发时间可以配置定时策略。
  - 配置周期策略：通过配置重复周期、触发时间、生效时间可以配置周期策略。
  - 云监控监控到所配置的告警策略中的某些指标达到告警阈值，从而触发伸缩活动，实现ECS实例的增加/减少或带宽的增大/减小。
  - 到达所配置的触发时间时，触发伸缩活动，实现ECS实例的增加/减少或带宽的增大/减小。

应用场景 - 电商网站



适用场景

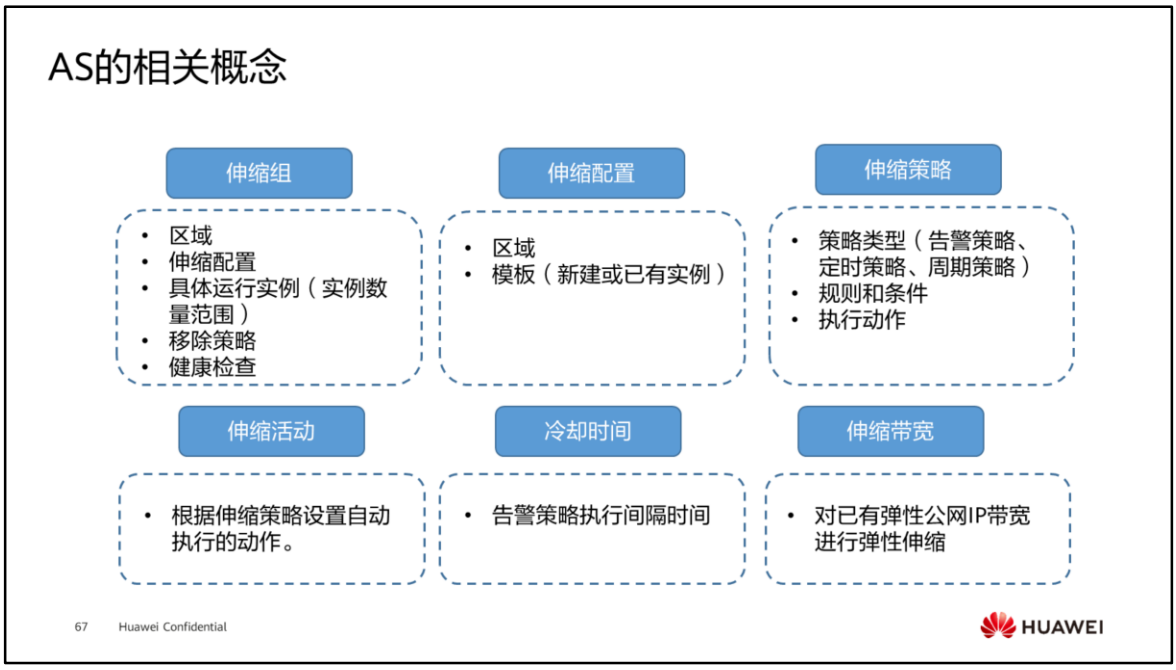
- 电商网站、存在明显波峰波谷的大流量网站

推荐原因

- 电商网站，在进行大型促销活动时，需要定时增加云服务器数量和带宽大小，以保证促销活动顺利进行。
- 访问流量较大的门户网站，业务负载变化难以预测，需要根据实时监控到的云服务器CPU使用率、内存使用率等指标对云服务器数量进行动态调整。

HUAWEI

- 弹性伸缩和负载均衡结合使用：
- 当用户在使用弹性伸缩时，业务增长时应用系统自动扩容，业务下降时应用系统自动缩容，在伸缩组添加和删除实例时，须确保所有实例均可分配到应用程序的流量。弹性伸缩和负载均衡结合使用可以解决这个问题。
- 使用负载均衡后，伸缩组会自动地将加入伸缩组的实例绑定负载均衡监听器。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，提高了应用系统的可用性。若伸缩组中的实例上部署了多个业务，还可以添加多个负载均衡监听器到伸缩组，同时监听多个业务，从而提高业务的可扩展性。



- AS的相关概念：
  - 伸缩组：伸缩组是具有相同应用场景的实例的集合，是启停伸缩策略和进行伸缩活动的基本单位
  - 伸缩配置：伸缩配置是伸缩组内实例（弹性云服务器）的模板，定义了伸缩组内待添加的实例的规格数据。包括云服务器类型、vCPU、内存、镜像、磁盘、登录方式等
  - 伸缩策略：伸缩策略可以触发伸缩活动，是对伸缩组中实例数量进行调整的一种方式。伸缩策略规定了伸缩活动触发需要满足的条件及需要执行的操作，当满足伸缩条件时，系统会自动触发一次伸缩活动
  - 伸缩活动：伸缩组中增加或减少实例的过程称为伸缩活动。伸缩活动的目的是使应用系统中当前实例数和期望实例数保持一致，或达到已设置的伸缩策略触发条件时，执行增加或减少实例数量的操作，保证业务正常运行
  - 冷却时间：为了避免告警策略频繁触发，必须设置冷却时间。冷却时间是指冷却伸缩活动的时间，在每次伸缩活动完成之后，系统开始计算冷却时间。伸缩组在冷却时间内，会拒绝由告警策略触发的伸缩活动。其他类型的伸缩策略（如定时策略和周期策略）触发的伸缩活动不受限制，但会重新开始计算冷却时间，单位为秒
  - 伸缩带宽：伸缩带宽可以根据用户配置的伸缩带宽策略自动调整带宽资源。弹性伸缩仅支持对按需购买的弹性公网IP带宽和共享带宽进行调整，不支持对包年包月的带宽进行调整

AS的创建流程

创建伸缩配置

- 在创建伸缩配置时，配置模板如何选择?

使用新模板

- 若用户对扩展的云服务器的规格有特殊要求，可通过使用新模板创建伸缩配置，可按照用户的需求配置新模板的规格参数，使得伸缩组内云服务器的规格均符合创建新模板的规格。

使用已有云服务器规格为模板

- 用户可以使用已有的弹性云服务器快速创建伸缩配置。此时，伸缩配置中的云服务器类型、vCPU、内存、镜像、磁盘参数信息将默认与选择的云服务器规格保持一致。

创建伸缩组

- 伸缩组是具有相同属性和应用场景的云服务器和伸缩策略的集合，是启停伸缩策略和进行伸缩活动的基本单位。
- 使用伸缩策略设定的条件自动增加、减少伸缩组中的实例数量，或维持伸缩组中固定的实例数量。
- 创建伸缩组，需要配置最大实例数、最小实例数、期望实例数和负载均衡器等参数。

HUAWEI

- 伸缩组配置：
  - 多可用区扩展策略：当选择两个及以上可用区时，才需要配置该选项
  - 最大/最小实例数：指伸缩组中云服务器个数的最大值/最小值
  - 期望实例数：伸缩组中期望运行的弹性云服务器数量，大小介于最小实例数和最大实例数之间。一般在业务高峰即将到来时，设置期望实例数，可快速部署大量服务器
  - 实例移除策略：当用户的伸缩组自动移除实例时，如果伸缩组内存在不属于当前配置的可用区的实例，移除实例时，会优先移除这些实例。其次，会评估伸缩组当前配置的可用区是否存在不平衡。如果某个可用区的实例数多于其他可用区，移除实例时会优先保证可用区均衡。如果该组使用的可用区是平衡的，则实例会按照用户配置的实例移除策略被移除

创建伸缩策略

- 伸缩策略的配置主要包含：策略类型和冷却时间。

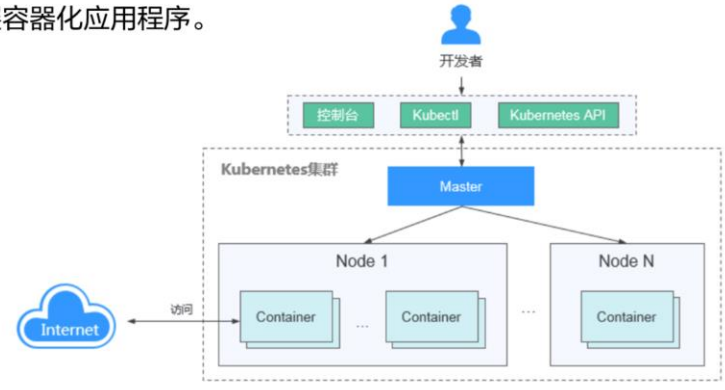
HUAWEI

- 当业务负载难以预测时，选择告警策略，系统会根据实时的监控数据（如CPU使用率）触发伸缩活动，动态调整伸缩组内的云服务器数量。每次伸缩活动完成之后，系统开始计算冷却时间。伸缩组在冷却时间内，会拒绝由告警策略触发的伸缩活动，其他类型的伸缩策略（如定时策略和周期策略）触发的伸缩活动不受限制。

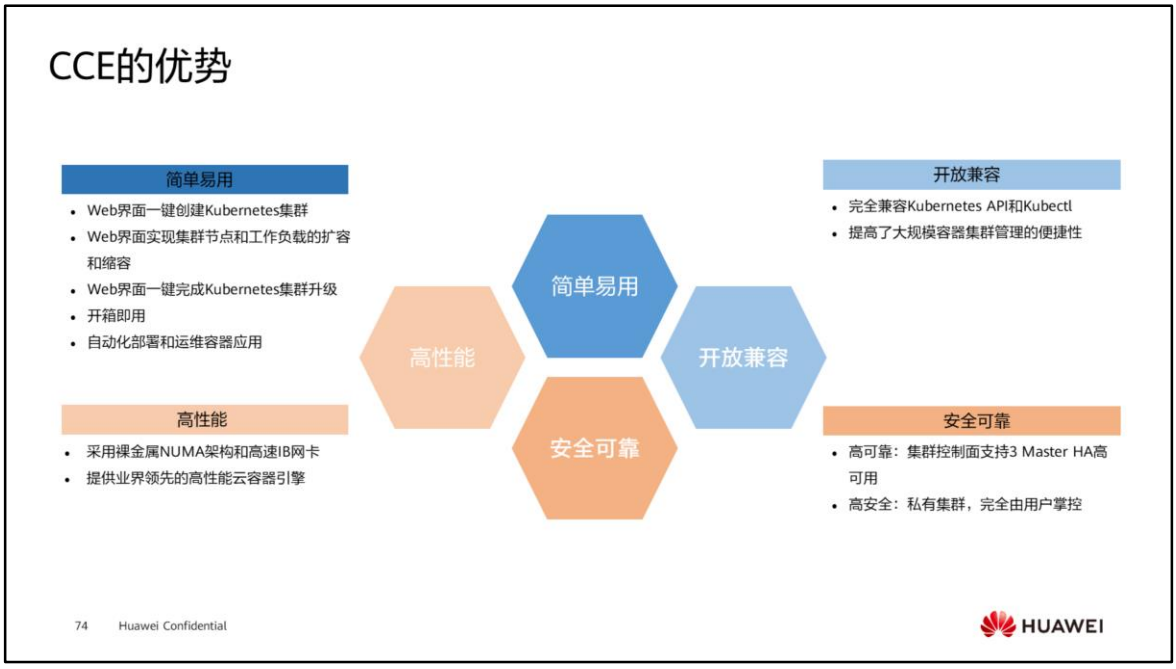
目录

什么是云容器引擎（CCE）

- 云容器引擎（Cloud Container Engine，CCE）提供高度可扩展的、高性能的企业级Kubernetes集群，支持运行Docker容器。借助云容器引擎，用户可在华为云上轻松部署、管理和扩展容器化应用程序。

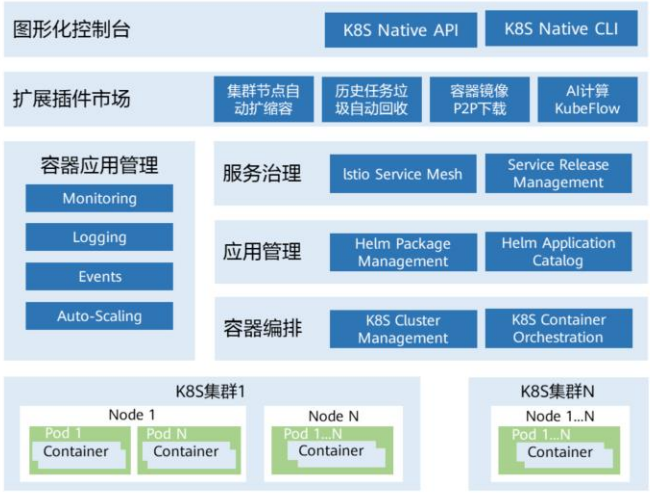


HUAWEI



- 简单易用：
  - 通过Web界面一键创建Kubernetes集群，支持管理虚拟机节点或裸金属节点，支持虚拟机与物理机混用场景
  - 一站式自动化部署和运维容器应用，整个生命周期都在容器服务内一站式完成
  - 通过Web界面轻松实现集群节点和工作负载的扩容和缩容，自由组合策略以应对多变的突发浪涌
  - 通过Web界面一键完成Kubernetes集群的升级
  - 深度集成应用服务网格和Helm标准模板，真正实现开箱即用
- 高性能：
  - 基于华为在计算、网络、存储、异构等方面多年的行业技术积累，提供业界领先的高性能云容器引擎，支撑业务的高并发、大规模场景
  - 采用高性能裸金属NUMA架构和高速IB网卡，AI计算性能提升3-5倍以上

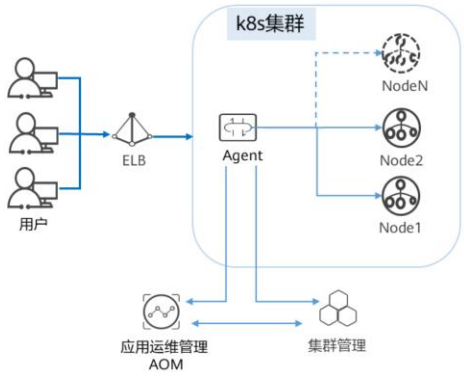
CCE的产品架构



HUAWEI

- 云容器引擎深度整合华为云高性能的计算（ECS/BMS）、网络（VPC/EIP/ELB）、存储（EVS/OBS/SFS）等服务，并支持GPU、NPU、ARM、FPGA等异构计算架构，支持多可用区（Available zone，简称AZ）、多区域（Region）容灾等技术构建高可用Kubernetes集群。

应用场景 - 集群弹性伸缩



适用场景

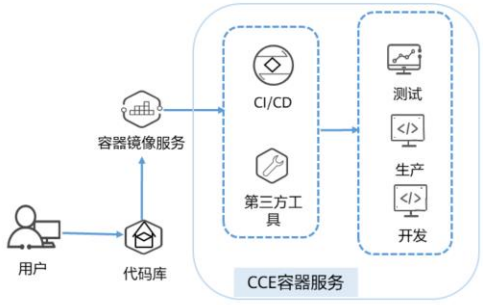
- 据用户的业务需求和预设策略，自动调整计算资源，使云服务器或容器数量自动随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行。

推荐原因

- 自由灵活：支持多种策略配置，业务流量达到扩容指标，秒级触发容器扩容操作
- 高可用：自动检测伸缩组中实例运行状况，启用新实例替换不健康实例，保证业务健康可用
- 低成本：只按照实际用量收取云服务器费用

- 具体应用场景：
  - 电商客户遇到促销、限时秒杀等活动期间，访问量激增，需及时、自动扩展云计算资源
  - 视频直播客户业务负载变化难以预测，需要根据CPU/内存使用率进行实时扩缩容
  - 游戏客户每天中午12点及晚上18:00-23:00间需求增长，需要定时扩容

应用场景 - DevOps



适用场景

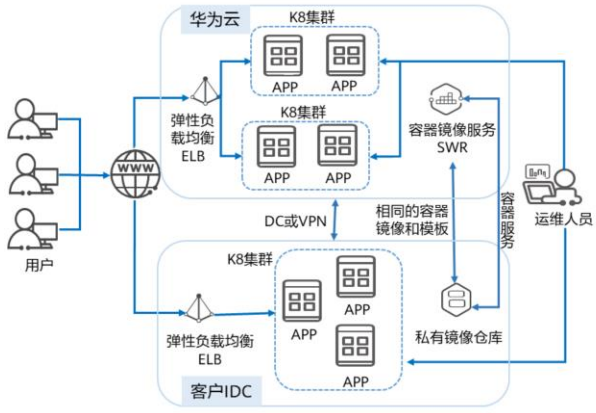
- 基于代码源自动完成代码编译、镜像构建、灰度发布、容器化部署流程。对接已有CI/CD，完成传统应用的容器化改造和部署。

推荐原因

- 高效流程管理：更优的流程交互设计，脚本编写量较传统CI/CD流水线减少80%以上，让CI/CD管理更高效
- 灵活的集成方式：提供丰富的接口便于与企业已有CI/CD系统进行集成，灵活适配企业的个性化诉求
- 高性能：全容器化架构设计，任务调度更灵活，执行效率更高

- DevOps：即Development and Operations，是一组过程、方法与系统的统称，用于促进软件开发、运维和质量保障部门之间的沟通、协作与整合。
- 应用场景：
  - 当前IT行业发展日益快速，面对海量需求必须具备快速集成的能力。经过快速持续集成，才能保证不间断的补全用户体验，提升服务质量，为业务创新提供源源不断的动力。大量交付实践表明，不仅传统企业，甚至互联网企业都可能在持续集成方面存在研发效率低、工具落后、发布频率低等方面的问题，需要通过持续交付提高效率，降低发布风险
- CI持续集成（ Continuous Integration ），CD持续交付(Continuous Delivery)、持续部署(Continuous Deployment)。

应用场景 - 混合云



适用场景

- 利用容器环境无关的特性，私有云和公有云容器服务实现网络互通和统一管理，应用和数据可在云上云下无缝迁移，从而实现资源的灵活使用以及业务容灾等目的。

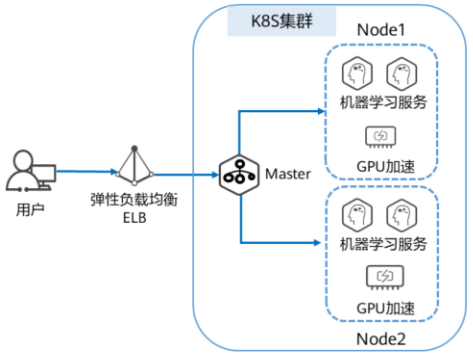
推荐原因

- 降低成本：业务高峰时，利用公有云资源池快速扩容，相比自建大量私有云成本更低
- 云上容灾：业务系统同时部署在云下和云上，云下提供服务，云上实现容灾
- 技术共享：云上云下技术能力共享，降低云下技术风险，需要时可利用云上的其他资源

HUAWEI

- 具体应用场景：
  - 多云部署、容灾备份：为保证业务高可用，需要将业务同时部署在多个云的容器服务上，在某个云出现事故时，通过统一流量分发的机制，自动地将业务流量切换到其他云上
  - 流量分发、弹性伸缩：大型企业客户需要将业务同时部署在不同地域的云机房中，并能自动弹性扩容和缩容，以节约成本
  - 业务上云、数据库托管：对于金融、安全等行业用户，由于业务数据的敏感性要求，将数据业务保留在本地的IDC中而将一般业务部署在云上，并需要进行统一管理
  - 开发与部署分离：出于IP安全的考虑，用户希望将生产环境部署在公有云上，而将开发环境部署在本地的IDC

应用场景 - AI计算



适用场景

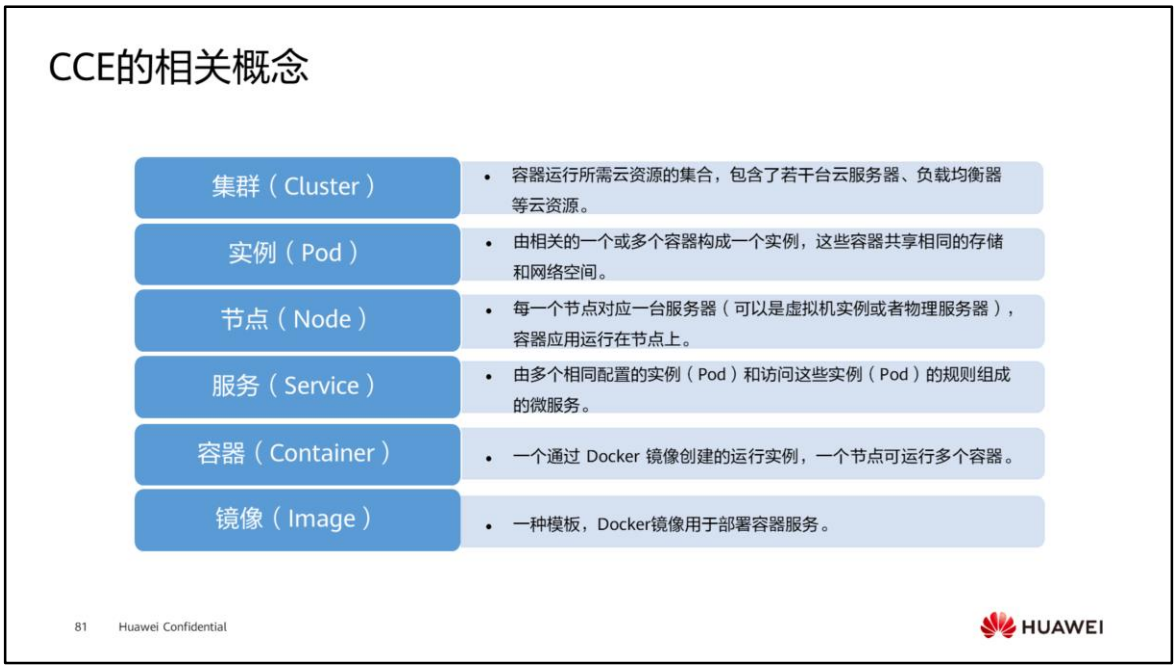
- AI计算

推荐原因

- 超强性能：裸金属NUMA架构与高速IB网卡，AI计算性能提升3~5倍
- 高效计算：GPU资源多容器共享调度，整体计算成本大幅降低
- 成熟应用：主流GPU型号全适配，并在华为云EI产品大规模使用

HUAWEI

- CCE通过集成Volcano，在高性能计算、大数据、AI等领域有如下优势：
  - 多种类型作业混合部署：支持AI、大数据、HPC作业类型混合部署
  - 多队列场景调度优化：支持多队列用于多租资源共享与分组规划，支持优先级与分时复用
  - 多种高级调度策略：支持gang-scheduling、公平调度、资源抢占、GPU拓扑等高级调度策略
  - 多任务模板：支持单一Job多任务模板定义，打破Kubernetes原生资源束缚，Volcano Job描述多种作业类型（Tensorflow、MPI、PyTorch等）
  - 作业扩展插件配置：在提交作业、创建Pod等多个阶段，Controller支持配置插件用来执行自定义的环境准备和清理的工作，比如常见的MPI作业，在提交前就需要配置SSH插件，用来完成Pod资源的SSH信息配置



- CCE的相关概念：
  - 集群：集群指容器运行所需要的云资源组合，关联了若干云服务器节点、负载均衡等云资源。可以理解为集群是“同一个子网中一个或多个弹性云服务器（又称：节点）”通过相关技术组合而成的计算机群体，为容器运行提供了计算资源池。
  - 实例：实例是 Kubernetes 部署应用或服务的最小的基本单位。一个Pod 封装多个应用容器（也可以只有一个容器）、存储资源、一个独立的网络 IP 以及管理控制容器运行方式的策略选项。
  - 节点：每一个节点对应一台服务器（可以是虚拟机实例或者物理服务器），容器应用运行在节点上。节点上运行着Agent代理程序（kubelet），用于管理节点上运行的容器实例。集群中的节点数量可以伸缩。
  - 服务：服务是将运行在一组 Pods 上的应用程序公开为网络服务的抽象方法。
  - 容器：一个通过 Docker 镜像创建的运行实例，一个节点可运行多个容器。容器的实质是进程，但与直接在宿主执行的进程不同，容器进程运行于属于自己的独立的命名空间。
  - 镜像：Docker镜像是一个模板，是容器应用打包的标准格式，用于创建Docker容器。或者说，Docker镜像是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源、配置等文件外，还包含了一些为运行时准备的配置参数（如匿名卷、环境变量、用户等）。
- 除这些基本概念外，还有很多其他概念，详细可参见：https://support.huaweicloud.com/productdesc-cce/cce_productdesc_0011.html。

CCE的配置流程

HUAWEI

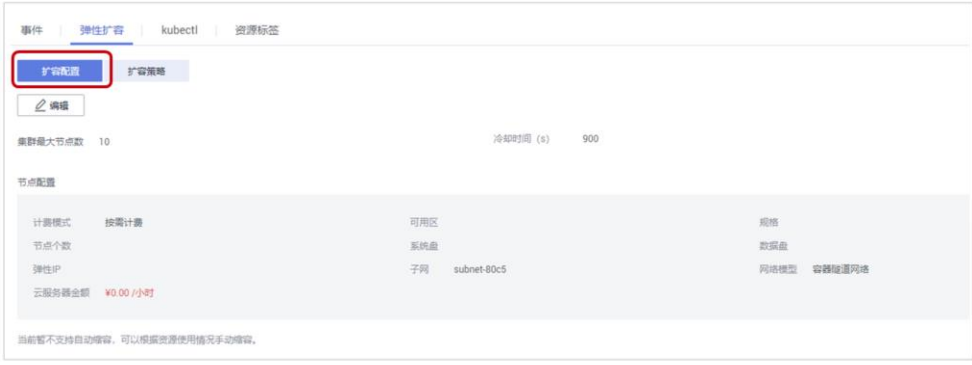
- 注册华为云帐号，并登录CCE控制台：注册并登录华为云账号，进入控制台，选择CCE控制台。
- 创建集群：用户可根据自己的需求，创建不同类型的集群。
- 部署工作负载：用户可通过镜像或编排模板创建工作负载（应用），也可以使用已有的镜像或编排模板，或者新建镜像或编排模板。

创建集群

- CCE集群的创建需要选择计费模式、区域、版本、集群管理规模、控制节点数等。

CCE的使用 - 集群弹性扩容

- CCE通过云容器引擎管理控制台，可以根据实际业务需要对集群的工作节点进行扩容和缩容，当集群中出现由于资源不足而无法调度的工作负载时自动触发扩容，从而减少人力成本。



CCE的使用 - 集群升级

- 当前仅支持虚拟机节点的CCE集群升级，暂不支持鲲鹏集群、CCE Turbo集群、裸金属节点或私有镜像的CCE集群升级。

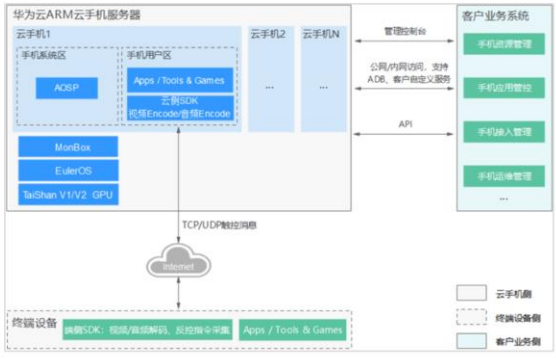
HUAWEI

- 集群升级注意事项：
  - 集群升级操作不可回退，请务必慎重并选择合适的时间段进行升级，以减少升级对业务带来的影响。
  - 集群升级前请参考Kubernetes版本发布说明，了解每个集群版本发布的特性以及差异，否则可能因为应用不兼容新集群版本而导致升级后异常。
  - 集群升级中请勿关机或重启节点，否则会导致升级失败。
  - 集群升级前请关闭弹性扩缩容策略，避免在升级过程中扩缩容节点，从而导致升级失败。
  - 如果本地修改了集群节点的配置，可能导致集群升级失败或升级后配置丢失，建议通过集群的配置管理和节点池的配置管理修改配置，以便在升级时自动继承。
  - 集群升级过程中，已运行工作负载业务不会中断，但API Server访问会短暂中断，如果业务需要访问API Server可能会受到影响。

目录

什么是云鲲鹏云手机（CPH）

- 华为云鲲鹏云手机（Cloud Phone，CPH），是基于华为云鲲鹏裸金属服务器，虚拟出带有原生安卓操作系统，具有虚拟手机功能的云服务器。同时，作为一种新型应用，云手机对物理手机起到了非常好的延伸和拓展作用，可以用于如云手游、移动办公等场景。



HUAWEI

- 作为一种新型服务，云手机对传统物理手机起到了非常好的延展和补充作用，可以用在诸如APP仿真测试、云手游、直播互娱、移动办公等场景，让移动应用不但可以在物理手机运行，还可以在云端智能运行：
  - 降本增效：面向如APP仿真测试等互联网行业场景，单台手机的处理效率非常有限，通过云手机的方式，大幅降低人工操作和设备采购维护成本。
  - 安全保障：云手机由于应用数据运行在云上，面向政府、金融等信息安全诉求较高的行业，提供更加安全高效的移动办公解决方案。员工通过使用云手机的方式登录办公系统，公私数据分离，同时企业也可对云手机进行智能管理，降本增效的同时，信息安全也更加有保障。
  - 探索游戏、直播行业新可能：云手机还可以为游戏、直播等行业提供全新的互动体验方式，开拓新的商业模式和市场空间。以云手游场景为例，因为游戏的内容实际是在云上虚拟手机上运行，可以提前安装部署和动态加载，所以对于最终玩家来说，游戏可以做到无需下载，即点即玩，大幅提高玩家转换率。同时可以让中低配手机用户也能流畅运行大型手游，增大游戏覆盖的用户范围。

什么是专属主机（DeH）

- 专属主机（Dedicated Host，DeH），是指用户可独享的专属物理主机资源。用户可以将云服务器创建在专属主机上，满足其对隔离性、安全性、性能的更高要求。同时，还可以在迁移业务至专属主机时，继续使用迁移前的服务器端软件许可，即支持自带许可（BYOL），达到节省开支、提高对云服务器的自治等目的。

HUAWEI

- DeH的应用场景：
  - 对合规性、安全性有需求行业：用户独占物理主机，保证对其专属主机享有更多控制权，且与其他用户的资源物理隔离，满足了用户对合规性、安全性的需求
  - 需使用自带许可（BYOL）特性的租户：如果用户已拥有操作系统或软件的许可证（一般是指按物理插槽数、物理内核数等进行认证的许可证），可以通过自带许可（BYOL）的方式将业务完整迁移到云平台，继续使用其许可证
  - 性能、稳定性极其敏感行业：与一般业务相比，某些特殊场景（如金融证券、游戏应用）对服务器的性能、稳定性和实时性要求更高。使用专属主机能进一步提升业务CPU、网络I/O资源环境的稳定性，确保应用可靠运行
  - 资源自主部署，灵活管理：支持指定专属主机创建云服务器，依据专属主机资源自定义规格。可以将云服务器从一台专属主机迁移至另一台专属主机，也可以将公共资源池的云服务器迁移至专属主机

什么是云耀云服务器（HECS）

- HECS（Hyper Elastic Cloud Server）云耀云服务器是可以快速搭建简单应用的新一代云服务器，具备独立、完整的操作系统和网络功能。提供快速的应用部署和简易的管理能力，适用于网站搭建、开发环境等低负载应用场景。具有高性价比、易开通、易搭建、易管理的特点。

HUAWEI

- 网站应用：云耀云服务器适用于对CPU、内存、硬盘空间和带宽无特殊要求，服务一般只需要部署在一台或少量的服务器上，一次投入成本少，后期维护成本低的场景，例如网站开发，Web应用。
- 开发测试环境：云耀云服务器可以提供基本水平的vCPU性能、平衡的计算、内存和网络资源，同时可根据工作负载的需要实现性能的突增，具有短期发挥更高性能的能力。适用于那些不会经常（或始终）用尽vCPU性能，但会偶尔突然使用的场景。例如开发、测试环境以及中低性能数据库等。
- 电商网站：云耀云服务器性能更高、计算能力更稳，配套高性能网络，综合性能及稳定性全面提升，可以为中低型负载提供较强的计算能力，适用于中小型电商网站系统的场景。

思考题

1. （判断题）容器也有像虚拟机一样的虚拟化层（Hypervisor）。

   正确

   错误

2. （判断题）在云平台镜像服务中的镜像和我们平时装系统的iso是一样的。

   正确

   错误

- 错误。容器是没有虚拟化层的。
- 错误。我们平时装系统是标准的iso镜像。而我们使用的镜像服务的镜像更像是一个经过处理后的iso模板。虚拟机都是通过该模板批量发放，而不是重装系统。

本章总结

- 本章介绍了计算类相关产品。通过本章的学习，我们了解到从硬件到虚拟化，到云平台，最后到云服务，每个阶段都是一次重大的技术变革，会产生很多新的技术，如弹性云服务器和云容器引擎。两者都可以承载用户系统，但架构截然不同。因此，要想更好地协助企业业务系统上云，我们需要更好地掌握每个云服务背后的技术原理。

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为云技术支持网站
  - https://support.huaweicloud.com/help-novice.html
- 华为云学院
  - https://edu.huaweicloud.com/

术语和缩略语

- AI：Artificial Intelligence，人工智能
- API：Application Programming Interface，应用编程接口
- AS：Auto Scaling，弹性伸缩
- BMS：Bare Metal Server，裸金属服务器
- CCE：Cloud Container Engine，云容器引擎
- CI/CD：Continuous Integration/Continuous Delivery，持续集成/持续交付
- CISC：Complex Instruction Set Computer，复杂指令系统计算机
- CPH：Cloud Phone，云鲲鹏云手机
- CPU：Central Processing Unit，中央处理器
- DeH：Dedicated Host，专属主机

术语和缩略语

- DevOps：Development and Operations，开发即运营
- DHCP：Dynamic Host Configuration Protocol，动态主机配置协议
- ECS：Elastic Cloud Server，弹性云服务器
- EI：Enterprise Intelligence，企业智能
- GPU：Graphics Processing Unit，图形处理器
- HECS：Hyper Elastic Cloud Server，云耀云服务器
- HPC：High Performance Computing，高性能计算
- HTTPS：Hypertext Transfer Protocol over Secure Sockets Layer，安全套接字层的超文本传输协议
- IB：InfiniBand，无限带宽
- IMS：Image Management Service，镜像服务
- K8S：Kubernetes，容器编排工具

术语和缩略语

- IPoIB：Internet Protocol over Infiniband，基于InfiniBand的因特网协议
- NUMA：Non-Uniform Memory Access，非一致性内存访问
- RDMA：Remote Direct Memory Access，远程直接数据存取
- RISC：Reduced Instruction Set Computer，精简指令集计算机
- SRIOV：Single Root Input/Output Virtualization，单根输入输出虚拟化
- VLAN：Virtual Local Area Network，虚拟本地网
- VPC：Virtual Private Cloud，虚拟私有云

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

网络云服务

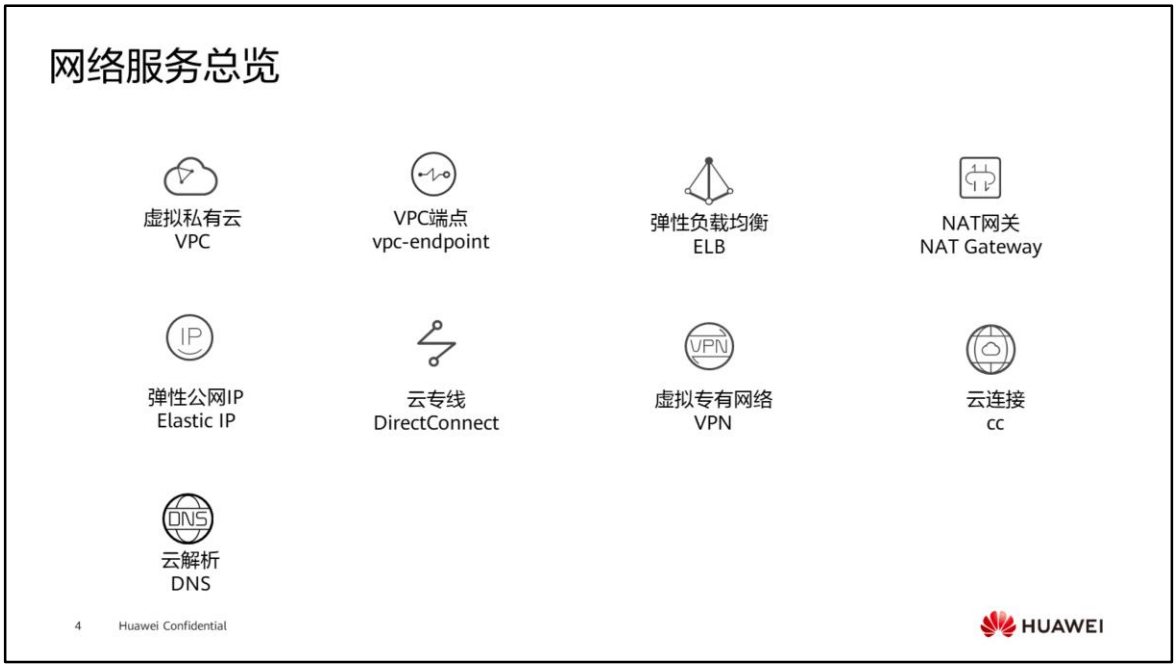
HUAWEI

前言

- 在整个ICT基础设施的发展过程中，网络资源一直是必不可少的存在。有了网络资源，设备与设备间，系统与系统间才有了交流，才能更好地去支撑企业业务的快速发展。
- 本章将带领大家了解华为云上的网络服务。

目标

- 学完本课程后，您将能够：
  - 了解到什么是网络服务，常见的网络服务有哪些，我们在什么情况下该使用哪一种类型的网络服务。
  - 掌握常见网络类服务的原理及使用。

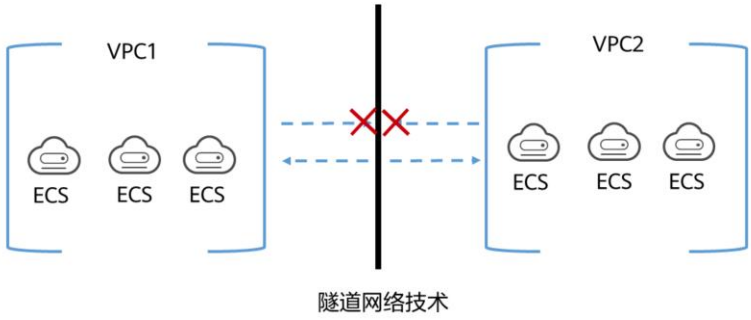


- 虚拟私有云：华为云上隔离的、私密的虚拟网络环境.。
- VPC端点：安全访问华为云上托管的服务。
- 弹性负载均衡：自动分发访问流量到多台云服务器。
- NAT网关：为云服务器提供网络地址转换服务。
- 弹性公网IP：提供独立的公网IP资源。
- 云专线DC：本地数据中心与VPC间的专属通道。
- 虚拟专用网络：本地数据中心与VPC间IPsec加密通道。
- 云连接：为租户提供多Region VPC互通及云上云下互通的混合云组网服务。
- 云解析服务 DNS：提供权威DNS服务和DNS管理服务。

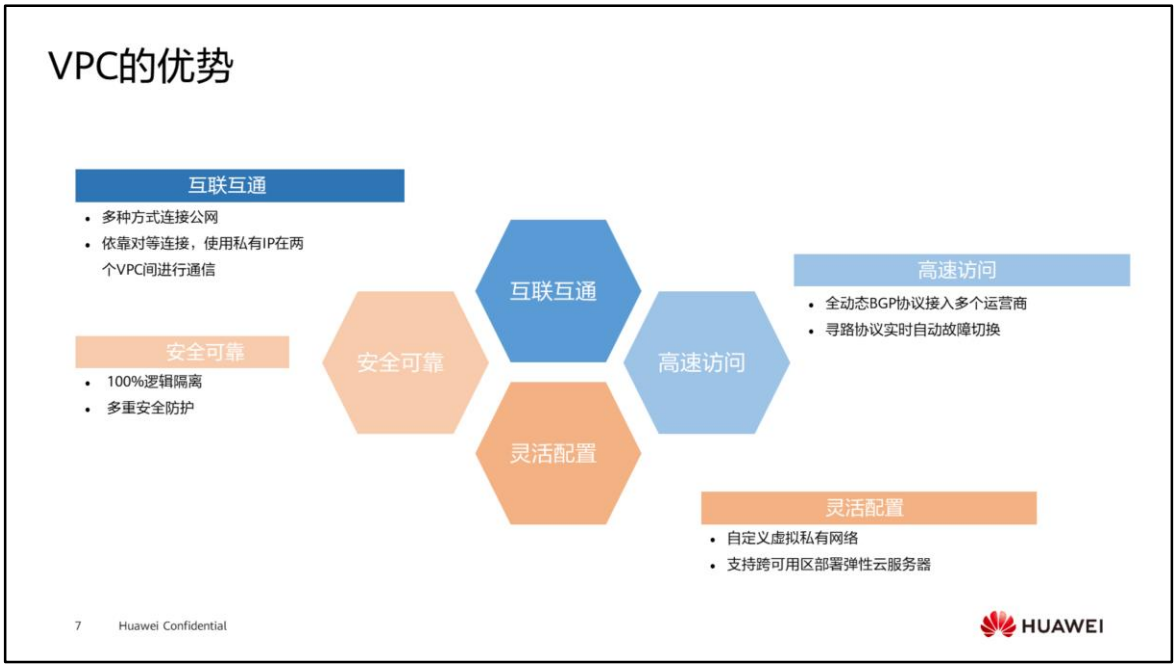
目录

什么是虚拟私有云（VPC）

- 虚拟私有云（Virtual Private Cloud）是用户在华为云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务，也可以基于VPC申请弹性带宽或弹性IP给业务系统使用。

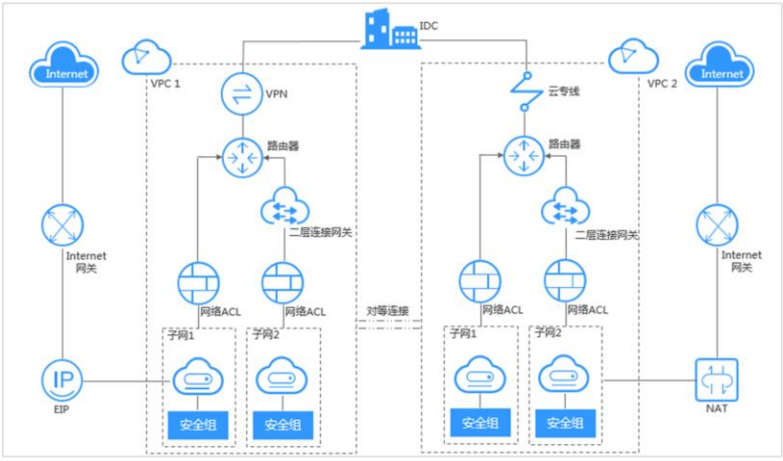


- 虚拟私是华为云网络基础，基于安全的隧道网络技术，提供安全、隔离的网络环境。用户可以自定义自己的VPC，包括划分子网、配置路由表、指定IP地址等，同时还可以配置网络安全策略。



- VPC优势：
  - 灵活配置：自定义虚拟私有网络，按需划分子网，配置IP地址段，DHCP、路由表等服务。支持跨可用区部署弹性云服务器
  - 安全可靠：VPC之间通过隧道技术进行100%逻辑隔离，不同VPC之间默认不能通信。网络ACL对子网进行防护，安全组对弹性云服务器进行防护
  - 互联互通：默认情况下，VPC与公网是不能通信访问的，依靠了弹性公网IP、弹性负载均衡、NAT网关、虚拟专用网络、云专线等多种方式连接公网。默认情况下，两个VPC之间也是不能通信访问的，依靠对等连接的方式，使用私有IP地址在两个VPC之间进行通信
  - 高速访问：使用全动态BGP协议接入多个运营商，支持多达21条线路。可以根据设定的寻路协议实时自动故障切换，保证网络稳定，网络时延低，云上业务访问更流畅

VPC的产品架构

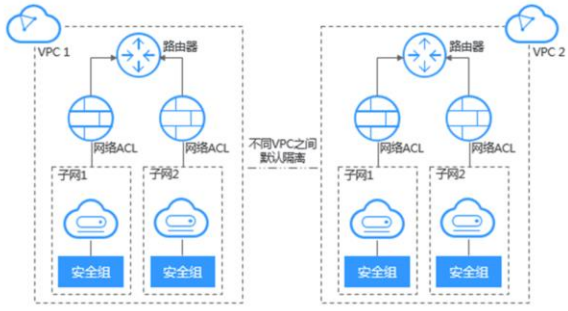


HUAWEI

- VPC组成部分：每个虚拟私有云VPC由一个私网网段、路由表和至少一个子网组成：
  - 私网网段：用户在创建虚拟私有云VPC时，需要指定虚拟私有云VPC使用的私网网段。当前虚拟私有云VPC支持的网段有10.0.0.0/8~24、172.16.0.0/12~24和192.168.0.0/16~24
  - 子网：云资源（例如云服务器、云数据库等）必须部署在子网内。所以，虚拟私有云VPC创建完成后，需要为虚拟私有云VPC划分一个或多个子网，子网网段必须在私网网段内
  - 路由表：在创建虚拟私有云VPC时，系统会自动生成默认路由表，默认路由表的作用是保证了同一个虚拟私有云VPC下的所有子网互通。当默认路由表中的路由策略无法满足应用（比如未绑定弹性公网IP的云服务器需要访问外网）时，可以通过创建自定义路由表来解决

应用场景 - 云端专属网络

- 场景描述：每个VPC代表一个私有网络，与其他VPC逻辑隔离。用户可以将业务系统部署在华为云上，构建云上私有网络环境。如果有多个业务系统，例如生产环境和测试环境要严格进行隔离，那么可以使用多个VPC进行业务隔离。

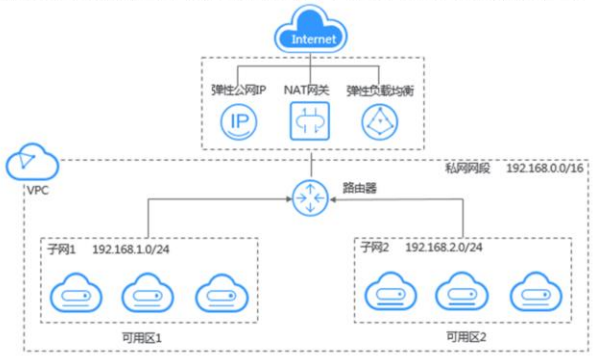


HUAWEI

- 当有互相通信的需求时，可以在两个VPC之间建立对等连接，通过对等连接来实现互通。

应用场景 - Web应用或网站托管

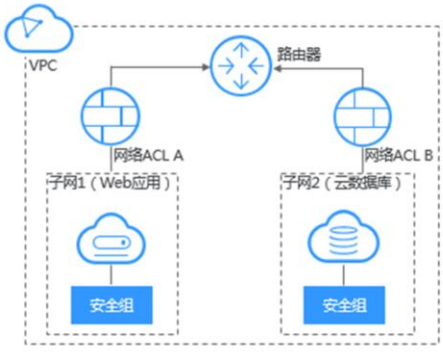
- 场景描述：在VPC中托管Web应用或网站，通过弹性公网IP或NAT网关连接弹性云服务器与Internet，运行弹性云服务器上部署的Web应用程序。同时结合弹性负载均衡ELB服务，用户可以将来自Internet的流量均衡分配到不同的弹性云服务器上。



HUAWEI

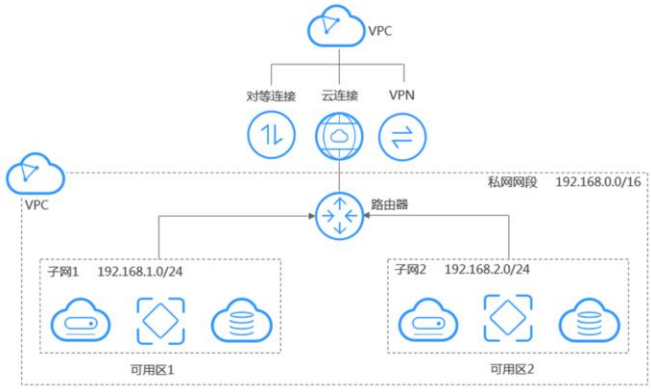
应用场景 - Web应用访问控制

- 场景描述：用户可以通过创建一个VPC，将Web服务器和数据库服务器划分到不同的安全组中。Web服务器所在的子网实现互联网访问，而数据库服务器只能通过内网访问，保护数据库服务器的安全，满足高安全场景。



应用场景 - 云上VPC连接

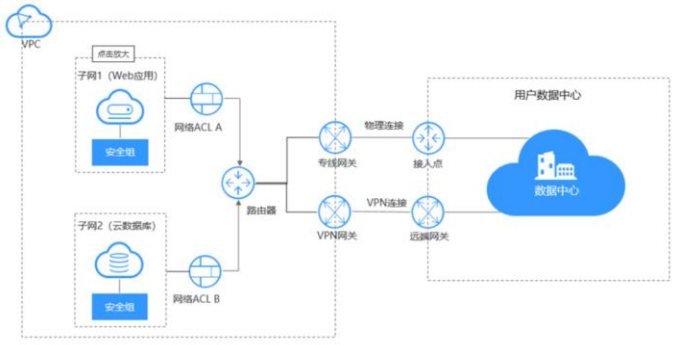
- 场景描述：当相同或者不同区域下的VPC需要互通连接时，可通过如下云产品实现。

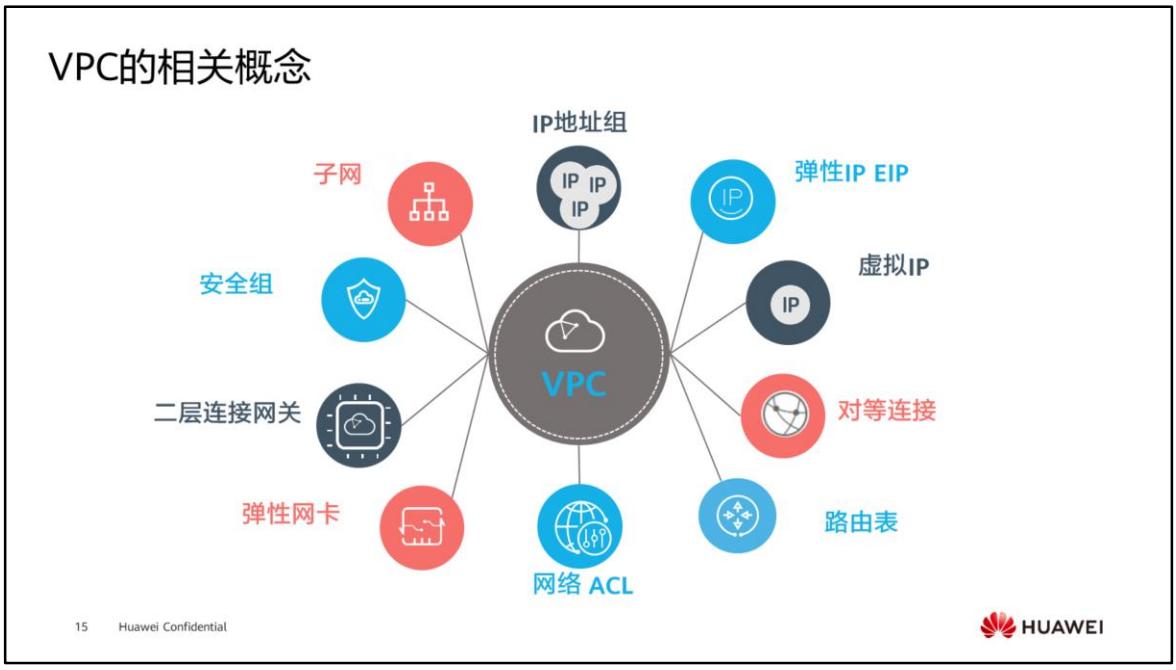


HUAWEI

应用场景 - 混合云部署

- 场景描述：对于自建本地数据中心（IDC）的用户，由于利旧和平滑演进的原因，并非所有的业务都能放置在云上，这个时候就可以通过如下产品构建混合云，实现云上VPC与云下IDC之间的互连。





- 弹性网卡即虚拟网卡，用户可以通过创建并配置弹性网卡，并将其附加到云服务器实例（包括弹性云服务器和裸金属服务器）上，实现灵活、高可用的网络方案配置。
- IP地址组是多个IP地址的集合，可被安全组规则引用，可统一管理具有相同安全要求或需要频繁修改的IP地址。通过使用IP地址组，可有效应对需要重复多次编辑安全组规则的场景，方便管理。

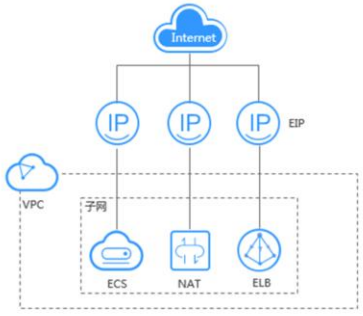
VPC - 子网

- 子网是虚拟私有云内的IP地址块。虚拟私有云中的所有云资源都必须部署在子网内。同一个虚拟私有云下，子网网段不可重复。子网创建成功后，网段无法修改。

- 默认情况下，同一个VPC的所有子网内的弹性云服务器均可以进行通信，不同VPC的弹性云服务器不能进行通信。
- 不同VPC的弹性云服务器可通过创建对等连接通信。

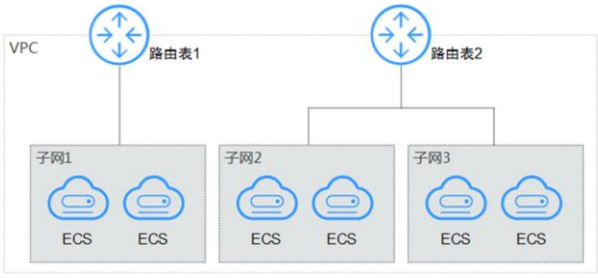
VPC - 弹性公网IP

- 弹性公网IP可以提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。拥有多种灵活的计费方式，可以满足各种业务场景的需要。一个弹性公网IP只能绑定一个云资源使用。



VPC - 路由表

- 路由表由一系列路由规则组成，用于控制虚拟私有云内子网的出流量走向。VPC中的每个子网都必须关联一个路由表，一个子网一次只能关联一个路由表，但一个路由表可以关联多个子网。



- 华为云提供了管理路由表的功能：添加自定义路由、查询路由、修改路由和删除路由等。
- 用户创建虚拟私有云时，系统会自动为其生成一个默认路由表，创建子网后，子网会自动关联默认路由表。用户可以在默认路由表中添加、删除和修改路由规则，但不能删除默认路由表。创建VPN服务时，默认路由表会自动下发路由，该路由不能删除和修改，用户可以将子网关联到自定义路由表或者复制该条路由到自定义路由表中，在自定义路由表中添加、修改和删除路由。
- 用户可以直接使用默认路由表，也可以为具有相同路由规则的子网创建一个自定义路由表，并将自定义路由表与子网关联。自定义路由表可以删除。
- 当前在部分区域中，路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，支持路由表与子网关联功能，请以实际界面为准。
    - 未解耦：在虚拟私有云详情页的“路由表”页签，可对路由表进行操作。
    - 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“路由表”，可对路由表进行操作。

VPC - 安全组

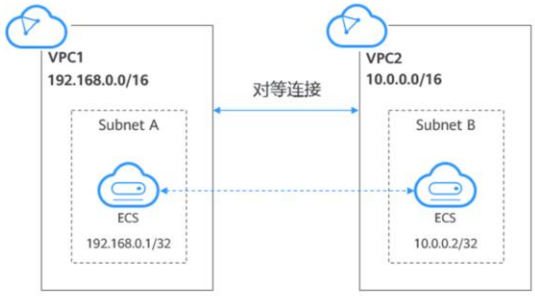
- 安全组是一个逻辑上的分组，为同一VPC内具有相同安全保护需求并相互信任的弹性云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当弹性云服务器加入该安全组后，即受到这些访问规则的保护。

HUAWEI

- 系统会为每个用户默认创建一个Sys-default安全组，默认安全组的规则是在出方向上的数据报文全部放行，入方向访问受限，安全组内的云服务器无需添加规则即可互相访问。

VPC - 对等连接

- 对等连接是指两个VPC之间的网络连接。用户可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。同一区域内，用户可以在自己的VPC之间创建对等连接，也可以在自己的VPC与其他帐户的VPC之间创建对等连接。不同区域间的VPC之间不能创建对等连接。

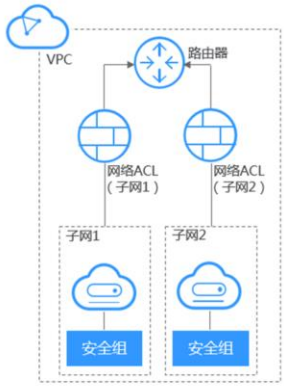


HUAWEI

- 在同一个帐户下，创建对等连接后，状态是已接受。需要在两端VPC内添加对等连接路由信息，才能使两个VPC互通。
- 跨帐户创建VPC对等连接时，一端VPC发起创建对等连接请求，对等连接状态为待接受。待对方接受该创建请求后，对等连接状态变为已接受，请求方和接受方须分别配置对等连接路由信息，才能使两个VPC互通。

VPC - 网络ACL

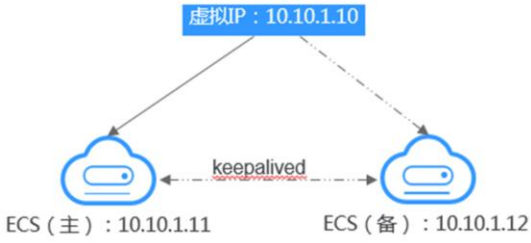
- 网络ACL是对一个子网或多个子网的访问控制策略系统，通过与子网关联的出方向/入方向规则判断数据包是否被允许流入/流出关联子网。



- 网络ACL与安全组类似，都是安全防护策略，当用户想增加额外的安全防护层时，就可以启用网络ACL。安全组只有“允许”策略，但网络ACL可以“拒绝” 和“允许”，两者结合起来，可以实现更精细、更复杂的安全访问控制。

VPC - 虚拟IP

- 虚拟IP是一个未分配给真实弹性云服务器网卡的IP地址。弹性云服务器除了拥有私有IP地址外，还可以拥有虚拟IP地址，用户可以通过其中任意一个IP（私有IP/虚拟IP）访问此弹性云服务器。同时，虚拟IP地址拥有和私有IP地址同样的网络接入能力。虚拟IP主要用在弹性云服务器的主备切换，达到高可用的目的。

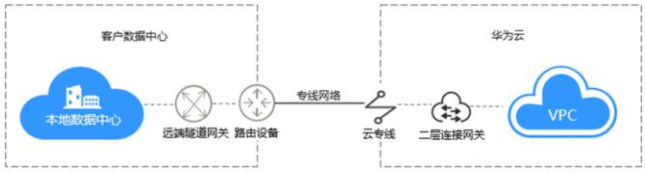


HUAWEI

- 虚拟IP的典型组网1：HA高可用模式；虚拟IP的典型组网2：高可用负载均衡集群。

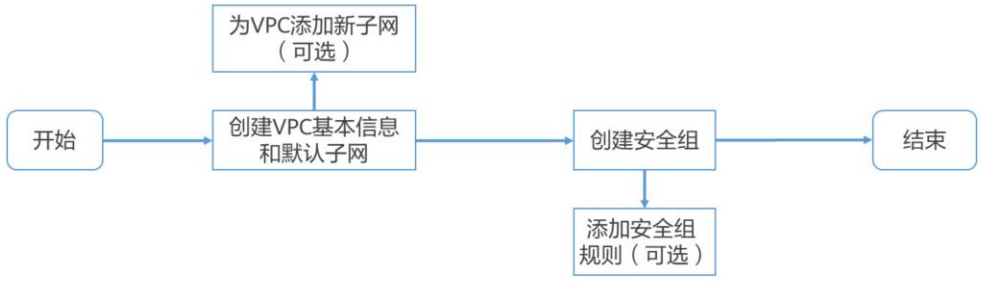
VPC - 二层连接网关

- 二层连接网关（Layer 2 Connection Gateway）是一种虚拟隧道网关，可基于云专线网络建立云上与云下之间的二层网络，解决云上和云下网络二层互通问题，允许用户在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。



- 通过云专线/VPN，建立的是云上与云下的三层网络通道，要求云上与云下子网网段不重叠。而当数据中心与云上子网网段相同，且需要云上与云下服务器在该相同子网网段互通时，可以通过二层连接网关来解决云上与云下二层网络通信问题。
- 二层连接网关作为虚拟私有云的隧道网关，与用户本地数据中心侧的隧道网关对应，可基于云专线/VPN网络使虚拟私有云与用户数据中心之间建立二层网络。
- 二层连接可将虚拟私有云的子网接入到二层连接网关中，并指定二层连接网关与企业数据中心侧的隧道网关建立连接，使虚拟私有云的子网与企业数据中心侧的子网建立二层通信。

VPC的配置流程



HUAWEI

- 在配置VPC之前，更重要的是根据业务需求做网络规划，确定需要用的网段在VPN和专线等场景网段不冲突，子网空间充足。
- 网络安全需要考虑不同业务对外的访问策略，将权限最小化，例如安全组只放通哪些源IP和端口。

VPC的配置 - 子网

- 申请VPC时会创建默认子网，当默认子网不能满足需求时，可以创建新的子网。
- 子网默认配置DHCP协议，即使用该VPC的弹性云服务器启动后，会通过DHCP协议自动获取到IP地址。
- 可用区：可用区是指在同一地域内，电力和网络互相独立的物理区域。

HUAWEI

- 网段：VPC的地址范围，VPC内的子网地址必须在VPC的地址范围内。目前支持网段范围：10.0.0.0/8~24、172.16.0.0/12~24、192.168.0.0/16~24。
- DNS服务器地址：默认情况下使用网络外部DNS服务器地址，如果需要修改DNS服务器地址，请确保配置的DNS服务器地址可用。
- DHCP（动态主机配置协议）：是一个局域网的网络协议。指的是由服务器控制一段IP地址范围，客户机登录服务器时就可以自动获得服务器分配的IP地址和子网掩码。

VPC的配置 - 安全组

- 每个用户都有一个默认的安全组，用户也可自行创建或在默认安全组中自定义添加新的出方向、入方向安全组规则。
- 入方向：指从外部访问安全组规则下的弹性云服务器。
- 出方向：指安全组规则下的弹性云服务器访问安全组外的实例。
- 默认安全组规则

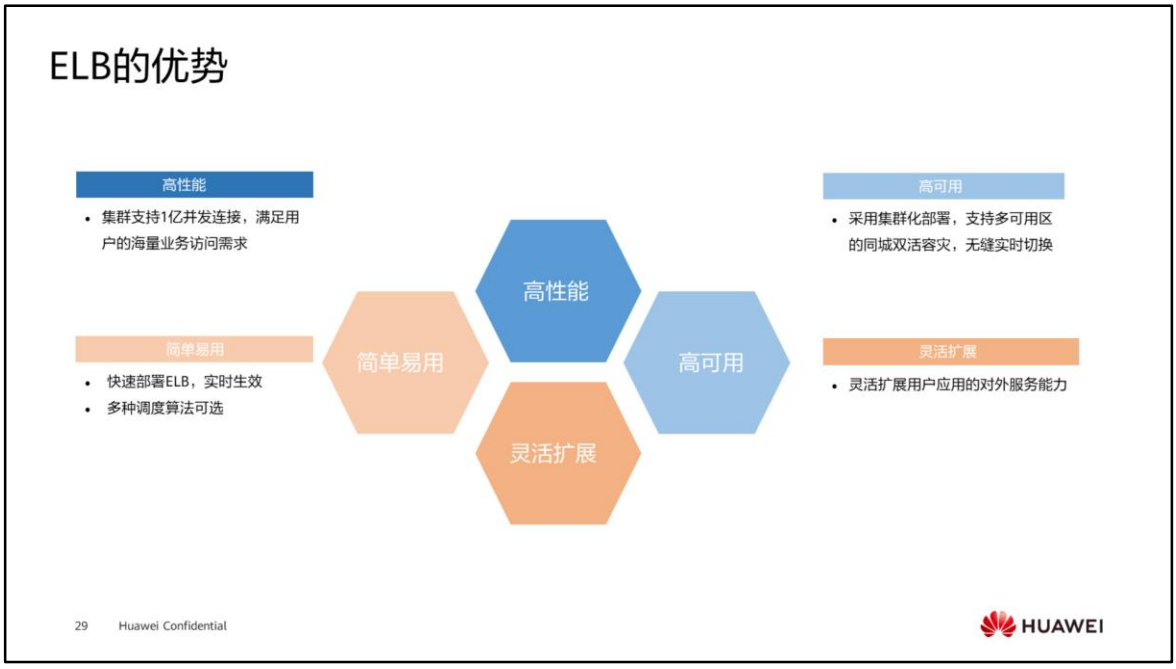
HUAWEI

- 用户无法删除默认安全组，但可以修改默认安全组的规则。
- 安全组需在网络互通的情况下生效。若实例属于不同VPC，但同属于一个安全组，此时实例不能互通。用户可以使用对等连接等产品建立VPC连接互通，安全组才能对不同VPC内实例的流量进行访问控制。
- 不同安全组内的弹性云服务器内网互通：在同一个VPC内，用户需要将某个安全组内一台弹性云服务器上的资源拷贝到另一个安全组内的弹性云服务器上时，可以将两台弹性云服务器设置为内网互通后再拷贝资源。同一个VPC内，在同一个安全组内的弹性云服务器默认互通。但是，在不同安全组内的弹性云服务器默认无法通信，此时需要添加安全组规则，使得不同安全组内的弹性云服务器内网互通。

目录

什么是弹性负载均衡（ELB）

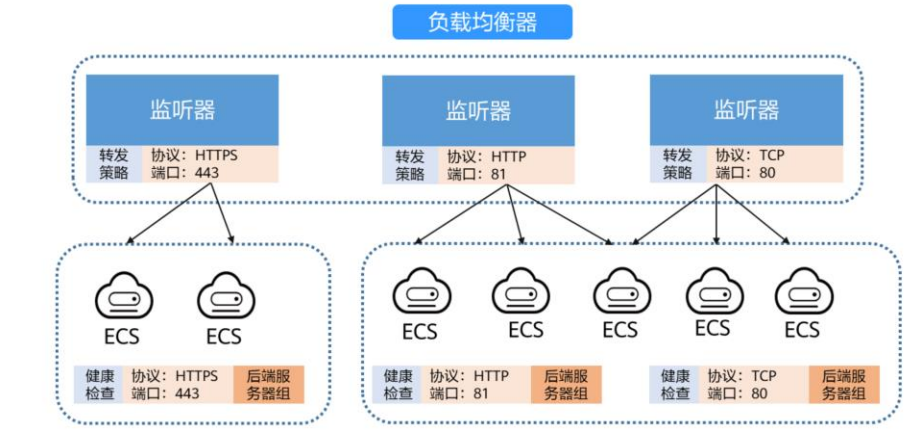
- 弹性负载均衡（Elastic Load Balance，ELB）是将访问流量根据分配策略分发到后端多台服务器的流量分发控制服务。弹性负载均衡可以通过流量分发扩展应用系统对外的服务能力，同时通过消除单点故障提升应用系统的可用性。



- ELB的优势：
  - 高性能：集群支持1亿并发连接，满足用户的海量业务访问需求
  - 高可用：采用集群化部署，支持多可用区的同城双活容灾，无缝实时切换
  - 灵活扩展：根据应用流量自动完成分发，与弹性伸缩服务无缝集成，灵活扩展用户应用的对外服务能力
  - 简单易用：快速部署，实时生效，支持多种协议、多种调度算法可选，用户可以高效地管理和调整分发策略

ELB的产品架构

- 弹性负载均衡主要由3部分组成：负载均衡器、监听器和后端服务器组。

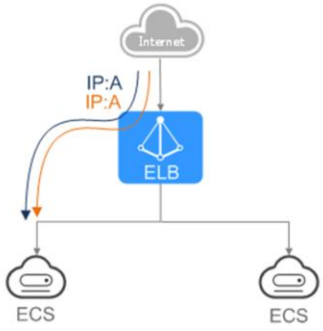


HUAWEI

- 弹性负载均衡由以下3部分组成：
  - 负载均衡器：接受来自客户端的传入流量并将请求转发到一个或多个可用区中的后端服务器
  - 监听器：弹性负载均衡器可添加一个或多个监听器。监听器使用用户配置的协议和端口检查来自客户端的连接请求，并根据用户定义的分配策略将请求转发到一个后端服务器组里的后端服务器
  - 后端服务器：每个监听器会绑定一个后端服务器组，后端服务器组中可以添加一个或多个后端服务器。后端服务器组使用用户指定的协议和端口号将请求转发到一个或多个后端服务器。可以为后端服务器配置流量转发权重，但不能为后端服务器组配置权重。用户可以开启健康检查功能，对每个后端服务器组配置运行状况进行检查。当后端某台服务器健康检查出现异常时，弹性负载均衡会自动将新的请求分发到其它健康检查正常的后端服务器上；而当该后端服务器恢复正常运行时，弹性负载均衡会将其自动恢复到弹性负载均衡服务中

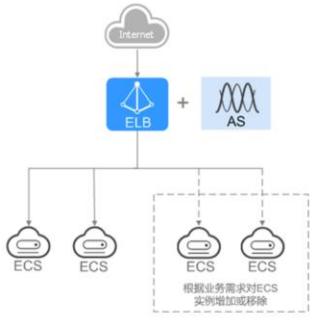
应用场景 - 高访问量业务进行流量分发

- 场景描述：对于业务量访问较大的业务，可以通过ELB设置相应的分配策略，将访问量均匀地分到多个后端服务器处理。例如大型门户网站，移动应用市场等。同时用户还可以开启会话保持功能，保证同一个客户请求转发到同一个后端服务器，从而提升访问效率。



应用场景 - 为潮汐业务弹性分发流量

- 场景描述：对于存在潮汐效应的业务，结合弹性伸缩服务，随着业务量的增长和收缩，弹性伸缩服务会自动增加或者减少ECS实例的数量，而负载均衡服务会根据流量分发、健康检查等策略灵活地使用ECS实例资源，在资源弹性的基础上大大提高资源可用性。

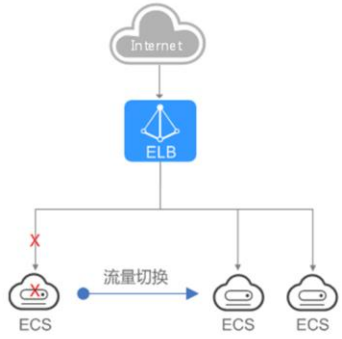


HUAWEI

- 潮汐效应在这里指的是某些业务在不同时间段有明显高低起伏的场景。

应用场景 - 消除单点故障

- 场景描述：对于可靠性有较高要求的业务，可以在负载均衡器上添加多个后端云服务器。负载均衡器会通过健康检查及时发现并屏蔽有故障的云服务器，并将流量转发到其他正常运行的后端云服务器，确保业务不中断。

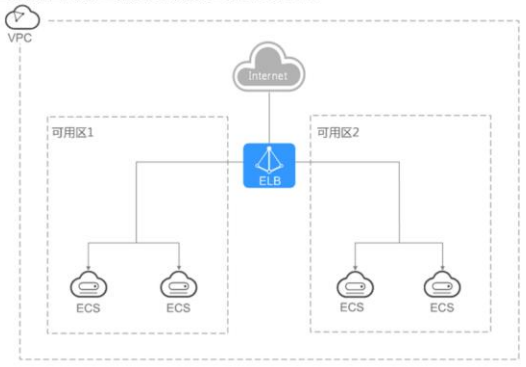


HUAWEI

- 单点故障（Single Point of Failure，SPOF）是指系统中一点失效，就会让整个系统无法运作的部件，换句话说，单点故障即会导致整体故障。 高可用性或者高可靠度的系统（商务系统、软件系统或工业系统）不会希望有单点故障造成整体故障的情形。

应用场景 - 实现业务跨可用区容灾部署

- 场景描述：对于可靠性和容灾有很高要求的业务，弹性负载均衡可将流量跨可用区进行分发，建立实时的业务容灾部署。即使出现某个可用区网络故障，负载均衡器仍可将流量转发到其他可用区的后端云服务器进行处理。

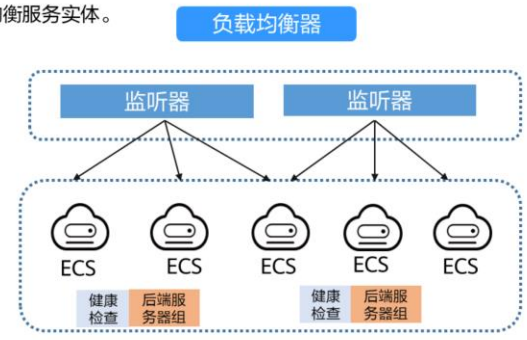


HUAWEI

- 是否将资源放在同一可用区内，主要取决于用户对容灾能力和网络时延的要求：
  - 如果应用需要较高的容灾能力，建议将资源部署在同一区域的不同可用区内
  - 如果应用要求实例之间的网络延时较低，则建议将资源创建在同一可用区内
- 若用户将业务跨可用区部署，弹性负载均衡可将流量跨可用区进行分发，建立实时的业务容灾部署。

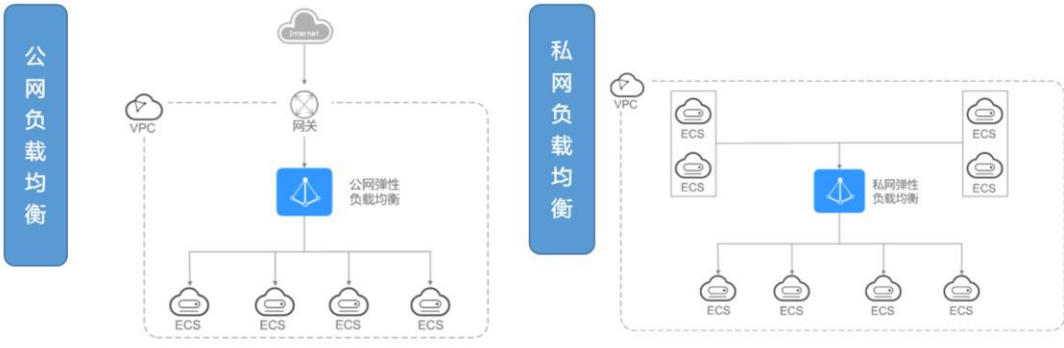
ELB的相关概念

- **负载均衡器：**负载均衡器是指用户创建的承载业务的负载均衡服务实体。
- **监听器：**监听器负责监听负载均衡器上的请求，根据配置的流量分配策略，分发流量到后端云服务器。
- **后端服务器组：**把具有相同特性的后端服务器放在一个组，负载均衡实例进行流量分发时，流量分配策略以后端服务器组为单位生效。
- **健康检查：**健康检查功能用于检查后端服务器组中服务器的状态，确保流量分发到后端服务器后能够正常访问，从而提高业务的可靠性。



ELB - 负载均衡器

- 负载均衡器是指用户创建的承载业务的负载均衡服务实体。常见的负载均衡器按照网络类型分有公网、私网负载均衡2种。

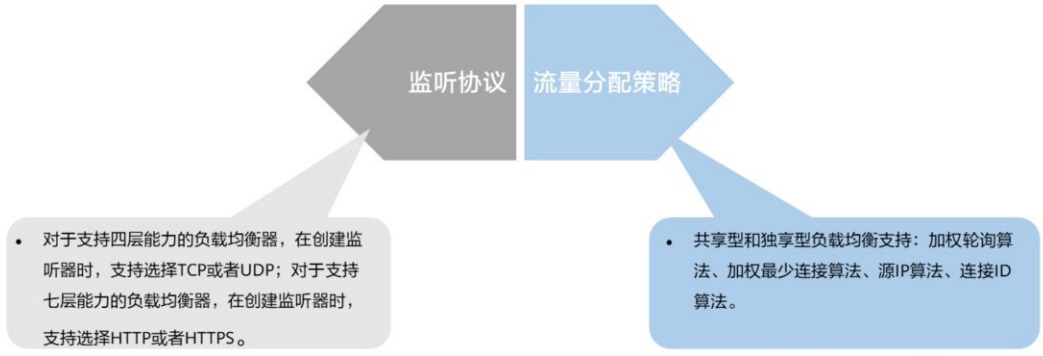


HUAWEI

- 公网负载均衡器通过公网IP对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端云服务器进行处理。
- 私网负载均衡器通过私网IP对外提供服务，将来自同一个VPC的客户端请求按照指定的负载均衡策略分发到后端进行处理。

ELB - 监听器

- 监听器负责监听负载均衡器上的请求，根据配置的流量分配策略，分发流量到后端云服务器处理。

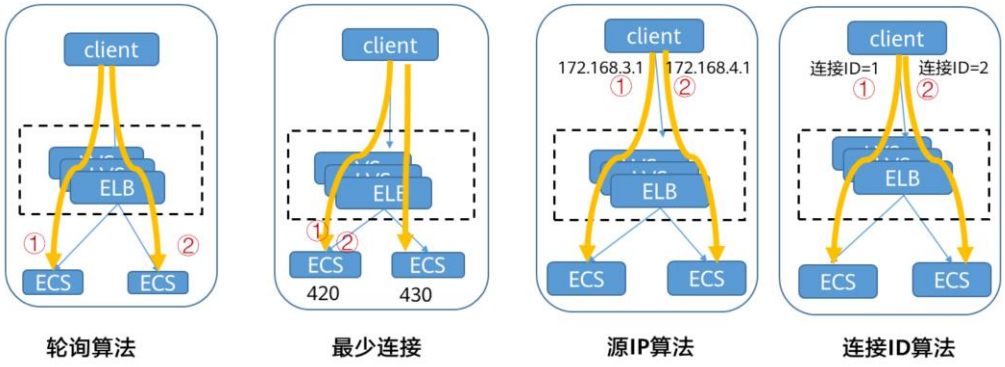


HUAWEI

- 负载均衡监听器通过指定的协议和端口进行流量转发。同时监听器将根据健康检查的配置自动检查其后端服务器的运行状况。如果发现某台服务器运行不正常，则会停止向该服务器发送流量，并重新将流量发送至正常运行的服务器。
- OSI七层协议模型主要是：应用层（Application）、表示层（Presentation）、会话层（Session）、传输层（Transport）、网络层（Network）、数据链路层（Data Link）、物理层（Physical）。
  - 第七层应用层协议包括：HTTP/SNMP/FTP/NFS/Telnet/SMTP
  - 第六层表示层协议包括：无
  - 第五层会话层协议包括：无
  - 第四层传输层协议包括：TCP/UDP
  - 第三层网络层协议包括：IP/ICMP
  - 第二层数据链路层协议包括：FDDI/Ethernet/Arpanet//PDN/SLIP/PPP
  - 第一层物理层协议包括：IEEE 802.1A/IEEE 802.2到IEEE 802.11

ELB的使用 - 后端服务器组和监听调度

- 负载均衡器会将客户端的请求转发给后端服务器处理。可以添加ECS实例作为负载均衡器的后端服务器，监听器使用用户配置的协议和端口检查来自客户端的连接请求，并根据用户定义的分配策略将请求转发到后端服务器组里的后端云服务器。具体策略如下：

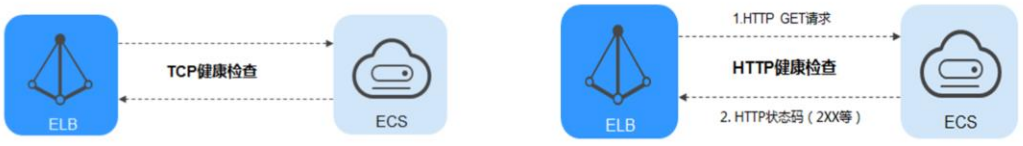


HUAWEI

- 用户可以设置后端服务器组内各后端服务器的转发权重。权重越高的后端服务器将被分配到更多的访问请求。三种算法支持权重设置：
  - 在加权轮询算法中，每台后端服务器的权重取值范围为【0，100】，新的请求不会转发到权重为0的后端。在非0的权重下，负载均衡器会将请求按权重值的大小分配给所有的后端服务器。当后端服务器的权重都设置为相等时，权重属性将不再生效，负载均衡器将按照简单的轮询策略分发请求
  - 在加权最少连接算法中，每台后端服务器的权重取值范围为【0，100】，新的请求不会转发到权重为0的后端。在非0的权重下，负载均衡器会通过overhead=当前连接数/权重 来计算每个服务器负载。每次调度会选择overhead最小的后端服务器
  - 在源IP算法中，每台后端服务器的权重取值范围为【0，100】，但是只做0和非0的区分。新的请求不会转发到权重为0的后端。在非0的权重下，由于使用了源IP算法，各个后端服务器的权重属性将不再生效，在一段时间内，同一个客户端的IP地址的请求会被调度至同一个后端服务器上
  - 在连接ID算法中，每台后端服务器的权重取值范围为【0，100】，但是只做0和非0的区分。新的请求不会转发到权重为0的后端。在非0的权重下，由于使用了连接ID算法，各个后端服务器的权重属性将不再生效，同一个连接ID的请求始终被派发至某特定的服务器。

ELB - 健康检查

- 健康检查功能用于检查后端服务器组中服务器的状态，确保流量分发到后端服务器时，能够正常访问，从而提高业务的可靠性。当异常的后端服务器恢复正常运行后，负载均衡器会将其自动恢复到负载均衡服务中，承载业务流量。

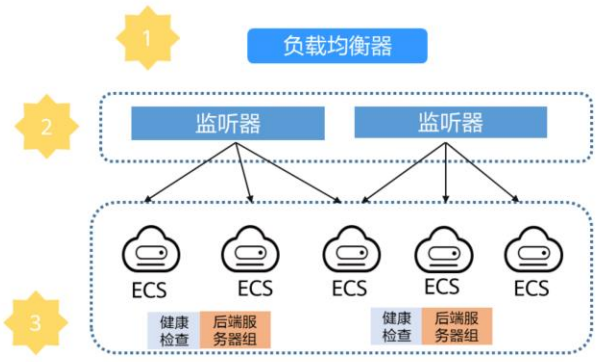


HUAWEI

- 健康检查的原理：
  - 对于四层（UDP）监听器，默认配置UDP健康检查，通过发送UDP探测报文获取后端服务器的状态信息。
  - 对于四层（TCP）和七层（HTTP/HTTPS）监听器，用户可以配置HTTP健康检查，通过HTTP GET请求来获取状态信息。
- 如果检查状态为Unhealthy则表示后端云服务器的服务异常，请检查服务器的配置。
- 安全组需放通网段100.125.0.0/16流量，否则无法进行健康检查。
- UDP的检查健康只能使用在UDP的后端云服务器组上。

ELB的配置流程

1. **创建负载均衡器：**
   - 购买弹性负载均衡
   - 选择负载均衡类型
   - 网络配置
2. **添加监听器：**
   - 选择目标负载均衡
   - 配置协议和端口号
3. **添加后端服务器组：**
   - 分配策略类型
   - 配置健康检查



HUAWEI

- 负载均衡监听器通过指定的协议和端口进行流量转发。同时监听器将根据健康检查的配置自动检查其后端云服务器的运行状况。如果发现某台云服务器运行不正常，则会停止向该云服务器发送流量，并重新将流量发送至正常运行的云服务器。

ELB的配置 - 创建负载均衡器

- 在使用负载均衡前，需要根据业务规划待创建负载均衡器的区域、类型、协议以及后端服务器等。

HUAWEI

- 在管理控制台左上角单击图标，选择区域和项目。
- 选择“服务列表 > 网络 > 弹性负载均衡”。
- 在“负载均衡器”界面单击“购买弹性负载均衡”，根据界面提示配置参数。
- 单击“立即购买”。
- 确认配置信息，并单击“提交”。
- 创建完成后，在“负载均衡器”界面，选择对应的区域即可看到新建的负载均衡器。

ELB的配置 - 添加监听器

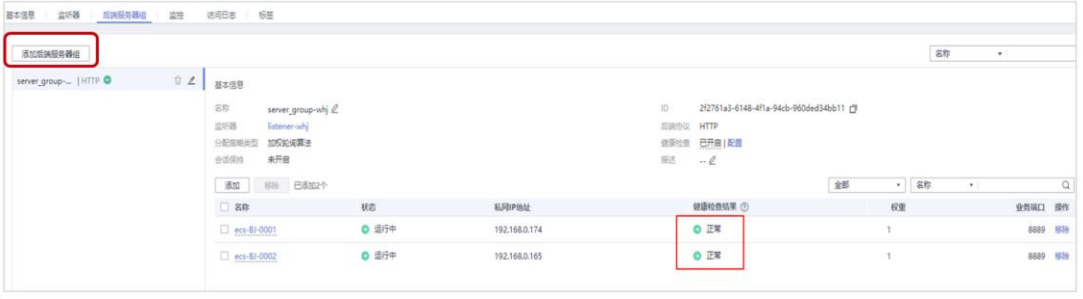
- 创建负载均衡器后，需要为负载均衡器配置监听器。监听器负责监听负载均衡器上的请求，根据配置流量分配策略，分发流量到后端服务器处理。

HUAWEI

- 前端协议/端口：负载分发的协议和端口。
- 获取客户端IP：
  - 开启此开关，后端服务器可以获取到客户端的真实IP地址。
  - 独享型负载均衡默认开启，且不可关闭。

ELB的配置 - 添加后端服务器组

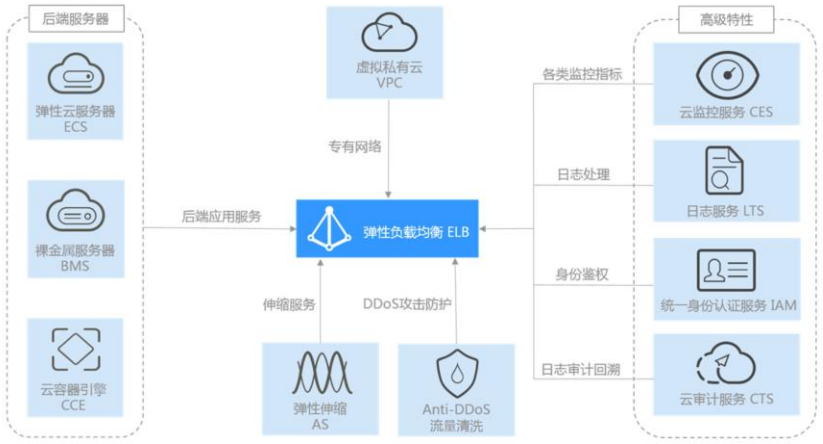
- 由于负载均衡器会将客户端的请求转发给后端服务器处理，因此，用户可以添加ECS实例作为负载均衡器的后端服务器。



HUAWEI

- 负载均衡采用的算法：
  - 加权轮询算法：根据服务器的权重，按顺序依次将请求分发给不同的服务器。它用相应的权重表示服务器的处理性能，按照权重的高低以及轮询方式将请求分配给各服务器，相同权重的服务器处理相同数目的连接数。
  - 加权最少连接：最少连接是通过当前活跃的连接数来估计服务器负载情况的一种动态调度算法。加权最少连接就是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。
  - 源IP算法：相同的源IP地址的请求始终被分发到相同的服务器处理。
  - 连接ID：同一个连接ID的请求始终被派发至某特定的服务器。

ELB其它服务的关系



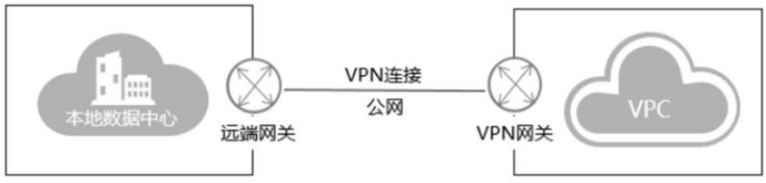
HUAWEI

- 通过相关计算服务部署用户业务，并接收ELB分发的访问流量。
- 创建ELB时需要使用虚拟私有云服务创建的弹性公网IP、带宽。
- 当配置了负载均衡服务后，弹性伸缩在添加和移除云服务器时，自动在负载均衡服务中添加和移除云服务器。
- 需要统一身份认证IAM提供鉴权。
- 使用云审计服务记录弹性负载均衡服务的资源操作。
- 当用户开通了弹性负载均衡服务后，无需额外安装其他插件，即可在云监控查看对应服务的实例状态。
- 当用户购买了Anti-DDoS服务后，配置了负载均衡器的公网IP，确保了弹性负载均衡服务免受外部攻击，提高安全可靠性。
- 配置访问日志时需要您对接云日志服务，查看和分析对七层负载均衡HTTP和HTTPS进行请求的详细访问日志记录。

目录

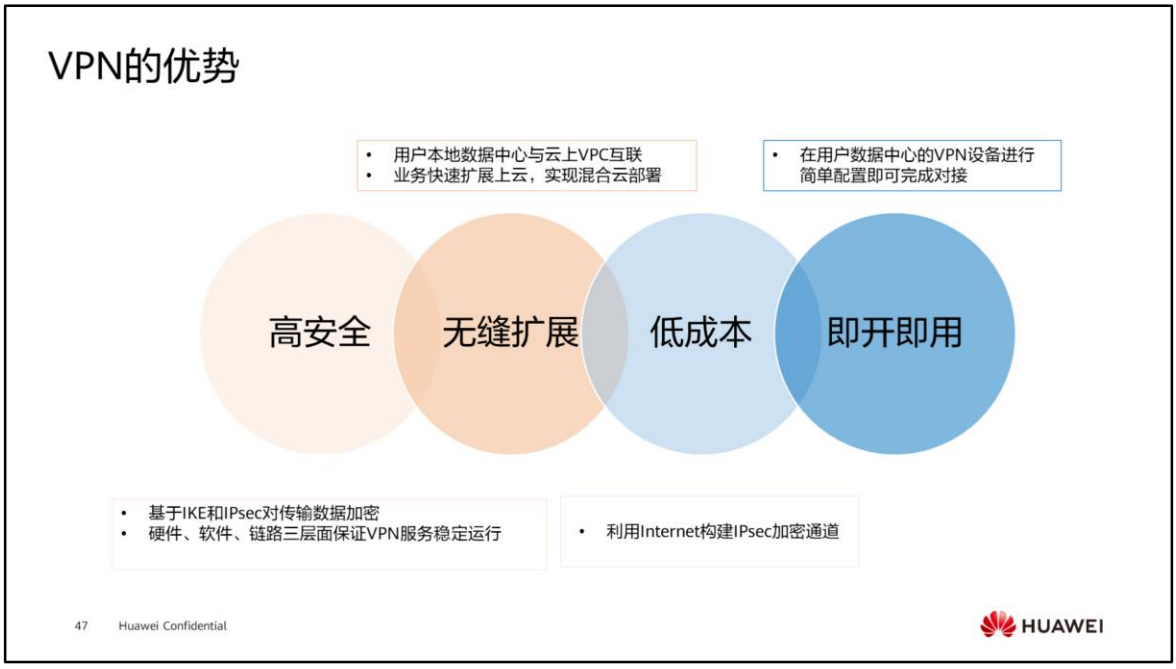
什么是虚拟专用网络（VPN）

- 虚拟专用网络（Virtual Private Network，以下简称VPN），用于在远端用户和虚拟私有云（Virtual Private Cloud，以下简称VPC）之间建立一条安全加密的公网通信隧道。当远端用户需要访问VPC的业务资源时，可以通过VPN连通VPC。



HUAWEI

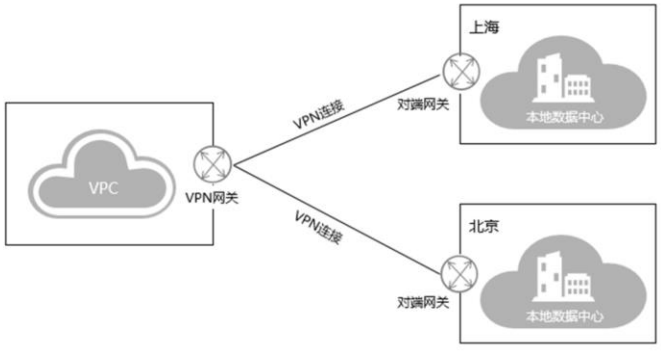
- VPN的隧道协议主要有三种：PPTP/L2TP/IPSec。



- VPN的优势：
  - 高安全：采用华为专业设备，基于IKE和IPsec对传输数据加密，提供了电信级的高可靠性机制，从硬件、软件、链路三个层面保证VPN服务的稳定运行。
  - 无缝扩展资源：将用户本地数据中心与云上VPC互联，业务快速扩展上云，实现混合云部署。
  - 连通成本低：利用Internet构建IPsec加密通道，使用费用相对云专线服务更便宜。
  - 即开即用：即开即用，部署快速，实时生效，在用户数据中心的VPN设备进行简单配置即可完成对接。

VPN的组网

- VPN由VPN网关和VPN连接组成，VPN网关提供了虚拟私有云的公网出口，与用户本地数据中心侧的远端网关对应。VPN连接则通过公网加密技术，将VPN网关与远端网关关联，使本地数据中心与虚拟私有云通信，更快速、安全地构建混合云环境。

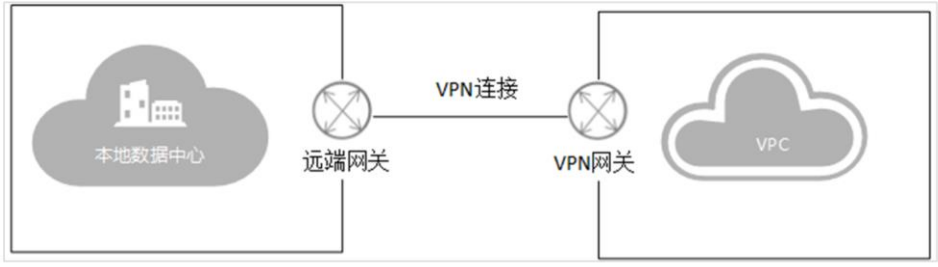


HUAWEI

- VPN的组成部分：
  - VPN网关：VPN网关是虚拟私有云中建立的出口网关设备，通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。VPN网关需要与用户本地数据中心的远端网关配合使用，一个本地数据中心绑定一个远端网关，一个虚拟私有云绑定一个VPN网关。VPN支持点到点或点到多点连接，因此，VPN网关与远端网关为一对一或一对多的关系。
  - VPN连接：VPN连接是一种基于Internet的IPsec加密技术，可帮助用户快速构建VPN网关和用户本地数据中心远端网关之间的安全、可靠的加密通道。当前VPN连接支持IPsec VPN协议。VPN连接使用IKE和IPsec协议对传输数据进行加密，保证数据安全可靠，且VPN连接使用公网技术，更加节约成本。

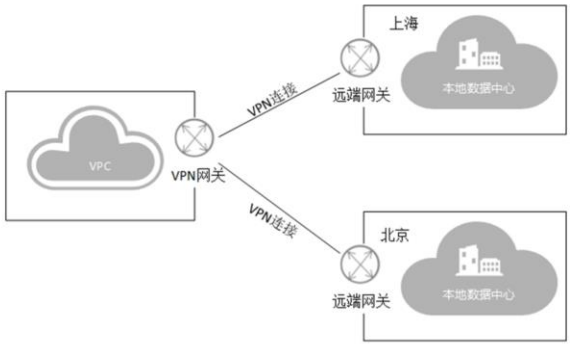
应用场景 - 单站点VPN连接

- 通过建立VPN将本地数据中心和VPC快速连接起来，构建混合云（线下到线上）。



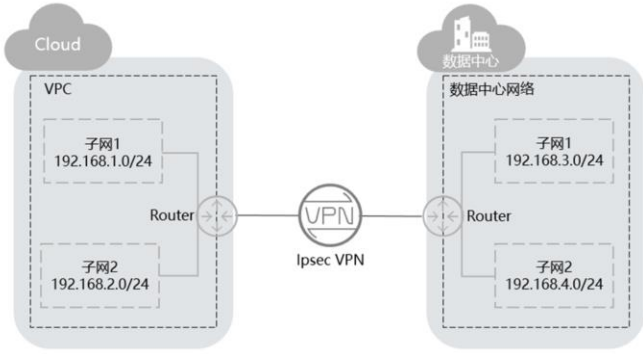
应用场景 - 多站点VPN连接

- 通过建立VPN将多个本地数据中心和VPC快速连接起来，构建混合云（线上）。



VPN的相关概念 - IPSec VPN

- IPSec VPN是一种加密的隧道技术，通过使用加密的安全服务在不同的网络之间建立保密而安全的通讯隧道。VPN服务使用的就是IPSec VPN技术。

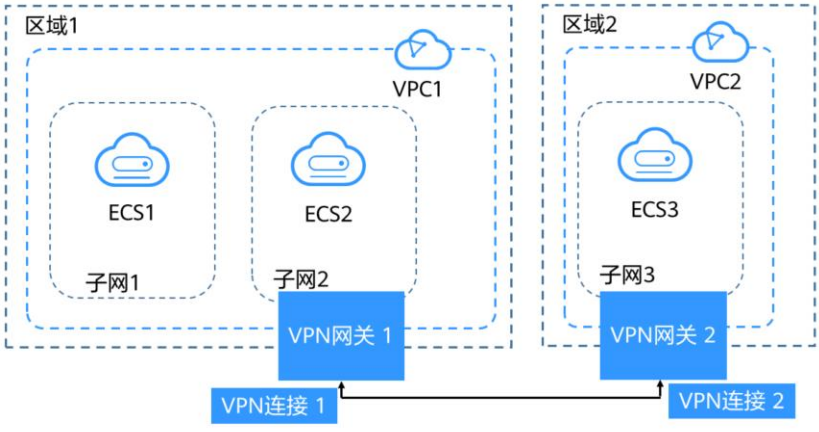


HUAWEI

- 如图所示，假设用户在云中申请了VPC，且同时申请了2个子网（192.168.1.0/24，192.168.2.0/24），在用户的数据中心Router下也有2个子网（192.168.3.0/24，192.168.4.0/24）。此时，用户可以直接通过VPN使VPC内的子网与数据中心的子网互相通信。

VPN的配置流程

- 用户可以在管理控制台分别创建VPN网关和VPN连接。



HUAWEI

- VPN为两个不同区域间网络互通，以图中为例。
- 区域1中ECS2需要与区域2中的ECS3进行通信，需要打通区域1 和区域2之间的VPN。
- 步骤1：创建区域1的VPN网关，配置计费模式、区域为区域1、VPC1、带宽、计费方式和加密策略等；
- 步骤2：创建区域1的VPN连接，配置本端子网，选择为子网2，配置远端子网，输入子网3的网段，配置远端网关（此处由于VPN网关2 未创建，需填写随意网络，后边再次修改）；
- 步骤3：创建区域2的VPN网关，配置计费模式、区域为区域2、VPC2、带宽、计费方式和加密策略等；
- 步骤4：创建区域2的VPN连接，配置本端子网，选择为子网3，配置远端子网，输入子网2的网段，配置远端网关（输入VPN网关1 地址）；
- 步骤5：修改VPN连接1 中的远端网关地址为VPN网关2地址；
- 步骤6：测试ECS2和ECS3的连通性，查看VPN连接状态。

VPN配置 - VPN网关

- 如果需要将VPC中的弹性云服务器和现有数据中心或私有网络连通，需要先创建VPN网关。

- VPN网关：
  - 用户根据需要修改VPN网关名称和描述信息，当VPN网关带宽不能满足需求时，可修改VPN网关带宽，当VPN网关所关联的VPN连接数不能满足需求时，可修改VPN网关规格。当用户需要将按带宽计费VPN网关的计费方式修改为包周期时，可修改VPN网关规格的计费方式。
  - 当无需使用VPN网关时，可删除VPN网关。已被VPN连接使用的VPN网关不可删除，请先删除相关的VPN连接，再删除VPN网关。
- 虚拟私有云：VPN接入的VPC名称。
- 类型：VPN类型。默认为选择“IPsec”。
- 计费方式：支持两种计费方式：按带宽计费/按流量计费。
  - 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。
  - 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。
- 带宽大小：
  - 本地VPN网关的带宽大小（单位Mbit/s），为所有基于该网关创建的VPN连接共享的带宽，VPN连接带宽总和不超过VPN网关的带宽。
  - 在VPN使用过程中，当网络流量超过VPN带宽时有可能造成网络拥塞导致VPN连接中断，请用户提前做好带宽规划。
  - 可以在CES监控中配置告警规则对带宽进行监控。

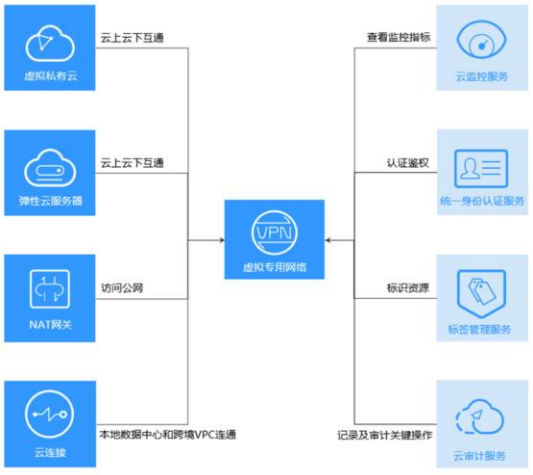
VPN配置 - VPN连接

- 如果需要将VPC中的弹性云服务器和用户的数据中心或私有网络连通，创建VPN网关后需要创建VPN连接。

HUAWEI

- VPN连接：
  - VPN连接是建立VPN网关和外部数据中心VPN网关之间的加密通道。当VPN连接的网络参数变化时，可以修改VPN连接。
  - 当无需使用VPN网络、需要释放网络资源时，可删除VPN连接。当购买的VPN网关计费模式为按需时，删除最后一个VPN连接时，会同时删除绑定的VPN网关。
- VPN网关：VPN连接挂载的VPN网关名称。
- 本端子网：VPC内需要与用户数据中心或者私有网络互通的子网。支持以下方式设置本端子网（选择子网；手动输入网段）。
- 远端网关：用户数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。
- 远端子网：用户数据中心或私有网络中需要与VPC通信的子网地址。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段重合。
- 预共享密钥（Pre Shared Key）：取值范围为6～128位。此项配置在VPC的VPN和用户数据中心的VPN中，配置需要一致。

VPN与其他云服务的关系



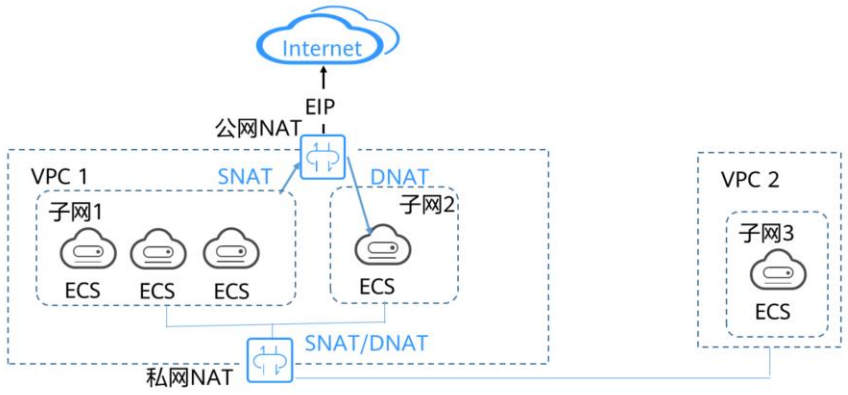
HUAWEI

- 通过VPC服务，创建VPC，本地数据中心才可以通过VPN上云。通过VPC服务，定义安全组中的规则，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。
- 通过云连接服务，可以实现本地数据中心和跨境VPC之间的稳定网络连通。
- 通过NAT网关服务，可以实现本地数据中心服务器访问公网或为公网提供服务。
- 通过VPC服务，定义安全组中的规则，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
- 通过云监控服务，查看VPN资源的监控数据，还可以获取可视化监控图表。
- 通过IAM服务，针对用户在华为云上创建的VPN资源，向不同用户设置不同的使用权限，可以安全地控制华为云VPN资源的访问权限。
- 通过云审计服务，记录与VPN服务相关的操作事件。

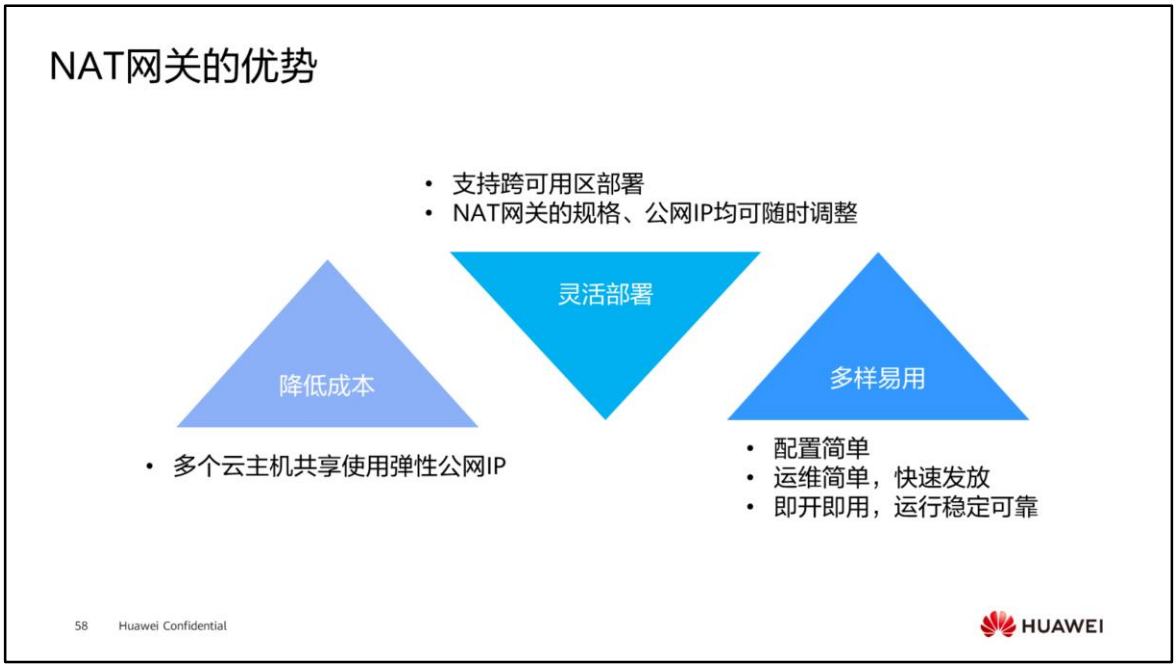
目录

什么是NAT网关

- NAT网关（NAT Gateway）能够为VPC内的计算实例提供网络地址转换服务，使多个计算实例共享弹性IP访问Internet。NAT网关可分为公网NAT网关和私网NAT网关。

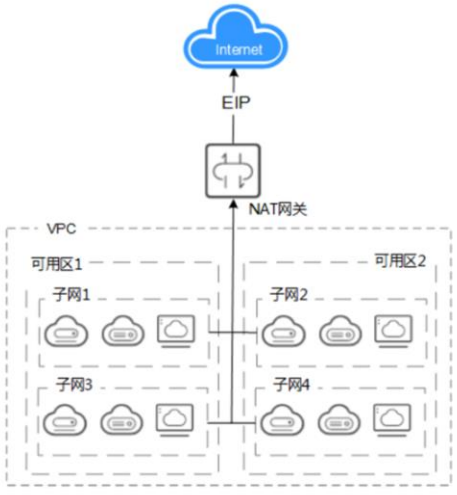


- 公网NAT网关能够为VPC内的弹性云服务器提供SNAT和DNAT功能，通过灵活简易的配置，即可轻松构建VPC的公网出入口。
- 私网NAT网关能够为虚拟私有云内的云主机提供网络地址转换服务，使多个云主机可以共享私网IP访问用户本地数据中心（IDC）或其他虚拟私有云。同时，也支持云主机面向私网提供服务。



- NAT网关的优势：
  - 灵活部署：NAT网关支持跨可用区部署，可用性高，单个可用区的故障不会影响NAT网关的业务连续性。NAT网关的规格、公网IP均可随时调整
  - 多样易用：对NAT网关进行简单配置后，即可使用，运维简单，快速发放，即开即用，运行稳定可靠
  - 降低成本：当用户的私有IP地址通过NAT网关发送数据，或者应用面向互联网提供服务时，NAT网关服务将私有地址和公网地址进行转换。用户无需为云主机访问Internet购买多余的弹性公网IP和带宽资源，多个云主机共享使用弹性公网IP，有效降低成本。

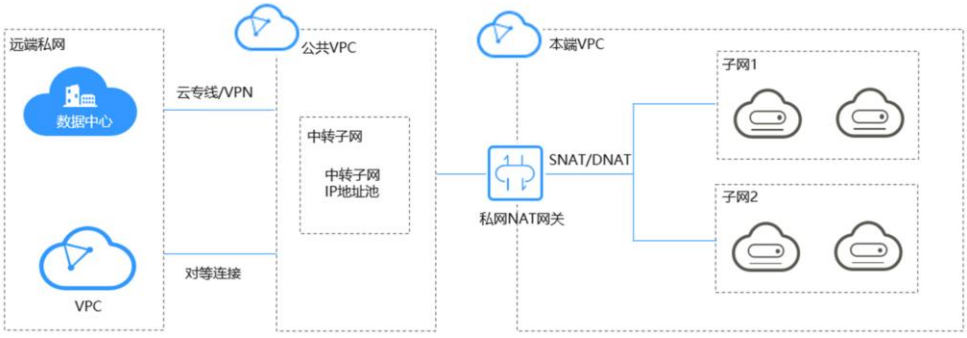
NAT网关的产品架构（公网NAT）



- 公网NAT网关分为SNAT和DNAT两个功能：
  - SNAT功能通过绑定弹性公网IP，实现私有IP向公有IP的转换，可实现VPC内跨可用区的多个云主机共享弹性公网IP，安全，高效地访问互联网
  - DNAT功能绑定弹性公网IP，可通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享弹性公网IP，为互联网提供服务

NAT网关的产品架构（私网NAT）

- 私网NAT网关能够为虚拟私有云内的云主机提供网络地址转换服务，使多个云主机可以共享私网IP访问用户本地数据中心（IDC）或其他虚拟私有云。

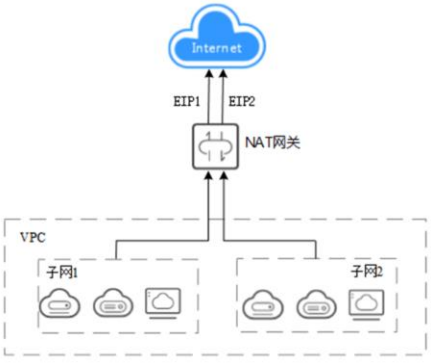


HUAWEI

- 中转子网：中转子网相当于一个中转网络，用户可以在中转子网中创建私网IP，即中转IP，使本端VPC中的云主机可以共享该私网IP访问用户IDC或其他远端VPC。
- 公共VPC：中转子网所在VPC。

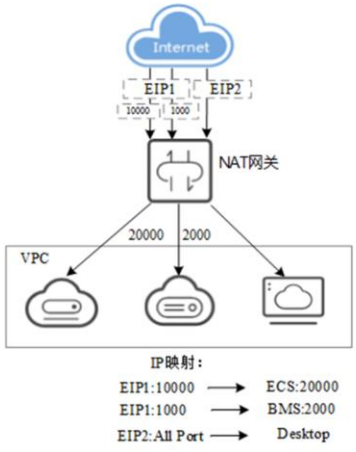
应用场景 - 使用SNAT访问公网（公网NAT）

- 场景描述：当VPC内的云主机需要访问公网，请求量大时，为了节省弹性公网IP资源并且避免云主机IP直接暴露在公网上，NAT网关可以为用户提供不同规格的连接数。根据业务规划，用户可以通过创建多条SNAT规则，来实现共享弹性公网IP资源。



应用场景 - 用DNAT为云主机面向公网提供服务（公网NAT）

- 场景描述：当VPC内的云主机需要面向公网提供服务时，可以使用NAT网关的DNAT功能。

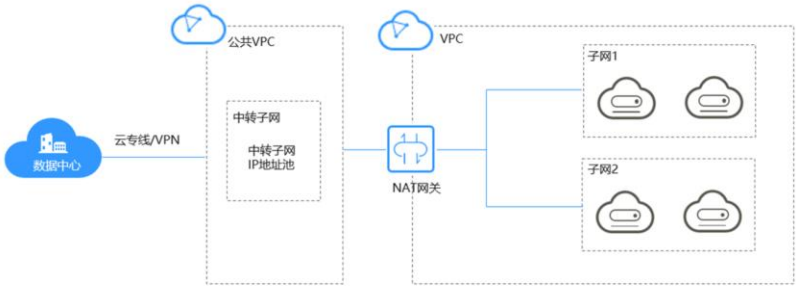


HUAWEI

- DNAT功能绑定弹性公网IP，可通过端口映射方式，NAT网关会将以指定的协议和端口访问该弹性公网IP的请求转发到目标云主机实例的指定端口上。也可通过IP映射方式，为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云主机实例上。使多个云主机共享弹性公网IP和带宽，精确地控制带宽资源。
- 一个云主机配置一条DNAT规则，如果有多个云主机需要为公网提供服务，可以通过配置多条DNAT规则来共享一个或多个弹性公网IP资源。

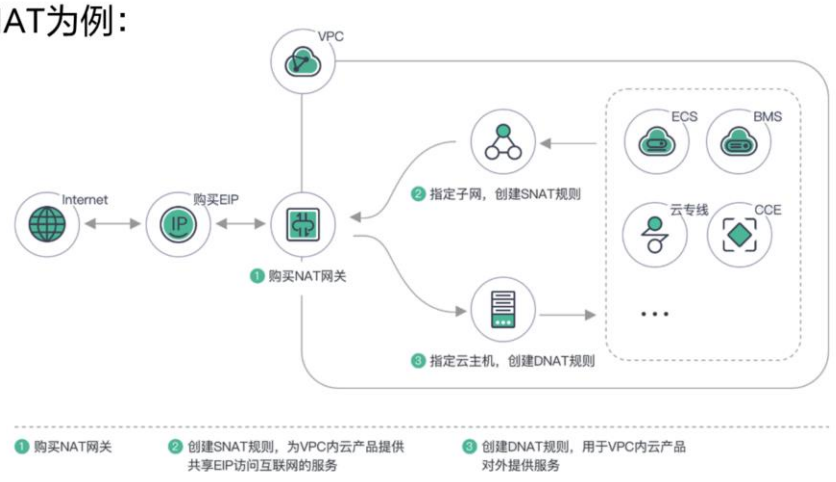
应用场景 - 企业网络统一管理（私网NAT）

- 场景描述：如公司总部要求所有分公司、部门将各自的地址映射为符合企业安全规范的统一地址段进行互通，用户可使用私网NAT，使企业上云后无需对网络做任何更改即可保持原有方式互通。



NAT网关的申请流程

以公网NAT为例：

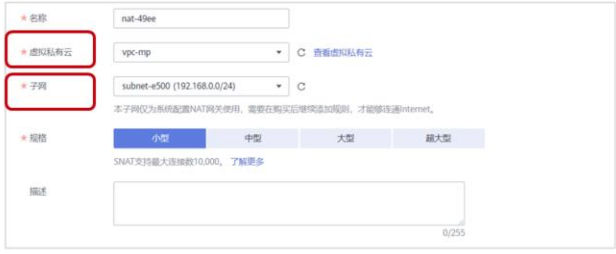


HUAWEI

- 在使用公网NAT之前需要准备弹性IP
- SNAT：SNAT功能通过绑定弹性公网IP，实现私有IP向公有IP的转换，可实现VPC内跨可用区的多个云主机共享弹性公网IP，安全，高效地访问互联网。
- DNAT：DNAT功能绑定弹性公网IP，可通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享弹性公网IP，为互联网提供服务。
- SNAT规则和DNAT规则一般面向不同的业务，如果使用相同的EIP，会面临业务相互抢占问题，请尽量避免。
- SNAT规则不能和全端口的DNAT规则共用EIP。

购买NAT网关

- 购买公网NAT网关必须指定公网NAT网关所在VPC、子网、NAT网关规格。
- 确认VPC默认路由表下是否存在0.0.0.0/0的默认路由。若存在，请在公网NAT网关创建成功后为此网关添加一条不同的路由或在新路由表中创建0.0.0.0/0的默认路由。



HUAWEI

- 子网：
  - 公网NAT网关所属VPC中的子网。
  - 子网至少有一个可用的IP地址。
  - 子网仅在购买公网NAT网关时可以选择，后续不支持修改。
- 规格：
  - 公网NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。

SNAT规则配置

- 当虚拟私有云中的云主机需要访问公网时，选择虚拟私有云；当云专线/VPN本地数据中心端的服务器需要访问公网时，选择云专线/云连接。

HUAWEI

- 场景：
  - 公网NAT网关创建成功后，需要创建SNAT规则。通过创建SNAT规则，虚拟私有云子网中全部或部分云主机可以通过共享弹性公网IP访问公网，或云专线/VPN用户侧端该网段下的服务器可以通过共享弹性公网IP访问公网。
  - 一个子网对应一条SNAT规则，如果VPC中有多个子网需要访问公网，则可以通过创建多个SNAT规则实现共享一个或多个弹性公网IP资源。
- 弹性公网IP：
  - 用来提供互联网访问的公网IP。
  - 这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前NAT网关中SNAT规则上的弹性公网IP。
  - 可选择多条EIP添加在SNAT规则中。一条SNAT规则最多添加20个EIP。SNAT规则使用多个EIP时，业务运行时会随机选取其中的一个。

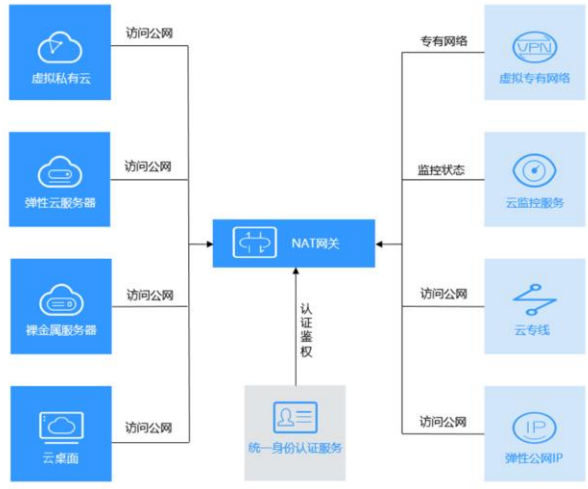
DNAT规则配置

- 虚拟私有云表示虚拟私有云中的云主机将通过DNAT的方式共享弹性公网IP，为公网提供服务；云专线/云连接表示通过云专线/云连接方式接入虚拟私有云本地数据中心中的服务器，将通过DNAT的方式访问公网。

HUAWEI

- 场景：
  - 公网NAT网关创建后，通过添加DNAT规则，则可以通过映射方式将用户VPC内的云主机对互联网提供服务。
  - 一个云主机的一个端口对应一条DNAT规则，如果有多个云主机需要为互联网提供服务，则需要创建多条DNAT规则。
- 公网端口：
  - 弹性公网IP的端口。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。
- 私网端口：
  - 在使用DNAT为云主机面向公网提供服务场景下，指云主机的端口号。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。
- 端口类型：
  - 所有端口：属于IP映射方式。此方式相当于为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云服务器实例上。
  - 具体端口：属于端口映射方式。公网NAT网关会将以指定协议和端口访问该弹性公网IP的请求转发到目标云主机实例的指定端口上。

NAT与其他服务的关系



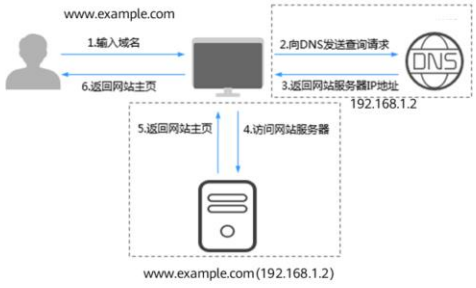
HUAWEI

- 通过云专线接入VPC的本地服务器，可以通过NAT网关访问公网或为公网提供服务。
- 通过VPN接入VPC的本地服务器，可以通过NAT网关访问公网或为公网提供服务。
- NAT网关可以为其他计算云服务或桌面云提供访问公网或者为公网提供服务的能力。
- 虚拟私有云内的弹性云服务器与Internet互连.
- EIP实现VPC中的云主机以NAT网关的形式共享弹性公网IP访问公网或为公网提供服务。
- 云监控服务查看NAT网关的监控数据，还可以获取可视化监控图表。
- 需要对华为云上创建的NAT网关资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。

目录

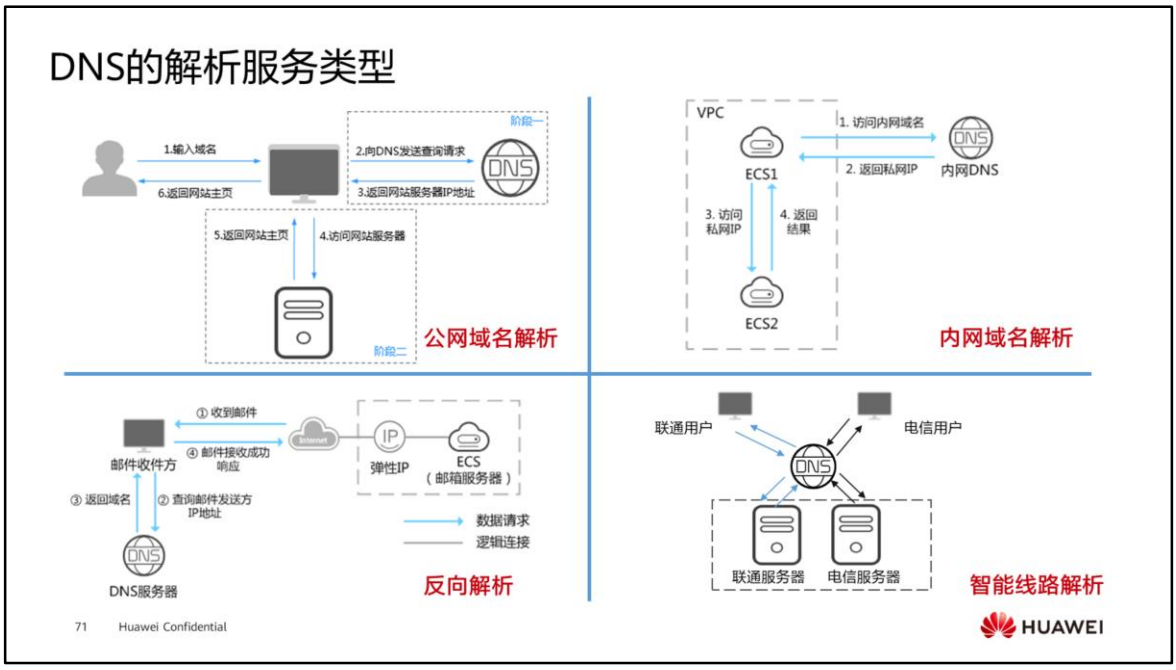
什么是DNS

- 域名解析服务（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。



HUAWEI

- 云解析服务（Domain Name Service，DNS）提供高可用、高扩展的DNS服务，把人们常用的域名（如www.example.com）转换成用于计算机连接的IP地址（如192.1.2.3）。云解析服务可以让用户直接在浏览器中输入域名，访问网站或Web应用程序。



- 公网域名解析：可以将公网域名与IP地址相关联，为用户提供基于Internet网络的域名解析服务，实现通过域名直接访问网站或者Web应用程序。公网域名解析是基于Internet网络的域名解析过程，可以把人们常用的域名（如www.example.com）转换成用于计算机连接的IP地址（如1.2.3.4）。公网域名解析支持通过直接在浏览器中输入域名，访问网站或Web应用程序。
- 内网域名解析：可以将在VPC内生效的内网域名与私网IP地址相关联，为用户的华为云上资源提供VPC内的域名解析服务。内网域名解析是基于VPC网络的域名解析过程，通过华为云内网DNS把域名（如ecs.com）转换成私网IP地址（192.168.1.1）。内网域名解析实现云服务器在VPC内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网DNS访问云上服务，如OBS、SMN等。
- 反向解析：支持通过IP地址反向获取该IP地址指向的域名，通常用于自建邮件服务器的场景，是提高邮箱IP和域名信誉度的必要设置。通常收件服务器在收到邮件时，会通过检测发件方邮箱的IP信誉度和域名信誉度，来判断是否为垃圾邮件。若收件服务器反向解析发件方IP地址无法获取邮箱域名，则会认为这是由恶意主机发送的垃圾邮件而拒收。因此，搭建邮箱服务器时，建议您为邮箱服务器的IP地址添加到域名的反向解析。如果没有为邮箱服务器添加反向解析记录，则收件方在收到邮件后，无法根据发件方的IP地址反向解析出邮箱域名。收件方会认为这是由恶意主机发送的垃圾邮件而选择拒收。因此，自建邮箱服务器时，为邮箱服务器的IP地址添加反向解析记录是必不可少的步骤。
- 智能线路解析：云解析服务的智能线路解析功能支持按运营商、地域等维度区分访问者IP的来源和类型，对同一域名的访问请求做出不同的解析响应，指向不同服务器的IP地址。当联通用户访问时，域名解析服务器返回联通服务器的IP地址；当电信用户访问时，返回电信服务器的IP地址，解决了跨网访问慢的难题，从而实现高效解析。还支持按IP网段划分访问者的自定义线路解析，可以更细粒度的设置解析线路，将访问者路由至不同的网站服务器。

域名格式和级别

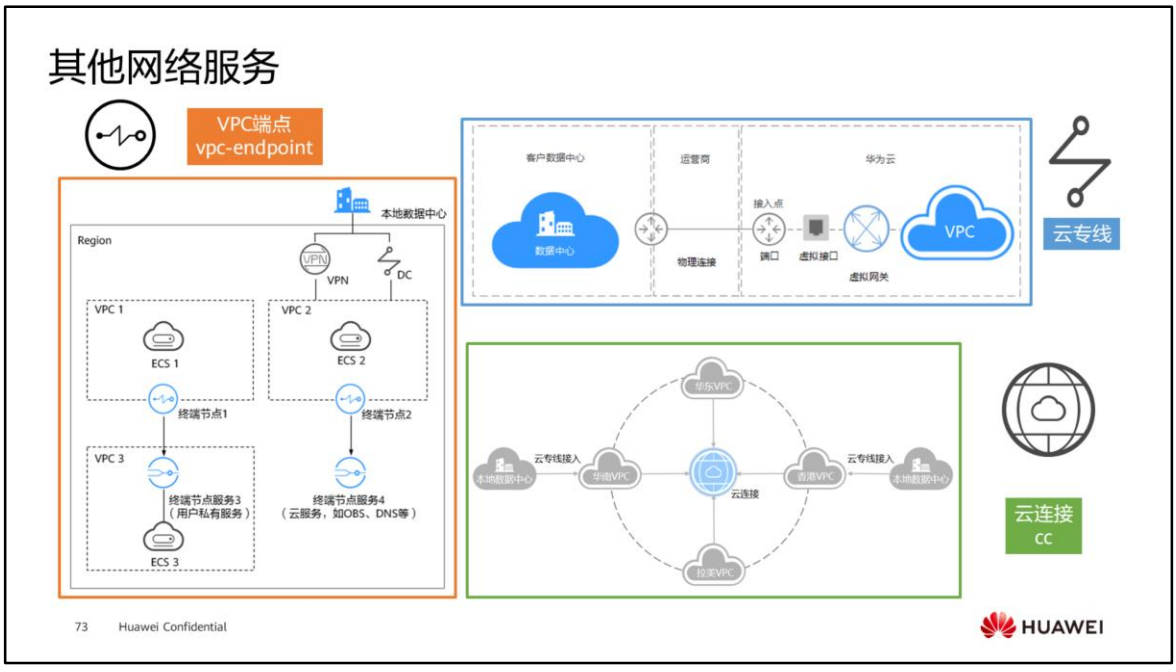
域名格式需满足如下要求：

- 域名以点号分隔成多个字符串
- 单个字符串由各国文字的特定字符集、字母、数字、连字符（-）组成，连字符（-）不得出现在字符串的头部或者尾部
- 单个字符串长度不超过63个字符
- 字符串间以点分割，且总长度（包括末尾的点）不超过254个字符

云解析服务定义域名级别如下：

- 根域名：.
- 顶级域名：.com，.net，.org，.cn等
- 主域名：即顶级域名的子域名，example.com，example.net，example.org等
- 二级域名：即主域名的子域名，abc.example.com，abc.example.net，abc.example.org等

- 华为云云解析服务支持创建主域名的一级子域名，比如创建example.com的子域名abc.example.com，或者example.com.cn的子域名abc.example.com.cn，不支持创建主域名的二级子域名，比如不支持创建def.abc.example.com，def.abc.example.com.cn这样的域名。



- VPC终端节点 VPCEP：终端节点（VPC Endpoint）可以在VPC内提供便捷、安全、私密的通道与终端节点服务（华为云服务、用户私有服务）进行连接，该服务使用华为云内部网络，无需弹性公网IP。
- 云专线（Direct Connect）：用于搭建用户本地数据中心与华为云VPC之间高速、低时延、稳定安全的专属连接通道，充分利用华为云服务优势的同时，继续使用现有的IT设施，实现灵活一体，可伸缩的混合云计算环境。
- 云连接（Cloud Connect）：能够提供一种快速构建跨区域VPC及云上多VPC与云下多数据中心之间的高速、优质、稳定的网络能力，帮助用户打造一张具有企业级规模和通信能力的全球云上网络。

思考题

1. （单选题）以下哪个概念不属于弹性负载均衡服务?
   A. 后端服务器组
   B. 监听器
   C. 负载均衡器
   D. NAT网关
2. （单选题）在同一区域（比如北京四的可用区1）VPC1与VPC2之间，以下说法中哪一项是正确的?
   A. 通过对等连接实现互通
   B. 彼此之间不可以互通
   C. 默认互通，但可以禁用
   D. 只能通过VPN实现互通

- D。
- A。

本章总结

- 本章介绍了网络基础知识和常见的网络云服务。通过学习，了解了网络的作用以及网络云服务的原理和应用场景。例如：VPC服务对应了企业内网，通过弹性IP服务，可将应用对外提供服务等等。只有掌握好网络云服务的原理和定位，我们才能够更好地为企业业务系统上云做准备。

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为云技术支持网站
  - https://support.huaweicloud.com/help-novice.html
- 华为云学院
  - https://edu.huaweicloud.com/

术语和缩略语

- ACL：Access Control Lists，访问控制列表
- AS：Autonomous Systems，自治域系统
- BGP：Border Gateway Protocol，边界网关协议
- CC：Cloud Connection，云连接
- DHCP：Dynamic Host Configuration Protocol，动态主机配置协议
- DNAT：Destination Network Address Translation，目的网络地址转换
- DNS：Domain Name Server，域名系统
- ECS：Elastic Cloud Server，弹性云服务器

术语和缩略语

- EIP：Elastic Internet Protocol，弹性公网IP
- ELB：Elastic Load Balance，弹性负载均衡
- HTTP：Hyper Text Transfer Protocol，超文本传输协议
- HTTPS：Hyper Text Transfer Protocol over Secure Socket Layer，超文本传输安全协议
- ICT：Information and Communication Technology，信息与通信技术
- IDC：Internet Data Center，互联网络数据中心
- IPSec：Internet Protocol Security，互联网安全协议
- NAT：Network Address Translation，网络地址转换

术语和缩略语

- SNAT：Source Network Address Translation，源网络地址转换
- TCP：Transmission Control Protocol，传输控制协议
- UDP：User Datagram Protocol，用户数据报协议
- VPC：Virtual Private Cloud，虚拟私有云
- VPCEP：Virtual Private Cloud Endpoint，虚拟私有云终端节点
- VPN：Virtual Private Network，虚拟私有网络
- WEB：World Wide Web，全球广域网

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

存储云服务

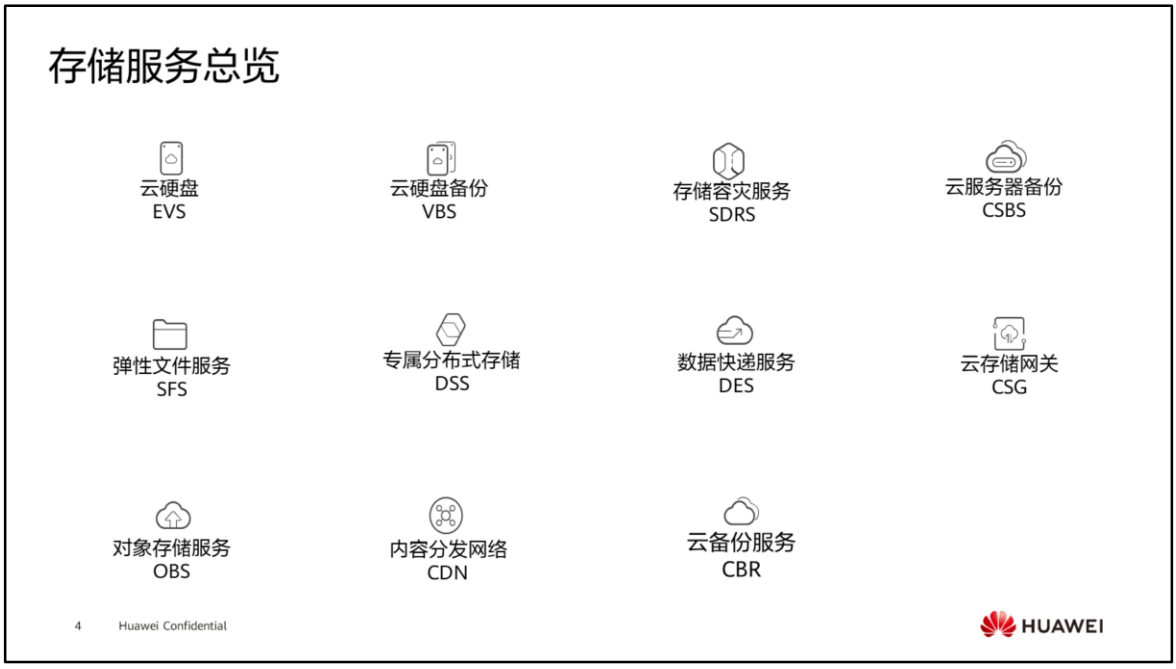
HUAWEI

前言

- 在日常生活中，数据无处不在，我们也有很多存储数据的设备，如U盘、云盘等，我们把这些设备统称为存储设备。在企业中，有哪些存储数据的设备？随着云时代的到来，又有哪些比较常见的云存储服务呢？
- 本章，我们将带领大家了解华为云中常见的存储服务。

目标

- 学完本课程后，您将能够：
  - 掌握存储领域的一些基础知识。
  - 了解华为云上常见存储服务的原理及使用。

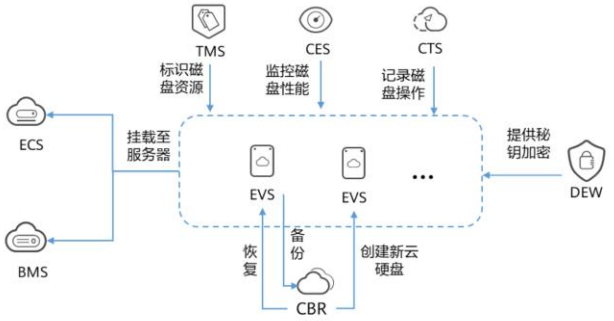


- 云硬盘：为计算服务提供持久性块存储
- 云硬盘备份：在线备份云硬盘，无需关机/重启
- 存储容灾服务：为云服务器提供RPO=0的保护
- 云服务器备份：为云服务器或磁盘提供保护
- 弹性文件服务：为计算实例提供托管式文件存储
- 专属分布式存储：提供独享的物理存储
- 数据快递服务：为数据上云提供安全快速的传输
- 云存储网关：为企业应用提供标准的文件存储访问接口
- 对象存储服务：稳定、安全、易用的云存储
- 内容分发服务：将源站内容分发至所有CDN节点
- 云备份服务：为云服务器、云硬盘提供备份

目录

什么是云硬盘（EVS）

- 云硬盘（Elastic Volume Service，EVS）可以为云服务器提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，可满足不同场景的业务需求。用于分布式文件系统、开发测试、数据仓库以及高性能计算等场景。



云硬盘与其他服务的关系

HUAWEI

- 云硬盘类似PC中的硬盘，需要挂载至云服务器使用，无法单独使用。可以对已挂载的云硬盘执行初始化、创建文件系统等操作，并且把数据持久化地存储在云硬盘上。
- 分布式文件系统（Distributed File System，DFS）是指文件系统管理的物理存储资源不一定直接连接在本地节点上，而是通过计算机网络与节点（可简单地理解为一台计算机）相连；或是若干不同的逻辑磁盘分区或卷标组合在一起而形成的完整的有层次的文件系统。

EVS的优势

规格丰富

- 提供多种规格的云硬盘，可满足不同业务场景的需求。

弹性扩展

- 支持按需扩容，平滑扩容，无需暂停业务。

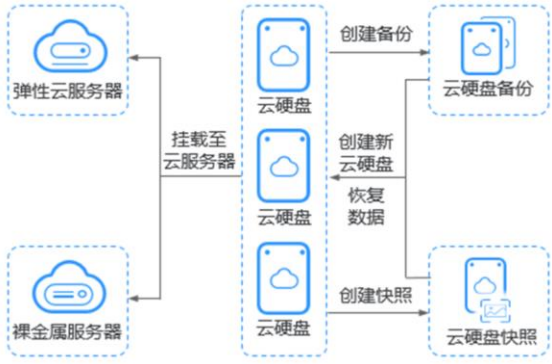
实时监控

- 配合云监控服务，随时了解云硬盘健康状态。

安全可靠

- 数据持久性高。支持加密、备份、快照多种保护机制。

EVS的产品架构



HUAWEI

- 云硬盘类似PC中的硬盘，需要挂载至云服务器或者裸金属服务器上使用，无法单独使用。用户可以对已挂载的云硬盘执行初始化、创建文件系统等操作，并且把数据持久化地存储在云硬盘上。除此之外，云硬盘还可以通过创建云硬盘备份和云硬盘快照来提高其可靠性。

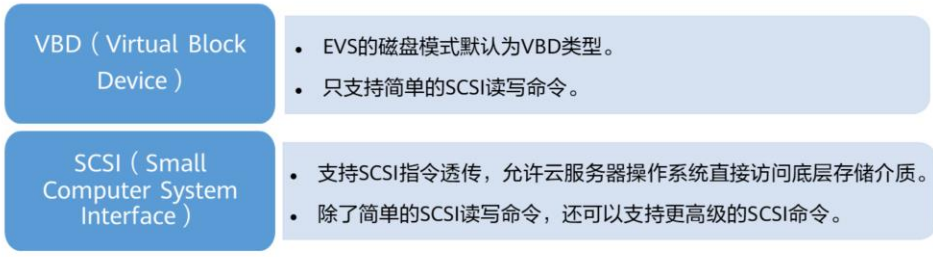
EVS的性能指标

参数	极速型SSD	超高IO	通用型SSD	高IO
描述	适用于需要超大带宽和超低时延的场景。	超高性能云硬盘，可用于企业关键性业务，适合高吞吐、低时延的工作负载。	高性价比的云硬盘，可用于高吞吐、低时延的企业办公。	可用于一般访问的工作负载。
最大IOPS（参考）	128000	50000	20000	5000
最大吞吐量（参考）	1000 MB/s	350 MB/s	250 MB/s	150 MB/s
单队列访问时延（参考）	200 μs	1 ms	1 ms	1 ms ~ 3 ms
典型应用场景	数据库 AI场景	超大带宽的读写密集型场景。转码类业务、I/O密集型场景、时延敏感型场景	企业办公、大型开发测试转码类业务、容器等高性能系统盘	日常办公应用、轻载型开发测试、不建议用于系统盘

- 说明：表格中为EVS云硬盘的常见类型，表格中的数据供参考，具体性能数据请以华为官网为准。
- 根据性能，EVS磁盘可分为极速型SSD、超高IO、通用型SSD、高IO、普通IO（上一代产品）。不同类型云硬盘的性能和价格有所不同，可根据应用程序要求选择所需的云硬盘。
- IOPS：Input/Output Operations per Second，每秒进行读写操作的次数。单个云硬盘IOPS性能 =“最大IOPS”与“基线IOPS + 每GB云硬盘的IOPS × 云硬盘容量”的最小值。

EVS的磁盘模式

- 根据是否支持高级的SCSI命令来划分磁盘模式，分为VBD(虚拟块存储设备，Virtual Block Device)类型和SCSI (小型计算机系统接口, Small Computer System Interface) 类型。

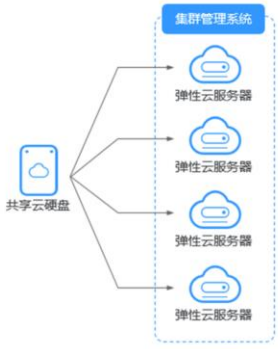


HUAWEI

- SCSI磁盘：BMS仅支持使用SCSI磁盘，用作系统盘和数据盘。
- SCSI共享盘：当您使用共享盘时，需要结合分布式文件系统或者集群软件使用。由于多数常见集群需要使用SCSI锁，例如Windows MSCS集群、Veritas VCS集群和CFS集群，因此建议您结合SCSI使用共享盘。

共享云硬盘

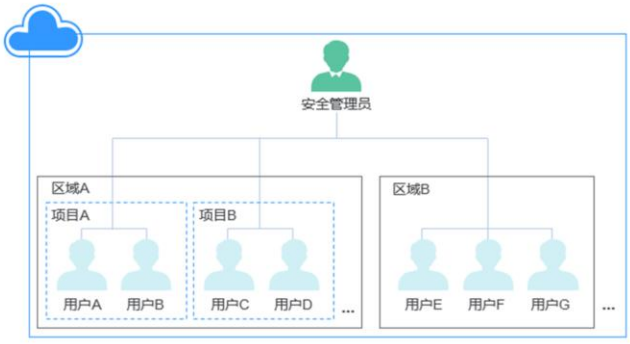
- 简单来说，就是一个云硬盘可以被多个云服务器或者裸金属服务器并发读写访问。共享云硬盘具备多挂载点、高并发性、高性能、高可靠性等特点，被广泛应用于需要支持集群、HA（High Available，高可用集群）能力的关键企业应用。



- 注意事项：使用共享云硬盘必须搭建共享文件系统或类似的集群管理系统，直接挂载至多台云服务器无法实现共享功能，且存在数据覆盖风险。一块共享云硬盘最多可同时挂载至16台云服务器。

云硬盘加密

- 当用户基于业务需求或者安全性考虑，需要对存储在云硬盘的数据进行加密时，这个时候就需要使用到云硬盘加密的功能。



HUAWEI

- 安全管理员可以直接授权EVS访问KMS（Key Management Service，密钥管理服务），使用加密功能。这个时候系统会为用户创建主密钥，此密钥就可以用来加密云硬盘。

云硬盘备份

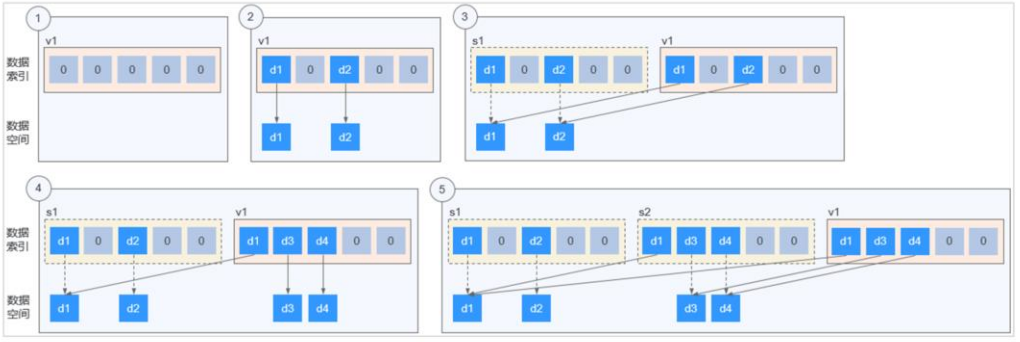
- 当云硬盘中的数据比较重要时，可以通过云硬盘备份功能，对现有数据进行备份。云硬盘备份功能可以在线备份，无需关闭云服务器，并且可以通过任意时刻的备份副本来恢复数据，以保证用户数据的正确性和安全性。

HUAWEI

- 对云硬盘设置备份策略后，系统会根据策略自动对云硬盘进行数据备份，后期用户就可以通过定期创建的备份作为基线数据，用来创建新的云硬盘或者恢复数据到源云硬盘。

云硬盘快照

- 云硬盘快照指的是云硬盘上的数据在快照创建时的完整拷贝或镜像，它是一种重要的数据容灾手段。当数据丢失时，用户可通过快照将数据完整地恢复到快照创建的时间点，从而保障数据的安全。



HUAWEI

- 如图所示，以通过云硬盘v1在不同时刻创建快照s1和s2为例：
  - 首先创建一个全新的云硬盘v1，没有任何数据。
  - 在云硬盘v1中写入数据d1和d2，此时使用新的数据空间存储d1和d2。
  - 当2修改后，云硬盘v1会创建快照s1，此时并不会另存一份数据d1和d2，而是建立快照s1与数据d1和d2的关联关系。
  - 在云硬盘v1中新写入数据d3，并将数据d2修改成d4，此时会使用新的数据空间存储d3和d4，并不会覆盖原有的d2数据。快照s1到数据d1和d2的关联关系仍然有效，因此若有需要，可以通过快照s1恢复原数据。
  - 当4修改后的云硬盘v1创建另一个快照s2，建立快照s2到数据d1、d3和d4的关联关系。

云硬盘备份 VS 快照

- 云硬盘的备份和快照都可以为存储在云硬盘中的数据提供冗余备份，那么它们的区别在哪呢?

指标	存储方案	数据同步	容灾范围	业务恢复
备份	与云硬盘数据分开存储，存储在对象存储（OBS）中，可以实现在云硬盘存储损坏情况下的数据恢复	保存云硬盘指定时刻的数据，可以设置自动备份。如果将创建备份的云硬盘删除，那么对应的备份不会被同时删除	与云硬盘位于同一个AZ内，云服务器备份支持跨区域复制	通过恢复备份至云硬盘，或者通过备份创建新的云硬盘，找回数据，恢复业务。数据持久性高。
快照	与云硬盘数据存储在一起	保存云硬盘指定时刻的数据。如果将创建快照的云硬盘删除，那么对应的快照也会被同时删除	与云硬盘位于同一个AZ内	通过回滚快照至云硬盘，或者通过快照创建新的云硬盘，找回数据，恢复业务。

- 说明：备份时由于数据搬迁会耗费一定的时间，创建快照和回滚快照数据的速度比备份快。

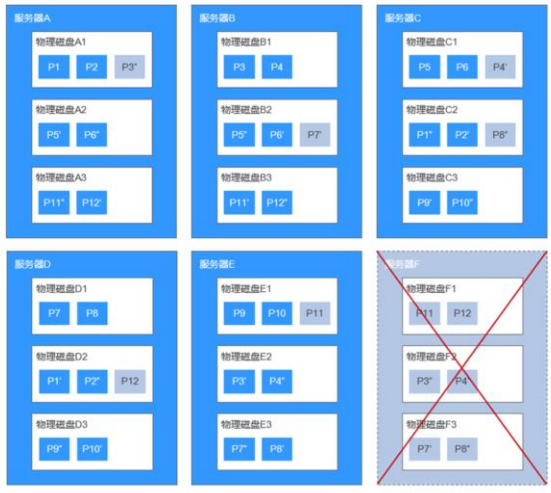
云硬盘三副本

- 云硬盘的存储系统采用三副本机制来保证数据的可靠性，即针对某份数据，默认将数据分为1 MB大小的数据块，每一个数据块被复制为3个副本，然后按照一定的分布式存储算法将这些副本保存在集群中的不同节点上。主要特点如下：
  - 存储系统自动确保3个数据副本分布在不同服务器的不同物理磁盘上，单个硬件设备的故障不会影响业务。
  - 存储系统确保3个数据副本之间的数据强一致性。

- 存储系统会确保3个数据副本之间的数据强一致性：例如，对于服务器A的物理磁盘A上的数据块P1，系统将它的数据备份为服务器B的物理磁盘B上的P1''和服务器C的物理磁盘C上的P1'，P1、P1'和P1''共同构成了同一个数据块的三个副本。若P1所在的物理磁盘发生故障，则P1'和P1''可以继续提供存储服务，确保业务不受影响。

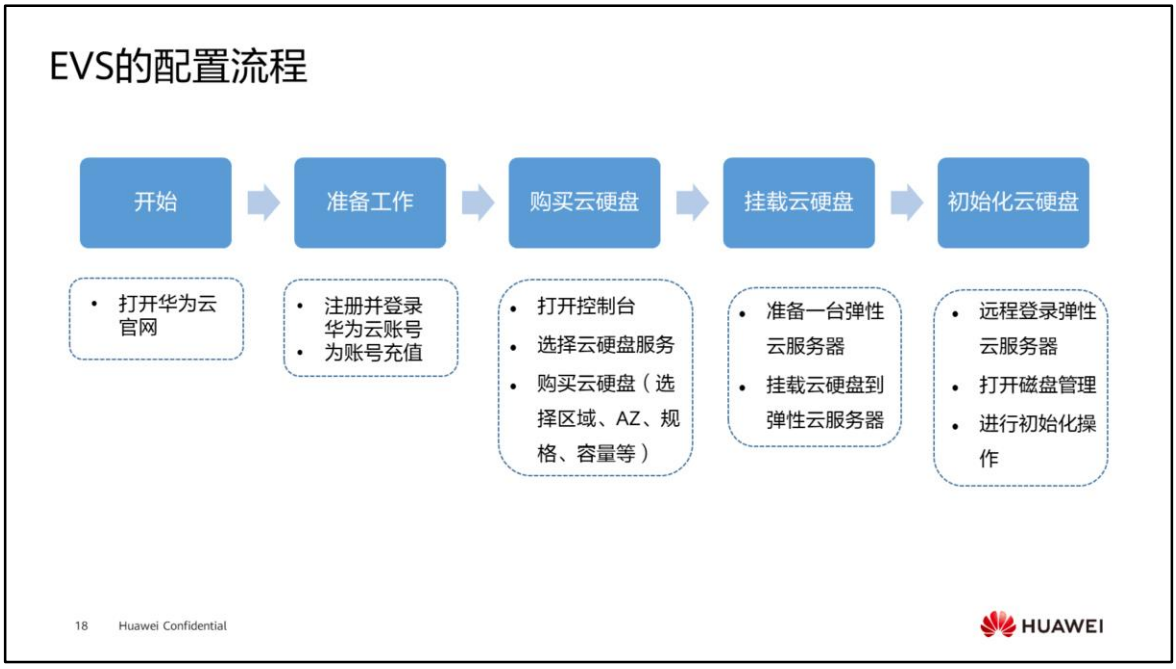
副本重建技术

- 当存储系统检测到硬件（服务器或者物理磁盘）发生故障时，会自动启动数据修复。由于数据块的副本分散存储在不同的节点上，数据修复时，将会在不同的节点上同时启动数据重建，每个节点上只需重建一小部分数据，多个节点并行工作，有效避免了单个节点重建大量数据所产生的性能瓶颈，将对上层业务的影响做到最小化。



HUAWEI

- 存储系统的每个物理磁盘上都保存了多个数据块，这些数据块的副本按照一定的策略分散存储在集群中的不同节点上。当存储系统检测到硬件（服务器或者物理磁盘）发生故障时，会自动启动数据修复。由于数据块的副本分散存储在不同的节点上，数据修复时，将会在不同的节点上同时启动数据重建。每个节点上只需重建一小部分数据，多个节点并行工作，有效避免了单个节点重建大量数据所产生的性能瓶颈，将对上层业务的影响做到最小化。



- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

挂载云硬盘

- 云硬盘不能单独使用，需要挂载到云服务器或者裸金属服务器上做初始化，才能被正常使用。
  - 非共享云硬盘只可以挂载至1台云服务器。
  - 共享云硬盘最多可同时挂载至多台云服务器，这些云服务器必须与共享云硬盘位于同一区域下的同一可用区。

HUAWEI

- 单独购买的云硬盘为数据盘，可以在云硬盘列表中看到磁盘属性为“数据盘”，磁盘状态为“可用”。此时需要将该数据盘挂载给云服务器使用。
- 系统盘必须随云服务器一同购买，并且会自动挂载，可以在云硬盘列表中看到磁盘属性为“系统盘”，磁盘状态为“正在使用”。当系统盘从云服务器上卸载后，此时系统盘的磁盘属性变为“启动盘”，磁盘状态变为“可用”。

问题研讨

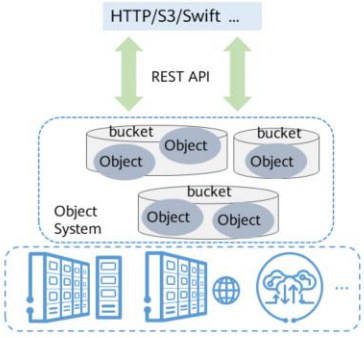
- 三副本技术和云备份、快照有什么区别?
- 云硬盘和我们平时使用的网盘又有什么区别?

- 三副本技术是云硬盘存储系统为了确保数据高可靠性提供的技术，主要用来应对硬件设备故障导致的数据丢失或不一致的情况。云硬盘备份、快照不同于三副本技术，主要应对人为误操作、病毒以及黑客攻击等导致数据丢失或不一致的情况。
- 云硬盘不能单独拿来存放数据，要借助于云服务器或者裸金属服务器。而网盘是可以直接存放数据的。站在产品分类的角度看，云硬盘属于IaaS类产品，而网盘属于SaaS类产品。

目录

什么是对象存储服务（OBS）

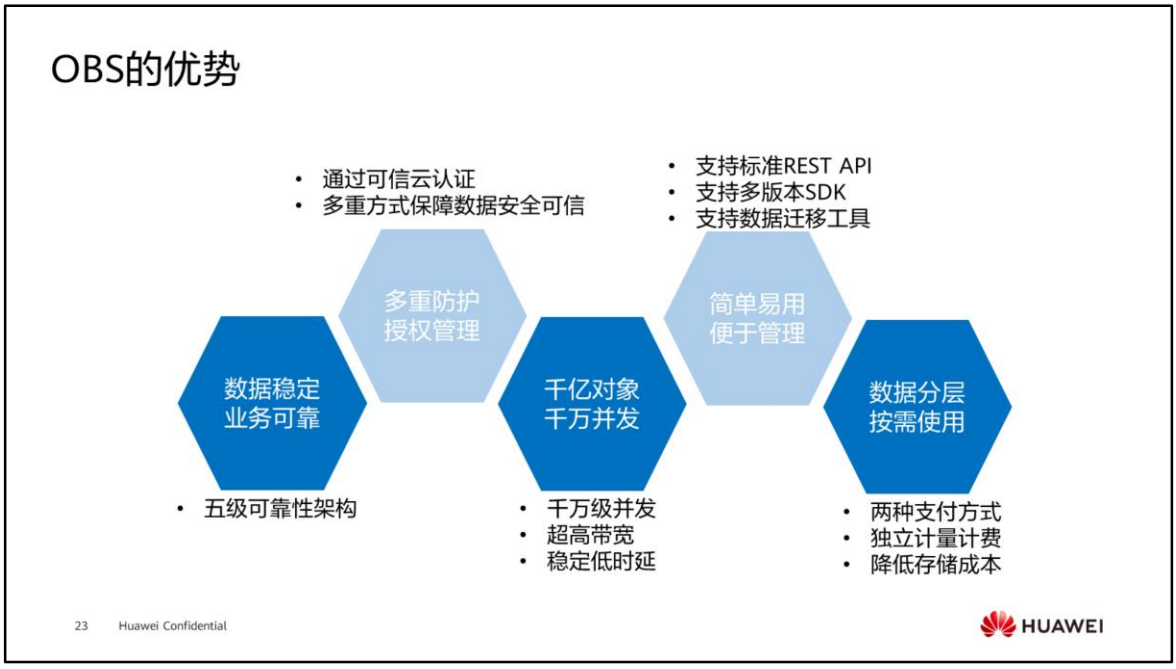
- 对象存储服务（Object Storage Service，OBS）是一个基于对象的海量存储服务，为用户提供海量、安全、高可靠、低成本的数据存储能力。



- 扁平化结构，租户间数据隔离
- 用户可以创建桶（就像文件夹）和上传或下载对象，可通过转发链接分享数据

HUAWEI

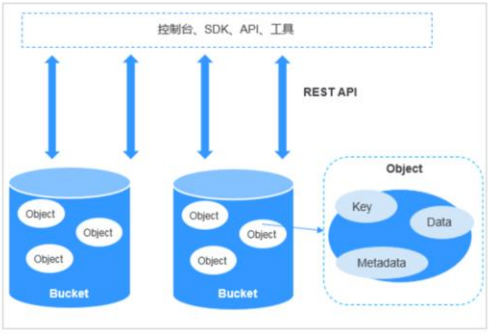
- OBS系统和单个桶都没有总数据容量和对象/文件数量的限制，为用户提供了超大存储容量的能力，适合存放任意类型的文件，适合普通用户、网站、企业和开发者使用。
- OBS是一项面向Internet访问的服务，提供了基于HTTP/HTTPS协议的Web服务接口，用户可以随时随地连接到Internet的电脑上，通过OBS管理控制台或各种OBS工具访问和管理存储在OBS中的数据。此外，OBS支持SDK和OBS API接口，可使用户方便管理自己存储在OBS上的数据，以及开发多种类型的上层业务应用。



- OBS的优势：
  - 数据稳定，业务可靠：OBS支撑华为手机云相册，数亿用户访问，稳定可靠。通过跨区域复制、AZ之间数据容灾、AZ内设备和数据冗余、存储介质的慢盘/坏道检测等技术方案，保障数据持久性高达99.9999999999%，业务连续性高达99.995%，远高于传统架构。
  - 多重防护，授权管理：OBS通过可信云认证，让数据安全放心。支持多版本控制、服务端加密、防盗链、VPC网络隔离、访问日志审计以及细粒度的权限控制，保障数据安全可信。
  - 千亿对象，千万并发：OBS通过智能调度和响应，优化数据访问路径，并结合事件通知、传输加速、大数据垂直优化等，为各场景下用户的千亿对象提供千万级并发、超高带宽、稳定低时延的数据访问体验。
  - 简单易用，便于管理：OBS支持标准REST API、多版本SDK和数据迁移工具，让业务快速上云。无需事先规划存储容量，存储资源可线性无限扩展，不用担心存储资源扩容、缩容问题。
  - 数据分层，按需使用：提供按量计费和包年包月两种支付方式，支持标准、低频访问、归档数据独立计量计费，降低存储成本。

OBS产品架构

- 桶（Bucket）是OBS中存储对象的容器。对象存储提供了基于桶和对象的扁平化存储方式，桶中的所有对象都处于同一逻辑层级，去除了文件系统中的多层级树形目录结构。
- 对象（Object）是OBS中数据存储的基本单位，一个对象实际是一个文件的数据与其相关属性信息（元数据）的集合体。用户上传至OBS的数据都以对象的形式保存在桶中。对象包括了Key，Metadata，Data三部分。



HUAWEI

- 对象是OBS中数据存储的基本单位，一个对象实际是一个文件的数据与其相关属性信息的集合体，包括Key、Metadata、Data三部分：
  - Key：键值，即对象的名称，为经过UTF-8编码的长度大于0且不超过1024的字符序列。一个桶里的每个对象必须拥有唯一的对象键值。
  - Metadata：元数据，即对象的描述信息，包括系统元数据和用户元数据，这些元数据以键值对（Key-Value）的形式被上传到OBS中。系统元数据由OBS自动产生，在处理对象数据时使用，包括Date，Content-length，Last-modify，Content-MD5等。用户元数据由用户在上传对象时指定，是用户自定义的对象描述信息。
  - Data：数据，即文件的数据内容。

永久AK/SK

- OBS支持通过AK/SK认证方式进行认证鉴权，即使用Access Key ID（AK）/Secret Access Key（SK）加密的方法来验证某个请求发送者身份。用户可以在“我的凭证”页面创建永久AK/SK。

HUAWEI

- AK/SK：
  - Access Key ID（AK）：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
  - Secret Access Key（SK）：与访问密钥ID结合使用的私有访问密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

临时AK/SK

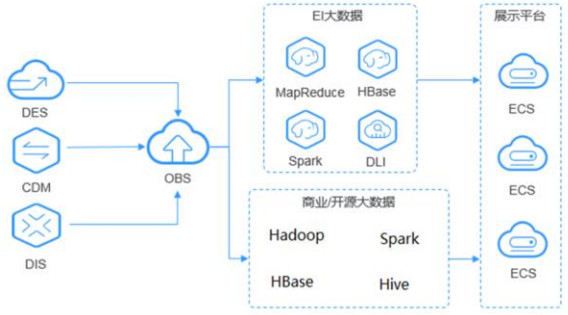
- 临时AK/SK和securitytoken是系统颁发给用户的临时访问令牌，有效期范围为15分钟至24小时，过期后需要重新获取。临时AK/SK和securitytoken遵循权限最小化原则，可应用于临时访问OBS。如果未使用securitytoken，会返回403错误。

返回值	描述
201	创建成功。
400	参数无效。
401	认证失败。
403	没有操作权限。
500	内部服务错误。

- 临时Access Key ID：临时访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- 临时Secret Access Key：与临时访问密钥ID结合使用的临时私有访问密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。
- securitytoken：与临时访问密钥ID和临时私有访问密钥结合使用，可以访问指定帐号下所有资源。

应用场景 - 大数据分析

- 场景描述：OBS提供的大数据解决方案主要面向海量数据存储分析、历史数据明细查询、海量行为日志分析和公共事务分析统计等场景，向用户提供低成本、高性能、不断业务、无需扩容的解决方案。

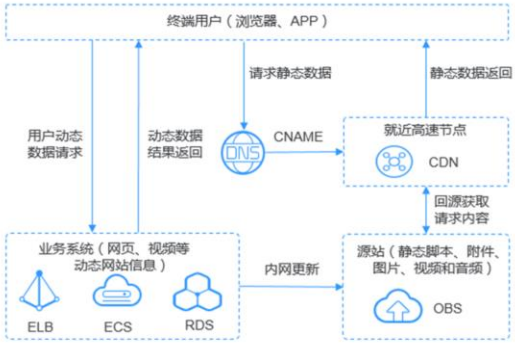


HUAWEI

- 海量数据存储分析的典型场景：PB级的数据存储，批量数据分析，毫秒级的数据详单查询等。
- 历史数据明细查询的典型场景：流水审计，设备历史能耗分析，轨迹回放，车辆驾驶行为分析，精细化监控等。
- 海量行为日志分析的典型场景：学习习惯分析，运营日志分析，系统操作日志分析查询等。
- 公共事务分析统计的典型场景：犯罪追踪，关联案件查询，交通拥堵分析，景点热度统计等。
- 建议搭配服务：MapReduce服务MRS，弹性云服务器ECS，数据快递服务DES。

应用场景 - 静态网站托管

- 场景描述：终端用户浏览器和APP上的动态数据直接与搭建在华为云上的业务系统进行交互，动态数据请求发往业务系统处理后直接返回给用户。静态数据保存在OBS中，业务系统通过内网对静态数据进行处理，终端用户通过就近的高速节点，直接向OBS请求和读取静态数据。



HUAWEI

- OBS提供低成本、高可用、可根据流量需求自动扩展的网站托管解决方案，结合内容分发网络CDN和弹性云服务器ECS快速构建动静态分离的网站/应用系统。
- 建议搭配服务：内容分发网络CDN，弹性云服务器ECS。

应用场景 - 企业云盘

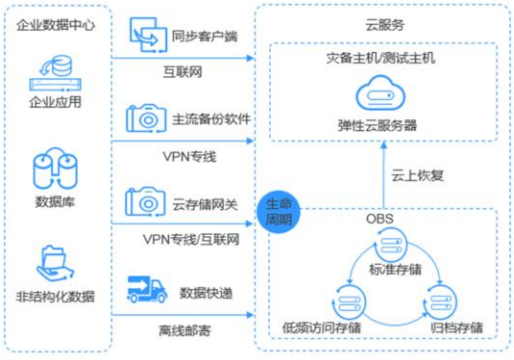
- **场景描述：**OBS提供高并发、高可靠、低时延、低成本的存储系统，存储容量可随用户数据量的提高而自动扩容。

HUAWEI

- 用户手机、电脑、PAD等终端设备上的动态数据与搭建在华为云上的企业云盘业务系统进行交互，动态数据请求发送到企业云盘业务系统处理后直接返回给终端设备。静态数据保存在OBS中，业务系统通过内网对静态数据进行处理，用户终端直接向OBS请求和取回静态数据。同时，OBS提供生命周期功能，实现不同对象存储类别之间的自动转换，以节省存储成本。
- 建议搭配服务：弹性云服务器ECS、弹性负载均衡ELB、关系型数据库RDS、云硬盘备份VBS。

应用场景 - 备份归档

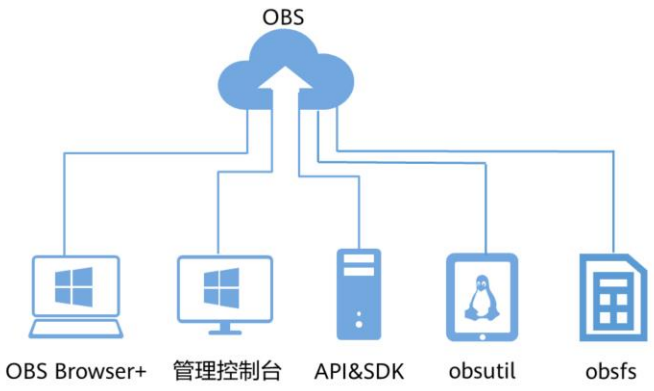
- **场景描述：**企业数据中心的各类数据通过使用同步客户端、主流备份软件、云存储网关或数据快递服务DES，备份至华为云对象存储服务OBS中。在需要时，可将OBS中的数据恢复到云上的灾备主机或测试主机。



HUAWEI

- OBS提供高并发、高可靠、低时延、低成本的海量存储系统，满足各种企业应用、数据库和非结构化数据的备份归档需求。
- 建议搭配服务：数据快递服务DES，弹性云服务器ECS。

OBS的访问方式



HUAWEI

- 通过控制台访问OBS，用户首先要使用用户的华为云账号或IAM用户登录控制台，在这种场景下OBS通过用户的账号或IAM用户信息进行鉴权。而在使用其他方式访问OBS时，例如工具（OBS Browser+，obsutil）、SDK或API，不需要用户提供华为云账号或IAM用户登录信息，取而代之的是通过账号或IAM用户的访问密钥（AK/SK）来进行鉴权。所以用户在使用这些方式访问OBS时，需要提前获取访问密钥（AK/SK）。
- obsutil：obsutil是一款用于访问管理华为云对象存储服务（Object Storage Service，OBS）的命令行工具，用户可以使用该工具对OBS进行常用的配置管理操作，如创建桶、上传文件/文件夹、下载文件/文件夹、删除文件/文件夹等。对于熟悉命令行程序的用户，obsutil是执行批量处理、自动化任务最好的选择。
- Obsfs：是对象存储服务（Object Storage Service，OBS）提供的一款基于FUSE的文件系统工具，用于将OBS并行文件系统挂载至Linux系统，让用户能够在本地像操作文件系统一样直接使用OBS海量的存储空间。

访问方式 - OBS Browser+

- 安装 OBS Browser+
  - 单击 OBS Browser+ 工具的下载链接下载该工具。
- 登录 OBS Browser+
  - OBS Browser+支持AK方式登录以及授权码登录两种登录方式。

HUAWEI

- OBS Browser+特性介绍：
  - OBS Browser+最多允许和保留100个历史账号登录。
  - 如果用户所在的网络环境需要通过代理访问，需要提前在设置中配置网络代理。
  - OBS Browser+不支持历史授权登录信息的查询和删除操作。
  - OBS Browser+对于过期的授权码信息会自动删除。

访问方式 - OBS Browser+

- 拖拽上传
  - OBS Browser+提供强大的拖拽上传功能，用户可以将本地的一个或多个文件或者文件夹拖拽到对象存储的对象列表或者并行文件系统的对象列表中。

HUAWEI

OBS的服务端加密功能

- 当启用服务端加密功能后：
  - 用户上传对象时，数据会在服务端加密成密文后存储。
  - 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。

HUAWEI

- KMS通过使用硬件安全模块（HSM）保护密钥安全地托管，帮助用户轻松创建和控制加密密钥。用户密钥不会明文出现在HSM之外，避免密钥泄露。对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足监督和合规性要求。
- 需要上传的对象可以通过数据加密服务器提供密钥的方式进行服务端加密。用户首先需要在KMS中创建密钥（或者使用KMS提供的默认密钥），当用户在OBS中上传对象时使用该密钥进行服务端加密。
- OBS支持通过接口提供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）两种方式，SSE-C方式是指OBS使用用户提供的密钥和密钥的MD5值进行服务端加密。

OBS的防盗链功能

一些不良网站想要扩充自己站点内容，但却不想增加成本，于是会盗用其他网站的链接。一方面损害了原网站的合法利益，另一方面又加重了服务器的负担。因此，产生了防盗链技术。OBS同时支持访问白名单和访问黑名单的设置：

- 白名单Referer为空，黑名单Referer不空时，允许所有黑名单中指定网站以外的其他网站的请求访问目标桶中的数据。
- 白名单Referer不为空，黑名单Referer为空或不空时，只允许白名单中指定网站的请求访问目标桶中的数据。

- 在HTTP协议中，通过表头字段Referer，网站可以检测目标网页访问的来源网页。有了Referer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者返回指定的页面。防盗链就是通过设置Referer，去检测请求来源的Referer字段信息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，否则阻止请求访问或返回指定页面。

OBS的多版本控制功能

- 通过OBS多版本控制功能，用户可以在一个桶中保留多个版本的对象，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。

HUAWEI

- 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的对象。
- 开启多版本控制，桶中已有对象版本ID（空）和内容都不会变化。再次上传该同名对象，对象版本示意图如左图所示；新上传对象，OBS自动为每个对象创建唯一的版本号。上传同名的对象将以不同的版本号同时保存在OBS中，如右图所示。

OBS的自定义域名功能

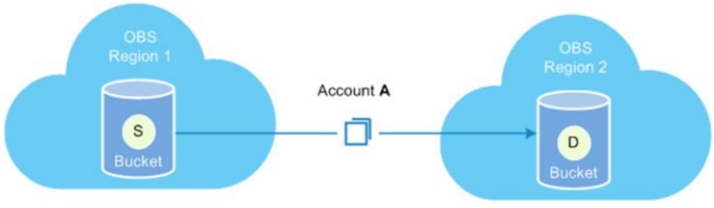
- 当用户需要将网站中的文件迁移到OBS，并且不想修改网页的代码，即保持网站的链接不变。此时可以使用自定义域名绑定方案。

HUAWEI

- 例如用户A的网站域名为www.example.com，网站文件为abc.html，网站链接为：http://www.example.com/abc.html。配置流程如下：
  - 在OBS上创建一个桶，并上传abc.html网站文件到该桶中。
  - 通过OBS控制台，将www.example.com这个自定义的域名绑定在已创建桶上。
  - 在域名服务器上，添加CNAME规则，将www.example.com映射成桶域名。
  - http://www.example.com/abc.html请求到达OBS后，OBS会找到www.example.com和桶域名的映射，转换变成访问桶的abc.html文件。即对http://www.example.com/abc.html的访问，经过OBS处理后，实际上访问的是http://桶域名/abc.html。
- 业务类型的详解介绍在CDN服务的讲解内容中会提到。
- 约束和限制：
  - 桶版本号为3.0及以上的桶支持自定义绑定域名功能。桶版本号可以在OBS管理控制台上，进入桶概览页后，在“基本信息”中查看。
  - 每个桶最多绑定5个自定义域名。
  - OBS自定义域名绑定暂时不支持HTTPS访问自定义域名，只支持HTTP访问自定义域名。
  - 客户自定义域名绑定成功后，若想使用HTTPS进行访问，需同时使用CDN，通过CDN管理控制台进行HTTPS证书管理，即可使用HTTPS访问。
  - 一个自定义域名只能绑定到一个桶域名上。

OBS的跨域复制功能

- 区域复制能够为用户提供跨区域数据容灾的能力，满足用户数据复制到异地进行备份的需求。
- 跨区域复制是指通过创建跨区域复制规则，在同一个账号下，将一个桶（源桶）中的数据自动、异步地复制到不同区域的另外一个桶（目标桶）中。

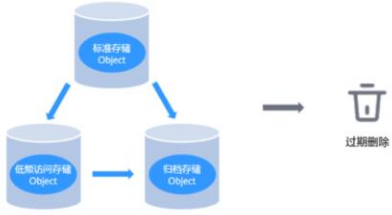


HUAWEI

- 启用跨区域复制规则后，符合以下条件的对象会被复制到目标桶中：
  - 新上传的对象（归档存储对象除外）。
  - 有更新的对象，比如对象内容有更新或者已复制成功的对象ACL有更新。
  - 桶中的历史对象（需要开启“同步历史对象”功能）。
- 适用场景：
  - 客户需要在多地访问相同的OBS资源。为了最大限度缩短访问对象时的延迟，用户可以使用跨区域复制，在离客户较近的区域中创建对象副本。
  - 由于业务原因，用户需要将OBS数据从一个区域的数据中心迁移至另一个区域的数据中心。
  - 出于对数据安全性以及可用性的考虑，用户希望对所有写入OBS的数据都在另一个区域的数据中心显式地创建一个备份，以便在数据发生不可逆损毁时，有安全、可用的备份数据。

OBS的生命周期管理

- 生命周期管理是指通过配置指定的规则，实现定时删除桶中的对象或者定时转换对象的存储类别。
- 生命周期管理可适用于以下典型场景：
  - 周期性上传的日志文件，可能只需要保留一个星期或一个月，到期后要删除它们。
  - 某些文档在一段时间内经常访问，但是超过一定时间后便可能不再访问了。这些文档需要在一定时间后转化为低频访问存储，归档存储或者删除。



HUAWEI

- 生命周期管理规则通常包含两个关键要素：
  - 策略：即用户可以指定对象名前缀来匹配受约束的对象，则匹配该前缀的对象将受规则影响；也可以指定将生命周期管理规则配置到整个桶，则桶内所有对象都将受规则影响。
  - 时间：即用户可以指定在对象最后一次更新后多少天，受规则影响的对象将转换为低频访问存储、归档存储或者过期并自动被OBS删除。
    - 转换为低频访问存储：即用户可以指定在对象最后一次更新后多少天，受规则影响的对象将转换为低频访问存储。
    - 转换为归档存储：即用户可以指定在对象最后一次更新后多少天，受规则影响的对象将转换为归档存储。
    - 过期删除：即用户可以指定在对象最后一次更新后多少天，受规则影响的对象将过期并自动被OBS删除。
    - 转换为低频访问存储的时间最少设置为30天，若同时设置转换为低频访问存储和转换为归档存储，则转换为归档存储的时间要比转换为低频访问存储的时间至少长30天，例如转换为低频访问存储设置为33天，则转换为归档存储至少需要设置为63天。若单独设置转换为归档存储，则没有时间限制。过期时间必须大于前两个转换时间的最大值。

OBS的权限管理

- OBS支持通过以下方式进行权限控制：

- 作用于云资源。
- IAM权限定义了允许和拒绝的访问操作。

- 桶策略作用于所配置的OBS桶及桶内对象。
- 对象策略是桶策略中针对对象的策略。

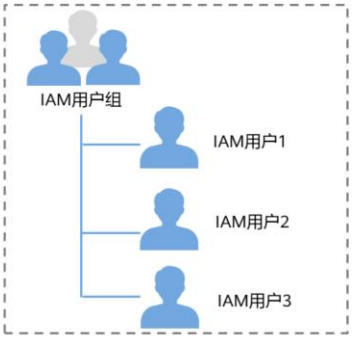
HUAWEI

- IAM权限：IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。
- 桶策略和对象策略：
  - 桶策略是作用于所配置的OBS桶及桶内对象的。OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限。
  - 对象策略是桶策略中针对对象的策略。
  - ACL：OBS ACL是基于账号级别的读写权限控制，提供桶和对象的ACL配置。
- IAM权限应用场景：
  - 使用策略控制帐号下整个云资源的权限时，使用IAM权限授权。
  - 使用策略控制帐号下OBS所有的桶和对象的权限时，使用IAM权限授权。
  - 使用策略控制帐号下OBS指定资源的权限时，使用IAM权限授权。
- 策略管理的应用场景：
  - 不用IAM权限控制访问权限的情况下，允许其他帐号访问OBS资源，可以使用桶策略的方式授权其他帐号对应的权限。
  - 当不同的桶对于不同的IAM用户有不同的访问控制需求时，需使用桶策略分别授权IAM用户不同的权限。
  - 桶拥有者允许其他帐号访问自己的桶时，可使用桶策略授权其他帐号对应的权

限。

权限管理 - IAM权限

- 通过IAM，用户可以在云账号中创建IAM用户，并使用策略来控制IAM用户对云资源的访问范围。



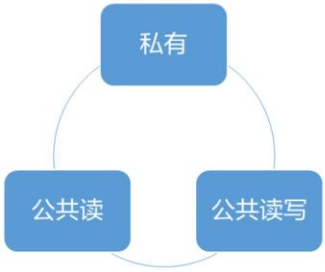
权限名称	描述
Tenant Administrator	拥有该权限的用户可以对OBS对象存储资源执行任意操作。
Tenant Guest	拥有该权限的用户可以查询OBS对象存储资源的利用情况。
OBS Buckets Viewer	具备该权限的用户，可以执行获取桶列表、查询桶元数据和位置信息的操作。

HUAWEI

- IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。对于OBS，IAM权限的OBS权限是作用于OBS所有的桶和对象的。如果要授予IAM用户操作OBS资源的权限，则需要向用户所属的用户组授予一个或多个OBS权限集。
- IAM权限主要面向对同账号下IAM用户授权的场景：
  - 使用策略控制账号下整个云资源的权限时，使用IAM权限授权。
  - 使用策略控制账号下OBS所有的桶和对象的权限时，使用IAM权限授权。
  - 使用策略控制账号下OBS指定资源的权限时，使用IAM权限授权。

权限管理 - 策略管理

- 桶策略是作用于所配置的OBS桶及桶内对象的。OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限。标准桶策略提供以下三种策略供用户设置。



标准桶策略：

- 私有：除桶ACL授权外的其他用户无桶的访问权限。
- 公共读：任何用户都可以对桶内对象进行读操作。
- 公共读写：任何用户都可以对桶内对象进行读/写/删除操作。

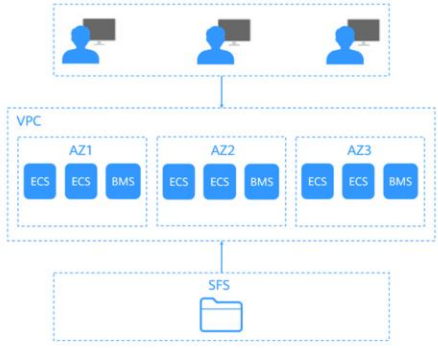
HUAWEI

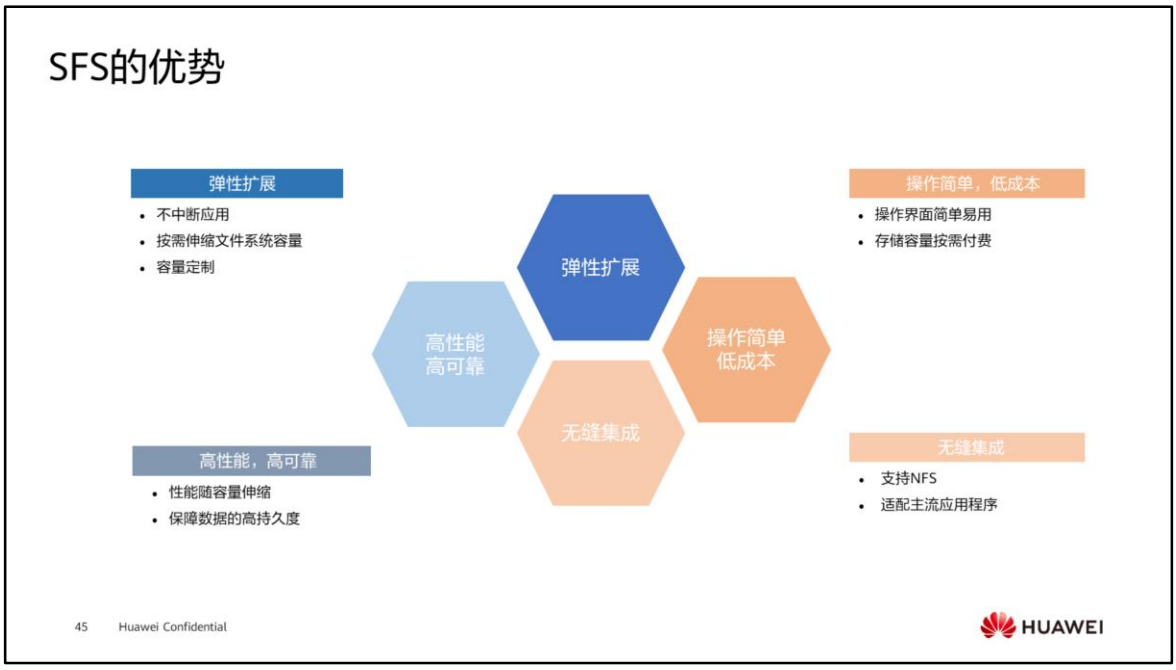
- 桶策略的应用场景：
  - 不用IAM权限控制访问权限的情况下，允许其他账号访问OBS资源，可以使用桶策略的方式授权其他账号对应的权限。
  - 当不同的桶对于不同的IAM用户有不同的访问控制需求时，需使用桶策略分别授权IAM用户不同的权限。
  - 桶拥有者允许其他账号访问自己的桶时，可使用桶策略授权其他账号对应的权限。

目录

什么是弹性文件服务（SFS）

- 弹性文件服务（Scalable File Service，SFS）可为用户提供按需扩展的高性能文件存储（Network Attached Storage，NAS），可为云上多个弹性云服务器、容器、裸金属服务器提供共享访问。

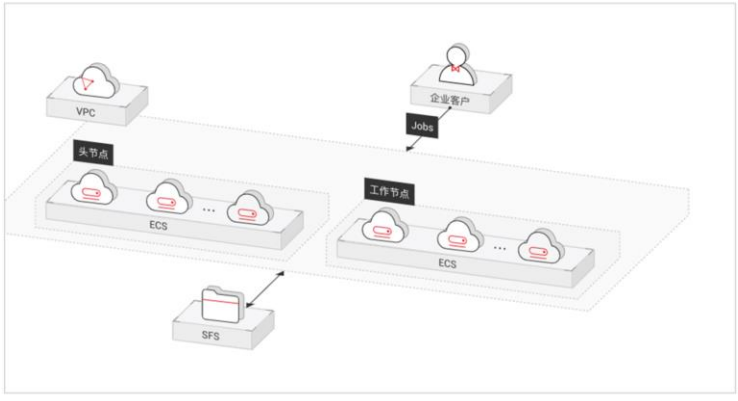




- 与传统的文件共享存储相比，弹性文件服务具有以下优势：
  - 弹性扩展：弹性文件服务可以根据用户的使用需求，在不中断应用的情况下，增加或者缩减文件系统的容量。一键式操作，轻松完成用户的容量定制
  - 高性能、高可靠性：性能随容量增加而提升，同时保障数据的高持久度，满足业务增长需求
  - 无缝集成：弹性文件服务同时支持NFS和CIFS协议。通过标准协议访问数据，无缝适配主流应用程序进行数据读写。同时兼容SMB2.0/2.1/3.0版本，Windows客户端可轻松访问共享空间
  - 操作简单、低成本：操作界面简单易用，用户可轻松快捷地创建和管理文件系统。并根据使用的存储容量按需付费，有效降低成本

SFS的应用场景 - HPC

- 满足工业设计CAD/CAE，生物制药，能源勘探，图片渲染和异构计算等高性能计算场景对共享文件存储的需求。

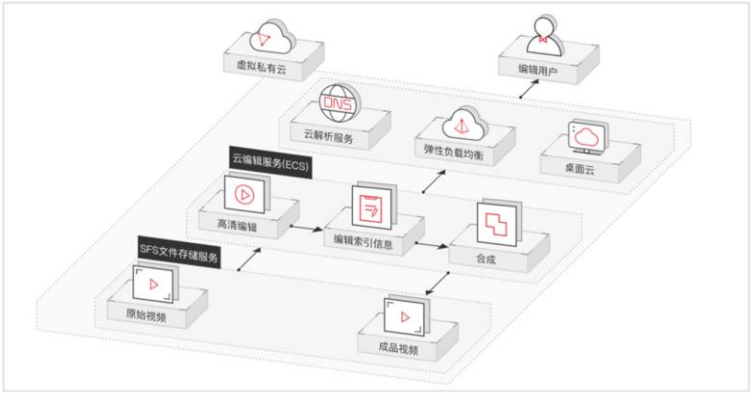


HUAWEI

- HPC是高性能计算（High Performance Computing）的简称。通常指以计算为目的，使用了很多处理器的单个计算机系统或者使用了多台计算机集群的计算机系统和环境。能够执行一般个人电脑无法处理的大资料量与高性能的运算。HPC具有超高浮点计算能力，可用于解决计算密集型、海量数据处理等业务的计算需求，如应用于工业设计CAD/CAE，生物科学，能源勘探，图片渲染和异构计算等涉及高性能计算集群来解决大型计算问题的领域。
- 工业设计CAE/CAD：如汽车制造中使用到的CAE/CAD等涉及仿真软件，在进行数据计算时需要计算节点之间进行紧密的通信，要求文件系统高带宽、低时延。
- 生物科学：要求参与大数据计算的文件系统高带宽、高存储且易于扩展。
  - 对生物基因数据进行测序、拼接、比对等处理，提供基因组信息以及相关数据系统的生物信息学领域。
  - 进行大规模分子动力学模拟来分析和验证蛋白质在分子和原子水平上的变化的分子动力学模拟领域。
  - 快速地完成高通量药物虚拟筛选从而大量缩短研发周期和减少投入资金的新药研发等领域。
- 能源勘探：野外作业，勘探地质，对地质资料进行处理和解释以及进行油藏和汽藏的识别要求文件系统内存大、高带宽。
- 图片渲染：图像处理、三维渲染，频繁处理小文件，要求文件系统数据读写性能强、容量大、高带宽。
- 异构计算：这种以不同类型的指令集和体系架构的计算单元为组成的系统计算方式要求文件系统高带宽、低时延。

SFS的应用场景 - 媒体处理

- 满足视频编辑、转码、合成以及高清视频和4K视频点播场景对共享文件存储的需求，支持多层高清视频编辑及4K视频编辑。

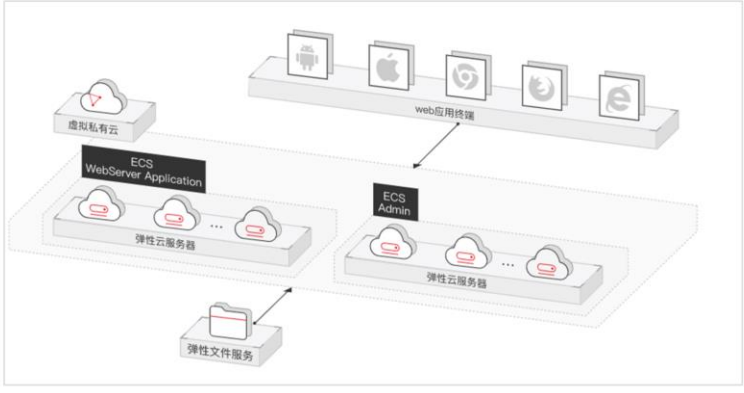


HUAWEI

- 媒体处理包括媒体素材的上传、下载、编目、节目转码和数据归档等工作，涉及音视频数据的存储、调用和管理，根据其业务特性对共享的文件系统有如下要求：媒体素材的视频码率高，文件规模大，要求文件系统容量大且易于扩展。
- 音视频的采集、编辑、合成等应用要求文件系统无抖动、低时延。
- 多用户同时进行编辑制作，要求文件系统提供稳定易用的数据共享。
- 视频渲染、特效加工需要频繁处理小文件，要求文件系统具有较高的数据读写性能。
- 弹性文件服务是基于文件系统的共享存储服务，具有高速数据共享，动态分级存储，按需平滑扩展，支持在线扩容等特点，能充分满足媒体处理中用户对存储容量，吞吐量，IOPS（每秒读写次数）和各种工作负荷下低时延的需求。

SFS的应用场景 - 内容管理和web服务

- SFS也可用于各种内容管理系统，为网站、在线发行、存档等各种应用存储数据及提供信息。可以很好地处理突发的高峰流量，无须担心扩容不及时带来问题。

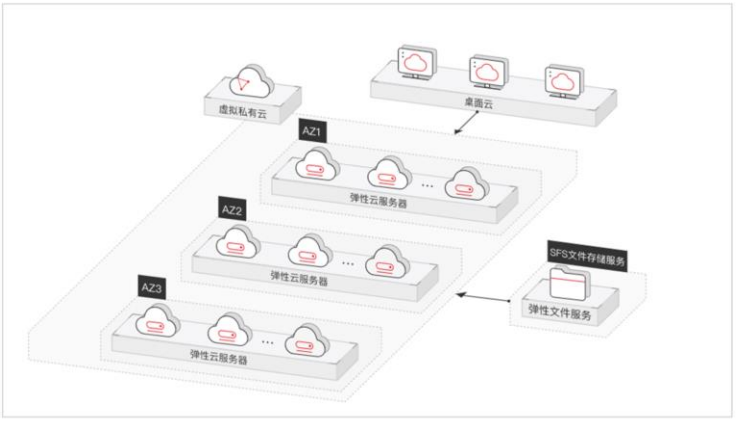


HUAWEI

- 对于I/O密集型的网站业务，SFS Turbo为多个Web Server提供共享的网站源码目录，存储，提供低延迟，高IOPS的并发共享访问能力。业务特点：
- 大量小文件：存放网站静态文件，包括HTML文件，Json文件，静态图片等。
- 读I/O密集：业务以小文件读为主，数据写入相对较少。
- 多个Web Server访问同一个SFS Turbo后台，实现网站业务的高可用。

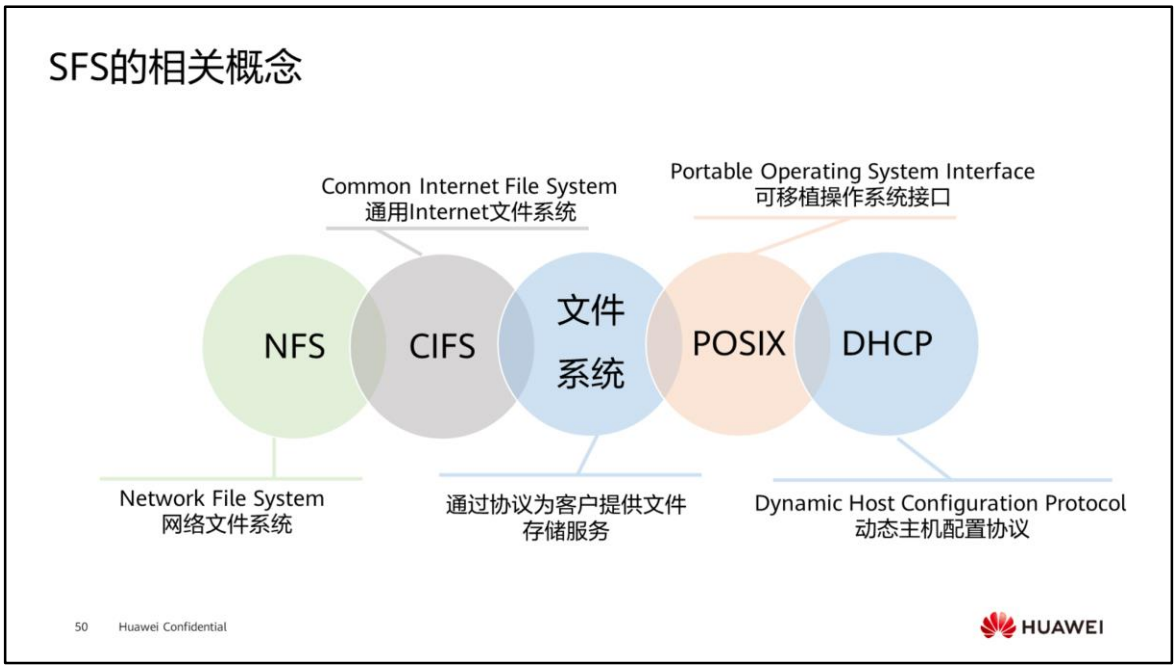
SFS的应用场景 - 文件共享

- SFS同时也适用于企业内部部门/员工众多、而且需要共享访问相同文档的场景。



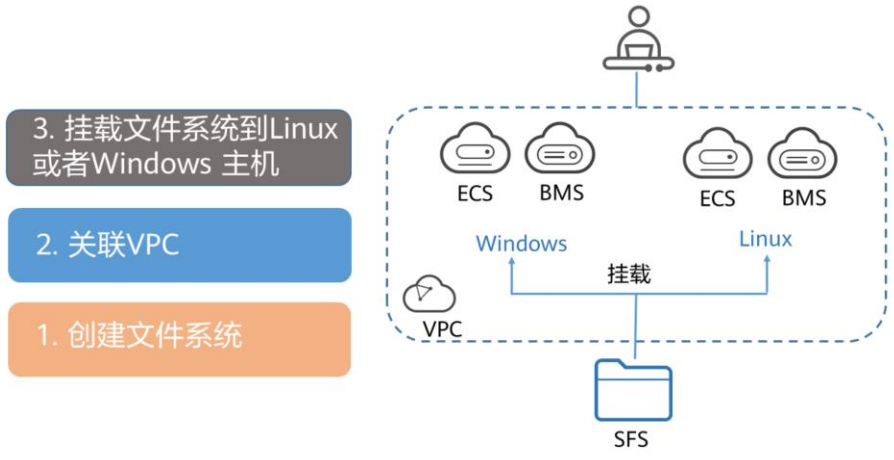
HUAWEI

- 推荐使用高IOPS、低时延的SFS Turbo文件服务，设计规格为99.99999999%（10个9）持久性，保障数据不丢失。



- SFS的相关概念：
  - NFS：NFS（Network File System），即网络文件系统。一种使用于分散式文件系统的协议，通过网络让不同的机器、不同的操作系统能够彼此分享数据。
  - CIFS：CIFS（Common Internet File System），通用Internet文件系统，是一种网络文件系统访问协议。CIFS是公共的或开放的SMB协议版本，由微软公司使用，它使程序可以访问远程Internet计算机上的文件并要求此计算机提供服务。通过CIFS协议，可实现Windows系统主机之间的网络文件共享。
  - 文件系统通过标准的NFS协议和CIFS协议为客户提供文件存储服务，用于网络文件远程访问，用户通过管理控制台创建挂载地址后，即可在多个云服务器上进行挂载，并通过标准的POSIX接口对文件系统进行访问。
  - POSIX：可移植操作系统接口（Portable Operating System Interface，POSIX），是IEEE为要在各种UNIX操作系统上运行软件而定义API的一系列互相关联的标准的总称。POSIX标准意在期望获得源代码级别的软件可移植性。也就是为一个POSIX兼容的操作系统编写的程序，可以在任何其它的POSIX操作系统上编译执行。
  - DHCP：动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）是一个局域网的网络协议。指的是由服务器控制一段IP地址范围，客户机登录服务器时就可以自动获得服务器分配的IP地址和子网掩码。默认情况下，DHCP作为Windows Server的一个服务组件不会被系统自动安装，还需要管理员手动安装并进行必要的配置。

SFS的配置流程



HUAWEI

- 创建文件系统：在多个云服务器中挂载使用，实现文件系统的共享访问。可创建SFS容量型和SFS Turbo两种不同类型的文件系统。

SFS的使用 - 挂载NFS文件系统到Linux服务器

当创建文件系统后，用户需要使用云服务器来挂载该文件系统，以实现多个云服务器共享使用文件系统的目的。以root用户登录弹性云服务器为例：

- 安装NFS客户端。
- 执行如下命令，查看是否能解析文件系统挂载地址中的域名。SFS Turbo文件系统无需域名解析操作，可跳过此步直接挂载。
  nslookup *文件系统域名*
- 执行如下命令，创建用于挂载文件系统的本地路径。
  mkdir *本地路径*
- 执行如下命令，将文件系统挂载到云服务器上。文件系统目前仅支持NFSv3协议挂载到Linux云服务器
  mount -t nfs -o vers=3 timeo=600 *挂载地址 本地路径*
- 挂载成功后，用户可以在云服务器上访问文件系统。

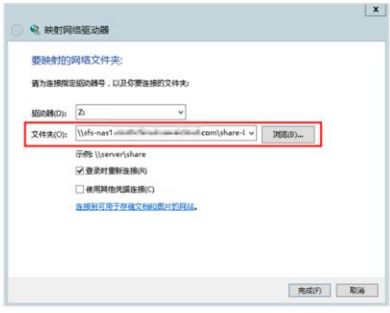
HUAWEI

- 在linux操作系统中：
  - nslookup是用来解析域名的。
  - mkdir=make directory，也就是创建目录的意思。本地路径指的就是要创建的文件夹名。
  - mount是挂载命令，-t是参数，用来指定挂载的文件系统类型，nfs表示网络文件共享类型；-o指定协议版本（如v3），超时时间（如600 s）等。

SFS的使用 - 挂载CIFS文件系统到Windows服务器

以挂载CIFS文件系统到云服务器（Windows）为例

- 登录已创建好的Windows 2012版本的弹性云服务器。
- 单击“开始”，右键单击“这台电脑”，选择“映射网络驱动器”。
- 在弹出的对话框中输入文件系统的挂载地址，即\\文件系统域名\路径。



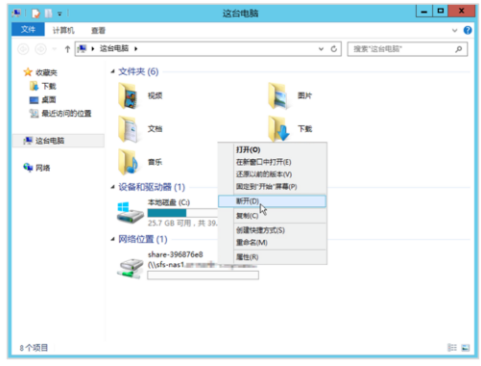
HUAWEI

- 前提条件：
  - 确定云服务器操作系统类型，不同操作系统安装NFS客户端的命令不同
  - 已完成创建文件系统，并获取到文件系统的挂载地址
  - 存在至少一台与文件系统所属VPC相同的云服务器
  - 云服务器（ECS）上已配置了用于内网解析文件系统域名的DNS服务器的IP地址，SFS Turbo文件系统无需域名解析操作

SFS的使用 - 卸载文件系统

当文件系统不再使用需要删除时，建议先卸载已挂载的文件系统后再删除。

- Linux系统
  - 登录弹性云服务器
  - 执行umount本地路径
- Windows系统
  - 登录弹性云服务器
  - 右键单击待卸载的文件系统，选择“断开”
  - 若网络位置下已挂载的文件系统已不存在，证明卸载成功

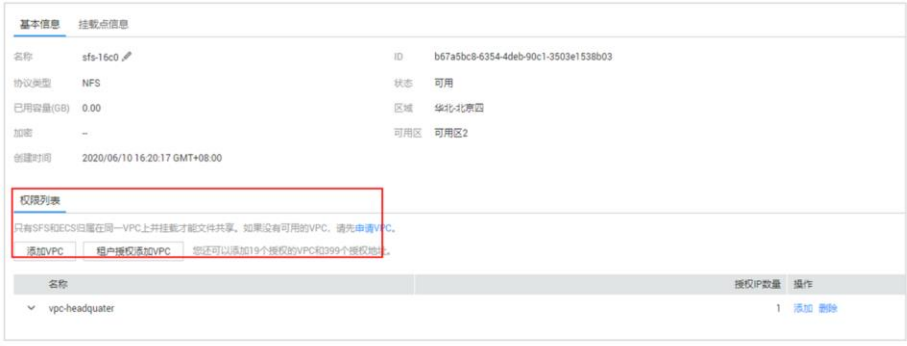


HUAWEI

- 前提条件：
  - 确定云服务器操作系统类型，不同操作系统安装NFS客户端的命令不同
  - 已完成创建文件系统，并获取到文件系统的挂载地址
  - 存在至少一台与文件系统所属VPC相同的云服务器
  - 云服务器（ECS）上已配置了用于内网解析文件系统域名的DNS服务器的IP地址，SFS Turbo文件系统无需域名解析操作。

SFS的使用 - 配置多VPC

- SFS文件系统支持配置多个VPC，使得归属于不同VPC的云服务器也能共享访问同一个文件系统。



HUAWEI

- 只要所属的VPC被添加到文件系统的VPC列表下，或云服务器被添加到了VPC的授权地址中，那么归属于不同VPC的云服务器也能共享访问同一个文件系统。

SFS vs OBS vs EVS

对比维度	弹性文件服务	对象存储服务	云硬盘
概念	提供按需扩展高性能文件存储，可为云上多个云服务器提供共享访问（类似Windows或Linux中的远程目录）。	提供海量、安全、高可靠、低成本的数据存储能力。	可以为云服务器提供高可靠、高性能、规格丰富的块存储服务（类似PC中的硬盘）。
存储数据的逻辑	存放的是文件，会以文件和文件夹的层次结构来整理和呈现数据。	存放的是对象，可以直接存放文件，文件会生成系统元数据，用户也可以自定义文件的元数据。	存放的是二进制数据，无法直接存放文件。如果要存文件，需要先格式化。
访问方式	需要指定网络地址进行访问，或将网络地址变为本地目录进行访问。使用NFS或CIFS的网络文件系统协议。	可以通过互联网或专线访问，需要指定桶地址，使用的是HTTP和HTTPS等传输协议。	只能在ECS/BMS中挂载使用，不能被操作系统应用直接访问，需要格式化。
使用场景	如高性能计算、媒体处理、文件共享、内容管理和Web服务等。	如大数据分析、静态网站托管、在线视频点播、基因测序等。	如高性能计算、企业核心集群应用、企业应用系统和开发测试等。

思考题

1. （判断题）挂载EVS时，必须先要关闭ECS主机。

   正确

   错误

2. （选择题）以下选项中，哪个不属于OBS的功能特点?

   A. 支持跨域复制

   B. 支持多版本控制

   C. 支持防盗链

   D. 可以挂载给云服务器

- 错误。挂载EVS可以不需要停ECS。
- D。挂载给云服务器是EVS的主要功能。

本章总结

- 有数据，就有存储的需求。通过本章的学习，我们对于存储的类型有了全新的认识，对华为云的存储服务也有了全新的了解。在企业上云的大趋势下，只有掌握好各类存储服务的定位、原理以及使用，我们才可以更好地匹配企业对于存储的需求，例如视频云需要何种类型的存储服务，数据库需要何种类型的存储服务等。

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为云技术支持网站
  - https://support.huaweicloud.com/help-novice.html
- 华为云学院
  - https://edu.huaweicloud.com/

术语和缩略语

- AK/SK：Access Key ID/Secret Access Key，访问密钥
- API：Application Programming Interface，应用编程接口
- AZ：Availability Zone，可用区
- BMS：Bare Metal Server，裸金属服务器
- CAD/CAE：Computer Aided Design/Computer Aided Engineering，计算机辅助设计/计算机辅助工程
- CIFS：Common Internet File System，通用Internet文件系统
- DES：Data Express Service，数据快递服务
- DHCP：Dynamic Host Configuration Protocol，动态主机配置协议
- ECS：Elastic Cloud Server，弹性云服务器
- EVS：Elastic Volume Service，云硬盘
- HA：High Available，高可用

术语和缩略语

- HPC：High-Performance Computing，高性能计算
- HTTP：Hypertext Transfer Protocol，超文本传输协议
- HTTPS：Hypertext Transfer Protocol over Secure Sockets Layer，安全套接字层的超文本传输协议
- IAM：Identity and Access Management，统一身份认证服务
- IOPS：Input/Output Per Second，每秒进行读写操作的次数
- NAS：Network Attached Storage，网络附加存储
- NFS：Network File System，即网络文件系统
- OBS：Object Storage Service，对象存储服务
- POSIX：Portable Operating System Interface，可移植操作系统接口
- SCSI：Small Computer System Interface，小型计算机系统接口
- SDK：Software Development Kit，软件开发工具包

术语和缩略语

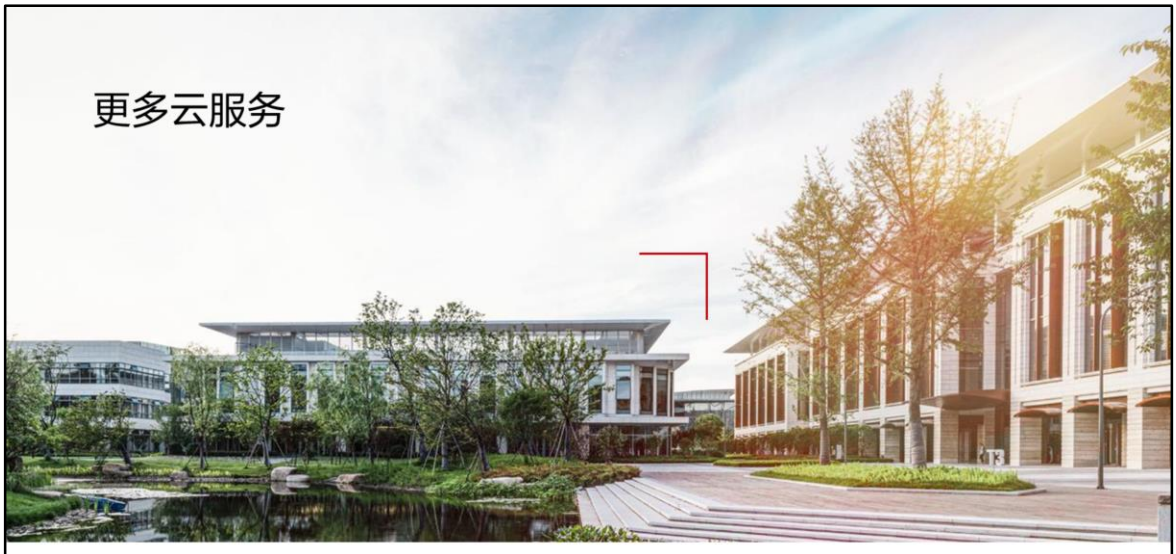
- SFS：Scalable File Service，弹性文件服务
- SSD：Solid-State Drive，固态硬盘
- VBD：Virtual Block Device，虚拟块设备
- VPC：Virtual Private Cloud，虚拟私有云

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

更多云服务



HUAWEI

前言

- 企业上云除了基础的计算服务、存储服务、网络服务的需求之外，有时候还需要其他服务，如数据库类服务，安全类服务、CDN服务、EI企业智能类服务等。这些服务具备云服务按需、易维护的优点，能在一定程度上减少用户侧投资和运维的压力。
- 本章，我们将带领大家了解数据库类服务、安全类服务、CDN服务、EI企业智能类服务。

目标

- 学完本课程后，您将能够：
  - 掌握数据库、安全、CDN、EI这些技术领域的基本知识。
  - 了解相关云服务的定位、原理及使用等。

目录

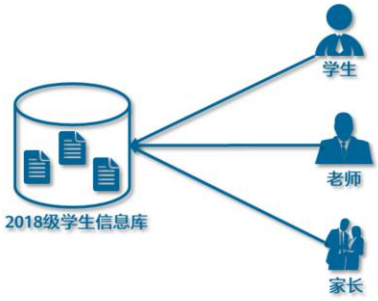
什么是数据库和实例

数据库

- 数据库其实就是文件的集合，只不过它会依照某种数据模型将数据组织起来并存放于其中。

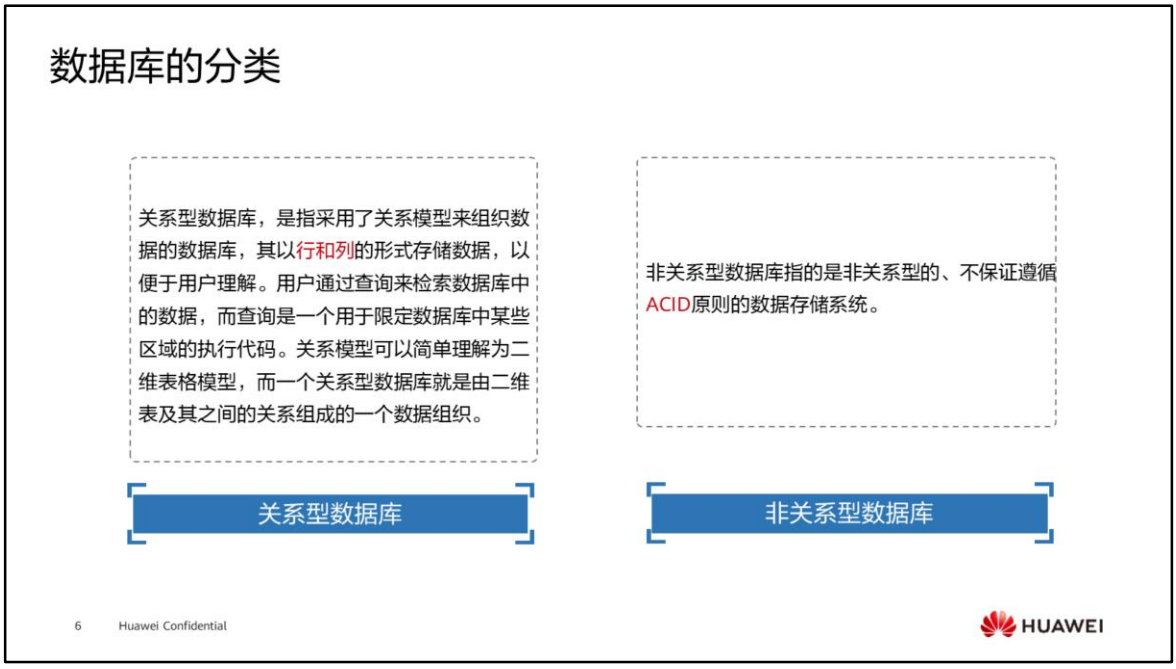
实例

- 实例其实就是内存和后台进程的集合，是位于用户和操作系统之间的一层数据管理软件。



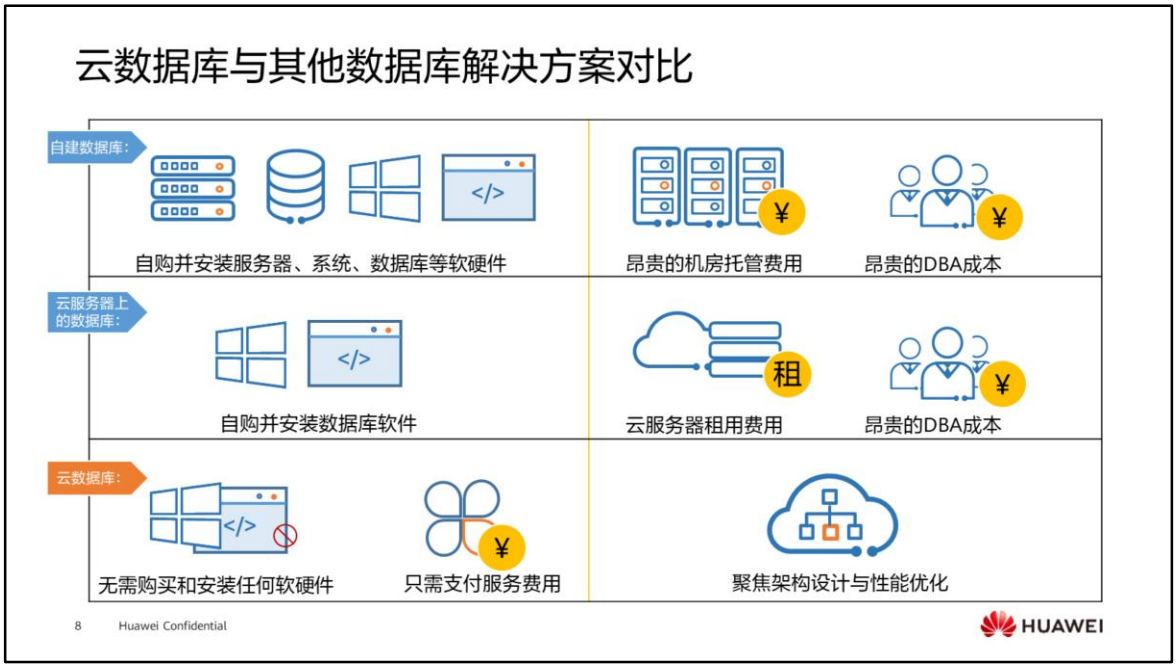
HUAWEI

- 我们都知道存储数据有很多种媒介，如：内存、磁盘等。其实数据库也是存储数据的一种媒介。
- 数据库，望文生意，存储数据的库。更专业点的解释是：存储电子文件的处所。用户可以对文件中的数据进行新增、截取、更新、删除等操作。
- 用户对数据库中的数据做任何的操作，包括数据定义、数据查询、数据维护、数据库运行控制等等都是在数据库实例下进行的，应用程序只有通过数据库实例才能和数据库打交道。
- 云数据库RDS的最小管理单元是实例，一个实例代表了一个独立运行的数据库。用户可以在云数据库RDS系统中自助创建及管理各种数据库引擎的实例。

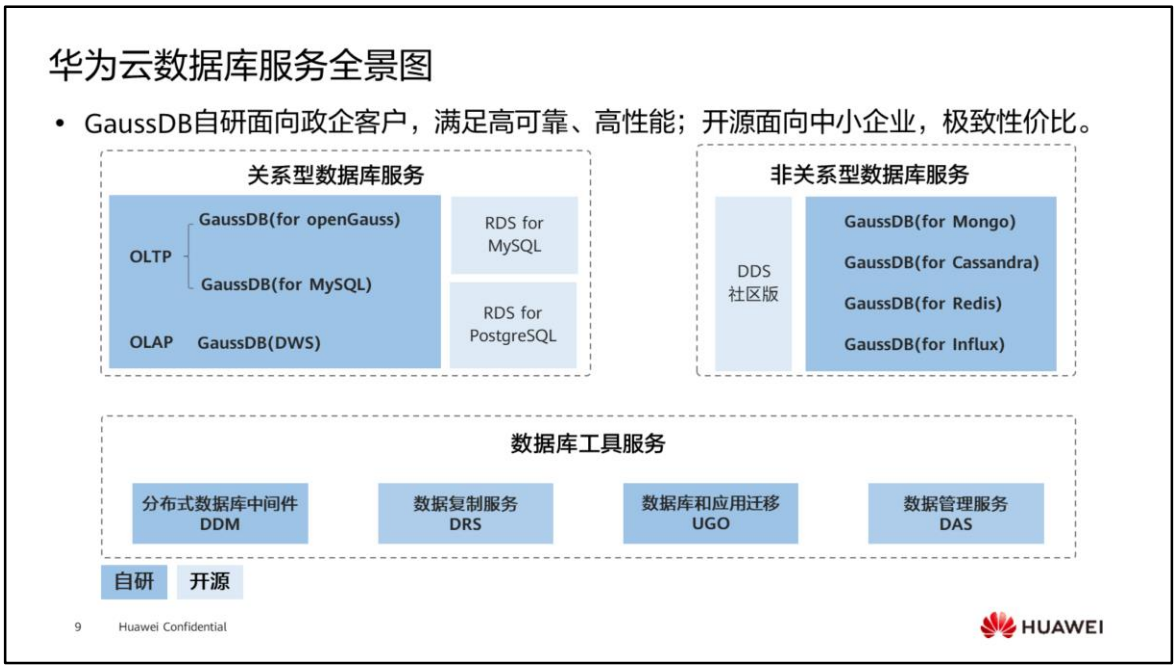


- ACID原则：
  - 原子性（Atomicity）：一个事务的所有系列操作步骤被看成一个动作，所有的步骤要么全部完成，要么一个也不会完成。如果在事务过程中发生错误，则会回滚到事务开始前的状态，将要被改变的数据库记录不会被改。
  - 一致性（Consistency）：一致性是指在事务开始之前和事务结束以后，数据库的完整性约束没有被破坏，即数据库事务不能破坏关系数据的完整性及业务逻辑上的一致性。
  - 隔离性（Isolation）：主要用于实现并发控制，隔离能够确保并发执行的事务按顺序一个接一个地执行。通过隔离，一个未完成事务不会影响另外一个未完成事务。
  - 持久性（Durability）：一旦一个事务被提交，它应该持久保存，不会因为与其他操作冲突而取消这个事务。

目录



- 自建数据库（参考）：需要自购数据库服务器、交换机等硬件，后期硬件损坏和更换至少还要消耗30%费用。1U机柜空间托管费用为至少3000元/年，共有2台1U服务器和1台1U内网交换机需要计费，机房托管费用：3000 × 3 = 9000元。1个初级DBA工程师月薪至少5000/月，假设当前项目占用该工程师30%的工作量，则人员成本为5000 × 12× 30% = 18000元。一次投入的沉没成本大。开源版无性能优化。需要独立准备备份资源，成本极高。公网流量收费，域名费用高。
- 云服务器上的数据库：需要购买云服务器主备实例，云服务租用后物理设备由服务商负责，无需机房托管付费。招聘DBA工程师运维数据库服务。弹性资源。开源版无性能优化。备份空间独立收费。公网流量收费。
- 云数据库：只需购买RDS实例费用，物理设备由服务商负责，无需付费。数据库维护由服务商负责，无人员成本。弹性资源。公网流量免费。免费使用自带的域名。更新速度快，紧跟MySQL最新版本。



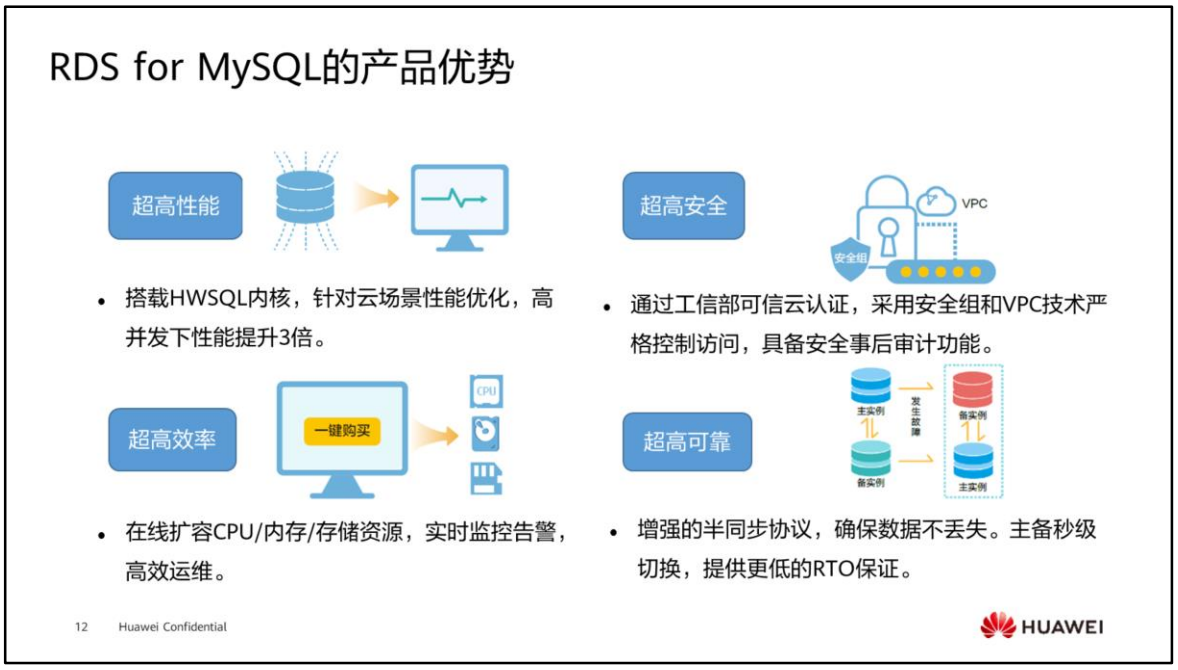
- 华为云数据库服务的介绍：
  - PostgreSQL，一种特性非常齐全的自由软件的对象-关系型数据库管理系统（ORDBMS），是以加州大学计算机系开发的Postgres，4.2版本为基础的对象关系型数据库管理系统。Postgres的许多领先概念只是在比较迟的时候才出现在商业网站数据库中。
  - NoSQL，泛指非关系型的数据库。随着互联网Web2.0网站的兴起，传统的关系数据库在处理Web2.0网站，特别是超大规模和高并发的SNS类型的web2.0纯动态网站时已经显得力不从心，出现了很多难以克服的问题。而非关系型的数据库则由于其本身的特点得到了非常迅速的发展。NoSQL数据库的产生就是为了解决大规模数据集合，多重数据种类带来的挑战，尤其是大数据应用难题，包含了键值（Key-Value）存储数据库，列存储数据库，文档型数据库，图形（Graph）数据库等。
  - 分布式数据库中间件（DDM），解决单机关系型数据库对硬件依赖性强、数据量增大后扩容困难、数据库响应变慢等难题。突破了传统数据库的容量和性能瓶颈，实现海量数据高并发访问。
  - 数据复制服务（DRS），是一种易用、稳定、高效、用于数据库在线迁移和数据库实时同步的云服务。数据复制服务围绕云数据库，降低了数据库之间数据流通的复杂性，有效地帮助用户减少数据传输的成本。
  - 数据管理服务（DAS），是一种提供数据库可视化操作的服务，包括基础SQL操作、高级数据库管理、智能化运维等功能，旨在帮助用户简单、安全、智能地进行数据库管理。

目录

什么是RDS for MySQL

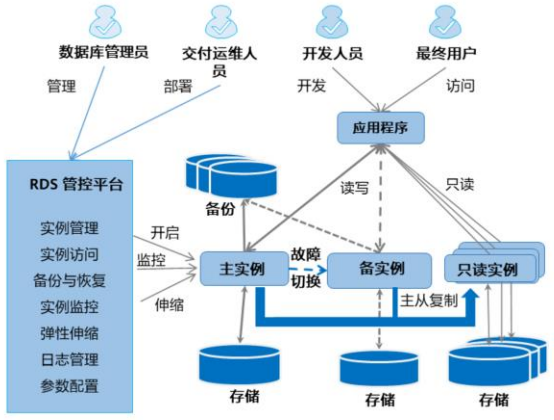
- MySQL是全球最受欢迎的开源数据库之一，性能卓越，搭配LAMP，成为WEB开发的高效解决方案。云数据库MySQL拥有即开即用、稳定可靠、安全运行、弹性伸缩、轻松管理、经济实用等特点，让用户更加专注业务发展。

- 云数据库RDS服务具有完善的性能监控体系和多重安全防护措施，并提供了专业的数据库管理平台， 让用户能够在云上轻松地进行设置和扩展云数据库。通过云数据库RDS服务的管理控制台，用户无需编程就可以执行所有必需任务，简化运营流程，减少日常运维工作量，从而专注于开发应用和业务发展：
  - 架构成熟稳定，支持流行应用程序，适用于多领域多行业；支持各种Web应用，成本低，中小企业首选。
  - 管理控制台提供全面的监控信息，简单易用，灵活管理，可视又可控。
  - 随时根据业务情况弹性伸缩所需资源，按需开支，量身订做。



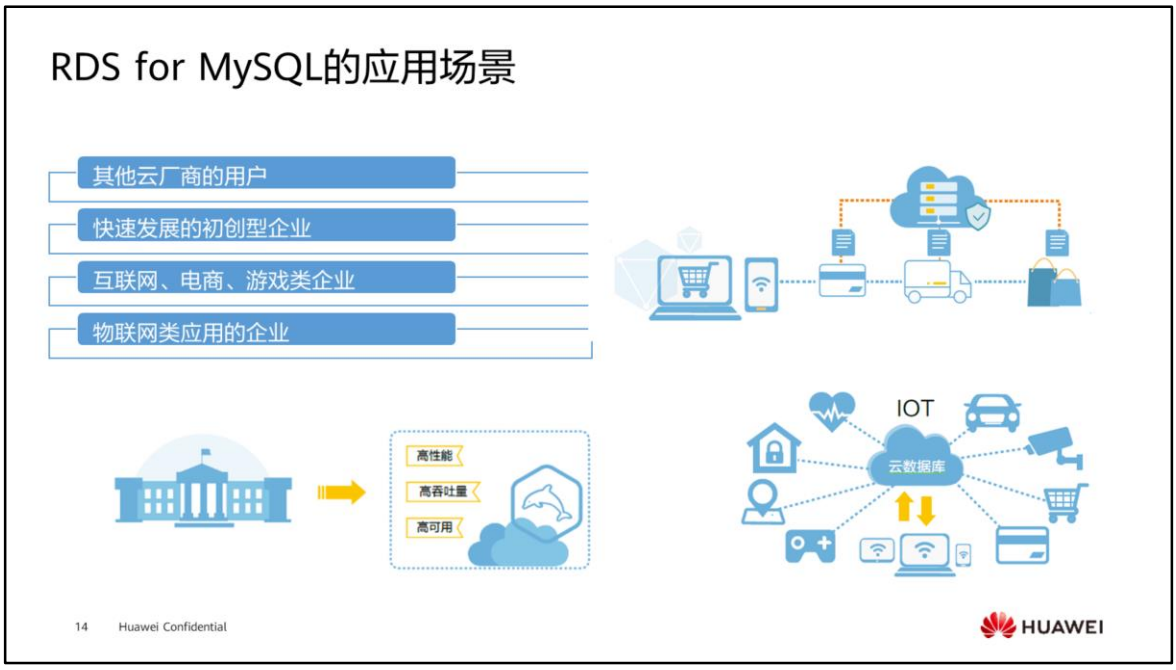
- 超高性能：华为云关系型数据库使用的是华为经过多年的研究、创新和开发，通过多重考验的服务器硬件，为用户带来稳定的、高性能数据库服务。华为云关系型数据库提供慢SQL检测，用户可以根据华为云关系型数据库服务提出的优化建议进行代码优化。可以配合同一地域的弹性云服务器一起使用，通过内网通信，缩短应用响应时间，同时节省公网流量费用。
- 超高安全：通过虚拟私有云（Virtual Private Cloud，简称VPC）和网络安全组实现网络隔离。通过主/子帐号和安全组实现访问控制。通过TLS加密、SSL加密实现传输加密。通过静态加密、表空间加密对数据进行加密。删除云数据库RDS实例时，存储在数据库实例中的数据都会被删除。当用户使用外网连接云数据库RDS实例时，可能会遭受DDoS攻击。云数据库RDS处于多层防火墙的保护之下，可以有力地抗击各种恶意攻击，保证数据安全，防御DDoS攻击、防SQL注入等。
- 超高效率：弹性扩容，快速升级，按需开通。无需投入软硬件成本，按需购买，弹性伸缩。无需系统托管。无需运维。按实际结算，100%利用率。
- 超高可靠性：云数据库RDS服务采用热备架构，故障秒级自动切换。每天自动备份数据，上传到对象存储服务（Object Storage Service，简称OBS）。支持按备份集和指定时间点的恢复。RDS支持将删除的主备或者单机实例，加入回收站管理。

RDS for MySQL的产品架构



HUAWEI

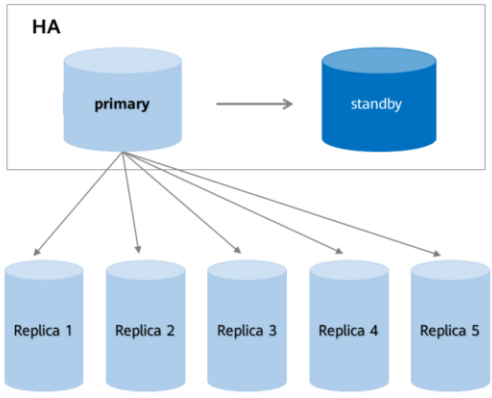
- RDS for MySQL的功能：
  - 弹性伸缩：
    - 水平伸缩：增删只读实例（最多5个）；
    - 垂直伸缩：实例规格变更，存储空间扩容（最大10 TB）。
  - 备份与恢复：
    - 备份：自动备份、手动备份，全量备份、增量备份，备份文件的增、删、查、复制等生命周期管理；
    - 恢复：恢复到备份保留期内任意时间点（Point-In-Time Recovery，PITR）或某个全量备份时间点，恢复到新实例/原实例。备份保存周期高达732天。
  - 日志管理：支持查看慢SQL日志、错误日志和下载日志等。
  - 参数配置：数据库管理员可以根据监控和日志等信息，对数据库引擎参数进行自定义设置，从而优化数据库。参数组的增、删、改、查、重置、比较、复制等生命周期管理，方便用户批量管理实例的数据库引擎参数。



- RDS for MySQL主要的应用场景有几个方向：
  - 除华为云外其他友商公有云平台的用户，这种客户的应用一般会采用MySQL；
  - 快速发展的初创企业考虑规模和成本，MySQL的价格优势较为友好；
  - 互联网、电商、游戏类企业的应用本身就大量采用MySQL，因此对于上云的数据库需求自然也是MySQL；
  - 物联网应用对规模和可靠性的要求比较高，MySQL具备高并发、高性能、支持大量连接、应用无需改造的优势，往往是用户的首选。

RDS for MySQL的特性 - 跨AZ高可用

跨AZ高可用



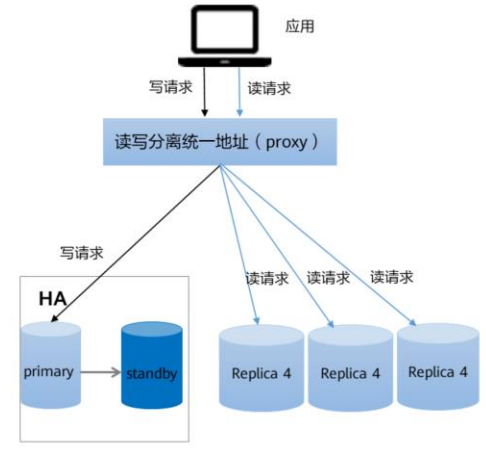
基本功能

- 跨AZ高可用，秒级主备切换。
- 可支持5个只读副本，可分担读流量。
- 备库不可见，对外呈现VIP（虚拟IP）。
- 只读副本不能单独存在，必须先购买单机或者主备。

HUAWEI

- 跨AZ高可用是一种有效的灾备机制，当用户的数据库业务对于可靠性要求较高时，可以通过将数据库主备集群跨AZ部署，以此来达到AZ级别的灾备效果，从而保障整个业务系统的可靠性。

RDS for MySQL的特性 - 读写分离



基本功能

- 统一读写分离地址，读写分离对应用透明。
- 各个节点只读权限可配置。
- 实例健康检查，当发现某个实例出现宕机或者延迟超过阈值时，将不再分配读请求给该实例。

优势点

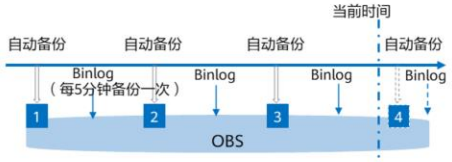
- 提供统一的读写分离地址，读写分离用户业务无需改造。
- 只读节点权重可自行设置。

HUAWEI

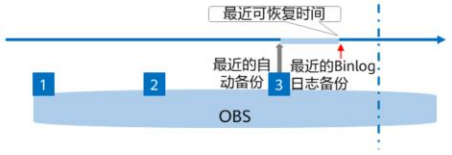
- 数据库的读写分离是指通过一个读写分离的连接地址来实现读写请求的自动转发。创建只读实例后，用户可以开通RDS的读写分离功能来连接地址，写请求自动访问主实例，读请求按照读权重设置自动访问各个实例。

RDS for MySQL的特性 - 任意时间点恢复（PITR）

全量数据备份 + Binlog 日志备份



任意时间点恢复（PITR）



基本功能

- 支持实例级、秒级恢复。
- 支持自定义配置的天数（即备份保留期，取值0-732）保留此自动备份。
- 用户可以将数据库备份恢复到5分钟前至备份保留期内的任意时间点，以此创建新的数据库实例或恢复到原数据库实例上。

优势点

- 备份保存周期和恢复时间相同，可支持732天。
- 备份空间免费赠送购买实例存储空间的100%。

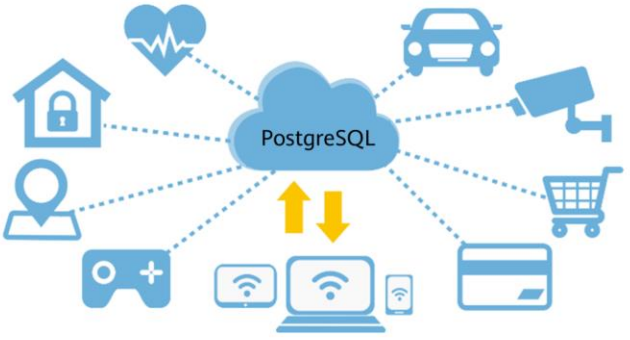
HUAWEI

- 数据库的任意时间点恢复是一种通过备份手段来完成数据恢复的技术，Binlog是记录MySQL数据库表结构变更以及表数据修改的二进制日志。

目录

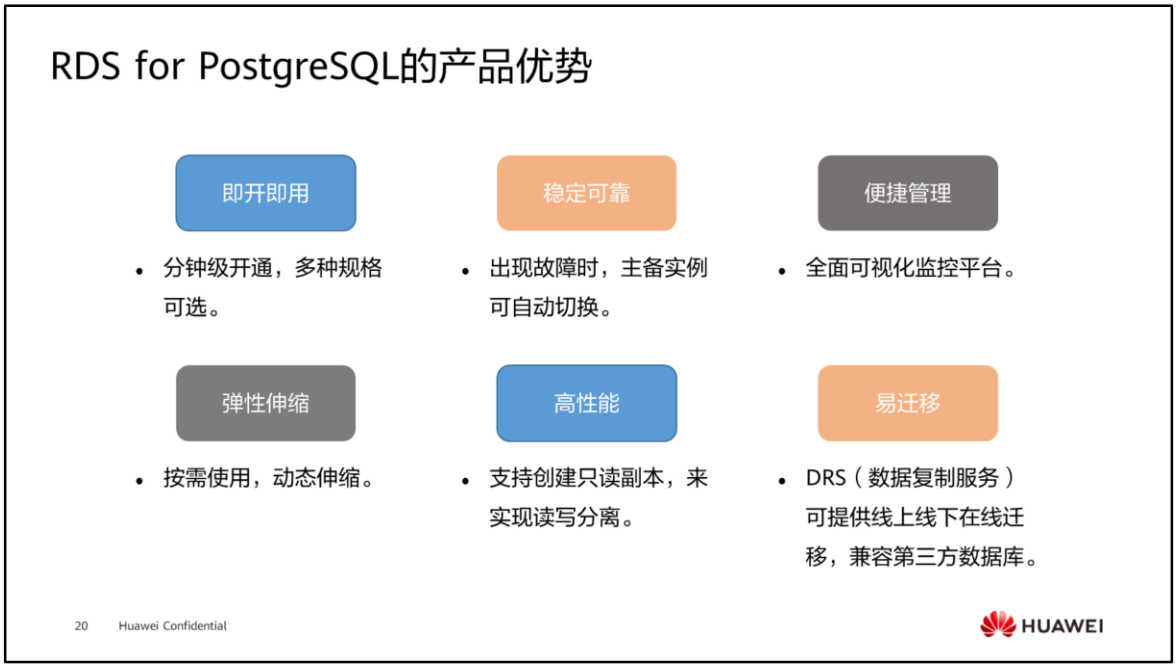
什么是RDS for PostgreSQL

- 华为云数据库PostgreSQL是一种典型的开源关系型数据库，在保证数据可靠性和完整性方面表现出色，支持互联网电商、地理位置应用系统、金融保险系统、复杂数据对象处理等场景。



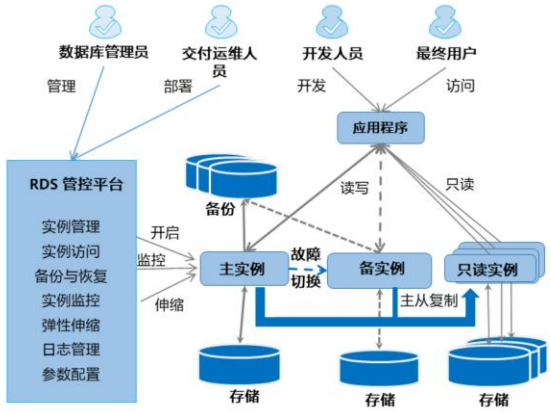
HUAWEI

- PostgreSQL是从加州大学伯克利分校写的POSTGRES软件包发展而来的。经过三十多年的发展，PostgreSQL已经是世界上可以获得的功能最强大的开源数据库。以可靠性、稳定性、数据一致性等优势获得了业内极高的声誉，已成为许多企业的首选开源关系数据库，业界简称PG。
- PostgreSQL是一个开源对象关系型数据库管理系统，并侧重于可扩展性和标准的符合性，被业界誉为“最先进的开源数据库”。云数据库PostgreSQL面向企业复杂SQL处理的OLTP在线事务处理场景，支持NoSQL数据类型（JSON/XML/hstore），支持GIS地理信息处理，在可靠性、数据完整性方面有良好声誉，适用于互联网网站、位置应用系统、复杂数据对象处理等应用场景。
- 支持Postgres插件，空间应用卓越，达到国际标准。
- 适用场景丰富，费用低，随时可以根据业务情况弹性伸缩所需的资源，按需开支，量身订做。



- PostgreSQL的优势有很多，当前主要用于去Oracle场景。

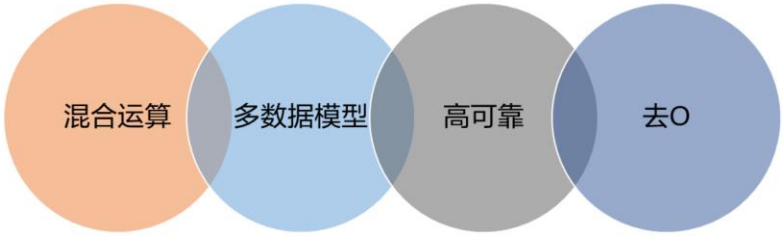
RDS for PostgreSQL的产品架构



HUAWEI

- RDS for PostgreSQL的特点：
  - 数据库类型：提供支持9.5/9.6/10.0/11/12版本，PG增强版。
  - 安全性：多种安全策略保护数据库和用户隐私，例如：VPC、子网、安全组、SSL 等。
  - 高可用性：将主数据库实例数据复制到一个备用数据库实例中，一旦主数据库实例发生故障导致不可用，即可在很短时间内切换到备用数据库实例上。
  - 监控：支持监控数据库实例及数据库引擎的关键性能指标，包括计算/内存/存储容量使用率、I/O活动、数据库连接数、QPS/TPS、缓冲池、读/写活动等。
  - 弹性伸缩：
    - 水平伸缩：增删只读实例（每个数据库集群最多5个只读实例）；
    - 垂直伸缩：数据库实例规格变更；
    - 一键扩容，不中断业务。
  - 日志管理：查询数据库错误日志和慢SQL日志，为用户做数据库调优提供参考。
  - 参数配置：数据库管理员可以根据监控和日志等信息，对数据库引擎参数进行自定义设置，从而优化数据库。

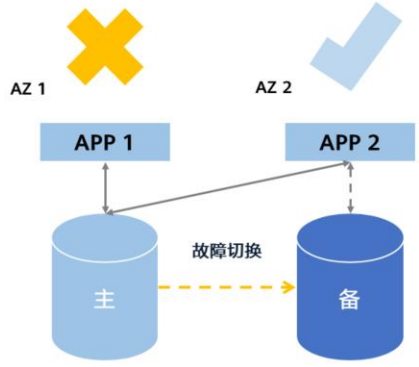
RDS for PostgreSQL的应用场景



HUAWEI

- 混合运算：支持OLTP+OLAP混合场景。
- 多数据模型：适用于时空、地理、异构、图像、文本检索、时序、流计算、多维等场景。
- 高可靠：企业级的可靠性、稳定性、数据一致性。
- 去O：提供两种方案
  - PG增强版；
  - PG社区版+oracle插件。

RDS for PostgreSQL的特性 - 高可用

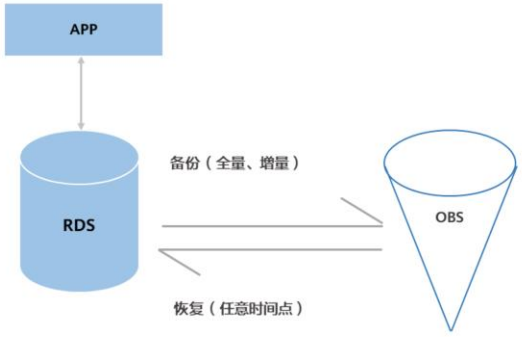


高可用集群：

- 支持可靠性优先和可用性优先两种选择。
- 支持AZ内/跨AZ部署，集群内自动故障切换。
- 支持手动主备切换，模拟故障发生。
- 支持只读实例自动挂到新的主库。
- 集群切换秒级完成。
- 备库不承担流量，保证RTO。
- 采用自研HA Monitor模块。
- 支持VIP切换，应用透明。
- 集群可多次主备倒换。
- 支持自动故障检测。

- RTO：恢复时间点目标。是指灾难发生后，从IT系统宕机导致业务停顿之刻开始，到IT系统恢复至可以支持各部门运作，业务恢复运营之时，此两点之间的时间段。
- HA Monitor：高可用监控。

RDS for PostgreSQL的特性 - 任意时间点恢复



- 备份周期：7~732天
- 按需使用：免费赠送EVS同等空间存储，无容量上限
- 数据可靠性：可达11个9
- 安全加密：KMS服务加密，多重防护

OBS归档存储代替磁带库，支持任意时间点恢复。

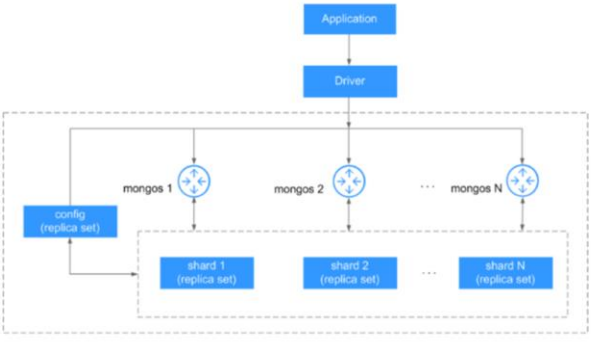
HUAWEI

- RDS：关系型数据库
- EVS：弹性云硬盘
- OBS：对象存储

目录

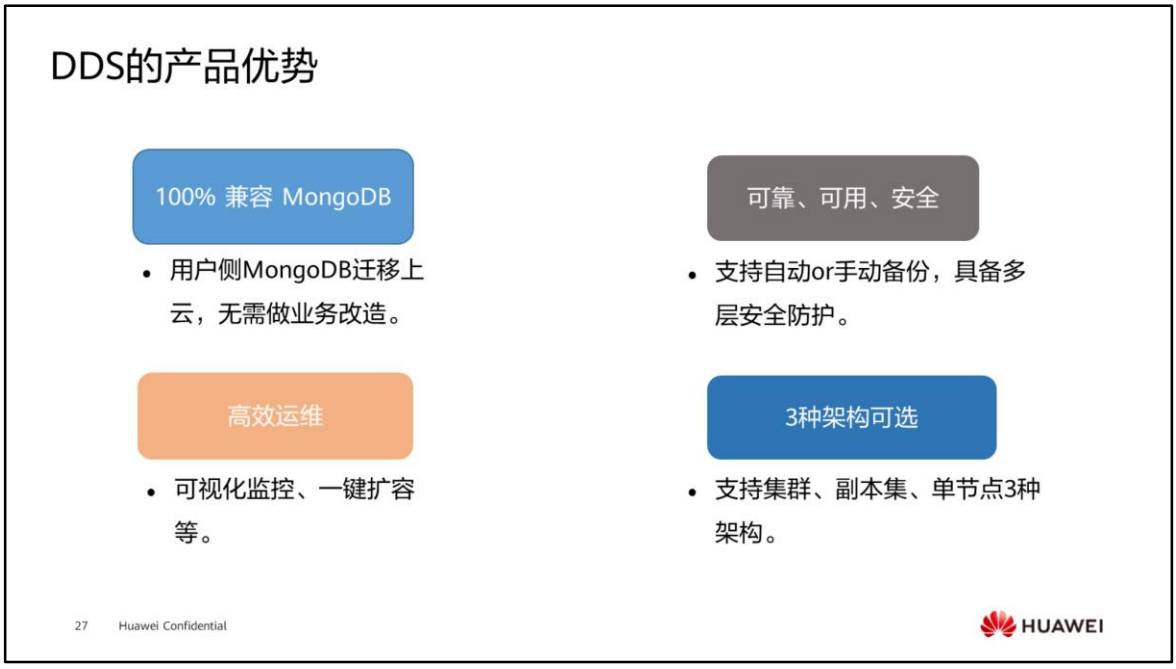
什么是DDS

- 文档数据库服务（Document Database Service，简称DDS）完全兼容MongoDB协议，是一款能够提供安全、高可用、高可靠、弹性伸缩和易用的数据库服务，同时支持一键部署、弹性扩容、容灾、备份、恢复、监控和告警等功能。



HUAWEI

- 每个集群即一个独立运行的文档数据库，分片集群架构由路由（mongos）、配置（config）和分片（shard）组成。
- 数据读写请求经mongos分发，通过查询config信息，并行分配到相应shard，可轻松应对高并发场景，且config和shard均采用三副本架构，保证高可用，集群架构如上图所示。

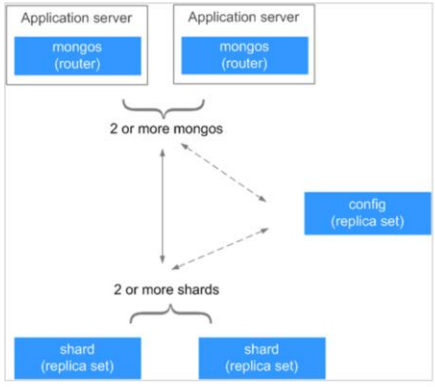


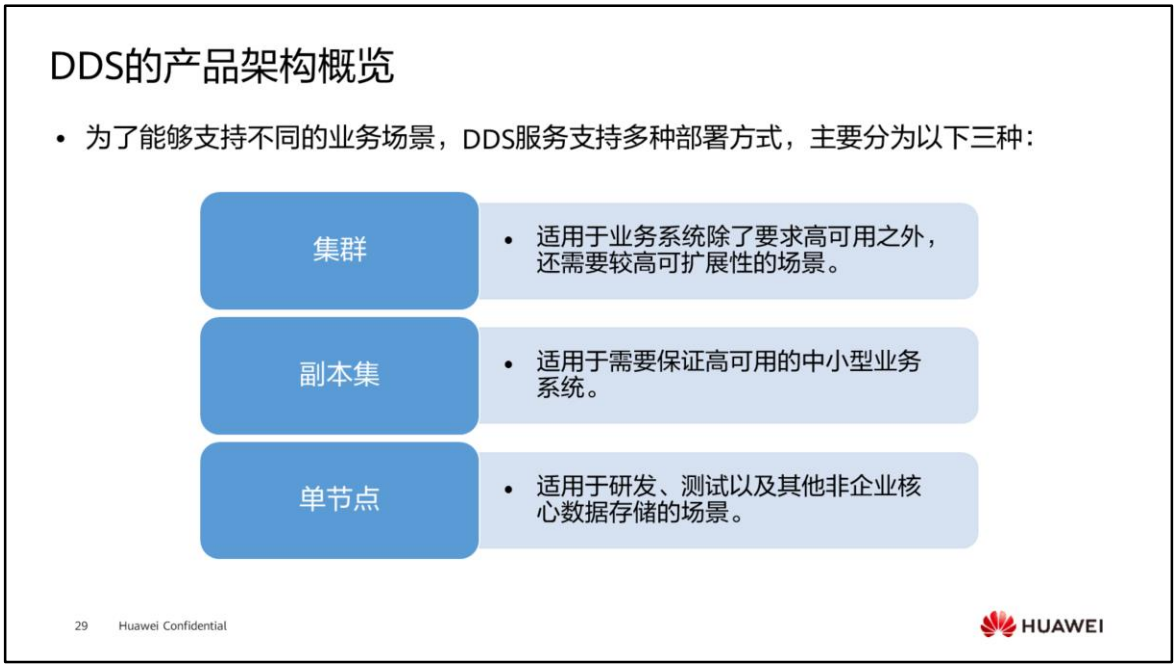
- 完全兼容：
  - 文档数据库服务是面向文档型的NoSQL数据库，完全兼容MongoDB协议。
- 可靠、可用、安全：
  - 通过虚拟私有云、子网、安全组、存储加密、DDoS防护以及SSL安全访问等多层安全防护体系，有力地抗击各种恶意攻击，保证数据安全。提供审计日志功能，审计日志最长支持保存两年。支持细粒度权限控制。集群和副本集支持高可用，一旦Primary节点发生故障导致节点不可用，即可在很短时间内切换到Secondary节点上，切换过程对应用透明。
  - 支持设置自动备份策略和实时手动备份。其中，自动备份保留时长最多达到732天，实时手动备份长期保留。
  - 支持通过备份文件进行数据恢复。其中，副本集支持实例级时间点恢复和库表级时间点恢复。
- 高效运维：
  - 控制台提供可视化实例管理平台，对实例重启、备份、数据恢复等高频需求实现一键式便捷操作。
  - 实时监控数据库实例及引擎的关键性能指标，包括CPU、内存使用率，磁盘利用率，command、delete、insert语句执行频率，活跃连接数等指标。

DDS的常用概念

- DDS集群通常由mongos、config、shard组成，每个组件都有着不同的作用。

mongos	• 负责查询与数据写入的路由，是实例访问的统一入口。
config	• 负责存储实例的配置信息，由1个副本集组成。
shard	• 集群实例的shard，负责存储用户的数据。

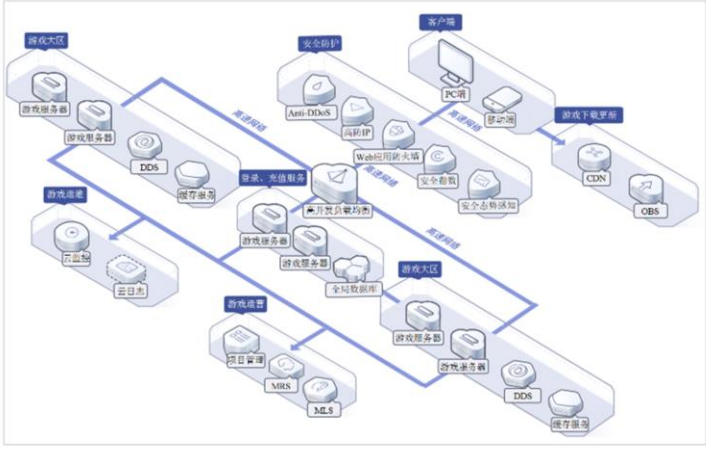




- DDS的部署方式主要有三种：
  - 集群方式：每个集群即一个独立运行的文档数据库，由路由（mongos）、配置（config）和分片（shard）组成。
  - 副本集方式：副本集架构由主节点、备节点和隐藏节点组成，自动搭建好三节点的副本集供用户使用，节点之间数据自动同步，保证数据的高可靠性。
  - 单节点架构是作为集群和副本集架构的补充，一般用于研发、测试以及其他非企业核心数据存储的场景。

应用场景 - 游戏

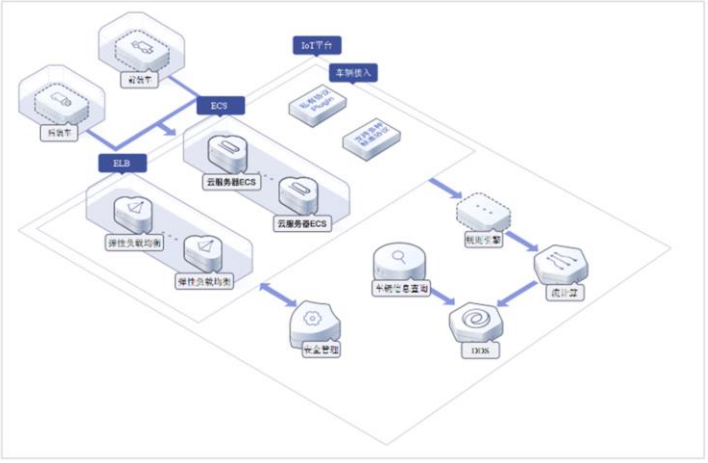
- 场景描述：在游戏应用中，可以将一些用户信息，如用户装备、用户积分等存储在DDS数据库中。游戏玩家活跃高峰期，对并发能力要求较高，可以使用DDS的集群类型，应对高并发场景。DDS副本集和集群架构的高可用特性，能够满足游戏在高并发场景下持续稳定运行。



HUAWEI

应用场景 - IoT

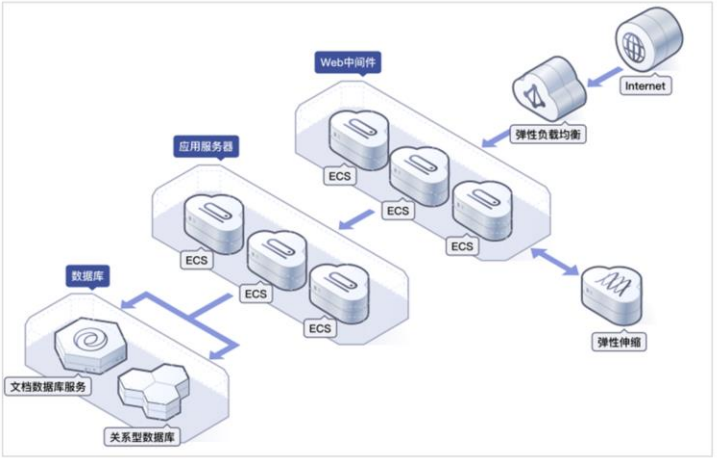
- 场景描述：DDS兼容MongoDB，具有高性能和异步数据写入功能，特定场景下可达到内存数据库的处理能力。同时，DDS中的集群实例，可动态扩容和增加mongos和shard组件的性能规格和个数，性能及存储空间可实现快速扩展，非常适合IoT高并发写入的场景。



HUAWEI

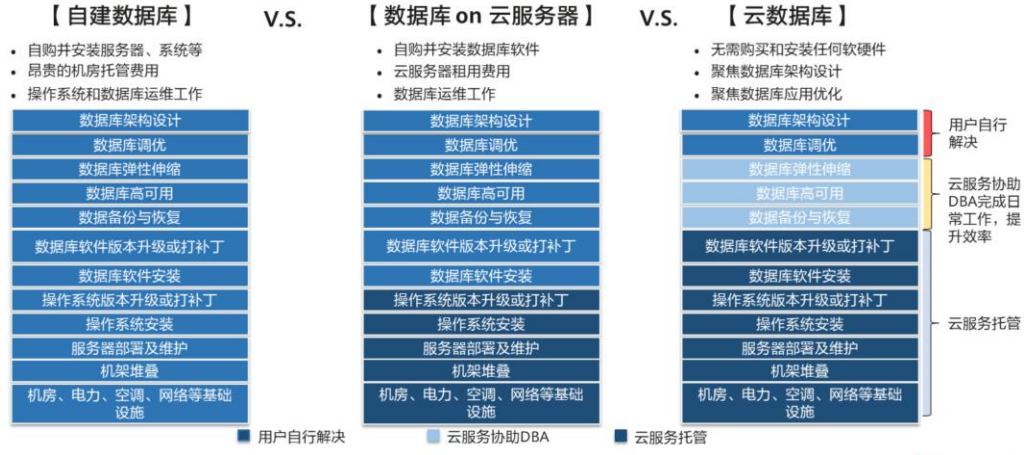
应用场景 - 互联网

- 场景描述：DDS的副本集模式采用三节点Replica Set的高可用架构，三个数据节点组成一个反亲和组，部署在不同的物理服务器上，自动同步数据。Primary节点和Secondary节点提供服务，两个节点分别拥有独立内网地址，配合Driver实现读取压力分配。



云数据库与其它数据库解决方案的区别

- **价值**：云数据库服务能帮助DBA实现数据库运维效率提升，让客户数据库团队能深入到应用的数据架构设计中。



HUAWEI

- 云数据库可以帮助用户减少数据库总拥有成本（TCO）和运维工作量（O&M），用户可以将主要精力聚焦在核心业务上。

目录

云上客户的安全诉求

CSA Top 威胁

- 数据泄露
- 身份、凭证和访问管理不足
- 不安全的接口和应用程序编程接口（API）
- 系统漏洞
- 账户劫持
- 恶意的内部人员
- 高级持续性威胁（APT）
- 数据丢失
- 尽职调查不足
- 滥用和恶意使用云服务
- 拒绝服务（DoS）
- 共享的技术漏洞

企业上云的关键安全诉求

业务连续不中断

- 防网络攻击、防黑客入侵、法律遵从、合规

运维全程可管控

- 配置安全策略、风险识别和处理、操作可审计、追溯

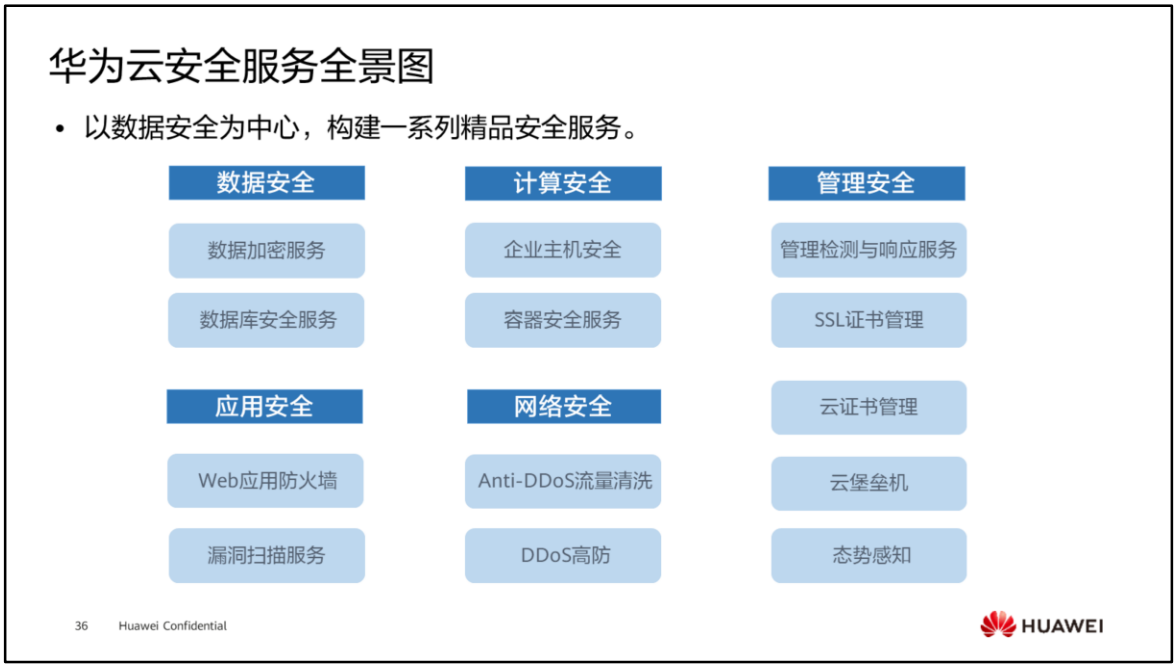
数据保密不扩散

- 防外部窃取、内部非授权员工不可见、云服务商不可见

国内法律合规要求

《网络安全法》
《网络安全等级保护制度》

第31条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦**遭到破坏**、**丧失功能**或**数据泄露**，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在**网络安全等级保护制度**的基础上，实行**重点保护**。



- 安全服务的种类有很多，从不同角度去看待安全，就会有不同类型的安全服务，本次我们主要从五大类来简单归纳。

目录

什么是HSS

- 企业主机安全服务（Host Security Service，HSS）通过提供主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

HSS的产品优势

集中管理

- 可实现检测和防护的一体化管控，让管理更简单。

精准防御

- 拥有先进的检测技术和丰富的检测库，提供精准防御。

轻量Agent

- Agent占用资源极少，不影响主机系统的正常运行。

全面防护

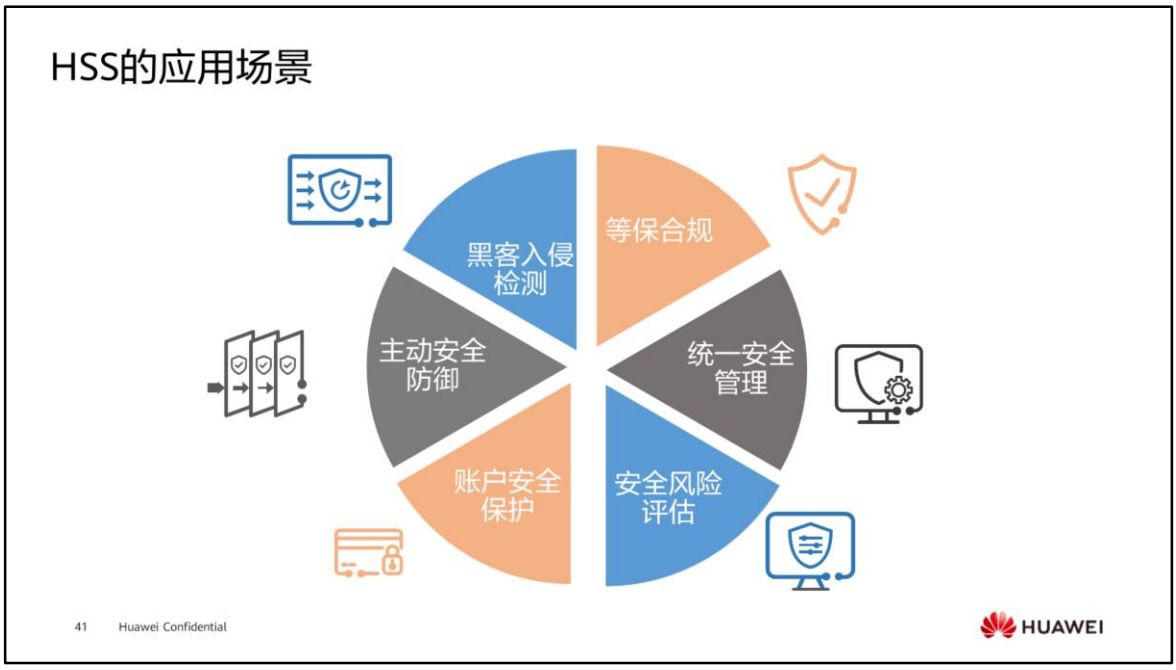
- 提供事前预防、事中防御、事后检测的全面防护。

HSS的工作原理

- 在主机中安装Agent后，用户的主机将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，用户可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

HUAWEI

- 组件功能：
  - 管理控制台：可视化的管理平台，便于用户集中下发配置信息，查看在同一区域内主机的防护状态和检测结果
  - HSS云端防护中心：HSS服务的server端
  - Agent：Agent通过HTTPS和WSS协议与HSS云端防护中心进行连接通信，默认端口：443

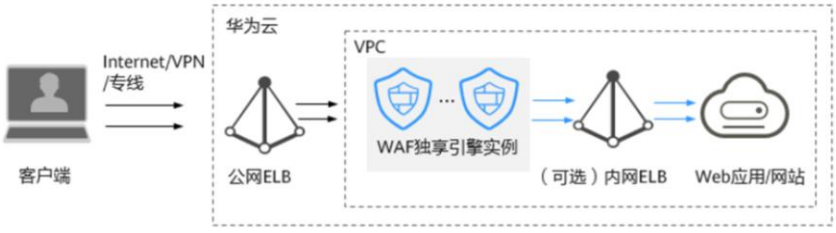


- HSS的应用场景：
  - 等保合规：企业主机安全是等保合规的关键项，企业主机安全服务提供的入侵检测功能，能协助各企业保护企业云服务器账户、系统的安全。
  - 统一安全管理：企业主机安全服务提供统一的主机安全管理能力，帮助用户更方便地管理云服务器的安全配置和安全事件，降低安全风险和管理成本。
  - 安全风险评估：对主机系统进行安全评估，将系统存在的各种风险（账户、端口、软件漏洞、弱口令等）进行展示，提示用户及时加固，消除安全隐患。
  - 账户安全保护：提供覆盖事前、事中和事后的账户安全保护功能。支持双因子认证登录，防止用户云服务器上的账户遭受暴力破解攻击，提高云服务器的安全性。
  - 主动安全防御：通过清点主机安全资产，管理主机漏洞与不安全配置，预防安全风险；通过网络、应用、文件主动防护引擎，主动防御安全风险。
  - 黑客入侵检测：提供主机全攻击路径检测能力，能够实时、准确地感知黑客入侵事件，并提供入侵事件的响应手段，对业务系统“零”影响，有效应对APT攻击等高级威胁。

目录

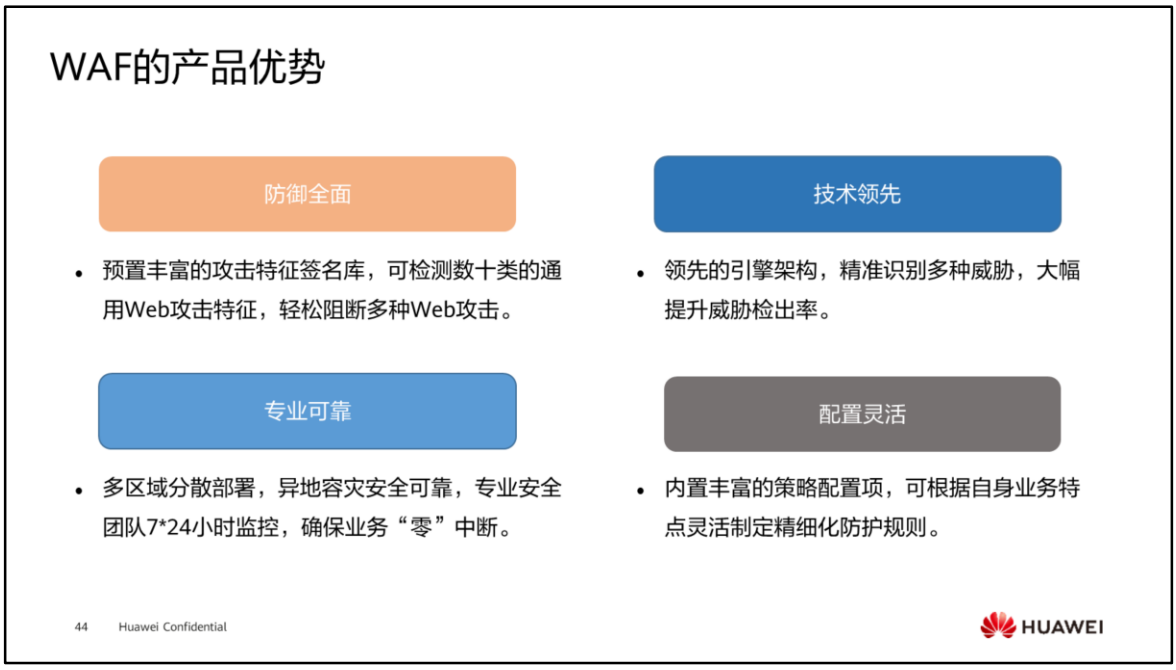
什么是WAF

- WAF：Web应用防火墙（Web Application Firewall），通过对网站业务流量进行全方位检测和防护，智能识别恶意请求特征和防御未知威胁，避免源站被黑客恶意攻击和入侵，防止核心资产遭窃取，为网站业务提供安全保障。



HUAWEI

- 随着互联网的发展，企业开始逐步将关键的业务功能迁移到了Web应用，虽然迁移到Web应用带来了经济利益并提高了业务的灵活性，但同时也带来了新的安全风险和合规性方面的需求，而近些年来，针对Web应用的攻击越来越多，新型的攻击手段层出不穷，传统的防火墙技术已经无法针对这些Web应用提供安全防护能力。在这种情况下，WAF成为了抵御应用层攻击强有力的工具。



- Web基础防护能力：
- 覆盖OWASP（Open Web Application Security Project）TOP 10中常见安全威胁，通过预置丰富的信誉库，对漏洞攻击、网页木马等威胁进行检测和拦截。
- 全面的攻击防护支持SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击检测和拦截。
- Webshell检测防护通过上传接口植入网页木马。
- 识别精准：
    - 内置语义分析+正则双引擎，黑白名单配置，误报率更低。
    - 支持防逃逸，自动还原常见编码，识别变形攻击能力更强。默认支持的编码还原类型：url_encode、Unicode、xml、C-OCT、十六进制、html转义、base64、大小写混淆、javascript/shell/php等拼接混淆。
- 深度检测深度反逃逸识别（支持同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等的防护）。
- header全检测支持对请求里header中所有字段进行攻击检测。

WAF的工作原理

- 网站成功接入WAF后，所有网站访问请求将先流转到WAF进行监控，恶意攻击流量在WAF上被检测过滤，而正常流量返回给源站，从而确保源站安全、稳定、可用。

HUAWEI

- 购买WAF后，在WAF管理控制台将网站添加并接入WAF。网站成功接入WAF后，网站所有访问请求将先流转到WAF，恶意攻击流量在WAF上被检测过滤，而正常流量返回给源站，从而确保源站安全、稳定、可用。
- 流量经WAF返回源站的过程称为回源。WAF通过回源IP代替客户端发送请求到源站服务器，在源站服务器看来，接入WAF后所有源IP都会变成WAF的回源IP，进而隐藏源站。

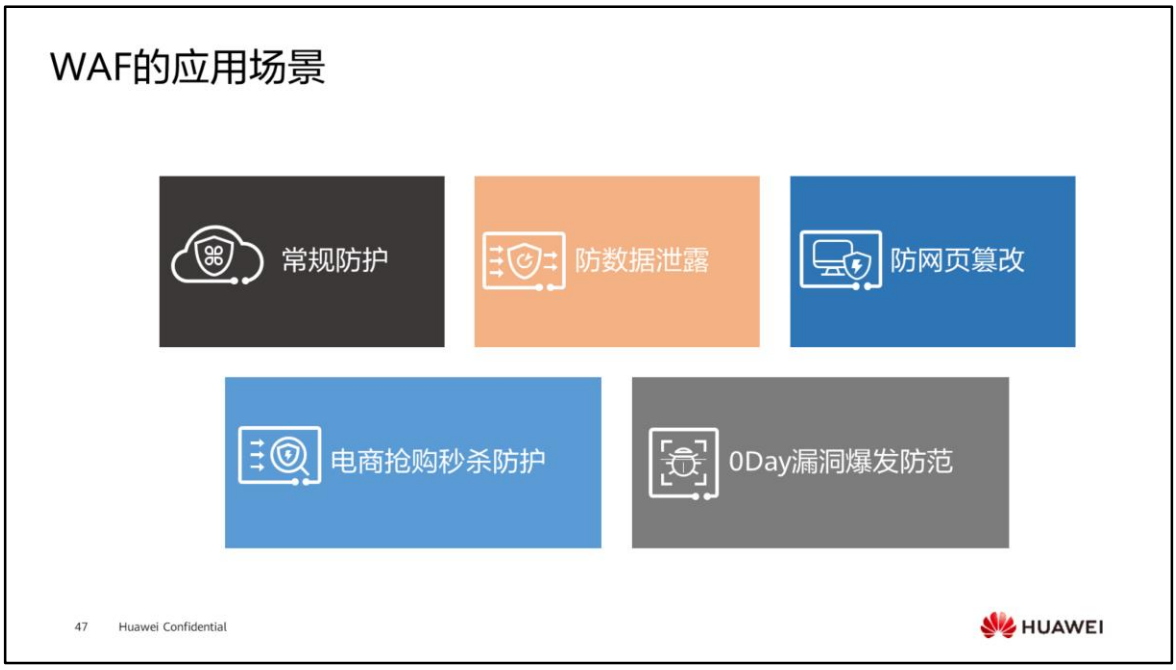
WAF的产品架构

- 为了能够支持不同的业务场景，WAF服务支持多种部署方式，主要分为以下三种：

云模式	• 业务服务器部署在华为云上、非华为云或线下。
独享模式	• 业务服务器部署在华为云上。
ELB模式	• 业务服务器部署在华为云上。

HUAWEI

- WAF的三种部署方式：
  - 云模式：
    - 防护对象：域名。
    - 弹性扩容能力强，可以防护华为云、非华为云和云下的Web业务，支持IPv6防护。
  - 独享模式：
    - 防护对象：域名或IP。
    - 资源由用户独享，可满足大规模流量攻击场景防护需求，时延低。
  - ELB模式：
    - 防护对象：域名或IP。
    - 旁路部署，业务零影响。当WAF发生故障时，流量将直接通过ELB发送给后端，不影响用户正常业务。

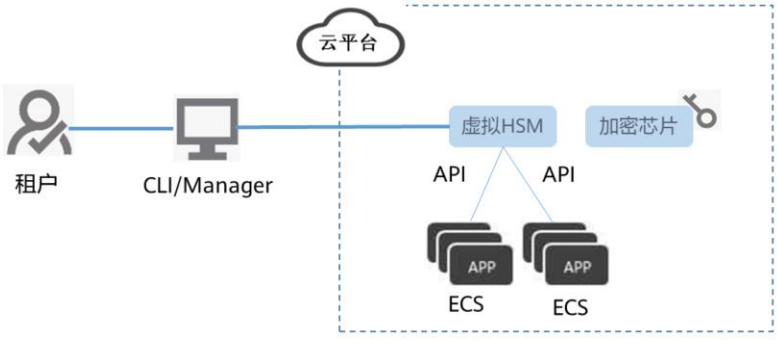


- WAF的应用场景：
  - 常规防护：帮助用户防护常见的Web安全问题，比如命令注入、敏感文件访问等高危攻击。
  - 电商抢购秒杀防护：当业务举办定时抢购秒杀活动时，业务接口可能在短时间承担大量的恶意请求。Web应用防火墙可以灵活设置CC攻击防护的限速策略，能够保证业务服务不会因大量的并发访问而崩溃，同时尽可能地给正常用户提供业务服务。
  - 0Day漏洞爆发防范：当第三方Web框架、插件爆出高危漏洞，业务无法快速升级修复时，Web应用防火墙会第一时间升级预置防护规则，保障业务安全稳定。WAF相当于第三方网络架构加了一层保护膜，和直接修复第三方架构的漏洞相比，WAF创建的规则能更快地遏制住风险。
  - 防数据泄露：恶意访问者通过SQL注入，网页木马等攻击手段，入侵网站数据库，窃取业务数据或其他敏感信息。用户可通过Web应用防火墙配置防数据泄露规则，以实现：
    - 精准识别：采用语义分析+正则表达式双引擎，对流量进行多维度精确检测，精准识别攻击流量；
    - 变形攻击检测：支持7种编码还原，可识别更多变形攻击，降低Web应用防火墙被绕过的风险。
  - 防网页篡改：攻击者利用黑客技术，在网站服务器上留下后门或篡改网页内容，造成经济损失或带来负面影响。用户可通过Web应用防火墙配置网页防篡改规则，以实现：挂马检测和页面不被篡改。

目录

什么是DEW

- 数据加密服务（Data Encryption Workshop，简称DEW）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、密钥对管理等服务，安全可靠地为用户解决数据安全、密钥安全、密钥管理等复杂问题。

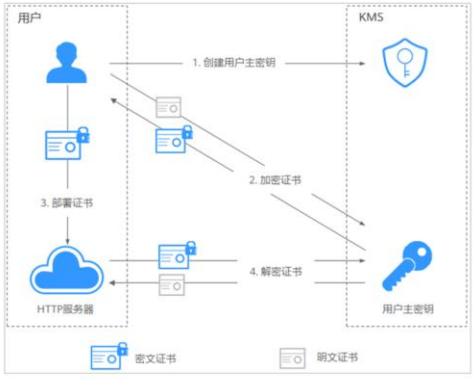


- 数据是企业的核心资产，每个企业都有自己的核心敏感数据，数据一旦泄露将对公司造成不可估量的损失，这些数据都需要被加密，从而保护他们不会被他人窃取，因此华为推出数据加密服务为客户的数据安全保驾护航。
- 密钥由硬件安全模块（Hardware Security Module，HSM）保护，并与多个华为云服务集成。用户也可以借此服务开发自己的加密应用。

- DEW服务分为三块，接下来我们将逐一介绍每一块内容。

密钥管理应用场景 - 小数据加解密

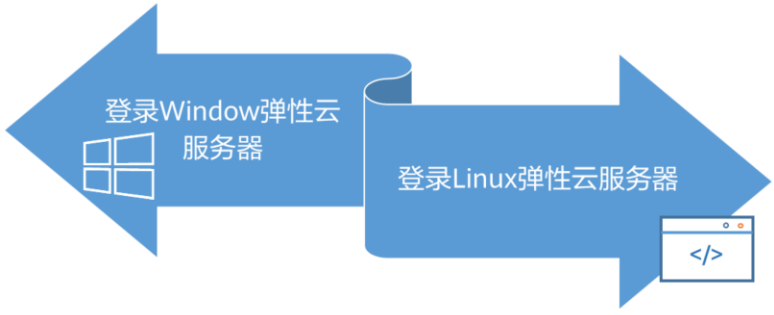
- 场景描述：当有少量数据（口令、证书、电话号码等）需要加解密时，用户可以通过KMS界面使用在线工具加解密数据，或者调用KMS的API接口使用指定的用户主密钥直接加密、解密数据。



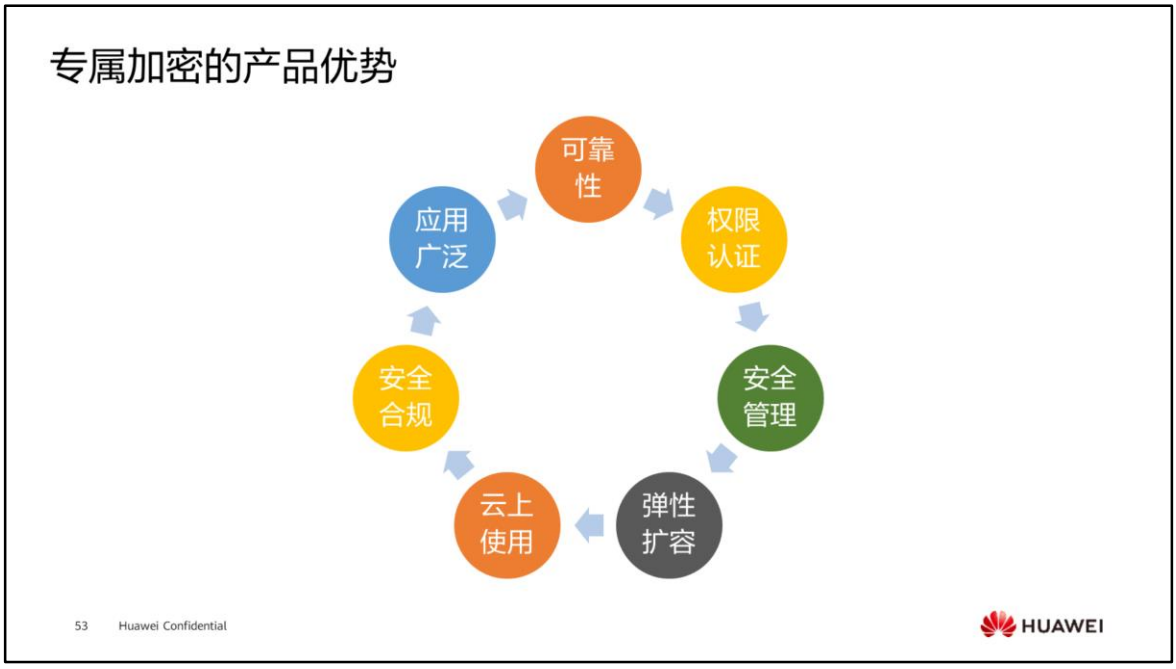
HUAWEI

- 上图流程说明如下：
  - 用户需要在KMS中创建一个用户主密钥。
  - 用户调用KMS的“encrypt-data”接口，使用指定的用户主密钥将明文证书加密为密文证书。
  - 用户在服务器上部署密文证书。
  - 当服务器需要使用证书时，调用KMS的“decrypt-data”接口，将密文证书解密为明文证书。

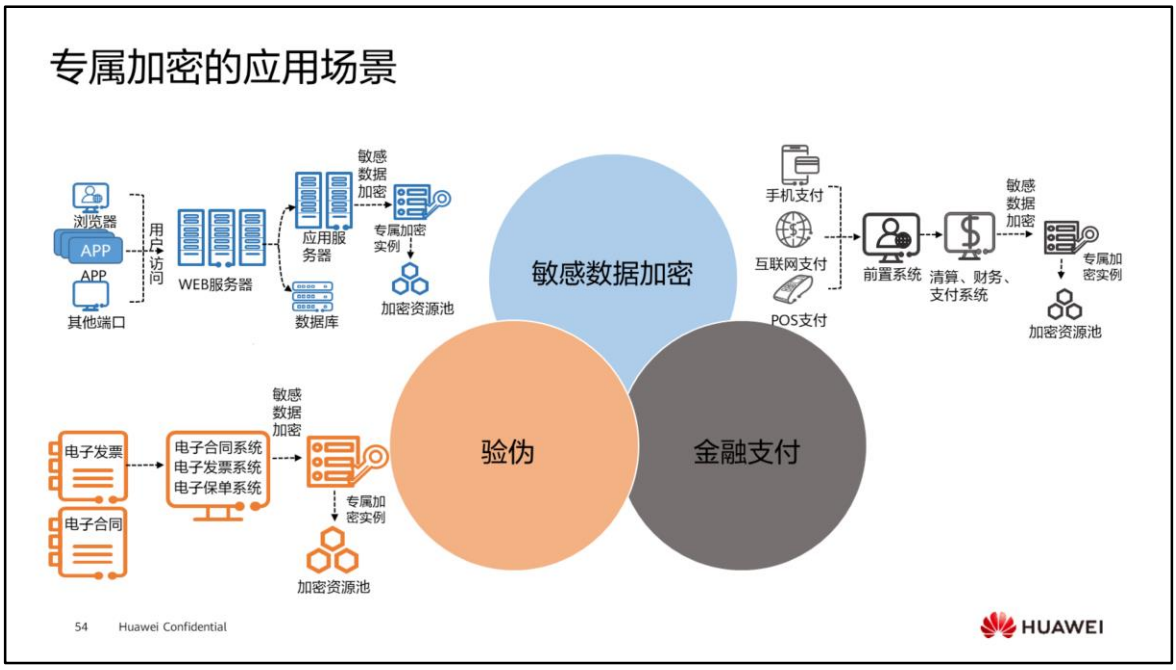
密钥对管理的应用场景



- 登录Windows操作系统的弹性云服务器时，需要使用密码方式登录。此时，用户需要先根据购买弹性云服务器时下载的私钥文件，获取该弹性云服务器初始安装时系统生成的管理员密码（Administrator帐户或Cloudbase-init设置的帐户）。该密码为随机密码，安全性高，请放心使用。



- 产品优势：
  - 云上使用：专属加密旨在满足用户将线下加密设备能力转移到云上的要求，降低运维成本。
  - 弹性扩容：灵活调整专属加密的数量，满足不同业务的加解密运算要求。
  - 安全管理：专属加密实例设备管理与内容（敏感信息）管理权限分离，用户作为设备使用者完全控制密钥的产生、存储和访问授权，Dedicated HSM只负责监控和管理设备及其相关网络设施。即使专属加密的运维人员也无法获取到用户的密钥。
  - 权限认证：敏感指令支持分类授权控制，有效防止越权行为。支持用户名口令认证、数字证书认证等多种权限认证方式。
  - 可靠性：基于国家密码局认证或FIPS 140-2第3级验证的硬件加密机，对高安全性要求的用户提供高性能专属加密服务。专属加密实例之间独享加密芯片，即使部分硬件芯片损坏也不影响使用。
  - 安全合规：提供经国家密码管理局检测认证的专属加密实例，帮助用户保护弹性云服务器上数据的安全性和隐私性要求，满足监管合规要求。
  - 应用广泛：提供认证合规的金融加密机、服务器加密机以及签名验签服务器等，灵活支撑用户业务场景。

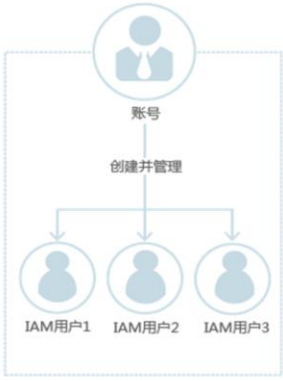


- 应用场景：
  - 敏感数据加密：适用于政府公共事业、互联网企业、包含大量敏感信息的系统应用。
  - 金融支付：适用于交通卡支付、电商支付、各种预付费卡支付等系统应用。
  - 验伪：保证电子合同、电子发票、电子保单、电子病例在传输、存储过程中的保密性和完整性。

目录

什么是IAM

- 统一身份认证（Identity and Access Management，简称IAM）是华为云提供身份认证和权限管理的基础服务，可以帮助用户管理用户，且安全地控制用户对华为云服务和资源的访问权限。

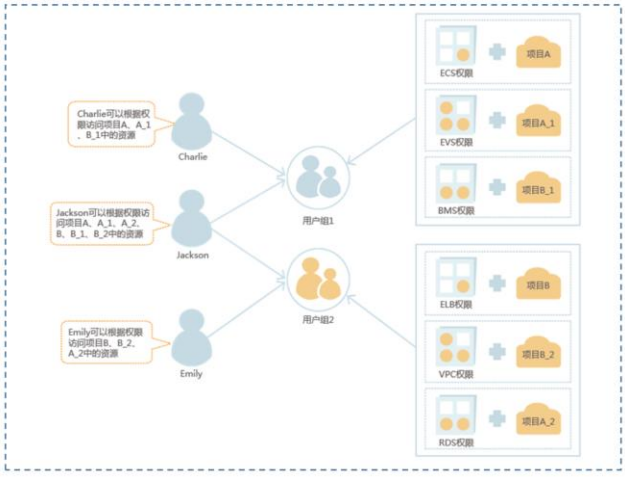


HUAWEI

- 在企业中一般有多个IT管理员，这些IT运维人员各有分工，每人管辖的资源不一样，岗位不相同，对应的权限也需要区分。因此不能让每个人都拿到超级管理员的权限，需要做分权分域管理。华为云IAM允许企业主账号分配多个子账号，以满足分权分域的需求。
- 身份凭证是识别用户身份的依据，用户通过控制台或者API访问华为云时，需要使用身份凭证来通过系统的鉴权认证。身份凭证包括密码和访问密钥，用户可以在IAM中管理自己以及帐号中IAM用户的身份凭证。

IAM的产品优势

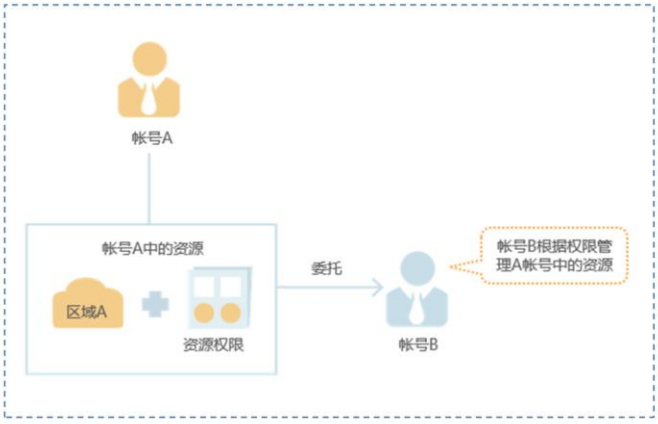
产品优势——对华为云的资源进行精细访问控制



HUAWEI

- 当用户在华为云购买了多种资源，例如弹性云服务器、云硬盘、裸金属服务器等，如果用户团队或应用程序需要使用用户在华为云中的资源，此时就可以使用IAM的用户管理功能，给员工或应用程序创建IAM用户，并授予IAM用户刚好能完成工作所需的权限，新创建的IAM用户可以使用自己单独的用户名和密码登录华为云。IAM用户的作用是多用户协同操作同一帐号时，避免分享帐号的密码。

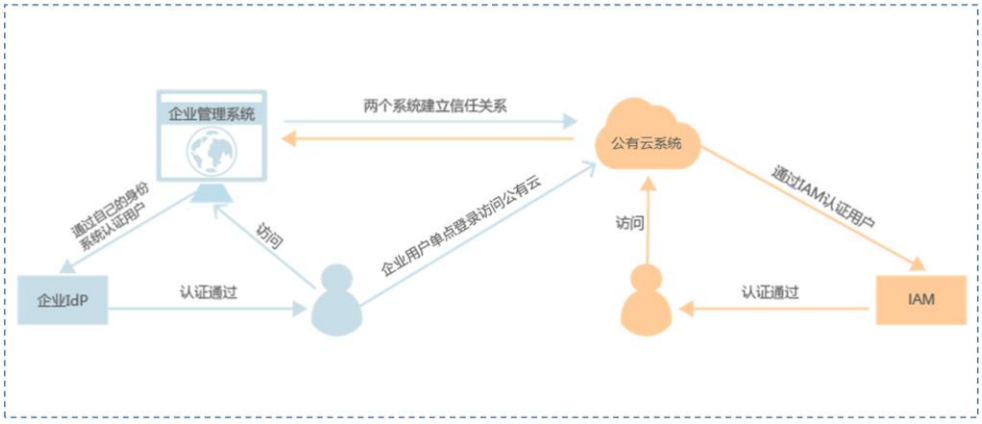
产品优势——跨帐号的资源操作与授权



HUAWEI

- 当用户希望把在华为云上购买的部分资源委托给一家专业的代运维公司来运维，通过IAM的委托功能，代运维公司可以使用自己的帐号对委托的资源进行运维。当委托关系发生变化时，用户可以随时修改或撤消对代运维公司的授权。图中帐号A即为委托方，帐号B为被委托方。

产品优势 - 使用企业已有帐号登录华为云



HUAWEI

- 当用户希望本企业员工可以使用企业内部的认证系统登录华为云，而不需要在华为云中重新创建对应的IAM用户时，可以使用IAM的身份提供商功能，建立用户所在企业与华为云的信任关系，通过联合认证使员工使用企业已有帐号直接登录华为云，实现单点登录。

目录

客户痛点与诉求

用户体验差

访问卡顿、访问速度慢
下载失败、访问失败
观看视频过程中的卡顿

高并发

访问的突发，下载量的高并发：如电商大促，热门游戏发布、热播剧上映

回源带宽高，成本压力大

不使用CDN，所有内容都必须回源，回源带宽高，成本压力大。

运维压力大

带宽压力大
请求数并发压力大
平台运维压力大

什么是CDN

- 内容分发网络（Content Delivery Network，简称CDN）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，使用户可以就近获得所需的内容。

- CDN服务缩短了用户查看内容的访问延迟，提高了用户访问网站的响应速度与网站的可用性，解决了网络带宽小、用户访问量大、网点分布不均等问题。

华为云CDN国内节点分布

- **国内节点分布：**与主导运营商合营的海量节点，国内加速节点2000+，海量带宽储备，带宽扩容无瓶颈。节点带宽储备能力≥100Tbps。涵盖了电信、联通、移动、教育网等主流运营商，以及多家中小型运营商。保证将用户请求精准调度至最优边缘节点，提供了有效且稳定的加速效果。

中国大陆节点资源图

HUAWEI

华为云CDN海外节点分布

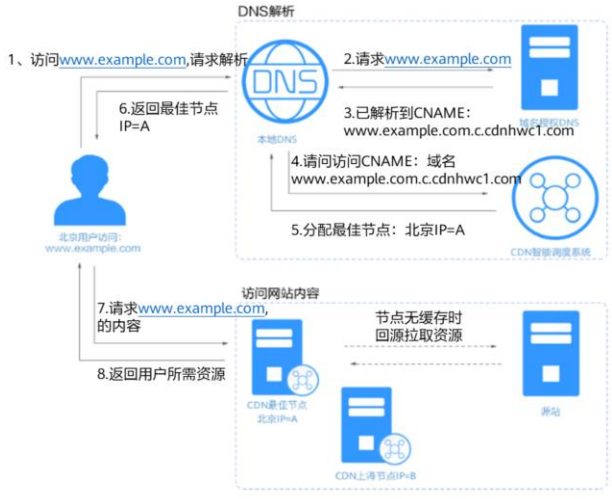
- **海外节点分布：**海外加速节点500+，覆盖全球70多个国家，跨国专线资源，T级冗余带宽，东南亚节点丰富且优质。

HUAWEI

CDN的产品优势

节点丰富	智能调度	安全防护	操作简单	稳定可靠
华为云CDN 2000+国内加速节点，500+海外加速节点。带宽储备能力≥100 Tbps，涵盖了电信、联通、移动、教育网等主流运营商，以及多家中小型运营商，有效将用户请求精准调度至最优边缘节点。	拥有全球更加精准的IP库，具有不断进化的能力。通过大数据实时反馈服务质量，动态调整用户的节点。	华为云CDN为用户提供中立、安全、可靠的云CDN服务。支持全网HTTPS安全传输，网站防盗链等高级安全控制功能。	华为云CDN接入方式简单快速，提供自助化的域名管理，并且支持多种可定制配置项，方便客户进行统计分析、日志管理、自定义缓存策略。	拥有多业务加速的技术能力，包括网站加速、下载加速、视频加速，针对用户的多种业务提供一站式的加速解决方案，提升整体用户体验。

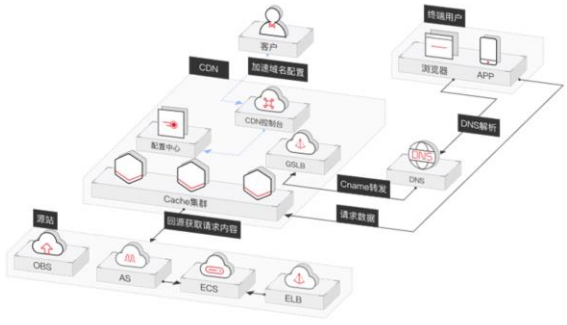
CDN的工作原理



HUAWEI

- 流程说明：
  - 用户在浏览器输入要访问的网站域名www.example.com，向本地DNS发起域名解析请求。
  - 本地DNS检查缓存中是否有www.example.com的IP地址记录。如果有，则直接返回给终端用户；如果没有，则向网站授权DNS查询。
  - 网站DNS服务器解析发现域名已经解析到了CNAME：www.example.com.c.cdnhwc1.com。
  - 请求被指向CDN服务。CDN对域名进行智能解析，将响应速度最快的CDN节点IP地址返回给本地DNS。
  - 用户获取响应速度最快的CDN节点IP地址。
  - 浏览器在得到最佳节点的IP地址以后，向CDN节点发出访问请求。
    - 如果该IP地址对应的节点已缓存该资源，节点将数据直接返回给用户，如图中步骤7和8，请求结束。
    - 如果该IP地址对应的节点未缓存该资源，节点回源拉取资源。获取资源后，结合用户自定义配置的缓存策略，将资源缓存至节点，如图中的北京节点，并返回给用户，请求结束。

应用场景 - 网站加速



- 网站加速

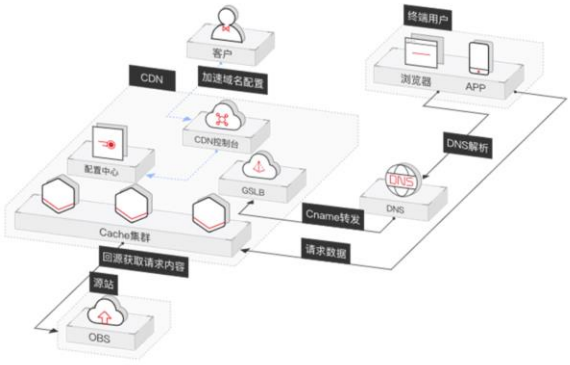
  适用于有加速需求的网站，包括门户网站、电商平台、资讯APP、UGC应用（User Generated Content，用户原创内容）等。CDN网络能够对加速域名下的所有内容在全国范围内提供良好的加速服务，包括静态内容和动态内容。支持自定义缓存规则，用户可以根据数据需求设置缓存过期时间。

- 优势
  - **接入简单：**六步完成域名配置，立即开启加速。
  - **安全加速：**可配置HTTPS和防盗链保障网站安全。
  - **配置灵活：**内容可永久缓存或短期缓存，动态内容也可设置不缓存。
- 可与华为云OBS、ECS、DNS搭配组成完整解决方案。

HUAWEI

- CDN网络能够为加速域名下的静态内容提供良好的加速服务。支持自定义缓存规则，用户可以根据数据需求设置缓存过期时间，缓存格式包括但不限于zip、exe、wmv、gif、png、bmp、wma、rar、jpeg、jpg等。

应用场景 - 下载加速



- 下载加速

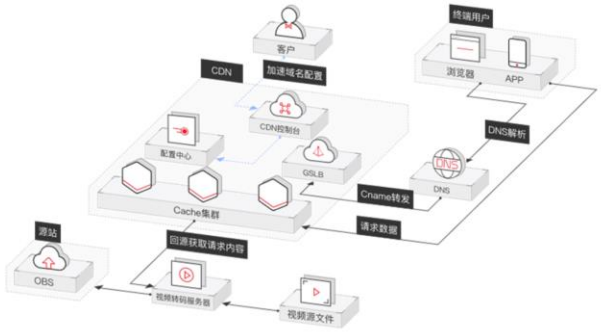
  适用于使用http/https文件下载业务的网站、下载工具、游戏客户端、APP商店等。现在越来越多的新业务需要通过网络对客户端软件进行实时更新，包括APP更新，手游更新等。

- 优势
  - **实时分析：**提供统计分析，日志监控方便用户对下载数据一目了然。
  - **安全可靠：**支持全网所有节点HTTPS传输，支持Referer黑白名单。
  - **高性价比：**搭配对象存储OBS使用，进一步提升性能，降低成本。
- 可与华为云OBS、DNS搭配组成完整解决方案。

HUAWEI

- 传统的下载类业务也需要支持更多的文件数量和更大的文件，如果所有的请求都通过源站服务器来处理，服务器和网络会成为很大的瓶颈，导致下载体验变差。使用CDN下载加速可以将下载量大的内容分发到各地的CDN节点，有效减轻源站的压力，同时保证了客户端高速下载的需求。

应用场景 - 点播加速



- 点播加速

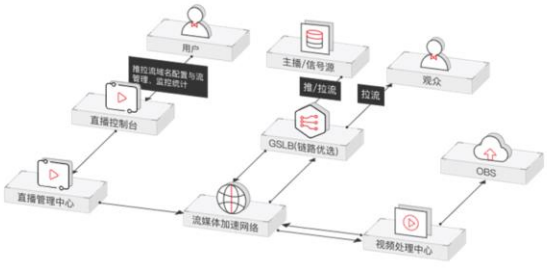
  适用于提供音视频点播服务的客户以及使用HLS协议的准直播客户。例如：在线教育类网站、在线视频分享网站、互联网电视点播平台、音乐视频点播APP等。

- 优势
  - **实时监控**：实时查看在 CDN 上产生的流量、带宽等数据，了解业务情况。
  - **安全控制**：支持防盗链访问控制，进行版权保护。
  - **配置灵活**：内容可永久缓存或短期缓存，也可设置不缓存。
- 可与华为云OBS、DNS搭配组成完整解决方案。

HUAWEI

- 传统的点播服务会加大服务器的负载，并消耗巨大的带宽资源，同时又无法保证终端用户访问时需要的高速体验，CDN点播加速可以提供快速、稳定和安全的点播加速服务，通过分布全国的CDN节点，将音视频内容扩展到距离用户最近的地方，随时随地为用户提供高品质的访问体验。
- 支持格式：视频：MP4/HLS/FLV 音频：MP3/ACC/OGG/FLAC 。

应用场景 - 直播加速



- 直播加速

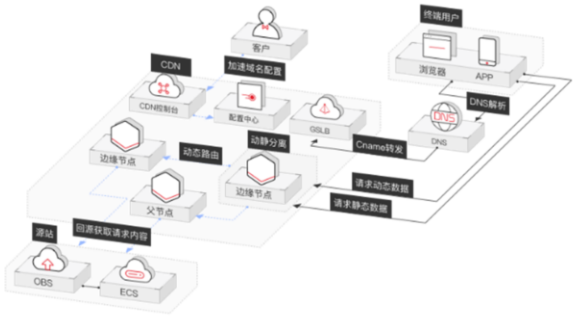
  适用于提供直播服务的用户。直播加速产品结合了流媒体技术和CDN技术，通过智能负载均衡系统将用户的直播访问定位至最佳节点，有效避开了网络中的拥塞，实现用户最快访问，改善服务效果，降低源站压力。为终端用户提供了端到端流畅的视频访问体验。

- 优势
  - **立体监控：**7*24小时监控，发现问题立即上报告警。针对网络、设备、质量、资源进行全方位立体监控，实时反馈题，确保高质量直播加速服务。
  - **方便快捷：**配置简单快捷，快速应对集中访问和流量快速增长需求。
  - **安全可靠：**提供URL鉴权，HTTPS和Referer防盗链等多种保护机制，减少盗播风险。
- 可与华为云OBS、DNS搭配组成完整解决方案。

HUAWEI

- 支持格式：输入的流：RTMP/HTTP、FLV/HTTP、TS，经转换支持输出RTMP/HTTP、FLV/HTTP、TS/HLS/HDS，同时支持HLS\HDS协议的纯分发。

应用场景 - 全站加速



- 全站加速

  适用于各行业动静态内容混合，含较多动态资源请求（如asp、jsp、php等格式的文件）的网站。

- 优势
  - **动静态分离：**融合动态加速与静态缓存技术，实现动静态内容自动分离加速。
  - **安全加速：**可配置HTTPS和防盗链保障网站安全。
  - **有序回源：**当源站出现访问突增的情况，可设置阈值，回源请求数超过阈值，按发出请求时间有序排队等待回源。
- 可与华为云OBS、ECS、DNS搭配组成完整解决方案。

HUAWEI

- 全站加速融合了动态和静态加速，用户请求资源时，静态内容从边缘节点就近获取，动态内容通过动态加速技术智能选择最佳路由回源获取。CDN全站加速有效提升动态页面的加载速度，避开网络拥堵路由，提高访问成功率，实现网站整体加速与实时优化。

目录

华为EI企业智能类服务全景图 - AI篇

- 为助力政企智能升级，让AI无处不在，无所不及，华为云提供了一系列的AI和大数据云服务供用户选择。

HUAWEI

- EI企业智能类服务主要包含两大类：人工智能类服务、大数据类服务。本页为AI类服务。详细介绍，请移步华为云官网：https：//www.huaweicloud.com/ei/

华为EI企业智能类服务全景图 - 大数据篇

- 为助力政企智能升级，让AI无处不在，无所不及，华为云提供了一系列的AI和大数据云服务供用户选择。

HUAWEI

- EI企业智能类服务主要包含两大类：人工智能类服务、大数据类服务。本页为大数据类服务。详细介绍，请移步华为云官网：https：//www.huaweicloud.com/ei/

一站式开发平台 ModelArts

- ModelArts是面向开发者的一站式AI开发平台，为机器学习与深度学习提供海量数据预处理及半自动化标注、大规模分布式Training、自动化模型生成及端-边-云模型按需部署能力，帮助用户快速创建和部署模型，管理全周期AI工作流。

ModelArts 3.0

感知智能-认知智能-决策智能

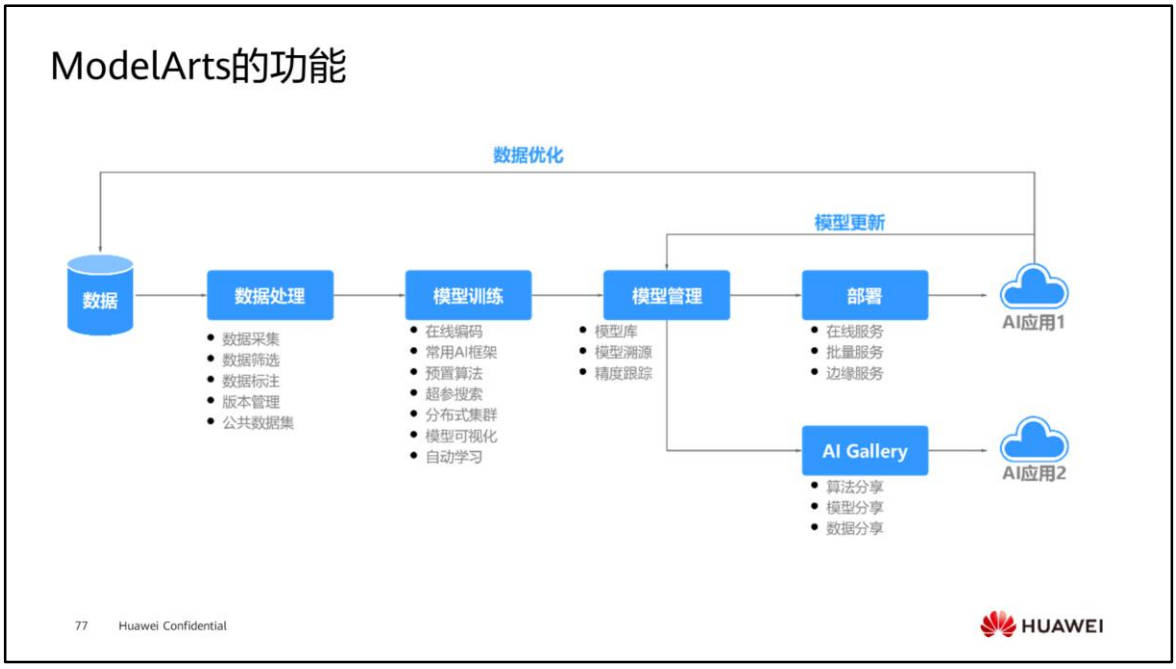
ModelArts Pro

首款企业级AI应用开发专业套件

知识计算

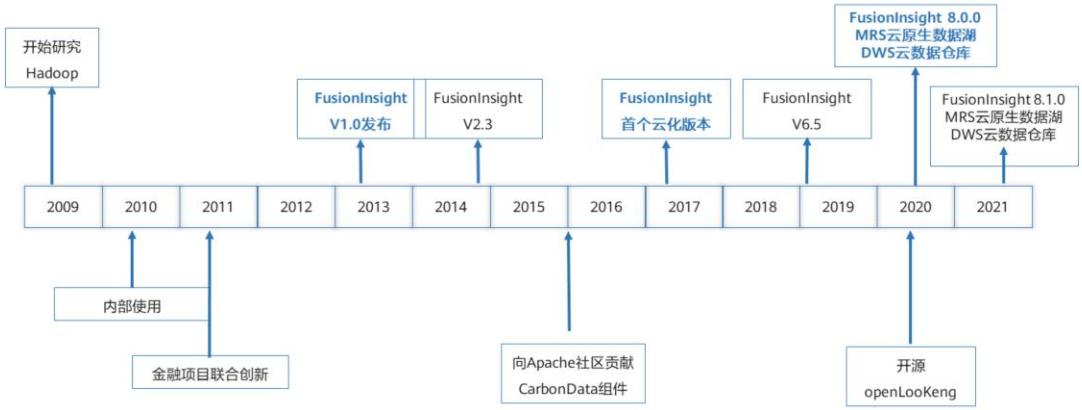
行业+AI结合的全新路径

- ModelArts可提供海量数据预处理及半自动化标注、大规模分布式训练、自动化模型生成及端-边-云模型按需部署能力，帮助用户快速创建和部署模型，管理全周期AI工作流。“一站式”是指AI开发的各个环节，包括数据处理、算法开发、模型训练、模型部署都可以在ModelArts上完成。从技术上看，ModelArts底层支持各种异构计算资源，开发者可以根据需要灵活选择使用，而不需要关心底层的技术。同时，ModelArts支持Tensorflow、MXNet等主流开源的AI开发框架，也支持开发者使用自研的算法框架，匹配用户的使用习惯。
- ModelArts的理念是让AI开发变得更简单、更方便。面向不同经验的AI开发者，提供便捷易用的使用流程。例如，面向业务开发者，不需关注模型或编码，可使用自动学习流程快速构建AI应用；面向AI初学者，不需关注模型开发，使用预置算法构建AI应用；面向AI工程师，提供多种开发环境，多种操作流程和模式，方便开发者编码扩展，快速构建模型及应用。



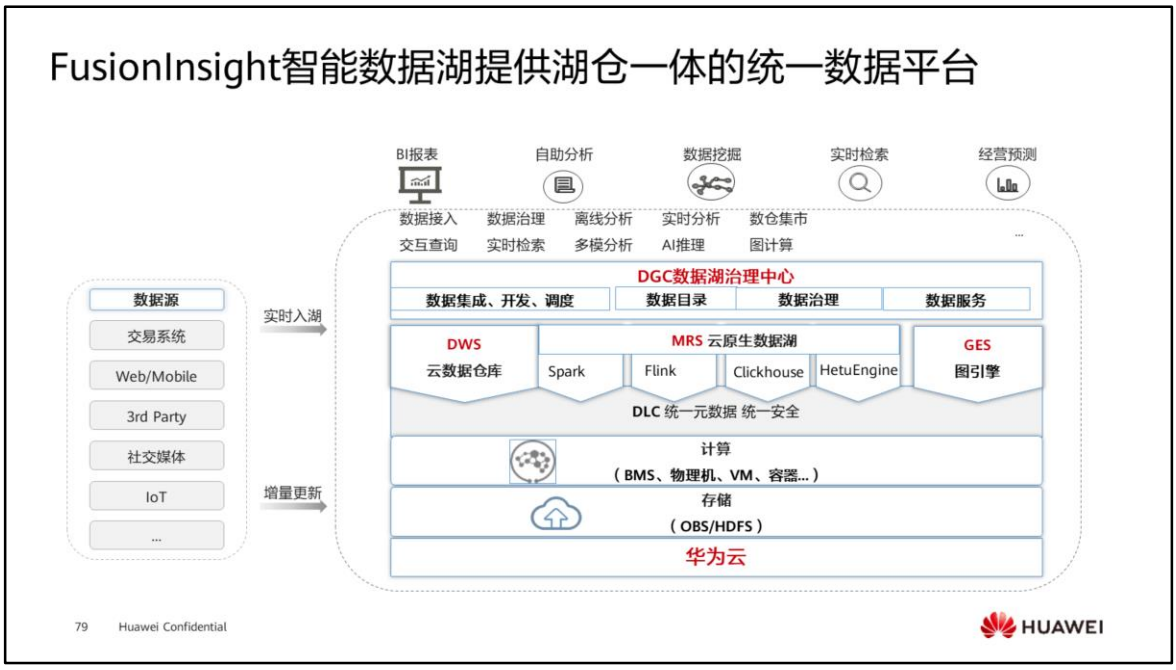
- ModelArts能够支撑开发者从数据到AI应用的全流程开发过程。包含数据处理、模型训练、模型管理、模型部署等操作，并且提供AI Gallery功能，能够在市场内与其他开发者分享模型。
- ModelArts支持应用到图像分类、物体检测、视频分析、语音识别、产品推荐、异常检测等多种AI应用场景。

FusionInsight 智能数据湖发展历程

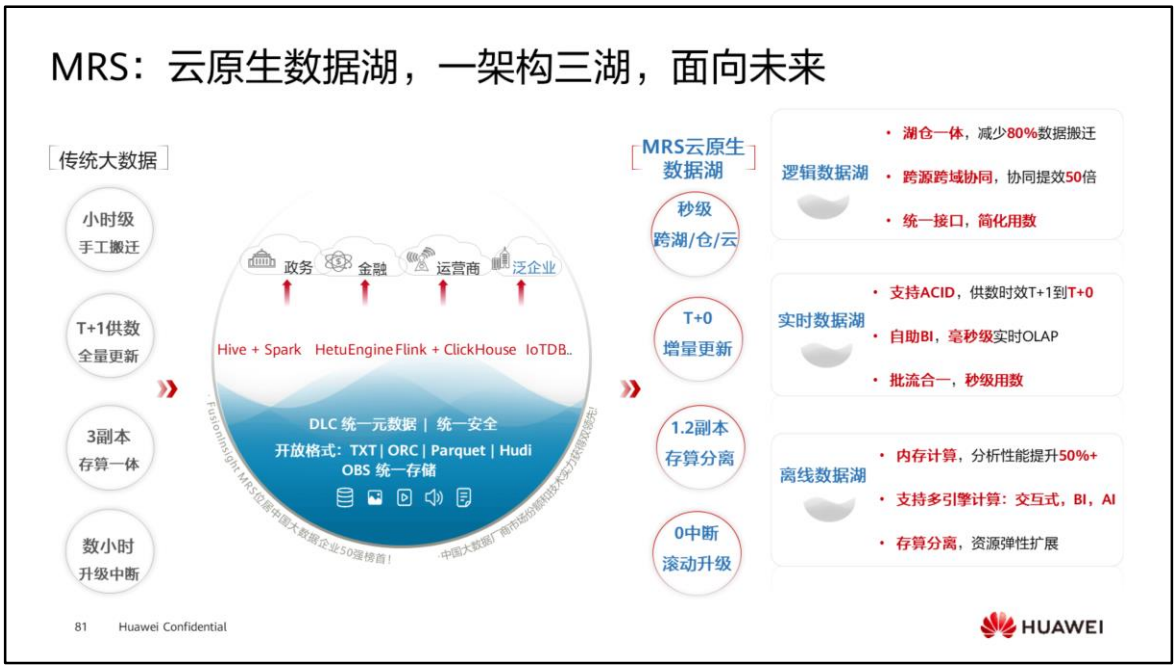


10+年的技术积累，遍布全球的研发团队，持续的版本更新迭代，支撑全球3000+客户持续演进。

HUAWEI



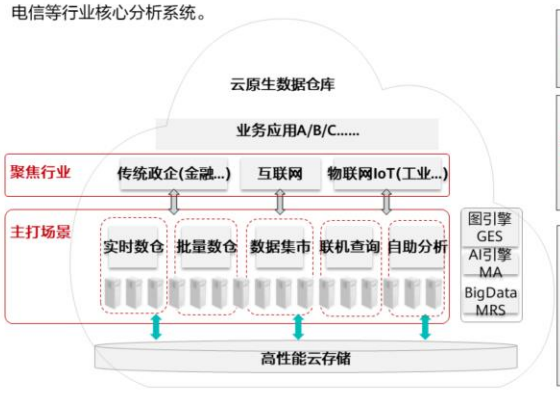
- FusionInsight解决方案主要包含MRS大数据、DWS数据仓库、CSS云搜索、GES图计算、DLI数据湖探索、DGC数据湖治理中心等云服务，支撑政企客户全量数据的实时分析、离线分析、交互查询、实时检索、多模分析、数仓集市、数据接入和治理等大数据应用场景，一站式解决分析域数据问题，释放海量数据价值，助力政企客户实现一企一湖、一城一湖。
- MRS云原生数据湖，一个架构实现三种数据湖，持续演进！
  - 逻辑数据湖：跨湖、跨仓、跨云协同提效30%+
  - 实时数据湖：毫秒级OLAP，时效性从T+1到T+0
  - 离线数据湖：湖内建仓，缩短分析链路，分析提效10倍+
- DWS云数据仓库
  - 高性能：性能比拼测试，完胜友商（阿里ADB，Gbase8A）
  - 高扩展：2048节点，100PB+



- 华为云FusionInsight MRS云原生数据湖，经过十多年发展，在大数据领域持续创新，通过一个架构，可以实现三种数据湖的能力：
  - 逻辑数据湖，跨湖、跨仓、跨云秒级协同分析，消灭数据孤岛：提供HetuEngine数据虚拟化引擎，实现跨湖、跨云的协同分析能力，减少80%以上数据搬迁，这对分散的数据，比如集团性质的企业很有用，像工行，总行加上分支行两百多个，逻辑分散，就经常需要跨域的手工搬迁。通过逻辑数据湖就可以实现逻辑的搬迁，减少数据的实际搬迁
  - 实时数据湖，毫秒级OLAP，供数时效T+1到T+0
  - 离线数据湖，支持多引擎计算，包含交互式、BI、AI等场景。通过存算分离方案，实现数据统一存储，存储计算解耦，计算存储按需灵活扩展，TCO降低六成
- FusionInsight MRS支持大规模集群分批次滚动升级，故障节点隔离功能，确保整体升级动作的稳定运行，保障关键业务连续性，在金融行业实现升级过程柜台办事无感知。

GaussDB（DWS）：新一代、全场景、云数据仓库

GaussDB（DWS）是一款具备分析及**混合负载能力**的分布式数据库，支持x86和Kunpeng硬件架构，支持**行存储与列存储**，提供**PB（Petabyte）级**数据分析能力、**多模分析**能力和**实时处理**能力，用于**数据仓库、数据集市、实时分析、实时决策**和**混合负载**等场景，广泛应用于金融、政府、电信等行业核心分析系统。



统一内核 统一架构

- 一套内核、一套架构支撑**公有云、混合云，用户体验一致**
- **同时支持虚拟机（ECS）、裸金属（BMS）、物理机（HCS）**模式

全球最大的金融数仓

- 业界首个第三方单集群**2048**节点规模权威认证
- 业界首个单集群**482**节点**四路全闪存**服务器，装机容量**20 PB**
- 获得全球授权专利280+
- **获得2020年度大数据产业生态联盟“数据仓库领域最佳产品奖”**

关键竞争力

高性能
TPC-DS性能业界领先

高扩展：
2048节点，>100 PB

高可用
强一致性；集群内 RPO=0，RTO<30 s；在线扩容

企业级特性：
逻辑集群、协同计算(+HD)、融合分析(+AI)、实时分析(+IoT)

HUAWEI

- 华为的数仓产品叫高斯数据库，GaussDB DWS就是新一代、全场景的云数据仓库。
- 同时支持x86和Kunpeng硬件架构，支持行存储与列存储，提供PB级数据分析能力、多模分析能力和实时处理能力。

GES图引擎服务：超大规模一体化图分析与查询

1 一站式图数据库、图引擎产品
- 集图数据库和图分析引擎一体化的产品
- 具备完善的图分析、图查询、图可视化能力
- 中国首个商用的、拥有自主知识产权的原生图产品

2 分析查询一体化
- 一份数据做两件事：查询和分析一体化
- 支持Cypher和Gremlin两种主流图查询语言，原生Rest API，开源接口兼容
- 30+高性能算法，覆盖多场景分析计算，具备10+图神经网络和图嵌入算法

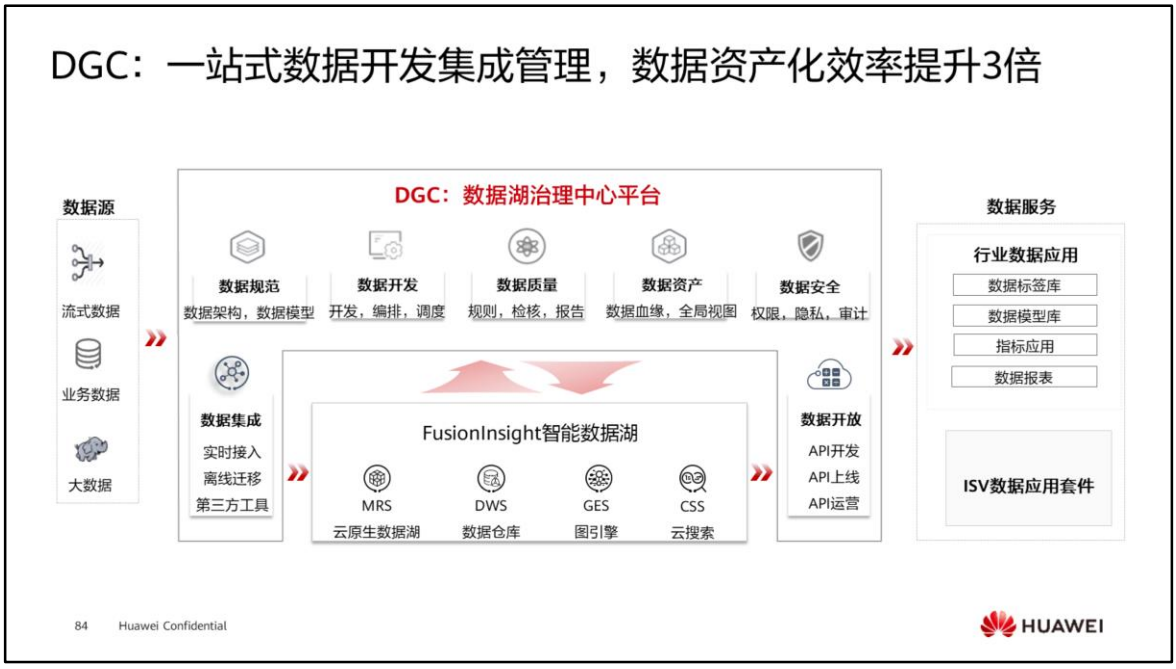
3 大规模、高性能
- 支持百亿点、万亿边规模大图
- 查询和算法性能优于业界竞品，6跳查询秒级响应，多种算法在大图计算上表现优秀

4 简单易用，支持no-code可视化分析
- 支持可视化编辑、实体的下钻等图可视化分析探索
- 向导式算法操作及算法结果的可视化呈现分析

5 自研内核，多次斩获国际大奖

HUAWEI

- GES图引擎，是一种图数据库技术
- 华为云的GES图引擎服务，支持百亿节点、万亿边的规模大图，自研内核并多次斩获国际大奖，比如19年人工智能峰会的最高奖，2020年国际金融科技大会人工智能优秀应用奖等。



- DGC数据治理平台，从数据接入、到数据规范、数据开发，数据的质量检查，形成数据资产，数据开放给上层服务，提供一整套数据治理功能。
- 方便行业伙伴快速地使用数据，也利于企业形成自己的数据资产。
- DGC是华为内部的产品名称，对外呈现时，智能数据湖和DGC一整套数据使能服务，品牌宣传为DAYU。
- 平台：
  - 一站式数据开发集成管理平台，40+异构数据源、全拖拽开发、多维实时搜索、0代码API开发，开发效率3倍提升。
  - 基于华为10+年数据治理经验沉淀出的数据架构、标准规范、数据开发、数据质量等云服务。
- 生态：
  - 100+开放API，使能行业ISV快速集成开发。
  - 10+合作伙伴提供数据标准、模型、指标、接口等行业数据模型。

思考题

1. （判断题）CDN是一款免费的云服务。

   正确

   错误

2. （多选题）以下关于CDN使用场景的描述，正确的有哪些?

   A. 网站加速

   B. 文件下载加速

   C. 点播加速

   D. 云服务器运行加速

- 错误。CDN按照流量或者带宽来进行收费。
- ABC。CDN主要针对于应用，并不能让云服务器运行得更快。

本章总结

- 本章讲解了数据库的分类：关系型和非关系型。介绍了不同数据库的适用场景和关键特性；通过本章的学习，我们掌握了安全相关知识，也意识到安全的重要性。整个华为云产品体系中，每个维度都需要安全服务的保障；新型产品的介绍，使我们能更全面地了解华为云，它不仅承载了传统业务上云的需求，更为新型业务做了良好的铺垫。只有更好地掌握相关云服务，我们才能更好地发展企业业务。

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为云技术支持网站
  - https://support.huaweicloud.com/help-novice.html
- 华为云学院
  - https://edu.huaweicloud.com/

术语和缩略语

AZ：Availability Zone，可用区

APP：Application，应用程序

API：Application Programming Interface，应用程序接口

APT：Advanced Persistent Threat，定向威胁攻击

CDN：Content Delivery Network，内容分发网络

CPU：Central Processing Unit，中央处理器

CSA：Cloud Security Alliance，云安全联盟

DDoS：Distributed denial of service attack，分布式拒绝服务攻击

DDS：Document Database Service，文档数据库服务

DDM：Distributed Database Middleware，分布式数据库中间件

术语和缩略语

DAS：Data Admin Service，数据管理服务

DWS：Data Warehouse Service，数据仓库服务

DEW：Data Encryption Workshop，数据加密服务

EI：Enterprise intelligence，企业智能

ELB：Elastic Load Balance，弹性负载均衡

HA：Highly Available，高可用

HSS：Host Security Service，主机安全服务

IT：Internet Technology，互联网技术

IAM：Identity and Access Management，统一身份认证

KMS：Key Management System，密钥管理系统

术语和缩略语

LAMP：Linux+Apache+PHP+Mysql，通常一起使用来运行动态网站

OLAP：Online Analytical Processing，联机分析处理

OLTP：Online Transaction Processing，联机事务处理

OBS：Object Storage Service，对象存储

PITR：point-in-time recovery，任意恢复时间点

RTO：Recovery Time Object，恢复时间点目标

UGC：User Generated Content，用户原创内容

VIP：Virtual IP Address，虚拟IP

WAF：Web Application Firewall，Web应用防火墙

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

华为云运维基础

HUAWEI

前言

- 华为云除了提供很多资源类服务来满足企业业务系统上云的需求之外，还需要保障好云上业务系统的正常运转和企业人员对于业务系统的监管需求。
- 因此，本章我们将带领大家了解华为云运维相关的知识。

目标

- 学完本课程后，您将能够：
  - 了解到一些关于运维、监控、审计方面的基础知识。
  - 了解到华为云上常见的监管类服务的定位、原理、使用等。

目录

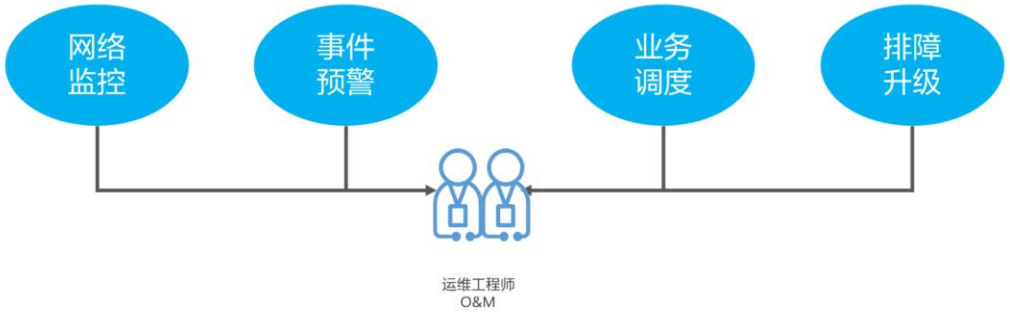
什么是运维

- 运维（Operations and Maintenance）本意为运行维护。负责监控、管理设备或系统，保障业务的正常运行。处理工作中遇到的各种问题并总结经验教训，优化提高运维的效率和质量。
- 本质上是对网络、服务器等设备及服务的生命周期各个阶段的运营与维护，在成本、稳定性、效率上达成一致可接受的状态。
- 运维的重点在于系统运行的各种环境，偏重的不是编程，而是对这类系统平台的使用和管理。

- 在ICT行业中，我们通常将执行运维动作的人称为运维工程师。

运维人员的职责

- 运维人员的职责是根据业务需要规划信息、网络、服务，通过网络监控、事件预警、业务调度、排障升级等手段，使服务处于长期稳定可用状态。



- 运维人员对公司互联网业务所依赖的基础设施、基础服务、线上业务进行稳定性加强，进行日常巡检发现服务可能存在的隐患，对整体架构进行优化以屏蔽常见的运行故障，多数据中接入提高业务的容灾能力。通过监控、日志分析等技术手段，及时发现和响应服务故障，减少服务中断的时间，使公司的互联网业务符合预期的可用性要求，持续稳定地为用户提供务。
- 做一个好的运维工程师，除了具备良好的综合技能水平，还要有一个负责任的工作态度，这也是优秀运维工程师具备的素质。
- 在互联网行业常见的组织架构中，运维与开发，测试都是基本的的技术岗位。从时间环节来讲，开发与测试从事的主要是在软件或服务上线投入使用前的工作，而运维则主要从事上线后的维护工作（运维开发除外）。从运维工作本身又可细分为如下分类：IT 运维、网络运维、业务运维、运维开发。

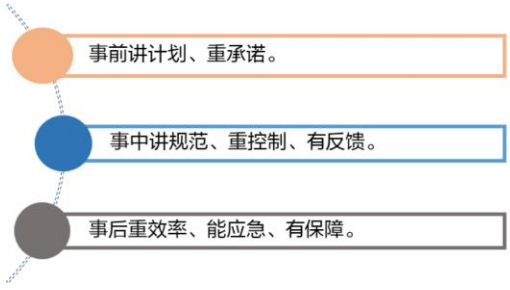
运维人员的分类

- 随着ICT数据中心的设备、操作系统、应用变得越来越多、复杂度越来越高，企业对于运维的工作要求也越来越高。因此，运维人员也开始有了细分。常见的运维岗位有以下几种：

- 硬件运维：
  - 机房规划（包括机房选址，网络部署，服务器部署规划）；
  - 网络系统的维护（网络调整、扩容，带宽监控，网络链路优化（QoS））；
  - 服务器的管理（采购、到货、上架、系统安装、交付、维修）。
- 系统运维：
  - 针对操作系统使用情况的运维包括：系统优化，性能监控等。
- 数据库运维：
  - 针对用户数据库开展的软件安装，配置优化，备份策略选择及实施，数据恢复，数据迁移，故障排除，预防性巡检等一系列服务。
- 应用运维：主要是针对用户使用的服务的运维，确保服务在不断迭代情况下的稳定性。
  - 变更管理，确保系统在不断迭代的过程中系统的稳定性；
  - 故障管理，包括应用监控，故障定位，故障恢复，应用优化；
  - 资源管理，确保应用系统在有限可用的资源之下正常地运行，并针对未来资源的增长使用进行预算审核；
- 很多时候系统运维和应用运维是结合在一起的，因为应用的稳定性需要依赖系统，所以在运维过程中，会一并运维。
- 网络运维：
  - 是指为保障企业网络与业务正常、安全、有效运行而采取的生产组织管理活动，简称运维管理或OAM。负责维护并确保整个服务的高可用性，同时不断优化系统架构提升部署效率。

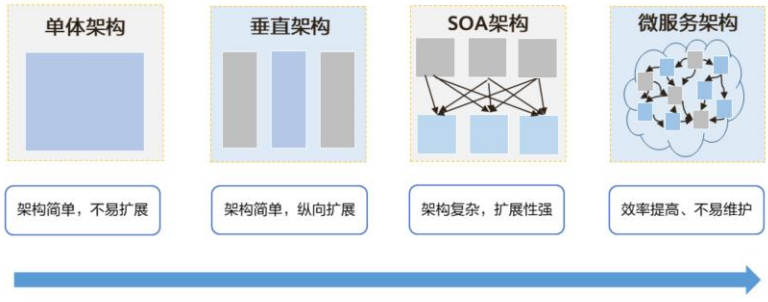
ICT运维的原则

- 前面大家已经了解了运维人员岗位的多样性。那么，ICT运维人员自己应该如何做好这份工作呢？运维看似简单，但是要想做好，更好地服务企业业务系统，我们首先就要知道ICT运维的总体原则。

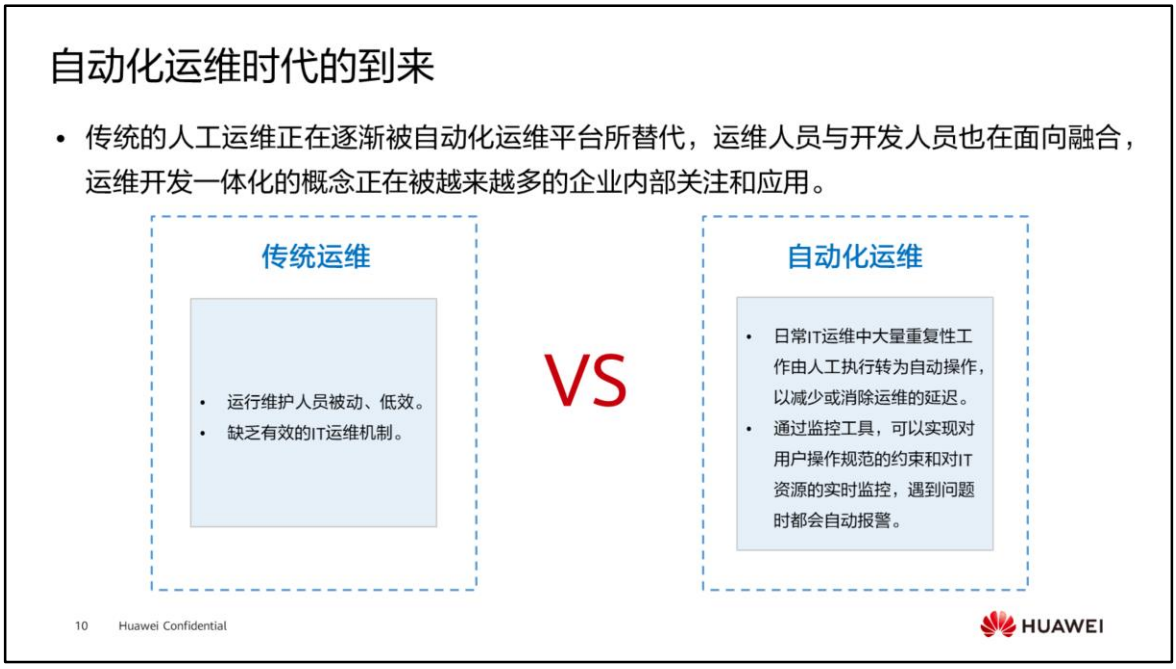


IT技术架构演变带来的运维压力

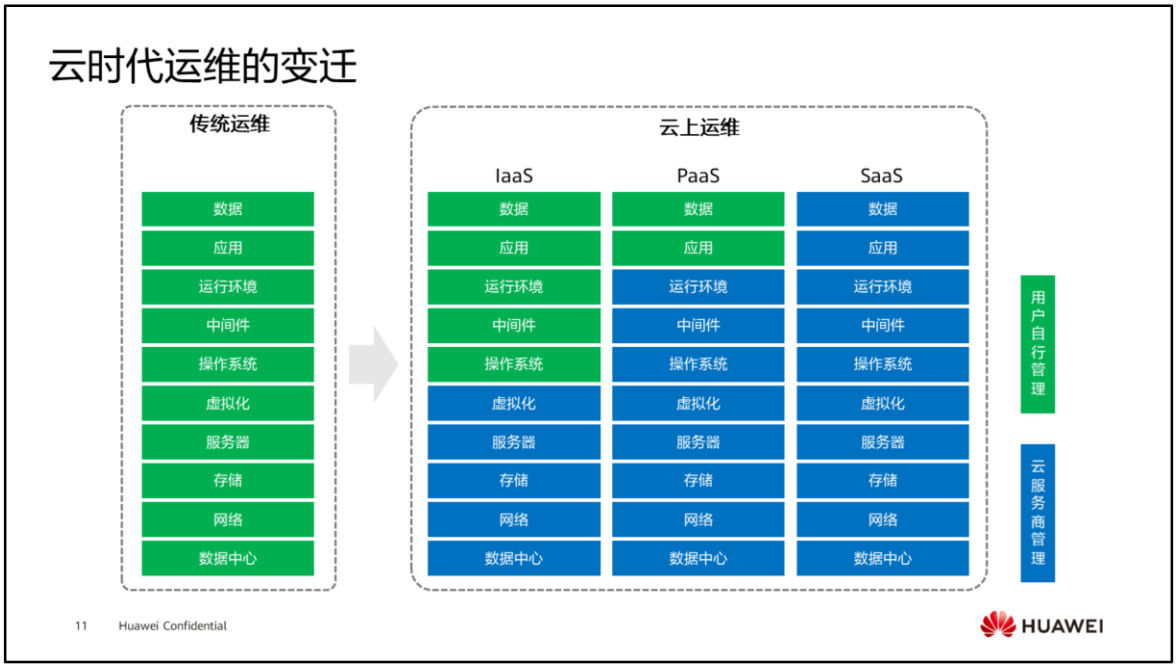
- 随着IT架构不断演进，系统架构变得越来越复杂，运维人员也面临着诸多的挑战。



- 随着IT架构的不断演进，架构的复杂度越来越高，在企业内部开发和运维往往是两个独立的部门，在工作和技术方向上存在明显的差异，这就造成了在共同完成一个应用项目的时候沟通不顺畅，进而导致应用进度推迟，企业效率大幅度下降。因此，整个体系架构需要不断演进，从传统运维走向自动化运维，将运维工程师、开发工程师、质量保障工程师的壁垒打破，从而形成一套高效的工作体系。
- 单体架构的特点：所有功能都集中在一个项目中。单体架构简单，前期开发成本低，周期短，小型项目首选。但是全部功能集中在一个项目中，随着项目的变大，变的不易开发，扩展，维护。
- 垂直架构的特点：以单体架构规模的项目为单位进行垂直划分项目，项目架构简单，前期开发成本低，周期短，小型项目的首选。通过垂直拆分，原来的单体项目不至于无限扩大。
- SOA（Service-Oriented Architecture）的特点：基于SOA的架构思想将重复公用的功能抽取为组件，以服务的方式给各各系统提供服务。各个项目（系统）与服务之间采用webservice、rpc等方式进行通信。能提高开发效率，提高系统的可重用性、可维护性。可以针对不同服务的特点制定集群及优化方案。
- SOA架构的缺点：系统与服务的界限模糊，不利于开发及维护。抽取的服务的粒度过大，系统与服务之间耦合性高。
- 微服务架构的特点：微服务架构风格的开发方法，是以开发一组小型服务的方式来开发一个独立的应用系统的。其中每个小型服务都运行在自己的进程中，并经常采用HTTP资源API轻量的机制来相互通信。服务拆分粒度更细，有利于资源重复利用，提高开发效率。可以更加精准地制定每个服务的优化方案，提高系统可维护性。适用于互联网时代，产品迭代周期更短。



- IT运维经历了十多年的兴衰沉浮，现在它正面临着一种新的姿态——自动化，这是IT技术发展的必然结果。现在IT系统的复杂性客观上要求它的运行和维护必须能够实现数字化和自动化。自动化运维是指IT运维中日常和重复性工作的自动化，以及人工工作向自动化的转变。自动化是IT运维的升华。IT运维自动化不仅是一个维护过程，也是一个管理提升过程。它是IT运维的最高水平，也是未来的发展趋势。
- DevOps（运维开发一体化）是一组过程、方法与系统的统称，用于促进开发、技术运营（运维）和质量保障（QA）部门之间的沟通、协作与整合。DevOps消除了两个传统部分之间的壁垒，让企业效率大幅度提升。



- 相比传统运维，云运维在很大程度上能够释放企业原有自行运维的成本压力。通过公有云的运维管理类服务，几乎能够让用户可以不花钱，就能够完成日常的运维，并且这一切的运维、管理类服务都是基于自动化运维技术来做支撑的。

华为云上常见的运维服务

目录

监控的意义

- 监控的目的就是防患于未然。通过监控，我们能够及时了解到企业网络的运行状态。一旦出现安全隐患，就可以及时预警，或者是以其他方式通知运维人员，让运维监控人员有时间处理和解决隐患，避免影响业务系统的正常使用，将一切问题的根源扼杀在摇篮中。

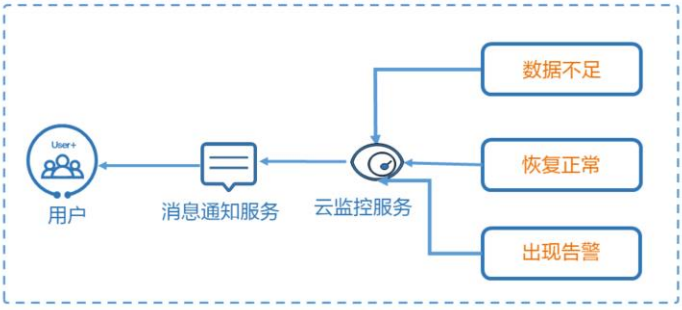
HUAWEI

什么是云监控服务（CES）

- **云监控服务**（Cloud Eye Service，简称CES）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。使用户可以全面了解华为云上的资源使用情况、业务的运行状况，并及时收到异常报警从而做出反应，保证业务顺畅运行。

主要功能：

- 自动监控
- 实时通知
- 监控面板
- 资源分组
- OBS转储



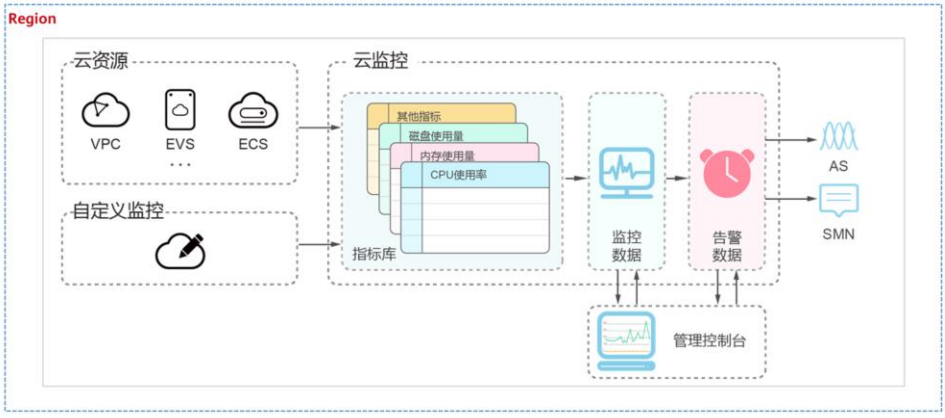
- 云监控服务主要具有以下功能：
  - 自动监控：云监控服务不需要开通，监控服务会根据用户创建的弹性云服务器资源或者弹性伸缩等自动启动。用户在创建和使用云服务后可直接到云监控服务查看该服务运行状态并设置告警规则。
  - 实时通知：通过在告警规则中开启消息通知服务，当云服务的状态变化触发告警规则设置的阈值时，系统通过短信、邮件通知或发送消息至服务器地址等多种方式实时通知用户，让用户能够实时掌握云资源运行状态变化。
  - 监控面板：使用户能在一个监控面板跨服务、跨维度地查看监控数据，将用户关注的重点服务监控指标集中呈现，既能满足用户总览云服务运行概况，又能满足排查故障时查看监控详情的需求。
  - 资源分组：资源分组支持用户从业务角度集中管理其业务涉及到的弹性云服务器、云硬盘、弹性IP、带宽、数据库等资源。从而按业务来管理不同类型的资源、告警规则、告警历史，可以迅速提升运维效率。
  - OBS转储：云监控服务各监控指标的原始数据的保留周期为两天，超过保留周期后原始数据将不再保存。用户开通对象存储服务OBS后，可将原始数据同步保存至OBS，以保存更长时间。

CES的优势

HUAWEI

- 实时监控：实时采样监控指标，提供有效的资源监控，通知随时触发，随时响应。
- 免费易用：监控免费自动开通，提供多聚合方式的历史监控图表。
- 通知多样：云监控提供邮件、短信、HTTP、HTTPS通知，用户可第一时间知悉业务运行的状况。
- 深入全面：针对ECS提供全面深入的主动监控服务，Open API、SDK、Agent支持指标上限。

CES的产品架构



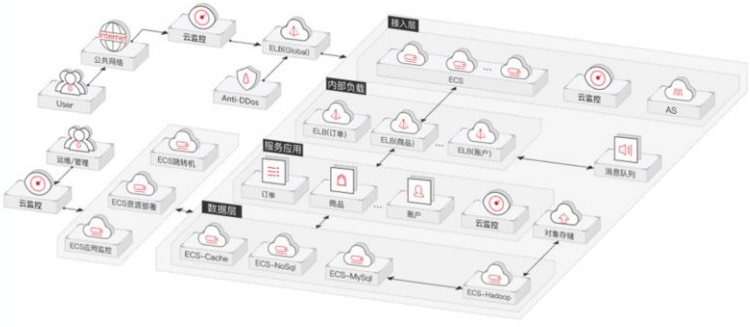
HUAWEI

- 统一可编辑的监控面板：针对系统关键监控信息，统一展示监控信息，便于直观检测查看。
- 告警触发服务器弹性伸缩：当电商网站在短期内出现波峰时，系统进行自动扩展，并通过告警模板对扩容的服务器快速复制告警策略。
- 全面的ECS主动监控：对服务器进行全方面细颗粒度监控，对网络流量指标进行自定义监控，预防网络瓶颈效应。
- 告警快速敏捷触发服务器弹性伸缩：服务器使用量达到阈值，自动进行扩容和缩容操作。
- 登录及安全日志监控：对用户登录日志进行实施监控，遇到恶意登录行为，触发告警并拒绝该IP地址的请求，保证安全。
- 深入全面的主机插件式监控：对登录服务器进行全方面细颗粒度监控，对网络流量指标进行自定义监控，预防网络瓶颈效应。

应用场景 - 电商业务解决方案

电商业务解决方案特点

- 统一可编辑的监控面板
  针对系统关键监控信息，统一展示监控信息，便于直观检测查看
- 告警触发服务器弹性伸缩
  当电商网站在短期内出现波峰时，系统进行自动扩展，并通过告警模板对扩容的服务器快速复制告警策略
- 全面的ECS主动监控
  对服务器进行全方面细颗粒度监控，对网络流量指标进行自定义监控，预防网络瓶颈效应



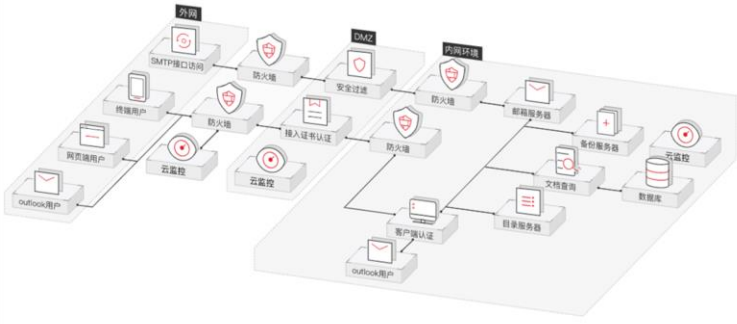
HUAWEI

- 上图解决方案中，云监控服务能够有限地监控业务运行状况，以便结合其他服务实现动态资源调整；也可以通过监控云服务以及网络、应用情况，及时上报消息通知到用户，提高整体安全性。

应用场景 - 企业办公应用

企业办公应用的特点

- 告警快速敏捷触发服务器弹性伸缩
  服务器使用量达到阈值，自动进行扩容和缩容操作
- 登录及安全日志监控
  对用户登录日志进行实施监控，遇到恶意登录行为，触发告警并拒绝该IP地址的请求，保证安全
- 深入全面的主机插件式监控
  对登录服务器进行全方面细颗粒度监控，对网络流量指标进行自定义监控，预防网络瓶颈效应



HUAWEI

- 上图解决方案中，云监控服务主要通过监控各服务情况，以此来保证安全性。

CES的使用 - 监控面板

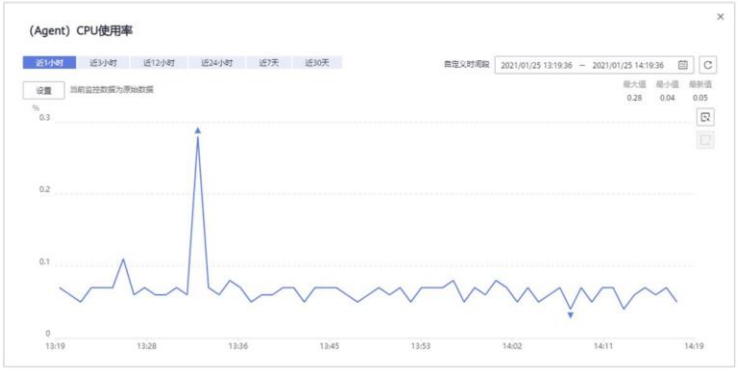
- 监控面板为用户提供自定义查看监控数据的功能，将用户关注的核心服务监控指标集中呈现在一张监控面板里，并且可定制成一个立体化的监控平台。

HUAWEI

- 监控面板还支持在一个监控项内对不同服务、不同维度的数据进行对比查看，帮助用户实现不同云服务间性能数据对比查看的需求。当前云监控支持每个用户最多创建20个监控面板，每个监控面板支持创建24个监控视图，单个视图最多添加20个监控项。

CES的使用 - 监控指标

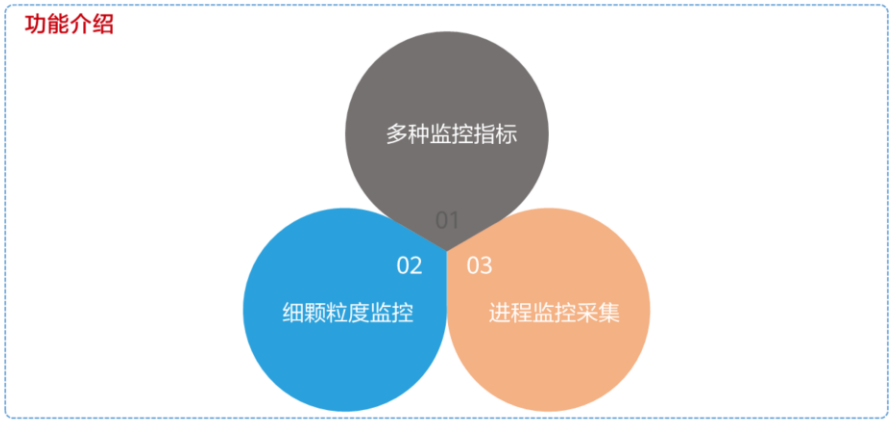
- 监控指标是云监控服务的核心概念，通常是指云平台上某个资源的某个维度状态的量化值，如云服务器的CPU使用率、内存使用率等。监控指标是与时间有关的变量值，会随着时间的变化产生一系列监控数据，帮助用户了解特定时间内该监控指标的变化。



HUAWEI

CES的使用 - 主机监控

- 主机监控分为基础监控、操作系统监控、进程监控。



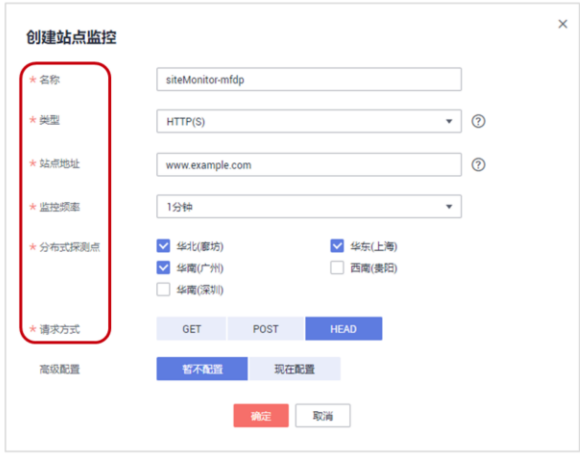
HUAWEI

- 主机监控分为基础监控、操作系统监控、进程监控：
  - 基础监控：ECS/BMS自动上报的监控指标。
  - 操作系统监控：通过在ECS或BMS中安装Agent插件，为用户提供服务器的系统级、主动式、细颗粒度监控服务。
  - 进程监控：针对主机内活跃进程进行的监控，默认采集活跃进程消耗的CPU、内存，以及打开的文件数量等信息。
- 功能介绍：
  - 多种监控指标：安装Agent后，云监控服务会提供CPU、内存、磁盘、网络等四十余种监控指标，满足服务器的基本监控运维需求。
  - 细颗粒度监控：安装Agent插件后，Agent相关监控指标为 1分钟上报 1 次。
  - 进程监控采集：当前活跃进程占用的 CPU、内存和打开文件数，让用户了解弹性云服务器或裸金属服务器的资源使用情况。

CES的使用 - 站点监控

功能介绍：

- 站点监控用于模拟真实用户对远端服务器的访问，从而探测远端服务器的可用性、连通性等问题。
- 站点监控可以探测域名、IP的可用性、访问响应时间、丢包率，并对监控结果告警。

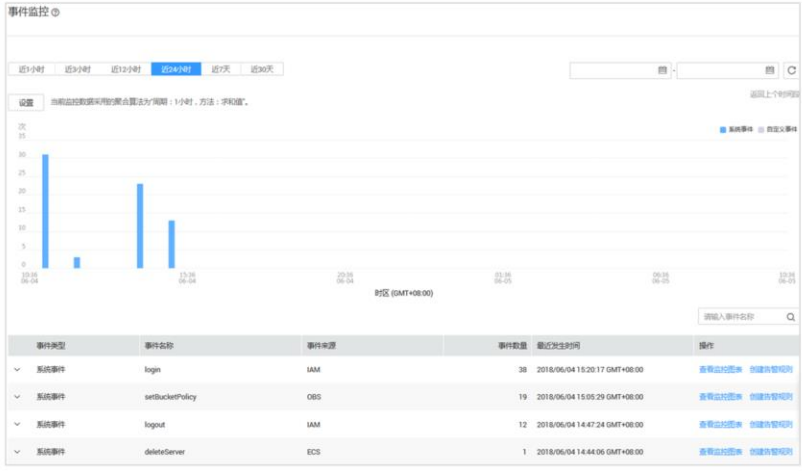


HUAWEI

- 目前站点监控功能免费。站点监控部署在华北-北京一，若在其他Region使用站点监控功能，需同时添加华北-北京一的权限。
- 功能优势：
  - 支持创建、修改、停用、启用、删除站点监控。
  - 提供简单的添加配置，不再浪费资源和精力配置复杂的开源产品。
  - 支持站点异常告警，不用担心网站出问题而无人知晓。

CES的使用 - 事件监控

- 事件监控提供了事件类型数据上报、查询和告警的功能。方便用户将业务中的各类重要事件或对云资源的操作事件收集到云监控，并在事件发生时进行告警。



HUAWEI

CES的使用 - 自定义监控

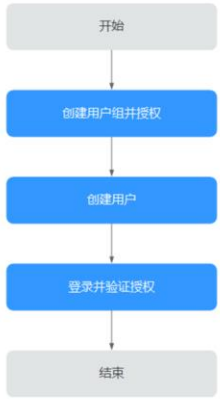
- 功能介绍：自定义监控展示用户所有自主定义上报的监控指标。用户可以针对自己关心的业务指标进行监控，将采集的监控数据通过使用简单的API请求上报至云监控服务进行处理和展示。

HUAWEI

CES的使用 - 权限管理

配置介绍：

- 在IAM控制台创建用户组，并授予云监控服务权限“CES Administrator”、“Tenant Guest”和“Server Administrator”。
- 在IAM控制台创建用户，并将其加入创建的用户组。
- 新创建的用户登录控制台，验证云监控服务的“CES Administrator”权限。



目录

日志的意义

- 日志是记录系统运行过程中各种重要信息的文件，在系统运行过程中由各进程创建并记录。为快速定位系统运行中出现的问题及开发过程中的程序调试问题提供详细信息。

HUAWEI

- 运维日志平台：
  - 企业应用的运维日志分散在不同的虚机上，包括应用运行日志、中间件日志等，日志分散，日志规模较大，为企业日志提供集中管理平台
- 优势：
  - 全托管式：提供日志采集、存储、老化、搜索和转储
  - 海量日志管理：支持每天百TB级日志的接入，十亿级日志秒级搜索
  - 性价比高：维护成本低，按需计费，轻松应对高峰日志流量

什么是云日志服务（LTS）

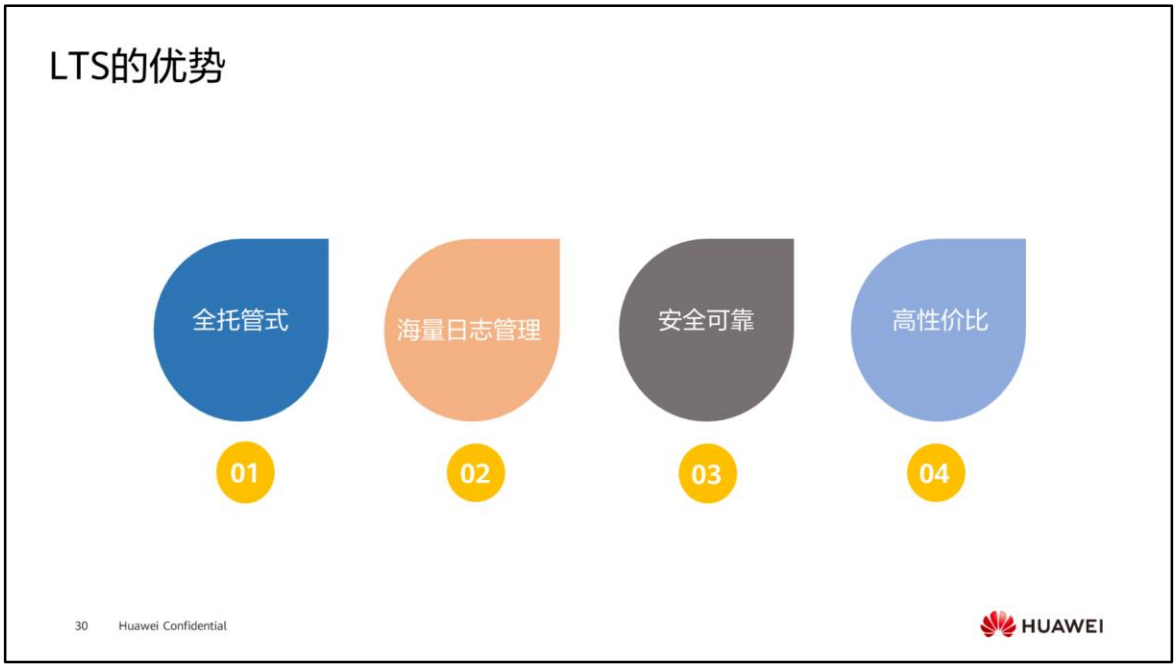
- **云日志服务**（Log Tank Service，简称LTS），用于收集来自主机和云服务的日志数据，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为用户提供一个实时、高效、安全的日志处理能力，可快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

主要功能：

- 实时采集日志
- 日志查询与实时分析
- 日志监控与告警
- 日志转储

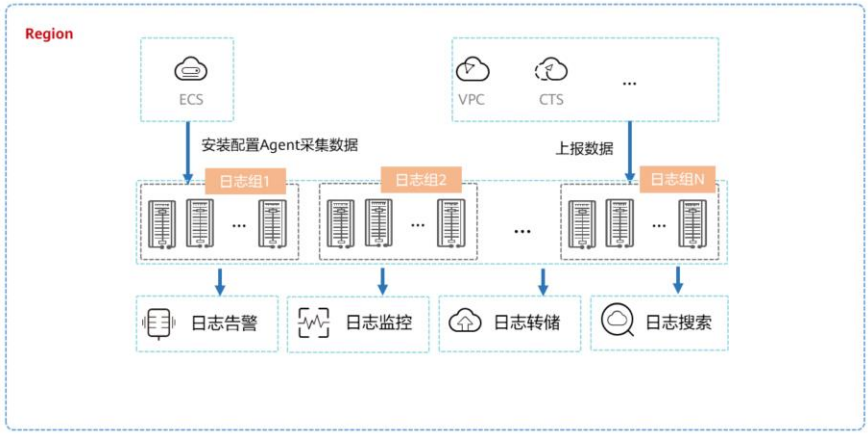
HUAWEI

- 实时采集日志
  - 云日志服务提供实时日志采集功能，采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。
  - 采集到日志数据按照结构化和非结构化进行分析。结构化日志是通过规则将日志流中的日志进行处理，提取出来有固定格式或者相似度高的日志内容做结构化的分类。这样就可以采用SQL的语法进行日志的查询。
- 日志查询与实时分析
  - 对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。
- 日志监控与告警
  - 云日志服务结合应用运维管理（Application Operations Management，简称AOM），支持对存储在云日志服务中的日志数据进行关键词统计，通过在一定时间段内，日志中关键字出现次数，实时监控服务运行状态。
- 日志转储
  - 主机和云服务的日志数据上报至云日志服务后，默认存储时间为7天，可以在1-30天之间进行设置。超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至对象存储服务（OBS）、数据接入服务（DIS）中长期保存。



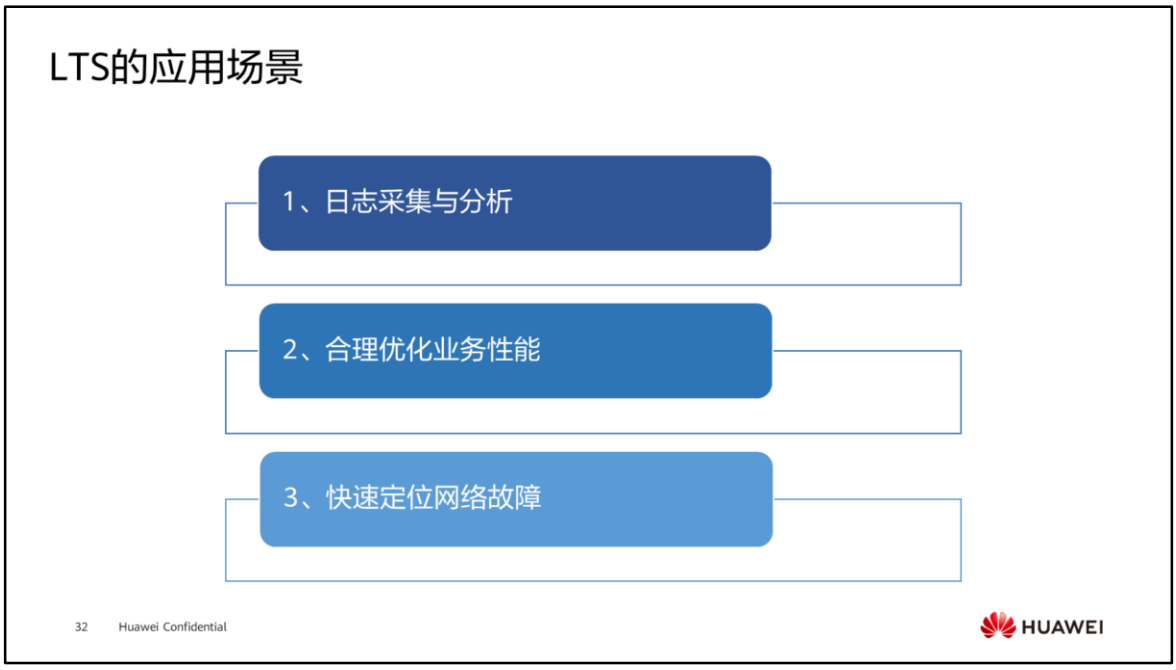
- 全托管式：华为云日志统一管理平台，提供从采集、接入、存储、搜索、转储（冷热分离）、结构化处理、SQL查询和可视化分析一站式服务。
- 海量日志管理：PB级海量日志管理，十亿级日志秒级搜索，每天可支持200 TB日志接入，亿级日志SQL聚合查询。
- 安全可靠：分权分域管理，HTTP加密等安全技术保障数据可靠性，SLA支持99.95%。
- 高性价比：相比传统日志管理系统，省去人工运维。灵活应对业务高峰，快速扩容，按需计费，无需预留额外资源。

LTS的产品架构



HUAWEI

- 通过安装Agent到弹性云服务器ECS中，LTS服务就能够借助Agent来采集相关日志数据，回传到日志服务中。结合日志服务的相关功能，为用户提供优质的日志服务体验。



- 日志采集与分析
  - 主机和云服务的日志数据，不方便查阅并且会定期清空，云日志服务采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。
- 合理优化业务性能
  - 网站服务（数据库、网络等）的性能和服务质量是衡量用户满意度的关键指标，通过用户的拥塞记录日志发现站点的性能瓶颈，以提示站点管理者改进网站缓存策略、网络传输策略等，合理优化业务性能。
- 快速定位网络故障
  - 网络质量是业务稳定的基石，将日志上报至云日志服务，确保问题发生时能及时查看、定位问题，助力用户快速定位网络故障，进行网络回溯取证。例如：快速定位问题根源的云服务器，如带宽过度使用的云服务器。通过分析访问日志，判断业务是否遭到了攻击、非法盗链和不良请求等，及时定位并解决问题。

LTS的使用 - 基本概念

HUAWEI

- 日志组的创建类型分为用户创建（主动）和云服务创建（被动），云服务创建指华为云其他云服务与云日志服务进行系统对接后，系统将自动在云日志服务控制台创建日志组和日志流，云服务的运行日志将发送到对应的日志流中。
- 日志读写以日志流为单位，用户可以在写入时指定日志流，将不同类型的日志分类存储，Agent采集日志后，将多条日志数据进行打包，以日志流为单位发往云日志服务，日志流的读写方式可以最大限度地减少读取与写入次数，提高业务效率。例如，用户可以将不同的日志（操作日志、访问日志等）写入不同的日志流，查询日志时可以进入对应的日志流快速查看日志。
- Agent是云日志服务的日志采集工具，运行在需要采集日志的主机中。首次使用云日志服务采集日志时，需要安装Agent，如果需要采集多台主机的日志，还支持批量安装Agent，在云日志服务控制台可以实时查看Agent的运行状态。

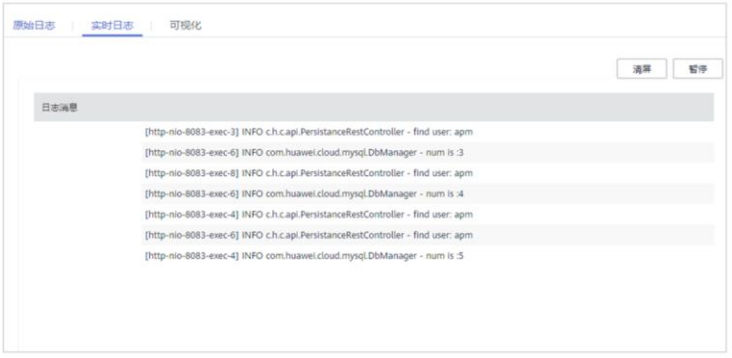
LTS的使用 - 日志查询

HUAWEI

- 优点：
  - 高性能数据库存储日志；
  - PB级存储、高吞吐量；
  - 日志转储投递；
  - 支持转储至OBS；
  - 提供上下文关联分析能力。

LTS的使用 - 实时日志

- 打开实时日志，LTS将每隔5秒自动更新最近的日志，该功能用于日志追踪场景。



HUAWEI

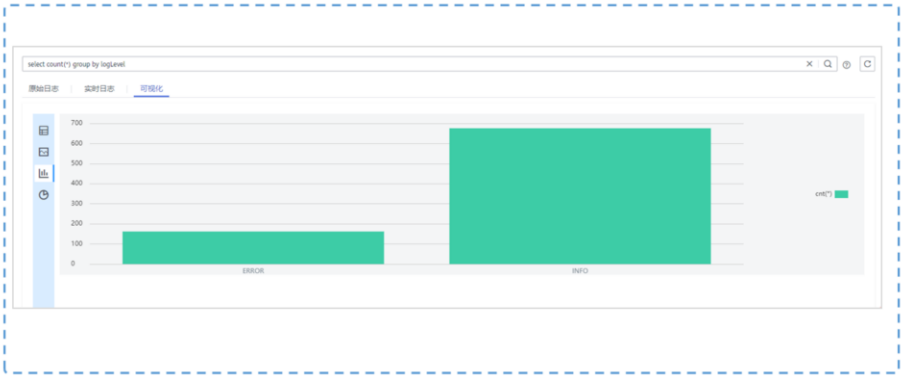
- 日志每隔大约1分钟上报一次，在日志消息区域，用户最多需要等待1分钟左右，即可查看实时上报的日志。同时，用户还可以通过页面右上方的“清屏”、“暂停”对日志消息区域进行操作。
  - 清屏：清除日志消息区域已经显示出来的日志。
  - 暂停：暂停日志消息的实时显示，页面定格在当前已显示的日志。暂停后，“暂停”会变成“继续”，再次单击“继续”，日志消息将继续实时显示。

LTS的使用 - 结构化分析日志

- 用户可通过添加提取规则，将原始日志按一定的规律进行提取，并将提取后的日志整合到一起，就可以通过常用的SQL语句来进行查询与分析。

LTS的使用 - 可视化报表

- 该功能通过对SQL查询的接口来进行可视化呈现。支持表格、趋势图、柱状图和饼图报表。



HUAWEI

- 可视化提供对结构化后的日志字段进行SQL查询与分析。对原始日志结构化后，等待1~2分钟左右即可对结构化后的日志进行SQL查询与分析。

LTS的使用 - 创建统计规则，对接告警中心

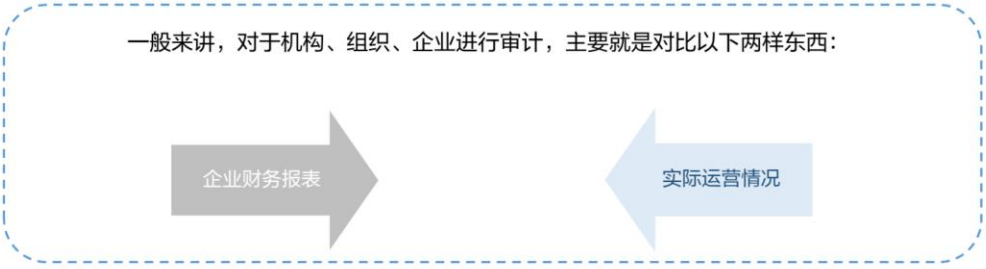
HUAWEI

- LTS服务本身不支持告警配置，需要配合应用运维管理（简称AOM）配置告警。

目录

什么是审计

- **审计**（Auditing）是对资料作出证据搜集及分析，以评估企业财务状况，然后就资料及一般公认准则之间的相关程度作出结论及报告，并将审核结果传达予利害关系人。在ICT行业中，审计主要涉及的是整个信息系统的生命周期。



审计的目的

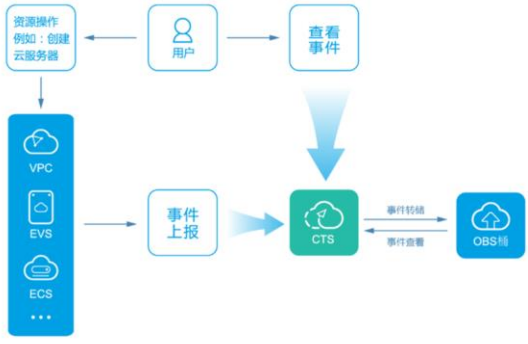
- 通过审计企业财务报表和实际运营情况，以此来保证企业财务收支的真实、合法和效益，最终达到保障企业运营健康，促进企业长期发展的目的。在ICT行业中，审计通常也是为了保障整个信息系统的健康运转。

HUAWEI

- 对业务上云的客户而言，关于审计方面的合规认证内容通常分为两部分：云服务商所负责的客户业务系统平台与资源的合规以及客户负责的自身业务系统的合规。
- 一方面，云审计服务是华为云自身合规性的组成部分之一，其几乎覆盖所有服务、所有资源的操作记录能力，以及审计日志在传输、存储、加密、容灾、防篡改等方面的安全能力，是认证中针对业务系统平台与资源合规的核心保障。另一方面，针对客户自身的业务系统的合规认证，云审计服务将在认证过程中积极响应，协助完成待满足项的解决方案设计和实现，支撑客户通过认证。

什么是云审计服务（CTS）

- **云审计服务**（Cloud Trace Service，简称CTS）主要是提供云账户下资源的操作记录，通过操作记录，用户可以实现安全分析、资源变更、合规审计、问题定位等功能。可以通过配置OBS对象存储服务，将操作记录实时同步保存至OBS，以便保存更长时间的操作记录。



HUAWEI

CTS的优势

传统审计

- 传统IT环境无法执行标准化审计流程，系统性地实时记录操作类与API记录的审查，如对服务器、数据库、操作系统等违规操作。且系统配置的变更，需要IT人员手工统计。
- 传统审计内容全靠人工手动记录并存储，无多副本保存，存在安全隐患，且无法长期保存。

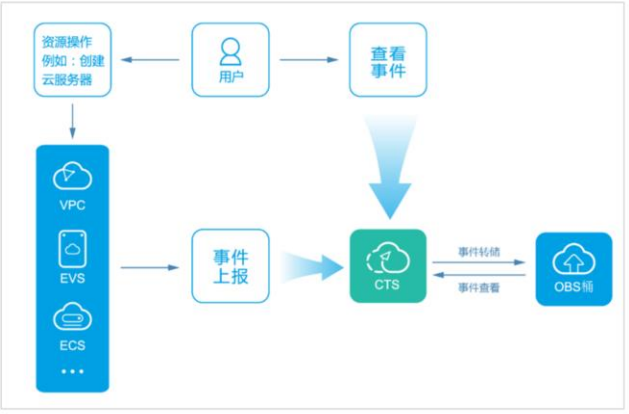
VS

云审计

- 云上资源变更均可被管控，实时系统性记录所有人的操作，无需手工统计。
- 云审计服务支持将操作记录合并，周期性地生成事件文件，实时同步转存到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的产品架构

- 主要功能
  - 记录审计日志
  - 审计日志查询
  - 审计日志转储
  - 事件文件加密



HUAWEI

- 记录审计日志：支持记录用户通过管理控制台或API接口发起的操作，以及各服务内部自触发的操作。
- 审计日志查询：支持在管理控制台对7天内操作记录按照事件类型、事件来源、资源类型、筛选类型、操作用户和事件级别等多个维度进行组合查询。
- 审计日志转储：支持将审计日志周期性地转储至对象存储服务（Object Storage Service，简称OBS）下的OBS桶，转储时会按照服务维度压缩审计日志为事件文件。
- 事件文件加密：支持在转储过程中使用数据加密服务（Data Encryption Workshop，简称DEW）中的密钥对事件文件进行加密。

CTS的基本概念

追踪器

使用云审计服务前需要开通云审计服务，开通云审计服务时系统会自动创建一个追踪器。该追踪器会自动识别并关联当前租户所使用的所有云服务，并将当前租户的所有操作记录在该追踪器中。

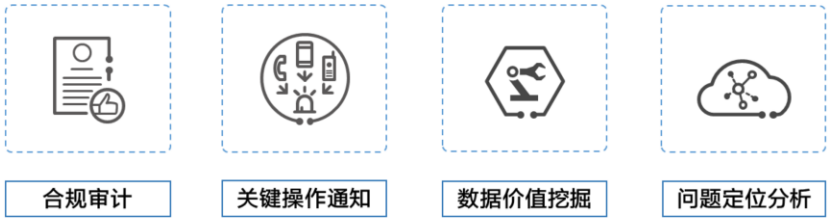
事件

事件即云审计服务追踪并保存的云服务资源的操作日志。“事件”能够帮助我们了解到哪个用户在什么时间对系统的哪些资源做了什么操作。

- 管理事件
  - 指云服务上报的事件。
- 数据事件
  - 指OBS服务上报的读写操作事件。

- 云审计服务管理控制台支持创建数据事件追踪器，追踪器用于记录用户的数据操作日志。

CTS的应用场景

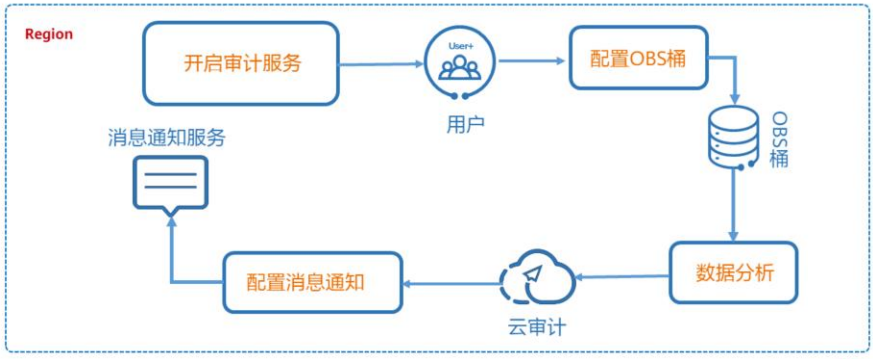


HUAWEI

- 云审计服务能够助力客户的业务系统通过等保合规、PCI DSS、ISO 27001等常见行业硬性规范中关于审计部分的认证。
- 云审计服务与函数工作流服务（FunctionGraph）共同提供关键操作通知功能，通知对象包括自然人及业务接口。
- 云审计服务支持对审计日志中的数据进行挖掘，为业务健康度分析、风险分析、资源跟踪、成本分析等提供支撑，并支持开放审计数据给客户，供客户自行挖掘数据价值。
- 云审计服务可通过配置查询条件，精确查找问题发生时的操作及其详情，降低问题发现、定位和解决的时间、人力成本。

CTS的使用 - 安全分析

- 云审计服务生成的每条事件均会记录哪个用户，在什么时间，从哪个IP发起了操作请求。通过执行安全性分析并检测用户行为模式，和对关键类的操作配置消息通知，用户可以更好地管控自己使用的云服务状况。



HUAWEI

- 安全分析的工作原理：
  - 登录用户，开启云审计服务，云审计服务会记录账号下所有操作日志；
  - 被记录的操作日志会被保存在OBS桶中；
  - 数据分析组件可以从桶中下载日志做分析；
  - 最终得出的结果可以配置到消息通知服务上报。

CTS的使用 - 资源变更

- 云审计服务生成的每条事件均会记录一次资源的变更以及变更的结果。用户可以根据这些记录统计和追溯资源的使用情况，以便更好地管控自己的云服务资源。

HUAWEI

- 资源变更的工作原理：
  - 用户对云服务做出的所有变更类操作都已经被审计服务记录；
  - 用户还可以通过配置关键类操作消息通知，及时获取服务的最新情况；
  - 账户下所有变更操作都将长久保存；
  - 用户可以通过日志进行查询资源变更的详细信息。

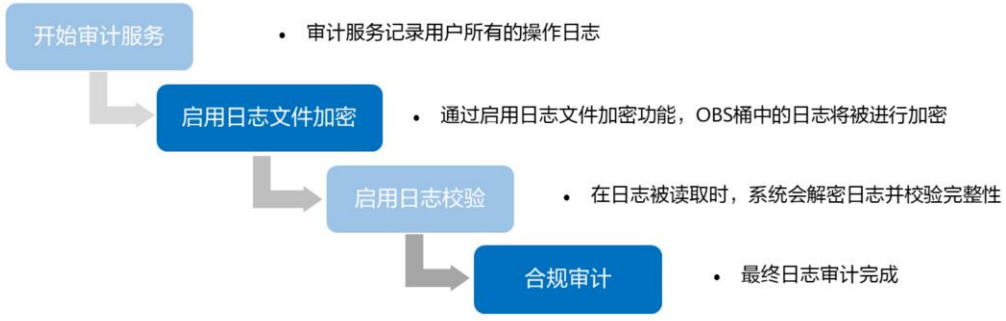
CTS的使用 - 故障定位

- 云审计服务生成的事件会记录失败操作的原因，用户可以根据原因轻松排除操作性故障。例如，扩容云主机配置时，删除了系统卷，导致最终创建失败。通过查看事件中记录的失败操作日志，我们可以很直观地找到具体原因。

- 故障定位的工作原理：
  - 用户在自己账号下进行了可能会导致相关故障的变更或误操作；
  - 审计服务会将这些操作全部记录；
  - 此时，用户可以通过搜资源名称来查询影响的结果；
  - 通过查询，用户可以获取详细信息，包括操作人，具体时间等；
  - 用户可以基于这些信息，去纠正这个错误操作。

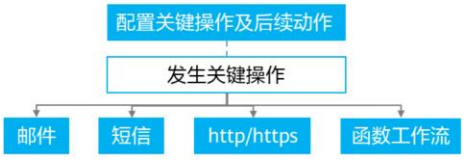
CTS的使用 - 合规审计

- 云审计服务提供的操作记录、操作查询能力，能够使用户更轻松地确保自身符合内部策略和监管标准，以此来满足IT合规设计认证要求（如金融云，可信云等）。



CTS的使用 - 关键消息通知

- 云审计服务支持以审计日志为触发器，发送消息通知到用户邮件、短信、业务系统接口，以及直接触发函数工作流，完成用户指定的操作。
  - 主要功能：
  - 系统核心组件、组网、安全配置变更，操作详情知会管理员，降低业务稳定性风险。
  - 配置面向http/https通知，将CTS收到的审计日志同步到客户自有的审计系统，独立审计。
  - 通过函数工作流，检测操作自动触发事件。



思考题

1. （判断题）云监控服务是一款免费的云服务。

   正确

   错误

2. （多选题）以下哪些是云审计服务的应用场景?

   A. 关键操作通知

   B. 合规审计

   C. 数据价值挖掘

   D. 问题定位分析

- 正确。云监控服务不收费，用户可以通过云监控服务来监控管理自己购买的云服务。
- ABCD。

本章总结

- 运维服务看似不起眼，但是至关重要，通过审计服务，我们能够更安全地管控平台；通过监控服务，我们能够实时地掌握平台的运行状况；通过日志服务，我们可以随时获取底层各种日志信息，以便更好地评估有可能会发生的风险。

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为云技术支持网站
  - https://support.huaweicloud.com/help-novice.html

术语和缩略语

CTS：Cloud Trace Service，云审计服务

CES：Cloud Eye Service，云监控服务

ECS：Elastic Cloud Server，弹性云服务器

IT：Internet Technology，互联网技术

ICT：Information And Communications Technology，信息通信技术

IAM：Identity and Access Management，统一身份认证服务

LTS：Log Tank Service，云日志服务

OBS：Object Storage Service，对象存储服务

SOA：Service-Oriented Architecture，面向服务的架构

术语和缩略语

SQL：Structured Query Language，结构化查询语言

VPC：Virtual Private Cloud，虚拟私有云

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.