ALIBABA CLOUD

阿里云

专有云企业版

全栈云平台

产品简介

产品版本：v3.18.0

文档版本：20240924

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
⚠ 警告	适用于可能会产生风险的场景。介绍用户在操作前就必须充分了解的信息、操作前必须要注意的事项或已具备的条件。	⚠ 警告 重启操作将导致业务短暂中断，建议您在业务低峰期执行重启操作，或确保已完成数据备份。如有必要，请联系阿里云技术支持提供协助。
ⓘ 重要	在操作前需要用户了解的提示信息、补充信息、注意事项、限制信息等。	ⓘ 重要 再次登录系统时，您需要修改登录账户的初始密码。
? 说明	用于额外的补充说明、最佳实践、窍门等，不是用户必须了解的信息。	? 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.产品全景


应用运维平台（AOP）
统一云管平台（Apsara Uni-Manager）
开放接口（API+SDK）
统一安全保障（云盾）
统一灾备平台（ASR）
物联网
物联网平台（IOT）
物联网边缘计算（IOTEdge）
IoT设备身份认证（IOTID）
IoT安全运营中心（SOC）
物联网网络管理平台（LinkWAN）
企业应用服务
无影云桌面（EDS）
API网关（API Gateway）
数据库产品
云数据库（RDS）
云原生关系型数据库（PolarDB）
数据库备份（DBS）
云数据库MongoDB版（MongoDB）
数据传输（DTS）
云原生分布式数据库（PolarDB-X）
图数据库（GDB）
云原生数据仓库（ADB）
数据管理（DMS）
数据库和应用迁移（ADAM）
云数据库Redis版（Redis）
数据库自治服务（DAS）
云数据库OceanBase版（OceanBase）
大数据&AI产品
云原生大数据计算服务（MaxCompute）
机器学习（PAI）
数据分析与展现（Quick BI）
大数据管家（BCC）
大数据开发治理平台（DataWorks）
数据总线（DataHub）
智能数据建设与治理（Dataphin）
数据可视化（DATAV）
数据资源平台（Data Q）
实时计算（Flink）
交互式引擎分析（Hologres）
云原生产品
消息列队（MQ）
异地多活（MSHA）
企业级分布式应用服务（EDAS）
分布式任务调度（SchedulerX）
应用实时监控服务（ARMS）
Prometheus监控服务（Prometheus）
云服务总线（CSB）
容器服务（ACS）
应用高可用服务（AHAS）
容器镜像服务（ACR）
计算服务
云服务器（ECS）
资源编排（ROS）
弹性高性能计算（EHPC）
运维编排（OOS）
服务器迁移中心（SMC）
弹性伸缩（ESS）
裸金属服务器
裸机管理
存储服务
块存储 CDS-EBS
对象存储 CDS-OSS
日志服务 CDS-SLS
表格存储 CDS-OTS
文件存储 NAS
混合云容灾服务 CDS-HDR
网络服务
负载均衡（SLB）
专有网络（VPC）
VPN网关（VPN ）
专有云DNS（DNS）
高速通道（EC）
云网管（CMN）
云接入网关（CGW）
转发路由器（TR）
飞天云计算操作系统
IDC数据中心

2.关于阿里云专有云

阿里云专有云是基于阿里云分布式架构，针对企业级市场使用特点，为客户量身打造的开放、统一、可信的企业级云平台。专有云与阿里云公共云同根同源，客户可在任何环境本地化部署公共云产品及服务，并具备一键扩张、弹性伸缩至公共云的能力。

面向不同客户业务规模、针对不同业务场景，专有云提供稳定安全、一应俱全和轻量化、易集成等多样配置的飞天企业版；对于业务场景更聚焦的客户，专有云还提供大数据、数据库、中间件、存储等优势场景独立输出的云产品独立部署版。

服务价值

阿里云专有云解决方案诞生自阿里云公共云，将公共云的技术带到专有云领域，即专有公共云，简称专有云。通过帮助企业在自己的数据中心交付完整的可定制的阿里云软件解决方案，让用户在本地就可以获得与阿里云公共云超大规模云计算和大数据产品相同的特性，为企业提供一致性的混合云体验，从而满足用户按需获得IT资源、保持业务持续性的需求。

阿里云专有云提供本地部署方式，可以脱离阿里云运行和独立管理。

阿里云专有云以丰富的产品和服务为依托，以阿里巴巴集团成功的数字化实践案例为基础，结合已在各个行业形成的成熟的解决方案和丰富的经验，能够帮助政府及企业级用户完成数字化转型。客户使用阿里云专有云计算的服务价值体现在以下四个方面：

- **规模按需**：满足客户超大规模业务量运行需求，单区域部署规模10000台，支持多Region业务运行；也可面向云化初期客户提供小型化云平台，降低上云门槛。
- **一应俱全**：与公共云同源，提供超过80款公共云产品，支持热升级，客户可在本地持续尽享阿里云最新产品服务；可一键式弹性扩展至公共云，提供不同应用场景需求下的混合云解决方案。
- **深耕行业**：丰富的政府、金融等行业的全栈云平台搭建经验，有效保障中大型政企客户更全更稳定的上云。
- **安全稳定**：原生安全体系架构提供多层级、一体化安全防护服务，首家通过等保2.0四产级认证，高分通过可信云认证、ISO27001、GDPR认证和平台级国密测评等安全认证；提供金融级两地三中心容灾、异地多活方案，强力保障系统高可靠和业务连续性。

发展历程

阿里云专有云从2015年7月发布V1.0版本后，到目前为止历经了三个版本的演进。未来阿里云专有云会向着更开放、更可信、更可控的全栈企业级云平台发展，持续为用户提供价值服务。

版本	发布时间	相关内容
V1.0	2015年7月	• 场景：大数据场景。 • 关键产品：IAAS+基础大数据产品。 • 平台特性：半自动化部署，ERMS账户体系。
V2.0	2016年5月	• 场景：互联网中台+大数据 • 关键产品：IaaS基础产品+大数据产品+Aliware中间件产品。 • 平台特性：统一运维管理；管控节点压缩，有效控制部署云平台底座的服务器体量。

V3.0	2017年7月	• 场景：互联网金融（含大数据）。 • 关键产品：IaaS基础产品+大数据产品+中间件产品（含docker）+云盾安全产品。 • 平台特性：等保合规（三级/四级），两地三中心，国际化。

3.引言

专有云定义

专有云按服务企业规模或业务需求的大小可以划分为两类：

- 面向行业云、大型集团云等的多租户、完整专有云架构，以超大规模数字化应用为业务驱动，以DevOps应用持续集成持续开发和生产环境的运营支撑为主要IT诉求，自上而下构建全栈云服务的专有云体系。
- 面向中小企业和中小型应用场景的单租户、简版专有云，向上衔接和承接大型SaaS应用、行业云及大型集团云等技术体系，同时完成本地计算任务。

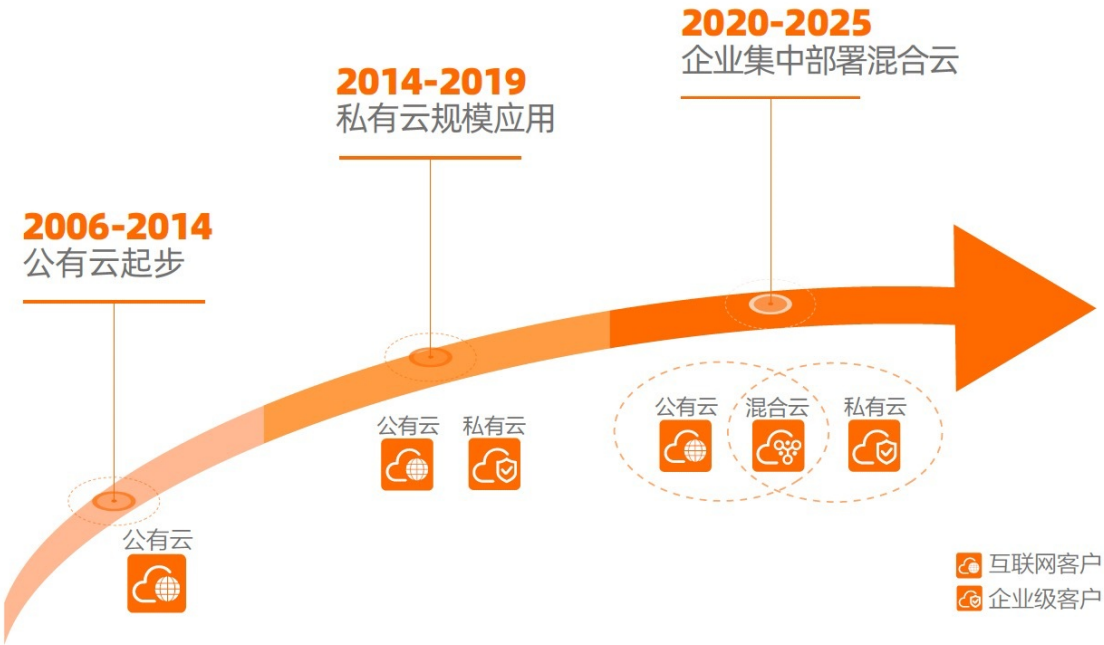
行业趋势

随着云计算技术日渐成熟，云计算在政务、金融、能源等传统行业的渗透逐步加深，越来越多企业都在数字化转型的道路上寻求通过深化上云路径驱动业务的根本转型。在此过程中，如何结合具体需求让上云降本增效，复杂场景和需求下如何实现精准管理运维，各应用业务如何创新协同最终实现企业业务数智化升级，成为了企业全面上云的普遍痛点。

近年来企业数字化程度加速，IT环境复杂度逐步加深，单一公有云提供的同质类服务，难以满足特殊行业安全合规等关键需求；而单一私有云，又因其计算资源扩展难，基础设施构筑成本高等因素，难以满足企业灵活快速响应的需求。混合云融合了公有云的弹性开放和私有云的可管可控，驱动企业传统业务的稳态与创新业务的敏态协同发展。

Gartner预测未来90%的企业将利用混合云解决方案管理基础设施，即同时采用公有云和专有云部署模式，以满足单一云部署模式难以实现的复杂应用场景需求。从专有云产品出发的混合云解决方案解决实现了多云体系和IaaS/PaaS技术间的无缝融合，使得企业核心应用系统上云和传统政企上云化繁为简，让企业专注于自身业务场景，释放更多潜在价值。IDC同样预测，到2023年中国50%以上的企业应用将部署在容器化的混合云/多云环境中，以提供敏捷的、无缝的部署和管理体验。

由此可见，混合云在未来成为企业上云首选已成为业界共识。



阿里云专有云

作为目前业界应用规模最大，具备丰富应用场景的践行者，阿里云专有云具备三大关键能力：

- **全自研原生专有云**：提供业界首个公共云架构的专有云平台，与阿里云公共云同宗同源，基于公共云领域的长期积累和创新，在资源自助服务、开发、管理上客户可以获得天然一致性体验。

- **大规模商用实践**：基于经过大规模商用验证的阿里云专有云，拥有丰富的政企业务打磨经验，阿里云公共云更是作为亚太领头羊，为客户生产业务提供最佳稳定性。
- **历经双11考验的同款算力**：经过多年双11考验的全栈云平台，通过持续迭代，不断优化IaaS、PaaS、DaaS层及AI、IoT、钉钉等80+云产品和服务，帮助客户更快践行业务创新。

核心优势

- **稳定**：公共云数百万用户持续打磨的金融级容灾方案，保证系统的高可用性及业务连续性。
- **安全**：采用原生云安全架构，为用户提供立体化分层防护，国内首家通过商用密码应用安全性评估的云平台，首个通过等保2.0四级评估云厂商。
- **开放**：提供标准兼容的开发接口，与多品牌硬件兼容，并可将人工智能、中间件、大数据等70+款云产品灵活部署到数据中心。
- **智能**：提供企业级云管理入口，可基于统一的云资产管理提供监管控一体化的智慧指挥和自动化运维，并拥有经过大规模验证的成熟AI算法。

阿里云专有云大事记

4.安全与合规

数据安全和用户隐私是阿里云专有云最重要的原则，阿里云致力于打造公共、开放、安全的专有云云计算服务平台。通过技术创新，不断提升计算能力与规模效益，将云计算变成真正意义上的基础设施。

阿里云专有云竭诚为用户提供稳定、可靠、安全、合规的云计算基础服务，帮助保护用户的系统及数据的可用性、机密性和完整性。

资质认证

阿里云的安全流程机制得到国内外相关权威机构的认可，阿里云将阿里巴巴集团基于互联网安全威胁的长期对抗经验融入到专有云平台的安全防护中，将众多的合规标准融入云平台合规内控管理和产品设计中，同时广泛参与各类云平台相关的标准制定并贡献最佳实践。

至目前为止，阿里云获得了海内外十余家机构的认证，是亚洲资质最全的云服务商。

阿里云获得的资质

资质	说明
ISO 27001	信息安全管理体系国际认证，从数据安全、网络安全、通信安全、操作安全等各个方面充分证明阿里云平台履行的安全职责。
CSA STAR	云安全管理体系国际认证，阿里云获得全球首个金牌。
ISO 20000	IT服务管理体系认证，意味着阿里云建立了标准的服务流程并严格执行云平台服务规范化，提高效率并降低IT整体风险。
ISO 22301	业务连续性管理体系认证，意味着阿里云具备业务连续性计划、灾备建设和定期演练，提升云平台稳定性。
等级保护测评（四级）	阿里专有云平台具备依据GB/T 22239 -2019《信息安全技术网络安全等级保护基本要求》制定的云计算平台等级保护2.0合规能力规范（第四级）要求的安全技术能力。
工信部云服务能力标准测试	云产品国家实验室认证是基于国家标准的唯一产品级分级认证。
服务组织控制（SOC）审计认证	阿里云通过了SOC1/2的TYPEII、SOC3审计。

阿里云专有云在国内获得的资质

资质/认证	颁发机构
ITSS云计算服务能力（私有云IaaS服务/一级）	中国电子工业标准化技术协会
可信云-云服务用户数据保护能力（私有云）	中国信息通信研究院
公安部信息系统安全等级评估报告（四级，专有云）	公安部信息安全等级保护评估中心
公安部信息系统专有云V3.0安全等级保护测评报告	公安部信息安全等级保护评估中心
公安部信息系统安全大数据轻量专有云平台安全评估报告	中国信息通信研究院
云测评证书-云计算参考架构-云解决方案	中国电子技术标准化研究院
可信云-开源解决方案（私有云敏捷版）/虚拟化及虚拟化管理软件	中国信息通信研究院

合规体系

阿里云依据标准和行业最佳实践不断完善自身的管理与机制，通过了一系列的标准认证、三方审计以及自评估，力求更好地向用户展示阿里云的合规实践。

阿里云面对不同角度、不同行业、不同地区的合规需求，整体合规工作可以划分为以下部分：

管理体系合规

这些合规认证体现了阿里云成熟的管理机制和遵从的行业最佳实践：

- ISO 27001：信息安全管理体系。
- ISO 20000：IT服务管理体系。
- ISO 22301：业务可持续性管理体系。
- CSA STAR：云服务安全的成熟度模型。
- 等级保护测评（四级）。
- 中国CNAS云计算国家标准测试。

体系化合规报告

这些合规认证展示了阿里云云平台管控的完整性和有效性，包括体系控制是否持续有效、职责分离是否准确、运维操作审计是否完善等。

SOC 1/2 TYPE II：服务组织控制（SOC）报告是阿里云邀请第三方机构出具的一系列独立的第三方检查报告，证明阿里云关键合规性控制和目标的持续有效性。这些报告的目的是帮助用户和用户的审计机构了解支持运营和合规性的控制措施。阿里云具备的SOC报告分为三种类型：

- SOC 1 TYPE II：针对财报的内控报告。
- SOC 2 TYPE II：安全性、可用性与机密性报告。
- SOC 3：安全性、可用性与机密性报告。

阿里专有云等保2.0合规能力白皮书

针对等级保护2.0要求，在中国云计算安全等级保护合规能力规范体系技术社区指导下，依据《云计算安全等级保护合规能力框架》，由公安部信息安全等级保护评估中心和阿里云计算有限公司共同编制，发布了《阿里专有云网络安全等级保护2.0合规能力白皮书》，从等保能力验证技术架构、阿里专有云等保2.0合规状况及白皮书使用建议等方面做了详细阐述。借助白皮书，客户能够快速获取多交付场景下的专有云平台侧的合规防护能力，同时结合客户侧的应用、安全管理、物理环境等方面的保护措施，共同构筑满足等保和客户需求的信息系统整体安全防御体系。

5.选择阿里云专有云

超大规模分布式云操作系统

阿里云专有云与公共云使用同一套底层架构——飞天大规模分布式计算系统内核，为上层的服务提供存储、计算和调度等方面的底层支持。

飞天分布式操作系统是由阿里云自主研发、服务全球的超大规模通用计算操作系统，它可以将遍布全球的百万级服务器连成一台超级计算机，以在线公共服务的方式为社会提供计算能力。飞天分布式操作系统能够提供足够强大的、通用的、普惠的计算能力。

> **说明**
>
> - ARM架构支持基于鲲鹏920芯片、飞腾FT-2000+芯片和飞腾S2500芯片的服务器。
> - X86架构支持Intel和海光芯片服务器。

飞天平台内核包含的模块覆盖了以下主要的功能：

- **分布式系统底层服务**：提供分布式环境下所需要的协调服务、远程过程调用服务、安全管理服务和资源管理服务。这些底层服务为上层的分布式文件系统、任务调度等模块提供支持。
- **分布式文件系统**：提供海量的、可靠的、可扩展的数据存储服务，将集群中各个节点的存储能力聚集起来，并能够自动屏蔽软硬件故障，为您提供不间断的数据访问服务；支持增量扩容和数据的自动平衡，提供类似于POSIX的用户空间文件访问API，支持随机读写和追加写的操作。
- **任务调度**：为集群系统中的任务提供调度服务，同时支持强调响应速度的在线服务和强调处理数据吞吐量的离线任务；自动检测系统中故障和热点，通过错误重试、针对长尾作业并发备份作业等方式，保证作业稳定可靠地完成。
- **集群监控和部署**：对集群状态、上层应用服务运行状态、上层应用服务性能指标进行监控，对异常事件产生警报和记录；为运维人员提供整个飞天平台以及上层应用的部署和配置管理，支持在线集群扩容、缩容和应用服务的在线升级。

统一的部署与管控系统

专有云飞天基础运维平台（tianji）提供了云服务产品的统一部署、验证、授权和管控能力，为云服务提供基础性的支撑。

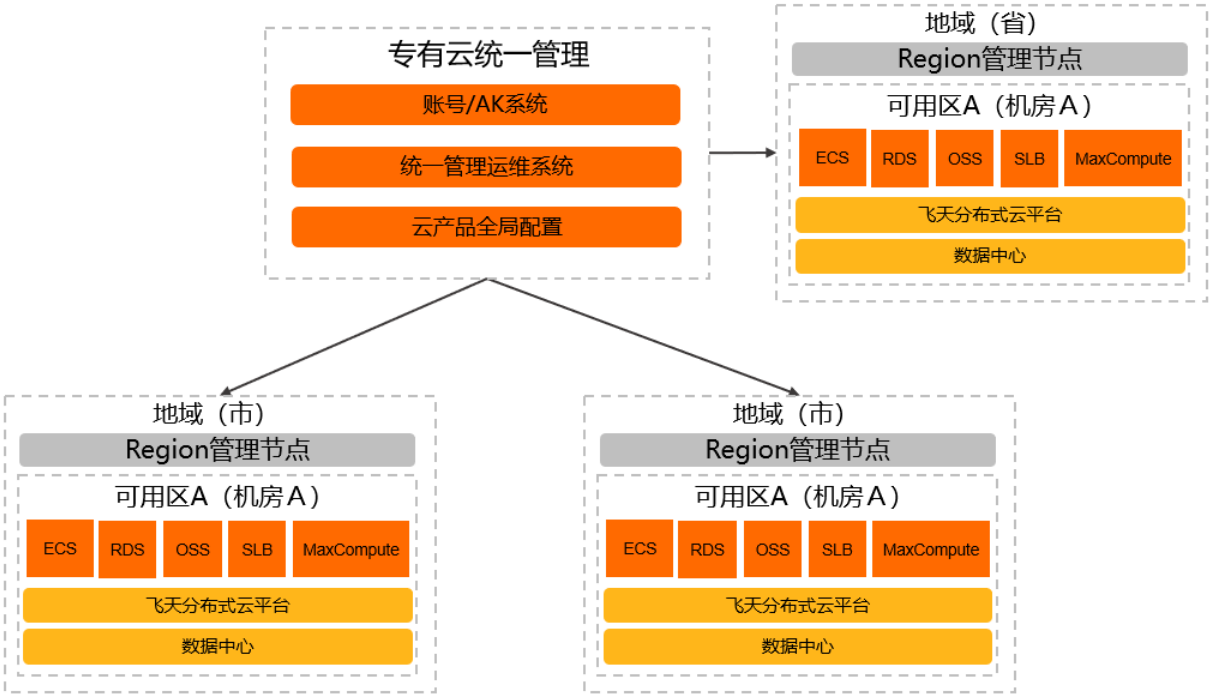
Tianji框架中包含部署框架、资源库、元数据库、认证授权、接口网关、日志服务、管控服务等模块：

- 部署框架：为所有的云服务提供统一的接入平台部署和服务间的依赖关系管理功能。
- 资源库：保存所有云服务和依赖组件的执行文件。
- 认证授权组件：为云服务提供访问控制能力，支持多租户的隔离。
- 接口网关：为云服务提供统一的API管理平台。
- 日志服务：为云服务提供日志存储、检索、获取等功能。
- 管控模块：监控各云服务的基础健康状态，支撑云平台的运维体系。

多数据中心跨地域统一管理

阿里云专有云已经实现各Region统一的运维、统一运营、统一计量的管理能力。

在阿里云专有云中，各Region可以使用VPC高速通道实现数据层面的打通、共享，真正地让云计算像水、电、煤一样成为国家的基础设施，带来普惠价值。融合资源池的管理系统可以集中管理和监控各个数据中心的计算、存储、网络资源及使用情况，提供统一的资源管理、资源部署、运维管理、服务管理和自助服务等能力。



高可靠的灾备解决方案

阿里云专有云容灾支持多种解决方案，包括异地容灾、同城容灾、混合云备份、多Region和容灾混合组网、两地三中心容灾等方案。

容灾系统通常是指在相隔较远的异地，建立两套或多套功能相同的系统，系统之间可以相互进行健康状态监视和功能切换，当一处系统因意外（如火灾、洪水、地震、人为蓄意破坏等）停止工作时，整个应用系统可以切换到另一处，保证系统功能仍可以继续正常工作。

阿里云专有云容灾解决方案，基于阿里云自身的云计算能力设计与开发，遵循国际通用的容灾标准。在网络条件符合设计要求的情况下，云平台可以实现网络接入层双活，用户应用层双活，数据持久化层主备。

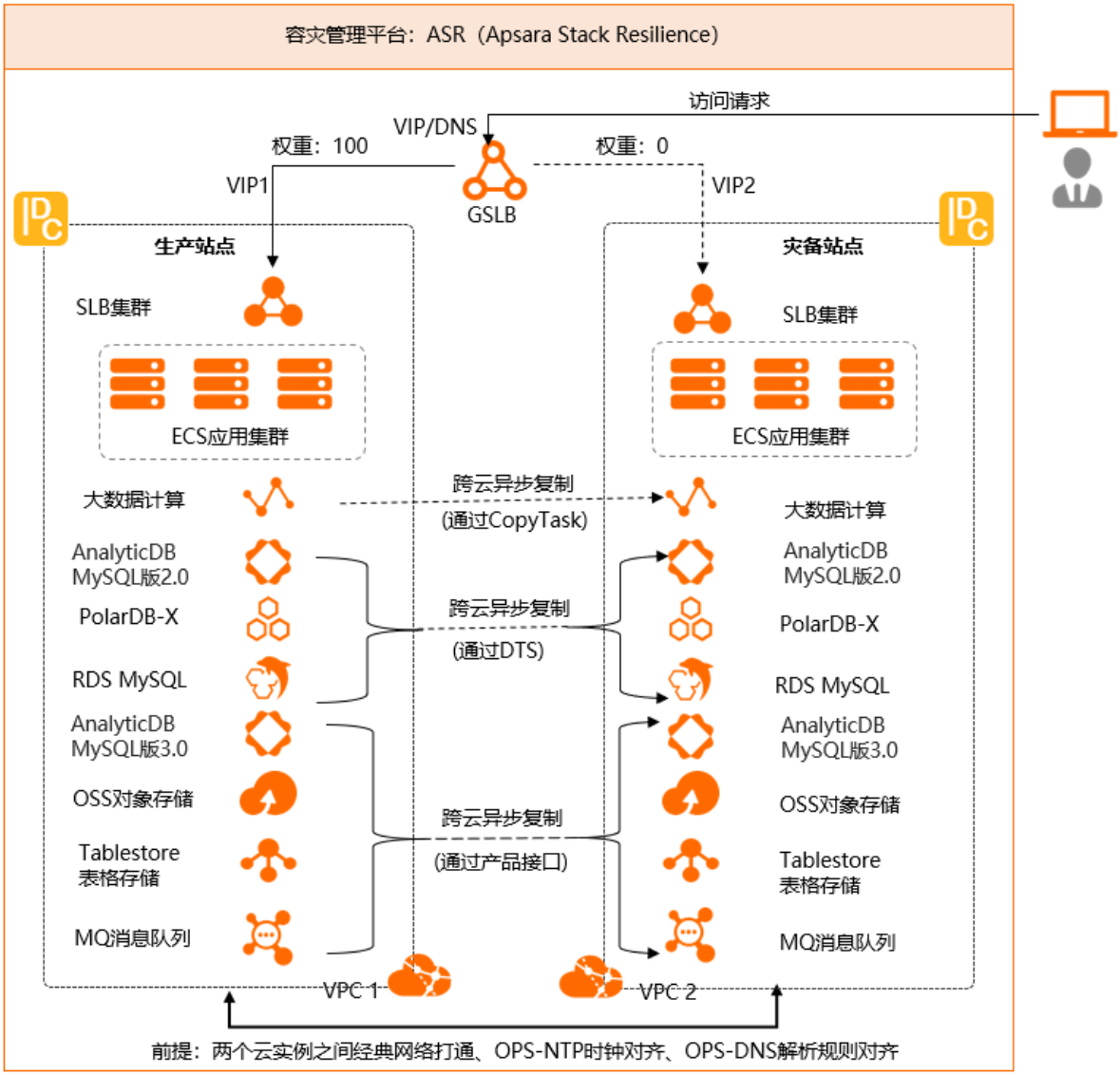
异地容灾

异地容灾方案采用主备模式，主备机房的资源都对用户可见，被保护的云产品实例（例如RDS实例、OSS Bucket等）的数量和规则在主备机房之间按照1:1的对等关系分配，并基于应用视角创建保护组、形成灾备关系。

异地容灾支持跨云异地容灾和跨Region异地容灾两种场景：

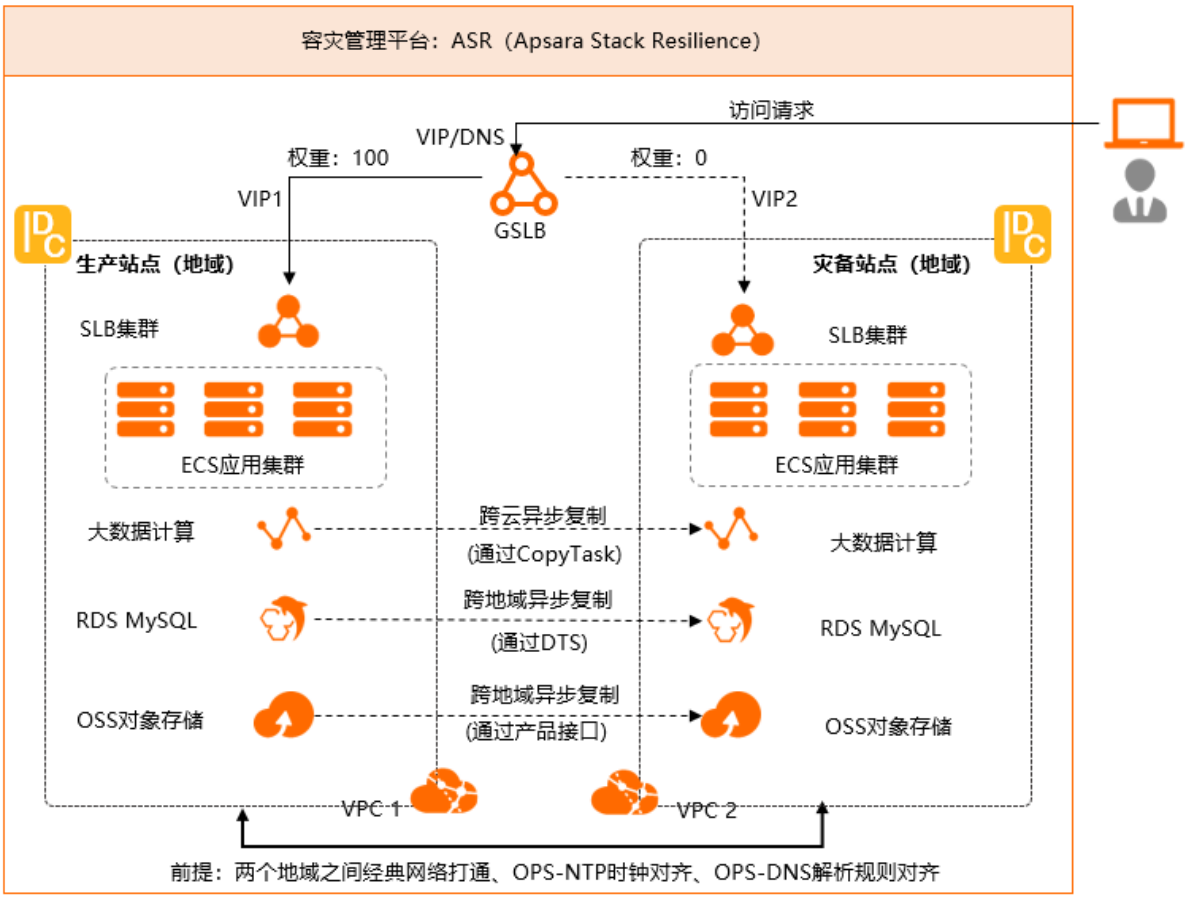
- **跨云异地容灾**

在两个云实例间进行灾备，生产站点和灾备站点是部署在异地的两个相互独立的云实例，两者运行独立的账号体系，用户登录这两个云实例需要分别做账号鉴权。



- **跨Region异地容灾**

  在两个Region间进行灾备，生产站点和灾备站点是同一个云实例下的两个Region，两者拥有相同的账号体系。跨Region异地容灾场景下，支持单元Region向中心Region容灾，以及单元Region向单元Region容灾。

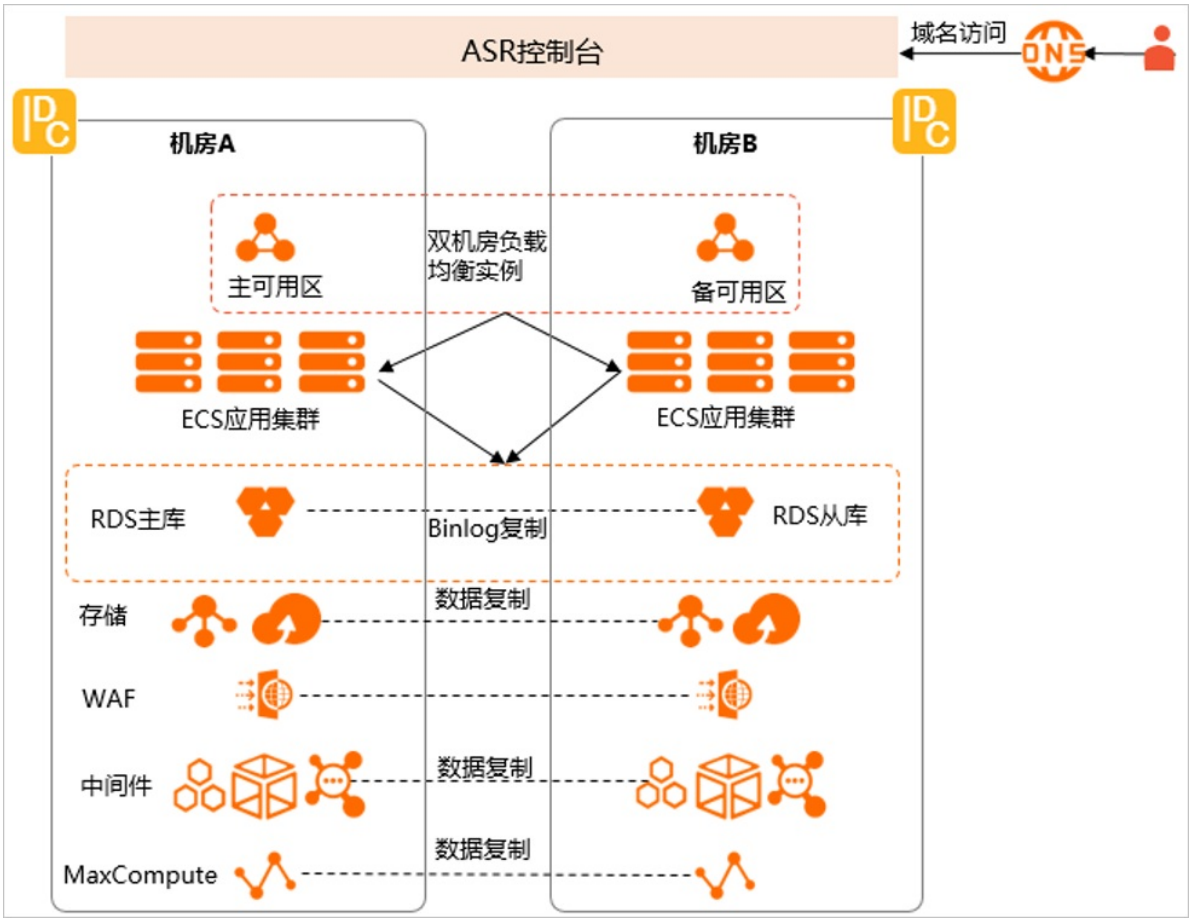


同城容灾

同城容灾是指在同一个Region的两个IDC，他们相互独立但互为容灾，当主机房出现异常时，通过同城容灾ASR（Apsara Stack Resilience）切换服务，将备机房切换到线上。

- **同城容灾（两机房）**

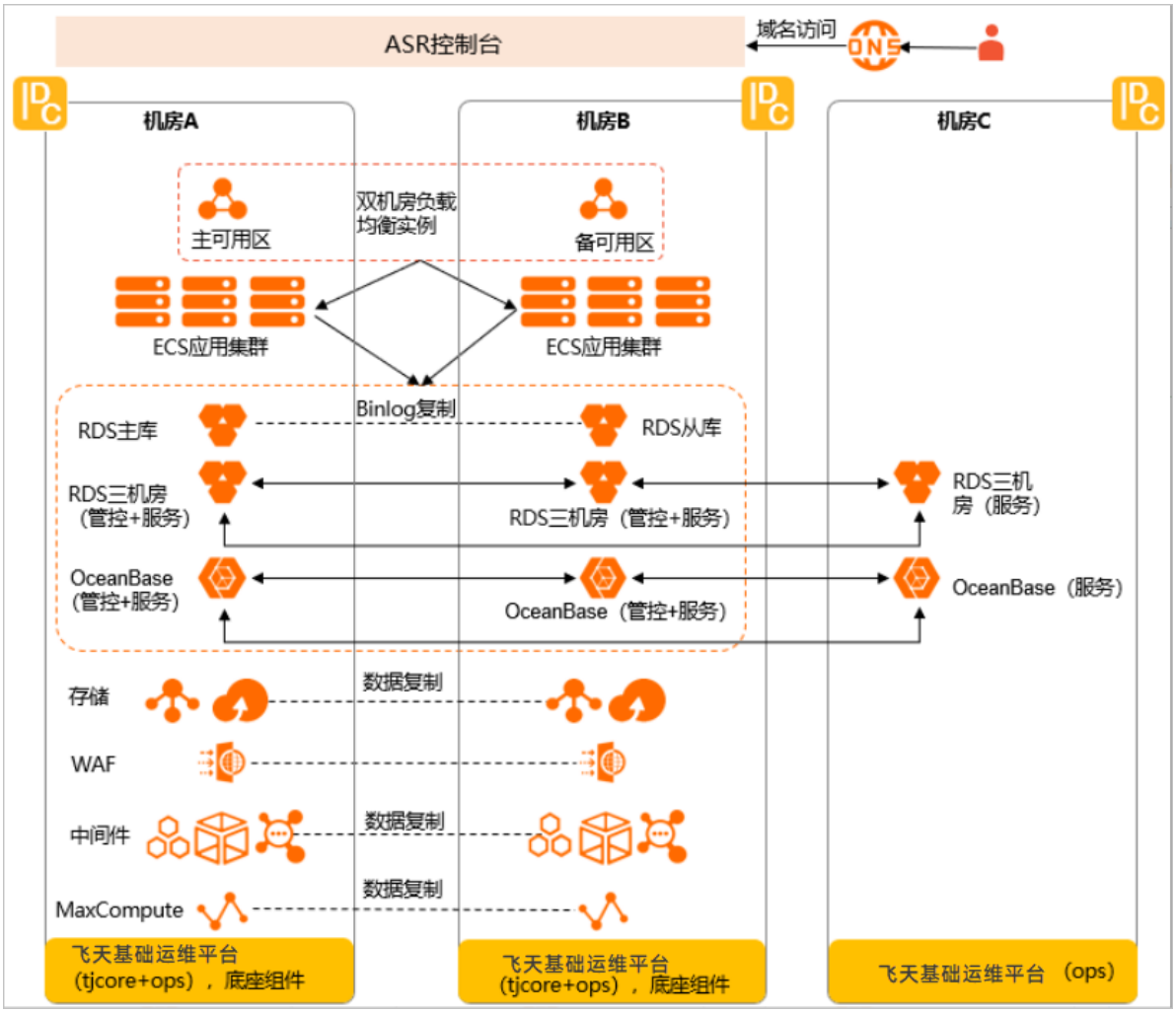
  用户应用通过域名访问两个机房里的各类云服务。当云产品切换到备机房时，云服务的域名不变，用户应用无需改造，让用户开发聚焦于业务，降低应用开发难度，方便用户使用云服务。



> **说明**
>
> 机房A为主机房，机房B为备机房。

- **同城容灾（三机房）**

  在同城容灾双机房基础上，可增加部署第三机房，数据库分布式部署，保障金融行业业务数据零丢失，数据恢复点目标RPO（Recovery Point Objective）为0。主备或双活形态的容灾产品在三机房场景中，容灾机制保持不变，依然按照双机房的策略实现故障恢复。

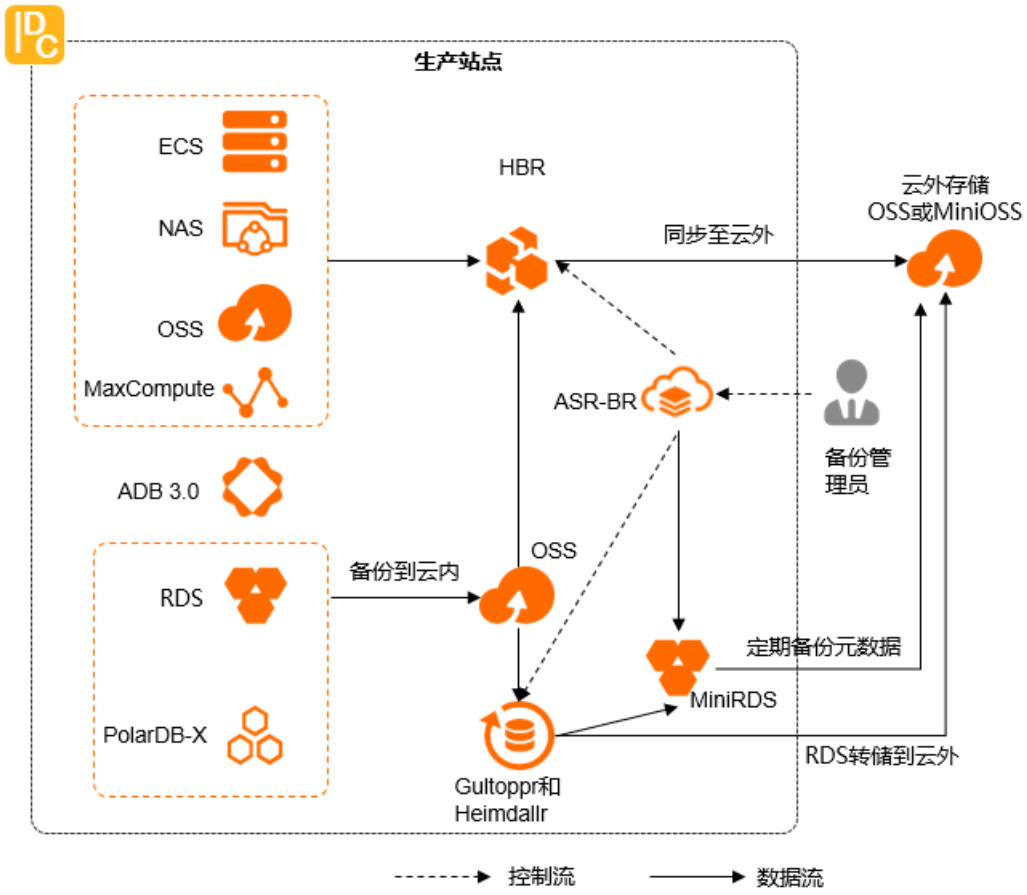


混合云备份

专有云混合云备份支持本地备份和跨地域备份两种架构模式：

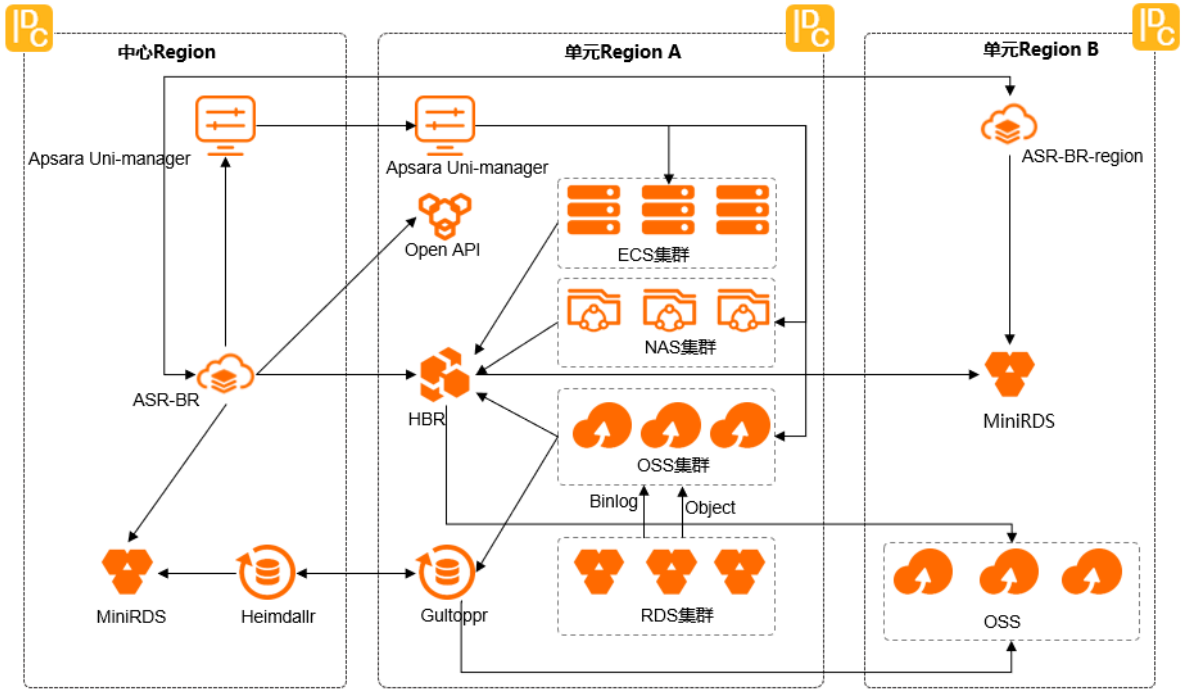
- **本地备份**

  在生产站点部署备份控制台ASR-BR（Apsara Stack Resilience for Backup and Recovery）以及相关的服务，将生产站点上的数据定期备份到支持OSS协议的存储中。该架构可以降低客户搭建成本。



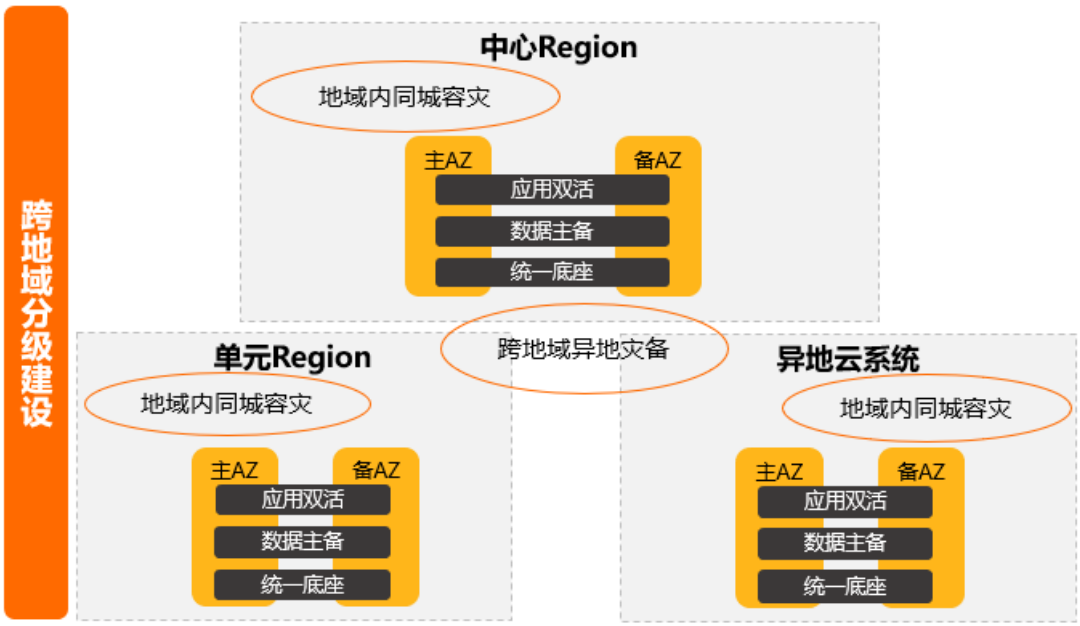
- **跨地域备份**

  在多Region架构中，将一个Region的数据备份到另一个Region。



多Region和容灾混合组网

阿里云专有云飞天企业版多Region场景下，支持地域内同城容灾、跨地域异地容灾和跨地域备份，可满足不同行业的灾备等级要求。

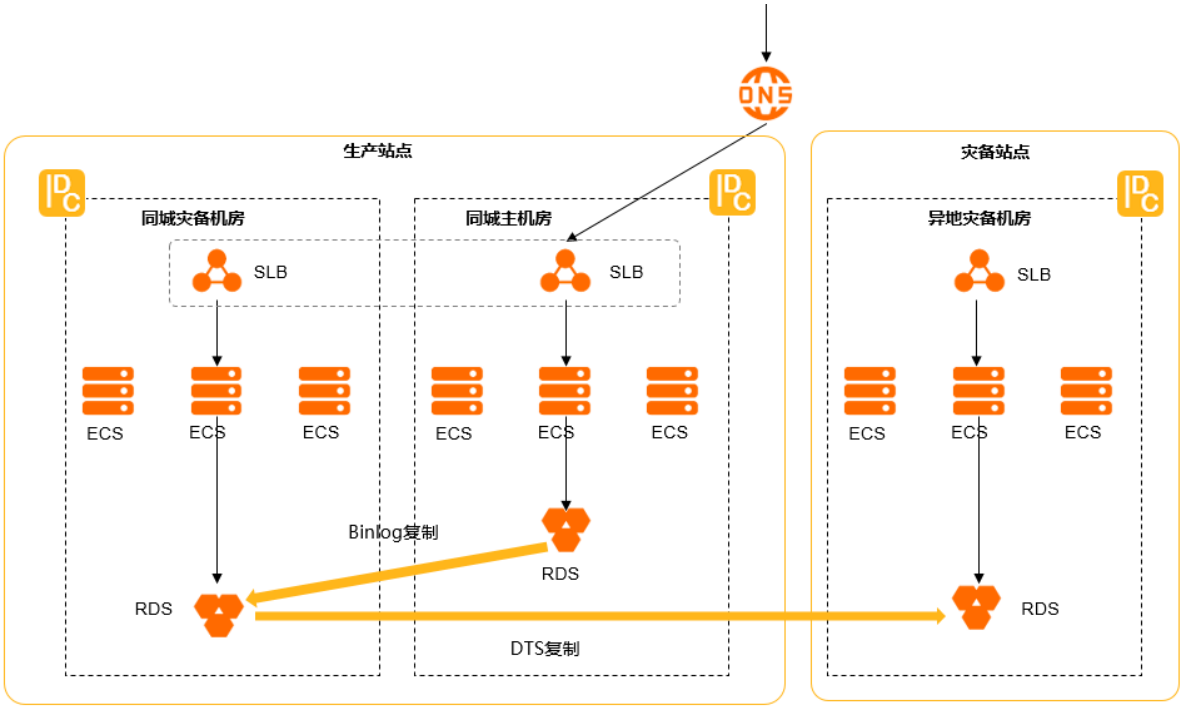


两地三中心

在两地三中心容灾方案中，两地指同城、异地，三中心是指生产中心、同城灾备中心、异地灾备中心，这一解决方案具备较高的灾难备份能力。当前两地三中心容灾方案支持的云产品包括云数据库RDS和对象存储OSS。

- RDS两地三中心容灾方案

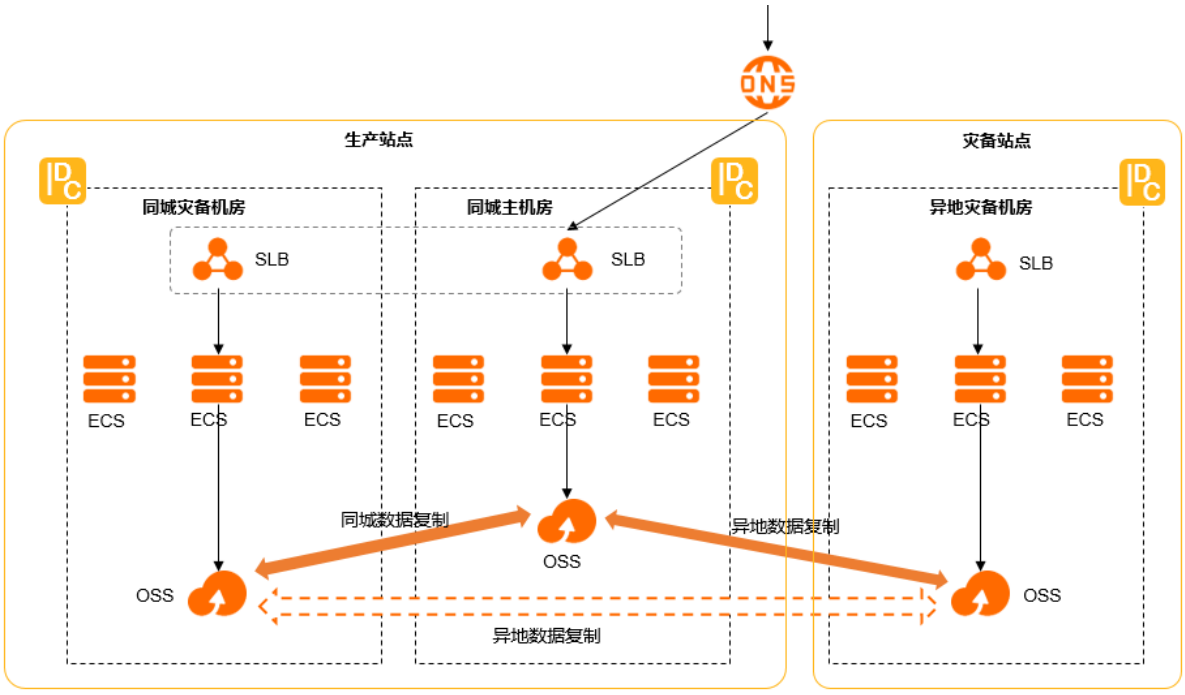
  RDS在生产站点和灾备站点中独立部署，其中生产站点有两个机房，RDS在这两个机房中都是独立部署。生产站点的两个RDS实例分别为主RDS和从RDS，组成了同城容灾。生产站点和灾备站点之间组成异地容灾，在两个云实例之间支持实例维度的容灾能力。



- OSS两地三中心容灾方案

OSS在生产站点和灾备站点中独立部署，其中生产站点有两个机房，OSS在这两个机房中都是独立部署。生产站点的两个机房组成同城容灾，两机房间支持Bucket维度的容灾能力。生产站点和灾备站点之间组成异地容灾，在两个云实例之间支持Bucket维度的容灾能力。

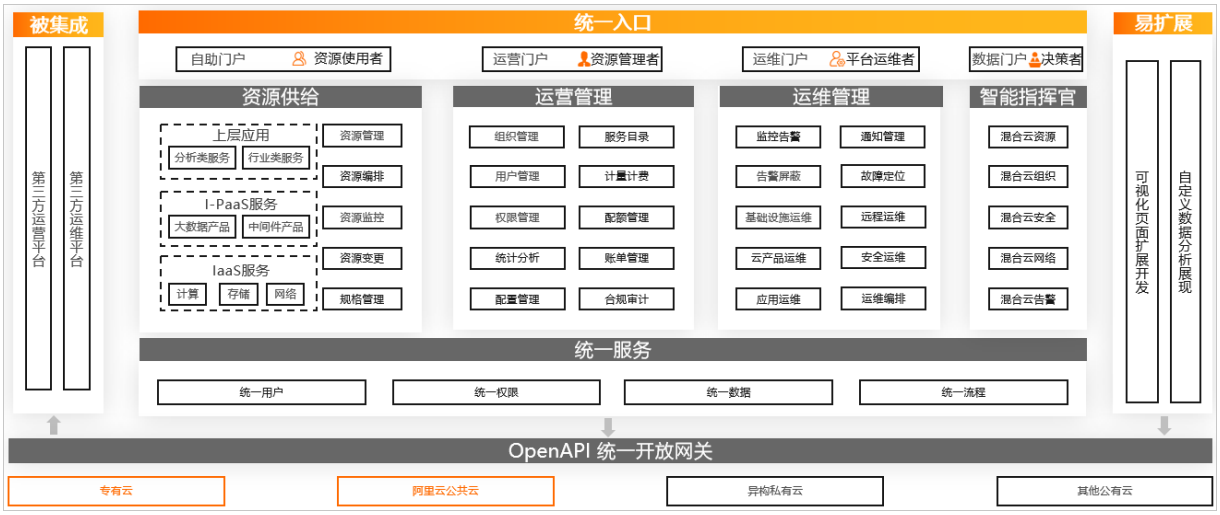
当生产站点的同城主机房发生故障后，灾备管理员通过同城容灾控制台启动切换计划，将OSS主实例一键切换至同城灾备机房，保证业务连续性。当生产站点的双机房都发生故障时，灾备管理员在灾备控制台ASR-DR（Apsara Stack Resilience for Disaster Recovery）上启动故障切换计划，将OSS保护组一键切换（Failover）至异地灾备站点，继续保证业务连续性。当生产站点恢复后，在主备Bucket之间创建反向数据复制通道，将灾备Bucket的增量数据同步到主Bucket。数据同步完成后，再启动故障回切计划，将业务流量从灾备站点切换（Failback）至生产站点。OSS两地三中心容灾方案为客户系统业务连续性提供双层保障。



统一云管平台Apsara Uni-manager

阿里云专有云提供统一的云管平台，统一云管平台Apsara Uni-manager是面向阿里云专有云和混合云场景的企业级云管理平台。它提供全方位的云资源供给、运维和运营管理能力，具备一体化管控、智能化运维、精细化运营及个性化扩展等核心竞争力，简化混合云管理，提升用户体验，加速企业数字化转型。

- **统一入口**：提供统一操作入口，主要由自助门户、运营门户、运维门户和数据门户组成，为不同业务的用户提供全面的云管理能力。
- **统一服务**：提供统一服务能力，包括统一用户、统一权限、统一数据和统一流程管理。
- **开放、易集成、易扩展**：具备多云管控能力，具有统一开放的API网关。北向将API网关提供给第三方集成商，通过业务数据采集，集成第三方数据和页面，南向将其提供给多云环境集成适配。



开放的云服务接口

在阿里云专有云中，云服务通过OpenAPI平台提供丰富的SDK包和RESTful API接口。客户可以使用开放接口来灵活访问专有云提供的各种云服务。同时还可以通过OpenAPI获取云平台的基础管控信息，将专有云平台接入到客户统一的管控系统。

6.专有云架构

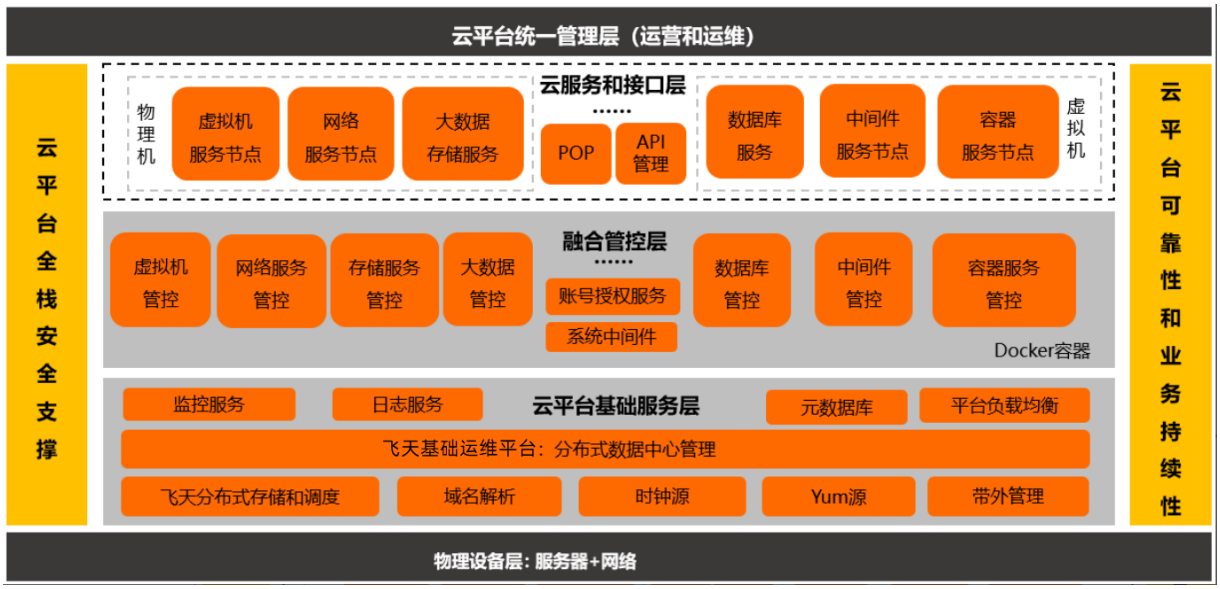
阿里云专有云采用原生云架构，以自研的阿里云操作系统、分布式技术和产品为基础，运用一套体系支撑所有云产品和云服务，提供完整的云平台开放能力，具备完善的企业级服务特性、容灾和备份能力，是客户完全自主可控的云平台。

系统架构

阿里云专有云系统架构主要分为以下五个部分：

- **物理设备层**：主要包括用于云计算的物理服务器和网络等硬件设备。
- **云平台基础服务层**：提供云平台运行的基础服务能力，包括带外管理、装机克隆、时钟源、YUM源服务、元数据库和平台日志服务等能力。
- **融合管控层**：为云产品的管控融合层。主要负责分管云平台各类云产品的管理和控制。
- **云服务与接口层**：一是通过融合的服务节点管理，对虚拟机和物理机提供统一管理和运维；二是通过开放的API管理平台，统一接口并支持定制化开发。
- **云平台统一管理层**：提供统一的运营和运维管理入口。

此外，阿里云专有云还提供了全栈的稳定性架构支撑，保障云平台的可靠性和业务持续性。

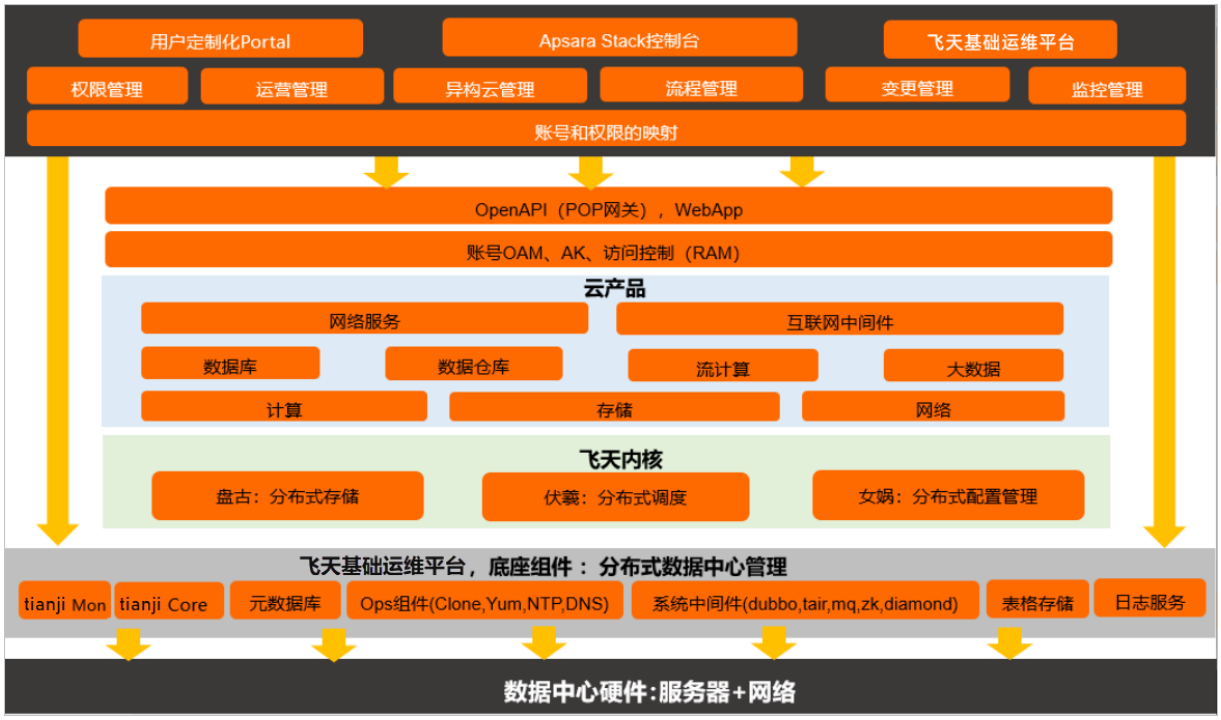


逻辑架构

专有云通过将物理服务器的计算、存储、网络设备虚拟化成虚拟计算、分布式存储和软件定义网络，并在此基础上提供云数据库、大数据处理、分布式中间件服务，为用户的应用系统提供IT基础服务的支撑能力，同时可以和用户现有的账号体系，监控运维系统进行对接。

专有云逻辑架构具有以下特点：

- 硬件基础包括物理服务器和网络设备，其中服务器支持X86、ARM两种架构。
- 飞天内核（分布式引擎）是飞天操作系统的内核，为各类基于飞天操作系统的阿里云产品提供了内核基础。
- 所有云产品都遵从统一的API框架、管理运维（账号、授权、监控、日志）体系和安全体系。

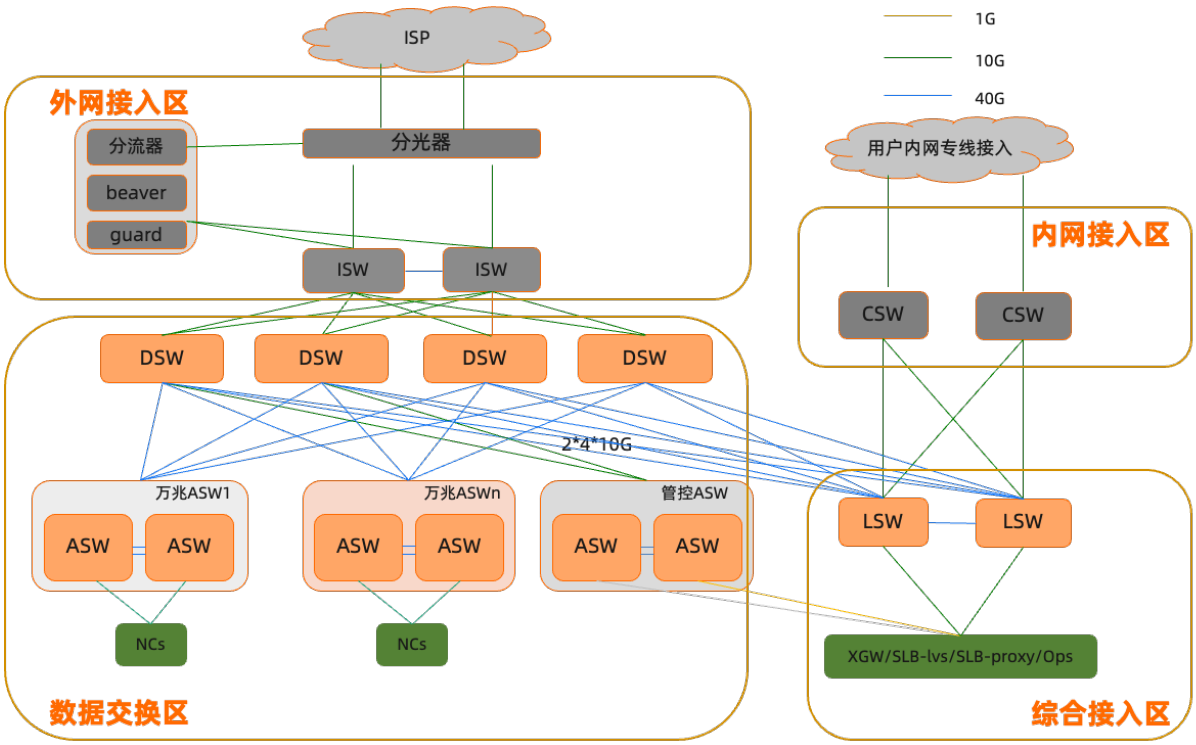


网络架构

阿里云专有云采用CLOS架构的大二层扁平组网，支持业务平面与带外管理平面隔离，具备交换机线性扩展和负载分担能力。

专有云网络架构定义了内网接入区、外网接入区、数据交换区和综合接入区四个网络区域。

- **内网接入区**：实现客户原自有网络资源与云上资源打通，既可以满足客户访问云上专有网络VPC，也可以满足客户的普通云服务接入。
- **外网接入区**：外部互联接入模块直接与ISP或者客户的骨干网络相连，业务服务区通过外网接入模块与公网互通或者多中心互通。
- **数据交换区**：为所有云业务服务器提供接入，所有云业务服务器间的内部流量交互在本模块内完成。
- **综合接入区**：接入各类云产品服务（如负载均衡SLB和专有网络VPC等）和基础服务。



网络区域中各层交换机承担的角色和作用

角色名称	所属区域	主要作用
ISW（互联交换机）	外网接入区	出口交换机，互联ISP或用户网络骨干。
CSW（内网接入交换机）	内网接入区	接入客户的内网骨干网络，实现云网络内外部的路由分发交互，包括VPC专线接入。
DSW（分布层交换机）	数据交换区	核心交换机，用于连接各个接入层交换机（ASW）。
ASW（接入层交换机）	数据交换区	接入交换机，用于接入云服务器，上行连接互联核心交换机DSW。
LSW（综合接入交换机）	综合接入区	云产品服务接入交换机，主要提供VPC和SLB等服务。

内网接入区

内网接入区由两台CSW组成，为内部用户提供VPC接入和普通云服务接入两类接入。

- **VPC接入**：由CSW提供内部用户与VPC的映射关系，将内部用户分别导入各个VPC内。在CSW上，同用户群保持相互隔离。
- **普通云服务接入**：CSW与综合接入区通过外部边界网关协议（eBGP）互联，直接提供业务接入区的所有资源访问支持。

通过使用VPC专线接入方案，客户可以完全掌控自己的虚拟网络，包括选择自有IP地址范围、配置路由表和网关等。此外，也可以通过专线、VPN等连接方式将VPC与传统数据中心组成一个按需定制的网络环境，实现应用上的平滑迁移上云。

外网接入区

外网接入区由两台ISW组成，接入ISP运营商或客户公网骨干网络，实现内外部的路由分发交互。

两台ISW之间通过内部边界网关协议（iBGP）相互备份路由。上联到ISP运营商或客户公网骨干网络，互联方式根据实际情况采用静态路由或者外部边界网关协议（eBGP），互联带宽根据客户的专有云网络规模和客户骨干网络带宽设计定义。

为了提升网络可靠性，推荐两台ISW接入多家运营商，使用BGP协议的方式与ISP运营商网络互通，每个运营商接入2个10GE网络。同时，外网接入区与数据交换区之间通过eBGP协议交互路由。外网接入区向数据交换区发布相关外网络由，接收数据交换区发出的云服务内部路由，实现云网络内部与外部交互。

此外，在外网接入区旁路挂载云盾网络安全防护系统，外网访问云网络的流量通过分光器引流至云盾网络检测与响应系统，监测到攻击流量时通过网络检测与响应系统发布相应的路由将攻击流量引入云盾网络安全防护系统进行清洗，并将清洗后的流量回注。

数据交换区

数据交换区是由DSW和ASW组成的典型的二层CLOS架构。

ASW两两堆叠作为叶子节点，根据网络规模大小可选择不同适用范围的数据交换模型。所有专有云业务的服务器上行至ASW堆叠设备，ASW和DSW之间通过eBGP协议互联，DSW之间相互没有连接。数据交换区与其他区域之间通过eBGP协议互联。

同时，数据交换区接收外网接入区的ISW发布的外网络由，并发布云产品地址网段到ISW。

综合接入区

综合服务区由各类云产品服务器（如洛神高性能云网关XGW、四层/七层负载均衡器和OPS管控服务等）分别与两台LSW互联，通过OSPF协议交换路由信息。两台LSW之间通过iBGP协议交互路由信息；LSW与数据交换区的DSW、内网接入区的CSW之间通过eBGP协议交换路由信息。

安全架构

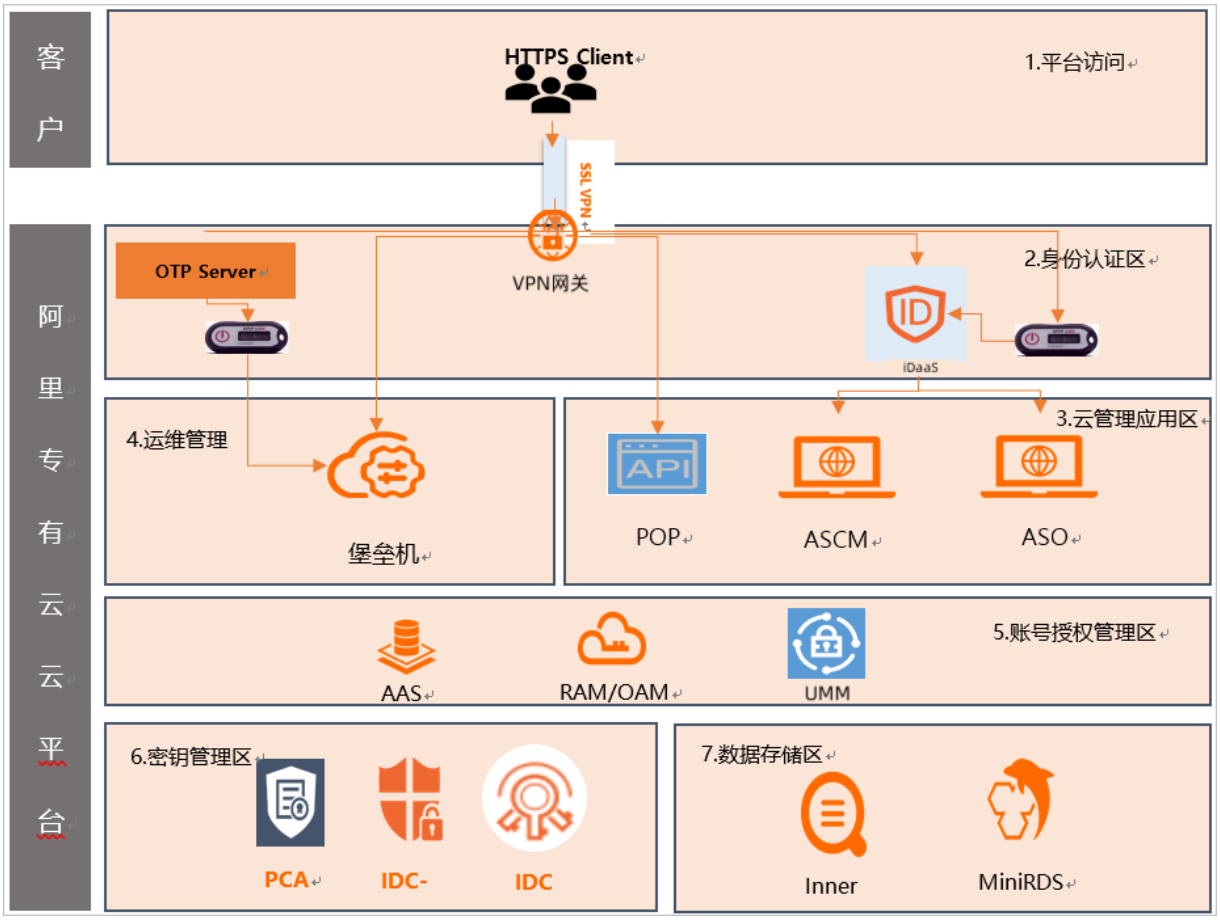
阿里云专有云提供从底层通信协议到上层应用的全方位安全能力，保证用户的访问和数据安全。

专有云提供完善的角色授权机制，保证多租户模式下资源访问的安全可控；专有云提供包括安全管理员、系统管理员及安全审计员多种安全角色，满足多重安全运营管理场景。

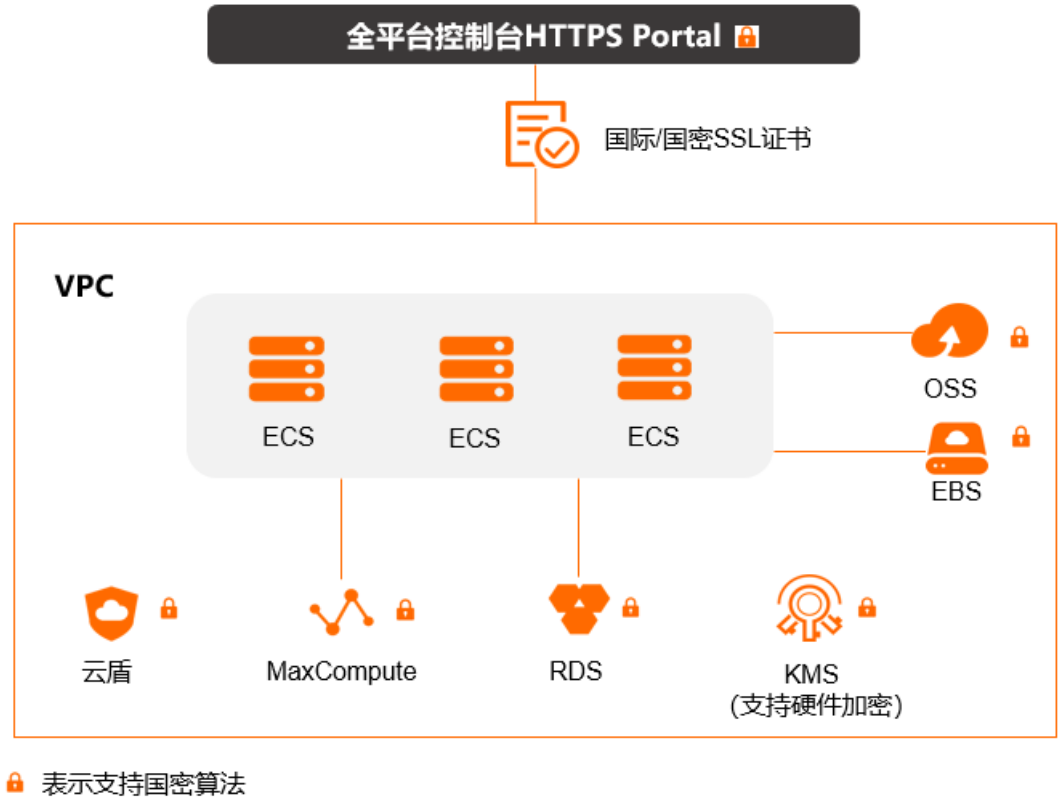
此外，阿里云专有云从V3版本引入云盾安全产品，为客户提供多层面、一体化的云安全防护解决方案。

国密算法支持

阿里云专有云所有控制台均需要通过HTTPS证书的方式访问，服务端同时部署国际算法（RSA）SSL证书和国密算法（SM）SSL证书；平台密钥管理服务经过国密适配和改造，支持硬件加密机。



关键云产品（块存储EBS、对象存储OSS、大数据计算服务MaxCompute、云数据库RDS等）均支持使用国密算法加密。同时，云盾加密服务提供国密加解密能力。



表示支持国密算法

底座组件

阿里云专有云底座包含三大类组件，共同为云平台的部署和运维提供支撑。

组件分类	组件名称	主要作用
Ops组件	Yum	用于安装软件包的软件源。 软件源在初始装机阶段即部署完毕，主要用于在物理服务器上安装操作系统、部署飞天、ECS等专有云的应用软件包及其依赖的组件
	Clone	机器克隆服务。
	NTP	时钟源服务。 部署在专有云的物理机服务器，从标准NTP时间源同步信息，并授时给其他宿主机。
	DNS	域名解析服务。 为专有云内部环境提供域名的正解析和反解析服务。 在两台OPS管控机器上各运行一个bind实例，通过keepalived组件提供高可用服务，在一台失效的情况下另外一台能够主动接管服务。
底座中间件	dubbo	分布式RPC服务。
	tair	缓存服务。
	mq	消息队列服务。
	ZooKeeper	分布式协同。
	Diamond	配置管理服务。
	SchedulerX	定时任务服务。
	飞天基础运维平台	数据中心管理服务。
	TianjiMon	数据中心监控服务。
	OTS-inner	表格存储服务。
	SLS-inner	云平台日志服务。

底座基础组件	mini-RDS	元数据库。
	POP	云平台开放接口Open API服务。
	OAM	账号系统。
	RAM	认证授权系统。
	WebApps	运维控制台支撑。

7.应用场景

阿里云专有云能够为不同规模、不同行业的用户提供灵活的、可扩展的行业解决方案。针对各行业业务特性，阿里云打造个性化专有云方案，为客户提供一站式的产品与服务，包括工业、农业、交通、政务、金融、交通、教育等各个方面。

城市大脑

城市管理是中国数据量最大的领域之一，政府各部门内部的信息从封闭流动走向了在线的数据开放流动。城市数据流动的时间和空间变大了，数据的价值也变大了。云计算成为城市基础设施，数据作为新的生产资料和战略资源，而人工智能技术则构筑了智慧城市的神经中枢，从而形成“城市数据大脑”。

价值特点

- 城市治理模式突破：以城市数据为资源，提升政府管理能力，解决城市治理突出问题，实现城市治理智能化、集约化、人性化。
- 城市服务模式突破：更精准地随时随地服务企业和个人，城市的公共服务更加高效，公共资源更加节约。
- 城市产业发展突破：产业AI布局 ，开放的城市数据资源是重要的基础资源，带动产业发展发挥，促进传统产业转型升级。

金融云

金融云是服务于银行、证券、保险、基金等金融机构的行业云，采用独立的机房集群提供满足一行三会监管要求的云产品，并为金融客户提供更加专业周到的服务。通过自建/共建楼模式 ，满足中大型金融机构需要完全物理隔离的独立云机房需求，能够将云计算、大数据平台输出到客户的数据中心。

价值特点

- 独立的资源集群。
- 更严格的机房管理。
- 更高的安全容灾能力。
- 更严格的网络安全隔离要求。
- 更严格的访问控制。
- 完全符合银行级的安全监管及合规要求。
- 专业的金融云行业安全运营团队、安全合规团队、安全解决方案团队。
- 专业的金融云客户经理和云架构师。
- 更严格的用户准入机制。

8.云平台服务

8.1. 统一云管平台

统一云管平台是面向阿里云专有云和混合云场景的企业级云管理平台。它提供全方位的云资源供给、运维和运营管理能力，具备一体化管控、智能化运维、精细化运营及个性化扩展等核心竞争力，简化混合云管理，提升用户体验，加速企业数字化转型。

统一云管平台由以下部分组成：

- Apsara Uni-manager运营控制台：通过一体化的管控入口，提供精细化资源治理、智能化数据分析和个性化功能扩展等能力，降低企业的云管理成本。
- Apsara Uni-manager运维控制台：通过统一的运维入口，提供监控告警、巡检管理、资源管理等通用运维能力以及计算、网络、存储运维控制台等产品运维能力，降低云环境的运维成本，保障云环境安全稳定运行。
- 混合云智能指挥官：通过高可视化的数据大屏，为企业IT的决策者提供了混合云多维度的全景数据展示，包括混合云总体运行状态和资源使用情况，并支持针对不同角色设置不同的首页仪表盘。
- 多云管理平台：旨在实现“阿里云专有云、阿里公共云的混合云场景，以及其他异构云场景中多个云平台的统一云资源管控”，全面支持开放式云服务接入标准规范，为客户提供多云平台的接入管理、云产品与云资源的管理以及组织、用户、权限的管理等功能，帮助客户在异构云平台环境中实现多个云中心管理入口统一、使用规范的云平台管理。

8.1.1. 产品详情

统一云管平台提供资源管理、人员管理统一云管平台营中心、安全中心、应用中心等功能，简化物理和虚拟资源的管理和部署，提升资源利用率，降低运营成本；提供通用运维、产品运维、安全合规和系统配置等功能，简化日常运维操作，提升运维效率；提供典型业务场景预置大屏、支持灵活的自定义大屏，全方位多维度展示业务数据。

运营管理

- **资源管理**

  资源管理提供开通和监管资源的能力，通过管理资源集、配置所需资源监控项，帮助运营人员清晰地了解各资源的使用情况，异常时及时避险。

- **人员管理**

  通过管理组织、用户和用户组，帮助企业对人员的归属、权限、群组做集中管控，提供不同场景下对用户生命全周期管理的能力，满足不同用户对系统和资源的访问需求，提升企业的管理效率。

- **权限管理**

  通过配置角色、RAM、数据权限和访问控制，实现不同场景下的权限划分，管控用户对系统和指定云产品的访问，由此提高系统安全性。

- **运营中心**

  通过配额管理、计量计费管理、统计分析、账单管理，帮助企业对资源使用量和资源计费进行集中把控，帮助运营人员快速全面的了解资源使用情况和账单计费信息，并提供灵活的调控功能，满足企业日常运营所需。

- **安全中心**

  从操作日志、多因素认证设备（MFA）、阿里云AccessKey三方面加固用户访问系统和资源时的安全。

- **应用中心**

  通过应用管理、任务管理、系统管理，提供给用户一个更加快捷便利的应用交付与部署的途径，满足三方ISV供应商入驻专有云平台、快速迭代的内部产品（解耦底座版本依赖）等场景。

运维管理

- **通用运维**

  通过告警管理、巡检管理、资源管理、库存管理、变更管理和备份归档，完成基础运维。

- **产品运维**

  提供包括计算运维、网络运维、存储运维、数据库运维、中间件运维、大数据运维、云平台运维、安全服务和应用服务九大模块的功能。

- **安全合规**

  通过操作日志审计、物理机密码管理、AK密钥管理、云平台加密管理和云产品访问矩阵审计实现对运维操作的安全合规管理。

- **系统配置**

  通过用户权限、平台配置、运维API管理等进行系统配置。

管理者大屏

- **预置大屏**

  预置包括混合云资源、混合云组织、混合云安全、混合云网络、混合云告警五个科技感大屏，全方位多维度实时展示混合云的运行和资源使用状态。

- **自定义大屏**

  通过提供可视化的大屏在线编辑器，支持按照模板创建自定义大屏，自定义数据、样式，快速实现业务数据大屏的个性化定制。

多云管理

- **多云接入管理**

  提供创建云平台的管理操作，支持接入多个阿里云专有云类型（包括企业版、敏捷版、敏捷版大数据版、DBStack、CNStack、ZStack等）与公共云类型云平台实例、支持自助接入异构云平台；同时提供第三方厂商适配器接入管理页面，支持用户进行适配器接入的统一管理。

- **云产品管理**

  提供多个云平台的云产品分类及云产品管理，支持对多个不同云平台的云产品进行统一归类定义，满足客户对于产品分类统一管理的要求；提供云平台的云产品服务目录，实现不同云平台环境中的服务能力整合。

- **多云资源统一管理**

  通过资源采集，将资源汇集在多云管理平台的同一列表中，提高用户统一管理的效率。

- **用户组织管理**

  提供组织管理、用户组管理和用户管理能力。

- **权限管理**

  提供基于角色的权限管理能力，包括角色的创建、修改、删除、查询等功能；支持对角色进行授权管理操作，包括角色权限的增删改查、赋权记录查询等功能。

  授权管理支持多种场景的授权操作：基于业务功能授权；基于云平台和云产品粒度授权；基于组织及项目粒度授权；基于项目级授权，对所属项目的用户、用户组实现单独授权；对组织、用户组、项目、用户直接进行授权。

- **项目管理**

  项目中主要包括用户组、云实例、云资源等属性，帮助客户实现以项目维度多云平台的用户、云服务资源的统一管控，支持客户通过项目粒度管理不同云平台资源，通过项目维度实现更细粒度的授权、管理。

- **多云计量管理**

  提供多云平台云资源计量统一管理的能力。通过多云计量管理，汇集组织在多个云平台中云资源的计量数据，提供资源计量的查看、搜索功能，支持对多个云平台中云资源的计量情况进行汇总统一展示。

- **审计日志**

  提供安全日志功能，支持查看多云管理平台的操作日志及纳管云平台的云产品操作日志，且提供日志的快速检索功能。

- **消息管理**

  通过自定义消息模板，支持对不同管理状态定义不同的消息模板内容；支持配置通过多种协同交互软件向用户发送消息。

8.1.2. 产品价值

统一云管平台帮助客户简单快速地建立自己的业务系统，有效提升资源利用率，降低运营成本；通过自动化运维流程，提供主动式监控告警、根源问题定位和故障自动修复等能力，降低云环境的运维成本，保障云环境的安全稳定运行。

统一入口体验佳

- 实现对混合云和多云资源的统一管理、灵活调度。
- 与公共云一致的云资源自助操作体验，简单易掌握。
- 从应用视角出发的一体化运营。

灵活权限利管控

- 提供运营管理、资源使用、资源监察、安全管理等多种预置角色，开箱即用。
- 可创建自定义角色，对权限共享范围、资源管理范围、应用操作权限、菜单权限灵活定义。
- 支持RAM鉴权，提供与公共云一致的权限管理方式。

智能分析助运营

- 全局数据实时更新联动，资源统一调度。
- 监控分析资源使用趋势，合理优化资源配置，提升资源利用效能。
- 提供详细计量计费账单，资源价值可视化，保障服务运营。

全面开放易集成

- 可视化API门户，有效降低学习成本，提升开发效率。
- 标准北向接口，提供多语言SDK。
- 支持页面级别的集成和个性化配置，快速对接第三方系统平台。

集中运维保平稳

- 对混合云资源、库存水位、告警等全方位集中监控，及时了解运行状况，识别风险隐患。
- 自动、实时更新云资源间的依赖拓扑，结合预置算法引擎及时提供疑似根因的判断，缩小排查范围，辅助故障定界。
- 提供运维原子化脚本操作封装平台和可视化编排能力，同时提供大量确定场景的故障自动化运维修复能力，减少人工操作占比。
- 共用公共云的资源库存AI算法，动态分析并自动计算最优扩容策略，保持客户用云成本处于高度优化状态，降低资源浪费。

指挥大屏全掌控

- 预置标准场景的大屏和灵活自定义大屏，全面覆盖各种业务场景。
- 通过不同的数据源类型（包括JSON、ASAPI、ASAPI大屏数据池、HTTP、JSONP、Excel）获取数据信息，提供全面易用的运维数据货架。

- 提供丰富的可视化组件和数据源，通过图表组件及数据源配置可灵活定制不同的大屏。
- 图形化（包括柱状图、饼图、仪表盘、地图等）展示运维数据，便于快速获取信息，直击大量运维数据背后的业务痛点，提升运维效率。

8.1.3. 应用场景

统一云管平台应用场景包括混合云管理、多级云管理、行业云运营、云运维管理。

混合云管理

客户建设专有云平台，需要统一云管平台根据企业组织模型对租户侧资源实现高效分发、权限管控、计量计费等运营管理，以提升资源使用效能、保障资源使用权限安全、提高组织资源运营管理效率。除此之外，当客户已部署阿里云专有云的同时，还拥有大量阿里云公共云资源或计划采购大量阿里云公共云资源时，也需要对混合云资源进行集中管理，为用户提供统一供给能力。

多级云管理

客户分级建设阿里云专有云，通常分为总部专有云和区域专有云两级，区域专有云自治管理，总部对区域专有云有集中管控能力。

运维人员在总部进行统一运维和多级云的统一管理；云用户将业务部署在不同的专有云上，根据实际需求选择资源归属云平台，满足业务发展。

行业云运营

客户建立自己的云运营平台，通过对运营平台进行个性化配置、流程对接等方式实现向外部客户进行云服务售卖及运营。

云运维管理

在云日常运维、自动化运维、安全运维、远程运维等场景下，实现对云的全方位、多维度运维管理。

8.2. 灾备管理平台ASR

当今社会各行各业信息化程度越来越高，IT基础设施稳定和安全的持续运转对企业发展和生存至关重要。随着国家网络安全等级保护2.0驱动，新基建迅速发展，云灾备已成未来趋势。为保障企业的业务连续性和数据安全，阿里云专有云提供异地容灾、同城容灾、备份等多种容灾解决方案，支持多种模式组合。专有云容灾方案基于阿里云自身的云计算能力设计与开发，遵循国际通用的容灾标准。

灾备管理平台ASR（Apsara Stack Resilience）是阿里云提供的基于图形交互的切换工具，目的是在灾难发生时快速实现容灾切换，尽可能地降低RTO。灾备管理平台提供基于应用系统视角的全场景一键式容灾管理，是企业业务连续性和数据安全保障的理想选择。

8.2.1. 产品详情

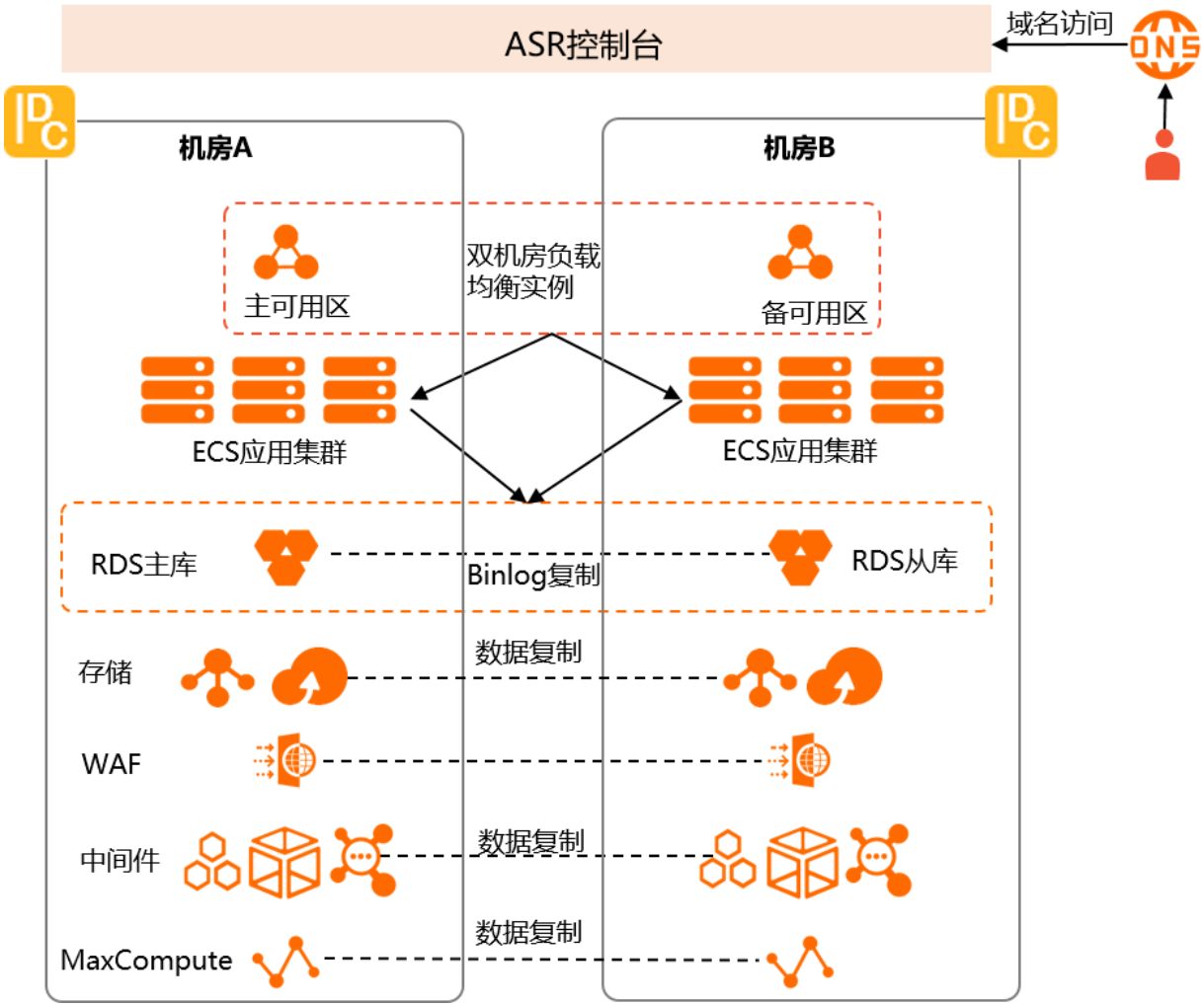
灾备管理平台ASR（Apsara Stack Resilience）是一款专注于全栈云容灾备份与恢复的云平台产品，可用于保障企业的数据安全和业务连续性。ASR提供了同城容灾、异地容灾和备份三种方案，支持多种模式组合，例如同城容灾和异地容灾结合的两地三中心容灾，旨在多场景下快速实现容灾切换和备份恢复。

同城容灾

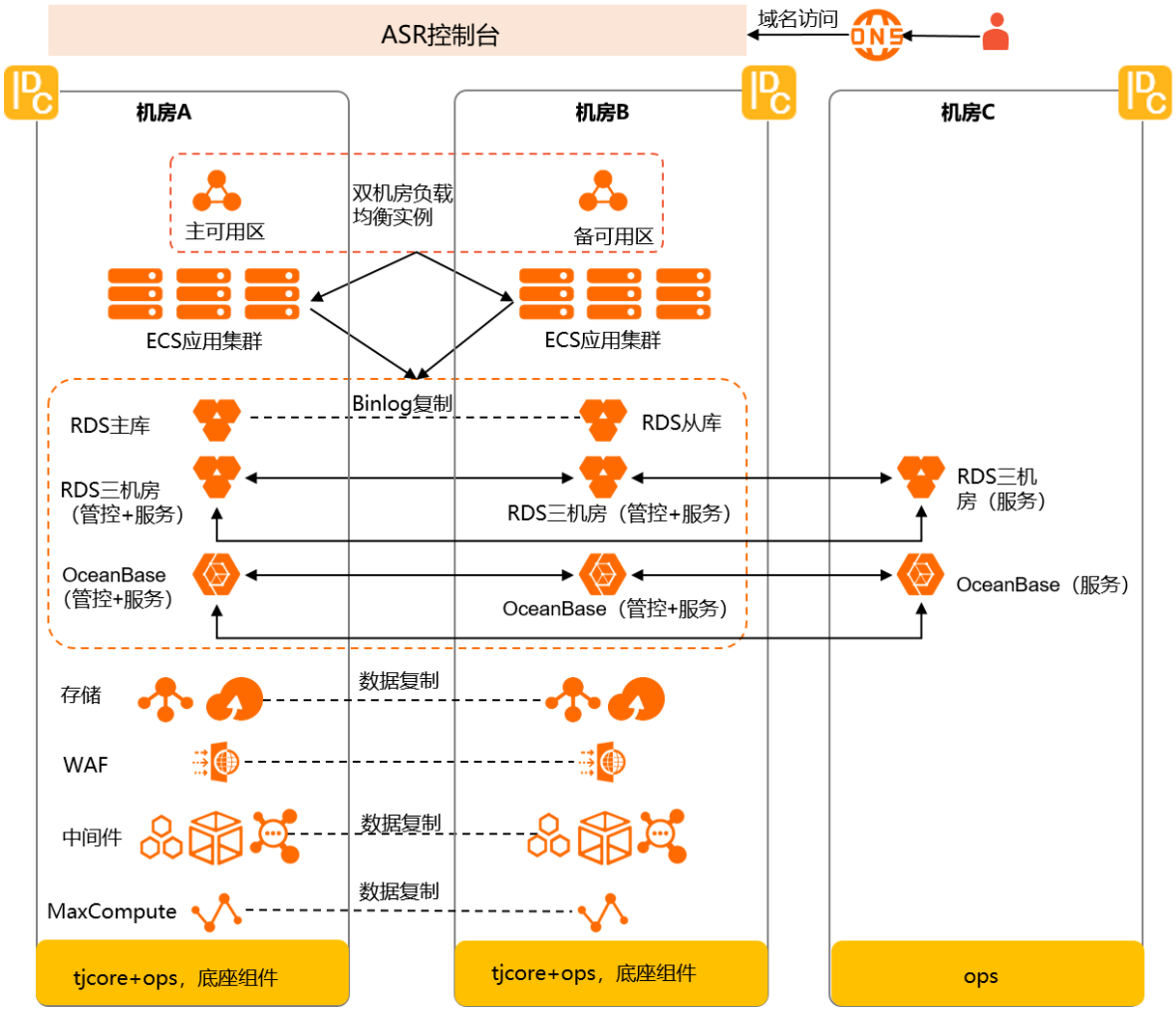
同城容灾是指在与生产中心同一城市不同地点设立同城灾备中心，应对影响范围较小的局部灾难。同城容灾架构全面覆盖核心云产品，包括网络产品、云计算产品、数据库产品、存储产品、中间件产品和大数据计算产品，实现跨可用区（AZ）高可用。在灾难发生时可以快速切换至备AZ，云产品对应用服务域名不变。

专有云同城容灾提供同城双机房和同城三机房等部署方案。在同城容灾双机房基础上，增加部署第三机房，数据库分布式部署。

同城容灾双机房架构图：


ASR控制台
域名访问
DNS
机房A
机房B
主可用区
双机房负载
均衡实例
备可用区
ECS应用集群
ECS应用集群
RDS主库
Binlog复制
RDS从库
存储
数据复制
WAF
中间件
数据复制
MaxCompute
数据复制

同城容灾三机房架构图：



同城容灾管理平台ASR的主要功能包括监控、演练、机房级故障恢复和单产品故障恢复。

- 云产品监控：定时检查云产品机房间同步状态、各机房业务状态和同步延迟时间，并通过容灾大屏实时监控双机房容灾情况。
- 容灾演练：提供可自定义的云产品热切换功能，满足用户例行的容灾演练需求。
- 机房级故障恢复：处理机房级故障，包括主机房断电、备机房断电、主机房网络孤岛、备机房网络孤岛以及脑裂。
- 单产品故障恢复：在云产品高可靠功能异常时，为云产品服务提供双重保证，帮助云产品故障恢复，保证云产品业务连续性。

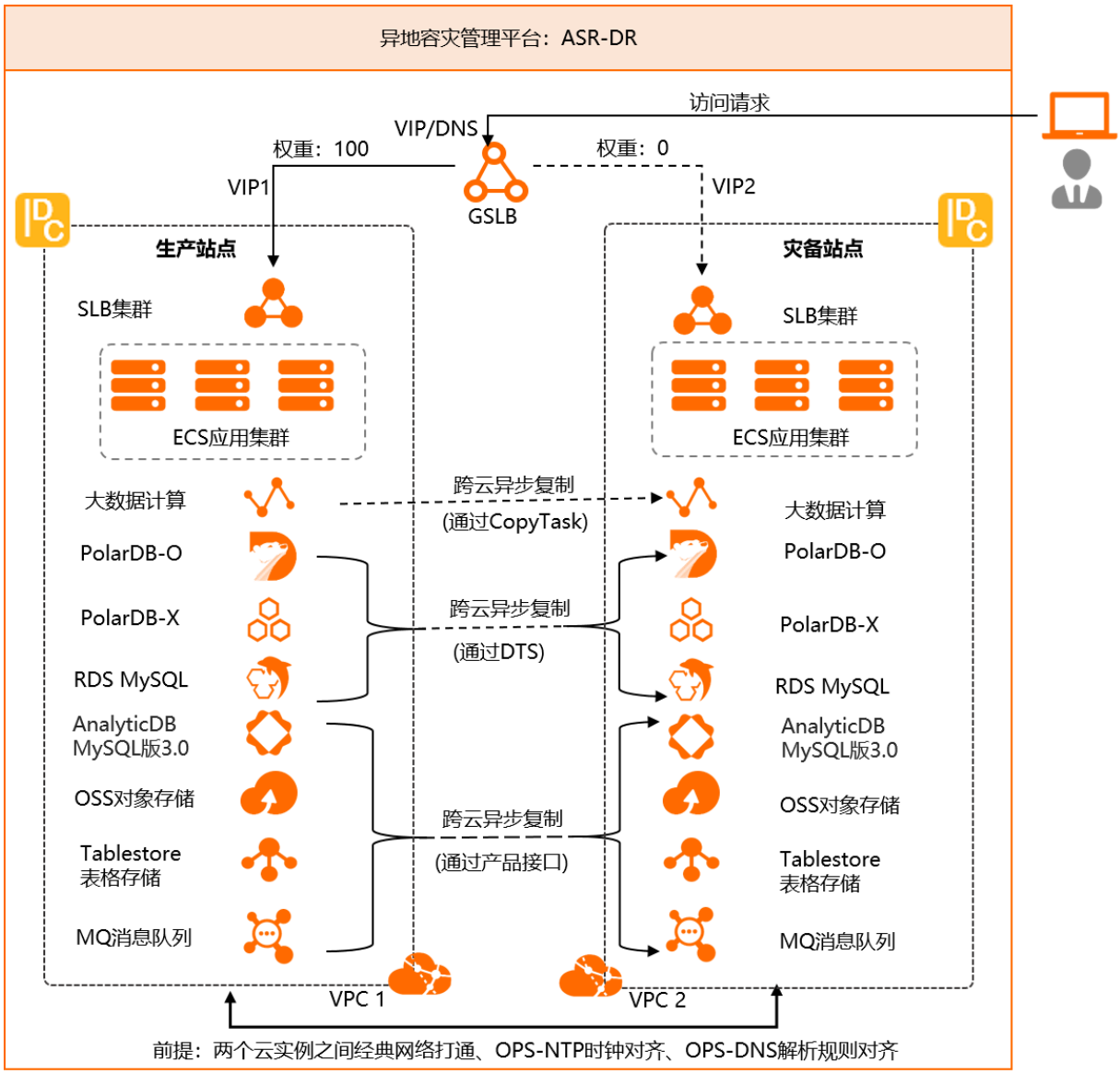
相比于其他方案，同城容灾的优势如下：

- 面向云原生应用，业务无需改造上云即支持容灾，应用接入同城容灾成本低。
- 全栈容灾，提供云平台管控、云产品、云管一体化容灾架构设计。
- 同城三机房支持部分云产品（RDS MySQL、OceanBase、PolarDB-X 2.0、Elasticsearch）同步延迟为0，满足金融云行业业务数据强一致需求。

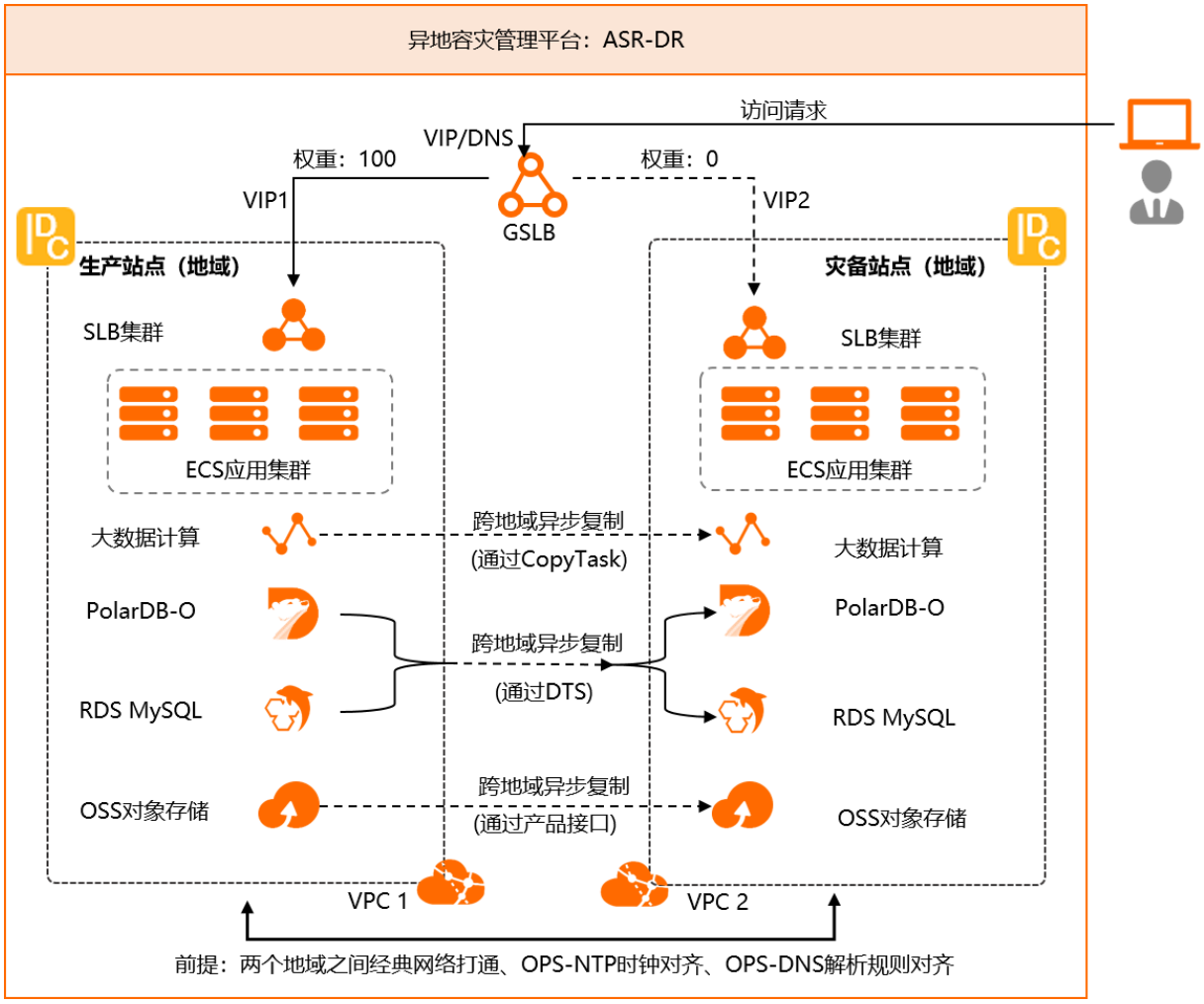
异地容灾

异地容灾是指在距离生产中心所在城市一定距离的另一城市设立灾备中心，应对生产中心可能发生的灾难。通过创建保护组，在生产站点和灾备站点对应资源之间建立一条热备通道，生产站点资源的数据修改会原封不动地异步热备到灾备站点对应的资源之中。生产站点发生故障时，通过故障计划中的故障切换将应用或服务切换到灾备站点上；生产站点故障恢复后，再通过故障计划中的故障回切将业务切换回生产站点，以此来实现业务的连续性。异地容灾的容灾形态包括跨云容灾和跨Region容灾，两种形态的容灾架构如下。

跨云容灾架构图：



跨Region容灾架构图：



异地容灾管理平台ASR-DR的主要功能包括容灾演练、系统管理和容灾大屏。

- 容灾演练：包括业务容灾和站点容灾，可以设置保护组、演练计划和故障计划，并对某一类型的计划进行关联，并按执行序号批量启动所关联的容灾计划，包括演练切换、演练回切、故障切换、故障回切。
- 系统管理：包括用户管理、生产云实例配置、灾备云实例配置、日志管理、容量管理、自身容灾和历史消息。
- 容灾大屏：显示演练计划和故障计划的RTO时长和同步延迟满足度等指标，并以不同的时间粒度显示过去某一段时间内演练计划和故障计划的成功数和失败数、容灾切换和回切过程的整体进度。

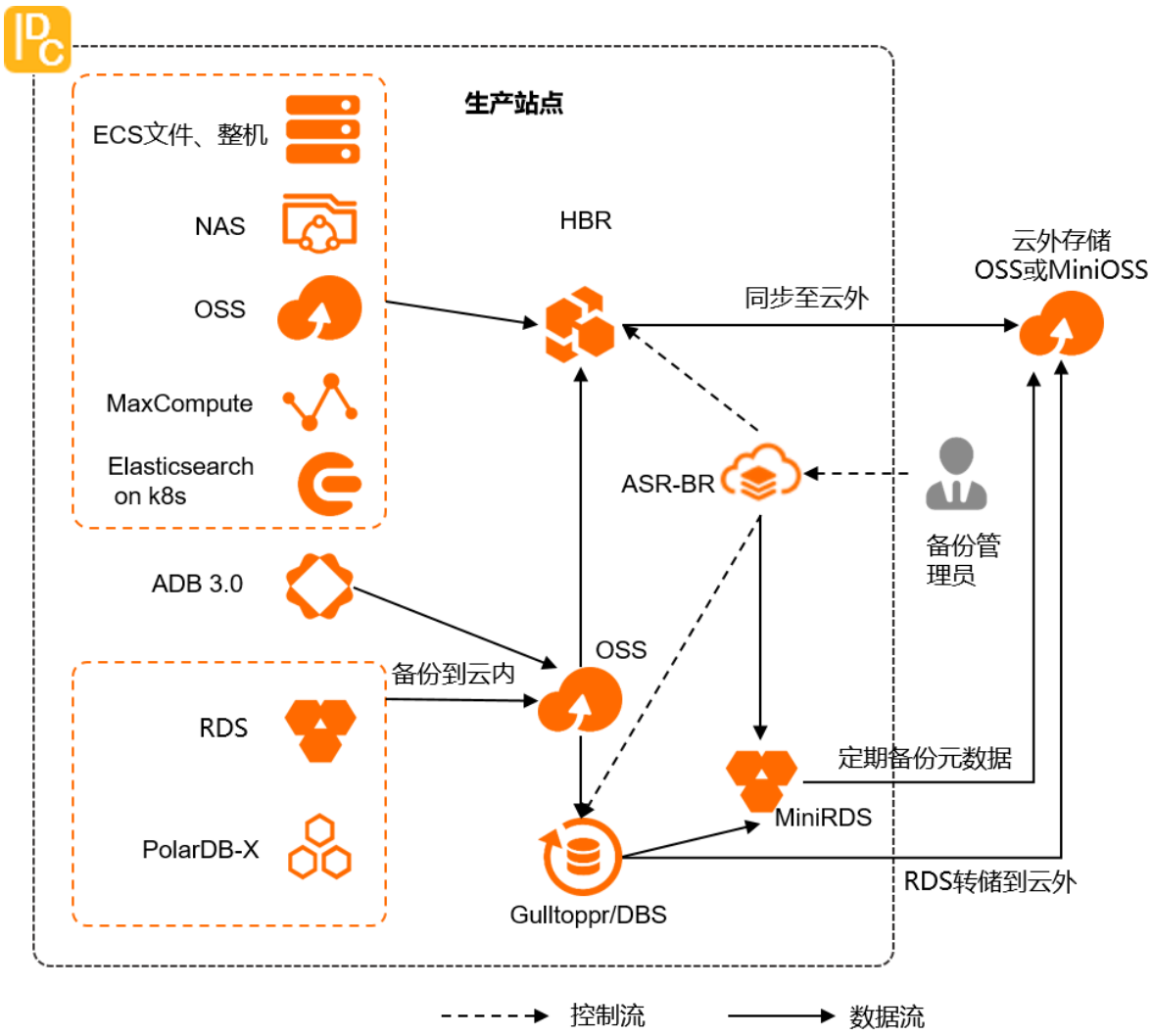
作为基于应用维度的保护组容灾服务，异地容灾的优势如下所示：

- 支持多种容灾场景，包括多对一容灾、主备互为容灾和多Reigon下跨Region容灾等。
- 提供直观的业务视角容灾，支持保护组容灾演练、保护组容灾切换、反向保护能力等。
- 单业务故障，不需要整云切换。

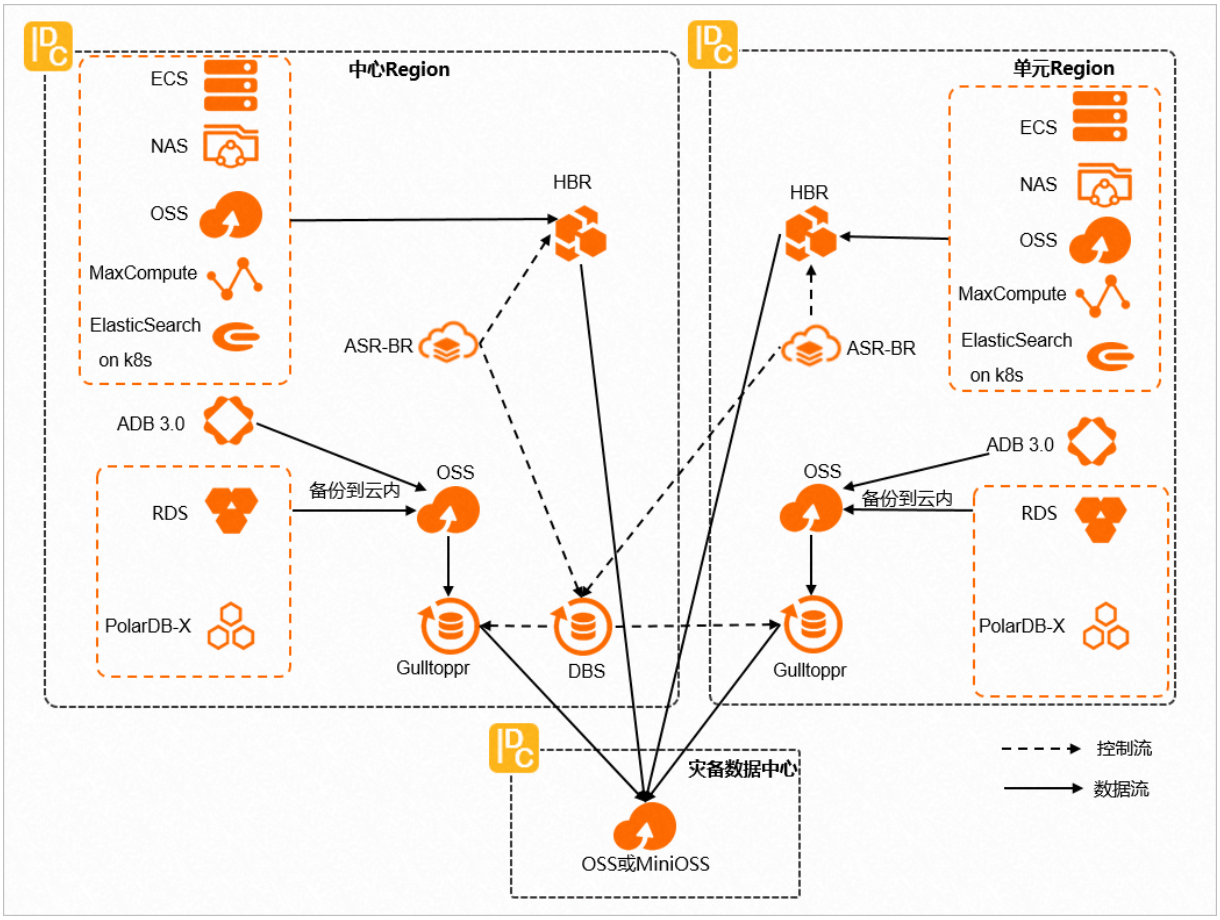
备份

通过建立一个或多个备份的灾备站点，用于生产中心的数据备份。备份管理平台ASR-BR具有云平台深度集成的云原生备份能力，是等级保护项目的必备产品。基于统一的备份管理平台，ASR-BR支持虚拟机备份（含云盘）、存储备份（不含云盘）、VMware备份恢复、数据库备份、大数据备份和云平台元数据本地备份，当前支持的产品包括：云数据库RDS、对象存储OSS、云服务器ECS（文件和整机）、文件存储NAS、云原生分布式数据库PolarDB-X 1.0、VMware虚拟机、大数据计算MaxCompute、云原生数据仓库AnalyticDB MySQL版3.0和Elasticsearch。

备份架构图（单Region场景）：



备份架构图（多Region场景）：



备份管理平台ASR-BR的主要功能包括备份、迁移和恢复。

- 备份：支持跨地域备份和本地备份，支持创建数据库类备份仓库、存储类备份仓库和重删存储类备份仓库，所有备份仓库均使用OSS存储。
- 恢复：包括常规恢复、云重建恢复、VMware云上恢复和VMware本地恢复。
- 迁移：通过迁移计划，支持将本地VMware迁移至专有云ECS。

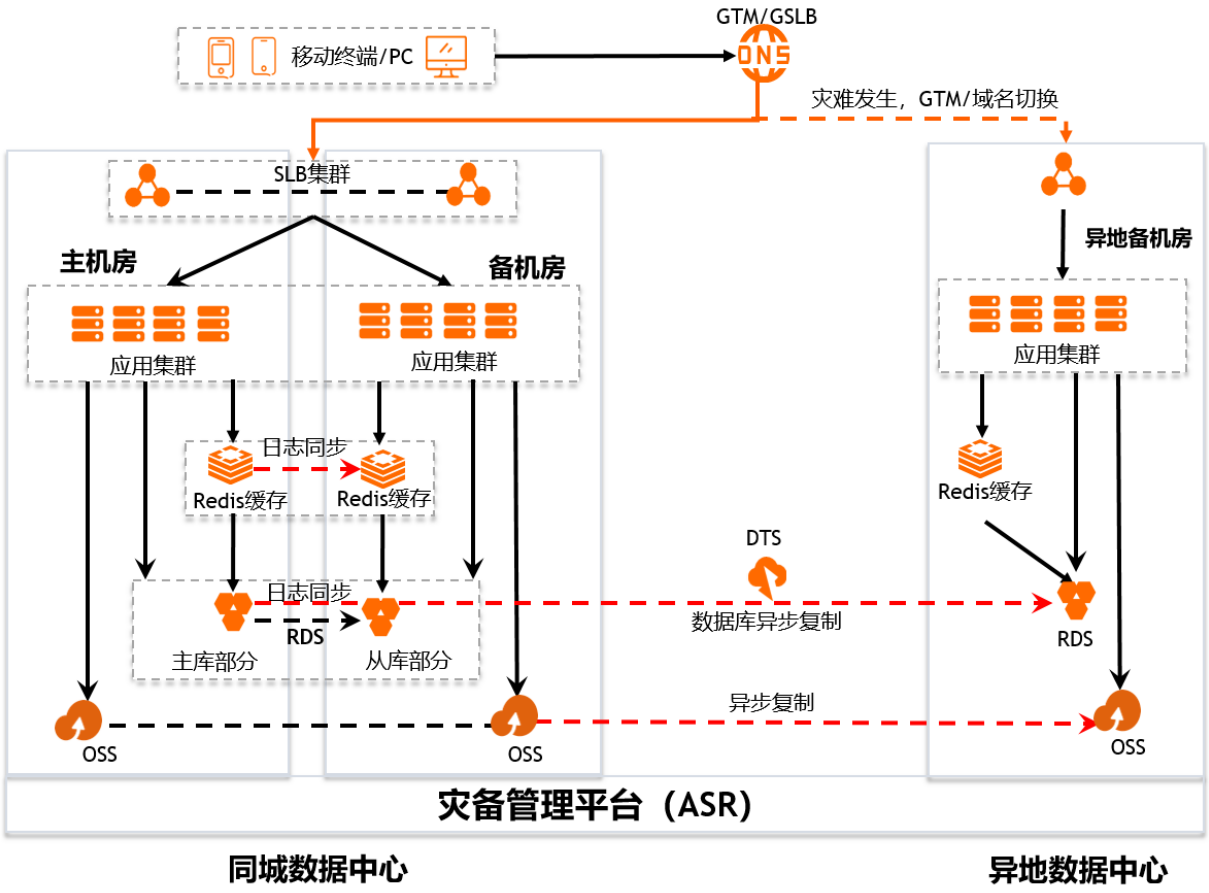
依托云平台深度集成的云原生备份能力，备份的优势如下所示：

- 提供统一的备份管理平台，支持数据库、存储、大数据计算服务MaxCompute备份。
- 数据库备份采用物理备份，备份时间短，不影响生产实例的性能。

两地三中心容灾

两地三中心容灾是指“同城容灾” 加 “异地容灾”的解决方案，该方案旨在防范出现城市级大范围自然灾害，具备区域性故障防范能力。两地指同城和异地，三中心指是指生产中心、同城容灾中心和异地容灾中心。在这种组合中，同城容灾两中心提供双活业务，数据采用同步复制。异地之间采用业务主备模式，数据采用异步复制。该方案业务侵入少，建设速度较快，能够提供金融级的可靠性和全栈产品统一容灾管理。

两地三中心容灾架构图：



与传统容灾相比，两地三中心容灾有如下的优势：

- 结合同城和异地容灾，实现更优的RPO和RTO。
- 可以应对城市级故障，满足对业务连续性要求较高的行业客户。

8.2.2. 产品价值

相较于只提供云主机的原生灾备服务，灾备管理平台ASR提供全场景灾备，包括异地容灾、同城容灾、备份等多种容灾解决方案，支持多种模式组合，是企业业务连续性和数据安全保障的理想选择。

同城容灾

- **根据应用特点提供不同的容灾方案**

  用户可根据应用特点选择合适上云容灾方案，云原生应用业务无需改造上云即支持容灾，应用接入同城容灾成本低，可覆盖所有分布式应用；传统应用架构可通过创建容灾保护组上云，业务无需改造。

- **数据强一致性**

  同城三机房支持部分云产品（RDS MySQL、OceanBase、Elasticsearch）实现同步延迟为0。

- **全栈容灾**

  同城容灾方案包括云平台底座、云产品、统一云管平台等全栈容灾设计，可以实现跨AZ高可用，灾难时可以快速切换至备AZ，云产品对应用服务域名不变。

- **全容灾场景**

  同城容灾方案覆盖全容灾场景，不仅可以为用户提供自定义的云产品热切换功能，满足用户例行的容灾演练需求，还可以进行机房级故障恢复和单产品故障恢复。

异地容灾

- **直观的业务视角**

  异地容灾方案提供基于业务为粒度的保护组容灾，支持直观可视的保护组容灾演练、保护组一键容灾切换、反向保护能力等。单业务故障时，不需要整云切换。

- **丰富的容灾场景**

  支持多对一容灾、主备互为容灾和跨Region容灾。

- **高效的容灾演练**

  灵活制定容灾演练计划，支持自定义云产品切换策略。演练计划流程化执行，无需手工编写演练脚本，演练效果直观可视。

- **可控的容灾管理**

  支持多租户，容灾资源按组织隔离，保障数据安全。各业务可独立切换，避免相互干扰。

备份

- **支持多产品备份**

  依托云平台深度集成的云原生备份能力，备份支持云数据库RDS、对象存储OSS、云服务器ECS（文件和整机）、文件存储NAS、云原生分布式数据库PolarDB-X 1.0、VMware虚拟机、大数据计算MaxCompute、云原生数据仓库AnalyticDB MySQL版（3.0）和Elasticsearch on k8s。

- **数据库产品备份效率高**

  采用物理备份，备份时间更短，无需担心数据库备份时间窗不足。

- **备份场景丰富**

  基于租户视角创建备份计划，支持云产品业务数据的周期性备份、手动备份、常规恢复与云重建恢复。

- **自动化安装和并网**

  通过安全Tunnel机制实现VPC和存储网络单向自动打通；通过云助手一键安装代理插件，无需手动安装。

- **安全性高**

  云平台集成的管理页面保证云账号权限体系一致，并且集成云安全管控机制，更加安全。

8.2.3. 应用场景

容灾方案由多种因素共同决定，主要包括投入的成本、可接受的RTO和RPO、灾难类型。不同的容灾方案对应的应用场景如下所示。

容灾方案	适用场景	典型行业
同城双机房	• 业务连续性要求高。 • 不依赖数据强一致。 • 双机房具有独立的供电、独立的网络，光纤距离不超50公里。	金融、医保、政务、能源、交通等行业。

同城三机房	• 业务连续性要求高。 • 要求数据强一致，保证同城同步延迟为0。 **说明** 支持同城三机房容灾的云产品：云数据库RDS MySQL版、云数据库OceanBase、搜索服务管控Elasticsearch。 • 三机房具有独立的供电、独立的网络，光纤距离不超50公里。	金融行业。
异地主备容灾	• 业务连续性要求较高。 • 不依赖数据强一致。 • 要求具备区域性故障防范能力。 • 城市相距百公里以上。	政务、能源、交通、医保等行业。
备份	• 保证核心业务数据的安全性。 • 虚拟机备份（含云盘）、存储备份（不含云盘）、Vmware备份恢复、数据库备份、大数据备份和云平台元数据备份有上云需求。 **说明** 当前支持的产品包括：云数据库RDS、对象存储OSS、云服务器ECS（整机、文件）、文件存储NAS、云原生分布式数据库PolarDB-X 1.0、VMware、大数据计算MaxCompute、云原生数据仓库AnalyticDB MySQL版（3.0）和Elasticsearch on k8s。	全部行业，特别是有等级保护要求的行业。
两地三中心	• 需要防范城市级大范围自然灾害。 • 具备区域性故障防范能力。 • 要求关键业务数据同步延迟约等于0。 • 预算充足。	金融行业。

8.3. 一站迁云服务中心

一站迁云服务中心面向客户不同上云策略需求，基于大量云迁移实践，向用户提供系统上云或跨云迁移过程支持。

一站迁云服务中心提供一整套帮助客户将业务系统迁移到阿里云专有云平台的工具。尤其是对建云过程中的网络规划和应用跨CPU芯片平台的迁云场景，客户使用一站迁云服务中心可以大幅降低迁云的成本、减少迁云的复杂度、提升迁云的效率。一站迁云服务中心全面评估应用上云的可行性、成本和效率，内置网络评估、服务器迁移、数据库替换评估、跨平台应用迁移和存储数据迁移等工具，确保可靠、快速上云。

8.3.1. 产品详情

一站迁云服务中心提供功能更丰富、传输性能更强、易用性更高且安全可靠的服务，帮助用户简化复杂的数据交互工作。

> **重要**
>
> 使用新版云迁移中心、方案中心、云治理中心功能，需要安装v3.17.0r-ascm-smartmigrate-hotfeature-SP001，详情请咨询技术支持人员。

云迁移中心

云迁移中心（Cloud Migration Hub，简称CMH）为广泛用户迁移上云项目提供自动与智能的系统调研、云上规划、迁移管理，简化和加速用户上云过程，辅助用户业务化可视化管理迁移全生命周期。

云迁移中心主要功能包含以下几点：

- 多源调研

  云迁移中心CMH适配多种常见的用户源端IT基础设施，推出了多种源端资源调研方式，覆盖不同的云厂商，不同的本地操作系统。通过自动化调研，帮助客户快速了解源端资源详情和工作负载。

- 拓扑分析

  云迁移中心CMH可以对调研信息进行智能分析，提供多种架构图来展示基础设施的部署位置，应用进程的调用关系，帮助用户直观了解待迁移系统的架构和部署。

- 迁移计划

  云迁移中心CMH支持自定义创建迁移计划，从而配合用户以真实业务维度进行迁移。通过选择内置的迁移场景，CMH将会把源端产品映射到阿里云，推荐合适的迁移工具、编排合适的迁移顺序，帮助用户端到端完成资源迁移。

- 资源部署

  云迁移中心CMH能够分析源端资源规格，并准确选择阿里云产品的合适规格予以匹配，并且实践基础设施即代码的方法论，自动生成IaC代码，调用自动化平台（Terraform）部署云资源。

- 批量迁移

  云迁移中心CMH支持使用批量助手创建迁移任务，从而减少重复的人工操作。另外，其调度中心的功能可以将迁移任务加入调度组，从而支持分时、分批调度，保障迁移带宽的有效利用，提升整体迁移效率。

- 一站管理

  CMH打通阿里云内部弹性服务器、云数据库、云存储等多款主流产品的迁移工具。用户可以在CMH中划分业务迁移批次，并一站式管理所有迁移任务，包括发起任务，跟踪进展等。

网络迁云中心

网络迁云中心基于阿里云混合云架构规范和大量云架构设计经验，为客户提供云上基础网络架构、云网络产品选型、混合云全连接方案等规划建议。

网络迁云中心主要从以下三个方面提供上云的规划建议：

- 架构：基础网络架构为云平台提供高带宽、低延时、稳定可靠的网络连通能力。
- 产品：云原生虚拟网络产品提供敏捷、弹性、稳定的网络服务。
- 方案：混合云网络解决方案满足业务混合云部署的全场景网络联通需求。

服务器迁移中心

服务器迁移中心支持将单台或多台迁移源迁移至阿里云，迁移源包括服务器、虚拟机、其他云平台的云主机或其他类型的服务器。

- 增量迁移：在业务不暂停的情况下，将源服务器系统产生的增量数据同步至阿里云。
- 批量迁移：API脚本化方式批量创建、执行迁移任务，查询迁移任务进度，批量管理迁移任务。
- 块复制迁移：通过获取迁移源磁盘分区结构，自动生成与迁移源磁盘分区结构一致的目标磁盘。
- 迁移至容器镜像服务：支持将Linux源服务器迁移到容器镜像服务，实现低成本容器化应用迁移。

- 多线程加速传输：多线程传输数据在带宽较大的场景最大化利用带宽资源，有效提升传输效率。
- 集中跟踪迁移进度：展示所有迁移源和迁移任务的状态，帮助用户迅速了解整体迁移进度，快速识别并排查迁移中出现的问题。

跨平台代码扫描

跨平台代码扫描工具针对不同架构的代码迁移场景提供自动化检查功能，能够大幅降低迁移工作的复杂度，提高迁移效率。

跨平台代码扫描工具致力于解决客户代码兼容性人工排查困难、迁移经验欠缺、反复依赖调试定位等投入工作量大、整体效率低的痛点。通过分析待迁移软件源码文件，提供代码迁移指导报告、可迁移性评估及可视化迁移建议，提升迁移效率。

> **说明**
>
> 跨平台代码扫描工具仅适用于开发和测试环境，目前仅支持x86到ARM芯片迁移场景的扫描与分析。

- 源码扫描功能支持绝大部分主流的开发语言，包括 C/CPP，Java，Python，Go等语言。
- 覆盖主流国产处理器，支持国产ARM处理器（鲲鹏、飞腾系列芯片），申威处理器。
- 支持二进制库文件的依赖分析。
- 部署形式灵活便捷，既支持云上产品化输出，也支持云上云下独立输出，满足存量升级和全新上云场景。
- 充分考虑用户实际使用场景，支持自动扫描。
- 扫描报告包含详细问题描述、代码片段和修改建议，同时为整体迁移工程提供大致的工作量评估参考。

操作系统替换评估

因CentOS社区政策调整，CentOS 7将面临生命周期终止，但仍有大量用户在使用CentOS系统，为满足用户在CentOS退出后对操作系统的诉求，龙蜥社区发布Anolis OS。为帮助CentOS客户平滑迁移至Anolis OS系统，龙蜥社区采用就地迁移策略开发迁移工具，提供自动化迁移流程和迁移评估辅助工具，帮助客户自CentOS迁移至Anolis OS系统。

一站迁云服务中心集成CentOS迁移Anolis OS系统的迁移工具，帮助用户在进行CentOS7到Anolis OS8系统迁移前进行评估，提示可能出现的问题。

JVM参数调优

JVM参数调优工具根据Java版本、供应商、平台和CPU架构等相关信息，实现JVM参数的优化、迁移。

JVM参数调优工具从以下四个方面为用户提供JVM参数相关的帮助：

- 参数生成：提供可视化界面，集成常用JVM参数，帮助用户生成准确的JVM参数字符串。
- 参数优化：针对用户的参数列表和环境信息，基于最佳实践提供优化建议。
- 参数迁移：基于用户输入的原始参数列表，针对目标版本和目标环境，基于最佳实践提供修改建议。
- 参数查询：支持查询一到多个JVM参数，展示每个JVM参数的所属模块、参数类别、参数值类型以及描述等信息。

数据库迁移中心

数据库迁移中心提供传统数据库向云上数据迁移的全链路分析和数据导入工具，包括数据库兼容性评估、迁移和性能测试能力。

存储迁移中心

存储迁移中心用简单高效的白屏化操作方式，为客户提供多种异构数据向对象存储OSS迁移的能力，并且拥有数据完整性校验、流量控制、性能优化、结果导出等管理和控制能力。

- 数据迁移：支持云外大规模异构数据通过单机或分布式模式向云内对象存储OSS迁移。

- 任务构建：提供源数据到目的数据节点的任务自动构建、暂停、恢复、删除功能。数据源自动挂载至工作节点，无需人工配置。
- 健康检查：支持工作节点、数据源节点的健康检查，保证成功构建启动迁移任务。
- 数据校验：支持迁移数据的完整性校验。
- 流量控制：支持迁移过程中工作节点的流量控制，合理利用带宽资源。

大数据迁移中心

大数据迁移中心为客户提供大数据计算服务MaxCompute、表格存储等不同类型数据源的大数据迁移功能。

阿里云针对目前主流的各种数据仓库解决方案推出一系列大数据产品，大幅降低架构复杂度和维护难度、缩减成本，解决数据实时性和查询能力受限制的问题，同时具备底层存储赋予的高度扩展性和弹性能力，为客户提供稳定与优良的数据服务。

大数据迁移中心提供从各种开源和其他厂商的大数据服务迁移到阿里云同类型架构产品的能力，整个迁移流程具有数据量大、迁移速度快、性能提升明显的特点，目前支持的数据源类型包括opentsdb、ftp、postgresql、sqlserver、tsdb、odps、hive、hbase11x、ots、cassandra、hbase094x、mysql、drds、hdfs、oceanbase、txtfile、mongodb、phoenix4x、phoenix5x、oracle、rdbms、oss。

方案中心

方案中心采用基础设施即代码（Infrastructure as Code）的设计理念，通过资源模板、Terraform模板和治理规则模板提供了云资源管理和配置能力。

用户可以通过方案中心编写模板的方式，在模板中定义阿里专有云资源（例如组织、用户、资源集、VPC、ECS云服务器、RDS云数据库实例等）、治理规则（检查资源配置、状态、性能、安全合规、标签）等进而为云登陆区自动创建和配置资源以及云治理中心执行资源治理而服务。

方案中心主要支持以下三种功能：

- 支持云资源管理和配置，资源模板支持组织、用户、资源集、VPC、ECS云服务器、RDS云数据库实例等云资源的定义。
- 兼容Terraform模板，方案中心支持terraform模板，登陆区可通过terraform模板创建资源。
- 支持云资源治理，可支持针对ECS、OSS、RDS、SLB、EIP等专有云主流资源超100条典型治理规则检查。

云登陆区

云登陆区服务助力企业设计并部署混合云上云框架，包括经典资源栈、组织&账号访问安全、可扩展网络架构等，为企业上（“登陆”）云搭建安全、高效和可管理的云基础环境。

云登陆区可以在企业的上云过程中，根据企业的上云战略，设计出符合大量最佳实践标准的规则模板包（包含：组织架构规划、网络规划、身份权限等），通过使用这些模板包快速创建云登陆区，来保证企业应用业务上云并运行在一个可扩展、安全合规的云环境，减少整个企业用户整体业务上云的实施时间，同时提高效率。另外，业务在云上正常运营期间，用户在管理和配置资源时需要进行重复且繁琐的大量操作，云登陆区服务可以帮助用户进行资源的快速批量创建和回收，并且持久化整体资源的每次变更记录，以解决常规使用、容灾演练和测试等场景所存在的资源管理效率低下问题。

云登陆区功能特性如下：

- 设计基于组织且符合安全运营体系的账号&权限模板包，创建账号&组织登陆区环境，建设基于组织的多账号管理的云基础环境，实现业务的隔离，降低账号管理复杂度。
- 结合企业的管控策略和实际业务规模，部署可扩展的基本资源栈环境，打造可靠的应用基础底座。
- 可以使用登陆区批量创建资源的模板规则包，快速创建精简配置的各种资源，提高用户创建和管理资源的效率。
- 多环境隔离的资源编排部署，同时可持续追溯登陆区环境资源的变更过程，大幅降低客户上云管云复杂度。

云治理中心

云治理中心利用规范化的最佳实践，通过智能化的治理规则，帮助客户实现专有云高效治理。云治理中心提供多场景的治理能力，通过定义治理规则、执行治理规则集，协助用户对专有云上资源做出持续治理，以优化运营成本，提高资源使用效率，快速响应变化，保证云环境始终运行于最佳状态。

主要功能及支持的场景治理能力包括：

- 配置与状态治理
- 标签治理
- 安全治理
- 性能优化治理

工作集群管理

专有云的客户在迁移上云的过程中，通常都会涉及计算资源迁移（如服务器资源）、存储迁移（如文件、数据库）、大数据迁移（将数据从IDC迁移到混合云的MaxCompute、表格存储等数据存储产品）等迁移场景。这些迁移通常都需要将任务分发到具体工作节点执行，需要用户线下执行创建服务器资源、安装迁移工具、收集迁移任务结果等步骤。这种迁移方法不仅操作复杂对用户非常不友好，并且无法对迁移任务和资源进行统一管理和分配，资源使用率低。

针对上述场景，一站迁云服务中心的工作集群管理提供一站式的高效集群任务管理系统，通过统一管理任务和迁移资源，降低操作复杂度，提高资源使用率。

8.3.2. 产品价值

一站迁云服务中心拥有整合的迁移工具链、独有的网络迁云评估和自动化编排能力、强大的国产操作系统兼容性、完善快速的数据迁云能力四大核心优势。

整合的迁移工具链

一站迁云服务中心为客户提供迁云场景中相关工具集的组合能力，从“网络-计算&应用-数据”三个层面整合整体工具链，提供统一入口。

独有的网络迁云评估和自动化编排能力

一站迁云服务中心具备独有的网络迁云评估和自动化编排能力：

- 网络拓扑迁云评估：通过构建一套day0到day1的网络调研规划工具，支持网络安全分区（VPC划分评估）、多出口网络协议和内部路由协议兼容性评估。
- 负载均衡SLB迁云场景评估：基于客户实际情况提出迁云可行性评估结果，并提供代码转换能力。
- 网络拓扑自动化编排能力：根据应用级虚拟网络拓扑架构，以IaC的方式生成可部署的自动化脚本，一键生成云上资源。

强大的国产操作系统兼容能力

一站迁云服务中心为客户提供覆盖多平台的软件和源码迁移能力：

- 面对CentOS系统即将停止服务场景，提供向Anolis OS系统平滑迁移的能力。Anolis OS系统100%兼容CentOS 7/8，应用程序无需任何改造或仅少量改造即可完成迁移。同时，支持全系列国产硬件，包括且不限于海光、鲲鹏、飞腾、龙芯、申威等芯片，适配、认证主流国产软件。
- 在服务器迁移工具上，大部分厂商都具备物理机到虚拟机（P2V）的迁移能力。阿里云服务器迁移中心SMC在此基础上还支持将物理机一键迁移至云上容器镜像，支持多平台、多场景迁移。
- 提供覆盖多平台软件和源码迁移评估的能力，既支持海光平台、也支持ARM平台；提供跨平台源码扫描（语言、编译器）和跨平台库/软件包扫描的能力。

完善快速的数据迁云能力

一站迁云服务中心提供完善的数据库工具链和存储数据迁移能力，满足结构化、非结构化数据的快速迁云场景：

- 数据库迁移工具ADAM提供数据采集、数据库智能分析、应用评估分析、数据库&应用改造、项目实施的完整工具链。
  - 数据采集：收集用户系统信息、性能、SQL等数据，以及应用收集。
  - 数据库智能分析：对采集到的数据进行智能分析，包含可行性分析、对象兼容性分析等。
  - 应用评估分析：提供应用画像，评估应用改造可能性，梳理数据库&应用联合架构。
  - 数据库&应用智能改造：适用于各类Oracle迁移场景，支持99%以上的数据与应用改造点自动识别、90%以上的改造建议，开箱即用。
  - 项目实施：最终由ADAM和数据传输服务DTS实施数据迁移。
- 非结构化存储数据迁云能力在以下五个方面解决客户问题：
  - 支持小文件合并传输
  - 支持断点续传
  - 海量文件快速比对
  - 支持对象存储OSS迁移到文件存储NAS和文件存储NAS迁移到对象OSS
  - 100TB海量小文件（100K）的传输稳定带宽最高可达500Mbps

8.3.3. 应用场景

一站迁云服务中心为提高用户的迁云效率提供多种针对性功能，大幅降低用户迁移时的风险与工作量，适用于多种迁云上云场景。

- 应用国产芯片适配改造上云
- 云下Oracle数据库迁移云上数据库
- 服务器/虚拟机平迁
- 云下存储迁移到云上对象存储OSS
- 应用迁移上云网络规划
- 云厂商更换迁移上云
- 容灾建站数据迁移
- 企业初始化组织、用户、批量创建云资源
- 云资源规格、安全、标签检查与治理

8.4. 混合云应用中心

混合云应用中心AHM（Apsara Hybrid Marketplace）是在专有云底座Tianji、PaaS平台之外的第三条产品研发交付链路，主要用于支撑第三方ISV或阿里云内部的SaaS类应用产品在专有云场景的部署，使用云平台租户侧资源进行应用交付，旨在拓宽专有云产品生态。

8.4.1. 产品详情

混合云应用中心为客户提供便利快捷的应用交付与部署途径。

应用管理

支持通过导入标准格式的云上产品包新增、更新应用商店中的云上产品应用。应用商店中的应用支持多版本选择，供用户选择指定版本构建应用部署环境；试用体验支持以应用最小化的资源要求，完成环境的交付，满足用户的试用要求。

同时，支持通过OpenAPI接口方式新增、更新应用。

环境管理

- 开通部署：支持应用以标准环境要求、以标准资源完成应用各个组件的资源配置要求和环境部署。
- 变量管理：支持定义环境的全局生效的全局变量、特定集群生效的集群变量；支持部署环境中内部调用数据库的密钥生成。
- 容器资源监控：支持基于Sunfile、Prometheus监控资源数据变化，展示容器资源使用情况。
- 下线部署：支持下线已部署的应用实例，释放资源。

任务管理

支持查看应用部署任务状态、执行进度；任务执行过程中出现执行失败时，支持手动重试或跳过相关步骤。

镜像仓库管理

支持为集群创建Docker镜像仓库，针对不同集群的提供不同镜像服务；部署应用时系统读取镜像仓库的配置，获取镜像来源。

8.4.2. 产品价值

混合云应用中心通过采用采用标准的OAM标准，支持将各类服务和资源整合打包为一个完整的解决方案，一键式将这个完整的解决方案部署到客户专有云环境。

接入标准

通用的OAM应用包格式，简单统一的接入标准，接入商无需关心底座版本。近似K8S风格的OAM格式，是阿里巴巴与微软合作共建的业界标准，不仅便于用户快速熟悉与上手，又具备将多个服务、资源定义组合为一个整体的协议格式；同时它也具备开放扩展的能力，能将专有云的资源能力扩展到其格式描述中，辅以对应的实现，从而完成整体环境的交付。

三方生态

建设完整的三方生态，ISV接入商通过交付控制台构建应用版本，经过测试验收、完整的交付验收，设定相关的售卖机制，实现产品应用的整体生命周期管理。我们将努力打造极简的运维管理体系，让客户或供应商几乎不用感知平台的运维状态

一键交付

一键式产品部署机制，用户需要试用或正式购买应用时，只需一个按钮即可完成产品环境的交付。

极简运维

接入基础监控能力，支持通过自定义策略实现自动化运维；坚持打造极简的运维管理体系，目标让客户和接入商几乎无需感知平台的运维状态。

8.4.3. 应用场景

专有云已在大量企业部署落地，企业客户想更好的用好“这朵云”的诉求也日益增强，期望引入更多优质云上产品（如阿里云及三方ISV的SaaS类产品）来满足其更多的业务诉求，混合云应用中心用于支撑阿里云或三方ISV应用在专有云售卖部署场景，满足客户在专有云环境产品应用的多样性需求。

混合云应用中心主要应用在以下场景中：

- 三方ISV供应商入驻专有云平台，发布各类云上产品、应用
- 解耦底座版本依赖，部署快速迭代的阿里云内部产品、应用
- 需要部署在用户租户侧使用全面专有云产品能力的云上、应用

9.计算服务

9.1. 云服务器

云服务器ECS（Elastic Compute Service）是阿里云提供的性能卓越、稳定可靠、弹性扩展的IaaS（Infrastructure as a Service）级别云计算服务。云服务器ECS，让客户像使用水、电、天然气等公共资源一样便捷、高效地使用服务器，实现计算资源的即开即用和弹性伸缩。

9.1.1. 产品详情

云服务器ECS提供一种处理能力可弹性伸缩的计算服务，它的管理方式比物理服务器更简单高效。根据业务需要，客户可以随时创建实例、扩容云盘或批量删除多台云服务器实例。

云服务器ECS实例（以下简称ECS实例）是一个虚拟的计算环境，包含CPU、内存等基础的计算组件，是云服务器ECS呈献给每个用户的实际操作实体。ECS实例是云服务器最为核心的概念，用户可以通过ECS管理控制台完成对ECS实例的一系列操作。其他资源，包括块存储、镜像、快照等，都需要与ECS实例结合后才能使用。

实例

实例是云服务器ECS为客户业务提供计算服务的最小单位，不同的实例规格提供的计算、网络与存储能力不同。一台ECS实例等同于一台虚拟服务器，包含CPU、内存、操作系统、网络配置、云盘等基础的组件。用户可以使用阿里云提供的控制台、API等管理工具创建和管理ECS实例，像使用本地服务器一样管理ECS实例的状态、应用等，还可以灵活地升级计算、网络、存储等资源规格。

根据业务场景和使用场景，云服务器ECS提供共享型、独享型、本地HDD盘型、本地SSD盘型、异构计算型等多种实例规格族。规格族是一个或多个具有相似属性的实例规格的组合。除此之外，云服务器ECS还提供弹性裸金属、超级计算集群等基于阿里云完全自主研发的下一代虚拟化技术而打造的新型计算类服务器实例。

- **弹性裸金属服务器**

  弹性裸金属服务器是从云计算角度设计的一款服务器，是基于阿里云完全自主研发的新一代软硬一体化、虚拟化技术架构（神龙架构）而打造的创新型计算产品，融合物理机和虚拟机特性，兼具虚拟机的弹性资源、分钟级交付、全自动运维和物理机的性能无损、完整特性、硬件级强隔离，并兼容阿里云生态产品，充分满足企业关键应用、高负载应用的上云要求，实现上云无障碍的目标。

- **超级计算集群**

  超级计算集群在弹性裸金属服务器的基础上，通过使用节点间的高速InfiniBand网络互联的CPU以及异构计算设备（如GPU）提供具有计算性能和并行效率的计算集群服务，适合搭建高性能计算、人工智能、机器学习、科学计算、工程计算、数据分析、音视频处理等应用。

块存储

块存储是阿里云为云服务器ECS提供的低时延、持久性、高可靠的数据块级随机存储。块存储具有丰富的产品类型，包括基于分布式存储架构的弹性块存储产品，以及基于物理机本地硬盘的本地存储产品。

- **弹性块存储**

  弹性块存储也称为云盘，为ECS实例提供数据块级别的随机存储，具有低时延、持久性、高可靠等特点，采用三副本的分布式机制，为ECS实例提供数据可靠性保证。可以随时创建或释放，也可以随时扩容。

- **本地存储**

  本地存储也称为本地盘，是指挂载在ECS实例所在物理机（宿主机）上的本地硬盘，是一种临时块存储。本地存储是专为对存储I/O性能拥有极高要求的业务场景而设计的存储产品。本地存储可以为实例提供块级别的数据访问能力，具有低时延、高随机IOPS、高吞吐量的I/O能力。

- **云盘扩容**

  随着业务发展和应用数据增长，用户可以选择多种方式来扩展云盘容量。支持扩容系统盘和数据盘，支持在线扩容和离线扩容，离线扩容必须重启ECS实例。

- **云盘加密**

  云盘提供一种简单安全的加密手段，支持对新创建的云盘进行加密处理。用户无需构建、维护和保护自己的密钥管理基础设施，无需更改任何已有的应用程序和运维流程，也无需执行额外的加密操作，且云盘加密功能不影响业务。

  云盘加密功能支持加密以下类型的数据：

  - 云盘中的数据
  - 云盘和实例间传输的数据（实例操作系统内数据不再加密）
  - 通过云盘创建的所有快照（加密快照）

镜像

镜像（Image）是ECS实例运行环境的模板，模板中包括特定的操作系统信息，也可通过自定义镜像的方式使系统镜像预装所需的应用程序。

镜像文件相当于副本文件，该副本文件包含了一个或多个云盘中的所有数据。对于云服务器ECS而言，这些云盘可以是单个系统盘，也可以是系统盘与数据盘的组合。用户可以使用镜像创建新的ECS实例或更换ECS实例的系统盘。

快照

快照是某一个时间点上某一块云盘的数据拷贝。快照功能通常应用于环境复制、容灾备份等场景。

- **场景示例**
  - 环境复制

    在云盘上进行数据的写入和存储时，用户可以通过为云盘创建快照，然后使用快照创建云盘，实现将某块云盘上的数据作为其他云盘的基础数据。

  - 容灾备份

    云盘本身提供安全的存储方式确保不丢失存储的数据。在云盘上的数据本身就是错误的情况下（例如由于应用错误导致的数据错误，或者黑客利用应用的漏洞进行恶意读写），如果用户定期创建快照，则当数据出现问题时，可以通过快照恢复到期望的数据状态。

- **快照一致性组**

  通过创建快照一致性组，用户可以为一台ECS实例中的多块云盘同时创建快照。快照一致性组能够保证在业务系统跨多块云盘的场景下，数据写入云盘的时序一致性，并保证其崩溃一致性。

  - 快照一致性组支持同时为一台ECS实例中的多块云盘创建快照。
  - 快照一致性组可应用于集群业务。
  - 创建快照一致性组后，如果产生系统故障或因误操作造成数据异常时，您可以通过快照一致性组回滚一个或多个云盘。

- **自动创建快照策略**

  自动快照策略适用于系统盘和数据盘，可以周期性地为磁盘创建快照。合理利用自动快照策略能提高数据安全和操作容错率。同时，自动快照策略可以有效避免手动创建快照存在的风险。

部署集

部署集（Deployment Set）是云服务器ECS提供的一种让客户直观感知宿主机、机架、交换机物理拓扑的能力，并且支持根据客户业务类型自行选择符合业务要求的部署策略，提升业务整体可靠性和性能。

当客户在同一可用区中使用多台ECS实例时，可以通过部署集功能提高业务可靠性或业务性能：

- 提升业务可靠性

  为了避免物理宿主机、机架或交换机发生故障时对业务造成较大的影响，通过部署集的部署策略实现相同的应用实例尽量不分布在同一台物理宿主机、机架或交换机上。

- 提升业务网络性能

在某些ECS实例间存在较多网络交互的业务场景中，通过部署集的部署策略将ECS实例尽可能集合到同一交换机下，以减少网络延时和保障网络带宽。

网络

- **专有网络**

  基于阿里云创建的自定义私有网络，不同专有网络之间通过隧道在逻辑上彻底隔离。用户可以在自己创建的专有网络内创建和管理云产品实例，比如云服务器ECS、云数据库RDS等。

  根据所属的专有网络和交换机网段，ECS实例一经创建即被分配一个私有IP地址，即内网IP。

- **弹性公网IP**

  弹性公网IP（Elastic IP Address，简称EIP）是可以独立申请持有的公网IP地址资源。将EIP绑定到专有网络中的ECS实例上，实例即可通过EIP与公网通信。EIP支持实例绑定、解绑，也可以单独删除或修改其公网带宽。

- **弹性网卡**

  弹性网卡（Elastic Network Interface，简称ENI）是一种可以附加到ECS实例上的虚拟网卡。通过弹性网卡，客户可以实现高可用集群搭建、低成本故障转移和精细化的网络管理。

安全组

安全组是一种虚拟防火墙，用于控制安全组内ECS实例的入流量和出流量，从而提高ECS实例的安全性。安全组用于状态检测和数据包过滤，用户可以基于安全组的特性和安全组规则的配置在云端划分安全域。

- 用户可以根据业务需求，自定义添加、修改安全组规则更精细地控制出入流量。安全组规则用于IP地址、CIDR地址块、其他安全组、前缀列表。
- 安全组规则新增或修改后，会自动应用于安全组内所有实例。
- 如果一台实例加入了多个安全组，则所有安全组的安全组规则均应用于该实例。在检测到访问请求时，系统会逐一检查适用于实例的安全组规则，根据安全组规则的协议、端口、优先级等属性进行判断，匹配到允许访问的安全组规则时才会建立会话。

标签

标签用于标记资源，由一对键值（Key-Value）组成。用户可以通过标签将相同作用的云服务器ECS资源归类，便于搜索和资源聚合。随着ECS实例的增多，利用标签将资源进行分组管理和归类更有利于搜索和批量操作（如更换镜像部署应用、升级补丁、添加安全组规则控制网络访问等批量操作）。

专有宿主机

专有宿主机（Dedicated Host，简称DDH）是阿里云专为企业客户定制优化的云端解决方案，具有物理资源独享、部署更灵活、配置更丰富、性价比更高等特点。

专有宿主机是由一个租户独享物理资源的云主机。作为该云主机的唯一租户，用户无需与其他租户共享云主机任何物理资源。用户还可以获得该物理服务器的CPU数量（Socket数）、物理CPU核数、内存大小等物理属性信息，并根据宿主机规格创建指定规格族的ECS实例。

云助手

云助手是专为云服务器ECS打造的原生自动化运维工具，通过免密码、免登录、无需使用跳板机的形式，在ECS实例上实现批量运维、执行命令（Shell、PowerShell和Bat）和发送文件等操作。

典型的使用场景包括：安装卸载软件、启动或停止服务、分发配置文件和执行一般的命令（或脚本）等。

密钥对

密钥对是一种安全便捷的登录认证方式，由公钥和私钥组成，仅支持Linux实例。

密钥对通过加密算法生成一对密钥，默认采用RSA 2048位的加密方式。如果用户需要使用密钥对登录Linux实例，必须先创建一个密钥对，并在创建实例时指定密钥对或者创建实例后绑定密钥对，然后使用私钥连接实例。

9.1.2. 产品价值

与普通的IDC机房或传统服务器相比，云服务器ECS具有高可用性、安全、弹性、易用等优势。

高可用性

相较于传统的服务器受限于硬件本身，云服务器ECS能够提供更高的运维标准，同时能够结合多种云服务功能，带来更高效的备份、容灾以及故障恢复的能力。

此外，还提供了如下支持：

- 行业合作伙伴以及生态合作伙伴，帮助客户完成更高、更稳定的架构。
- 多种多样的培训服务，让客户从业务端到底层的基础服务端，在整条链路上实现高可用。

安全性

选择了云计算，最关心的问题就是云计算的安全与稳定。阿里云已通过多个国际安全标准认证，包括ISO27001、MTCS Level-3等。这些安全合规对于客户数据的私密性、客户信息的私密性以及客户隐私的保护都有非常严格的要求。

- **在专有网络之上，可以产生更多的业务可能性。** 用户只需进行简单配置，就可提高业务的灵活性、稳定性以及业务的可发展性。
- **对于原来拥有自建的IDC机房，也不会产生问题。** 阿里云专有网络可以拉专线到原有的IDC机房，形成混合云的架构。阿里云可以提供各种混合云的解决方案和非常多的网络产品，形成强大的网络功能，让客户的业务更加灵活。
- **专有网络更加稳定和安全。**
  - 专有网络允许用户自由地分割、配置和管理自己的网络。
  - 面对互联网上不断的攻击流量，专有网络天然就具备流量隔离以及攻击隔离的功能。业务搭建在专有网络上后，专有网络会为业务筑起第一道防线。
- **全面的安全防护能力。** 为云服务器提供全方位的安全防护能力，包括安全策略、主机加固、数据安全、监控告警等方面，提高客户业务的安全性，有效抵御外部的攻击和非法侵入。

总之，专有网络提供了稳定、安全、快速交付、自主可控的网络环境。对于传统行业以及未接触到云计算的行业和企业而言，借助专有网络混合云的能力和混合云的架构，它们将享受云计算所带来的技术红利。

弹性

云计算最大的优势就在于弹性。

- **计算弹性**
  - **纵向的弹性，即单个服务器的配置变更。**

    在传统IDC模式下，客户很难做到对单个服务器进行变更配置。而对于阿里云，客户可以根据业务量的增长或者减少自由变更云服务器的配置。
  - **横向的弹性**

    对于游戏应用或直播平台出现的高峰期的情况，若在传统的IDC模式下，用户无法随时准备资源进行扩容。而在云计算模式下，客户可以使用弹性的方式度过这样的高峰；当业务高峰消失时，客户可以将多余的资源释放掉，以减少业务成本。

    利用横向的扩展和缩减，配合弹性伸缩，完全可以做到定时定量的伸缩，或者按照业务的负载进行伸缩。
- **存储弹性**

  阿里云拥有很强的存储弹性。当需要扩容存储时，在传统的IDC模式下，客户只需增加服务器配置或更换服务器；在云计算模式下，客户可以按需扩容已挂载云盘的容量或者新增数据云盘。
- **网络弹性**

云上的网络也具有非常大的灵活性。只要客户选择了阿里云的专有网络，那么所有的网络配置与线下IDC机房配置可以是完全相同的，并且可以拥有更多的可能性。可以实现各个机房之间的互联互通，各个机房之间的安全域隔离，对于专有网络内所有的网络配置和规划都会非常灵活。

总之，对于阿里云的弹性而言，是计算的弹性、存储的弹性、网络的弹性以及客户对于业务架构重新规划的弹性。客户可以使用任意方式去组合自己的业务。

易用性

简单易用的统一管理、控制界面，可以提供弹性计算实例及相关服务全流程的自动化开通、变更等能力，包括：

- 丰富的产品类别，如独享型、共享型、弹性裸金属等。
- 基于业务视角，提供基于租户不同业务，不同组织的VPC划分。
- 不同存储类型，供租户灵活选用。
- 简单易用的安全组策略部署。

此外，在产品易用性方面还提供镜像服务、集群部署、自定义标签、虚机迁移、配置变更等功能。

9.1.3. 应用场景

ECS实例应用非常广泛，既可以作为简单的Web服务器单独使用，也可以与其他阿里云产品（例如对象存储OSS、负载均衡等）搭配提供强大的多媒体解决方案。

企业官网、简单的Web应用

网站初始阶段访问量小，只需要一台低配置的云服务器ECS实例即可运行应用程序、数据库、存储文件等。随着网站发展，客户可以随时提高ECS实例的配置，增加ECS实例的数量，无需担心低配服务器在业务突增时带来的资源不足问题。

多媒体、大流量的App或网站

云服务器ECS实例与对象存储OSS搭配，将OSS作为静态图片、视频、下载包的存储空间，以降低存储费用，同时配合负载均衡 ，可大幅减少用户访问等待时间、降低带宽费用、提高可用性。

访问量波动大的App或网站

对于访问量可能在短时间内产生巨大波动的业务，通过使用弹性伸缩，实现在业务增长时自动增加ECS实例，并在业务下降时自动减少ECS实例，保证满足访问量达到峰值时对资源的要求，同时降低了成本。如果搭配负载均衡，则可以实现高可用架构。

I/O要求较高的数据库服务

使用较高配置的I/O优化型ECS实例，同时采用SSD云盘，可实现支持高 I/O 并发和更高的数据可靠性。也可以采用多台稍微低配的I/O优化型ECS实例，搭配负载均衡，实现高可用架构。

9.2. 弹性伸缩

弹性伸缩（Auto Scaling）是根据业务需求和策略自动调整计算能力（即实例数量）的服务。用户可以指定实例类型（即ECS实例或ECI实例），业务需求增长时，自动增加指定类型实例来保证计算能力；业务需求下降时，自动减少指定类型实例来节约成本。

弹性伸缩本身不收取任何费用，具有自动化、降成本、高可用、灵活智能以及易审计等优势，能够帮助用户自动调整指定类型的实例数量，适用于业务量不断波动的应用程序和业务量稳定的应用程序。

9.2.1. 产品详情

弹性伸缩（Auto Scaling）是根据企业的业务需求和策略，自动调整其弹性计算资源大小的管理服务。

弹性伸缩将根据企业的业务配置，自动弹性伸缩所需ECS实例或ECI实例的数量。在业务需求增长时，自动增加ECS实例或ECI实例以保证计算能力；在业务需求下降时，自动减少ECS实例或ECI实例以节约成本。

弹性伸缩主要提供弹性扩张、弹性伸缩以及弹性自愈三个功能，具体说明如下所示：

功能类型	说明
弹性扩张	当企业的业务升级时，弹性伸缩会自动完成底层资源升级，避免访问延时和资源超负荷运行。 例如，当ECS实例或ECI实例的CPU使用率突破80%时，弹性伸缩可以根据企业的配置弹性扩张ECS或ECI资源，自动创建ECS实例或ECI实例，并自动将ECS实例添加到负载均衡实例的后端服务器组和RDS实例的访问白名单中，或自动将ECI实例添加到负载均衡实例的后端服务器组。
弹性伸缩	当企业的业务需求下降时，弹性伸缩会自动完成底层资源释放，避免资源浪费。 例如，当伸缩组内的ECS实例或ECI实例的CPU使用率低于30%时，弹性伸缩将根据企业的配置进行自动收缩，将ECS实例或ECI实例从伸缩组中移除，并将ECS实例从负载均衡实例的后端服务器组和RDS实例的访问白名单中移除，或将ECI实例从负载均衡实例的后端服务器组中移除。
弹性自愈	伸缩组内的ECS实例或ECI实例未处于运行中（running）状态时，将被弹性伸缩检测为不健康。 如果检测某台ECS实例或ECI实例不健康，弹性伸缩将自动释放该ECS实例或ECI实例并创建新的ECS实例或ECI实例。通过弹性自愈功能，可以有效地避免伸缩组内的健康ECS实例或ECI实例数量低于用户设置的最小值。

伸缩组

伸缩组是弹性伸缩的核心单元，是一组具有相同应用场景和相同实例类型的实例的集合。如果企业有多个应用场景，企业可以创建多个伸缩组，弹性伸缩会按照企业的配置分别为每个伸缩组调整实例数量，以满足业务需求。伸缩组定义了组内实例数量的最大值、最小值及其相关联的负载均衡实例和RDS实例等属性。

伸缩配置

伸缩配置定义了用于弹性伸缩的实例的配置信息，实例的配置来源是伸缩组扩容ECS实例或ECI实例时使用的实例配置模板。自动扩容时，伸缩组根据实例配置来源创建ECS实例或ECI实例，并将创建的实例添加到伸缩组。

实例配置来源包括实例启动模板和伸缩配置两种，其中，实例启动模板只适用于伸缩组类型为ECS的伸缩组。伸缩组内只能有一项生效的实例配置来源，例如，选用一条新的伸缩配置后，当前生效的启动模板或伸缩配置会失效。

伸缩规则

伸缩规则定义了具体的扩展或收缩操作，例如加入或移出N个ECS实例或ECI实例。伸缩规则的作用由伸缩规则的类型来决定，可用于触发伸缩活动或者智能设置伸缩组边界值。

弹性伸缩支持步进规则、预测规则、目标追踪规则以及简单规则四种伸缩规则类型。其中，预测规则基于历史监控数据预测未来的指标值，用来智能设置伸缩组边界值，而步进规则、目标追踪规则和简单规则用于在触发伸缩活动时控制增加或减少实例的数量。

伸缩活动

执行伸缩规则、手动添加或移出已有实例时，均会产生一条伸缩活动。伸缩活动主要用来描述伸缩组内ECS实例或ECI实例的变化情况，用于记录伸缩组内实例数、伸缩组边界值、期望实例数等数量的变化情况，触发伸缩活动后，所有扩张和收缩动作都交由系统自动完成。

自动触发任务

自动触发任务指用于自动触发伸缩规则的任务，包括定时任务和报警任务。

- 定时任务：如果业务量的变化时间可预测，例如业务存在周期性的高峰期和低谷期，弹性伸缩支持预设定时任务，通过定时任务可以在指定的时间扩缩容，即在业务高峰到达前准备好充足的计算资源，或者在业务高峰后释放空闲的计算资源。

- 告警任务：如果面对突发或者时间上不可预料的业务场景，定时任务就难满足业务，弹性伸缩支持配置报警任务，通过基于指定的监控指标动态扩缩容资源，提供更灵活的伸缩规则触发方式，即在业务高峰期增加伸缩组内实例数量来缓解业务压力，或者在业务低谷时释放伸缩组内实例来减小生产成本。

9.2.2. 产品价值

与手动管理ECS实例或ECI实例相比，使用弹性伸缩可以有效地降低基础设施成本和运维成本。弹性伸缩具有自动化、降成本、高可用性、灵活智能以及易审计等优势。

自动化

根据用户预设的配置信息，弹性伸缩能够自动化实现弹性扩张和弹性收缩功能，无需用户人工干预，避免因手动操作而引入的低错。弹性伸缩与负载均衡（SLB）及关系型数据库（RDS）紧密集成，也可以自动管理SLB后端服务器和RDS白名单。

降成本

弹性伸缩按需取用，自动释放，提高资源的利用率，有效降低成本。例如，根据业务实际需求自动调整实例数量，在业务量高峰期时，将自动增加ECS实例或ECI实例；在业务量回落时，自动减少ECS实例或ECI实例。通过对实例数量的自动化伸缩，可以节省基础设施成本，用户也无需投入大量人力来调整计算资源，节约了人力成本和时间成本。

高可用性

弹性伸缩通过实时监控实例状态，自动替换不健康实例，来确保业务的高可用性。可以有效避免因不能及时发现ECS实例或ECI实例的不健康状态，而导致业务连续性受到影响的情况。

灵活智能

弹性伸缩的伸缩模式丰富多样，可同时配置固定数量、健康、定时、动态、自定义模式。同时支持多种配置方式和丰富的弹性伸缩策略，灵活智能地有效降低手动配置的复杂度，提高操作效率。

易审计

弹性伸缩自动记录每一个伸缩活动的详细信息，有助于用户快速定位问题根源，降低了排查难度。弹性伸缩还提供伸缩组监控功能，可以通过云监控查看伸缩组内的实例运行状态。用户无需多次查看多台ECS实例或ECI实例的运行状态，有助于用户快速了解整体的业务供给能力。

9.2.3. 应用场景

弹性伸缩有着广泛的典型应用场景，不仅适合业务量不断波动的应用程序，同时也适合业务量稳定的应用程序。

无规律的业务量波动

某新闻网站播出了热点新闻，访问量突增，新闻的时效性降低后，访问量回落，需要及时、自动扩展云计算资源。由于该新闻网站的业务量波动无规律，访问量突增和回落的具体时间难以预测，所以手动调整实例很难做到及时性，而且调整数量也不确定。企业可以利用弹性伸缩的报警任务，由阿里云自动根据CPU使用率等衡量指标进行弹性伸缩。

有规律的业务量波动

某游戏公司每天18:00业务需求急速增长进入高峰期，到22:00业务需求降低，高峰期结束，需要定时扩缩容云计算资源。该游戏公司的业务量波动有规律，但是每天手动调整计算能力会浪费人力和时间成本。企业可以利用弹性伸缩的定时任务，由阿里云定时自动进行弹性伸缩。

无明显的业务量波动

某通信公司的业务支撑系统需要全天运作，业务量一段时间内无明显波动。如果现有计算资源突然出现故障，会导致业务受到严重影响，很难及时进行故障修复或者替换。企业可以利用弹性伸缩的高可用优势，开启健康检查模式。

混合型的业务场景

如果某视频直播公司的业务场景比较复杂，日常业务量波动不明显，但在某个时间段内，业务量是在一定基础上波动的。

例如，用户已经订购了一部分包年包月的ECS实例，只是想针对波动的业务量合理调整ECS实例数量。用户可以手动将已订购的包年包月ECS实例加入伸缩组，再结合弹性伸缩的报警任务，由阿里云自动根据CPU使用率等衡量指标进行弹性伸缩，更经济、稳定地管理业务的计算能力。除手动调整实例数量和报警任务，弹性伸缩还支持定时任务、健康检查等。用户可以根据业务场景灵活组合以上功能，从而在使用弹性伸缩的时候获得更丰富灵活的使用体验。

9.3. 资源编排

资源编排服务（Resource Orchestration Service， 简称ROS）是阿里云提供的一项简化云计算资源管理的服务。

企业可以遵循ROS定义的模板规范编写资源栈模板，在模板中定义所需的云计算资源（例如：ECS实例、RDS数据库实例）、资源间的依赖关系等。ROS的编排引擎将根据模板自动完成所有资源的创建和配置，以达到自动化部署和运维的目的。通过在云上构建自己的基础架构，真正实现基础设施即代码（Infrastructure as Code）。与直接调用各云服务的API相比，大大提高客户业务开展效率。

9.3.1. 产品详情

资源编排服务ROS是阿里云提供的一项简化云计算资源管理的服务，通过资源栈和模板实现阿里云资源的自动部署和运维。

资源栈

资源编排服务通过资源栈（Stack）的逻辑集合来统一管理一组阿里云资源，支持以资源栈为单位对阿里云资源进行创建、更新、重新创建和删除等操作。

模板

资源编排服务中的模板是一个JSON格式的文本文件，使用UTF-8编码，用于创建资源栈，是描述基础设施和架构的蓝图。通过在模板中定义阿里云资源的配置细节，来说明资源间的依赖关系。

ROS模板也是一种标准化的资源和应用交付方式。如果客户是独立软件供应商（ISV），则可以通过ROS模板交付包含云资源和应用的整体系统和解决方案。ISV可以通过这种交付方式，整合阿里云的资源和ISV的软件系统，实现统一交付。

开发者和管理员可以编写模板，在模板中定义所需的阿里云资源（例如：ECS实例、RDS数据库实例）、资源间的依赖关系等。ROS的编排引擎将根据模板自动完成所有资源的创建和配置，实现自动化部署及运维。

9.3.2. 产品价值

资源编排服务ROS可以帮助企业对阿里云资源进行建模和配置。企业只需创建一个描述自己所需的所有阿里云资源（例如ECS 实例、RDS数据库实例等）的模板，然后ROS将根据模板来创建和配置这些资源，以便企业更简单、便捷地管理云资源。

提升部署效率

企业可以使用ROS把云上的整套环境抽象成模板。后续无论是业务增长需要把云上环境扩展到新可用区，还是部署开发、测试和生产环境，企业都可以使用相同模板进行一键部署，提高效率的同时也避免了手动创建的人为错误。

节省成本

通过将云上环境模板化，企业可以按需通过ROS进行大规模自动化部署，没有需求时批量删除相关资源栈。充分利用云上资源的弹性供应，降低成本。

合规管控

ROS符合基础设施即代码（Infrastructure as Code）的理念。企业可以通过模板定义基础设施，模板的创建、更新都可以进行代码审核，并可融入CI/CD流程，从而确保模板符合企业所在组织的管理规范，提高云上环境的安全合规性。

9.3.3. 应用场景

资源编排服务ROS具有广泛的应用场景，既可以帮助企业快速上云，又可以实现按需批量部署和业务环境分发。同时，ROS仅使用通过审核的模板部署云上环境，从而满足IT合规性，规避财务风险。

企业快速上云

使用阿里云沉淀的最佳实践，无需专业IT技能和云上架构设计经验，一键给出解决方案级别的所有资源，优化云上架构。

按需批量部署

应业务扩展需求，或在DevOps场景中，使用模板按需部署多套应用运行环境。

业务环境分发

在中心化IT管理场景中，对于各组织各团队的业务需求，进行统一的跨地域跨账号的标准化环境分发。

云上环境管控

为满足内部合规管控需求，仅使用通过审核的模板部署云上环境，从而满足IT合规性，规避财务风险。

9.4. 弹性高性能计算

弹性高性能计算（Elastic High Performance Computing，简称E-HPC）是阿里云提供的性能卓越、稳定可靠、弹性扩展的高性能计算服务。

E-HPC将计算能力积聚，用并行计算方式解决更大规模的科学、工程和商业问题，在材料科学、石油勘探、金融市场、应急管理、医学和互联网等领域有广泛应用，为用户提供快捷、弹性、安全、与阿里云产品互通的技术计算云平台。

9.4.1. 产品详情

E-HPC主要面向需要大规模计算能力的教育科研机构、企事业单位，支持HPC、AI和大规模数据分析等应用，可以为客户提供高性能CPU、GPU实例的IaaS服务、高性能计算软件栈的PaaS服务和根据应用模版定制的SaaS服务。

集群管理

集群指运行高性能计算的节点集合，提供单节点无法提供的强大计算能力。E-HPC支持一键部署集群环境，用户可以根据实际业务需求，快速创建不同配置的E-HPC集群进行高性能计算，同时支持在作业需求增长时扩容集群节点，在集群不再使用时，释放集群。

用户管理

在集群中提交作业时，E-HPC根据用户来标识提交人身份。通过创建不同权限的用户，可以区分管理员和普通用户角色；根据业务需要，可以修改用户信息或删除用户。

节点管理

E-HPC集群中包含管控节点和计算节点，其中计算节点用于执行高性能计算作业，管控节点用于进行作业调度、域账号管理和远程登录。当节点异常时，支持重启节点进行修复；当计算节点长时间空闲时，支持删除节点以节省资源。

队列管理

集群中的计算节点必须属于一个队列，支持通过队列将运行不同作业或执行不同任务的计算节点进行分类，便于筛选节点；支持根据业务需求设置调度器，调度不同队列进行作业计算。

作业管理

作业是提交到E-HPC集群进行高性能计算的基本工作单元，包括Shell脚本、可执行文件等。作业执行的顺序根据用户设置的队列和调度器决定。支持通过控制台或者命令行创建并提交作业，在作业运行失败或不再需要运行时可以停止作业。

9.4.2. 产品价值

相较于一般HPC集群，E-HPC具有灵活部署、数据安全、高可用性、云产品互通性等优势。

灵活部署

支持通过控制台快速创建高性能计算集群，一键部署业务所需的高性能计算环境和应用程序以及其他依赖。帮助用户快速构建处理能力出色的应用，解放计算带来的压力。

数据安全

- 基于专有网络VPC实现网络访问隔离，VPC内的集群节点可以通过安全组防火墙实现三层网络访问控制，充分保障集群网络的安全性。
- 集群数据存储在文件存储NAS中，利用NAS的传输加密与存储加密特性，保障集群数据不被窃取或篡改。同时，NAS的数据在后端采用多副本存储，可以有效降低数据安全风险。

高可用性

E-HPC集群节点基于云服务器ECS、超级计算集群SCC和GPU云服务器组建，可以极大提高集群的可用性。

云产品互通性

E-HPC整合云服务器ECS、专有网络VPC、文件存储NAS、GPU云服务器等其他云产品，使用体验与其它阿里云产品保持一致，可以轻松上手。

9.4.3. 应用场景

E-HPC可以将计算能力积聚，用并行计算方式解决更大规模的科学、工程和商业问题，主要应用于气象预报、能源勘探、生命科学、教育科研、制造业仿真、动画渲染等领域。

气象预报

E-HPC支持结合数值模型计算分析气象数据与环境数据，可以预测天气、环境等气象信息。

能源勘探

E-HPC可以帮助勘探行业进行勘探数据分析，分析并模拟出勘测区域的地质构造，从而精确寻找资源位置。

生命科学

- 生物信息学

  使用E-HPC对大量生物基因组进行测序等处理，从而获取基因组信息和数据分析系统，解决生物和医学领域的难题。

- 分子动力学模拟

  使用E-HPC进行大规模的分子动力学模拟，预测分析并验证生物蛋白质分子与脂质分子间的相互作用和变化。

- 新药研发

  使用E-HPC帮助研发人员实现大量小分子库的快速并发处理。

教育科研

E-HPC可以给政府、高校的高性能计算中心提供高性能计算服务，用于研究过程中的数值模拟、仿真验证等工作。让教育专家和科学研究者专注于本学科的基础研究，省去了学习掌握处理器和高性能计算知识的时间。

制造业仿真

在智能汽车、航天航空、机械建筑等制造行业中，利用E-HPC高性能和可弹性扩展的特性，对复杂的工程架构和力学结构进行仿真模拟，可以根据仿真结果优化产品结构和性能。

动画渲染

E-HPC支持大规模多机并发业务，可以用于影视动画行业进行图形渲染。

9.5. 服务器迁移中心

服务器迁移中心SMC（Server Migration Center）是阿里云自主研发的迁移平台。使用SMC可将客户的单台或多台迁移源（即源服务器）迁移至阿里云专有云。迁移源概指待迁移的IDC服务器、虚拟机、其他云平台的云主机或其他类型服务器。

9.5.1. 产品详情

服务器迁移中心SMC帮助客户自动化迁移源服务器应用环境，方便、快捷地将源服务器系统迁移至阿里云专有云。

增量迁移

在业务不暂停的情况下，在自定义的时间间隔内，将源服务器系统产生的增量数据迁移至阿里云专有云，有效减少源服务器系统业务暂停时间和最终交割时间。

块复制迁移

自动获取迁移源磁盘分区结构，通过块复制功能在迁移时自动生成与迁移源磁盘分区结构一致的目标磁盘，实现在保持源服务器磁盘分区结构的情况下完成服务器迁移。

批量迁移

使用SMC提供的API接口脚本化创建、执行迁移任务，支持迁移任务进度查询、迁移任务批量管理。

多线程加速传输

支持多线程传输数据，在带宽较高的场景下能最大化利用带宽，有效提升传输效率。

集中跟踪迁移进度

批量迁移源服务器时，支持集中跟踪每台迁移源的迁移状态。SMC控制台展示所有迁移源和迁移任务的状态，帮助客户迅速了解整体迁移进度，识别并排查迁移中出现的问题。

9.5.2. 产品价值

服务器迁移中心SMC作为阿里云自主研发的迁移工具，具有多平台支持、平滑迁移、配置简单以及保障数据安全等优势。

支持多平台、多环境迁移

- 支持多种Windows和Linux操作系统版本。
- 支持将源服务器从自建IDC机房、本地虚拟机（VMware、Xen、KVM、Hyper-V等）、其他厂商云服务器迁移至阿里云专有云。

不依赖源服务器的底层环境

- 支持物理机到云（P2C）、虚拟机到云（V2C）、云到云（C2C）迁移。
- 支持多种格式文件系统、磁盘类型。
- 支持不停机迁移。整个迁移过程无需停机，不影响源服务器系统业务。

简单轻量且配置灵活

- SMC客户端轻量免安装。
- 提供多种迁移方案，支持按需配置。
- 一键运行迁移后，全程自动托管。

数据传输安全有保证

- 默认采用SSL 2048位RSA密钥加密传输通道。
- 支持通过VPN网关、高速通道物理专线等私网迁移。

支持断点续传

数据传输中断后，重新运行客户端并重新启动迁移任务即可继续迁移。

支持增量迁移

在第一次全量迁移完成后，用户还可以进行多次增量迁移，有效减少源服务器系统业务暂停时间及最终交割时间。

支持不停机迁移

迁移过程只是完整复制源系统的数据，无需停机，也不会干涉影响源服务器系统的业务。

9.5.3. 应用场景

服务器迁移中心SMC主要应用于各种服务器的迁移场景，支持将单台或多台源服务器迁移至阿里云专有云。

自建IDC机房迁移至专有云

IDC机房服务器老化、运维繁琐、升级扩容慢、维护成本高，用户可通过SMC将自建IDC机房迁移至阿里云专有云，充分享受云上高可用性、高安全性和高弹性的优势。

本地虚拟机迁移至专有云

与本地虚拟机相比，云上的服务器成本更低、管理灵活性更大、资源丰富程度更高，用户可通过SMC可将本地虚拟机（VMware、Virtual Box、XEN、KVM、Hyper-V等）迁移至阿里云专有云。

其他厂商云迁移至专有云

由于其他厂商云的某些功能、性能、安全、成本等无法满足当前业务需求，用户可通过SMC可将其他厂商云（如亚马逊AWS、微软Azure、谷歌GCP、腾讯云、UCloud、电信云、青云等）迁移至阿里云专有云。

跨账号或跨地域云服务器迁移

如果阿里云专有云ECS实例无法通过升级、扩容等方法满足当前业务需求，用户可将不同阿里云账号、不同地域或不同VPC下的ECS实例进行迁移。如果客户的网络可以打通VPC内网，建议在创建迁移任务时网络模式选择内网传输，使用内网传输能获得比通过公网更快速更稳定的数据传输效果，提高迁移工作效率。

9.6. 运维编排

阿里云运维编排服务（Operation Orchestration Service，简称OOS），是阿里云提供的云上自动化运维服务，能够自动化管理和执行任务。

9.6.1. 产品详情

用户可以通过模版来定义执行任务、执行顺序、执行输入和输出，然后通过执行模版来完成任务的自动化运行。OOS支持跨产品使用，使用OOS可管理ECS、RDS、SLB、VPC等云产品。

模版

OOS使用模版来定义所需要编排的运维操作，模板内容支持YAML和JSON两种格式，可分为公共模版和自定义模版两种类型。

执行

OOS支持多种运行模式，包括自动化、半自动化和交互式，帮助用户完成多样化的运行任务。

- 自动执行：建议先在测试环境使用，以便完全了解模板所进行的运维操作，并且结果符合预期，然后才在生产环境进行。
- 单步执行：类似于调试（Debug）功能。需要详细地了解每一个任务的执行时，可使用单步执行模式。

9.6.2. 产品价值

OOS可以帮助企业更好地规范、管理和执行自动化运维操作。用户以模板的方式定义所需要进行的操作，然后再通过系统运行，从而提高整体运维操作的效率、增强运维操作的安全性，并降低手工运维的错误。

可视化的执行过程和执行结果

通过提供可视化的执行过程，可以查看完整的执行过程和执行结果，具体包括：

- 直观地看到各个任务的执行详情、参数和输出。
- 清晰地看到执行的流程、顺序和错误跳转。

全托管自动化

提供全托管的自动化执行，即无服务器（Serverless）的自动化执行。执行过程无须消耗和使用业务侧的计算资源（如ECS实例），即可满足创业型公司、中小型企业以及大型企业客户的自动化运维需求。完全的自动化模式下无需人工守护，让用户更加专注于业务的高速增长。

高效的批量管理

传统场景下，执行批量任务相比执行单一任务的管理复杂度大幅增加，OOS可以提供实时的进度管理、运行状况统计和快速的错误定位，从而提高整体的运维效率。

完备的鉴权和审计

支持使用资源访问管理和用户权限管理系统（RAM）管理OOS，无论是运维编排自身的操作，还是通过运维编排执行的对其他云产品的操作，均支持鉴权和审计，无需担心操作的安全性。

快速模板构建能力

OOS提供高易用性的模板构建能力，用户无需从零开始构建。OOS提供热门云产品的快速集成能力云产品动作，帮助用户快速地构建模板，降低模板编写的难度，提高整体运维的效率。同时，OOS为常见的运维场景提供了公共模板，只需选择一个类似的模板快速地复制和修改，即可满足运维需求。

标准化运维任务（Operations as Code）

将日常所需要的运维任务以模板的方式提供，并遵循代码（Code）的管理方式来管理模板。从创建到审核，再同步到生产账号中，后续的运维任务只从标准模板中选择运行，确保运维动作的安全，像源代码一样的规范，并以此完成运维即代码（Operations as Code）的最佳实践。

运维权限收敛（委托授权）

运维人员的权限管理非常地复杂，太大的权限意味着太高的风险，太小的权限又无法完成运维操作，如何可以让运维人员完成运维任务，同时又避免他进行非预期的操作。OOS提供委托授权模式，具有高权限的管理人员编写OOS模板，并配置固定的role，此时即完成了委托授权。然后将执行此模板的权限开放给其他低权限的运维人员，即可完成运维任务，又避免了高权限的风险。

9.6.3. 应用场景

OOS的常见应用场景包括批量操作、更新镜像、需要审批的运维场景、定时任务的运维等应用场景，且用户也可根据自身实际场景自定义诸多灵活多样的模版。

批量操作

批量地执行运维命令，即需要针对多个目标（如ECS实例）进行常规操作，以确保业务的正常和平滑运行，并保持业务的健康状态。例如，批量检查ECS实例中的硬盘剩余空间：首先选择需要检查的实例列表（多种选择方式，如名字匹配、标签分组、资源组分组等），然后通过云助手命令执行硬盘检查，最终统一查看结果。

更新镜像

为了保证ECS实例的运行环境始终是安全的，包括安装最新补丁，或者更新所依赖的组件等，可以使用OOS更新镜像，从一个源镜像开始逐步更新，最终生成一个新镜像，然后用于测试和生产。

需要审批的运维场景

在很多场景下都需要使用审批来确保操作是安全并符合预期的。通过在模板中增加审批动作（ACS::Approve）可以在运维动作实际执行前进行人工审批，以确保运维动作执行的必要性，避免浪费和误操作。

定时任务

定时执行所定义的运维动作。例如，在某测试场景中，需要清除某账号下因为测试所产生的对象存储OSS文件，则可以创建一个模板，每天凌晨运行，以确保测试环境是一个全新的环境，避免干扰下一次的测试结果。

9.7. 裸机管理服务BMS

裸机管理BMS（BareMetal Mangement Service）是指将物理服务器通过云平台来按需和弹性的提供给租户使用的一种云服务，通常用来为核心数据库、关键应用系统、高性能计算等业务提供计算资源支撑。

裸机管理服务通过专有云统一运维界面进行管理，它可以直接对物理机执行节点级别的管理，包括物理机节点的添加、删除、电源管理、系统部署等操作。在完成基本的服务器上架以及相关准备工作后，管理员可在UI界面批量部署裸金属设备，部署完成后可使用裸金属设备创建裸金属主机，支持自定义安装操作系统（x86下的AliOS/CentOS和SW下的deepOS/AliOS），并对裸金属主机进行全生命周期管理。

9.7.1. 产品详情

裸机管理服务包含裸机实例管理、托管实例管理两大服务模块，帮助客户实现物理服务器裸机的管理。

服务模块		功能模块	描述
	概览	实例大盘概览的功能	针对用户侧实例资源信息运营管理的需求，提供实例资源大盘信息监控展示的能力。 具备实例状态监控，镜像、磁盘监控，CPU、内存、网络负载监控的能力。组织配额使用率排名的能力，实例资源使用率排名的能力。

裸机实例管理	裸机实例	实例的列表管理功能	针对用户所申请实例的相关运营管理需求，提供查询，信息展示，运营操作以及单台裸机的资源监控的能力。 • 信息展示包含实例名称/SN、实例状态、Agent状态、电源状态、网络信息、镜像信息、机型配置信息、创建时间等。 • 运维操作包含业务状态变更（如停止、启动、重启、删除等），带外控制管理等操作。 • 单台裸机的资源监控可实现对CPU、内存、磁盘、网络等负载情况的监控。
		申请实例功能	提供用户申请实例的相关功能，具备用户为实例配置基本信息、配置镜像类型、配置网络参数、密码权限的能力。
	镜像	自定义镜像功能	针对用户根据运营所需镜像的个性化管理需求，提供对自定义镜像的查询、信息展示、管理操作以及自定义上传的能力。 • 自定义上传功能可配置上传镜像的区域信息、平台类型、系统架构类型，方便对镜像进行分类管理。 • 信息展示包含镜像名称/ID、大小、架构、平台、格式、可用状态、创建时间等。
		公共镜像功能	提供对公共镜像的查询、状态变更以及导出的能力。
	裸机实例监控	裸机资源监控功能	实现裸机资源CPU使用率、内存使用率、磁盘负载、网络负载、服务器在线数量等相关资源监控的能力。
	裸机实例告警	裸机资源告警功能	提供对实例资源中托管类型的裸机所产生的故障告警的监控及处理的能力。
托管实例管理	概览	托管概览功能	针对用户对托管主机的运营需要，提供托管大盘信息监控展示的能力； 具备托管主机的健康度检测的能力，告警未处理情况监控的能力，关键指标数量监控的能力，带内/带外库存使用率监控的能力。
	带内托管实例	带内托管功能	针对用户侧存量服务器的带内托管的能力需求，提供查询、信息展示、运营操作以及新增托管实例的能力。 其中新增带内托管实例的功能，具备用户为所托管实例配置基本信息、机房信息、网络参数、SSH信息、密码权限的能力。
	带外托管实例	带外托管功能	针对用户侧存量服务器的带外托管的能力需求，提供查询、信息展示、运营操作以及新增托管实例的能力。 其中新增带外托管实例的功能，具备用户为所托管实例配置基本信息、机房信息、带外信息的能力。
	托管实例监控	托管实例资源监控功能	实现对托管实例资源CPU使用率、内存使用率、磁盘负载、网络负载、服务器在线数量等相关资源监控的能力。
	托管实例告警	托管告警功能	提供对实例资源中托管类型的裸机所产生的故障告警的监控及处理的能力。对已处理和未处理的故障告警支持分类管理，操作更简洁明了。

9.7.2. 产品价值

裸机管理服务是一整套通用的解决方案，可为应用提供专属的物理服务器，保障核心应用的高性能和稳定性。简单来说，裸机管理服务可认为是为服务器裸机安装相应的操作系统，并获取其配置信息，最后实现对裸金属主机的生命周期控制，例如开机、关机、重启等操作。整个操作过程仅需要保证服务器主机有网络并且通电即可。

裸机管理服务为用户提供了高性能的计算集群，为不适合虚拟化的应用提供了一种解决方案，扩展并增强了Aliclone能力，并且通过“共池”管理能力，触达企业传统IT应用领域，提升客户迁移上云的效率，助力客户业务更平滑上云。

9.7.3. 应用场景

当前企业和政府用户在面向如下应用场景时，通常需要采用裸机管理服务：

- 计算任务需要访问无法虚拟化的硬件设备。
- 数据库主机需求。
- 安全隔离：在资源层面是将整个实例只给一个租户独享，且租户间天然物理隔离，实例间不存在资源抢占。因此，非常适合对安全合规或者性能隔离有强诉求的业务应用。
- 快速部署和利旧云基础设施时，政企客户有很多服务器纳管的诉求，需要裸机管理服务将这类服务器统一到一朵云中管理；也可以采用裸机管理服务对接传统存储阵列（SAN、NAS），保证客户的投资和使用习惯。
- 传统企业客户有大量的存量虚拟化或者第三方云平台（例如VMware、OpenStack等），这类软件由于嵌套虚拟化带来的性能或者兼容性问题通常不适合在虚拟机中运行。裸机管理服务可以很好地支持这类应用，并有助于将存量云应用与现有全栈云产品打通。
- 专用硬件、安全性、可靠性和其他控制要求。

9.8. 容器服务

容器服务（Container Service）是一种高性能可伸缩的容器管理服务，支持企业级Kubernetes容器化应用的生命周期管理。容器服务简化集群的搭建和扩容等运维工作，整合阿里云虚拟化、存储、网络和安全能力，打造云端最佳的Kubernetes容器化应用运行环境。容器服务是Kubernetes认证服务供应商，全球首批通过Kubernetes一致性认证的平台服务，为企业提供专业的支持和服务。

9.8.1. 产品详情

容器服务拥有强大的Kubernetes集群管理能力，提供集群管理、一站式容器生命周期管理和高可用调度策略等功能，帮助企业轻松高效地在云端运行Kubernetes容器化应用。

集群管理

- 通过控制台10分钟一键创建经典Dedicated Kubernetes集群，支持GPU服务器。
- 提供容器优化的OS镜像，提供稳定测试和安全加固的Kubernetes和Docker版本。
- 支持多集群管理、升级和伸缩功能。

一站式容器生命周期管理

- 网络
  - 提供阿里云优化的高性能VPC/ENI网络插件，性能优于普通网络方案20%。
  - 支持容器访问策略和流控限制。
- 存储
  - 支持阿里云云盘、对象存储OSS，提供标准的FlexVolume驱动。

- 支持存储卷动态创建，迁移。

- 日志
  - 支持高性能日志自动采集和阿里云日志服务集成。
  - 支持和第三方开源日志解决方案集成。
- 监控
  - 支持容器级别和VM级别的监控。
  - 支持集成第三方开源监控解决方案。
- 权限
  - 支持集群级别的RAM授权管理。
  - 支持应用级别的权限配置管理。
- 应用管理
  - 支持灰度发布，支持蓝绿发布。
  - 支持应用监控，应用弹性伸缩。
- 组件管理

  提供多种类型的组件，您可以根据业务需求部署、升级、卸载组件。

高可用调度策略

- 支持服务级别的亲和性策略和横向扩展。
- 支持跨可用区高可用和灾难恢复。
- 支持集群和应用管理的OpenAPI，轻松对接持续集成和私有部署系统。

性能指标

- 单个集群性能：支持单集群最大1000节点，10万容器的管理。
- 集群数量：支持最多200个集群的管理。
- 容器启动时间：10s内成功启动100个20 MB的容器实例。

9.8.2. 产品价值

容器服务提供快捷的操作方式，拥有强大的Kubernetes集群管理能力，支持管理多种集群形态，根据业务情况完成极致弹性的资源扩缩，实现一站式的IAAS、资源、容器的管理能力，提供最优的IaaS层能力，支持企业级的安全稳定。

快捷的操作方式

- 通过Web界面一键创建、升级Kubernetes集群。

  在使用自建Kubernetes集群的过程中，可能需要同时处理多个版本的集群。每次升级集群的过程都是一次大的调整和巨大的运维负担。容器服务的升级方案使用镜像滚动升级以及完整元数据的备份策略，方便地回滚到先前版本。
- 通过Web界面轻松地实现Kubernetes集群的扩容和缩容。

  使用容器服务Kubernetes集群可以方便地一键垂直扩缩容来快速应对数据分析业务的波动。

强大的集群管理能力

- 容器服务在社区Kubernetes的基础上进行了增强，提供专有集群、边缘集群等多种集群形态。
- 兼容开源生态，支持专有云、多云、混合云等多种云场景。

极致弹性的资源

- 根据容器资源使用情况，快速自动地调整容器数量，支持容器的水平扩缩容。
- 根据集群节点资源使用情况，快速自动地调整节点数量。
- 支持类型丰富的节点，能纳管X86、ARM、神龙、GPU、边缘等不同类型的节点。

一站式的容器管理

- 应用管理：支持灰度发布，蓝绿发布、应用监控，应用弹性伸缩。
- 日志：支持日志采集及将采集的日志集成到日志服务；支持集成第三方开源日志解决方案。
- 监控：支持容器级别和VM级别的监控；支持集成第三方开源监控解决方案。
- 镜像仓库：高可用，支持大并发；支持镜像加速；支持大规模P2P分发。

最优的IaaS层能力

- 网络：提供持续的网络集成和最佳的网络优化。
- 存储：自建Kubernetes集群无法使用云上的存储资源，容器服务集成阿里云多种存储产品/能力，例如阿里云云盘、文件存储NAS等，实现与云存储的的无缝集成。
- 负载均衡：支持创建负载均衡实例（公网、内网）。

  使用自建Kubernetes集群的过程中，业务的频繁发布可能会对自建Ingress产生配置压力，增大出错概率。容器服务的SLB方案支持原生的阿里云高可用负载均衡，可以自动完成网络配置的修改和更新。该方案经历了大量用户长时间的使用，稳定性和可靠性大大超过用户自建的入口实现。

企业级的安全稳定

容器服务提供了Docker CE保证、推动Docker修复的能力。遇到Docker Engine hang、网络问题、内核兼容等问题时，容器服务可以为客户提供最佳实践。

- 专门的团队保障容器的稳定性。
- 提供经过稳定测试和安全加固的Linux版本和Kubernetes版本。

9.8.3. 应用场景

容器服务适应于DevOps持续交付、基于云原生技术的机器学习、微服务架构、混合云架构、弹性伸缩架构等场景。

DevOps持续交付

配合Jenkins帮助客户自动完成从代码提交到应用部署的DevOps完整流程，确保只有通过自动测试的代码才能交付和部署，高效替代业内部署复杂、迭代缓慢的传统方式。

- DevOps自动化：实现从代码变更到代码构建，镜像构建和应用部署的全流程自动化。
- 环境一致性：容器技术让用户交付的不仅是代码，还有基于不可变架构的运行环境。
- 持续反馈：每次集成或交付，都会实时反馈结果。
- 推荐搭配产品：云服务器ECS。

基于云原生技术的机器学习

帮助数据工程师在异构计算资源集群上轻松开发、部署机器学习应用，跟踪试验和训练、发布模型，自动集成多种分布式存储系统，加速训练数据读写。无需关心繁琐部署运维，专注核心业务，快速从0到1。

- 支持生态：内置对TensorFlow、Caffe、MXNet、Pytorch等主流深度学习计算框架支持和优化。
- 快速弹性：一键部署机器学习开发、训练、推理服务，秒级启动和弹性伸缩。
- 简单可控：轻松创建、管理大规模GPU计算集群，并且可以监控GPU利用率等核心指标。
- 深度整合：无缝接入阿里云存储、日志监控和安全基础架构能力。
- 推荐搭配产品：云服务器ECS / GPU服务器EGS + 对象存储OSS / 文件存储NAS / CPFS。

微服务架构

企业生产环境中，通过合理微服务拆分，将每个微服务应用存储在阿里云镜像仓库。客户只需迭代每个微服务应用，由阿里云提供调度、编排、部署和灰度发布能力。

- 负载均衡和服务发现：支持4层和7层的请求转发和后端绑定。
- 丰富的调度和异常恢复策略：支持服务级别的亲和性调度，支持跨可用区的高可用和灾难恢复。
- 微服务监控和弹性伸缩：支持微服务和容器级别的监控，支持微服务的自动伸缩。
- 推荐搭配产品：云服务器ECS + 云数据库 RDS 版 + 对象存储OSS。

混合云架构

在容器服务控制台上同时管理云上云下的资源，不需在多种云管理控制台中反复切换。基于容器基础设施无关的特性，使用同一套镜像和编排同时在云上云下部署应用。

- 在云上伸缩应用：业务高峰期，在云端快速扩容，把一些业务流量引到云端。
- 云上容灾：业务系统同时部署到云上和云下，云下提供服务，云上容灾。
- 云下开发测试：云下开发测试后的应用无缝发布到云上。
- 推荐搭配产品：云服务器ECS + 专有网络VPC + 高速通道（Express Connect）。

弹性伸缩架构

容器服务可以根据业务流量自动对业务扩容/缩容，不需要人工干预，避免流量激增扩容不及时导致系统挂掉，以及平时大量闲置资源造成浪费。

- 快速响应：业务流量达到扩容指标，秒级触发容器扩容操作。
- 全自动：整个扩容/缩容过程完全自动化，无需人工干预。
- 低成本：流量降低自动缩容，避免资源浪费。
- 推荐搭配产品：云服务器ECS + 云监控。

9.9. 容器镜像服务

容器镜像服务ACR是面向容器镜像、Helm Chart等符合OCI标准的云原生制品安全托管及高效分发平台。支持便捷的容器镜像权限管理、容器镜像同步分发、内容加签保障等能力，便于客户进行容器镜像全生命周期管理。容器镜像服务简化了Registry的搭建及运维工作，并联合容器服务等云产品，帮助企业降低交付复杂度，打造云原生应用一站式解决方案。

9.9.1. 产品详情

容器镜像服务ACR是面向容器镜像、Helm Chart等符合OCI标准的云原生制品安全托管及高效分发平台，提供了制品管理、镜像分发、制品安全和部署集成等功能。

制品管理

- 安全托管：支持按照命名空间划分，安全托管容器镜像。
- 生命周期管理：支持查询制品、镜像版本，删除制品、镜像仓库。
- 细粒度权限管理：支持用户、ASCM部门和资源集权限管理。
- 版本不可变：支持镜像和OCI制品版本的不可变。

镜像同步

- 触发器：支持容器镜像更新后，自动触发对应触发器的事件。
- 镜像同步：支持手动触发某个镜像版本的同步，实现多地域容器镜像的容灾备份。支持镜像推送后自动同步和跨账号同步镜像。

制品安全

- 加密分发容器镜像：支持配置HTTPS加密协议分发容器镜像。

- 容器镜像加签：支持容器镜像加签，保障镜像从分发到部署全链路一致性，避免中间人攻击和非法镜像的更新及运行。
- 镜像安全扫描：支持容器镜像安全扫描，识别镜像的漏洞风险。

部署集成

- 免密拉取：在容器服务平台部署，支持免密拉取配置，避免每次设置Secret。
- 部署选择：在容器服务平台部署，支持可视化选择ACR中的镜像仓库及版本。

9.9.2. 产品价值

容器镜像服务的优势主要体现在易用性、安全性和可集成性这三个方面。

简单易用

- 无需自行搭建及运维，一键创建镜像仓库。
- 支持多地域，提供稳定快速的镜像上传、下载服务。

安全可控

- 完善的镜像权限管理体系，确保镜像的分享安全，团队的协作便利。
- 提供镜像安全扫描功能，保证镜像漏洞可识别，漏洞级别可提示。

高效分发

- 支持单地域大规模分发，支持500节点以内并发拉取规模。
- 支持多地域同步、跨云同步分发场景，支持手动、自动灵活的同步方式。

云产品间无缝集成

与容器服务等云产品深度集成，实现镜像更新后的持续部署。

9.9.3. 应用场景

容器镜像服务适应于DevOps持续交付、自动同步镜像等场景。

DevOps持续交付

配合Jenkins帮助客户自动完成从代码提交到应用部署的DevOps完整流程，确保只有通过自动测试的代码才能交付和部署，高效替代业内部署复杂、迭代缓慢的传统方式。

- DevOps自动化

  实现从代码变更到代码构建，镜像构建和应用部署的全流程自动化。

- 环境一致性

  容器技术让用户交付的不仅是代码，还有基于不可变架构的运行环境。

- 持续反馈

  每次集成或交付，都会实时反馈结果。

自动同步镜像

容器业务全国多地域、多云部署，存在容器应用一次提交，多地域多云部署场景。使用容器镜像服务同步能力，提高自动化分发效率，降低人工运维成本，提高灾备能力。

- 多场景同步
  - 支持跨地域、跨云跨账号同步的同步场景。
  - 支持手动、镜像更新自动同步的同步方式。

- 调度优化

  支持同步调度优化，提高同步成功率。
- 安全合规

  同步数据链路加密，保障同步数据安全。

10.存储服务

10.1. 云定义存储

云定义存储CDS（ Cloud Defined Storage）是阿里云提供的以云定义存储的分布式文件系统，具有安全、低成本、高可靠、统一管控、云上和云下资源弹性扩展等特点，能有效解决在本地高效存储和获取数据的问题。

针对不同行业的非结构化数据访问、海量日志数据处理等需求，CDS通过部署对象存储OSS、日志服务SLS、块存储EBS、表格存储Tablestore（简称OTS）等不同服务，提供非结构化数据（例如文档、图片、视频等）存储，日志数据存储以及日志查询和分析功能，适用于移动应用、大型网站等大数据场景下的非结构化数据存储以及海量日志数据的存储、查询和分析。CDS能为不同领域的企业用户提供低成本、安全可靠的一体化存储解决方案。

10.1.1. 产品详情

CDS的存储集群上支持部署对象存储服务、日志服务等。当CDS中部署不同云服务时，支持的功能特性不同。

对象存储OSS、块存储EBS和表格存储Tablestore（简称OTS）四种数据存储服务的区别请参见下表。

分类	特点	场景
块存储	是为ECS实例提供的块设备，高性能、低时延，满足随机读写，可以像使用物理硬盘一样格式化建文件系统使用。	可用于大部分通用业务场景下的数据存储。
对象存储	可以理解为一个海量的存储空间，最适合存储互联网上产生的图片、短视频、音频等海量非结构化数据。用户可以通过API在任何时间、任何地点访问对象存储中的数据。	常用于互联网业务网站搭建、动静资源分离等业务场景。
表格存储	提供了表操作、数据操作、数据版本和生命周期、主键列自增、条件更新、通道服务、二级索引、多元索引等功能。	适用于海量数据存储与分析，互联网社交Feed流，海量交易记录与用户模型的存储和实时查询，海量、高效、灵活的车联网数据存储，海量物联网数据存储，高效的查询与分析和海量电商交易订单与用户推荐数据库场景。

对象存储OSS

对象存储OSS（Object Storage Service ）是阿里云提供的安全、低成本、高可靠的云存储服务。

功能特性	说明
Bucket和Object管理	在上传任何文件（Object）到OSS之前，用户需要先创建存储空间（Bucket）来存储文件。创建存储空间后，通过配置存储空间功能例如防盗链、生命周期等来管理文件。
Object上传和下载	用户可以上传任意类型文件到存储空间中。上传文件后，通过单个获取已上传文件的地址或者批量导出文件URL列表可以进行文件的分享和下载。
访问控制	OSS为权限控制提供访问控制列表（ACL）。ACL是授予存储空间和文件访问权限的访问策略。 用户可以在创建存储空间或上传文件时配置ACL，也可以在创建存储空间或上传文件后的任意时间内修改ACL。

静态网站托管	静态网站是指所有的网页都由静态内容构成，包括客户端执行的脚本（例如JavaScript）。用户可以通过静态网站托管功能将静态网站托管到OSS的存储空间，并使用存储空间的访问域名访问此网站。
防盗链	OSS支持对存储空间设置防盗链，即通过对访问来源设置白名单的机制，避免OSS资源被其他人盗用。防盗链功能通过设置Referer白名单，限制仅白名单中的域名可以访问存储空间内的资源。
日志管理	用户访问OSS的过程中会产生大量的访问日志，用户可以通过日志存储功能将OSS的访问日志按照固定命名规则，以小时为单位生成日志文件写入指定的Bucket。 实时日志查询功能将OSS与日志服务SLS相结合，能直接查询OSS访问日志，帮助用户完成OSS访问的操作审计、访问统计、异常事件回溯和问题定位等工作，提升工作效率并帮助用户更好地基于数据进行决策。
跨域资源共享	跨域资源共享CORS（Cross-Origin Resource Sharing）简称跨域访问，是HTML5提供的标准跨域解决方案，允许Web应用服务器进行跨域访问控制，使得跨域数据传输得以安全进行。
生命周期	通过生命周期规则定期删除过期的文件，从而节省存储费用。
合规保留策略	针对存储空间设置基于时间的合规保留策略。当策略锁定后，用户可以在Bucket中上传和读取文件，但是在Object的保留时间到期之前，任何用户均无法删除Object和策略。Object的保留时间到期后，才可以删除Object。此特性允许用户以“不可删除、不可篡改”方式保存和使用数据。
图片管理	通过图片样式功能，在一个样式（Style）中包含多个图片处理参数，快速实现复杂的图片处理操作。 为了防止OSS内允许匿名访问的图片文件被盗用，用户可以开启原图保护功能。开启原图保护后，匿名访问者只能使用携带样式参数的请求或通过签名URL访问原图。
云存储网关	用户通过标准的NFS和SMB协议即可读写指定OSS Bucket里的对象。并且利用本地存储空间作为热数据缓存，使用户在享受OSS Bucket海量空间的同时，保障数据访问的高性能。

块存储EBS

块存储EBS（Elastic Block Storage）是为云服务器ECS提供的低时延、持久性、高可靠的块级随机存储。块存储提供基于分布式存储架构的弹性块存储产品。

弹性块存储产品为ECS实例提供数据块级别的随机存储，具有低时延、持久性、高可靠等特点，采用三副本的分布式机制，为ECS实例提供数据可靠性保证。可以随时创建或释放，也可以随时扩容。

EBS支持云盘。云盘是为云服务器ECS提供的数据块级别的块存储产品。根据性能不同，云盘包括高性能云盘、普通性能云盘、高效云盘和SSD云盘。一块云盘只能挂载到同一可用区的一台ECS实例上。

功能特性	说明
云盘管理	云盘创建后，将云盘挂载到云服务器ECS实例，为ECS提供存储空间。使用云盘存储数据前，需要格式化云盘。
存储集	通过创建存储集，用户可以按照业务类型等维度对块存储（EBS）集群进行划分并绑定相应EBS集群到存储集的不同分区，实现不同业务之间EBS集群的隔离。

云盘快照	通过创建快照，用户可以保留某个时间点一块云盘的数据拷贝，有计划地对云盘创建快照，从而保证业务可持续运行。快照适用于环境复制、容灾备份等场景中。
云盘加密	云盘加密提供了一种简单安全的加密手段，能够对新创建的云盘进行加密处理。
快照一致性组	通过创建快照一致性组，用户可以为一台ECS实例中的多块云盘同时创建快照。快照一致性组能够保证在业务系统跨多块云盘的场景下，数据写入云盘的时序一致性，并保证其崩溃一致性。
自动快照策略	自动快照策略适用于系统盘和数据盘，可以周期性地为云盘创建快照。合理利用自动快照策略能提高数据安全和操作容错率。
云盘异步复制	云盘异步复制是一种基于块存储数据复制能力实现同地域跨可用区数据保护的功能。该功能可以将某一块云盘的数据，异步复制到同一地域不同可用区内的另一块云盘中，实现存储数据的同地域跨可用区容灾备份。用户可以通过该功能建立关键业务的容灾能力，保护数据库数据的同时提升业务的连续性。
一致性复制组	通过创建一致性复制组，用户可以统一操作和管理生产站点和灾备站点之间的复制对。
多实例挂载	开启了多重挂载功能的高性能云盘可以同时挂载到同可用区内的多台支持NVMe协议的ECS实例上，从而实现多台ECS实例对同一块高性能云盘的并发读写访问。

表格存储Tablestore

表格存储Tablestore（OTS）是阿里云自主研发的海量NoSQL数据存储服务，具有国家颁发的软件著作权证书。表格存储构建在阿里云飞天分布式系统之上，提供海量结构化数据的存储和实时访问。表格存储提供了表操作、数据操作、数据版本和生命周期、主键列自增、条件更新、通道服务、二级索引、多元索引等功能。

- 通用功能
  - 在数据存储模型上，支持schema free的表结构，属性列的使用不需要预先定义，增加或者减少属性列不需要做表级别变更。同时支持表级别的数据生命周期，过期数据自动删除。
  - 采用多节点集群架构，平台内管理节点支持高可用机制，日常运维管理节点故障不影响业务正常运行。
  - 采用三副本技术，并将数据副本文件保存在不同机架上。单集群可以支持纯SSD存储实例或者SSD与SATA混合存储实例，以满足对成本和性能上的不同需要。
  - 采用全冗余架构，无单点故障；可支持在线平滑升级，动态增加或者删除结点以及进行集群热升级，不需要停机维护，数据可以自动迁移；读写并发和存储容量支持同步线性扩容，单集群最大规模不低于500台。
  - 支持高并发读写。读写并发能够随着机器数量水平扩展，读写性能与单表数据量无直接关系。
  - 支持身份验证，支持多租户，具备完善的权限认证与隔离机制，保障用户数据的私密性，支持VPC网络及HTTPS访问。提供多种鉴权和授权机制及主子账号功能，授权粒度达到表级别和API级别。
- 表操作

  支持列出实例中的全部数据表、创建一张数据表、查询数据表的配置信息、更新数据表的配置信息以及删除一张数据表。
- 基础数据操作

  表格存储提供了PutRow、GetRow、UpdateRow和DeleteRow的单行数据操作接口以及BatchWriteRow、BatchGetRow和GetRange的多行数据操作接口。用户可以通过单行数据操作接口或者多行数据操作接口读写表中数据。
- 数据版本和生命周期

  使用数据版本以及数据生命周期（TTL）功能，用户可以有效的管理数据，减少数据存储空间，降低存储成本。

- 主键列自增

  设置非分区键的主键列为自增列后，在写入数据时，无需为自增列设置具体值，表格存储会自动生成自增列的值。该值在分区键级别唯一且严格递增。

- 条件更新

  只有满足条件时，才能对数据表中的数据进行更新；当不满足条件时，更新失败。

- 过滤器

  在服务端对读取的结果再进行一次过滤，根据过滤器中的条件决定返回哪些行。由于只返回符合条件的数据行，所以在大部分场景下，可以有效降低网络传输的数据量，减少响应时间。

- 通道服务

  通道服务（Tunnel Service）是基于表格存储数据接口之上的全增量一体化服务。通道服务提供了增量、全量、增量加全量三种类型的分布式数据实时消费通道。通过为数据表建立数据通道，用户可以简单地实现对表中历史存量和新增数据的消费处理。

功能	描述
全增量一体的数据通道	通道服务不仅提供增量数据消费能力，还提供了可并行的全量数据消费以及全量加增量数据消费功能。
增量数据变化保序	通道服务为数据划分一到多个可并行消费的逻辑分区，每个逻辑分区的增量数据按写入时间顺序保序，不同逻辑分区的数据可以并行消费。
消费延迟监控	通道服务通过DescribeTunnel API提供了客户端消费数据RPO（恢复点目标，recovery point objective）信息，并在控制台提供了通道数据消费监控。
数据消费能力水平扩展	通道服务提供了逻辑分区的自动负载均衡功能，提高水平扩展数据消费速度。

- 二级索引

  通过创建一张或多张索引表，使用索引表的主键列查询，二级索引（Secondary Index）相当于把数据表的主键查询能力扩展到了不同的列。使用二级索引能加快数据查询的效率。

  为了满足用户的强一致性查询等需求，表格存储在支持全局二级索引的同时，推出了本地二级索引。

功能	描述
单列索引和组合索引	支持为数据表中的某一列或者多个列建立索引。
索引同步	全局二级索引和本地二级索引的数据同步方式不同。 ◦ 使用全局二级索引时，表格存储以异步方式将数据表中被索引的列和主键列的数据自动同步到索引表中，正常情况下同步延迟达到毫秒级别。 ◦ 使用本地二级索引时，表格存储以同步方式将数据表中被索引的列和主键列的数据自动同步到索引表中，当数据写入数据表后，即可从索引表中查询到数据。
覆盖索引（Covered Indexes）	支持索引表中带有属性列。在创建数据表时预先定义一些列（称为预定义列）后，可以对任意预定义列和数据表主键列进行索引，指定数据表的若干个预定义列作为索引表属性列。索引表中也可以不包含任何属性列。 当指定数据表的若干个预定义列作为索引表属性列时，读取索引表可以直接得到数据表中对应预定义列的值，无需反查数据表。

存量索引	支持新建的索引表中包含数据表中的存量数据。
稀疏索引（Sparse Indexes）	如果数据表的某个预定义列作为索引表的属性列，当数据表某行中不存在该预定义列时，只要索引列全部存在，仍会为此行建立索引。但是如果部分索引列缺失，则不会为此行建立索引。

- 多元索引

  多元索引（Search Index）基于倒排索引和列式存储，可以解决大数据的复杂查询难题，包括非主键列查询、全文检索、前缀查询、模糊查询、多条件组合查询、嵌套查询、地理位置查询和统计聚合（max、min、count、sum、avg、distinct_count、group_by、percentiles和histogram）等功能。

功能	描述
多元索引管理	创建多元索引后，您可以查询多元索引描述信息、查询多元索引列表以及删除多元索引。
生命周期管理	数据生命周期（Time To Live，简称TTL）是多元索引的一个属性，即数据的保存时间。多元索引会自动清理超过保存时间的数据，减少用户的数据存储空间，降低存储成本。如果数据表无UpdateRow更新写入操作，则您可以使用多元索引TTL。
日期数据类型	多元索引支持丰富的日期数据类型，您可以将数据表中整型（Integer）或者字符串（String）类型的数据在多元索引中映射为日期数据类型。当通过多元索引进行范围查询时，使用日期数据类型查询会比使用字符串类型查询更快。
数组和嵌套类型	多元索引除了提供Long、Double、Boolean、Keyword、Text、GeoPoint等基本类型外，还提供了数组类型和嵌套类型两种特殊类型。 ◦ 数组类型：数组类型属于附加类型，可以附加在Long、Double、Boolean、Keyword、Text、GeoPoint等基本类型之上。例如Long类型+数组后，即为数组长整型，该字段中可以包括多个长整型数字，查询数据时其中任何一个匹配都可以返回该行数据。 ◦ 嵌套类型（Nested）：代表嵌套文档类型。嵌套文档是指对于一行数据（文档）可以包含多个子行（子文档），多个子行保存在一个嵌套类型字段中。对于嵌套类型字段，需要指定其子行的结构，即子行中包含哪些字段以及每个字段的属性。
排序和翻页	使用多元索引查询数据时，通过预先定义排序方式或者查询时指定排序方式，您可以按照指定排列方式获取到返回数据。当返回结果行数较多时，通过使用跳转翻页或者连续翻页可以快速定位到所需数据。
分词	为Text类型的字段设置分词类型后，系统会将可分词类型的内容根据设定的分词类型分成多个词。非Text类型的字段不能设置分词类型。分词类型包括单字分词、分隔符分词、最小数量语义分词、最大数量语义分词和模糊分词。
折叠（去重）	当数据查询的结果中含有某种类型的数据较多时，可以使用折叠（Collapse）功能按照某一列对结果集做折叠，使对应类型的数据在结果展示中只出现一次，保证结果展示中类型的多样性。
全匹配查询	MatchAllQuery可以匹配所有行，常用于查询表中数据总行数，或者随机返回几条数据。
匹配查询	MatchQuery采用近似匹配的方式查询表中的数据。对Text类型的列值和查询关键词会先按照设置好的分词器做切分，然后按照切分好后的词去查询。对于进行模糊分词的列，建议使用MatchPhraseQuery实现高性能的模糊查询。

短语匹配查询	类似于MatchQuery，但是分词后多个词的位置关系会被考虑，只有分词后的多个词在行数据中以同样的顺序和位置存在时，才表示行数据满足查询条件。如果查询列的分词类型为模糊分词，则使用MatchPhraseQuery可以实现比WildcardQuery更快的模糊查询。
精确查询	TermQuery采用完整精确匹配的方式查询表中的数据，类似于字符串匹配。对于Text类型字段，只要分词后有词条可以精确匹配即可。
多词精确查询	类似于TermQuery，但是TermsQuery可以指定多个查询关键词，查询匹配这些词的数据。多个查询关键词中只要有一个词精确匹配，该行数据就会被返回，等价于SQL中的In。
前缀查询	PrefixQuery根据前缀条件查询表中的数据。对于Text类型字段，只要分词后的词条中有词条满足前缀条件即可。
范围查询	RangeQuery根据范围条件查询表中的数据。对于Text类型字段，只要分词后的词条中有词条满足范围条件即可。
通配符查询	通配符查询中，要匹配的值可以是一个带有通配符的字符串，目前支持星号（*）和半角问号（?）两种通配符。要匹配的值中可以用星号（*）代表任意字符序列，或者用半角问号（?）代表任意单个字符，且支持以星号（*）或半角问号（?）开头。
多条件组合查询	BoolQuery查询条件包含一个或者多个子查询条件，根据子查询条件来判断一行数据是否满足查询条件。每个子查询条件可以是任意一种Query类型，包括BoolQuery。
嵌套类型查询	NestedQuery用于查询嵌套类型字段中子行的数据。嵌套类型不能直接查询，需要通过NestedQuery包装，NestedQuery中需要指定嵌套类型字段的路径和一个子查询，其中子查询可以是任意Query类型。
地理距离查询	GeoDistanceQuery根据一个中心点和距离条件查询表中的数据，当一个地理位置点到指定的中心点的距离不超过指定的值时，满足查询条件。
地理长方形范围查询	GeoBoundingBoxQuery根据一个长方形范围的地理位置边界条件查询表中的数据，当一个地理位置点落在给出的长方形范围内时满足查询条件。
地理多边形范围查询	GeoPolygonQuery根据一个多边形范围条件查询表中的数据，当一个地理位置点落在指定的多边形范围内时满足查询条件。
列存在性查询	ExistsQuery也叫NULL查询或者空值查询，一般用于判断稀疏数据中某一行的某一列是否存在。例如查询所有数据中address列不为空的行。
统计聚合	使用统计聚合功能可以实现求最小值、求最大值、求和、求平均值、统计行数、去重统计行数、百分位统计、按字段值分组、按范围分组、按地理位置分组、按过滤条件分组、直方图统计、获取统计聚合分组内的行、嵌套查询等；同时多个统计聚合功能可以组合使用，满足复杂的查询需求。
并发导出数据	多元索引中提供了Search接口，Search接口支持全功能集，包括所有的查询功能，以及排序、统计聚合等分析能力，其结果会按照指定的顺序返回。 但是在有些场景中，例如对接计算系统Spark、Presto等或者一些圈选场景，只需要使用完整的查询能力，能将命中的数据以更快的速度全部返回，不关心整个结果集的顺序。为了支持此类需求，多元索引中提供了ParallelScan接口。 ParallelScan接口相对于Search接口，保留了所有的查询功能，但是舍弃了排序、统计聚合等分析功能，带来了5倍以上的性能提升，因此可以实现1分钟内上亿级别数据行的导出能力，导出能力可以水平扩展，不存在上限。

虚拟列	虚拟列功能支持用户在创建多元索引的时候将表中一列映射到多元索引中的虚拟列。新的虚拟列类型可以不同于表中的原始列类型，以便支持用户在不修改表结构和数据的情况下新建一列，新的列可以用于查询加速或者采用不同的分词器。 ◦ 一个Text字段支持不同的分词器：单个字符串列可以映射到多元索引多个Text列，不同Text列采用不同的分词，以便满足不同的业务需求。 ◦ 查询加速：不对表中数据做清洗和重建，只需要将相应列映射为其他类型，即可在部分场景下提升查询性能。例如数字类型转换为Keyword类型可以提高精确查询（TermQuery）的性能，String类型转换为数字类型可以提高范围查询（RangeQuery）的性能。
动态修改schema	表格存储数据表是schema free的，而多元索引是强schema的。创建多元索引时，您需要指定添加到多元索引中的列，这样使用多元索引查询数据时才能查询到这些列。通过动态修改多元索引的schema，您可以在多元索引中新增、更新或者删除索引列，修改多元索引的路由键等。
模糊查询	请根据查询场景选择合适的方式实现模糊查询。 ◦ 对于通配符查询中查询模式为*word*的场景，例如通过"123" 匹配手机号码中任意位置包含123的号码，请使用模糊分词方式来实现模糊查询。 ◦ 对于其他复杂查询场景，请使用通配符查询方式来实现模糊查询。

日志服务SLS

日志服务SLS（Log Service）是针对日志类数据的一站式服务，在阿里巴巴集团经历大量大数据场景锤炼而成。用户无需开发就能快捷完成日志数据采集、加工、消费以及查询分析等功能，提升运维、运营效率，建立DT时代海量日志处理能力。

功能特性	说明
实时采集与消费（LogHub）	LogHub支持客户端、网页、协议、SDK/API（移动、游戏）等多种日志无损采集方式和SDK、Storm Spout、Spark Client等消费方式，支持多种格式日志的实时采集和消费，协助用户实现多设备、多来源的日志采集消费流程化处理。
查询与实时分析（Search/Analytics）	针对采集到服务端的日志数据进行实时索引、查询分析，并根据查询分析结果建立动态的数据报表，支持多场景的日志数据可视化分析。
告警管理	支持为查询和分析结果设置告警。设置告警后，日志服务定期检查查询和分析结果，当检查结果满足预设条件时发送告警通知，实现实时的服务状态监控。
Scheduled SQL	提供Scheduled SQL功能，用于定时分析数据、存储聚合数据、投影与过滤数据。本文介绍Scheduled SQL功能的背景信息、功能简介、基本概念、调度与执行场景、使用建议等信息。
数据加工	提供可托管、可扩展、高可用的数据加工服务。数据加工服务可用于数据的规整、富化、流转、脱敏和过滤。
时序存储	提供数据接入、查询与分析、可视化等功能。

混合云容灾

混合云容灾HDR产品详情如下：

- 解决的核心问题

  应用级容灾保障业务持续性（Business Continuity）：在数据中心故障或长时间系统维护作业时，在容灾站点快速恢复应用运行，缩短业务停机时间，极大减少损失。利用混合云容灾服务的服务器整机复制能力，您可以方便地跨可用区进行ECS容灾，无需重构。

- 支持的业务类型

  为企业关键应用提供高标准容灾方案，提供秒-分级的RPO和RTO容灾。

10.1.2. 产品价值

CDS具有部署形态灵活、高性能、高可靠性等优势。CDS中部署不同的云服务时，云服务也具有各自的优势。

整体优势

部署形态灵活

以云服务的方式定义存储，用户可以灵活选择融合部署或者分离部署不同服务，支持动态灵活扩容。

高性能

- 通过整合所有存储节点的资源（例如CPU、硬盘等），实时动态均匀分配数据存储以及处理任务，实现并发数据处理，避免了单点故障造成的瓶颈，提升整个集群的处理能力。
- 存储集群具有良好的性能扩展能力，能满足应用程序不断增长的存储性能需求。

高可靠性

存储集群采用纠删码机制，将数据分块存储在不同机架的不同机器上，并会在数据块异常时进行快速恢复。

高可用性

- 存储集群采用全冗余架构，无单点故障。通过自动的故障检测和数据迁移，对应用屏蔽了机器和网络的硬件故障，提供高可用性。
- 存储集群采用纠删码机制，在保证一定数据冗余情况下，有效提升了存储集群的空间利用率。

高扩展性

通过扩展存储集群、增加和升级存储集群中的服务器硬件、增加存储集群中的存储节点数量等多种方式提升集群的服务能力。存储集群可支持在线平滑升级，动态增加或者删除存储节点以及进行集群热升级，不需要停机维护，数据可以自动迁移。

访问安全性

提供多种权限管理机制，并对应用的每一次请求都进行身份认证和鉴权，以防止未授权的数据访问，确保数据访问的安全性。

管理便捷

- 应用程序无需关心数据分区的管理、软硬件升级、配置更新、集群扩容等繁琐的运维任务。
- 支持将审计日志自动存储到日志存储服务中，并可通过日志存储服务下载日志，便于长期存储、管理审计日志信息。
- 通过CDS Ops统一运维平台对存储集群以及运行在存储集群上的对象存储服务、日志存储服务、块存储EBS等进行日常运维管理。

对象存储OSS优势

OSS与自建存储对比的优势

对比项	对象存储OSS	自建服务器存储
可靠性	• 数据自动多重冗余备份。 • 支持硬盘级，节点级、机柜级和集群级别故障。最大支持2个节点损坏，可以实现业务不中断持续提供数据读写操作。	• 受限于硬件可靠性，易出问题，一旦出现磁盘坏道，容易出现不可逆转的数据丢失。 • 人工数据恢复困难、耗时、耗力。

安全	• 提供企业级多层次安全防护。 • 多用户资源隔离机制。 • 提供多种鉴权和授权机制，以及白名单、防盗链、主子账号、STS临时授权访问功能。	• 需要另外购买清洗和黑洞设备。 • 需要单独实现安全机制。
数据处理能力	提供图片处理功能。	需要额外采购，单独部署。

OSS的其他优势

- 方便、快捷的使用方式
  - 提供标准的RESTful API接口（部分接口与Amazon S3 API兼容）、丰富的SDK包、客户端工具、控制台。您可以像使用文件一样方便地上传、下载、检索、管理用于Web网站或者移动应用的海量数据。
  - 支持流式写入和读出。特别适合视频等大文件的边写边读业务场景。
  - 支持数据生命周期管理。您可以自定义将到期数据批量删除。
  - 提供超大的存储空间：您可以通过增加节点数量扩展存储空间。对象存储OSS单Bucket存放文件数量无上限，实测存放万亿小文件，读写性能无损失。
- 强大、灵活的安全机制

  灵活的鉴权、授权机制。提供STS和URL鉴权和授权机制，以及白名单、防盗链、主子账号功能。
- 丰富的图片处理服务

  支持JPG、PNG、BMP、GIF、WebP、TIFF等多种图片格式的转换，以及缩略图、剪裁、水印、缩放等多种操作。

块存储EBS优势

块存储提供了基于分布式存储架构的弹性块存储产品。

弹性块存储产品为ECS实例提供数据块级别的随机存储，具有低时延、持久性、高可靠等特点，采用三副本的分布式机制，为ECS实例提供数据可靠性保证。可以随时创建或释放，也可以随时扩容。

弹性块存储支持在不停止业务运行的情况下进行在线扩容，包括系统盘和数据盘。在扩容期间，用户无需停止ECS实例，也无需卸载云盘。

表格存储Tablestore优势

扩展性

- 表格存储中表的数据量没有上限，随着表数据量的不断增大，表格存储会进行数据分区的调整从而为该表配置更多的存储并提供更高的并发访问能力。
- 在不影响运行性能的前提下，支持单组件集群中使用的CPU，硬盘、内存、网卡规格不一致，可以最大限度地兼容已有设备。

高性能

高性能实例能够提供单个毫秒级的单行平均访问延时，读写性能不受单表数据大小的影响。

数据可靠性

- 表格存储通过存储多个数据备份及备份失效时的快速恢复，提供极高的数据可靠性。
- 支持对集群内服务器硬盘故障自动容错处理，支持硬盘热插拔，故障硬盘的业务恢复时间小于1分钟。
- 支持对数据进行备份，支持全量或增量备份，并支持从存储中恢复数据。
- 支持数据中心间的数据集群备份，满足多中心之间的数据互备需求，备份过程可视化管理。
- 支持对关键组件元数据、文件、表进行备份和恢复。

高可用性

通过自动的故障检测和数据迁移，表格存储对应用屏蔽了机器和网络的硬件故障，提供高可用性。

管理便捷

- 应用程序无需关心数据分区的管理、软硬件升级、配置更新、集群扩容等繁琐的运维任务。
- 支持将审计日志自动存储到日志服务中，并可通过日志服务下载日志，便于长时间存储、管理审计日志信息。

访问安全性

- 表格存储提供多种权限管理机制，并对应用的每一次请求都进行身份认证和鉴权，以防止未授权的数据访问，确保数据访问的安全性。
- 支持数据访问权限管理，包括登录权限、创建表权限、读写权限、白名单控制权限等。
- 支持通过云管平台管理权限控制，包括管理员分级等；通过云管平台，提供集中统一的用户权限管理功能，将系统中各组件零散的权限管理功能集中呈现和管理，对普通用户屏蔽掉内部的权限管理细节，对管理员简化权限管理的操作方法，提升权限管理的易用性和用户体验。

强一致性

表格存储保证数据写入强一致，写操作一旦返回成功，保证数据3副本均写入磁盘，并且应用就能立即读到最近更新的数据。

灵活的数据模型

表格存储的表无固定格式要求，每行的列数可以不相同，支持多种数据类型（Integer、Boolean、Double、String、Binary）。

多元化数据索引

除了支持主键查询，表格存储还支持二级索引和多元索引的索引方式，提供强大的数据查询能力。

- 二级索引：相当于给数据表提供了另外一种排序方式，即对查询条件预先设计了一种数据分布，可加快数据查询的效率。
- 多元索引：基于倒排索引和列式存储，支持多字段自由组合查询、模糊查询、地理位置查询、全文检索等，可解决大数据的复杂查询难题。

监控集成

用户可以从表格存储控制台实时获取每秒请求数、平均响应延时等监控。

多租户

- 隔离：支持多租户并行执行，租户任务提交到不同的队列执行，租户间资源隔离。
- 权限：支持通过控制台，实现的租户统一管理，实现租户资源的动态配置和管理，资源隔离，资源使用统计等功能，支持多级租户的管理功能。
- 调度：支持多集群和多资源池的多租户调度。

日志服务SLS优势

全托管服务

- 应用性强，简单快速即可接入服务进行使用。
- LogHub 覆盖 Kafka 全部功能，提供监控、报警等功能数据，并支持弹性伸缩（可支持PB/Day规模）。
- LogSearch/Analytics 提供快速查询、仪表盘和报警功能。
- 提供超过30种接入方式，与开源软件（Storm、Spark）无缝对接。

生态丰富

- LogHub支持30多种日志数据源，无论是嵌入式设备、网页、服务器、程序等都能轻松接入。在消费端，支持与Storm、Spark Streaming等对接。
- LogSearch/Analytics 查询分析语法完整，兼容SQL92，支持JDBC协议与对接Grafana。

实时性强

- LogHub：写入即可消费；Logtail（采集Agent）实时采集传输。
- LogSearch/Analytics：写入后3秒内即可进行查询分析，在千亿数据规模多个查询分析条件下实现数据的秒级查询结果返回。

高吞吐

日志服务具备高吞吐特性，通过日志服务软件优化，单机吞吐性能可参考如下：

- 数据写入：单机原始日志写入最高可达400 MB/s以上，索引日志写入最高可达150 MB/s以上。
- 实时消费：实时消费最高可达400 MB/s以上。
- QPS：单机QPS最高可达1万以上。

> **说明** 单机吞吐性能，根据硬件不同存在波动。

弹性

提供PB级别数据弹性伸缩能力。

混合云容灾

简单易用

- 容灾站点部署简单、控制台集中管控。
- 可按需进行故障切换和容灾演练，一键启动、快速清理。

RPO/RTO分级

企业需要对重要性级别不同的应用制定阶梯化的RPO/RTO。企业的基础架构，尤其是网络情况会制约能达到的容灾指标。

- 基于磁盘级实时数据复制技术，可以提供秒级-分钟级的RPO/RTO。
- 混合云大数据容灾提供近0 RPO的大数据容灾。

跨可用区容灾

- 支持将Windows、Linux应用服务器做高效的容灾复制和恢复，实现应用级跨可用区容灾。
- 您可以只针对关键应用的数据，包括SQL Server、Oracle数据库等进行定时备份和恢复，实现数据级跨可用区容灾。

10.1.3. 应用场景

CDS能为不同领域的企业用户提供低成本、安全可靠的一体化存储解决方案。企业用户可以通过在CDS中部署不同服务来满足不同场景的需求。

对象存储OSS

图片和音视频等应用的海量存储

OSS可用于图片、音视频、日志等海量文件的存储。各种终端设备、Web网站程序、移动应用可以直接向OSS写入或读取数据。OSS支持流式写入和文件写入两种方式。

离线数据归档存储

根据OSS低成本和高可用的特性，可以将企业内部长期需要离线归档的数据转存至OSS。

数据多地容灾

您存储的数据可以通过跨区域复制或跨云复制等能力实现两个集群或两个云系统之间的数据异步（近实时）复制，帮助您实现两地三中心的技术架构、多地数据容灾备份，使您可以在极端灾难中保证业务流畅。

块存储EBS

块存储EBS（Elastic Block Storage）是为云服务器ECS提供的低时延、持久性、高可靠的块级随机存储。块存储提供了基于分布式存储架构的弹性块存储产品。弹性块存储产品根据是否可挂载到多台ECS实例分为云盘和共享云盘。

云盘

云盘根据性能不同分为普通性能云盘和高性能云盘，高效云盘和SSD云盘。

- 普通性能云盘和高性能云盘面向OLTP数据库（例如MySQL、PostgreSQL、Oracle、SQL Server等关系型数据库）、NoSQL数据库（例如MongoDB、HBase、Cassandra等非关系型数据库）、ElasticSearch分布式日志（ELK，即ElasticSearch、Logstash和Kibana日志分析等）场景，高性能云盘为ECS实例提供最高25000的随机IOPS性能。
- 高效云盘面向中度I/O负载的应用场景，为ECS实例提供最高3000的随机IOPS性能，可用作系统盘。
- SSD云盘为I/O密集型应用提供稳定的高随机IOPS性能，适用于对数据可靠性要求高的中小型开发测试环境。

表格存储Tablestore

场景一：海量数据存储与分析

表格存储提供低成本、高并发、低延时的海量数据存储与在线访问，提供增量以及全量数据通道并支持MaxCompute等大数据分析平台的SQL直读直写，高效的增量流式读接口让数据轻松完成实时流计算。

- 支持多种大数据计算平台、流计算以及实时计算服务。
- 提供高性能与容量型两种规格的实例，满足不同的业务需要。

场景二：互联网社交Feed流

使用表格存储来存储大量的IM聊天、以及评论、跟帖和点赞等社交Feed流信息，表格存储的弹性资源能够以较低的成本满足访问波动明显大并发低延时的需要。

- 内置PK自增列，简化外部系统依赖。
- 高性能实例平均读写性能不受数据量大小影响。
- 高可靠的海量消息存储，消息多终端同步。

场景三：海量交易记录与用户模型的存储和实时查询

低延时、高并发，弹性资源让用户的风控系统永远工作在最佳状态，牢牢控制交易风险，灵活的数据结构能够让业务模式跟随市场需求快速迭代。

- 轻松存储全量历史交易记录。
- 3副本强一致保证数据安全。
- Schemafree模型，属性列字段随用随加，适应业务快速发展。

场景四：海量、高效、灵活的车联网数据存储

无需分库分表，简化业务逻辑，Schemafree数据模型轻松接入不同车辆设备的监控数据。与多种大数据分析平台、实时计算服务等无缝结合，轻松完成实时在线查询以及业务报表分析。

- 无需分库分表，简化业务逻辑。
- 车况、轨迹查询性能稳定可预期。
- Schemafree数据模型轻松接入不同车辆设备的监控数据。

场景五：海量物联网数据存储，高效的查询与分析

表格存储轻松满足IoT设备、监控系统等时序数据的存储需求，大数据分析SQL直读以及高效的增量流式读接口让数据轻松完成离线分析与实时流计算。

- 满足超大规模IoT设备、监控系统的数据写入与存储需求。
- 对接多种离线、流式数据分析平台，一份数据同时满足不同业务的分析计算场景。
- 支持数据生命周期管理。

场景六：海量电商交易订单与用户推荐数据库

大量的历史交易订单使用表格存储让用户无需担心数据规模与访问性能，配合大数据计算服务，轻松实现精准营销，弹性资源，让用户从容应对所有用户在线高峰时刻。

- 数据规模与访问并发自动扩展，满足波峰波谷各个时段的访问需求。
- 支持多种大数据分析平台直接分析用户行为。
- 海量交易订单毫秒级的查询延时。

日志服务SLS

日志服务的典型应用场景，包括数据采集、实时计算、数仓与离线分析、产品运营与分析、运维与管理。

数据采集与消费

通过日志服务LogHub功能，可以大规模低成本接入各种实时日志数据（包括Metric、Event、BinLog、TextLog、Click等）。

- 使用便捷：提供30+实时数据采集方式，让您快速搭建平台、减轻运维负担。
- 弹性伸缩：无论是流量高峰还是业务增长都能轻松应对。

数据清洗与实时计算（ETL/Stream Processing）

日志中枢（LogHub）支持与各种实时计算及服务对接，并提供完整的进度监控、报警等功能，并可以根据SDK/API实现自定义消费。

- 操作便捷：提供多种语言的SDK以及编程框架，与各流计算引擎无缝对接。
- 功能完善：支持报警机制，并提供丰富的监控数据。
- 弹性伸缩：PB级弹性能力，0延迟。

日志实时查询与分析

实时查询分析（LogAnalytics）可以实时索引LogHub中数据，提供关键词、模糊、上下文、范围、SQL聚合等丰富查询手段。

- 实时性强：写入后即可查询。
- 海量低成本：支持PB/Day索引能力，成本为自建方案的15%。
- 分析能力强：支持多种查询手段，及SQL进行聚合分析，并提供可视化及报警功能。

混合云容灾

跨可用区容灾

混合云容灾服务支持业务的跨可用区（Zone）容灾能力，应对不同的业务需求，当生产站点发生故障时，业务系统切换到容灾站点，有效避免了地域性灾害导致的系统故障，保障业务的可用性，满足业务的RTO/RPO核心指标。

10.2. 文件存储NAS

阿里云文件存储NAS（Apsara File Storage NAS）是面向阿里云ECS实例、E-HPC和容器服务等计算节点的文件存储服务。它是一种可共享访问、弹性扩展、高可靠以及高性能的分布式文件系统。

创建NAS文件系统实例和挂载点后，即可在ECS、容器服务等计算节点内通过标准的NFS协议挂载文件系统，并使用标准的POSIX接口对文件系统进行访问。多个计算节点可以同时挂载同一个文件系统，共享文件和目录。NAS文件系统支持集群内海光服务器和Intel服务器的混部。

10.2.1. 产品详情

NAS提供简单可扩展文件存储以供与ECS配合使用，多个ECS实例可以同时访问NAS文件系统，并且存储容量会随着用户添加和删除文件而自动弹性增长和收缩，为在多个实例或服务器上运行产生的工作负载和应用程序提供通用数据源。

文件系统管理

文件系统是文件存储NAS为客户业务提供存储文件的地方，通过计算节点挂载访问。以传统的目录树形式管理文件的数据和元数据。支持数百个计算节点同时访问，进行数据共享和高并发读写。

用户可以通过NAS控制台管理用户账号下的文件系统，包括创建、删除文件系统及查询文件系统详情。

在文件系统详情页面展示了文件系统的基本信息，包括文件系统ID、区域、文件系统容量等信息。

挂载点管理

挂载点是文件系统实例在专有网络或经典网络内的一个访问目标地址，每个挂载点都对应一个域名，用户mount时通过指定挂载点的域名来挂载对应的NAS文件系统到本地。用户可以通过NAS控制台查看文件系统挂载点，修改挂载点状态及挂载点权限组。

权限组

权限组是NAS提供的白名单机制，通过向权限组内添加规则来允许IP地址或网段以不同的权限访问文件系统。每个挂载点都必须与一个权限组绑定。

统一命名空间

统一命名空间构建了一个虚拟的根目录，其中的文件系统就是它的一级子目录。通过统一命名空间，在操作多个文件系统时，用户可以获得和单个文件系统一致的使用体验，节省维护时间。用户可以通过NAS控制台创建统一命名空间及挂载点，并向统一命名空间添加、移除和修改文件系统、查看统一命名空间详情，实现统一命名空间跨域编排的功能。

生命周期管理

生命周期管理功能可以帮助用户管理NAS上数据的冷热分离，通过配置生命周期策略，用户可以将长时间没有访问的文件，自动保存到低频 （IA）介质存储容量。低频（IA）介质存储容量的成本更低，通过将冷数据转存到低频（IA）介质存储容量，可以降低这部分存储量的成本。在低频（IA） 介质存储容量保存的数据，依然按照原有的方式进行访问。

权限控制和ACL隔离

NAS文件系统支持目录级读写权限ACL。用户可以为文件或目录配置ACL，实现细粒度的目录极读写权限管理。针对不同目录或文件，文件系统管理员需要给不同的用户和群组设置相应的权限，实现访问隔离。

审计日志

NAS支持日志审计功能，实时记录与文件系统实例操作的相关日志，可以用于故障的调查和分析。

10.2.2. 产品价值

与传统存储此相比，文件存储NAS具有多共享、高可靠、多芯片支持、弹性伸缩优势。

多共享

同一个文件系统可以同时挂载到多个计算节点上，共享访问，节约大量拷贝和同步成本。

高可靠

提供高数据可靠性，相比自建NAS存储，可以大量节约维护成本，降低数据安全风险。

弹性伸缩

文件系统容量可以弹性扩展或缩减，轻松应对业务的随时扩容和缩容。

易用性

支持NFSv3（Linux）、NFSv4（Linux）、SMB2.1（Windows）和SMB3.0（Windows），无论是在ECS实例内，还是在容器服务等计算节点中，都可通过标准的POSIX接口对文件系统进行访问操作。

多芯片支持

支持集群内海光服务器和Intel服务器的混部。

10.2.3. 应用场景

文件存储NAS适用于负载均衡共享存储和高可用、企业办公文件共享、数据备份及服务器日志共享等场景。

负载均衡共享存储和高可用

在负载均衡SLB连接多个ECS实例的场景中，建议将这些ECS实例上的应用的数据存放在共享的文件存储NAS上，实现数据共享和负载均衡服务器高可用。

企业办公文件共享

如果企业员工办公需要访问和共享相同的数据集，建议管理员创建NAS文件系统，为组织中的个人提供数据访问，并设置文件或目录级别的用户和用户组权限。

数据备份

如果用户希望将线下机房的数据备份到云上，同时要求云上的存储服务兼容标准的文件访问接口，建议使用NAS文件系统备份机房的数据。

服务器日志共享

如果用户希望将多个计算节点上的应用服务器日志存放在共享的文件存储上，建议使用NAS文件系统存储这些服务器日志，方便日志的集中处理与分析。

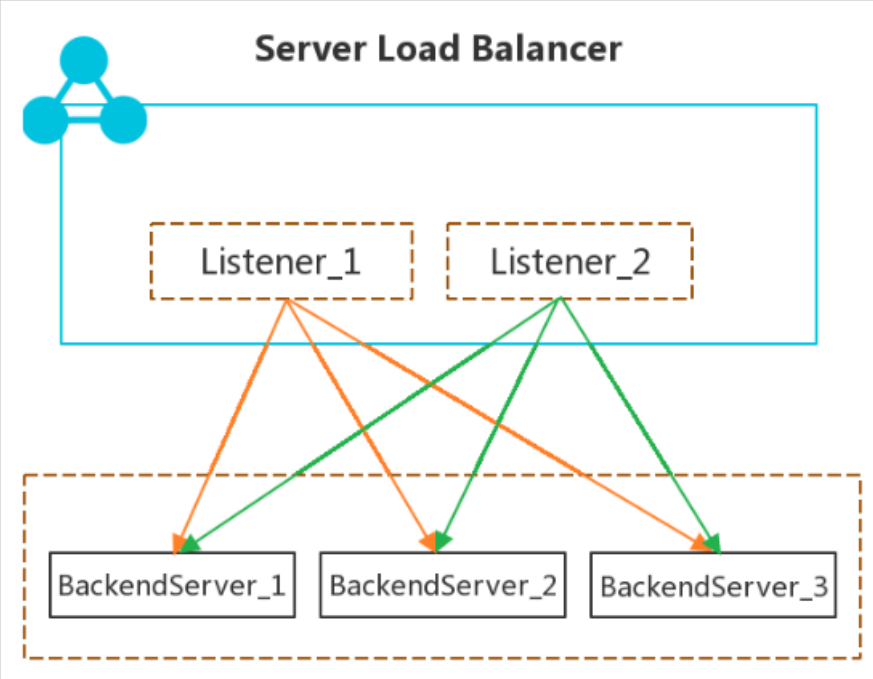
11.网络服务

11.1. 负载均衡

负载均衡SLB（Server Load Balancer）是将访问流量根据转发策略分发到后端多台云服务器（ECS实例）的流量分发控制服务。负载均衡扩展了应用的服务能力，增强了应用的可用性。

11.1.1. 产品详情

负载均衡由负载均衡实例、监听和后端服务器三部分组成。



负载均衡实例 （Instances）

一个负载均衡实例是一个运行的负载均衡服务，用来接收流量并将其分配给后端服务器。要使用负载均衡服务，用户需要创建一个负载均衡实例，并至少添加一个监听和两台ECS实例。

监听 （Listeners）

监听用来检查客户端请求并将请求转发给后端服务器。监听也会对后端服务器进行健康检查。

后端服务器（Backend Servers）

后端服务器是一组接收前端请求的ECS实例。用户可以单独添加ECS实例到后端服务器池，也可以通过虚拟服务器组或主备服务器组来批量添加和管理。

11.1.2. 产品价值

负载均衡具有高可用、可扩展、低成本、安全和高并发的优势。同时，本文从负载均衡、单负载均衡实例、多负载均衡实例和后端ECS实例四个方面阐述了高可用优势。

高可用

采用全冗余设计，无单点，支持同城容灾。根据应用负载进行弹性扩容，在流量波动情况下不中断对外服务。

对象	高可用优势说明
负载均衡	负载均衡实例采用集群部署，可实现会话同步，以消除服务器单点故障，提升冗余，保证服务的稳定性。其中四层负载均衡通过LVS（Linux Virtual Server）联合keepalived的方式实现，七层负载均衡通过Tengine（淘宝网发起的Web服务器项目，在Nginx的基础上，针对有大访问量的网站需求进行了优化）实现。 来自公网的请求通过等价多路径路由ECMP（Equal-Cost Multipath Routing）到达LVS集群。LVS集群内的每台LVS通过组播报文将会话同步到该集群内的其它LVS机器上，从而实现LVS集群内各台机器间的会话同步。同时，LVS集群会对Tengine集群进行健康检查。负载均衡将状态异常的设备从Tengine集群移除，保证七层负载均衡的可用性。
单负载均衡实例	阿里云允许用户在多个地域创建多可用区来实现单负载均衡实例的高可用。当主可用区出现故障或不可用时，负载均衡有能力在非常短的时间内（约30秒）切换到备可用区并恢复服务；当主可用区恢复时，负载均衡同样会自动切换到主可用区提供服务。
多负载均衡实例的高可用	如果用户对可用性的要求特别高，负载均衡实例自身的可用性保障机制可能无法满足用户的需求。例如当网络攻击或配置错误等情况导致负载均衡实例不可用时，由于未出现可用区级故障，不会触发负载均衡实例的可用区切换。此时，用户可以创建多个负载均衡实例，通过云解析DNS对访问进行调度，或通过全球负载均衡解决方案实现跨地域容灾备份。
后端ECS实例的高可用	负载均衡通过健康检查来判断后端ECS实例的可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。 开启健康检查功能后，当后端某个ECS实例健康检查出现异常时，负载均衡会自动将新的请求分发到其他健康检查正常的ECS实例上，而当该ECS实例恢复正常运行时，负载均衡会将其自动恢复到负载均衡服务中。关于健康检查的详细机制的更多信息，请参见用户指南中的健康检查概述。

可扩展

根据业务的需要，用户可以随时增加或减少后端服务器的数量，扩展应用的服务能力。

低成本

与传统硬件负载均衡系统高投入相比，成本可下降60%。

安全

结合云盾安全产品，可提供DDoS攻击防护能力。

高并发

集群支持亿级并发连接，单实例提供千万级并发能力。

11.1.3. 应用场景

负载均衡SLB（Server Load Balancer）产品适用于高访问量、扩展应用程序、消除单点故障、同城和跨地域容灾的场景。

应用于高访问量的业务

如果应用访问量很高，用户可以通过配置监听规则将流量分发到不同的ECS实例上。此外，用户可以使用会话保持功能将同一客户端的请求转发到同一台后端ECS，提高访问效率。

扩展应用程序

用户可以根据业务发展的需要，随时添加和移除ECS实例来扩展应用系统的服务能力，适用于各种Web服务器和App服务器。

消除单点故障

用户可以在负载均衡实例下添加多台ECS实例。当其中一部分ECS实例发生故障后，负载均衡会自动屏蔽故障的ECS实例，将请求分发给正常运行的ECS实例，保证应用系统仍能正常工作。

同城容灾 （多可用区容灾）

为了提供更加稳定可靠的负载均衡服务，用户可以在多个地域创建多可用区以实现同地域容灾。当某一个地域的主可用区出现机房故障或不可用时，负载均衡仍然有能力在非常短的时间内（大约30s中断）切换到同一地域的另外一个备可用区恢复服务能力；当主可用区恢复时，负载均衡同样会自动切换到主可用区提供服务。建议用户结合自身的应用需要，综合考虑后端服务器的部署。如果每个可用区均至少添加了一台ECS实例，那么此种部署模式下的负载均衡服务的效率是比较高的。

在负载均衡实例下绑定不同可用区的ECS实例。正常情况下，用户访问流量将同时转发至主、备可用区内的ECS实例；当可用区A发生故障时，用户访问流量将只转发至备可用区内的ECS实例。此种部署既可以避免因为单个可用区的故障而导致对外服务的不可用，也可以通过不同产品间可用区的选择来降低延迟。

跨地域容灾

用户可以在不同地域下部署负载均衡实例，并分别挂载相应地域内不同可用区的ECS。上层利用云解析做智能DNS，将域名解析到不同地域的负载均衡实例服务地址下，可实现全局负载均衡。当某个地域出现不可用时，暂停对应解析即可实现所有用户访问不受影响。

11.2. 专有网络

专有网络是用户自己独有的云上私有网络。专有网络为云上的资源提供网络服务，不同专有网络间逻辑隔离。用户可以掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等。用户也可以在自己定义的专有网络中使用阿里云资源如云服务器ECS（Elastic Compute Service）、云数据库RDS（Relational Database Service）和负载均衡等。

11.2.1. 产品详情

专有网络VPC（Virtual Private Cloud）是用户自己独有的云上私有网络，是一个隔离的网络环境，专有网络之间逻辑上彻底隔离。用户可以掌控自己的专有网络也可以在自己定义的专有网络中使用阿里云资源。

专有网络

每个专有网络都由一个私网网段、至少一个路由器和至少一个交换机组成。

- 私有网段：在创建专有网络和交换机时，用户需要以CIDR地址块的形式指定专有网络使用的私网网段。用户可以使用下表中标准的私网网段及其子网作为专有网络的私网网段。

网段	可用私网IP数量 （不包括系统保留地址）
192.168.0.0/16	65,532
172.16.0.0/16	65,532

- 路由器（vRouter）：专有网络的枢纽。作为专有网络中重要的功能组件，它可以连接专有网络内的各个交换机，同时也是连接专有网络和其他网络的网关设备。每个专有网络创建成功后，系统会自动创建一个路由器，每个路由器关联一张路由表。
- 交换机（vSwitch）：组成专有网络的基础网络设备，用来连接不同的云资源。创建专有网络后，用户可

以通过创建交换机为专有网络划分一个或多个子网。同一专有网络内的不同交换机之间内网互通。用户可以将应用部署在不同可用区的交换机内，提高应用的可用性。

自定义路由表和路由条目

创建专有网络后，系统会默认创建一个路由表控制专有网络的路由，所有专有网络内的交换机默认使用该路由表。用户不能创建也不能删除系统路由表，但用户可以在专有网络内创建自定义路由表，将自定义路由表和交换机绑定来控制子网路由，更灵活地进行网络管理。

用户可以在专有网络的路由表（系统路由表和自定义路由表）中添加自定义路由，将流量转发到目标下一跳。路由表中采用最长前缀匹配作为流量的路由选路规则。最长前缀匹配是指IP网络中当路由表中有多条路由条目可以匹配目的IP时，采用掩码最长（最精确）的一条路由作为匹配项并确定下一跳。

高可用虚拟IP

高可用虚拟IP（High-Availablility Virtual IP Address，简称HaVip）是一种可以独立创建和释放的私网IP资源。HaVip可以与高可用软件（例如keepalived）配合使用，搭建高可用主备服务，提高业务的可用性。例如，ECS实例除了可以拥有主私网IP地址外，还可以绑定高可用虚拟IP，以获得多个私网IP地址。

网络ACL

网络ACL（Network Access Control List）是专有网络中的网络访问控制功能。用户可以自定义设置网络ACL规则，并将网络ACL与交换机绑定，实现对交换机中云服务器ECS实例的流量的访问控制。

多种连接方式

阿里云提供多种连接方式，用户可以将专有网络连接到互联网、用户的本地数据中心或其他专有网络：

- 连接到互联网

  用户可以通过绑定弹性公网IP、配置NAT网关方式，将专有网络与互联网连接，使专有网络内的云服务可以和互联网通信。

- 连接到其他专有网络

  用户可以通过创建一对路由器接口连接到其他专有网络，建立高速、安全地私网通信。

- 连接到本地数据中心

  用户可以通过物理专线将本地数据中心和专有网络连接起来，将本地应用平滑迁移到云上。

11.2.2. 产品价值

专有网络VPC（Virtual Private Cloud）具有安全可靠、灵活可控、简单易用以及较强的可扩展性。

安全可靠

每个专有网络都有一个独立的隧道号，一个隧道号对应着一个虚拟化网络。专有网络之间通过隧道号进行隔离：

- 由于专有网络内部存在交换机和路由器，因此可以像传统网络环境一样划分子网。每一个子网内部的不同云服务器使用同一个交换机互联，不同子网间使用路由器互联。
- 不同专有网络之间内部网络完全隔离，可以通过对外映射的IP（弹性公网IP和NAT IP）互连。
- 由于使用隧道封装技术对云服务器的IP报文进行封装，所以云服务器的数据链路层（二层MAC地址）信息不会进入物理网络，实现了不同云服务器间二层网络隔离，因此也实现了不同专有网络间二层网络隔离。
- 专有网络内的云服务器使用安全组防火墙进行三层网络访问控制。

灵活可控

用户可以通过安全组规则、访问控制白名单等方式灵活地控制访问专有网络内云资源的出入流量。

简单易用

用户可以通过专有网络控制台快速创建并管理专有网络。专有网络创建后，系统会自动为其创建一个路由器和一张路由表。

可扩展性强

用户可以在一个专有网络内创建不同的子网，部署不同的业务。此外，用户可以将一个专有网络与本地数据中心相连或者将一个专有网络与其他专有网络相连，扩展网络架构。

11.2.3. 应用场景

专有网络VPC（Virtual Private Cloud）是完全隔离的虚拟网络环境，配置灵活，可满足不同的应用场景。

安全部署应用程序

用户可以将对外提供服务的应用程序部署在专有网络中，并且可以通过创建安全组规则、访问控制白名单等方式控制互联网访问。用户也可以在应用程序服务器和数据库之间进行访问控制隔离，将Web服务器部署在能够进行公网访问的子网中，将应用程序的数据库部署在没有配置公网访问的子网中。

部署主动访问公网的应用程序

用户可以将需要主动访问公网的应用程序部署在专有网络中的一个子网内，通过NAT网关路由其流量。通过配置SNAT规则，子网中的实例无需暴露其私网IP地址即可访问互联网，并可随时替换公网IP，避免被外界攻击。

跨可用区容灾

用户可以通过创建交换机为专有网络划分一个或多个子网。同一专有网络内不同交换机之间私网互通。用户可以通过将资源部署在不同可用区的交换机中，实现跨可用区容灾。

构建混合云

用户可以通过VPN网关、高速通道物理专线将本地数据中心和云上专有网络打通，构建混合云。然后将本地的IT基础架构无缝地扩展到阿里云上，借助阿里云海量的计算、存储、网络等资源，应对业务波动，提高应用的稳定性。通过该方式，用户可以将本地应用程序无缝地迁移至云上，并且不必更改应用程序的访问方式。

11.3. 弹性公网IP

弹性公网IP（Elastic IP Address，简称EIP）是可以独立购买和持有的公网IP地址资源。目前，EIP可绑定到专有网络类型的云服务器ECS（Elastic Compute Service）实例、专有网络类型的负载均衡SLB（Server Load Balancer）实例、辅助网卡类型的弹性网卡ENI（Elastic Network Interface）和NAT网关（NAT Gateway）上。

EIP是一种NAT IP。它实际位于阿里云的公网网关上，通过NAT方式映射到了被绑定的云资源上。和云资源绑定后，云资源可以通过EIP与公网通信。

11.3.1. 产品详情

弹性公网IP（Elastic IP Address，简称EIP）是可以独立购买和持有的公网IP地址资源。EIP和云资源绑定后，云资源可以通过EIP与公网通信。

绑定云资源

EIP支持与专有网络类型ECS实例、专有网络类型SLB实例、NAT网关、辅助弹性网卡绑定，提供访问公网和被公网访问的能力。

升配

EIP支持升级带宽峰值。升级带宽峰值后，立即生效。

解绑云资源

如果用户的云资源不再需要公网通信，可以将云资源与EIP解绑。

释放

如果用户不再需要使用EIP，可将其释放。

11.3.2. 产品价值

EIP具有可独立购买持有、弹性绑定、网络能力可配置的优势。

独立购买与持有

用户可以单独持有一个EIP，作为账号下一个独立的资源存在，无需与其它计算资源或存储资源绑定购买。

弹性绑定

用户可以在需要时将EIP绑定到需要的资源上，在不需要时将其解绑并释放。

可配置的网络能力

用户可以根据业务需要随时调整EIP的带宽峰值，带宽峰值的修改即时生效。

11.3.3. 应用场景

EIP适用于公网连接和容灾场景。

公网连接

EIP通过绑定不同的云资源，可应用于不同的公网连接场景：

- 专有网络类型ECS实例：ECS实例绑定EIP后，ECS实例可以和公网通信。
- 专有网络类型SLB实例：SLB实例绑定EIP后，SLB实例可以转发来自公网的请求。
- NAT网关：NAT网关绑定EIP后，可以使用EIP配置DNAT和SNAT条目，为多个ECS实例提供连接公网的能力。
- 辅助弹性网卡：通过绑定弹性网卡，可以构造出更健壮、更灵活、扩展性更强的IT解决方案，同时让单台服务器具备多个公网IP的能力。

容灾

用户通过部署主备系统实现容灾需求。当主服务器故障时，可以先将EIP与主服务器解绑，再绑定至备服务器，保证业务连续性。

11.4. 高速通道

阿里云高速通道（Express Connect），帮助不同网络环境间实现高速、稳定、安全的私网通信，可以避免网络质量不稳定问题，同时可以免去数据在传输过程中被窃取的风险。

11.4.1. 产品详情

阿里云高速通道（Express Connect）可在本地数据中心IDC（Internet Data Center）和云上专有网络VPC（Virtual Private Cloud）间建立高速、稳定、安全的私网通信，也可以在VPC间搭建私网通信通道，提高网络拓扑的灵活性和跨网络通信的质量和安全性。

高速通道支持位于相同地域或不同地域，同一组织或不同组织的VPC之间进行内网互通。

物理专线

高速通道提供了一种快速安全连接阿里云与本地数据中心的方法。用户可以通过租用一条运营商的专线将本地数据中心连接到阿里云接入点，建立专线连接。此连接绕过公网，更加安全可靠、速度更快、延迟更低。用户可以选择使用点对点以太网连接或MPLS VPN连接，仅支持10 Gbps单模光口实现连接。用户可以通过自主申请独享接入建立专线连接。

边界路由器

基于软件自定义网络SDN（Software Defined Network）架构下的三层Overlay技术和交换机虚拟化技术，阿里云将客户的物理专线接入的端口隔离起来，并抽象成边界路由器VBR（Virtual border router）。VBR是CPE（Customer-premises equipment）设备和VPC之间的一个路由器，作为数据从VPC到本地数据中心的转发桥梁。边界路由器同VPC中的路由器一样，同样管理一个路由表。在该路由表中配置路由条目，可以对边界路由器中的流量转发进行管理。

对等连接

用户可以在两个VPC之间，VPC与VBR之间建立对等连接。

11.4.2. 产品价值

阿里云高速通道具有高速互通、稳定可靠、安全及按需购买等价值。

高速互通

依靠阿里云的网络虚拟化技术，可以将不同网络环境连通，两侧直接进行高速内网通信，不再需要绕行公网，网络延迟低、带宽高。

稳定可靠

阿里云高速通道产品依托阿里云优质的基础设施实现，保障用户网络间通信稳定可靠。

安全

高速通道在网络虚拟化层进行网络间通信，所有通信数据在阿里云自建设施中传输，且多租户互相隔离，让用户的私密数据免去传输过程中被窃取的风险。

11.4.3. 应用场景

高速通道适用于本地IDC与云上专有网络建立可靠、安全和高速的私网通信场景。高速通道提供多种上云服务，用户可以根据业务场景进行选择，轻松构建跨架构的融合网络。

面向大中型企业的多地容灾高可用网络架构

当本地数据中心的关键业务对可用性要求极高时，建议在多个接入点建立专线连接，该拓扑确保了因光纤切断、设备故障或接入点位置故障导致的连接故障的恢复能力。

面向大型企业的高弹性、高可用网络架构

当业务规模爆发式增长，原数据中心无法满足需求时，可在云上快速部署业务，满足业务增长需求。同时使用高速通道的ECMP链路聚合功能，实现专线带宽弹性扩容，企业可以轻松面对TB级别的带宽流量。该拓扑提供了对设备故障、专线连接故障和接入点位置故障的恢复能力。

面向企业非关键业务的简单网络架构

对于不需要高弹性和高可用性的非关键业务，例如，云上搭建的开发测试环境，建议直接通过高速通道建立本地IDC和云上网络的私网连接。该拓扑结构可保证云上云下通信的安全性、可靠性。

11.5. NAT网关

NAT网关（NAT Gateway）是一款企业级的公网网关，NAT网关提供SNAT（源网络地址转换）和DNAT（目的网络地址转换）功能。具有10 Gbps级别的转发能力和跨可用区的容灾能力。

11.5.1. 产品详情

NAT网关（NAT Gateway）是一款企业级针对公网访问的安全网关产品，提供公网地址转换服务，具有10 Gbps级别的转发能力和跨可用区的容灾能力。

源网络地址转换SNAT功能

NAT网关提供SNAT（Source Network Address Translation）功能，为专有网络VPC（Virtual Private Cloud）内无公网IP的云服务器ECS（Elastic Compute Service）实例提供访问互联网的代理服务。

此外，NAT网关的SNAT功能具有安全防护的能力，只有当VPC内的ECS实例主动访问外部才可以建立连接进行通信，而外部无法主动访问VPC内的ECS实例。SNAT功能会屏蔽VPC内ECS实例对外的端口，保护VPC内的ECS实例免受外部的入侵和攻击。

目的网络地址转换DNAT功能

NAT网关支持DNAT（Destination Network Address Translation）功能，将NAT网关上的公网IP映射给ECS实例使用，使ECS实例能够提供互联网服务。

11.5.2. 产品价值

NAT网关具有灵活易用的转发能力、高性能、高可用和按需变配等产品价值。

灵活易用的转发能力

NAT网关作为一款企业级VPC公网网关，提供SNAT和DNAT功能。用户无需基于云服务器自己搭建公网网关，功能灵活、简单易用、稳定可靠。

安全防护

NAT网关的SNAT功能具有安全防护的能力，只有当VPC内的ECS实例主动访问外部才可以建立连接进行通信，而外部无法主动访问VPC内的ECS实例。SNAT功能会屏蔽VPC内ECS实例对外的端口，保护VPC内的ECS实例免受外部的入侵和攻击。

高性能

NAT网关是基于阿里云自研分布式网关，使用SDN技术推出的一款虚拟网络硬件。NAT网关支持10 Gbps级别的转发能力，为大规模公网应用提供支撑。

高可用

NAT网关跨可用区部署，可用性高。单个可用区的任何故障都不会影响NAT网关的业务连续性。

按需变配

NAT网关的规格、EIP的带宽规格和个数，均可以随时升降，轻松应对业务变化。

11.5.3. 应用场景

NAT网关适用于专有网络VPC（Virtual Private Cloud）类型的ECS实例主动访问公网和被公网访问的场景。

搭建访问公网服务的SNAT网关

用户可以创建NAT网关，并为NAT网关绑定弹性公网IP（Elastic IP Address，简称EIP），然后通过NAT网关的SNAT功能，实现VPC内的多个ECS实例共享EIP上网，节省公网IP资源。

搭建提供公网服务的DNAT网关

用户可以创建NAT网关，并为NAT网关绑定EIP，然后配置NAT网关的DNAT功能。配置成功后，VPC内的ECS实例可以通过端口映射或IP映射面向公网提供服务。

> **说明**
> - 端口映射：NAT网关会将以指定协议和端口访问EIP的请求转发到目标ECS实例的指定协议和端口上。
> - IP映射：NAT网关会将所有访问EIP的请求都转发到目标ECS实例上。

11.6. IPv6网关

IPv6网关（IPv6 Gateway）是专有网络VPC（Virtual Private Cloud）的一个IPv6流量网关。IPv6网关提供跨可用区级的高可用能力以及提供万兆级吞吐量，可为用户快速构建安全、可靠的IPv6环境。

11.6.1. 产品详情

IPv6网关（IPv6 Gateway）是专有网络VPC（Virtual Private Cloud）的一个IPv6流量网关。根据业务需要，用户可以通过配置IPv6公网带宽和仅主动出规则，灵活控制IPv6的出流量和入流量。

IPv6网关为用户提供IPv6私网通信、IPv6公网通信以及IPv6公网通信（仅主动访问互联网）。

IPv6地址

系统为VPC中的实例分配的IPv6地址。IPv6地址在二进制下长度为128位，以16位为一组，每组以“：”隔开。通常每组以4位十六进制数表示。IPv6地址的示例：2001:xxx:0102::0304。

IPv6网关

VPC环境下一个IPv6公网流量的出入口，提供IPv6公网带宽管理、仅主动出规则管理功能。

IPv6公网带宽

IPv6地址的公网带宽，决定IPv6地址是否具备公网通信能力。

IPv6地址只有开通了IPv6公网带宽，才能与互联网进行通信。

仅主动出规则

仅主动出规则是IPv6网关对IPv6公网流量的管理规则。

设置了仅主动出规则的IPv6地址将具备主动访问IPv6公网的能力，但不允许互联网IPv6终端主动对VPC中实例的IPv6地址发起连接。

VPC IPv6网段

VPC开启IPv6功能时，系统将自动为VPC分配子网掩码为/56的IPv6 网段。开通IPv6网段后，系统将为开通了IPv6网段的VPC自动创建一个免费版的IPv6网关。用户可以使用IPv6网关管理IPv6公网带宽和IPv6公网仅主动出规则。

交换机IPv6网段

交换机IPv6网段的子网掩码默认为/64。交换机开启IPv6功能时，用户可以自定义交换机IPv6网段的最后8位。

IPv6路由表

当交换机开启了IPv6网段后，系统路由表中会自动添加一条IPv6系统路由条目和一条IPv6自定义路由条目。用户可以在路由表控制台查看自动添加的IPv6系统路由条目和IPv6自定义路由条目。

11.6.2. 产品价值

IPv6网关具有高可用、高性能、灵活管理公网通信的优势。

高可用

IPv6网关提供跨可用区级的高可用能力，帮客户打造极致稳定的IPv6公网网关服务。

高性能

单个IPv6网关实例可提供万兆级吞吐量，满足超大业务的IPv6公网需求。

灵活管理公网通信

用户可以通过调整公网带宽和设置仅主动出规则，灵活设置IPv6地址的公网通信能力。

11.6.3. 应用场景

IPv6网关可以帮助客户快速构建安全、可靠的IPv6环境。

业务快速支持IPv6，构建云上隔离IPv6环境

为已有VPC开启IPv6，VPC将同时支持IPv4、IPv6双协议栈。为业务所在的ECS集群分配IPv6地址，ECS将同时具备IPv4地址和IPv6地址。ECS的IPv6地址默认只具备VPC内IPv6私网通信权限。

ECS IPv4/IPv6双栈集群可以通过IPv4私网，或者IPv6网络连通。

VPC中实例经IPv6地址与互联网互相通信

IPv6地址开通IPv6公网带宽后，IPv6地址即具备了IPv6公网通信权限。VPC中实例与IPv6网络通信的IPv6流量将经过IPv6网关，IPv6网关作为双栈VPC中IPv6公网流量的出入口。

VPC ECS集群原有的IPv4业务流量，依然经负载均衡、NAT网关与IPv4公网进行通信。负载均衡、NAT网关是双栈VPC中IPv4公网流量出入口。

VPC中实例经IPv6地址仅主动访问互联网

业务只需要主动访问IPv6终端，但不希望ECS实例的IPv6地址被外部IPv6终端连接。

为指定ECS实例设置IPv6公网仅主动出规则，即经IPv6地址可主动访问IPv6网络，外部IPv6终端主动发起的访问将被IPv6网关丢弃。

11.7. VPN网关

VPN网关是一款基于互联网的网络连接服务，通过建立加密通道的方式实现企业本地数据中心、企业办公网络和互联网客户端与阿里云专有网络VPC（Virtual Private Cloud）之间安全可靠的私网互联。

11.7.1. 产品详情

VPN网关通过IPsec-VPN和SSL-VPN两种方式在企业本地数据中心、企业办公网络、互联网客户端与阿里云专有网络VPC（Virtual Private Cloud）之间建立安全可靠的网络连接。

IPsec-VPN

IPsec-VPN是一种基于路由的网络连接技术，提供灵活的流量路由方式，便于配置和维护VPN策略。

IPsec-VPN支持在企业本地数据中心、企业办公网络与VPC之间建立网络连接，也支持在不同地域的VPC之间建立网络连接。

SSL-VPN

SSL-VPN是一种基于OpenVPN架构的网络连接技术。部署后，仅需要在互联网客户端中加载证书并发起连接，互联网客户端便可与VPC之间建立网络连接。

11.7.2. 产品价值

VPN网关配置简单，可以快速建立安全、稳定的网络连接，相比于使用物理专线建立网络连接的方式，使用VPN网关可以有效缩短网络连接的建设周期，降低使用成本。

安全

使用IPsec协议或者证书对传输数据进行加密，保证数据安全可信。

稳定

底层采用双机热备架构，故障时实现秒级切换，保证会话不中断，业务不受影响。

简单

开通即用，配置实时生效，实现快速部署。

低成本

基于互联网建立加密通道，相比使用物理专线成本更低。

11.7.3. 应用场景

VPN网关适用于构建混合云网络、云上资源互通、远程办公等场景。

构建混合云网络

IPsec-VPN可以在企业本地数据中心和VPC之间建立加密通信通道，实现云下云上网络的连接，构建混合云网络。

云上资源互通

IPsec-VPN可以在同地域或者不同地域的VPC之间建立加密通信通道，实现相互隔离的VPC之间的资源互通。

远程办公

SSL-VPN可以在互联网客户端和云上VPC之间建立加密通信通道，互联网客户端通过互联网可以随时随地安全地连接VPC，满足远程办公的需要。

11.8. 云接入网关

云接入网关旨在为客户提供快速上云和灵活构建混合云等基于特定场景的网络服务，可满足云基础设施从私有云或公共云向混合云演进的差异化需求。

云接入网关提供主机型和网络型两种规格：

- 主机型：包括管控节点和转发网关节点。产品基础包包含软件管控和一个转发网关实例；扩容包每个授权支持一个转发网关实例。每个转发网关实例实例支持48台裸机接入VPC网络。
- 网络型：仅包含软件管控。

11.8.1. 产品详情

云接入网关提供通用裸机网络接入VPC、开放网络服务和流量可视化能力。

裸机网络

- 支持裸机加入VPC、从VPC中移除裸机。
- 支持私网访问，在ECS安全组允许裸机网段访问的前提下，相同VPC内裸机和ECS默认互通。
- 支持公网访问，通过指定裸机交换机的方式，支持裸机通过SNAT方式主动访问公网；通过指定裸机私网IP和端口号，支持通过DNAT条目，实现公网主动访问裸机的指定端口上的应用；支持将裸机添加为Internet类型负载均衡的的后端服务器，提高可靠性。

- 支持客户IDC通过VPC专线并网访问VPC内裸机。
- 裸机网络具备与ECS一致的访问云服务能力（例如：裸机访问RDS、OSS。注意：块存储、NAS除外）。

混合云网络

动态VIP提供动态VIP创建功能，与通过飞天基础运维平台创建的静态VIP资源同步变更，实现灵活对外部服务。

开放网络服务平台

平台能力

- 支持创建、删除服务集群
- 支持资源管理
- 支持VPC流量引流到服务集群

服务接入

- 生态负载均衡：支持接入VPC私网高级负载均衡能力（认证合作伙伴：F5，深信服，radward等）
- 生态虚拟防火墙：支持接入VPC私网、VPC专线安全防护及地址转换能力（认证合作伙伴：山石）
- 生态NPM：支持接入虚拟网络流量采集和分析能力（认证合作伙伴：云杉，天旦等）

流量可视化

- 支持显示数据中心互联（DCI）场景的流量趋势、TOP5流量列表、协议分布信息。
- 支持显示DCI场景的详细流列表会话信息。
- 支持显示DCI场景的流量源产品和目的产品名称。
- 支持指定业务的流量优先级调度，（目前支持大数据计算服务MaxCompute、云数据库RDS、元数据库管理产品）。
- 支持规划人员按需选择分析器数量（支持最大200G分析能力）。

11.8.2. 产品价值

云接入网关为混合云客户提供完整、高效、安全、易用、可视的网络服务。

裸机接入VPC

云接入网关主机型提供裸机接入VPC能力。

- 兼容：对裸机零侵入，支持通用10G/25G服务器借助转发网关接入VPC网络。支持客户利旧存量服务器，实现投资保护。
- 统一：云接入网关与阿里云VPC产品集成，实现ECS、裸机网络联通及资源统一管理。
- 易用：云接入网关与裸机管理对接，对裸机资源进行统一管理，按需分配。随裸机资源分配自动完成裸机租户网络配置。
- 安全：支持裸机网络多租户隔离，裸机网络与云平台底层网络隔离。

混合云网络

提供动态VIP功能，与通过飞天基础运维平台创建的静态VIP资源同步变更，实现灵活对外部服务。

开放网络服务平台

云接入网关提供开放网络服务平台能力，为生态网元提供标准接入、快速部署、高效运维支撑。

- 自动化部署：通过标准化、模型化支持生态合作伙伴虚拟网络设备的自动化部署。
- 高可靠性：支持虚拟网络设备A/S高可用集群模型，主备切换自动进行流量切换。

- 集中式管理：将合作伙伴虚拟网络设备集中部署在独立VPC中，实现集中式管理并降低部署成本。

流量可视化

云接入网关提供的流量可视化特性具有可观测、可回溯、可过滤、易排查的优势。

- 可观测：用户可以观测到实时的流量趋势、TOP5流量、协议类型分布、详细会话信息。
- 可回溯：用户可以查询过去一段时间内的流量趋势、TOP5流量、协议类型分布、详细会话信息（可回溯的时长根据会话量数量而定）。
- 易排障：用户通过查询详细会话，可以完整了解指定时间段内的会话详情，有助于快速定位网络故障。
- 可过滤：用户可以选定TCP或者UDP，也可以指定源IP、目的IP、目的端口等条件进行过滤查询，通过缩小范围，快速查询特定流量的详细会话情况。

11.8.3. 应用场景

云接入网关主要应用于通用裸机接入VPC、混合云网络全联接、云产品拓扑可视化、云环境流量可视化场景。

通用裸机接入VPC

支持利旧客户存量物理机，实现云内物理机和虚拟机网络统一管理。

- 在以下场景可以采用裸机管理和云接入网关主机型服务，裸机管理提供物理机操作系统管理能力，云接入网关提供VPC网络接入能力：
  - 快速部署和利旧云基础设施，需要将存量服务器与专有云服务器统一到一朵云中管理。
  - 期望在专有云内申请裸机资源部署存储阵列（SAN、NAS）。
  - 现有应用无法部署到虚拟化计算实例ECS，但需要与云上应用网络高频交互。
  - 由于机型、成本等原因无法使用神龙服务器。
  - 需要在云上部署自建数据库，ECS无法满足性能、组播等功能需求。
  - 有物理机资源隔离需求，应用独占物理服务器。
- 以下场景裸机管理无法提供主机管理能力，可独立使用云接入网关主机型服务，并由用户完成主机系统安装、网络配置：
  - 服务器需接入VPC，但依赖特殊操作系统、网络配置。如需部署Oracle RAC的服务器。
  - 特殊设备接入VPC，如加密机。

混合云网络全联接

整合和扩展阿里云网络产品能力，为客户提供高效、低价、安全、易用的混合云全场景网络联通和运维服务。

云产品拓扑可视化

用户可以直观了解云环境中专有网络VPC内的网络资产数量（VPC内VPC互联，VBR上联，NAT网关，公网SLB，弹性公网IP，VPN网关，IPV6网关，路由表，vSwitch，vSwitch内的ECS、RDS、SLB实例），并且支持快速跳转至对应资产的管理页面进行资源调节，帮助云租户随时掌控网络资产情况。

流量可视化

通过云平台的业务性能监控、网络资源监控、运维排障、流量采集，实现对业务流量的可观测性。支持数据中心互联（DCI）场景流量趋势、TOP5流量列表、协议分布、流列表会话信息展示，还支持部分云产品的流量优先级调度。

11.9. 专有云DNS

专有云DNS是运行在专有云环境的一套基于DNS标准协议封装的DNS产品，为企业内网环境（专有云VPC网络、专有云经典网络、企业自建IDC内网）提供域名解析服务。专有云DNS通过设置域名与IP地址的对应规则和策略，可以将来自客户端的域名访问请求重定向到云平台中的云产品资源、云平台中的自建业务应用、企业内网的业务系统、互联网服务提供商的服务资源等。

11.9.1. 产品详情

专有云DNS为企业内网环境（专有云VPC网络、专有云经典网络、企业自建IDC内网）提供域名解析服务和全局流量调度服务（GSLB服务）。

内网DNS解析管理

内网DNS解析管理用于管理用户在专有云中创建的全局内网域名、全局转发配置以及全局递归开关配置，这些配置的变更对所有的VPC网络环境、经典网络环境同时生效。

为所有VPC网络内的服务器提供无差别的全局域名解析服务，DNS服务地址采用Region化的Anycast部署，在特定的Region内提供在机房级容灾场景下的服务无缝切换。

全局内网域名

提供全局内网域名的数据管理功能，支持内网域名的注册、搜索、功能备注和删除操作，还支持域名主机记录的添加、删除和修改操作。支持A、AAAA、CNAME、MX、 PTR、 TXT、SRV、NAPTR、CAA 、NS记录类型。

- 支持域名的一条主机记录添加多个解析记录(A、AAAA、PTR)，解析响应默认应答所有记录，并支持随机轮转，实现简单负载均衡功能。
- 支持域名的一条主机记录添加多个解析记录(A、AAAA、CNAME)，并按照权重进行一条解析记录应答，实现复杂的负载均衡功能。

全局转发配置

支持域名级别的转发操作，将特定域名的解析操作转发到其他DNS服务器上进行解析；支持全局默认的转发操作，将默认的解析操作转发到其他DNS服务器上进行解析。

转发配置提供强制转发模式和优先转发模式两种转发操作模式。

- 强制转发模式：只使用转发目的DNS服务器做域名解析，如果解析不到（解析超时）则返回DNS客户端提示查询失败。
- 优先转发模式：优先使用转发目的DNS服务器做域名解析，如果查询不到再使用本地DNS服务器做域名解析。

全局递归配置

支持递归解析功能，提供互联网域名的递归解析操作，满足企业主机访问互联网服务的需求。支持打开、修改和关闭全局默认转发配置功能。

内网PrivateZone

内网PrivateZone功能支持用户创建VPC粒度的租户独有域名，域名可以根据需要灵活绑定VPC和解绑VPC，实现租户隔离效果，这些配置的变更仅对绑定的VPC网络环境生效。

为绑定的VPC网络内的服务器提供个性化的域名解析服务，DNS服务地址采用Region化的Anycast部署，在特定的Region内提供在机房级容灾场景下的服务无缝切换。支持域名与VPC绑定和解绑的功能。

> **说明**
>
> 该功能仅在专有云DNS标准版中支持。

租户内网域名

提供租户内网域名的数据管理功能，支持内网域名的注册、搜索、功能备注和删除操作，还支持域名主机记录的添加、删除和修改操作。支持A、AAAA、CNAME、MX、 PTR、 TXT、SRV、NAPTR、CAA 、NS记录类型。

- 支持域名的一条主机记录添加多个解析记录(A、AAAA、PTR)，解析响应默认应答所有记录，并支持随机轮转，实现简单负载均衡功能。
- 支持域名的一条主机记录添加多个解析记录(A、AAAA、CNAME)，并按照权重进行一条解析记录应答，实现复杂的负载均衡功能。

租户转发配置

支持域名级别的转发操作，将特定域名的解析操作转发到其他DNS服务器上进行解析；支持全局默认的转发操作，将默认的解析操作转发到其他DNS服务器上进行解析。

转发配置提供强制转发模式和优先转发模式两种转发操作模式。

- 强制转发模式：只使用转发目的DNS服务器做域名解析，如果解析不到（解析超时）则返回DNS客户端提示查询失败。
- 优先转发模式：优先使用转发目的DNS服务器做域名解析，如果查询不到再使用本地DNS服务器做域名解析。

内网全局流量管理

内网全局流量管理提供客户业务域名多云容灾能力，通过将客户业务域名接入内网全局流量管理（GTM），实现多专有云之间的流量负载管理。

内网全局流量管理提供企业内网全局流量调度（GSLB）功能，可以按照用户配置的调度策略对请求源的DNS查询按照需要进行IP地址的智能分配，同时支持多云混合部署并实现多云间的配置数据同步。

> **说明**
>
> 该功能仅在专有云DNS内网GTM标准版中支持。

调度实例管理

- 支持调度实例的管理，一个调度实例对应了一个应用实例。
- 支持地址池的管理，一个地址池对应了一个应用实例的一个服务集群。
- 支持调度域的管理，提供调度实例归属的调度域的设置，让客户可以按照企业自己的命名规范进行全局调度实例的统一管理和编码。

调度线路管理

调度线路管理支持自定义线路和优先级，实现按照地理位置、应用分组对客户端进行就近访问和智能流量调度，实现应用访问加速。

数据同步管理

- 提供全局数据同步链路的管理，实现多个内网全局流量管理服务的数据同步功能的配置管理和状态查看，包括本地系统信息、已经建立数据同步关系的集群节点信息、主辅关系信息的展示，同时也提供同步链路创建的功能。
- 提供同步链路变更消息管理的功能，用于管理所有的Master节点主动添加Slave节点的请求消息的确认。

11.9.2. 产品价值

通过专有云DNS，用户在企业内网环境（专有云VPC网络、专有云经典网络、企业自建IDC内网）中可以实现：

- 访问VPC内的其他ECS主机。
- 访问云平台提供的云服务实例资源。

- 访问客户自定义的企业级业务系统。
- 访问互联网上的业务和服务。
- 为企业业务提供全局负载均衡，实现同城双活/多活、异地双活/多活、异地容灾等多种形态的业务多活和容灾架构。
- 通过企业专线，与企业自建DNS实现互通。

企业域的域名管理

专有云DNS提供企业域的域名管理操作和解析操作。

- 支持云资源实例域名（包括ECS主机实例域名）的正解和反解。
- 支持企业内网业务域名的正解和反解。
- 支持常见的域名解析记录类型（包括A、AAAA、CNAME、NS、MX、TXT、SRV、PTR）的添加、修改和删除操作。
- 支持域名的一条主机记录添加多个解析记录（包括A、AAAA、PTR），解析响应默认应答所有记录，并支持随机轮转，实现简单负载均衡。

与企业自建IDC进行灵活并网

专有云DNS提供企业域的域名转发操作，实现灵活组网和并网操作，实现与企业自建DNS系统进行级联的操作。

- 支持全局默认转发功能。
- 支持按域名转发功能。

企业主机访问互联网

在开通对外访问公网的情况下，专有云DNS支持公网域名递归解析功能，提供互联网域名的递归解析操作，满足企业主机访问互联网服务的需求。

提供租户隔离功能

提供基于VPC的PrivateZONE管理和解析功能，满足专有云DNS按租户对DNS数据和解析隔离的需求。

- 提供Private权威Zone的增删改查，提供Private权威Zone与VPC绑定和解绑的功能。
- 提供Private转发Zone的增删改查，提供Private转发Zone与VPC绑定和解绑的功能。

> **说明**
>
> 该特性仅限专有云DNS标准版。

全局流量管理功能

提供在企业内网环境下的全局负载均衡（GSLB）功能。

- 支持域名的一条主机记录添加多个解析记录（包括A、AAAA、CNAME），按照权重进行一条解析记录应答，实现复杂的全局流量调度。
- 支持调度线路管理，可以自定义线路和优先级，实现按照地理位置、应用分组对客户端进行就近访问和智能流量调度，实现应用访问加速
- 支持解析配置数据在多个全局流量管理集群之间进行同步（支持多朵云的场景）。
- 支持地址池的管理方式，按照应用服务集群对企业应用进行统一管理。
- 支持自定义全局调度域，按照企业自己的命名规范进行全局调度实例的统一管理和编码。

统一管控平台

- 管控系统集成在专有云统一管控平台中，统一账号统一管理。

- 数据管理和服务管理支持Web操作，操作简单容易理解。

11.9.3. 应用场景

专有云DNS作为基础核心网络服务，掌管着企业专有云流量入口大门，除了提供基础域名解析服务，还为应用提供多种流量负载和调度的服务，实现专有云、自建IDC和公有云的互联互通。专有云DNS伴随企业客户共生共赢，提供贴身的基础服务保障，为企业云环境建设、机房高可用、流量负载均衡、容灾切换等多种IT架构提供丰富的解决方案，为企业客户的IT业务提供保驾护航服务。

基础解析

在VPC环境访问云资源实例

在VPC内的ECS实例/Docker实例中访问RDS、SLB、OSS云实例。

在VPC环境访问ECS主机名

对VPC内的ECS实例/Docker实例按照企业自己的规则定义主机名，实现ECS实例/Docker实例按照主机名进行远程访问和远程管理。

在VPC环境访问内网服务域名

在专有云环境中开发自己的PaaS服务或者SaaS服务，并且通过域名对内提供服务，在VPC环境内需要访问这个自建的PaaS服务或者SaaS服务。

对专有云环境中提供的内网服务基于Round-Robin简单流量调度

在专有云环境中开发自己的SaaS服务并且通过域名对内提供服务，而且这个服务部署在多个机房或者多个区域，通过专有云DNS服务，可以在VPC环境内访问这个自建SaaS服务并将流量平均分摊到不同的节点。

在VPC网络、经典网络环境访问互联网服务

在VPC网络、经典网络环境里面访问互联网上提供的服务。

在专有云环境中实现多个网络环境服务互联

将专有云的环境与企业内网环境、公有云环境或者其他外部环境做业务打通，实现域名互联互通

租户隔离

云环境中租户资源强隔离

在专有云环境中实现租户资源强隔离的功能，希望各个租户配置的内网域名解析数据和默认转发配置对其他租户不可访问也不可见，租户可以配置自己的私有域名解析数据完成各种各样的业务寻址调度场景。

云环境中全局资源互通

在专有云环境中实现所有租户共享全局资源和配置的功能，系统管理员可以配置全局域名解析数据和全局解析配置完成各种各样的业务寻址调度场景

云环境中基于租户VPC的智能调度

针对专有云环境中的某个租户，对于同样的主机解析记录，实现该租户不同VPC内解析结果都不一样的功能。

全局调度

对专有云环境中提供的内网服务基于权重进行流量调度

在专有云环境中开发自己的PaaS服务或者SaaS服务并且通过域名对内提供服务，且这个服务是部署在多个机房或者多个区域，在云内环境或者云外环境访问这个自建的PaaS服务或者SaaS服务，并将流量根据后端集群建设容量，按照比例将流量分摊到不同的节点。

对专有云环境中提供的内网服务基于请求源的地理位置或者所属应用分组进行流量调度

在专有云环境中开发自己的PaaS服务或者SaaS服务并且通过域名对内提供服务，且这个服务是部署在多个机房或者多个区域，在云内环境或者云外环境访问这个自建的PaaS服务或者SaaS服务，并将流量根据请求源的地理位置或者所属应用分组路由到不同的节点。

企业容灾

对专有云环境中的内网服务提供容灾调度的能力

在专有云环境中开发自己的PaaS服务或者SaaS服务并且通过域名对内提供服务，且这个服务是部署在多个机房或者多个区域，在云内环境或者云外环境访问这个自建的PaaS服务或者SaaS服务，在容灾场景下将内网业务访问流量从后端集群A（主站点）切到后端集群B（备站点）。

11.10. 云企业网

云企业网CEN（Cloud Enterprise Network）是运行在专有云网络上的一张高可用网络。云企业网通过转发路由器TR（Transit Router）为用户提供一种能快速构建同地域专有网络之间、多个专有网络与多个本地数据中心之间高速、优质、稳定的企业级组网解决方案。

11.10.1. 产品详情

云企业网通过转发路由器TR（Transit Router）在同地域专有网络之间、专有网络与本地数据中心之间搭建私网通信通道。同时，转发路由器支持关联转发、路由学习、自定义路由表、路由策略等丰富的网络互通和路由管理能力，允许企业自定义网络连通性，帮助企业打造一张灵活、可靠、大规模的企业级互连网络。

网络实例连接

转发路由器支持连接专有网络VPC（Virtual Private Cloud）实例和边界路由器VBR（Virtual Border Router）实例。

- 同地域的VPC实例连接至转发路由器实例后可实现网络互通。
- 转发路由器实例连接VBR实例后，VBR实例关联的本地数据中心可与连接至转发路由器下的VPC实例实现网络互通。

路由

转发路由器支持关联转发、路由学习、自定义路由表、自定义路由条目和路由策略多种路由管理功能，帮助企业自定义网络连通性。

- **自定义路由表**

  转发路由器连接网络实例后，通过路由表存储网络实例的路由。转发路由器通过查询路由表中的路由条目信息转发网络实例的流量。

  每个转发路由器默认携带一个默认路由表，支持为转发路由器创建自定义路由表。默认路由表和自定义路由表之间互不相通，可以实现访问隔离。

- **关联转发**

  关联转发功能控制网络实例的流量转发。网络实例连接与转发路由器路由表建立关联转发关系后，转发路由器将通过查询该路由表中的路由条目信息转发网络实例的流量。

- **路由学习**

  路由学习功能控制网络实例的路由传播。网络实例连接与转发路由器路由表建立路由学习关系后，网络实例的路由才被允许传播至转发路由器路由表中。

- **自定义路由条目**

  转发路由器路由表支持添加自定义路由条目。通过在转发路由器路由表中添加自定义路由条目可以辅助控制网络实例流量的转发。

- **路由策略**

  路由策略功能控制转发路由器路由表的路由传播。路由策略可以决定是否将转发路由器路由表中的路由传播给网络实例，也可以修改转发路由器路由表中路由的属性。

组播

- 转发路由器默认支持组播流量转发。同地域的VPC实例连接至转发路由器实例后，支持在VPC实例之间建立组播网络。
- 支持在转发路由器下创建Connect连接对接本地数据中心，转发路由器下的VPC实例和云下本地数据中心可通过Connect连接传输组播流量，实现云上云下组播网络互通。

健康检查

VBR实例通过物理专线连接本地数据中心。将VBR实例连接至转发路由器实例后，可通过健康检查功能探测物理专线的连通性。

11.10.2. 产品价值

云企业网配置简单，可以在同地域专有网络之间、多个专有网络与多个本地数据中心之间快速构建安全、灵活、高速、优质、稳定的网络通信通道，帮助企业打造一张大规模的企业级互连网络。

大规模网络互联

转发路由器能快速连接同地域下的多个VPC实例和云下网络，实现资源互通。同地域下转发路由器支持300个VPC互联，满足企业网络规模扩张的需求。

低时延高速率

转发路由器提供低延迟、高速率的网络传输能力。同地域资源互通最大速率可达到网络设备端口转发速率。

高可靠高质量

转发路由器提供主备两个节点，主备节点自动切换，保障业务不中断。全网任意两个节点之间存在多组高质量传输链路，底层链路中断网络自动收敛，业务无感知。

11.10.3. 应用场景

云企业网适用于同地域专有网络互通、同地域云上云下网络互通、组播网络互通等场景。

同地域VPC互通

同地域VPC实例连接至转发路由器后，可实现网络互通。

本地IDC和VPC互通

本地数据中心通过VBR实例连接至转发路由器，可与同地域下已连接至转发路由器的VPC实例互通。

云上组播网络

同地域VPC实例连接至转发路由器后，可通过转发路由器实现组播网络互通。

云上云下组播网络互通

本地数据中心可通过Connect连接直接连接至转发路由器，通过Connect连接实现与转发路由器下VPC实例的组播网络互通。

12.数据库服务

12.1. 云数据库RDS

阿里云关系型数据库RDS（Relational Database Service）是一种稳定可靠、可弹性伸缩的在线数据库服务。基于高性能存储，提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案。

12.1.1. 产品详情

阿里云关系型数据库RDS包含MySQL、SQL Server、PolarDB、PostgreSQL四种数据库引擎，可以方便快捷地创建出适合自己应用场景的数据库实例。

产品引擎介绍

- RDS MySQL：基于阿里云的自研内核AliSQL，经过双十一高并发、大数据量的考验，拥有优良的性能。RDS MySQL支持X86、ARM多集群混部，集成了实例管理、账号管理、数据库管理、备份恢复、白名单、透明数据加密以及数据迁移等基本功能。除此之外还提供如下高级功能：
  - **只读实例：** 在对数据库有大量读请求和少量写请求时，单个实例可能无法承受读取压力，为了实现读取能力的弹性扩展，减少单个实例的压力，RDS MySQL的实例支持只读实例，利用只读实例满足大量的数据库读取需求，以此增加应用的吞吐量。
  - **读写分离：** 读写分离功能是在只读实例的基础上，额外提供了一个读写分离地址，联动主实例及其所有只读实例，创建自动的读写分离链路。应用程序只需连接读写分离地址进行数据读取及写入操作，读写分离程序会自动将写入请求发往主实例，而将读取请求按照权重发往各个只读实例。用户只需通过添加只读实例的个数，即可不断扩展系统的处理能力，应用程序上无需做任何修改。
- RDS PostgreSQL：先进的开源数据库，它的优点主要集中在对SQL规范的完整实现以及丰富多样的数据类型支持，包括JSON数据、IP数据和几何数据等。除了完美支持事务、子查询、多版本控制（MVCC）、数据完整性检查等特性外，RDS PostgreSQL还集成了高可用和备份恢复等重要功能，减轻企业运维压力。
- RDS SQL Server：拥有高可用架构和任意时间点的数据恢复功能，可强力支撑各种企业应用。支持实例管理、账号管理、数据库管理、白名单、备份恢复、透明数据加密以及数据迁移等基本功能。
- PolarDB：稳定、安全且可扩展的企业级关系型数据库，基于PostgreSQL，并在性能、应用方案和兼容性等方面进行了增强，提供直接运行Oracle应用的能力。用户可以在PolarDB上稳定运行各种企业应用，同时得到高性价比的服务。

调度服务

调度服务主要负责RDS底层资源的分配和整合，对用户而言就是实例的开通和迁移。例如，通过RDS控制台或者API创建实例，调度服务会计算出最适合的物理服务器来承载流量。RDS实例迁移所需的底层资源也由调度服务分配和整合。在经过长时间的实例创建、删除和迁移后，调度服务会计算资源碎片化程度，并定期发起资源整合以提高服务承载量。

数据链路服务

云数据库RDS提供全数据链路服务，包括DNS、负载均衡等。

- DNS：DNS模块提供域名到IP的动态解析功能，以便规避RDS实例IP地址改变带来的影响。在连接池中设置域名后，即使对应的IP地址发生了变化，仍然可以正常访问RDS实例。

  例如，某RDS实例的域名为**test.rds.aliyun.com**，对应的IP地址为**10.10.10.1**。某程序连接池中设置为**test.rds.aliyun.com** 或 **10.10.10.1** 都可以正常访问RDS实例。

  一旦该RDS实例发生了实例迁移或者版本升级后，IP地址可能变为**10.10.10.2**。如果程序连接池中设置的是域名**test.rds.aliyun.com**，则仍然可以正常访问RDS实例。但是如果程序连接池中设置的是IP地址**10.10.10.1**，就无法访问RDS实例了。
- SLB：负载均衡（SLB）模块提供实例IP地址（包括内网IP 和外网IP），以便屏蔽物理服务器变化带来的影响。

例如，某RDS实例的内网IP地址为**10.1.1.1**，对应的Proxy或者DB Engine运行在**192.168.0.1**上。在正常情况下，负载均衡模块会将访问**10.1.1.1**的流量重定向到**192.168.0.1**上。当**192.168.0.1**发生了故障，处于热备状态的**192.168.0.2**接替了**192.168.0.1**的工作。此时负载均衡模块会将访问**10.1.1.1**的流量重定向到 **192.168.0.2** 上，RDS实例仍旧正常提供服务。

实例变配

云数据库RDS变配时，系统自动在后台执行如下流程：

1. 申请资源：申请新实例所需的资源。
2. 同步数据：将原实例的全量和增量数据同步至新实例中。
3. 实例切换：数据同步接近完成时，原实例将被设置为只读并等待数据完全同步，随后系统会将SLB后端中原实例的Proxy IP地址移除并挂载新实例的Proxy IP地址，完成地址切换。
4. 变配完成：释放原实例资源并将新实例的状态为修改为运行中。

备份恢复服务

云数据库RDS可以随时发起数据库的备份，能够根据备份策略将数据库恢复至任意时刻，提高了数据可回溯性。

- 备份：备份模块负责将主备节点上面的数据和日志压缩并上传。RDS默认将备份上传到OSS中。在备节点正常运作的情况下，备份总是在备节点上面发起，以避免对主节点提供的服务带来冲击；在备节点不可用或者损坏的情况下，备份模块会通过主节点创建备份。支持如下两种备份方式：
  - 物理备份：直接备份所有数据库中的文件。
  - 逻辑备份：通过SQL从数据库中抽取数据并以文本的形式进行备份。
- 恢复：恢复模块负责将OSS上面的备份文件恢复到目标节点上。
  - 回滚主节点功能：用户发起数据相关的误操作后可以通过回滚功能按时间点恢复数据。
  - 修复备节点功能：在备节点出现不可修复的故障时自动新建备节点来降低风险。
  - 创建只读实例功能：通过备份来创建只读实例。
- 转储：转储模块负责备份文件的上传、转储和下载。目前备份数据全部上传至OSS进行存储，用户可以根据需要获取临时链接来下载。在某些特定场景下，转储模块支持将OSS上面的备份文件转储至归档存储来提供更长时间和更低费用的离线存储。

监控服务

云数据库RDS提供物理层、网络层、应用层等多方位的监控服务，保证业务可用性。

- Service：Service模块负责服务级别的状态跟踪，监控负载均衡、OSS、归档存储和日志服务等RDS依赖的其他云产品是否正常，包括功能和响应时间等。对RDS内部的服务，Service也会通过日志来判定是否正常运作。
- Network：Network模块负责网络层面的状态跟踪，包括ECS与RDS之间的连通性监控，RDS物理机之间的连通性监控，路由器和交换机的丢包率监控。
- OS：OS模块负责硬件和OS内核层面的状态跟踪。
  - 硬件检修：不断检测CPU、内存、主板、存储等设备的工作状态，预判是否会发生故障，并提前进行自动报修。
  - OS内核监控：跟踪数据库的所有调用，并从内核态分析调用缓慢或者出错的原因。
- Instance：Instance模块负责RDS实例级别的信息采集。
  - 实例的可用信息。
  - 实例的容量和性能指标。
  - 实例的SQL执行记录。

高可用服务

高可用服务由Detection、Repair、Notice等模块以及多个高可用策略组成，主要保障数据链路服务的可用性，除此之外还负责处理数据库内部的异常。

- Detection：Detection模块负责检测DB Engine的主节点和备节点是否提供了正常的服务。通过间隔为8~10秒的心跳信息，HA节点可以轻易获得主节点的健康情况，结合备节点的健康情况和其它HA节点的心跳信息，Detection模块可以排除网络抖动等异常引入的误判风险，快速完成异常切换操作。
- Repair：Repair模块负责维护DB Engine的主节点和备节点之间的复制关系，还会修复主节点或者备节点在日常运行中出现的错误。
  - 主备复制异常断开的自动修复。
  - 主备节点表级别损坏的自动修复。
  - 主备节点Crash的现场保存和自动修复。
- Notice：Notice模块负责将主备节点的状态变动通知到负载均衡或者Proxy，保证用户访问正确的节点。

  例如：Detection模块发现主节点异常，并通知Repair模块进行修复。Repair模块进行了尝试后无法修复主节点，通知Notice进行流量切换。Notice模块将切换请求转发至负载均衡或者Proxy，此时流量全部指向备节点。与此同时，Repair在别的物理服务器上重建了新的备节点，并将变动同步给Detection模块。Detection模块开始重新检测实例的健康状态。
- 高可用策略：高可用策略是根据用户自身业务的特点，采用服务优先级和数据复制方式之间的不同组合，以组合出适合自身业务特点的高可用策略。
  服务优先级有以下两个级别：
  - 复原时间目标RTO（Recovery Time Objective）优先：数据库应该尽快恢复服务，即可用时间最长。如果对数据库在线时间要求较高，则应该使用RTO优先策略。
  - 复原点目标RPO（Recovery Point Objective）优先：数据库应该尽可能保障数据的可靠性，即数据丢失量最少。如果对数据一致性要求较高，则应该使用RPO优先策略。

  数据复制有以下三种方式：
  - 强同步
    - 应用发起的更新在主实例执行完成后，会将日志同步传输到所有备实例，至少1个备实例收到并存储日志后，事务才完成提交。
    - 在强同步模式下，实例的复制方式会始终保持强同步，无论出现何种状况，都不会退化为异步。
    - 当实例的节点数≥3时，才支持强同步。因此，只有三节点企业版实例支持强同步。三节点企业版实例的数据复制方式无法修改。
  - 半同步

    应用发起的更新在主实例执行完成后，会将日志同步传输到备实例，备实例收到日志，事务就算完成了提交，不需要等待备实例执行日志内容。

    当备实例不可用或者主备实例间出现网络异常时，半同步会退化为异步。
  - 异步

    应用发起更新请求，即进行增加、删除、修改数据的操作时，主实例完成操作后会立即响应应用，同时主实例向备实例异步复制数据。因此，在异步数据复制方式下，备实例不可用时不会影响主实例上的操作，而主实例不可用时可能会导致主备实例数据不一致。

可以根据自身业务特点，选择服务优先级和数据复制方式的不同组合方式，提高可用性。

数据迁移服务

云数据库RDS提供了数据迁移服务DTS（Data Transmission Service）工具，方便用户快速迁移数据库。

DTS提供了三种迁移模式，分别为结构迁移、全量迁移和增量迁移。

- 结构迁移

  DTS会将迁移对象的结构定义迁移到目标实例，目前支持结构迁移的对象有表、视图、触发器、存储过程和存储函数。
- 全量迁移

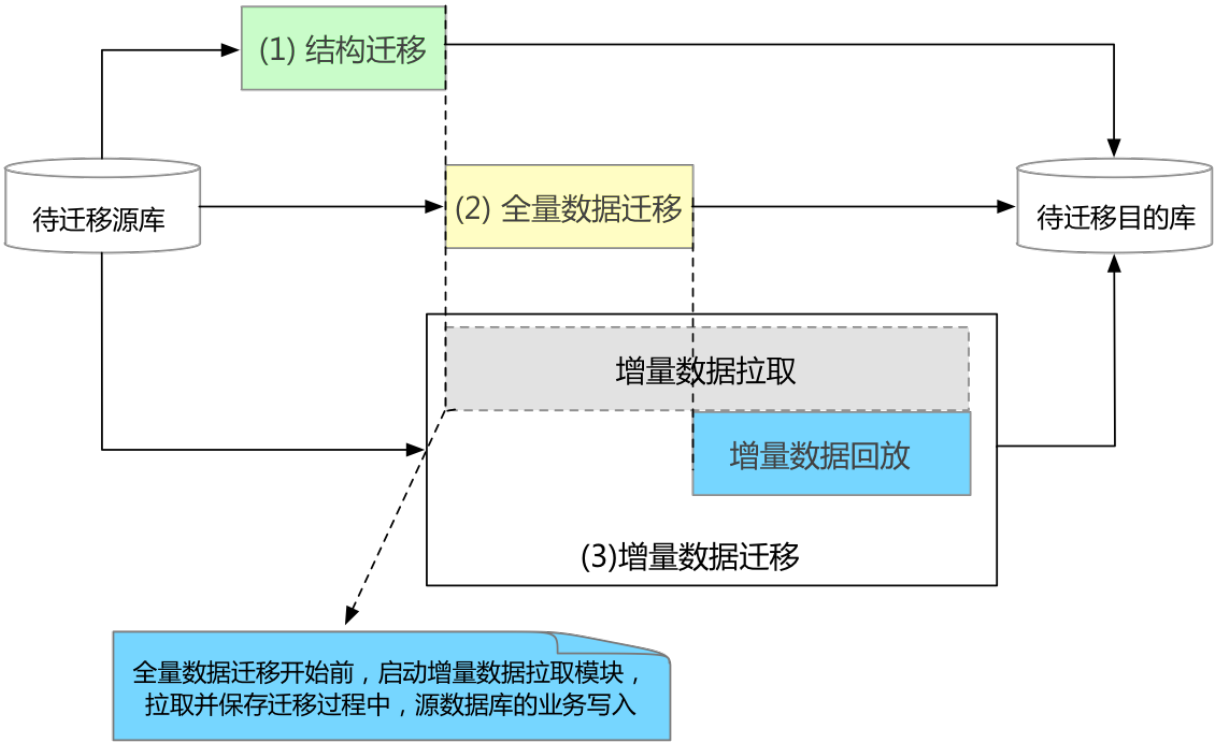
  DTS会将源数据库迁移对象已有数据全部迁移到目标实例中。

> **重要** 在全量迁移过程中，为了保证数据一致性，无主键的非事务表会被锁定。锁定期间这些表无法写入，锁定时长依赖于这些表的数据量大小。在这些无主键非事务表迁移完成后，锁才会释放。

- 增量迁移

  DTS会将迁移过程中数据变更同步到目标实例。

  > **重要** 如果迁移期间进行了DDL操作，这些结构变更不会同步到目标实例。



独享规格

RDS独享规格是具有固定计算能力、存储空间以及IO性能的RDS实例规格类型，具有更加稳定的性能表现。此外，独占物理机规格是独享规格中配置最高的规格，独享所有资源。

- 资源隔离：为了保持计算性能的稳定，RDS在不同实例之间实施了计算资源的隔离。独享规格的RDS实例会分配到完全独享的CPU线程核数，保证该实例不会受到物理机中其他实例行为的影响。
- 存储空间：独享规格的存储空间是固定预留的（Reserved），相对于通用规格，拥有更高的稳定性。通过双机热备的特性，在某一台主机的磁盘故障时自动进行热切换，对用户透明无感知。

读写分离

- 统一读写分离地址，方便维护。

  不开通读写分离时，用户需要在应用程序中分别配置主实例和每个只读实例的连接地址，才能实现将写请求发往主实例而将读请求发往只读实例。

  RDS读写分离功能提供一个独享代理地址，用户连接该地址后即可对主实例和只读实例进行读写操作，读写请求被自动转发到对应实例，可降低维护成本。

  同时，用户只需添加只读实例的个数，即可不断扩展系统的处理能力，应用程序无需做任何修改。

- 原生链路支持，提升性能，减少维护成本。

如果用户在云上自行搭建代理层实现读写分离，数据在到达数据库之前需要经历多个组件的语句解析和转发，对响应延迟有较大的影响。而RDS读写分离内置在RDS原生生态里，能够有效降低延迟，提升处理速度，同时减少客户的维护成本。

- 可设权重和阈值，符合多场景使用。

  用户可以设置主实例和只读实例的读请求权重，以及设置只读实例的延迟阈值。

- 实例健康检查，提升数据库系统的可用性。

  读写分离模块将自动对主实例和只读实例进行健康检查，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，读写请求在剩余的健康实例间进行分配。以此确保单个只读实例发生故障时，不会影响应用的正常访问。当实例被修复后，RDS会自动将该实例纳回请求分配体系内。

> **说明** 为避免单点故障，建议用户为一个主实例创建至少两个只读实例。

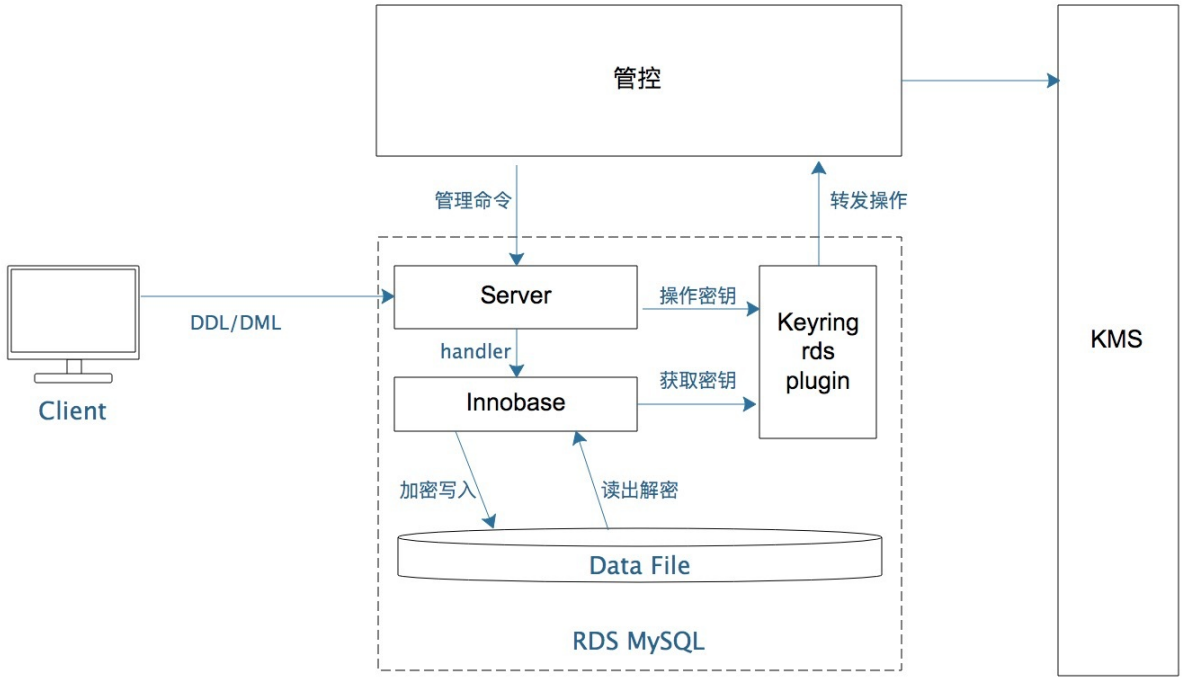
数据安全

RDS提供多层网络安全防护，包含专有网络VPC、白名单等功能，保证数据的安全。

- 支持专有网络VPC（Virtual Private Cloud），在TCP层提供网络隔离保护。
- 支持DDoS防护，实时监测并清除大流量攻击。
- 支持1000个以上IP地址白名单配置，隔绝非法访问。
- 支持密码访问鉴权方式，确保访问安全可靠。

透明数据加密TDE服务

透明数据加密TDE（Transparent Data Encryption）可对数据文件执行实时I/O加密和解密，未持有密钥的用户即使获取了数据文件也无法提取数据内容，保证了数据的隐私和安全。



TDE由如下4个角色进行协同工作：

- 管控：协调TDE整体的运转，通过KMS密钥管理功能，管理和控制RDS实例中用户对密钥的使用和轮转。
- RDS：执行管控命令、执行DDL/DML请求、提供透明加解密服务。
- KMS：密钥管理服务，负责生成密钥。
- Client：用户，发出加密请求。

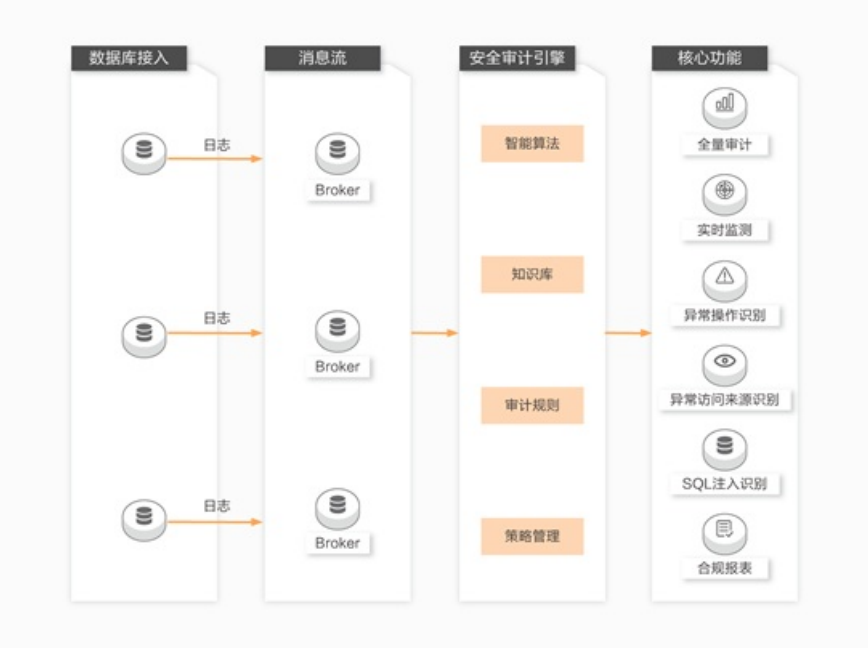
SQL优化技术

自动SQL优化服务是阿里云数据库自治服务（DAS）中最为核心服务之一，以自优化的自治能力实现SQL优化的闭环。

- 负载（Workload）异常检测，识别数据库业务变化，问题SQL的快速识别与定位，如新增慢SQL，性能恶化SQL，不高效SQL等。
- 针对问题SQL，自动调用SQL诊断优化服务生成优化建议，如最优索引的创建、SQL语句改写、引擎推荐等等。
- 自动完成优化建议风险评估，根据数据库实例负载情况、实例画像自动生成灰度计划，自动编排优化任务。
- 自动选取运维窗口，依据灰度计划，完成相关线上变更，目前阶段主要支持索引的自动上线变更。
- 针对上线的变更，启动多维度的优化效果跟踪，持续实时全面的性能回归风险评估，符合预期，自动计算优化收益，不符预期，自动回滚。

SQL审计

SQL审计以记录数据库中的所有活动为基础，对数据库中的所有操作进行全面和精准的审计，对数据库遭受到的风险行为进行实时告警，同时生成合规报告，提高数据资产安全。



开启SQL审计功能可以记录所有DML和DDL操作信息，并内置安全引擎，实时审计数据库的活动。

- 实时检测：对各类攻击和威胁进行实时检测，及时发现安全隐患。
- 高危操作识别：通过智能算法、海量模型识别高危操作。
- 异常访问来源识别：自动识别新增或者异常的访问来源。

12.1.2. 产品价值

云数据库RDS拥有易于使用、高性能、高安全性、高可靠性的优点。

易于使用

- 即开即用：用户可以通过API进行RDS规格定制，创建后RDS实时生产出目标实例。
- 按需升级：随着数据库压力和数据存储量的变化，用户可以灵活调整实例规格，且升级期间RDS不会中断数据链路服务。
- 透明兼容：RDS与原生数据库引擎的使用方法一致，用户无需二次学习，上手即用。另外RDS兼容现有的程序和工具。使用通用的数据导入导出工具即可将数据迁移到RDS，迁移过程中的人力开销非常低。
- 管理便捷：用户可以自行通过阿里云控制台完成数据库的增加、删除、重启、备份、恢复等管理操作。

高性能

- 参数优化：所有RDS实例的参数都是经过多年的生产实践优化而得，在RDS实例的生命周期内，阿里云持续对其进行优化，确保RDS一直基于最佳实践在运行。
- SQL优化：针对用户应用场景特点，RDS会锁定效率低下的SQL语句并提出优化建议，以便用户优化业务代码。

高安全性

- 防DDoS攻击：当用户使用外网连接和访问RDS实例时，可能会遭受DDoS攻击。当RDS安全体系认为实例正在遭受DDoS攻击时，云盾DDoS防护系统会自动启动流量清洗功能，拦截攻击流量。

  > **说明** 该功能需开通阿里云的安全产品。

- 访问控制策略：
  - 用户可以指定允许访问RDS的IP地址白名单，白名单以外的IP地址将被拒绝访问。
  - 每个账号只能查询、操作赋予了相应权限的数据库。
- 系统安全：
  - RDS处于多层防火墙的保护之下，可以有效抵抗各种恶意攻击，保证数据的安全。
  - RDS服务器不允许直接登录，只开放特定的数据库服务所需要的端口。
  - RDS服务器不允许主动向外发起连接，只能接受被动访问。
- TDE加密：透明数据加密TDE（Transparent Data Encryption）可以对实例数据文件执行实时I/O加密和解密。数据在写入磁盘之前会进行加密，从磁盘读入内存时会进行解密。TDE不会增加数据文件的大小。开发人员无需更改任何应用程序，即可使用TDE功能。

高可靠性

- 双机热备：RDS采用热备架构，物理服务器出现故障后服务秒级完成切换，整个切换过程对应用透明。
- 多副本冗余：RDS服务器中的数据构建于RAID之上，数据备份存储在OSS上。
- 数据备份：RDS提供自动备份的机制，用户可以自行选择备份周期，也可以根据自身业务特点随时发起临时备份。
- 数据恢复：支持按备份集和指定时间点来创建克隆实例恢复数据，数据验证无误后即可将数据迁回RDS主实例，从而完成数据回溯。

12.1.3. 应用场景

通过结合其他云产品，云数据库RDS可以适用于更多典型的应用场景。

数据多样化存储

RDS支持搭配云数据库Redis版、对象存储OSS等产品使用，适用于多样化存储的场景。

- 缓存数据持久化：RDS可以和云数据库Redis版搭配使用，组成高吞吐、低延迟的存储解决方案。与RDS相比，云数据库缓存产品有两个特性。
  - 响应速度快，云数据库Redis版请求的时延通常在几毫秒以内。
  - 缓存区能够支持比RDS更高的每秒查询率QPS（Query Per Second）。
- 多结构数据存储：OSS是阿里云对外提供的海量、安全、低成本、高可靠的云存储服务。RDS可以和OSS搭配使用，组成多类型数据存储解决方案。例如，当业务场景为论坛时，RDS搭配OSS使用，注册用户的图像、帖子内容的图像等资源存储在OSS中，以减少RDS的存储压力。

读写分离

通过读写分离功能可以实现数据读取和写入操作的分离，扩展系统的处理能力。

云数据库RDS MySQL支持直接挂载只读实例，分担主实例读取的压力。RDS MySQL的主实例和只读实例都具有独立的连接地址，当开启读写分离功能后，系统就会额外提供一个读写分离地址，联动主实例及其下的所有只读实例，实现自动的读写分离。应用程序只需连接同一个读写分离地址进行数据读取及写入操作，读写分离模块会自动将写入请求发往主实例，而将读取请求按照用户设置的权重发往各个只读实例。用户只需通过添加只读实例的个数，即可不断扩展系统的处理能力，应用程序上无需做任何修改。

大数据分析

将RDS数据导入大数据计算服务（MaxCompute），可以实现批量结构化数据的存储和计算，提供海量数据仓库的解决方案以及针对大数据的分析建模服务。

12.2. 云原生关系型数据库PolarDB

云原生关系型数据库PolarDB是由阿里云自研的一款云原生关系型数据库，基于云原生架构、计算存储分离、软硬件一体化设计，为用户提供具备超高弹性和性能、高可用和高可靠保障、高性价比的数据库服务。PolarDB支持SQL和NoSQL两种数据访问模式，同时支持MySQL和PostgreSQL两种主流数据库的协议，使得PolarDB可以轻松地与已有数据库进行整合，提供更高效的数据处理能力。

云原生关系型数据库PolarDB采用通用的专有云基础设施，用户使用较低的成本即可享受到PolarDB的核心能力。

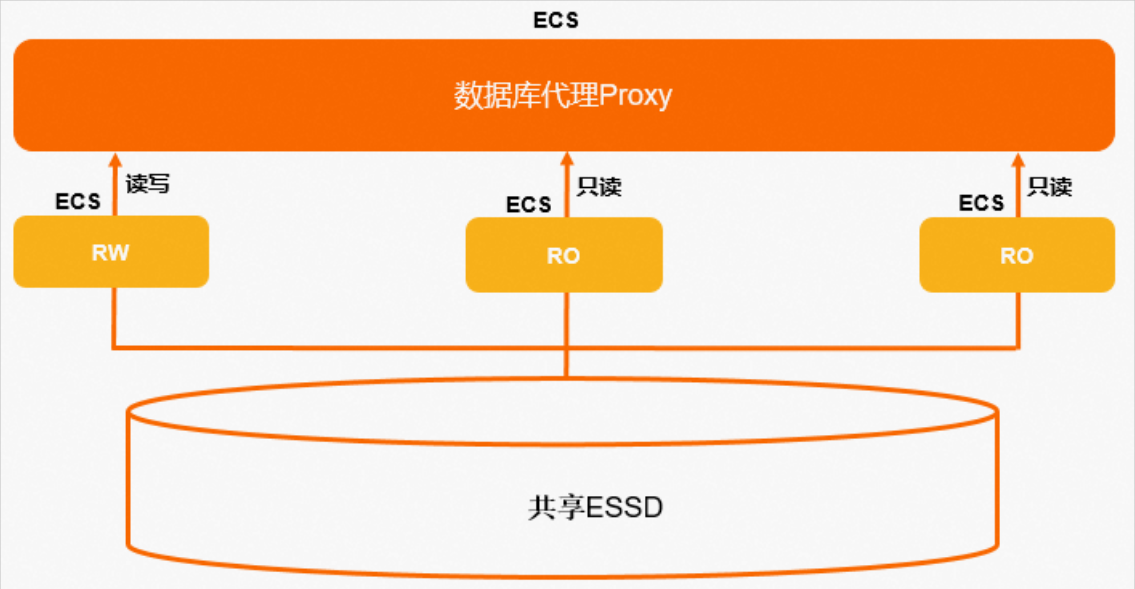
- PolarDB采用阿里云多年深度优化的PolarDB数据库内核，相对开源内核大幅提升数据库性能。
- 采用最新一代阿里云高性能计算和存储基础设施，客户使用成本大幅下降。
- 云原生的计算和存储分离架构，一写多读，灵活弹性，配置升降级和增加节点分钟级生效。
- 多个计算节点共享存储，新增只读节点时只需增加计算节点资源，大幅降低扩容成本。

12.2.1. 产品详情

云原生关系型数据库PolarDB是一款强大的云原生关系型数据库，具有高可用性、高性能、易于扩展等优势，适合各种规模的企业级应用。

存算分离

云原生关系型数据库PolarDB采用计算与存储分离的架构，数据库代理和计算节点分别采用独立的ECS进行部署，共享存储层使用ESSD云盘，极大降低用户使用PolarDB的成本。



> **说明**
>
> 如果创建PolarDB MySQL版实例时选择了1个节点，则PolarDB MySQL版将采用单节点架构，单节点架构仅一个数据库计算节点承担读写功能。
>
> - 单节点架构支持通过增加只读节点操作添加节点变为多节点架构，添加节点后允许用户开启数据库代理。
> - 多节点架构也支持通过删除只读节点操作删除节点变为单节点架构。

超级MySQL

- 100%兼容原生MySQL和阿里云RDS MySQL，用户可以在不修改应用程序任何代码和配置的情况下，将MySQL数据库迁移至PolarDB MySQL版。
- 持续提供一写多读或多写多读、共享存储、60亿行数据稳定运行、秒级DDL、主从切换无闪断、闪回查询、分区表增强等高价值特性。

12.2.2. 产品价值

用户可以像使用传统数据库一样使用云原生关系型数据库PolarDB。此外，云原生关系型数据库PolarDB还拥有传统数据库所不具备的优势：

- **高性价比**
  - 多个计算节点共享存储，新增只读节点时只需支付计算节点费用，大大降低扩容成本。
- **超高弹性**
  - 分钟级增删节点。
  - 存储容量在线扩容，无需中断业务。
- **超高性能**

  深度优化数据库内核，同时采用物理复制、高速网络和分布式共享存储，大幅提高性能，相比开源MySQL性能最大提升6倍。
- **高可用和高可靠保障，数据安全可靠**
  - 共享分布式存储的设计，彻底解决了主从异步复制所带来的备库数据非强一致的缺陷，使得整个数据库集群在应对任何单点故障时，可以保证数据零丢失。

- 热备集群部署在PolarDB MySQL 版集群所在地域的备可用区或者同一可用区下的不同机房，具有独立的存储能力，用于集群的热备切换。当PolarDB整个集群或者主可用区不可用时，热备集群会快速切换为主集群承担集群的读写业务。

- 数据安全
  - 采用白名单、VPC网络、数据多副本存储等全方位的手段，对数据库数据访问、存储、管理等各个环节提供安全保障。

- **无锁备份**
  - 利用底层分布式存储的快照技术，只需分钟级别即可完成对上TB数据量大小的数据库的备份，且整个备份过程不需要加锁，效率更高，影响更小。

12.2.3. 应用场景

云原生关系型数据库PolarDB可广泛应用于各种业务场景中，满足不同业务的需求，提供高性能、高可用、高可扩展的数据库服务。

- PolarDB单节点架构是个人用户测试、学习的最佳选择，也可作为初创企业的入门级产品。
- PolarDB多节点架构适用于有大量流量高峰读请求和数据智能分析需求的大中型企业的生产数据库场景，如政务系统、互联网新零售行业、汽车制造行业、教育行业、企业大型ERP系统等。

12.3. 云数据库MongoDB版

云数据库MongoDB版（ApsaraDB for MongoDB）是一款完全兼容MongoDB协议的高性能文档数据库服务，基于飞天分布式系统和高可靠存储引擎，提供高可用、弹性扩容、读写分离、数据安全、备份恢复、智能运维和在线管理数据库等功能。

12.3.1. 产品详情

云数据库MongoDB版支持高可用、弹性扩容、读写分离、数据安全、备份恢复、智能运维和在线管理数据库等功能，为业务稳定提供保障。

高可用

灵活的部署架构

云数据库MongoDB版支持副本集架构和分片集群架构，可以满足不同的业务场景。

- 副本集架构：通过部署多种节点来达到高可用的效果，每个副本集实例包含一个Primary节点（主节点）、一个Secondary节点（从节点）和一个Hidden节点（隐藏节点），用户可以直接使用Primary节点和Secondary节点。
  - Primary节点：负责读写操作的节点，每个副本集实例中只能有一个Primary节点。
  - Secondary节点：通过oplog（操作日志）同步Primary节点的数据，可在Primary节点故障时通过选举成为新的Primary节点，保障高可用。

    > **说明** 通过Secondary节点的连接地址进行连接时，只能读取数据不能写入数据。

  - Hidden节点：通过oplog（操作日志）同步Primary节点的数据，可在Secondary节点故障时接替该故障节点成为新的Secondary节点，保障高可用。

    > **说明** Hidden节点仅用作高可用，对用户不可见。

- 分片集群架构：由Mongos节点、Shard节点和ConfigServer节点组成，用户可以自由地选择Mongos节点和Shard节点的个数和配置，组建服务性能不同的云数据库MongoDB版分片集群实例。
  - Mongos节点：负责将读写操作路由到对应Shard节点中。一个Mongos节点相当于一个主节点。
  - Shard节点：负责存储数据库数据。一个Shard节点相当于一个三节点副本集架构。

- ConfigServer节点：用于存储集群和Shard节点的元数据，即各Shard节点中包含的数据信息。一个ConfigServer节点相当于一个三节点副本集架构。

  > **说明** ConfigServer节点为固定规格（1核 2 GB，磁盘空间为20 GB），暂不支持修改。

主备切换

云数据库MongoDB版提供主备切换功能，当实例的某个节点发生故障时，系统会自动触发主备切换机制，保障功能的整体可用性。

同城容灾

为满足业务的高可用需求，云数据库MongoDB版提供了同城容灾功能。用户可以在创建实例时选择双可用区，当某一可用区因不可抗因素失去通信时，高可用系统将自动触发切换操作，确保实例持续可用。

弹性扩容

- 多种实例规格

  云数据库MongoDB版提供的副本集架构和分片集群架构均支持多种实例规格，用户可以根据实际需要灵活变配。

- 芯片架构

  云数据库MongoDB版支持多种芯片（例如X86和ARM），用户可以根据实际需要选择芯片架构，实现扩容、容灾或进行混合部署等。

读写分离

云数据库MongoDB版采用三节点副本集的高可用架构，三个数据节点位于不同的物理服务器上，自动同步数据。Primary节点（主节点）和Secondary节点（从节点）提供服务，两个节点分别拥有独立域名，配合MongoDB Driver实现读取压力分配。

数据安全

- DDoS防护

  云数据库MongoDB版支持DDoS防护功能，能够有效进行事前防护。

- IP访问白名单

  为保障数据库的安全稳定，云数据库MongoDB版提供对实例进行IP访问过滤功能，即将访问数据库的IP地址或IP段添加至目标实例的白名单中。正确使用白名单可以让云数据库MongoDB版得到高级别的访问安全保护，建议用户定期维护白名单。

- 专有网络

  专有网络是一种隔离的网络环境，安全性和性能均高于传统的经典网络。

- SSL加密

  为提高链路的安全性，用户可以启用SSL（Secure Sockets Layer）加密，然后安装SSL CA证书到相关的应用服务。SSL加密功能在传输层对网络连接进行加密，在提升通信数据安全性的同时，保证数据的完整性。

- 透明数据加密TDE

  透明数据加密TDE（Transparent Data Encryption）可对数据文件执行实时I/O加密和解密，数据在写入磁盘之前进行加密，从磁盘读入内存时进行解密。TDE不会增加数据文件的大小，用户无需更改任何应用程序，即可使用TDE功能。为提高数据安全性，用户可以启用TDE功能，对实例数据进行加密。

- 审计日志

  审计日志用于记录客户端连接后对数据库执行的所有操作，便于后续的故障分析、行为分析和安全审计等行为。审计日志能有效帮助用户获取数据的执行情况，加以自助分析。

备份恢复

- 数据备份
  云数据库MongoDB版提供自动备份和手动备份两种备份方法。
  - 自动备份

    云数据库MongoDB版提供设置备份时间和备份频率功能，用户可以根据业务需求设置备份时间和备份频率，实例将按照用户设置的时间和频率自动备份MongoDB数据。
  - 手动备份
    云数据库MongoDB版提供的备份实例功能，方便用户根据实际需求在任意时间对实例进行备份。
    - 物理备份：备份云数据库MongoDB版实例中数据库相关的物理文件，备份速度较逻辑备份更快，且恢复速度也更快。
    - 逻辑备份：通过mongodump工具将对数据库的操作记录存储到逻辑备份文件中。恢复时通过回放命令的形式还原数据。
- 下载备份文件

  云数据库MongoDB版固定保留备份文件7天，在此期间用户可以下载备份文件，使用备份文件恢复自建数据库。
- 数据恢复

  云数据库MongoDB版副本集实例支持数据回滚功能，即恢复备份数据到当前实例。

智能运维

- 全面监控

  云数据库MongoDB版提供了丰富的性能监控项，例如CPU使用率、内存使用率、磁盘空间容量等，方便用户查看和掌握实例的运行状态。
- 性能优化
  数据库自治服务DAS（Database Autonomy Service）是一种基于机器学习和专家经验实现数据库自感知、自修复、自优化、自运维及自安全的云服务，帮助用户消除人工操作引发的服务故障，有效保障数据库服务的稳定、安全及高效。
  - 性能趋势

    监控云数据库MongoDB版实例在某个时间段的基础性能及其运行趋势，包括CPU使用率、使用内存量、总连接数和网络流量等，还可以在自定义性能趋势图表中，选择仅展示部分基础性能指标，以便有针对性地监控和分析实例的性能及运行趋势。
  - 实时性能

    支持查看云数据库MongoDB版实例的读写延迟、QPS、操作统计、连接统计和网络流量等性能指标的实时数据，方便实时了解数据库性能情况。
  - 实例会话

    实时查看云数据库MongoDB版实例与客户端间的会话信息，包括客户端信息、所执行的命令和已连接的时长等，还可以根据业务需求终止异常会话。
  - 空间分析

    查询云数据库MongoDB版实例的空间概况、空间变化趋势、异常列表和数据空间，通过这些信息及时发现数据库中空间的异常情况，避免影响数据库稳定性。
  - 慢日志

    支持查看云数据库MongoDB版实例的慢日志信息，以发现、分析、诊断和跟踪慢日志，为构建索引提供参考依据，从而提升实例资源的利用率。

在线管理数据库

数据管理服务DMS（Data Management Service）是一种集数据管理、结构管理、用户授权、安全审计、数据趋势、数据追踪、BI图表、性能优化和服务器管理于一体的可视化、图形化数据管理服务。用户可以通过数据管理服务DMS登录云数据库MongoDB版数据库，并获取云数据库MongoDB版的数据库列表，然后在线管理云数据库MongoDB版的数据库。

12.3.2. 产品价值

云数据库MongoDB版是阿里云基于飞天分布式系统和高可靠存储引擎研发的一款完全兼容MongoDB协议的文档数据库服务，具有Schema Free（无固定模式）、高可用、弹性扩容、数据安全、智能运维、网络隔离和在线管理数据库等优势。

Schema Free（无固定模式）

云数据库MongoDB版采用Schema Free（无固定模式）的方式，免去用户变更表结构的痛苦。用户可以将模式固定的结构化数据存储在云数据库RDS中，模式灵活的业务存储在云数据库MongoDB版中，高热数据存储在云数据库Redis或云数据库Memcache中，实现对业务数据的高效存取，降低存储数据的投入成本。

高可用

- 高可用架构、同城容灾和自动备份功能，保障业务的可用性。
  - 云数据库MongoDB版支持三节点副本集和分片集群高可用架构，多个数据节点分别位于不同的物理服务器上，当某一节点发生故障时，其他节点可自动同步数据，保障实例的高可用性。
  - 云数据库MongoDB版支持创建双可用区实例，当某一可用区因不可抗力因素失去通信能力时，另一可用区的实例可自动同步数据，确保实例的持续可用性。
  - 云数据库MongoDB版支持自动备份功能，系统根据设置的备份时间自动备份数据并上传至对象存储OSS，提高数据容灾能力的同时有效降低磁盘空间占用。通过备份文件将实例数据恢复至原实例，有效防范因误操作等原因对业务数据造成不可逆的影响。
- 主备切换，保障功能可用性。

  云数据库MongoDB版提供主备切换功能，当实例的某个节点发生故障时，系统会自动触发主备切换机制，保障功能的整体可用性。

弹性扩容

- 灵活变更实例配置，满足业务性能。

  云数据库MongoDB版提供了变更实例配置功能，支持多种实例规格，用户可以根据业务需要变更实例的配置，快速应对业务变化。
- 支持多种芯片架构，实现混合部署。

  云数据库MongoDB版支持多种芯片（例如X86和ARM），用户可以根据实际需要选择芯片架构，实现扩容、容灾或进行混合部署等。

数据安全

- 事前防护

  云数据库MongoDB版支持DDoS防护功能。
- 事中防护
  - 设置IP白名单，提高数据库访问安全性。

    将访问数据库的IP地址或IP段添加至目标实例的白名单中，以保障数据库的安全稳定。
  - 设置SSL（Secure Sockets Layer）加密，提高链路安全性。

    SSL加密功能在传输层对网络连接进行加密，在提升通信数据安全性的同时，保证数据的完整性。用户可以启用SSL加密，然后安装SSL CA证书到相关的应用服务，以提高链路安全性。
  - 设置透明数据加密TDE（Transparent Data Encryption），提高数据安全性。

    透明数据加密TDE可对数据文件执行实时I/O加密和解密，数据在写入磁盘之前进行加密，从磁盘读入内存时进行解密。TDE不会增加数据文件的大小，用户无需更改任何应用程序，即可使用TDE功能。用户可以启用TDE功能，对实例数据进行加密，以提高数据安全性。
- 事后审计

云数据库MongoDB版支持将审计日志自动存储到日志服务中，并可通过日志服务下载日志，便于存储、管理审计日志信息。

智能运维

- 全面监控，方便运维人员了解实例状态。

  云数据库MongoDB版提供了丰富的性能监控项，例如CPU使用率、内存使用率、磁盘空间容量等，方便实时查看和掌握实例的运行状态。

- 性能优化，有效保障数据库服务的稳定、安全及高效。

  云数据库MongoDB版支持查看和自定义实例的性能趋势，实时查看实例性能，实例空间情况和慢日志，帮助用户消除人工操作引发的服务故障，有效保障数据库服务的稳定、安全及高效。

网络隔离

云数据库MongoDB版支持使用专有网络VPC（Virtual Private Cloud）来获取更高程度的网络访问控制。使用专有网络VPC和IP白名单将极大程度提升云数据库MongoDB版实例的安全性。

用户可以通过自定义专有网络中的路由表、IP地址和网关等解决资源冲突问题。

部署在专有网络VPC中的云数据库MongoDB版实例默认只能被同一个专有网络VPC中的ECS实例访问。如果需要，用户可以通过申请公网IP（申请公网IP前需要先设置白名单）接受来自公网的访问（不推荐），例如来自ECS EIP的访问和自建IDC公网出口的访问。

在线管理数据库

云数据库MongoDB版支持用户通过数据管理服务DMS（Data Management Service）登录数据库，并获取数据库列表，然后在线管理数据库。

12.3.3. 应用场景

云数据库MongoDB版采用Schema Free（无固定模式）的方式，免去用户变更表结构的痛苦，适用于灵活多变的业务场景，在游戏、移动APP和物联网等多个领域被广泛采用。

游戏

云数据库MongoDB版作为游戏服务器的数据库，用于存储用户信息。用户的游戏装备、积分等直接以内嵌文档的形式存储，方便进行查询与更新。

移动APP

云数据库MongoDB版支持二维空间索引，可以支撑基于位置查询的移动APP的业务需求。同时云数据库MongoDB版动态存储方式适合存储多重系统的异构数据，满足移动APP应用的需求。

物联网

- 云数据库MongoDB版的性能高，具有异步数据写入功能。
- 云数据库MongoDB版分片集群实例提供Mongos节点、Shard节点和ConfigServer节点三种组件，用户可以自由地选择Mongos节点和Shard节点的个数和配置，组建服务性能不同的云数据库MongoDB版分片集群实例，适合物联网高并发写入的场景。
- 云数据库MongoDB版提供二级索引功能满足动态查询的需求，利用云数据库MongoDB版的Map-Reduce聚合框架进行多维度的数据分析。

其他各领域

- 物流

  使用云数据库MongoDB版存储订单信息，订单状态在运送过程中会不断更新，以云数据库MongoDB版内嵌数组的形式来存储，一次查询就能将订单所有的变更读取出来，方便快捷且一目了然。

- 社交

- 使用云数据库MongoDB版存储用户信息以及用户发表的朋友圈信息，通过地理位置索引搜索附近的人、地点等。
- 使用云数据库MongoDB版存储聊天记录。

- 视频直播

  使用云数据库MongoDB版存储用户信息、礼物信息等。

12.4. 云数据库Redis版

云数据库Redis（KVStore for Redis）是兼容开源Redis协议标准的数据库服务，基于双机热备架构及集群架构，可满足高吞吐、低延迟及弹性变配等业务需求。

12.4.1. 产品详情

云数据库Redis支持多种架构，拥有数据可持久化存储、可用性高、弹性扩展和智能运维等特性。

架构灵活

标准架构

主备节点的数据实时同步，主节点提供日常服务访问，备节点提供高可用HA（High Availability）能力。当主节点发生故障，系统会切换至备节点以接管业务，保证业务平稳运行。

标准架构通常适用于以下场景：

- 对Redis协议兼容性要求较高的业务。
- 将Redis作为持久化数据存储使用的业务。
- 单个Redis性能压力可控的场景。
- Redis命令相对简单，排序和计算之类的命令较少的场景。

集群架构

由代理节点、数据分片和配置服务器组件构成，可通过增加数据分片的方式实现横向扩展。每个数据分片均为双副本（分别部署在不同机器上）高可用架构，主节点发生故障后，系统会自动进行主备切换保证服务高可用。

集群架构通常适用于以下场景：

- 数据量较大的场景。
- 整体读写请求的QPS压力较大的场景。
- 吞吐密集型、高性能应用场景。

读写分离架构

由代理节点、主从节点和只读节点构成。只读节点采取链式复制架构，扩展只读节点个数可使整体实例性能呈线性增长。

读写分离架构通常适用于以下场景：

- 读请求QPS压力较大的场景（如热点数据集中）。
- 对Redis协议兼容性要求较高的业务场景，例如规避集群架构的使用限制。

数据安全

数据备份与恢复

- 备份：基于RDB快照存储实现数据持久化，系统会按照默认的策略（每天发起一次备份）从备节点自动备份数据，用户可以根据业务需求修改备份策略，也可以手动发起临时的备份。

- 恢复：支持从指定的备份集恢复至当前实例或新实例，恢复至新实例时，新实例中的数据将和该备份集中的数据一致，可用于数据恢复、快速部署业务或数据验证等场景。
- 下载备份文件：备份文件会保留7天，如果需要更长时间的备份存档（例如监管或信息安全需要），用户可以将备份文件下载到本地进行存储。

多层网络安全防护

- 支持专有网络VPC，不同的专有网络之间二层逻辑隔离，拥有较高的安全性和性能。
- 结合云盾DDoS防护系统，实时监测并清除大流量攻击。
- 支持配置1000个以上IP地址白名单配置，隔绝非法访问，在连接实例前必须完成白名单设置。
- 支持密码访问鉴权方式，确保访问安全可靠；同一实例中，最多可创建20个账号，用户根据业务需求为账号设置相应的权限，从而更加灵活地管理实例，最大限度地避免误操作。
- 支持SSL（Secure Sockets Layer）加密，可在开启后安装SSL证书到应用服务，实现传输层对网络连接进行加密，在提升通信数据安全性的同时，保证数据的完整性。

深度内核优化

阿里云专家团队对Redis源码进行深度内核优化，有效防止内存溢出，修复安全漏洞。

高可用性

双副本

数据分片是由主备节点组成双副本，主备节点通过RDB+AOF实现数据实时同步。其中，主节点对外提供业务访问，备节点提供高可用HA（High Availability）能力。当主节点发生故障，系统会切换至备节点以接管业务，保证业务平稳运行。

冗余与自动检测

- 系统各组件采用冗余设计，节点故障后持续运行，无单点失败风险。
- 系统会自动侦测硬件故障，发生故障时能够进行故障转移，在数秒内恢复服务。

弹性扩展

Redis实例创建完成后，随着业务量的变化，如果实例的性能不足或者过剩，可通过变更实例的配置，调整实例的架构或内存规格，以满足不同场景下对实例的性能和容量需求。

智能运维

性能监控平台

支持丰富的性能监控指标（如CPU使用率、连接数等），支持查询过去一个月内指定时间段的监控数据，帮助用户掌握Redis服务的运行状况和问题溯源。

可视化管理平台

支持基于Web的可视化管理控制台，可提供丰富的运维和管理功能（例如备份数据、参数设置等），帮助用户便捷、可视化地管理实例。

数据库内核版本管理

云数据库Redis不断对内核进行深度优化、修复安全漏洞，提升服务稳定性，可在控制台的小版本升级功能，一键将内核升级至最新版本。

12.4.2. 产品价值

云数据库Redis版具有性能卓越、弹性扩容、资源隔离、数据安全、高可用、简单易用等诸多优势。

性能卓越

- 支持集群功能，提供128 GB及以上集群实例规格，可满足大容量和高性能需求。

- 提供32 GB及以下的主-从双节点实例，满足一般用户的容量和性能需求。
- 在不影响运行性能的前提下，支持单组件集群中使用的CPU、硬盘、内存、网卡规格不一致，可以最大限度地兼容已有设备。

弹性扩容

- 存储容量一键扩容：可根据业务需求通过控制台对实例存储容量进行调整。
- 在线扩容不中断服务：可在线进行调整实例存储容量，无需停止服务，不影响业务。

资源隔离

- 针对实例级别的资源隔离，可以更好地保障单个用户服务的稳定性。
- 具备多租户隔离能力从而避免相互影响，可控制不同实例所能使用的系统资源，包括CPU、内存、IO、磁盘空间等。
- 通过多实例方式，支持云平台集群下多租户并行执行，租户任务提交到不同的实例下的队列执行。通过划分Redis实例实现租户间资源隔离。

数据安全

- 数据持久化存储：采用内存+硬盘的存储方式，在提供高速数据读写能力的同时满足数据持久化需求。支持从持久化数据库中读取数据加载到缓存数据库。
- 数据主从双备份：所有数据在主从节点上进行双备份，确保数据不丢失。
- 访问控制：支持密码认证方式以确保访问安全可靠。
- 数据传输加密：支持安全套接层协议SSL（Secure Sockets Layer）和安全传输层协议TLS（Transport Layer Security）的安全加密，保障数据传输的安全性。

高可用

- 每个实例均有主从双节点：避免单点故障引起的服务中断。
- 硬件故障自动检测与恢复：自动侦测硬件故障并在数秒内切换，尽量减少突发硬件故障对服务的影响。
- 支持对集群内服务器硬盘故障自动容错处理，支持硬盘热插拔，故障硬盘的业务恢复时间小于2分钟。

简单易用

- 兼容Redis命令，任何Redis客户端都可以轻松地与Redis实例建立连接进行数据操作。
- 支持批量命令。

权限管理

- 支持数据访问权限管理，包括登录权限、创建表权限、读写权限、白名单控制权限等。
- 支持通过云管平台管理权限控制，包括管理员分级等。
- 通过云管平台，提供集中统一的用户权限管理功能，将系统中各组件零散的权限管理功能集中呈现和管理，对普通用户屏蔽掉内部的权限管理细节，对管理员简化权限管理的操作方法，提升权限管理的易用性和用户体验。
- 支持通过控制台，实现多租户统一管理，以及租户资源的动态配置和管理、资源隔离、资源使用统计等功能，支持多级租户的管理功能。

调度

支持多集群和多资源池的多租户调度。

12.4.3. 应用场景

云数据库Redis版在游戏行业、视频直播、电商行业都拥有丰富的应用场景。

游戏行业应用

游戏行业可以选择云数据库Redis版作为重要的部署架构组件。

Redis作为存储数据库使用

游戏部署架构相对简单，主程序部署在ECS上，所有业务数据存储在Redis中，作为持久化数据库。云数据库Redis支持持久化功能，主备双机冗余数据存储。

Redis作为缓存加速应用访问

Redis作为缓存层，加速应用访问，而数据则存储在后端的数据库（RDS实例）中。

Redis的服务可靠性至关重要，一旦Redis服务不可用，将导致后端数据库无法承载业务访问压力。云数据库Redis提供双机热备的高可用架构，保障极高的服务可靠性。主节点对外提供服务，当主节点出现故障，系统自动切换备用节点接管服务，整个切换过程对用户全部透明。

视频直播类应用

视频直播类业务往往会重度依赖Redis业务，存储用户数据及好友互动关系。

双机热备保障高可用

云数据库Redis版提供双机热备的方式，可以极大地保障服务的可用性。

集群版解决性能瓶颈

云数据库Redis版提供集群版实例，破除Redis单线程机制的性能瓶颈，可以有效地应对视频直播类流量突起，满足高性能的需求。

轻松扩容应对业务高峰

云数据库Redis版可支持一键扩容，整个升级过程对用户全透明，可以从容应对流量突发对业务产生的影响。

电商行业应用

电商行业大量采用Redis，多数应用在商品展示、购物推荐等模块。

秒杀类购物系统

大型促销秒杀系统，系统整体访问压力非常大，一般的数据库根本无法承载这样的读取压力。

云数据库Redis支持持久化功能，可以直接选择Redis作为数据库系统使用。

带有计数系统的库存系统

底层用RDS存储具体数据信息，数据库字段中存储具体计数信息。使用Redis实例来进行计数的读取，RDS实例存储计数信息。云数据库Redis部署在物理机上，底层基于SSD高性能存储，可以提供极高的数据存储能力。

12.5. 数据传输服务DTS

数据传输服务DTS（Data Transmission Service）是阿里云提供的一种支持关系型数据库及大数据等多种数据源之间数据交互的数据服务。相对于传统数据迁移或同步工具，DTS提供功能更丰富、传输性能更强、易用性更高且安全可靠的服务，帮助客户简化复杂的数据交互工作，客户可专注于上层的业务开发。

12.5.1. 产品详情

数据传输服务DTS（Data Transmission Service）包含数据同步、数据迁移、数据订阅等功能特性。

数据同步

数据同步功能旨在帮助客户实现数据源之间的数据实时同步。

数据同步具备多种特性，如下表所示：

特性	说明
动态增减同步对象	在数据同步过程中，客户可以随时增加或减少需要同步的对象。
完善的性能查询体系	数据同步提供同步延迟、同步性能（RPS、流量）趋势图，客户可以方便查看同步链路的性能趋势。
完善的监控体系	数据同步提供同步作业状态、同步延迟的报警监控功能。客户可以根据业务敏感度，自定义同步延迟报警阈值。

数据迁移

DTS的数据迁移功能支持同/异构数据源之间的数据迁移，同时提供了库表列三级映射、数据过滤等ETL特性，能帮助客户方便、快速地实现各种数据源之间的数据迁移。

DTS默认使用在线迁移，客户仅需配置迁移的源、目标实例及迁移对象即可，DTS会自动完成整个数据迁移过程。在线迁移支持数据不停服迁移，但要求DTS服务器能够同时跟源实例、目标实例连通。

数据迁移具备多种ETL特性，如下表所示：

特性	说明
库表列三级对象名映射	可以实现对源跟目标实例的库名、表名或列名不同的两个对象之间进行数据迁移。
迁移数据过滤	客户可以对要迁移的表设置SQL条件过滤要迁移的数据，例如客户可以设置时间条件，只迁移最新的数据。

数据订阅

数据订阅功能旨在帮助客户获取数据库的实时增量数据，客户可根据自身业务需求自由消费增量数据。

数据订阅具备多种特性，如下表所示：

特性	说明
动态增减订阅对象	在数据订阅过程中，客户可以随时增加或减少需要订阅的对象。
在线查看订阅数据	数据传输DTS控制台支持在线查看订阅通道中的增量数据。
修改消费时间点	数据订阅支持客户随时修改需要消费数据对应的时间点。
完善的监控体系	数据订阅提供订阅通道状态、下游消费延迟的报警监控功能。客户可以根据业务敏感度，自定义消费延迟报警阈值。

数据加工

DTS提供数据加工功能ETL，可实现数据的抽取、清洗转换和加载。同时在配置迁移或同步任务时，支持库列名映射、设置过滤条件，用于修改名称和筛选特定数据。

数据加工具备多种特性，如下表所示：

特性	说明
高计算时效性	通过DTS强大的数据库流式数据采集能力，ETL既保障了数据的准确性，同时也具备行业内高计算时效性。
灵活的任务监控与管理	ETL提供任务列表页以供任务监控和管理，能够对已经搭建的任务进行启停、查看详情等操作。

数据一致性

DTS通过日志读取和回放模块、数据校验和断点续传功能，保障源库和目标库数据的一致性。

12.5.2. 产品价值

相对于第三方的数据迁移或同步工具，DTS提供丰富多样、高性能、安全可靠的传输链路，同时也提供诸多便利功能，极大地方便了传输链路的创建及管理。

丰富多样

- DTS支持数据迁移、数据订阅及数据同步多种传输方式。

  > **说明** 数据订阅及数据同步均为实时数据传输方式。

- 数据迁移功能支持不停服的迁移方式，可实现数据迁移过程中应用停机时间降低到分钟级别。

高性能

- DTS使用高规格服务器来保证每条迁移同步链路都能拥有良好的传输性能。
- 相对于传统的数据同步工具，DTS的实时同步功能可将并发粒度缩小到事务级别，能够并发同步同张表的更新数据，极大提升同步性能。
- 解耦数据抓取及数据写入模块，实现数据抓取及数据写入的全并发，极大提高系统整体吞吐能力。
- 针对数据库中待迁移表采用多种智能分片策略，实现表间并发迁移和表内并发迁移，保证数据同步的并行能力并有效解决数据库数量、单表数据量过大问题。
- 采用高效的网络协议和数据压缩技术，减少长传链路的数据量，降低数据传输延迟，采用多TCP连接设计，提升异常网络环境下的同步性能及稳定性。
- 支持水平扩展能力，通过增加任务数量达到线性扩展。
- DTS底层使用多种性能优化措施。

安全可靠

- DTS内部对部分传输链路提供7×24小时的数据准确性校验，快速发现并纠正传输数据，保证传输数据可靠性。
- DTS底层为服务集群，集群内任何一个节点宕机或发生故障，控制中心都能够将这个节点上的所有任务快速切换到其他节点上。
- DTS各模块间采用安全传输协议及安全token认证，有效保证数据传输可靠性。
- 支持同城或跨城多机房部署，若其中一个机房发生故障，可以快速切换到另外一个机房。

简单易用

- DTS提供可视化管理界面，提供向导式的链路创建流程，客户可以在其控制台简单轻松地创建传输链路。
- DTS控制台展示了链路的传输状态及进度、传输性能等信息，客户可以方便管理自己的传输链路。
- DTS提供链路断点续传功能，可解决网络或系统异常等突发情况导致的链路中断问题，此功能可以定期监测所有链路的状态，一旦发现链路异常，先尝试自动修复重启，如果链路需要客户介入修复，那么客户可以直接在控制台修复，并重启链路。

12.5.3. 应用场景

数据传输服务DTS（Data Transmission Service）适用于不停服迁移数据库、加速全球化业务访问速度、数据异地灾备和异地多活等场景。

不停服迁移数据库

传统的迁移工具有无法保证数据的一致性、需要长时间停止服务等弊端，甚至在迁移过程中对业务的影响较大。DTS提供不停服迁移解决方案，让数据迁移过程中的业务停服时间降低到分钟级别。

不停服迁移的迁移类型包含结构迁移、全量数据迁移及增量数据迁移三个阶段。当进入增量数据迁移阶段时，目标实例会保持跟源数据库之间的数据实时同步，客户可以在目标数据库进行业务验证，当验证通过后，直接将业务切换到目标数据库，从而实现整个系统迁移。

> **说明** 在整个迁移过程中，仅当业务从源实例切换到目标实例期间，可能会产生业务闪断，其他时间业务均能正常服务。

加速全球化业务访问速度

对于客户分布比较广的业务，例如全球化业务，如果按照传统架构，只在单地区部署服务，那么其他地区的客户需要跨地区远距离访问服务，导致访问延迟大、客户体验差的问题。DTS将中心的数据实时同步到各个单元，各个地区的客户的读请求，可以路由到就近的单元，从而避免远距离访问，降低访问延迟，加速全球化访问速度。

快速搭建定制化BI系统

由于自建BI系统操作复杂，且无法满足越来越高的实时性要求。阿里云提供了非常完善的BI体系。DTS可以帮助客户将本地自建数据库的数据实时同步到阿里云的BI存储系统（例如MaxCompute、AnalyticDB或流计算），助力客户在阿里云上快速搭建满足自身业务定制化BI系统。

数据实时分析

为了在不影响线上业务的情况下实现实时数据分析，需要将业务数据实时同步到分析系统中，实时获取业务数据必不可少。DTS提供的数据订阅功能，可以在不影响线上业务的情况下，帮助客户获取业务的实时增量数据，通过SDK将其同步至分析系统中进行实时数据分析。

轻量级缓存更新策略

DTS提供的数据订阅功能，可以帮助客户异步订阅数据库的增量数据，并更新缓存的数据，保证数据完整性、实现轻量级的缓存更新策略。

这种缓存更新策略的优势如下：

- 更新路径短，延迟低

  缓存失效为异步流程，业务更新数据库完成后直接返回，不需要关心缓存失效流程，整个更新路径短，更新延迟低。

- 应用简单可靠

  应用无需实现复杂双写逻辑，只需启动异步线程监听增量数据，更新缓存数据即可。

- 应用更新无额外性能消耗

  因为数据订阅是通过解析数据库的增量日志来获取增量数据，获取数据的过程对业务、数据库性能无损。

业务异步解耦

DTS提供的数据订阅，可以将深耦合业务优化为通过实时消息通知实现的异步耦合，让核心业务逻辑更简单可靠。

读能力横向扩展

对于有大量读请求的应用场景，单个数据库实例可能无法承担全部的读取压力。客户可以使用DTS的实时同步功能构建只读实例，利用这些只读实例承担大量的数据库读取工作负载，实现读取能力的弹性扩展，分担数据库压力。

12.6. 数据管理DMS

数据管理DMS（Data Management Service）是一款支撑数据全生命周期的一站式数据管理平台，致力于无缝打通OLTP、OLAP和NoSQL等数据源，支持超过10种数据源的统一管理。提供全域数据资产管理，数据库设计开发和数据集成、开发、消费、治理等能力，致力于帮助企业高效、安全地挖掘数据价值，助力企业数字化转型。

12.6.1. 产品详情

数据管理DMS按照使用场景划分了7个功能模块，包括：数据资产、SQL窗口、数据库开发、集成与开发（DTS），安全与规范、解决方法和运维管理。

数据资产

- 实例管理：查看、录入、编辑实例信息，对实例进行授权、回收权限、禁用、启用、删除等管理操作。
- 数据类目：对实例、库、表进行业务分类归属管理，便于管理人员、开发人员及运维人员更好地管理或使用数据表。
- 敏感数据管理：对企业内的所有中、高敏感字段进行统一管理，增强对敏感数据的管控。

SQL窗口

- 可视化操作区域：查看当前数据库的所有表、字段、索引数据，对目标表进行表结构编辑、数据导入、数据导出等操作。
- SQL命令区域：编写SQL命令，支持对SQL语句进行格式化与执行，支持对结果集进行编辑、更新。
- 执行结果区域：查看执行结果和执行历史。
- 提供快捷操作功能：表列表、同步元数据、导出、表结构版本管理、操作审计、风险审计、超级SQL模式等。

数据库开发

- 结构变更
  - 结构设计：对目标库表进行符合研发规范的表结构设计。可按需自定义不同业务线的研发流程，保障多套环境（例如开发环境、测试环境、生产环境）之间结构的一致性。
  - 结构同步：对比不同数据库之间的表结构，产生差异化脚本并执行到目标数据库。适用于对比、同步多套数据库环境的表结构。
  - 影子表同步：根据源表的表结构自动创建影子表，适用于全链路压测等场景。
  - 空库初始化：将源数据库的表结构同步至空数据库中，实现快速同步数据库表结构，适用部署多区域、多单元的数据库环境。
  - 表一致性修复：基于一个基准表，对比一批目标表，产生差异化脚本并执行到目标环境。用于保障两套环境之间的结构一致性，或对比逻辑库分库的表结构一致性。
- 数据变更
  - 普通数据变更：支持INSERT、UPDATE、DELETE、TRUNCATE等SQL语句，用于数据初始化、历史数据清理、问题修复、功能测试等。
  - 历史数据清理：定期清理历史数据，防止历史数据堆积对生产环境的稳定性产生影响。
  - 数据导入：支持大批量数据快速导入至数据库，节省人力物力成本。
- 无锁变更
  - 无锁数据变更：满足客户对大量数据变更的需求，减小数据变更对数据库性能、数据库空间等的影响，保证执行效率。
  - 无锁结构变更：解决结构变更时的锁表问题，较好地规避数据库锁表和主备延迟现象。
- 数据导出
  - SQL结果集导出：导出SQL查询语句的结果集。
  - 数据库导出：导出数据库和部分表，或导出数据库、部分表的表结构或表数据，用于提取相关数据进行数据分析。
- SQL审核：对SQL语句进行审核并提供优化建议，避免无索引或不规范的SQL语句，降低SQL注入风险。
- 数据库克隆：提供库级别的数据复制能力，可以用于整库数据同步，多环境数据库初始化。
- 测试数据构建：支持批量生成各类随机值、地区名、虚拟IP地址等信息，大大减轻准备测试数据的负担。
- DevOps：自定义研发流程和控制研发流程质量，合理有效地保障研发流程顺利开展，减少误操作，保护

数据安全，提高开发效率。

集成与开发（DTS）

- 数据传输、迁移
  - 数据迁移：实现同构、异构数据源之间的数据迁移，适用于数据上云迁移、阿里云内部跨实例数据迁移、数据库拆分扩容等业务场景。
  - 数据订阅：获取、消费数据库的实时增量数据，适用于缓存更新策略、业务异步解耦、异构数据源的数据实时同步和复杂ETL的数据实时同步等业务场景。
  - 数据同步：实现数据源之间的数据实时同步，适用于数据异地多活、数据异地灾备、本地数据灾备、跨境数据同步、查询与报表分流、云BI及实时数据仓库等业务场景。
  - 异构数据库迁移（ADAM）：提供数据库平滑迁云解决方案。全面评估数据库上云可行性、成本和云存储选型，帮助企业降低数据库和应用迁移的风险、技术难度和实施周期。
- 数据集成、开发、应用
  - 批量加工：低代码数据开发工具，批处理复杂大数据，用于企业精细化运营、数据营销、智能推荐等大数据业务场景。
  - 流式加工：实时数据加工工具，流式数据抽取、转换、加工和装载。丰富企业实时数据处理和计算场景，赋能企业数字化转型。
  - 任务编排：支持复杂的任务编排与调度，提高数据开发效率。
  - 数据服务：快速对外输出DMS上的受管数据，只对外暴露最小单元的数据，保障数据安全。
  - 数据可视化：将数据库中的数据以多种可视化方式展现出来，直观呈现业务，有助于洞察业务，辅助业务决策。

安全与规范

- 权限：申请实例、数据库、表、数据列、数据行的查询、变更、导出、登录权限。
- 安全规则：通过精细化管控数据库的规则集合，打造数据库的操作规范和研发流程。
- 审批流程：根据不同的用户行为选择或设置不同的审批流程。
- 访问IP白名单：对企业内员工使用DMS的范围进行有效管控，达到仅在部分特定信任网络环境下使用DMS的效果。
- 操作审计：查询SQL窗口产生的SQL语句列表、工单列表、登录列表、操作日志等，方便快速地定位、排查数据库问题以及提供审计用途。
- 敏感数据管理：帮助企业及时有效地发现与识别敏感数据资产，避免敏感数据滥用，有效保护企业的敏感数据资产。

解决方案

T+1全量数据快照：以天或小时为周期将业务表的全量数据入仓，方便以日或月为维度进行统计分析。例如，统计截止前一天的订单总额，了解业务运行情况。

运维管理

- 用户管理：添加、删除DMS用户，管控用户权限，授权实例、数据库、表、行、敏感列。
- 任务管理：新建SQL任务或管理任务。
- 配置管理：更改DMS系统层面的配置，实现更灵活的管理需求。例如，开启云上实例资源自动同步。
- 数据库分组：将多个环境或引擎类型相同的数据库绑定为一个分组，在SQL变更或结构设计中快速载入分组中的所有数据库，变更会对分组中的所有数据库生效。

12.6.2. 产品优势

DMS支持丰富的数据源、操作流程安全可控、细粒度的权限管控等功能，极大提升了数据管理的便捷性和安全性。

丰富的数据源支持

- 关系型数据库：
  - MySQL：云数据库RDS MySQL、云原生数据库PolarDB-X、其他云厂商MySQL、自建MySQL
  - SQL Server：云数据库RDS SQL Server、其他云厂商SQL Server、自建SQL Server
  - PostgreSQL：云数据库RDS PostgreSQL、其他云厂商PostgreSQL、自建PostgreSQL
  - 自建达梦数据库DamengDB
  - 自建Oracle
  - 云数据库OceanBase、自建OceanBase
- NoSQL数据库：Redis：云数据库Redis、其他云厂商Redis、自建RedisMongoDB：云数据库MongoDB、其他云厂商MongoDB、自建MongoDB图数据库GDB（Graph Database）
- OLAP数据库：云原生数据仓库AnalyticDB MySQL云原生数据仓库AnalyticDB PostgreSQL

统一的操作入口且支持审计

- 管理员录入数据库实例后，数据库的查询、变更结构、变更数据等需求均可以在DMS平台内完成。
- 所有操作可按照人员、数据库、表、时间等多维度进行搜索审计。

细粒度的权限管控

普通用户不再接触数据库账号和密码，只需根据实际需要在DMS平台内申请目标库、表或字段的查询、导出、变更权限，权限到期后DMS会自动回收。

可定制的审批流程

每个数据库实例可定义满足业务实际需要的各模块审批流程，可同时满足效率、安全等维度的要求。例如：

- 测试环境轻管控，可减少流程或不设置流程。
- 生产环境重管控，可配置具体操作经过指定人员逐层审批后方可生效执行。

自定义表结构设计规范

可按照需求自定义MySQL表结构的设计规范，例如字段类型、索引类型、索引个数、字段名长度、表名长度、发布流程等相关规范。

便捷的周期任务编排调度

可快速搭建各种数据库SQL任务节点编排、周期调度，实现历史数据转储、周期报表产出等便捷的数据价值挖掘。

12.6.3. 应用场景

数据管理DMS主要应用于数据安全与研发效能保障、上云迁移、容灾多活、T+1数仓建设、实时数仓建设、跨实例查询等场景中。

数据安全与研发效能保障

将数据库实例接入DMS，通过自定义安全规则和敏感数据识别、脱敏规则，保障数据安全及稳定性。基于DMS定时任务及SQL变更窗口，解决人工运维的困境。

- 能够解决：
  - 效率低下，运维、变更全靠人进行沟通操作，运维人员成瓶颈的问题。
  - 稳定性受挑战，人工维护数百个实例，无法提前发现并预防故障发生的问题。
- 优势：
  - 通过DMS管控大批量实例，真正实现研发全自助，提升效能。
  - 通过DMS，从0到1构建企业数据安全防护体系，保障企业数据安全。

T+1数仓建设

将业务表的数据按照每天或每小时1次的频率在数据仓库中形成数据快照，方便用户以小时、日、月等时间维度对数据进行统计分析。

- 能够解决：
  - 传统T+1数仓建设涉及的计算量非常大，需要使用复杂逻辑将T+1增量数据与全量数据进行聚合，影响T+1数据生成效率的问题。
  - 增量数据采用实时或定时方式拉取，对业务系统影响较大的问题。
  - 无法支持任意时间点的数据切片的问题。
- 优势：
  - 生命周期拉链表实时增量更新，生成小时快照、天快照效率较传统方案提升5倍。
  - DTS无插件和日志解析的方式对生产系统消耗极少，不影响业务系统正常运行。
  - 支持任意时间点的数据切片。

跨实例查询

为不同环境的在线或异构数据源提供及时的关联查询服务。支持MySQL、SQL Server、PostgreSQL、Redis等不同类型数据库，不论数据库实例部署在哪个地域或环境，通过一条SQL就能实现这些数据库实例之间的关联查询。

能够解决：

- 垂直、水平拆分后的跨数据库查询：常见的商品库、订单库的实时关联查询，多地域、多单元的汇总关联查询。
- 异构数据库的关联查询：数据从SQLServer迁移至MySQL，进行关联查询做一致性对比。
- 混合云场景的关联查询：本地IDC自建环境与跨云环境进行数据关联查询。

12.7. 云原生数据仓库AnalyticDB MySQL版

云原生数据仓库 AnalyticDB MySQL 版是阿里巴巴针对海量数据分析自主研发的实时高并发在线分析RT-OLAP（Realtime OLAP）云计算服务，支持对千亿级数据进行即时的（毫秒级）多维分析透视和业务探索。 作为海量数据下的实时计算系统，AnalyticDB for MySQL给使用者带来了极速的、自由的大数据在线分析计算体验。

12.7.1. 产品详情

AnalyticDB for MySQL提供系统资源管理、集群管理、数据库管理、账号与权限管理。

系统资源管理

云原生数据仓库 AnalyticDB MySQL 版中通过ECU（弹性计算单元）进行资源管理，通过操作系统底层技术和飞天操作系统提供分布式资源调度能力。

AnalyticDB for MySQL为每个数据库集群创建完全独立的控制节点、计算节点、存储进程。用户可以通过控制ECU规格和节点组数量来控制控制节点、计算节点、存储进程的配置。通过ECU规格可以区分的资源包括CPU核数、内存大小（独占）以及磁盘大小。

集群管理

- **集群变配**：云原生数据仓库 AnalyticDB MySQL 版支持变更集群的配置，如增减基础版集群的节点组数量，或增减弹性版集群的计算节点与存储节点资源。
- **集群监控**：通过云原生数据仓库 AnalyticDB MySQL 版控制台实时查看集群监控信息，包括查询响应时间、写入响应时间、磁盘使用量等。

数据库管理

- **兼容MySQL**：

  - 云原生数据仓库 AnalyticDB MySQL 版兼容MySQL、支持JDBC、ODBC标准访问接口。
  - 支持MySQL生态的多种开发工具。例如，DMS控制台、MySQL命令行客户端、DBeaver、Navicat、SQL WorkBench/J等工具。
  - 采用关系模型存储，可以使用SQL进行自由灵活地计算分析，无需预先建模。
  - 支持主流数据类型，包括数值型、字符型、日期型、二进制型等各种数据类型。
- **支持行列混存**：AnalyticDB for MySQL支持单表物理混合存储的行列混存模式，能够轻松面对混合负载的业务场景。
  - OLTP明细查询：OLTP中的明细查询通常需要通过SELECT查询一整行的明细数据，这一类查询的特点是单次I/O即可实现整行数据的读取和写入。AnalyticDB for MySQL的数据查询特点为以较小的I/O代价快速返回您需要的查询结果。
  - OLAP大规模多维分析：主要是海量数据的统计分析、JOIN等，并且大部分是针对宽表中的某几列进行统计查询，AnalyticDB for MySQL更加擅长处理OLAP场景下的负载。
  - 吞吐量大：支持每天千亿级别的实时数据写入。
- **数据一致性**：AnalyticDB for MySQL支持数据强一致性（即数据实时可见性），写入和更新数据后可以立即查询生效。
- **元数据**：`TABLES` 存储数据库集群内所有的数据表基本信息。`USER_PRIVILEGES` 存储数据库集群内所有用户授权信息。`COLUMNS` 存储数据库集群内所有表的每个字段定义信息。
- **DDL**：支持通过DDL创建表、修改表属性、修改索引、已创建的表中增加列、查看全部有权限的数据库列表等。
- **DML**：AnalyticDB for MySQL与标准MySQL的查询兼容高达95%以上，可以方便、灵活地使用SELECT语句进行数据查询。支持通过INSERT、DELETE、UPDATE更新数据库中的数据。
- **数据迁移与同步**：
  - 通过阿里云数据集成服务将MaxCompute、OSS、MySQL、Oracle、SQLServer中的数据同步至AnalyticDB for MySQL。
  - 通过Kettle将关系型数据库、Hbase等NoSQL数据，以及Excel、Access中的数据同步至AnalyticDB for MySQL。
  - 通过INSERT外表方式将OSS数据导入AnalyticDB for MySQL或者将AnalyticDB for MySQL数据导出到OSS。
  - 通过LOAD DATA将本地数据写入AnalyticDB for MySQL。
  - 如果数据已经存在于AnalyticDB for MySQL数据库的其他表中，可以通过 `INSERT INTO...SELECT FROM` 同步数据。
- **全文索引**：AnalyticDB for MySQL支持SQL 92标准、兼容MySQL协议，具备结构化数据、非结构化数据的融合检索和多模分析能力，以及完善的分布式JOIN、GROUP BY、AGGREGATION能力。通过SQL语言提供全文检索功能，极大的降低了用户的学习成本。且AnalyticDB for MySQL将常用的结构化数据分析与灵活的非结构化数据分析进行了统一，使用同一套SQL语言来操作多种类型数据，大幅降低了开发成本。
- **备份恢复**：AnalyticDB for MySQL支持全量备份和日志备份，用户可以自定义备份周期和频率以及备份时间。
- **数据库诊断**：云原生数据仓库 AnalyticDB MySQL 版提供慢SQL分析功能，能够查看慢日志趋势和统计信息，并且提供SQL建议和诊断分析。
- **数据库白名单**：支持设置AnalyticDB for MySQL集群的白名单，以允许外部设备访问该集群。

账号与权限管理

AnalyticDB for MySQL支持标准MySQL模式的权限模型。

- 支持对数据库、表、列级别进行ACL授权。
- 支持数据库管理员账号授权给任意合法账号。
- 支持每个角色授予不同的权限。
- 支持ADD USER/REMOVE USER语句添加和删除用户。

- 支持GRANT语句进行授权，REVOKE语句进行权限回收。
- 支持SHOW GRANTS ON语句查看各级对象上的用户权限。
- 支持LIST USERS语句查看全部有权限的用户。
- 数据库管理员账号：集群初始建立时创建的账号，具有创建数据库普通账号和授权权限。
- 数据库普通用户：在被授权的情况下，有对数据库各项DDL、DML权限。

12.7.2. 产品价值

AnalyticDB for MySQL是一套RT-OLAP系统，采用关系模型存储、分布式计算技术，具有强大的实时计算能力，能够支撑较高并发查询量，同时通过动态的多副本数据存储计算技术也保证了较高的系统可用性。

优势	描述
海量数据计算能力	支持计算单表万亿记录、PB级别的数据。
全量数据分析	数据分析中使用的不再是抽样数据，而是全量数据，分析结果具有最大的代表性。
查询响应极速	支持在毫秒级内对百亿级数据进行多维透视。
高并发、高可用	支持高并发查询量，并且通过动态的多副本数据存储计算技术来保证系统的高可用性，能够直接作为面向最终用户（End User）产品（包括互联网产品和企业内部的分析产品）的后端系统。
查询形式自由灵活	支持通过SQL灵活地对海量数据进行多维分析、数据透视、数据筛选。
数据导入多通道并行	支持离线通道、在线通道双模式并行数据导入，导入性能随集群规模线性扩展。
安全机制精细	支持精确到列级别的权限管理和超细粒度的用户操作审计，通过公私钥机制保护数据安全。
兼容性良好	兼容MySQL协议（包括数据元信息）、兼容商业分析工具和应用、内置支持多种数据源数据快速接入，大幅度降低业务系统和商业软件的接入成本。
隔离	具备多租户隔离能力从而避免实例间的相互影响，可控制不同实例所能使用的系统资源，包括CPU、内存、IO、磁盘空间等。
权限	支持通过控制台实现租户统一管理、租户资源的动态配置和管理、资源隔离以及资源使用统计等功能，同时也支持多级租户的管理功能。

12.7.3. 应用场景

AnalyticDB for MySQL在电商、广告、金融等行业拥有诸多成熟的使用场景。

应用场景	描述
电商行业	A-CRM、爆款选品、自动化运营、SKU组合分析等。
O2O	数据分析和CRM系统、地理围栏系统。
广告行业	数字营销，M-DMP系统。
金融行业	实时多维数据分析、交易流水查询系统、报表系统等。
大安全	人群透视分析，潜在关键元素挖掘，关系网络分析，明细查询等。

交通、交警	车辆卡口数据分析和研判。
物流和物联网	车联网数据分析、企业安监数据分析、传感器数据存储和检索、物流实时数据仓库。

12.8. 云原生数据仓库AnalyticDB PostgreSQL版

云原生数据仓库AnalyticDB PostgreSQL版是一种分布式分析型数据库，采用MPP架构，由多个计算节点组成，存储和计算能力可水平扩展，提供大规模并行处理数据仓库服务，支持PB级数据的在线分析和离线ETL任务处理。

12.8.1. 产品详情

云原生数据仓库AnalyticDB PostgreSQL版基于PostgreSQL内核，具备分布式架构、高性能数据分析、服务高可用、数据安全、数据同步等功能特性。

分布式架构

云原生数据仓库AnalyticDB PostgreSQL版基于MPP分布式大规模并行处理架构，数据按HASH值或Random方式均匀分布在各个节点间，分析计算在节点间全并行执行。通过增加节点，实现存储和计算能力的水平扩展，保证数据量增加而查询响应时间不变。

云原生数据仓库AnalyticDB PostgreSQL版支持分布式事务，保证节点间的数据一致性，支持三种数据库事务隔离级别，即SERIALIZABLE，READ COMMITTED，READ UNCOMMITTED 。

高性能数据分析

云原生数据仓库AnalyticDB PostgreSQL版支持表按列存储或者按行存储。行存储具备高性能更新处理性能，列存储具备高性能OLAP聚合分析性能。AnalyticDB PostgreSQL版支持BTree，Hash，BitMap索引，实现高性能分析过滤查询。

云原生数据仓库AnalyticDB PostgreSQL版采用Cascade架构SQL优化器，通过基于代价优化（CBO）和基于规则优化（RBO）相结合，实现子查询自动解关联等SQL优化功能，复杂分析语句免调优。

服务高可用

云原生数据仓库AnalyticDB PostgreSQL版基于阿里云飞天平台构建系统自动监控、诊断、故障处理体系，简化运维。

协调节点保存数据库元信息，并接收客户端查询请求，完成SQL语句的编译和优化工作。协调节点采用主备模式（Master/Slave），保证元信息的强同步一致性。如果主协调节点（Master）发生故障，系统将实现故障自动检测切换并自愈。

所有计算节点（Segment）均采用主备（Primary/Minor）模式，数据写入和更新在主备计算节点间强同步，保证双份存储。如果计算节点发生故障，系统将实现故障自动检测切换并自愈。

云原生数据仓库AnalyticDB PostgreSQL版支持对集群内服务器硬盘故障自动容错处理，支持硬盘热插拔，故障硬盘的业务恢复时间原则上可小于2分钟。

数据同步及工具

MySQL/PostgreSQL数据库支持通过DTS或Dataworks数据集成工具进行数据同步到云原生数据仓库AnalyticDB PostgreSQL版，目前业界流行的ETL工具均支持以云原生数据仓库AnalyticDB PostgreSQL版为目标的ETL数据导入和作业调度。同时云原生数据仓库AnalyticDB PostgreSQL版可将存储于OSS中的格式化文件作为数据源，通过外部表模式进行实时操作，使用标准SQL语法实现数据查询。

云原生数据仓库AnalyticDB PostgreSQL版支持业界主流的BI报表工具，包括QuickBI、DataV、Tabular、帆软等。支持业界主流的ETL工具，包括Informatic、Kettle等。

数据安全

云原生数据仓库AnalyticDB PostgreSQL版支持IP白名单配置，最多支持配置1000个允许连接数据库实例的服务器IP地址，从访问源进行直接的风险控制。支持DDoS防护在网络入口实时监测，当发现超大流量攻击时，对源IP进行清洗，清洗无效情况下可以直接拉进黑洞。

通过pgcrypto插件，可在表或列级别，使用加密算法函数MD5、SHA1、SHA224/256/384/512、Blowfish、AES128/256、Raw Encryption、PGP Symmetric-Key、PGP Public Key，对数据进行安全加密存储。

云原生数据仓库AnalyticDB PostgreSQL版具备完善的权限认证与隔离机制，保障用户数据的私密性。支持通过多租户模式实现资源隔离。

SQL功能支持

- 支持数据按行存储或者按列存储。
- 支持多种索引，包括B-Tree、Bitmap、Hash索引。
- 支持分布式事务和标准隔离级别，数据在节点间保持一致性。
- 支持字符、日期、数学系统函数。
- 支持存储过程、UDF、触发器。
- 支持视图。
- 支持表按区间或值进行表分区，支持多级表分区定义。
- 支持分区表以及多种分区管理操作，包括新增分区、删除分区、重命名分区、清空截断分区、交换分区、分裂分区等。
- 支持33种内置数据类型。

12.8.2. 产品价值

云原生数据仓库AnalyticDB PostgreSQL版具备实时分析、稳定可靠、简单易用、性能卓越、灵活扩展、资源隔离、权限管理、资源调度、多芯片混部等产品优势。

实时分析

MPP水平扩展架构，PB级数据查询秒级响应；向量化计算，及列存储智能索引，领先传统数据库引擎；Cascade架构SQL优化器，复杂分析语句免调优。

稳定可靠

支持分布式ACID数据一致性，实现跨节点事务一致，所有数据双节点强同步冗余。分布式部署，全透明化监控、切换、恢复，提高重要数据基础设施保障。

简单易用

丰富的SQL语法及函数支持，众多Oracle函数支持，支持存储过程、UDF、支持事务和数据库隔离级别。业界主流BI软件和ETL工具可直接联机使用。

性能卓越

支持行存储和列存储，支持多种索引机制。向量引擎分析计算性能卓越，Cascade SQL优化器实现复杂查询免调优。支持高性能云存储数据OSS并行数据导入。

灵活扩展

- 按需等比扩展计算单元，CPU、内存、存储空间，从而提高OLAP性能。
- 支持透明的OSS数据操作，非在线分析冷数据可灵活转存到OSS对象存储，数据存储容量无限扩展。
- 在线扩容后，数据重分布过程中支持数据增、删、改、查。

资源隔离

通过多实例方式，支持云平台集群下多租户并行执行，租户任务提交到不同的实例下的队列执行。通过划分AnalyticDB PostgreSQL实例实现租户间资源隔离。

权限管理

支持通过控制台，实现的租户统一管理，实现租户资源的动态配置和管理、资源隔离、资源使用统计等功能，支持多级租户的管理功能。

资源调度

支持多集群和多资源池的多租户调度。

多芯片支持

支持ARM架构集群和X86架构集群混部。

12.8.3. 应用场景

云原生数据仓库AnalyticDB PostgreSQL版适用于多种OLAP数据分析业务，在企业数据仓库、大数据分析平台、数据湖分析等场景中得到广泛应用。

OLAP数据分析业务

- ETL离线数据处理：复杂SQL优化，海量数据大规模聚合分析。
  - 支持标准SQL，OLAP窗口函数，存储过程。
  - Cascade分布式SQL优化器，实现复杂查询免调优。
  - MPP架构支持存储和计算能力水平扩展，支持PB级数据分析处理。
  - 支持数据按列存储，实现高性能大表关联聚合，同时提供高压缩比，节省存储空间。
- 在线高性能查询：任意维度数据即时探索，数据实时入库更新。
  - 高吞吐数据写入及更新（INSERT/UPDATE/DELETE）。
  - 基于行存储及多种索引（B-Tree,Bitmap，Hash Index）实现点查询毫秒级返回。
  - 支持分布式事务，标准数据库隔离级别，支持HTAP混合负载。
- 多模数据分析：多种非结构化数据源。
  - 支持PostGIS插件扩展，实现地理数据分析处理。
  - 通过MADlib插件扩展，内置多种机器学习算法，实现AI Native DB。
  - 支持通过向量检索，实现非结构化数据（图片，语音，文本）的高性能检索分析。
  - 支持JSON等格式，支持日志等半结构化数据处理分析。

企业数据仓库

生产交易系统数据，包括云数据库RDS MySQL、PostgreSQL、PolarDB等或传统数据库Oracle、SQL Server，通过数据传输服务（DTS）实时同步数据；或通过数据集成服务（DataX）批量同步数据到AnalyticDB PostgreSQL版。AnalyticDB PostgreSQL版支持海量数据的ETL处理操作，这些任务也可以被Dataworks进行调度。同时支持高性能在线分析，支持QuickBI、DataV、Tableau、帆软等做报表展现和即时查询。

大数据分析平台

对于MaxCompute、Hadoop、Spark中保存的海量数据，可通过数据集成服务或通过OSS云存储中转，快速批量导入到AnalyticDB PostgreSQL版 ，做高性能分析处理和在线数据探索。

数据湖分析

AnalyticDB PostgreSQL版可以通过外部表机制，高并行直接访问海量云存储OSS上的数据，构筑阿里云统一数据湖分析平台。

12.9. 云原生多模数据库Lindorm

云原生多模数据库Lindorm是面向物联网、互联网、车联网等场景设计的云原生多模超融合数据库，支持宽表、时序、文本、对象、流、空间等多种数据的统一访问和融合处理，兼容多种开源标准接口，集成三方生态工具。

12.9.1. 产品详情

云原生多模数据库Lindorm是一款适用于多种模型的云原生数据库服务。根据业务需求，用户可以使用阿里云提供的控制台来创建云原生多模数据库Lindrom实例、升级实例的引擎版本、扩缩容节点或者释放实例。

实例

实例是云原生多模数据库Lindorm为用户业务提供服务的最小单位，不同的实例规格提供的计算与存储能力不同。一个Lindorm实例可以存储和计算多种模型的数据，例如宽表、时序、文本、对象、流、空间等。

存储引擎

云原生多模数据库Lindorm支持宽表引擎、时序引擎、搜索引擎、文件引擎等存储引擎，兼容HBase/Cassandra/S3、OpenTSDB、Solr、HDFS、Kafka等多种开源标准接口，同时提供SQL查询、时序处理、文本检索分析等能力。

网络

- 专有网络

  专有网络VPC（Virtual Private Cloud）是用户自己独有的云上私有网络，不同的专有网络之间通过二层逻辑隔离，拥有较高的安全性和性能。Lindorm-cli部署在ECS实例上时，通过专有网络连接至Lindorm实例，可获得更高的安全性和更低的网络延迟。

- 公网

  公网即互联网，当本地设备需要连接至Lindorm实例时，用户可以为Lindorm实例申请公网连接地址。通过公网连接可能存在一定的安全风险，推荐通过专有网络连接以获取更高的安全性。

弹性伸缩

云原生多模数据库Lindorm支持弹性伸缩能力，根据用户业务需求和策略，自动调整其弹性计算资源大小和存储资源大小的管理服务，能有效降低基础设施成本和运维成本。

- 云原生多模数据库Lindorm的存储资源支持秒级在线扩缩，计算资源（宽表引擎、时序引擎、搜索引擎）支持分钟级在线扩缩。
- 云原生多模数据库Lindorm支持各个引擎的节点变配功能，可以快速弹性扩展，高效地应对业务量高峰。

多模超融合

- 云原生多模数据库Lindorm支持多种模型之间数据互通，例如搜索引擎可以无缝作为宽表引擎和时序引擎的索引存储，提高多维检索与分析的速度。
- 云原生多模数据库Lindorm具备数据接入、存储、检索、计算、分析等一体化融合处理能力。
- 云原生多模数据库Lindorm支持统一的SQL访问，可以跨多模引擎关联查询。

冷存储

云原生多模数据库Lindorm支持冷存储功能，可以存储数据库中的冷数据，从而降低存储成本。用户可以根据需求设置冷热分界线自动将表中的冷、热数据分类归档至冷、热存储中。

二级索引

云原生多模数据库Lindorm宽表引擎支持高性能原生二级索引功能。高性能原生二级索引功能支持为单表创建多个索引表，每个索引表有不同的存储策略（例如压缩算法或者冷热分离策略）。确保主表和索引表数据的一致性，索引表的数据会自动被更新，可以提高写入效率。

数据生态服务

云原生多模数据库Lindorm通过LTS（Lindorm Tunnel Service）完成数据的导入和迁移。LTS是面向Lindorm业务场景特点定制的数据生态服务，可以满足用户的数据迁移、实时订阅、数湖转存、数仓回流、单元化多活、备份恢复等需求。

集群管理系统

- Lindorm宽表引擎提供集群管理系统，通过集群管理系统可以对实例进行智能运维，包括以下内容：
  - 查看实例的各个可用区的容量情况、Server列表、表属性、表大小等信息。
  - 管理数据库的表和Namespace。
  - 管理数据库账号和权限。
  - 通过SQL语句简单查询数据库中的数据。
  - 查看实例、分组、节点以及Namespace、表等多个层面的实时监控指标。
  - 支持实例的健康巡检，通过查看巡检报告帮助用户快速分析定位问题。
- Lindorm搜索引擎提供集群管理系统，通过集群管理系统管理索引表，包括创建、删除以及更新配置等操作。

12.9.2. 产品价值

云原生多模数据库Lindorm基于云原生架构具有弹性伸缩、低成本、高性能、简单易用、高可用、高可靠、开放生态等优势。

弹性伸缩

- 基于存储计算分离的全分布式架构，支持计算资源和存储资源的独立弹性伸缩。
- 存储资源支持秒级在线扩缩，计算资源（宽表引擎、时序引擎、搜索引擎）支持分钟级在线伸缩。

低成本

- 提供性能型、标准型、容量型多种存储规格，可满足不同场景的性价比选择。
- 多种引擎共享统一的存储池，减少存储碎片，降低使用成本。
- 内置深度优化的压缩算法，数据压缩率高达10:1以上，相比snappy提高50%以上。
- 内置面向数据类型的自适应编码，数据无需解码，即可快速查找。
- 支持智能冷热分离，多种存储规格混合使用，大幅降低数据存储综合成本。

高性能

- 宽表引擎：支持千万级并发吞吐，支持百PB级存储，吞吐性能是开源HBase的3~7倍，P99时延为开源HBase的1/10。
- 时序引擎：写入性能和查询性能是InfluxDB的1.3倍，是OpenTSDB的5~10倍。
- 搜索引擎：基于Lucene引擎深度优化，综合性能比开源Solr或ES提升30%。

简单易用

- 兼容多种开源标准接口，包括HBase/Cassandra/Phoenix、OpenTSDB、Solr，业务可以无缝迁移。
- 云托管服务，免运维。
- 图形化系统管理和数据访问，操作简单。

高可用

- 系统采用分布式多副本架构，集群自动容灾恢复。

- 支持跨可用区、强一致的容灾能力，具备金融级可用性标准。
- 支持全球多活部署。

高可靠

- 底层多副本存储，实现了数据的高可靠性。
- 提供企业级备份能力。

开放生态

- 支持与MySQL、HBase、Cassandra等系统的平滑在线数据搬迁。
- 可轻松与Spark、Flink、DLA、MaxCompute等计算引擎无缝对接。
- 支持无缝订阅Kafka、SLS等日志通道的数据，并具备快速处理能力。
- 通过Lindorm Stream，可以实时订阅Lindorm的增量变更数据，自定义消费。

12.9.3. 应用场景

云原生多模数据库Lindorm是阿里云自研的云原生多模型数据库，面向海量多模型数据的低成本存储分析，构建万物互联时代的数据底座。云原生多模数据库Lindorm可以提供单个毫秒响应的性能，支持水平扩展到PB级存储和千万级QPS，在阿里巴巴核心服务、大数据场景、金融、车联网和互联网场景中起到关键支撑的作用。

阿里巴巴集团内部最佳实践

Lindorm在阿里巴巴集团内部成熟业务中得到广泛使用，应用在手淘消息、支付宝账单，菜鸟物流信息等实时数据的存储和分析场景中，为阿里巴巴集团提供了低成本、高并发和弹性伸缩等优势。

大数据场景

Lindorm支持海量数据的低成本存储、快速批量导入和实时访问，具备高效的增量及全量数据通道，可轻松与Spark、MaxCompute等大数据平台集成，完成数据的大规模离线分析，为业务提供了低成本、快速导入和弹性伸缩等优势。

金融和零售

使用Lindorm存储金融交易中的海量订单记录，金融风控中的用户事件、画像特征、规则模型、设备指纹等重要数据，提供低成本、高并发、灵活可靠的能力，满足用户在金融交易与风控场景中的数据实时存储需求。

车联网

使用Lindorm存储车联网中的行使轨迹、车辆状况、精准定位等重要数据，提供低成本、弹性、灵活可靠的能力，满足用户在网约车、物流运输、新能源车检测等场景中的数据存储处理需求。

互联网社交

使用Lindorm存储互联网社交场景中的聊天、评论、帖子、点赞等重要数据，提供易开发、高可用、延迟的能力，可以大幅减少用户访问等待时间，提供稳定可靠的现代社交Feed流系统。

12.10. 数据库自治服务DAS

数据库自治服务DAS（Database Autonomy Service）是一种基于机器学习和专家经验实现数据库自感知、自修复、自优化、自运维及自安全的云服务，帮助用户消除数据库管理的复杂性及人工操作引发的服务故障，有效保障数据库服务的稳定、安全及高效。

12.10.1. 产品详情

数据库自治服务DAS（Database Autonomy Service）提供统一管理、自治服务（智能诊断和优化）、企业级数据库服务、数据库安全审计等功能。

统一管理

对多种类数据库进行集中管理、统一监控，能够为用户节省一半以上的管理成本，显著减少因人为误操作导致故障的概率。

- 统一监控

  通过DAS平台，即可查看所有环境、所有集群、所有实例的性能趋势情况和实时性能情况。

  - 低成本

    用户无需耗费人力开发和部署采集、计算、存储程序，直接使用DAS即可监控数据库。

  - 指标丰富

    支持数据库各项关键指标的采集、计算和展示。

  - 细粒度的监控

    支持按业务需要设置细粒度的监控，最小支持秒级监控，帮助用户快速发现异常。

- 统一告警

  支持自定义告警规则的触发条件和告警信息的发送人等。

  - 默认告警模版

    基于阿里巴巴的数据库运维经验，为各种数据库引擎定义了默认的告警模版，方便用户直接使用。

  - 灵活配置

    支持各种告警规则、告警模版、告警联系人、告警联系组的灵活配置，用户可以为企业内不同的使用者定义不同的告警模版。

  - 异常发现

    自动发现没有定义告警的数据库实例，避免出现因为告警信息发送不及时，导致业务受损的情况。

自治服务（智能诊断和优化）

DAS基于机器学习和细粒度的监控数据，能够提供7*24小时的异常检测，支持自动SQL限流、异常快照、自动SQL诊断和优化、存储空间自动扩展、计算资源自动扩展等服务。DAS还能通过异常发现、根因分析、进行止损或优化、效果跟踪、回滚或沉淀知识库等手段，实现诊断流程的闭环和优化效果的可量化，确保数据库的持续可用。

自治服务主要包含如下功能：

- SQL诊断和优化
- 慢SQL分析
- 空间分析
- 性能趋势
- 会话管理
- 全量SQL分析
- 诊断报告
- 7*24小时异常检测
- 自动SQL限流
- 自动SQL优化
- 自动SQL Review和优化
- 容量评估和规格推荐
- 弹性伸缩

企业级数据库服务

- **Dashboard**

DAS总结阿里巴巴数据库团队多年的数据库运维和管理经验，提供多种监控场景，支持查看跨实例、跨集群、跨环境、跨功能模块的护航大盘、实例大盘等。

- **多环境、多集群管理**

  DAS满足企业管理多套环境多套集群的需求，支持环境级别、集群级别的性能监控指标的聚合和下钻，贴近企业级管理视角。

- **巡检评分**

  DAS支持巡检评分，自动对用户接入DAS的所有数据库实例进行巡检，包括基础巡检以及SQL、容量、性能、安全巡检等，并给出健康评分，帮助用户一目了然地确认数据库运行情况。

数据库安全审计

DAS提供高危SQL识别、SQL注入检测、新增访问来源识别、敏感数据访问发现等服务，具备实时检测、全量审计、快速识别数据库异常访问和拖库等行为的能力，有效保障数据库安全。数据库安全审计包含如下功能：

- SQL注入识别
- 高危SQL识别
- 新增访问来源识别

12.10.2. 产品价值

数据库自治服务DAS（Database Autonomy Service）具备节约成本、提升稳定性、持续可用、安全高效、高可靠性等优点。

- **节约成本**
  - DAS提供统一监控功能、统一告警功能，用户无需耗费人力和资源搭建性能监控平台和告警平台。
  - DAS提供统一的管理平台，用户无需在多个管理平台上切换，提升工作效率、节省人力成本。
- **提升稳定性**
  - DAS提供丰富的数据库性能监控和告警功能，可以快速发现和定位数据库异常，提升数据库的稳定性。
  - 运维和管理一站化，无需多平台间切换，显著减少误操作概率。
- **持续可用**

  DAS基于机器学习和专家经验实现数据库自感知、自修复、自优化、自运维及自安全的云服务，保障用户的数据库持续可用。
- **安全高效**
  - DAS提供高危SQL识别、SQL注入检测、新增访问来源识别、敏感数据访问发现等服务，能够快速识别数据库是否存在异常访问、拖库等行为，有效保障数据库安全。
  - DAS采用无侵入式设计，不会侵入客户的数据库环境，也无需在数据库实例上安装客户端。
  - DAS采用安全的数据链路，数据库的信息利用KMS进行加密存储，加密压缩后才进行传输，保障数据安全。
- **高可靠性**

  DAS支持同城容灾。

12.10.3. 应用场景

数据库自治服务DAS（Database Autonomy Service）支持统一管理、批量管理、智能诊断、安全审计等功能，适用于多种典型企业级数据库管理场景。

- **统一管理**

  DAS支持多种引擎的数据库统一管理，构建监控和告警平台，3分钟即可接入阿里云上数据库，实现统一监控、统一告警。

- 关系型数据库：
  - 云数据库RDS MySQL
  - 云数据库RDS PostgreSQL
  - 云原生数据库PolarDB PostgreSQL版（兼容Oracle）
- NoSQL数据库：
  - 云数据库Redis版
  - 云数据库MongoDB版

- **批量管理**

  DAS提供企业级数据库管理服务，贴近业务管理视角，支持全局、应用组、实例的多种管理维度，并且提供了自定义大盘、批量管理、巡检等企业级能力，同时支持与企业原有数据库管理系统集成。

  - 自定义：支持用户自定义性能大盘，支持多个实例、多指标的对比分析。
  - 巡检评分：支持从基础到参数、性能、安全等的巡检，自动生成可靠的数据库巡检结果。
  - 支持被集成：支持内嵌到企业原有的系统，有效减少企业内的迁移成本和学习成本。

- **智能诊断**
  - DAS基于机器学习和细粒度的监控数据，实现7*24小时的异常检测，相比传统的基于阈值的告警方式，能够更为及时的发现数据库的异常变化，并自动进行诊断、止损或者优化，保证数据库的稳定。
  - DAS通过异常发现、根因分析、进行止损或优化、效果跟踪、回滚或沉淀知识库等手段，实现诊断流程的闭环和优化效果的可量化，确保数据库持续可用。

- **安全审计**

  DAS提供高危SQL识别、SQL注入检测、新增访问来源识别、敏感数据访问发现等服务，能够快速识别数据库受否存在异常访问、拖库等行为，有效保障数据库安全。

12.11. 数据库备份DBS

数据库备份（Database Backup，简称DBS）是一款可以为数据库提供连续数据保护、低成本的备份服务平台。它可以为多种环境的数据提供强有力的保护，包括企业数据中心、其他云厂商及公共云。数据库备份拥有一套完整的数据备份和数据恢复解决方案，具备实时增量备份以及精确到秒级的数据恢复能力。

数据库备份DBS可以实现实时的数据备份，在线数据发生变化时，数据库备份会获得变更的数据，并将数据实时写入云存储，帮助用户实现秒级RPO的数据备份。

12.11.1. 产品详情

数据库备份DBS（Database Backup）是一款低成本、高可靠的云原生数据库备份平台。根据业务需求，用户可以使用阿里云提供的控制台来创建备份计划、备份数据、下载备份集以及恢复数据等。

存储池

数据库备份DBS存储池可用来存储备份数据。除DBS自带的内置存储外，用户可以在存储池中添加对象存储OSS或自建NAS存储，然后在备份时选择目标存储池的备份策略，即可将备份数据存放至目标存储池。

备份网关

数据库备份DBS提供备份网关功能，用户可以通过DBS控制台下载安装包，并在数据库服务器上安装备份网关，实现数据库从本地备份到云端OSS上。

备份方式

常用的数据备份方式为逻辑备份、物理备份。

- 逻辑备份：数据库对象级备份，备份内容是表、索引、存储过程等数据库对象。例如MySQL

mysqldump、Oracle exp/imp等。

- 物理备份：数据库文件级备份，备份内容是操作系统上数据库文件。例如MySQL XtraBackup、Oracle RMAN等。

数据恢复

数据库备份DBS提供数据恢复能力，支持秒级任意时间点恢复，并且用户可以灵活选择恢复对象。

应急恢复

数据库备份DBS提供应急恢复功能，用户可通过使用DBS沙箱功能，实现从目标备份集快速创建新的数据库实例，让备份数据快速可用。多个沙箱实例之间的读写不会互相影响，也不会影响原数据库。

12.11.2. 产品价值

数据库备份DBS支持多种环境的数据库备份，通过专线接入、公网等接入技术，DBS可以实现用户本地IDC数据库备份、ECS自建数据库的备份、其他云环境和RDS的数据库备份，可以通过简单的配置实现数据库全量备份、增量备份以及数据恢复。

对比优势

对比项	DBS云备份解决方案	自建备份系统
成本	• 冷热数据分级存储，适用于长期归档。 • 压缩、紧凑备份格式、增量备份，降低存储成本。	• 一次性投入大量资产。 • 存储受硬盘容量限制，需人工扩容。 • 单线或双线接入速度慢，有带宽限制，峰值时期需人工扩容。 • 多级存储介质引入，运维成本骤增。
安全	• 使用SSL和AES256加密技术，保护备份数据传输和存储安全。 • 多用户资源隔离机制，支持异地灾备机制。 • 提供多种鉴权和授权机制及白名单、防盗链、主子账号功能。 • 备份有效性随时验证，任务状况主动通知。 • 提供用户自定义的鉴权机制。	• 需要另外购买清洗和黑洞设备。 • 需要单独实现安全机制。
易用性	• 仅需5分钟，从配置到备份运行。 • 细粒度备份，整个实例、单库、多表和单表自由选择。 • 完整生命周期管理，全局规则控制，自动转存、清理和复制分发。 • 备份恢复统一Web管理界面。	• 备份脚本和工具，学习成本高。 • 灵活性不足，一般只能提供基础能力。
性能	• 秒级RPO，日志内存实时捕获，任意时间点恢复。 • 恢复对象精准匹配，单表恢复，RTO大幅降低。 • 流式备份，数据不落盘，备份窗口全程无锁，自适应并发调速。	受限于多个工具短板，容易产生瓶颈点。

可靠性	• 基于阿里飞天盘古提供分布式高可靠存储。 • 备份过程中，实时校验数据完整性。 • 海量用户验证，风险快速发现并修复。	• 多个工具拼凑，问题指数级增长。 • 受限于硬件可靠性，易出问题，一旦出现磁盘坏道，容易出现不可逆转的数据丢失。
扩展性	• 除了支持备份阿里云数据库，DBS还支持将ECS自建数据库、本地机房数据库、AWS/腾讯云等其他云厂商数据库备份到阿里云上。 • 除了支持恢复到原始数据库，DBS还支持恢复到其他环境，如本地数据库通过DBS备份，恢复到阿里云数据库上。	仅支持特定环境，一般不具备扩展性。

低成本

DBS使用OSS作为内置存储，备份数据会转换成专用格式，并经过压缩保存到内置存储，降低存储成本。

安全

功能	说明
传输存储加密	使用SSL和AES256加密技术，保护备份数据传输和存储安全。
异地备份	提升数据保护级别。
报警	备份异常、恢复异常、恢复成功等关键事件通知。

灵活易用

功能	说明
细粒度备份	整个实例、多库、单库、多表和单表，自由选择备份粒度。
单表恢复	细粒度恢复，恢复对象精准匹配，降低RTO。
生命周期管理	备份数据，全局规则控制，自动转存、清理和复制分发。
引导式界面	备份恢复采用统一Web管理界面，从购买、配置到运行，仅需5分钟。

高性能

数据库备份DBS通过使用阿里实时数据流技术，可以读取数据库日志并进行实时解析，然后存储到云端存储上，实现对数据库的增量备份。通常，DBS可以将增量备份的延迟控制在秒级别以内，根据实际网络环境不同，延迟时长也会不同。

在进行数据恢复时，可以使用存储的增量备份实现精确到秒的数据库恢复。最大限度保障数据安全。

功能	说明
实时备份	日志内存实时捕获，RPO达到秒级。
并行备份	全程无锁备份、多线程并行备份、数据拉取自适应分片。
任意时间点恢复	提供可恢复日历及时间轴选择。
多规格	弹性扩展，无缝支撑企业不同阶段性能要求。

12.11.3. 应用场景

数据库备份DBS提供数据全量备份、增量备份和数据恢复功能，满足用户以下多种典型场景的应用需求。

实时备份

数据库作为企业重要资产，备份数据库必不可少，根据数据重要程度，备份频率从每周备份、每天备份到每小时备份不等。即使每小时备份，在遇到数据库故障时，也可能会丢失1小时数据，这对于游戏、金融等行业是无法接受的。为了降低在故障发生后数据丢失，数据库备份DBS提供了实时数据备份，RPO达到秒级。

库表级恢复

全量数据备份是最普遍的备份解决方案，发生数据误删除时，传统方案需要将整个实例数据全部恢复，然后从中找出误删除表，其他数据都丢弃掉，大部分时间花费在无效工作上，这种方案会大大延长故障恢复时间。为了降低故数据库障恢复时间，数据库备份DBS提供了表级数据恢复，准确匹配恢复需求。

- **时间短**：选择库表级恢复时，数据库备份DBS只会读取单个表的数据进行恢复，极大缩短了恢复时间。
- **备份灵活**：支持同时结合增量备份，可恢复至任意时间点。

长期归档

出于安全合规要求，部分数据需要长期保存，传统方式是选择磁盘或磁带，其中会遇到多种问题，例如硬件故障导致备份可靠性差。如果关键时刻数据无法恢复，后果难以想象，随着数据海量增加，管理难度还会不断攀升等。

为了解决数据库长期归档问题，数据库备份DBS提供完整生命周期管理，根据备份集访问频率，用户可选择不同性价比存储方式，自动管理备份集转存和过期清理。

异地灾备

作为完整数据库灾备方案，除了要有本地数据库备份外，还要在异地做数据库备份。传统方案是将备份集拷贝到本机其他盘、其他机器，这些都无法抵御地震、台风等自然灾害。如果要做到异地容灾，需要用户在其他地区自行搭建备份机房，前期投入成本很大。

为了解决数据库异地灾备问题，数据库备份DBS提供按量付费服务，对于本地IDC数据库、其他云数据库、ECS自建数据库和RDS数据库，可以通过DBS将数据备份到阿里云OSS上，实现异地容灾备份。

另外，除了冷备中心外，用户还可以通过数据传输DTS来构建热备中心。当业务中心发生故障时，业务流量会切换到本地数据中心、或者备份中心。

> **说明**
> - 冷备中心：投入成本低，数据存储在OSS中，恢复时间在数小时级别。
> - 热备中心：投入成本高，数据存储在数据库中，恢复时间在分钟级别。

12.12. 云原生分布式数据库PolarDB-X

PolarDB-X是阿里巴巴自主设计研发的高性能云原生分布式数据库产品，为用户提供高吞吐、大存储、低延时、易扩展和超高可用的云时代数据库服务。

PolarDB-X始终保持对阿里巴巴集团“双十一购物狂欢节”所有相关业务的全面支撑。历经十余年淬炼，具备了强数据一致性、高系统稳定性、快速集群弹性等核心关键特性，并在司法财税、交通物流、电力能源等公共事业领域有广泛深入应用。

PolarDB-X坚定遵循自主可控、开放生态的发展思路，持续围绕MySQL开源生态构建分布式能力，以求最大程度降低用户的学习使用成本。

12.12.1. 产品详情

PolarDB-X在高可用性、混合负载、全局二级索引、备份恢复等方面都有比较好的用户沉淀和技术支持。

高可用性和容灾

为了保证副本间的强一致性，现代数据库往往采用以Paxos为代表的多数派复制协议。Paxos通常要求集群中至少存在3个节点，每次写入都要获得超过半数节点的确认，即便其中1个节点宕机，集群也仍然能正常提供服务。Paxos算法能够保证副本间的强一致性，彻底解决副本不一致问题。

PolarDB-X在副本复制方面采用了X-Paxos。X-Paxos是阿里巴巴自研的Paxos协议实现，起源于AliSQL（阿里内部的MySQL分支）。基于朴素的Paxos实现，它在功能、性能上都做了大量优化，且经历了数十载的双十一考验，稳定可靠。

混合负载

PolarDB-X是一款支持HTAP（Hybrid Transaction/Analytical Processing）的数据库，在支持高并发、事务性请求的同时，也对分析型的复杂查询提供了良好的支持。

为了提高复杂分析型查询的速度，PolarDB-X将计算任务切分并调度到多个计算节点上，从而利用多个节点的计算能力，加速查询的执行。这种方式也称为MPP并行计算（Massively Parallel Processing，简称MPP）。目前只有PolarDB-X只读实例默认开启了MPP并行计算能力。

全局二级索引

全局二级索引（Global Secondary Index，GSI）是PolarDB-X中的一项重要特性，相比于本地二级索引，全局二级索引中的数据按照指定的拆分方式分布在各个存储节点上。通过全局二级索引，用户能够按需增加拆分维度、提供全局唯一约束等。

全局二级索引还支持以下特性：

- 支持选择覆盖列，减少回表操作开销。
- 在线表结构变更，添加GSI不锁主表。
- 支持通过HINT指定索引，自动判断是否需要回表。

全局日志变更

MySQL binlog是MySQL记录变更数据的二进制日志，它可以看做是一个消息队列，队列中按顺序保存了MySQL中详细的增量变更信息，通过消费队列中的变更条目，下游系统或工具实现了与MySQL的实时数据同步，这样的机制也称为CDC（Change Data Capture，增量数据捕捉）。

PolarDB-X是兼容MySQL生态的分布式数据库。通过实例内PolarDB-X的CDC组件，能够提供与MySQL binlog格式兼容的变更日志，并且对外隐藏掉实例扩缩容、分布式事务、全局索引等分布式特性，让您获得与单机MySQL数据库一致的使用体验。

备份与恢复

数据备份和恢复是数据库必不可少的能力，PolarDB-X提供不同粒度的数据恢复能力，包括实例级的一致性备份恢复能力、表级的表回收站能力、SQL级的SQL闪回能力等。

全链路监控和审计

PolarDB-X具有丰富的监控和审计功能，帮助用户实时监测数据库的各项性能指标和运行状态。

12.12.2. 产品价值

云原生+MySQL生态

PolarDB-X已作为标准云产品在世界范围内的13个地区提供服务。依托云资源和容器化部署能力，PolarDB-X可以在数分钟内完成集群创建和变配，整个过程中无需进行手工干预。

阿里云及开源社区的多种生态工具对PolarDB-X持续提供不断完善的支持，包括但不限于以下产品：数据传输服务DTS、数据库备份DBS、数据管理服务DMS、数据库自治服务DAS、数据集成Data Integration、云监控、性能测试PTS。

PolarDB-X积极拥抱并努力回馈MySQL生态，目前已经形成对MySQL生态从协议、语法、事务行为、账号体系、安全到命令行工具的全方位兼容。

存储计算分离架构

旨在最大限度地发挥其云数据库的弹性扩展能力，PolarDB-X采用了基于存储计算分离的Shared-Nothing系统架构，该架构使用户可以根据业务需要进行分层容量规划。

PolarDB-X的存储节点（DN）基于阿里巴巴自研的跨可用区部署的三节点强一致数据库X-DB构建。X-DB使用InnoDB引擎，提供MySQL语法全兼容能力，以及对复杂查询的处理能力。X-DB结合PolarDB-X面向HTAP的CBO查询优化器，可精确控制计算下推行为，从而获得更佳的整体性能。

透明分布式体验

让用户以使用单机MySQL数据库的体验，操作分布式数据库是PolarDB-X一贯追求的目标。为此PolarDB-X提供了简单易用的透明分布式能力：

默认主键拆分，让移植到PolarDB-X的数据和业务摆脱对设计**分区键**的依赖。

高性能强一致分布式事务，PolarDB-X采用自研X-Paxos协议，保证数据存储在故障切换过程中RPO=0的基础上，使用TSO策略和分布式的MVCC能力保证了分布式事务的隔离性和一致性。

分布式线性扩展，PolarDB-X基于一致性Hash的分区策略，有效的进行负载均衡和热点抑制，且在扩展过程中保持计算下推和数据一致性的同时实现业务零感知，并行和流控能力为扩展期间业务连续性提供了有力保障。

全局Binlog和全局一致性备份，分别解决分布式数据库各节点数据库向下游流转的难题及各节点备份时间差造成的恢复一致性问题。

12.12.3. 应用场景

PolarDB-X适用于高负载低延时交易、大峰谷差流量和数据集中存储等场景。

高负载低延时交易

场景描述

交易场景广泛存在于互联网业务中，交易系统是信息系统中最为核心的组件之一。业务连续性、事务一致性和系统安全性是交易系统正常运行的基础，长时间高负载低延时的运行是互联网时代交易系统的发展方向。

产品能力

PolarDB-X采用搭载自研多数派共识协议X-Paxos，并应用于存储节点提供三副本强一致能力，确保高可用切换和容灾场景下RPO=0。基于全局时钟TSO策略和分布式的MVCC多版本，分布式事务可确保多节点数据访问的事务一致性。PolarDB-X已通过中国信通院《金融级分布式事务数据库稳定性专项评测》，且持续12年支撑“双十一”全球购物狂欢节，集稳定性与高性能于一身。

大峰谷差流量

场景描述

大峰谷差是指特定周期内系统峰值负载是谷值负载的20倍以上的系统访问场景，该场景多见于“秒杀”、“拼团”和“限时优惠”相关业务中。系统管理员常陷于容量安全与成本控制之间的两难，所以成本优化方案和平滑扩缩容能力是该场景的核心诉求。

产品能力

PolarDB-X采用分布式线性扩展机制，在扩展过程中保持计算下推和数据一致性的同时实现业务零感知，结合流量控制能力进一步提升扩展过程的业务稳定性。同时PolarDB-X提供历史数据清理和归档能力，使庞大的数据存储成本得到有效控制。

数据集中存储

场景描述

该场景也称“数据大集中”或“数据归集”，属于企业数据架构中的ODS层，具有承担各垂直业务数据源的数据汇总功能。高并发写入、大容量存储、多维度查询、低成本流出是该场景的主要诉求。

产品能力

- PolarDB-X可根据访问量和存储量方便的进行Scale-Up/Down和Scale-Out/In，按需满足高并发写入、大容量存储需求。
- 基于并行计算的DML以及大事务的支持能力，可以有效满足跑批处理和执行效率。
- 高性能全局二级索引（GSI）让用户不局限于拆分规则，可根据任意维度对PolarDB-X进行查询。
- 全局Binlog是保证事务有序性的分布式数据库统一变更日志服务，且兼容MySQL Binlog文件格式和Dump协议，使下游数据消费轻松便捷。

分布式快速改造

场景描述

当业务体量即将突破单机数据库承载极限和单表过大导致性能、维护问题时，分布式改造是解决上述问题的高性价比方案。数据库作为分布式改造的重点难点，“和使用单机数据库一样使用分布式数据库”一直是广大用户的核心诉求。

产品能力

PolarDB-X推出“透明分布式”系列能力，从连接、开发到管理行为均最大限度保留单机MySQL的使用体验，让用户的分布式改造周期大幅缩短，研发运维团队的原有技术栈最大限度保留。目前，PolarDB-X具备从单机到分布式的平滑演进能力，支持动态通过DDL将一张大表动态调整为分布式的分区表，结合分布式事务、以及兼容MySQL binlog的数据回流，可完成单机到分布式的快速改造。

数据库国产化替换

场景描述

信息系统国产化是大型企业实现数字化转型的重要一环，数据库作为核心基础软件首当其冲，目前数据库国产化改造已经在电信、泛金融、能源和企事业单位广泛开展。

产品能力

PolarDB-X是阿里云自研的云原生分布式数据库，具备国产化、自主可控的能力。另外，具有公有云、专有云、DBStack和软件版多种部署形态、完善的交付和服务团队，已经帮助百余家企业完成商业数据库替换、核心数据库系统分布式改造、分布式数据库技术培训与架构咨询等多项任务。

混合负载访问

场景描述

互联网业务的实时化、智能化趋势催生了事务数据与分析数据在相同数据源内进行混合访问（HTAP）的需求。数据一致性、访问便捷度和访问安全性是混合负载访问场景的主要诉求。

产品能力

PolarDB-X基于并行计算和弹性扩展能力，可实现对在线数据做实时报表分析；同时引入智能读写分离、只读副本做分析，保障OLTP和OLAP访问的隔离性的同时，提供统一访问入口，自动选择查询执行引擎。使用一份数据完成两种类型访问，免去ETL的成本和延时。

12.13. 图数据库GDB

图数据库GDB（Graph Database）是一种支持Property Graph图模型、用于处理高度连接数据查询与存储的实时、可靠的在线数据库服务。支持Apache TinkerPop Gremlin查询语言，帮助企业快速构建基于高度连接的数据集的应用程序。

图数据库GDB非常适合社交网络、欺诈检测、推荐引擎、实时图谱、网络、IT运营这类高度互连数据集的场景。例如，在一个典型的社交网络中，常常会存在“谁认识谁，上过什么学校，常住什么地方，喜欢什么餐馆之类的查询”，传统关系型数据库对于超过3度的查询十分低效难以胜任，但图数据库可轻松应对社交网络的各种复杂存储和查询场景。

12.13.1. 产品详情

借助图数据库GDB构建行业知识图谱，可以充分运用企业的多元异构数据，提供更聪明的决策建议。

标准图查询语言

支持属性图，高度兼容Gremlin、OpenCypher图查询语言。

高度优化的自研引擎

高度优化的自研图计算层和存储层，云盘多副本保障数据超高可靠，支持通过只读节点扩展并发能力。

服务高可用

支持高可用实例，节点故障迅速转移，保障业务连续性。

易运维

提供备份恢复、自动升级、监控告警、故障切换等丰富的运维功能，大幅降低运维成本。

12.13.2. 产品价值

图数据库GDB具有支持标准图查询语言、实时在线、架构灵活、自动索引、优化超级顶点查询性能、支持自动机器学习等产品优势。

支持标准图查询语言

支持Gremlin和Cypher语言，兼容市面主流图查询产品，降低开发门槛。

实时在线

即时处理海量数据，分析洞察数据价值，可通过只读节点水平扩展并发查询性能。

灵活架构

支持Schema free，满足更灵活多变的数据架构调整需求。

自动索引

自动建立索引，优化查询效率的同时更易维护。

优化超级顶点查询性能

通过自动建立索引优化超级顶点的查询性能。

支持自动机器学习

原生支持对接自动机器学习平台，通过AI算法洞察关系数据规律，产生智能决策。

12.13.3. 应用场景

图数据库GDB针对高度互联数据的存储和查询场景进行设计，并在内核层面进行了大量优化，非常适合社交网络、欺诈检测、推荐引擎、知识图谱、网络、IT运营等高密互连数据集的场景。

社交网络

图数据库可以轻松应对海量高度互连社交数据的实时存储和高效查询，帮助企业快速构建复杂的社交网络系统。例如，在一个典型的社交网络中，通常存在“谁认识谁，谁上过什么学校，谁常住什么地方，谁喜欢什么餐馆”等查询，传统关系型数据库对于超过三度的查询往往会很低效甚至无法支持，但图数据库从基因层面提供了解决方案，轻松应对社交网络的各种复杂存储和查询。

金融欺诈检测

在金融领域，图数据库经常用于欺诈检测。例如，通过贷款、分期消费者的联系人（或者联系人的联系人）信用信息，对用户进行信用评分，如果评分较低，则拒绝贷款或者提升利率；通过申请人的个人信息（包括电话号码、家庭住址），判断申请人信息是否属实。通常，欺诈者是通过“黑市”购买的用户信息然后拼凑出“个人信息”，并且这些信息会被反复使用，使用图数据库，可以快速发现申请人提供的个人信息与现有用户信息的关系。

实时推荐引擎

图数据库非常适合实时推荐场景。企业可以将用户的购买行为、位置、好友关系、收藏等数据实时存储在图数据库中，然后利用图数据库能对高度互连数据提供高效查询的特点，通过各种维度的快速查询实时进行多维度个性化推荐。例如，在某App中，通过用户位置及以前的购买行为信息，当某用户A到达某商场B，App可以向用户实时推荐附近的门店及商品等信息。

知识图谱

图数据库可以帮助企业快速构建知识图谱。将图谱数据存储在图数据库中，既可以通过外部输入实时更新，也可以对图数据库内部图谱信息进行分析，不断发现并完善图谱数据。例如，基于图数据库，可以快速实现针对足球明星的知识图谱应用，帮助用户发现感兴趣的信息。

网络、IT运营

图数据库非常适合网络、IT运营相关场景。例如，企业可以将路由器、交换机、防火墙、服务器等各种网络设备、终端及其拓扑信息存储在图数据库中，当某服务器或终端遭受恶意攻击或者受到感染时，您可以通过图数据库快速分析并找到传播路径，然后进行相关追踪及处理。

12.14. 数据库和应用迁移服务ADAM

数据库和应用迁移服务（Advanced Database & Application Migration，简称 ADAM）是一款将IT系统轻松的从原有的运行环境迁移上云的产品，在讲传统IT架构改造成互联网架构方面（例如将Oracle数据库迁移到云数据库PolarDB）积累多年的成功经验。ADAM支持的源库有Oracle 10g/11g/12c版本、Teradata 13/14/15版本、DB2_LUW版本。

12.14.1. 产品详情

ADAM包含完整的迁移系统，分别在项目前期、应用迁移阶段和割接上线阶段提供相应的平台来帮助客户完成端到端的迁移过程。

数据采集器

- 数据库采集器负责收集并汇总源数据库信息，包含环境、对象、SQL、空间、性能和事务六方面信息，全面覆盖数据库实际运行状况。同时，针对数据冗余、信息安全问题，对采集结果中SQL数据进行脱敏、去重、一致性校验等处理，保证采集结果的准确性。
- 应用采集器负责分析并收集应用框架与运行时信息，包含应用机器性能信息、应用代码中SQL信息、运行时SQL调用堆栈、应用与数据库间调用关系、应用与应用间调用关系五方面信息，全面覆盖应用实际运行状况。同时，也对结果数据进行脱敏、去重、一致校验处理。

智能分析平台

智能分析平台的目标是根据采集到的源库数据，从应用采集到的运行数据，给出最适合的目标库方案。智能分析平台包括数据库评估、数据库改造迁移、应用评估改造三部分。

- **数据库评估**
  - 源库画像分析：源库画像通过对数据库采集器采集到的源库数据进行分析，给出多个维度的评估分析，包括对源库性能、容量、特性、外部连接（DB Link）和对象全景查询。其中全景分析对对象提供关联关系、特征标识等信息。

  - 目标库选型建议：计算出每一个表组对应的云数据库规格，提供CPU核数、内存大小、磁盘大小等指标，满足用户的性能需求。根据评估分析结果给出目标方案的云资源成本，方便客户进行迁移到目标库的成本分析。
  - 目标库兼容评估服务：针对不同的目标数据库及版本，ADAM提供源数据库对象和目标数据库之间的兼容性分析和改造的建议。兼容性级别分为完全兼容、不兼容两种。其中修改后兼容的方案由ADAM智能分析引擎自动化提供并写入迁移计划。
- 数据库改造迁移

智能分析平台

智能分析平台的目标是根据采集到的源库数据，从应用采集到的运行数据，给出最适合的目标库方案。智能分析平台包括数据库评估、数据库改造迁移、应用评估改造三部分。

数据库评估

- 源库画像分析：源库画像通过对数据库采集器采集到的源库数据进行分析，给出多个维度的评估分析，包括对源库性能、容量、特性、外部连接（DB Link）和对象全景查询。其中全景分析对对象提供关联关系、特征标识等信息。
- 目标库选型建议：计算出每一个表组对应的云数据库规格，提供CPU核数、内存大小、磁盘大小等指标，满足用户的性能需求。根据评估分析结果给出目标方案的云资源成本，方便客户进行迁移到目标库的成本分析。
- 目标库兼容评估服务：针对不同的目标数据库及版本，ADAM提供源数据库对象和目标数据库之间的兼容性分析和改造的建议。兼容性级别分为完全兼容、不兼容两种。其中修改后兼容的方案由ADAM智能分析引擎自动化提供并写入迁移计划。

数据库改造迁移

- 生成迁移计划：根据评估分析的结果生成从源库到目标数据库的迁移计划，使用迁移工具可以利用迁移计划将源库的Schema快速迁移到目标数据库，其中迁移计划包含的ADAM智能转换结果将保证最大兼容度。
- 迁移计划校验：校验迁移计划与源库中结构的一致性，并针对不一致的数据提示合并，这样保证了目标库与源库的数据结构最大一致性。
- 结构迁移/订正：根据迁移计划中的转换建议，生成目标库的DDL，连接到目标库进行数据库结构创建，并为转换流程提供实时更正功能，保证结构迁移中最大成功率。
- 数据迁移服务：自动连接DTS数据迁移服务。

应用评估改造

- 应用画像：应用画像通过对采集到的应用数据或应用的WAR包进行分析，提供多维度的评估分析，包括对应用的软件栈、系统信息、对象详情、SQL和调用栈等的评估分析。应用画像包括静态分析和动态分析，其中动态分析依赖对应用数据的采集，而静态分析可以直接对Java应用的WAR包进行分析，定位应用对数据库对象的访问点。
- 应用评估：应用评估主要针对数据库与应用迁移的改造过程，帮助用户快速梳理数据库异构迁移过程中的应用修改内容。

兼容性分析模块

兼容性分析模块基于阿里巴巴内部多年沉淀的宝贵经验，给出源库对象迁移到多种目标库上的兼容性和修改建议，包括对源库特性的匹配和源库使用场景的匹配。

- 特性匹配主要指识别出对象使用了哪些特性，并给出在目标库上对应的解决方案。
- 场景匹配是针对一些特定的使用场景，通常是可能影响到性能的一些使用方式，评估这些使用方式在目标库上是否能够很好地支持，如果需要调整的话给出调整的解决方案。

兼容性分析模块作为支持评估工具和迁移工具的核心模块，其本身也可以单独运行直接处理迁移人员查询请求，给出评估结果。

模式转换模块

模式转换模块提供表和其它对象从源库到目标库的自动转换能力。通过使用模式转换模块，客户可以将所支持的转换对象直接转换为目标库上对应的对象或转换成Java代码。目前模式转换模块支持将表结构在目标库上自动创建，未来可以支持更多其它对象自动转换为目标库上适当形式的对象。

应用迁移模块

应用迁移模块的核心是为系统迁移人员提供一个辅助迁移环境，加快迁移过程。

- 实时收集待迁移应用的数据库请求，将代码调用栈返回给用户，帮助用户定位代码中需要改动的位置。
- 实时收集待迁移应用的数据库访问SQL，通过兼容性分析并将分析结果实时反馈给用户，指导用户按照正确的方式进行代码的迁移工作。
- 实时收集待迁移应用的数据库访问返回数据和性能数据，与原应用进行比对，保证迁移工作在功能和性能上可以和原应用一致。
- 可以同时连接多个目标数据源，当迁移目标数据库为多个时，有动态 SQL 路由能力，可以根据访问的对象将请求路由到正确的目标数据源中，迁移过程中应用不需要显式的连接多个数据源，降低迁移工作复杂性。

类似于调试器，实时提供修改建议，让开发人员实时修改并实时验证。让开发人员在开发测试环境中可以方便的进行迁移和验证工作，在业务系统所有测试案例通过AMS测试后，即可宣告迁移工作完成，为迁移工作给出标准。

12.14.2. 产品价值

ADAM沉淀多年迁移经验积累，在智能分析、数据库改造、应用改造定位等方面具有优势。

多年迁移经验

积累并提炼了阿里巴巴内部多年的成功迁移经验，尤其是从传统IT架构向互联网和云架构改造升级方面的成功实践。从迁移前的可行性分析、场景分析、目标数据库选型、兼容性评估、工作量评估、应用改造建议，以及最后新老系统割接、自动化测试等有着全流程的工具和实践经验。

智能分析

在迁移前采集客户系统运行环境里的源数据库信息，然后对采集到的数据进行评估分析，最后得出分析报告集（包含专家意见）。报告集的内容包括目标数据库方案、源库不同类型对象的兼容度和不兼容原因、迁移后风险对象及SQL、应用相关的改造建议、迁移方案的成本等。此外，分析结果还包括目标数据库迁移计划。

数据库改造

依据智能分析阶段得到的目标数据库迁移计划，利用数据库改造迁移服务，客户可以自动化的将源库的 Schema 对象迁移到目标库，其中完全兼容和改造后兼容的对象在迁移过程中自动完成改造。对于不兼容对象，客户可以参考系统中提示来做改造并验证正确性。

应用改造定位

利用应用采集器采集到的应用数据（包括 SQL、调用栈等）来定位应用的SQL访问位置，同时结合数据库分析得到的对象信息及兼容改造建议，帮助客户快速定位应用的改造点，极大的提高应用改造的效率。ADAM的数据库与应用的融合分析能力是ADAM的特色，将显著降低数据库迁移的门槛。

12.14.3. 应用场景

ADAM帮助企业将数据库和应用程序从原有的运行环境迁移到阿里云专有云。

传统IT系统上云

传统企业的IT系统使用的是IOE+小型机架构，这种架构扩容只能升级硬件，高配置硬件升级带来的性能提升跟硬件升级投入的成本并不是成正比的，越往上升级性价比越低，无法做到平滑线性的扩容。而互联网分布式架构则能做到平滑扩容，并且硬件投入跟性能提升成正比。

如果需要将IT系统系由传统统架构改造成互联网分布式架构，ADAM能够提供一站式的迁移服务。迁移之前分析迁移可行性、目标存储选型以及应用改造成本；在实施迁移的过程中提供应用改造专家建议；应用割接的时候提供数据迁移服务，尽可能减少系统停机时间。

云上IT系统迁移

如果系统已经在阿里云上，随着业务增长，现有的存储（如只使用云数据库RDS）不满足需求，需要更换或者新增存储（如使用MaxCompute存放历史数据、使用AnalyticDB存放分析型数据）来替代或者辅助现有唯一的存储RDS，涉及到存储选型、应用改造，ADAM提供目标存储选型以及应用改造专家服务来帮助完成系统扩展改造。

12.15. 云数据库OceanBase

云数据库OceanBase是一款高性能、分布式的金融级关系型数据库，通过在底层分布式引擎实现的Paxos多数派协议和多副本特性，拥有令人称道的高可用和容灾能力，不负永不停机的数据库系统的盛名 ，可以完美支持多地多活、异地容灾等高可用部署，实现跨机房、跨地域、甚至跨洲际部署，实现金融级可用性和事务的强一致性。

OceanBase独有的读写分离架构和面向SSD固态盘的高效存储引擎，为用户带来了超高性能的体验。OceanBase定位为云数据库，通过在数据库内部实现多租户隔离，实现一个集群服务多个租户，且租户之间完全隔离，不会相互影响。

12.15.1. 产品详情

云数据库OceanBase向用户提供完整的关系型数据库服务，用户可以通过SQL接口访问和管理实例中的数据。

OceanBase兼容MySQL5.6版本大部分功能，基于MySQL的业务只需零修改或少量修改即可迁移到OceanBase，提高了应用开发和迁移的效率。同时，OceanBase在数据库内部实现了分区表和二级功能，可以完全取代 MySQL常用的分库分表方案。同时，OceanBase控制台还提供实例升降级、性能数据查看、优化建议等功能，让用户可以轻松管理复杂的数据库。

高效的存储引擎

云数据库OceanBase采用share-nothing的分布式架构，每个OBServer都是对等的，管理不同的数据分区。单机的存储引擎采取读写分离的架构，将当前更新的动态数据存入内存称为MemTable，存量的基线数据存在磁盘，称为SSTable。一个Partition的所有数据（基线数据、增量数据和事务日志）都放在一个OBServer中，因此，针对一个Partition的读写操作不会有跨机的操作，数据的写入也分布到多点并行执行。

读写分离的存储结构带来很多好处，因为有大量的静态基线数据，可以很方便对其进行压缩，减少存储成本；另外做行级缓存也不用担心写入带来的缓存失效问题。其缺点是读的路径变长，数据需要实时合并可能带来性能问题，OceanBase采用了很多的优化手段，比如bloom filter cache对不存在的行做过滤（insert row判断行是否存在无需I/O操作），尽量优先读取更新的内容（Active MemTable），如果发现用户读取的列已经读取到，则无需进一步读取基线数据进行合并。

由于增量数据写在内存中，内存写到一定量后需要与基线数据合并生成新的基线，这个过程称为合并，合并会造成一些额外的压力，可能对客户的请求有影响。云数据库OceanBase采取轮转合并的策略， 即将多个IDC中的其中一个IDC的流量切走进行合并，待合并完成后再将流量切到已合并的IDC上，这样可以避免对业务的影响，同时这种策略也可以用在升级维护中。当需要进行版本升级的时候，可以将其中一台OBServer的流量切走进行升，升级完成后逐步灰度切流，一旦出现问题即可快速无损回滚。

可扩展性

对比传统的关系数据库，OceanBase从数据库层面提供真正意义上的水平扩展能力。

OceanBase基于分布式系统实现，可以很方便地进行扩容和缩容，且能做到用户无感知。同时，OceanBase所具备的集群内动态负载均衡、多机分布式查询、全局索引的能力更进 一步加强了其可扩展性。

对于用户的分库表方案，OceanBase还提供了分区表和二级分区的功能，可以完全取代 MySQL。

高可用性

同一数据保存在多台（ >=3）服务器中的半数以上服务器上，例如3台中的2台，每一笔写事务也必须到达半数以上服务器才生效。因此，当少数服务器故障时不会有任何数据丢失，能够实现RPO等于零。

不仅如此，OceanBase底层实现的Paxos高可用协议，在主库故障后，剩余的服务器会很快自动选举出新的主库， 实现自动切换，并继续提供服务。

多租户隔离

OceanBase定位为云数据库，从数据库底层实现多租户和租户之间的资源隔离。通过这一技术，OceanBase的一个集群可以服务多个业务。每个业务会创建一个或者多个租户，租户之间互相隔离，可以设置每个租户允许使用的资源。

当某个租户使用的资源超出配额时，系统会自动对该租户进行服务降级，避免影响其它租户。

定制化产品组件

OceanBase拥有多种定制化产品组件，拓展产品功能并提高运行维护能力。主要产品组件包括OceanBase云平台、OBProxy、备份恢复工具、历史库平台等。

- OceanBas云平台（OceanBase Cloud Platform，简称OCP）是 OceanBase数据库集群的云管控平台，涵盖资源和容量管理、集群和实例生命周期管理、OpenAPI以及基于实时计算的性能监控和告警等功能模块，为用户提供一站式OceanBase数据库运维管控服务。用户及第三方也可以通过OCP提供的OpenAPI定制开发适合自身需求的管控工具和平台。
- OBProxy是OceanBase集群的反向代理，应用程序通过MySQL驱动程序连接OBProxy后，就能访问整个OceanBase集群。OBProxy主要提供语句路由功能以及让OceanBase的分布式架构对前端应用透明。路由功能可以有效提升OLTP型语句的执行性能，分布式架构对业务透明可以有效减少由于网络闪断、节点故障等事件对业务的影响。
- 备份恢复工具支持通过集群和租户两个粒度对OceanBase集群中的数据进行备份和恢复，给用户提供多副本之外的数据安全保障。基于OceanBase的数据存储方式，备份和恢复过程都包括对持久化的基线数据和内存中增量数据的操作，并且可以恢复到指定时间点。备份数据的存储可以选择OSS云存储或本地存储。
- 历史库平台为用户提供了一站式数据存储、归档解决方案。用户可以方便地配置迁移任务，指定规则将符合条件的数据从在线数据库（OceanBase、MySQL、Oracle）迁移到低成本的OceanBase历史库集群中。提供迁移限速配置、迁移后数据校验、校验成功后删除在线数据等功能，方便易用。

12.15.2. 产品价值

云数据库OceanBase是一款高性能、分布式的金融级关系型数据库，当用户的业务飞速发展的时候，OceanBase总是可以自由扩展，提供低延迟、高吞吐的数据库服务，让用户有更好的体验。例如2017年的双11，OceanBase承担了100%的交易流和支付流量，支付峰值25.6万笔/秒，数据库处理峰值4200万次/秒，为互联网金融的蓬勃发展做出了巨大贡献。

低成本

使用云数据库OceanBase，在同等情况下，要比使用MySQL等传统关系数据库节省大量的硬件成本。

弹性可扩展

云数据库OceanBase是一款真正意义的分布式关系型数据库，由一个个独立的通用计算机作为系统各个节点，数据根据容灾、可用性自动分布在各个节点，OceanBase总是可以不断的扩展节点的数量，满足业务需求。

持续可用

当某个节点出现异常时，云数据库OceanBase可以自动剔除此服务节点，对应的数据服务由其他节点提供。甚至当某个数据中心出现异常，云数据库OceanBase可以在短时间内将服务节点切换到其他数据中心，保证业务持续可用。

零数据丢失

云数据库OceanBase每一次事务提交，对应日志总是会在多个（三个）数据节点实时同步，并持久化。其中，任何节点发生不可恢复的故障，OceanBase总是可以在其他的节点恢复每一笔已经完成的交易，实现了真正金融级别的可靠性要求。

12.15.3. 应用场景

云数据库OceanBase拥有更高的性能，并向用户提供金融级别的可靠性，全分布式的架构让他的存储容量总是可以不断扩展。

金融级数据可靠性需求

金融环境下通常对数据可靠性有更高的要求，OceanBase每一次提交事务，总是会在多个数据中心实时同步对应日志，并持久化。即使发生数据中心级别的灾难，也可以在其他的数据中心恢复每一笔已经完成的交易，实现真正金融级别的数据可靠性需求。

让数据库适应飞速增长的业务

业务的飞速成长，通常会成倍给数据库带来压力。OceanBase是一款真正意义的分布式关系型数据库，由一个个独立的通用计算机作为系统各个节点，数据根据容量大小、可用性自动分布在各个节点，当数据量不断增长时，OceanBase可以扩展节点的数量，满足业务需求。

连续不间断的服务

分布式的OceanBase集群，当某个节点出现异常时，可以自动剔除此服务节点，该节点对应的数据有多个其他副本，对应的数据服务也由其他节点提供。甚至当某个数据中心出现异常，OceanBase可以在短时间内将服务节点切换到其他数据中心，可以保证业务持续可用。

13.中间件服务

13.1. 企业级分布式应用服务EDAS

企业级分布式应用服务EDAS（Enterprise Distributed Application Service）是一个应用托管和微服务管理的云原生PaaS平台，提供应用开发、部署、监控、运维等全栈式解决方案，同时支持Spring Cloud和Apache Dubbo（以下简称Dubbo）等微服务运行环境，助力用户的应用轻松上云。

13.1.1. 产品详情

EDAS作为阿里巴巴分布式服务架构的核心产品，涵盖了应用生命周期管理、运维管控等众多功能。

应用托管

用户的应用可以部署到ECS集群和K8s集群中，如果有多套环境，还可以使用命名空间进行隔离。目前，不同类型的集群对应用框架及程序打包方式有一些限制。

应用	可选集群	打包方式
Spring Cloud、Dubbo和HSF	ECS集群	WAR/JAR
	K8s集群	WAR/JAR/镜像

您可以通过控制台和工具两种方式将应用托管到EDAS中。

应用生命周期管理

应用部署完成后，可以通过EDAS控制台进行其它应用生命周期管理操作。

生命周期管理包括创建、部署、扩容、缩容、停止、删除等。因部署的集群类型不同，生命周期管理操作有些差异。

应用开发

EDAS支持基于原生Spring Cloud、原生Dubbo以及HSF开发的应用托管到EDAS中。

- Spring Cloud框架下开发的应用只需添加依赖、修改很少的配置，即可托管到EDAS。无需搭建Eureka和Consul，节省部署、运维成本，并能够获取EDAS企业级的应用托管、服务治理、监控报警和应用诊断等能力。
- Dubbo框架下开发的应用只需添加依赖、修改很少的配置，即可托管到EDAS。无需搭建ZooKeeper和Redis，节省部署、运维成本，并能够获取EDAS企业级的应用托管、服务治理、监控报警和应用诊断等能力。
- HSF是在阿里巴巴内部广泛使用的分布式RPC服务框架。连通不同的业务系统，解耦系统间的实现依赖；统一了分布式应用中服务的发布/调用方式，从而帮助您方便、快速的开发分布式应用；提供或使用公共功能模块，并屏蔽了分布式领域中的各种复杂技术细节。

微服务治理

EDAS为各种框架的微服务应用提供了服务查询、调用链查询、离群实例摘除和服务鉴权等完整的微服务治理能力。

- 服务查询：在具体地域及命名空间下，查看应用中的Dubbo、Spring Cloud和HSF服务。
- 调用链查询：通过设置查询条件，可以准确找出哪些业务性能较差，甚至异常。
- 离群实例摘除：在微服务架构中，当服务提供者的应用实例出现异常，而服务消费者无法感知时会影响服务的正常调用，并影响消费者的服务性能甚至可用性。离群实例摘除功能会检测应用实例的可用性并进行动态调整，以保证服务成功调用，从而提升业务的稳定性和服务质量。
- 服务鉴权：当您的某个微服务应用有安全要求，不希望其它所有应用都能调用时，可以对调用该应用的其

它应用进行鉴权，仅允许匹配鉴权规则的应用调用。

- 弹性伸缩：弹性伸缩能够感知应用内各个实例的状态，并根据状态动态实现应用扩容、缩容。在保证服务质量的同时，提升应用的可用率。
- 限流降级：限流降级用于解决后端核心服务因压力过大造成系统反应过慢或者崩溃问题，通常用于例如商品秒杀、抢购、大促、防刷单等大流量场景
- 健康检查：健康检查对容器与应用进行定时检查和汇报，然后将结果上报到控制台，从而帮助您了解集群环境下整个应用的运行状态，排查和定位问题。
- 全链路流量控制：您可以通过全链路流量控制实现应用新、旧版本的平滑过渡。

配置管理

EDAS已经集成了应用配置管理ACM。用户可以在EDAS中使用ACM对应用配置进行集中管理和推送，还可以基于命名空间在不同环境间进行配置的隔离和同步。配置管理包括创建、管理配置，查看历史版本和查询监听。

应用监控

在应用托管到EDAS后，可以对应用进行监控，包括监控总览、监控详情、接口调用监控、日志和通知报警。

- 应用监控：实时监控应用的IaaS层资源和服务的健康状态，帮助您快速发现、定位问题。同时支持开通高级监控（应用实时监控服务ARMS）。
- 日志：无需登录实例就可以查看实例上所部属的应用运行日志。当应用出现异常情况的时候，您可以通过查看日志来排查问题。
- 实时日志（适用于在K8s集群中部署的应用）：当应用出现异常情况的时候，您可以通过查看实时日志来排查Pod相关问题。
- 通知报警：当某些资源使用过度时，通过短信与邮件的方式通知给相应的联系人及时处理线上问题。

系统管理

EDAS在系统管理中提供了账号、角色、权限等功能。用户可以通过系统管理的功能管理、控制权限。

- 主子账号体系： 通过主子账号体系。您能够根据自己企业的部门划分、团队划分和项目划分在EDAS平台上建立对应的主子账号关系；同时，ECS资源也以主子账号关系进行划分，便于用户进行资源的分配。
- 角色与权限控制：应用的生命周期管理通常涉及研发、运维和机器资源等角色，不同的角色对于应用的管理操作各不一致。因此EDAS提供了角色和权限控制机制，方便用户为不同的账号定义各自的角色，并分配相应的权限。
- 服务鉴权：为保证您每一次分布式调用的稳定与安全。在服务注册、服务订阅以及服务调用等每一个环节，都进行严格的服务鉴权。

13.1.2. 产品价值

EDAS支撑了整个阿里巴巴99%以上的大规模应用系统，其中涵盖了包括会员、交易、商品、店铺、物流和评价在内的所有在线核心系统，在稳定性、可靠性等多个维度具有独特的优势。

更可靠

- 阿里巴巴近10年使用与沉淀的核心技术产品。
- 支持全集团所有核心应用稳定运行。
- 历次双十一大促考验。
- 完善的鉴权体系保证每一次服务调用的安全可靠。

更全面

- 完善的PaaS平台支持应用生命周期的管理。
- 完整的服务治理解决方案管理分布式服务。
- 全面的应用诊断排查系统轻松定位故障根源。

- 线上压测轻松获取线上机器运行性能指标和实时运行水位。
- 自动弹性伸缩从容应对突发流量高峰。

更深入

- 深入业务指标，实现全盘报表。
- 立体化多维度监控，实现全息排查。
- 链路跟踪洞察每一次分布式调用。
- 依赖分析剖析每一处系统瓶颈。

更开放

- 多款互联网中间件已经开源。
- 捐献Apache顶级项目，极佳的业界口碑。
- 无捆绑，可以轻松使用开源软件替换。

13.1.3. 应用场景

EDAS是分布式架构和数字化业务上云的首选应用托管平台，具有广泛的应用场景。

微服务解决方案

EDAS支持Apache Dubbo、Spring Cloud和HSF三大主流微服务框架。内置的HSF框架为久经阿里双11考验的高效微服务框架，孵化自阿里众多业务场景的最佳实践。同时零代码入侵就能完成Apache Dubbo和Spring Cloud应用上云，有效降低运维成本，支持灰度发布、流量控制等多种高级特性，助力您在云上轻松构建微服务应用。

- **能够基于成熟微服务框架快速构建应用** ：借助阿里久经考验的微服务框架HSF在云上构建微服务应用。
- **Apache Dubbo和Spring Cloud上云**：无需构建ZooKeeper、Eureka和Consul等微服务依赖的自建服务，极大降低运维成本。
- **满足企业级高级特性需求** ：内置灰度发布、流量控制和环境隔离等企业级高级特性。

应用托管解决方案

免去运维人员逐台登录逐台部署服务器的繁杂操作，免集群维护。用户只需要登录EDAS控制台，就可以通过WAR包、JAR包或镜像等多种方式快速部署应用，基于ECS提供全应用生命周期管理，包括发布、回滚、应用分组管理、多版本并存，并集成监控、日志等能力，极大的提升了ECS的集群管理效率。

- **大幅降低运维成本** ：免IaaS运维及集群维护，有效降低运维人力成本。
- **应用全生命周期管理** ：可视化管理应用生命周期，应用运行状态了如指掌。

容器托管解决方案

EDAS支持以容器的形式托管应用，无缝对接阿里云容器服务Kubernetes版，用户无需理解容器服务底层细节。通过EDAS控制台就能完成应用在容器里的全生命周期管理，包括监控、诊断等服务。用户可以低门槛拥抱容器新技术，最大化利用资源。

- **无缝支持Kubernetes**：Kubernetes集群托管给EDAS，用户仅需关注应用生命周期管理即可。
- **容器与微服务完美结合** ：基于Kubernetes，快速构建容器上的微服务架构。
- **无需构建镜像** ：支持WAR包和JAR包直接部署，EDAS代为构建镜像并部署到Kubernetes集群，有效简化流程降低使用门槛。

13.2. 分布式任务调度SchedulerX 2.0

分布式任务调度SchedulerX 2.0是阿里巴巴基于Akka架构自研的的新一代分布式任务调度平台，提供定时、工作流任务编排、分布式批量调度等功能，具有高可靠、海量任务、秒级调度能力。企业可以在控制台配置、管理自身的定时调度任务、查询任务执行记录和运行日志，还可以通过工作流进行任务编排和数据传递。SchedulerX 2.0提供了简单易用的分布式编程模型，简单几行代码就可以将海量数据分发到多台机器上执行。

13.2.1. 产品详情

SchedulerX 2.0主要提供调度、执行和运维三方面的功能。

调度

SchedulerX 2.0支持定时（多种定时表达式）和工作流调度。

- 多种表达式的定时调度
  - Crontab：支持Unix Crontab表达式，详情请参见Quartz Cron表达式。不支持秒级别调度。
  - Fixed rate：Crontab必须被60整除，不支持其它数量级时间间隔的任务，如每隔40分钟的定时任务。Fixed rate专门用来做定期轮询，可以弥补Crontab的不足，且表达式简单。不支持秒级别调度。
  - Second delay：适用于对实时性要求比较高的业务，例如执行间隔为10秒的定时调度任务。支持秒级别调度。
  - 日历：支持多种日历，还可以自定义导入日历。适用于金融业务，如需要在每个交易日执行定时任务。
  - 时区：适用于跨国业务，如需要在每个国家所在时区执行定时任务。
- 工作流调度

  使用有向无环图DAG（Directed Acyclic Graph）进行任务编排，操作简单，前端直接拖拖拽拽即可。详细的任务状态图能直观的看到下游任务为什么没执行。

在定时调度和工作流调度中支持基于多语言的多种任务类型。

- Java：可以在用户进程中执行，也可以通过上传JAR包动态加载。
- Shell：前端直接写Shell脚本。
- Python：前端直接写Python脚本，需要Python环境。
- Go：前端直接写Go脚本，需要Go环境。
- HTTP：HTTP任务无需依赖Client，在控制台配置完即可使用。
- 自定义：可以自定义任务类型，然后实现一个Plugin即可。

执行

SchedulerX 2.0支持多种执行方式和主流的分布式编程模型。

- 多种执行方式
  - 单机：随机挑选一台机器执行。
  - 广播：所有机器同时执行且等待全部结束。
  - 并行计算：map/mapreduce模型，1~300个子任务，有子任务列表。
  - 内存网格：map/mapreduce模型，100,000以下子任务，无子任务列表，基于内存计算，比网格计算快。
  - 网格计算：map/mapreduce模型，1000,000以下子任务，无子任务列表，基于文件H2计算。
  - 分片运行：类似elastic-job模型，控制台配置分片参数，可以将分片平均分给多个客户端执行。支持多语言版本。
- 分布式编程模型
  - Map模型：类似于Hadoop MapReduce里的Map。只要实现一个Map方法，简单几行代码就可以将海量数据分发到多台机器上执行。
  - MapReduce模型：MapReduce模型是Map模型的扩展，废弃了postProcess方法，新增Reduce接口，需要实现MapReduceJobProcessor。

运维

SchedulerX 2.0支持数据大盘、报警监控、日志搜集、失败重试，数据时间和重刷数据等运维能力。

- 数据大盘

  控制台提供了执行记录大盘和执行列表，可以看到每个任务的执行历史，并提供操作。

- 查看日志

  每次执行的调度任务都可以在详情中查看运行日志。如果任务执行失败，前端直接就能看到错误日志，非常方便。

- 原地重跑

  任务失败，修改完代码发布后，可以立即重新执行。

- 标记成功

  任务执行失败后，后台已经手动订正数据，可以直接将任务标记为成功，无需再花费数小时重新执行任务。

- 停止调度任务

  实现JobProcessor的`kill()`接口，用户可以在前端停止正在运行的任务，甚至子任务。

- 数据时间

  SchedulerX 2.0可以处理有数据状态的任务，在创建任务的时候设置调度时间，而实际上处理的数据时间可能和任务执行时间不一致，可以配置时间偏移，调度时间加上时间偏移即数据时间。例如一个任务是每天00:30运行，但是实际上要处理前一天的数据，就可以向前偏移一个小时。调度时间不变，执行的时候通过`context.getDataTime()`获得的就是前一天23:30。

- 重刷数据

  既然任务具有了数据时间，就会用到重刷数据。例如一个工作流最终产生一个报表，但是业务发生变更（新增一个字段）或者发现上一个月的数据有错误，那么就需要重刷过去一个月的数据。通过重刷数据功能，可以重刷某些任务/工作流的数据（只支持天级别），每个实例都是不同的数据时间。

- 失败自动重试
  - 实例失败自动重试：在任务管理的高级配置中，可以配置实例失败重试次数和重试间隔，例如重试3次，每次间隔30秒。如果重试3次仍旧失败，该实例状态才会变为失败，并发送报警。
  - 子任务失败自动重试：如果是分布式任务（并行计算/内网网格/网格计算），子任务也支持失败自动重试和重试间隔，同样可以通过任务管理的高级配置进行配置。

- 报警监控

  支持通过邮件、钉钉、短信或电话进行任务执行失败、超时和无可用机器报警通知。

13.2.2. 产品价值

SchedulerX 2.0具备高性能、高可靠、丰富的场景和简单易用等优势。

高性能

通过分布式的架构和Akka异步特性，支持海量任务和秒级别调度。

高可靠

通过主备机制、消息At-least-once delivery、定期轮检等多种手段，保证任务调度和运行的高可靠。

丰富的调度和计算场景

支持定时调度、API调度、任务编排；支持单机、广播、分布式计算多种计算模型。

简单易用

接入简单，提供很多易用的运维工具，如前端可以查看执行记录和运行日志，支持原地重跑、重刷数据等操作。

13.2.3. 应用场景

SchedulerX的应用场景包含定时触发、定期触发和手动触发调度任务。

固定时间点触发的任务

例如：2025年11月11日0点执行的一次任务。

周期性触发的任务

例如：每秒钟（或者每小时、每天、每星期、每月等）执行一次的任务。

通过控制台手动触发的任务

例如：可以通过控制台手工触发任务的调度执行。任务触发执行后，由用户实现的Job处理器接口中的代码决定具体要完成的业务逻辑功能（例如扫表、触发RPC调用、入库、执行本地脚本等）。

13.3. 消息队列RocketMQ版

消息队列RocketMQ版（简称RocketMQ）是阿里云基于开源Apache RocketMQ构建的低延迟、高并发、高可用、高可靠的分布式消息中间件。

RocketMQ基于高可用分布式集群技术，提供消息订阅和发布、消息轨迹查询、定时（延时）消息、资源统计等一系列消息云服务，是企业级互联网架构的核心产品。RocketMQ为分布式应用系统提供异步解耦、削峰填谷的能力，同时具备海量消息堆积、高吞吐、可靠重试等互联网应用所需的特性，是支持阿里巴巴双11的核心产品。

RocketMQ目前提供TCP协议和HTTP协议层面的接入方式，支持Java、C++、.NET等多种编程语言，方便不同编程语言开发的应用快速接入RocketMQ消息云服务。

13.3.1. 产品详情

RocketMQ提供了TCP协议和HTTP协议的多种开发语言的接入方式以及多维度的管理工具，同时针对不同的应用场景提供了一系列的特色功能。

协议接入

- 支持TCP协议和HTTP协议，提供Java、C/C++和.NET SDK等多种语言的SDK。

管理工具

- Web控制台：支持Topic管理、Group管理、消息查询、消息轨迹、资源报表。
- OpenAPI：提供API允许客户将RocketMQ管理工具集成到自己的控制台。
- mqadmin命令集：专有云输出提供一套丰富的管理命令集，以命令方式对RocketMQ服务进行管理。

消息类型

- 普通消息：RocketMQ中无特性的消息，区别于有特性的消息。
- 定时（延时）消息：允许消息生产者指定消息进行定时（延时）投递，最长支持40天。
- 事务消息：实现类似X/Open XA的分布事务功能，以达到事务最终一致性状态。
- 顺序消息：允许消息消费者按照消息发送的顺序来消费消息。

特色功能

- 大消息：支持4 MB大消息（包含消息属性）。
- 消息查询：RocketMQ提供了三种消息查询的方式，分别是按Message ID、Message Key以及Topic查

询。

- 消息轨迹：通过消息轨迹，用户能清晰定位消息从发布者发出，经由RocketMQ服务端，投递给消息订阅者的完整链路，方便定位排查问题。
- 集群消费和广播消费：当使用集群消费模式时，RocketMQ认为任意一条消息只需要被消费者集群内的任意一个消费者处理即可；当使用广播消费模式时，RocketMQ会将每条消息推送给消费者集群内所有注册过的消费者，保证消息至少被每台机器消费一次。
- 重置消费位点：根据时间重置消费进度，允许用户进行消息回溯或者丢弃堆积消息。
- 死信队列：将无法正常消费的消息储存到特殊的死信队列供后续处理。
- 资源报表：消息生产和消费数据的统计功能。通过该功能，用户可查询在一段时间范围内发送至某Topic的消息总量或者TPS（消息生产数据），也可查询在一个时间段内某Topic投递给某Group ID的消息总量或TPS（消息消费数据）。
- 异地多活：可购买RocketMQ异地多活增强组件，在项目存在MSHA产品的前提下，根据地域将业务划分到不同生产中心，各生产中心同时对外提供服务，并且数据相互同步备份，当其中一个生产中心故障时，可以通过MSHA切流将业务快速切换到其他容灾站点继续处理，实现业务的平滑迁移和快速恢复。

专有云部署

- 灵活部署：支持专有云独立部署，同时支持混合云架构。
- 运维管控：专有云支持mqadmin命令集、OpenAPI运维管理工具，方便管控平台集成以及统一运维。

13.3.2. 产品价值

作为消息领域内一款专业级的消息中间件产品，RocketMQ具有高可靠、高可用、高性能等优势，并支持多种协议接入，支持独立部署。

专业

- 消息领域业内专业的消息中间件，消息保证不丢，技术体系丰富成熟。
- 开源社区产品名为Apache RocketMQ；产品多次在国内外获奖。
- 阿里云内部1000多款核心应用使用，每天流转几千亿条消息，经过双11交易、商品等核心链路真实场景的验证，稳定可靠。

高可靠

- 一份消息多份落盘存储，经过严格的断电测试，消息依然保证不丢失。
- 允许海量消息堆积，单个Topic即使堆积100多亿条消息，系统高流量压力下依然可靠。
- 默认消息持久化存储3天，支持最多重置消费位点消费3天之内任何时间点的消息。

高可用

- 通过异地多活，实现故障场景下业务的快速平滑迁移，将业务恢复和故障恢复解耦，保障了业务连续性。

高性能

- 支持水平扩展。
- 支持最大4 MB消息（含消息属性）。

支持多种协议

- 提供TCP协议和HTTP协议层面的接入方式，支持Java、C++、.NET等多种编程语言。

独立部署

- 支持专有云独立输出，支持物理机部署，仅几台机器便可搭建完整消息云服务。
- 专有云配套mqadmin命令集和管理类OpenAPI ，方便运维人员实时监控系统状态。
- 支持混合云架构，允许通过专线的方式接入公有云服务。

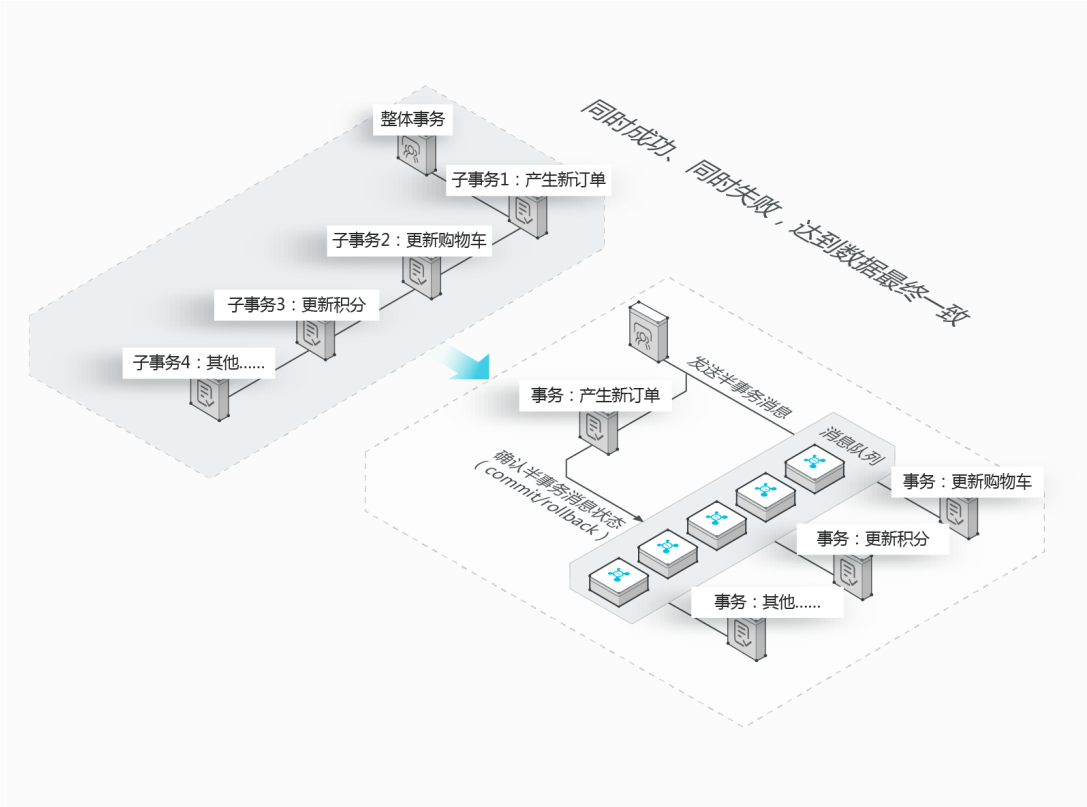
13.3.3. 应用场景

RocketMQ可应用于分布式事务、实时计算、物联网应用和大规模缓存同步。

分布式事务

在传统的事务处理中，多个系统之间的交互耦合到一个事务中，响应时间长，影响系统可用性。引入分布式事务消息，交易系统和消息队列之间，组成一个事务处理，能保证分布式系统之间数据的最终一致；下游业务系统（购物车、积分、其他）相互隔离，并行处理。

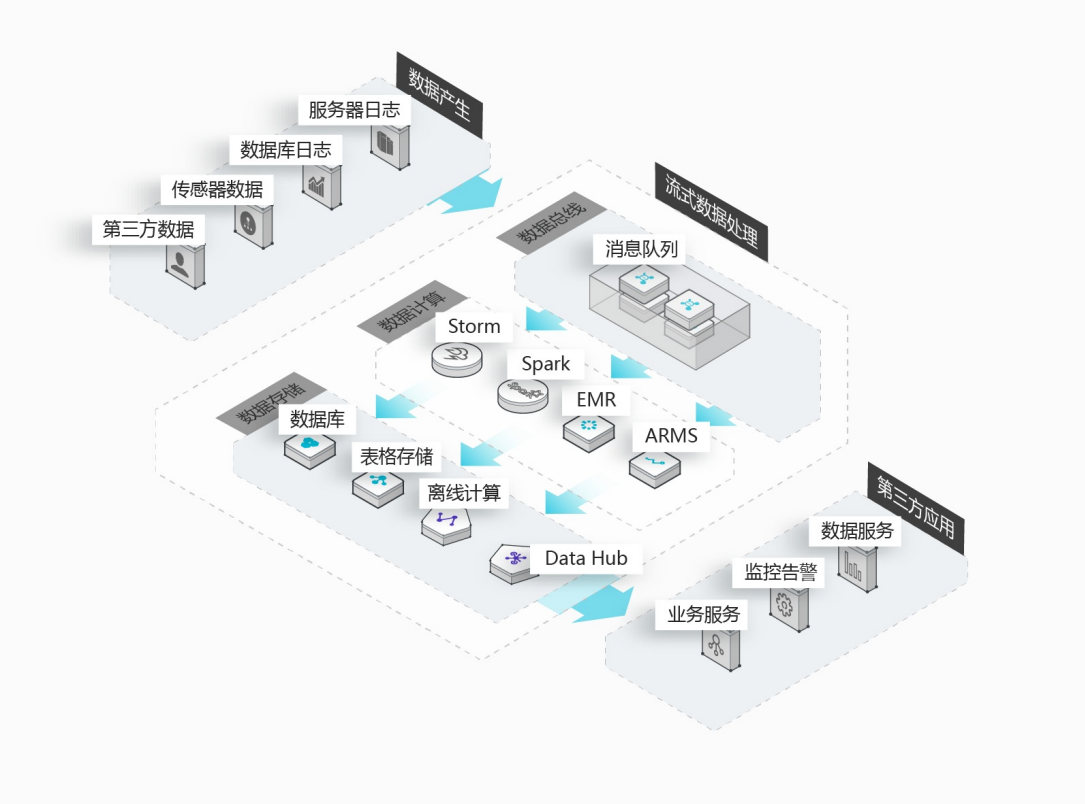
图 1. 分布式事务场景



实时计算

通过RocketMQ，将源端不停产生的数据实时流入到计算引擎，实现实时计算。用户可采用以下计算引擎：Spark/Storm/EMR/ARMS/BeamRunner。

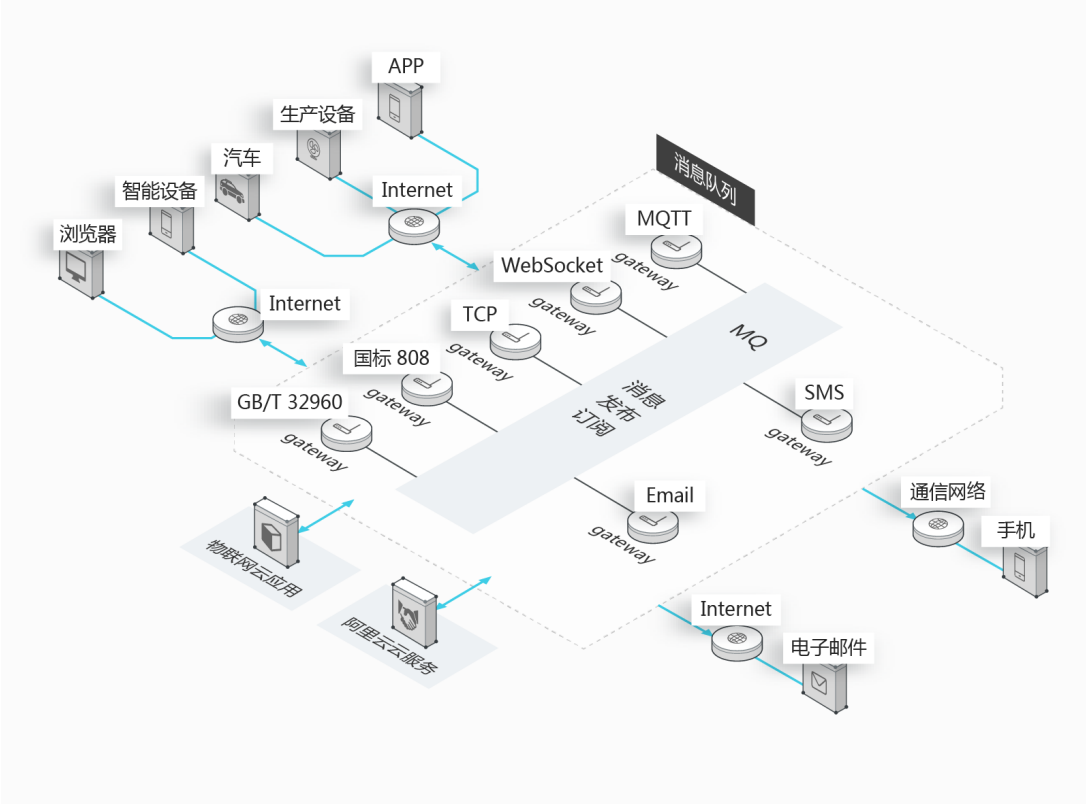
图 2. 实时计算场景



物联网应用

物联网设备通过微消息队列连接云端，双向通信，数据传输；设备数据通过RocketMQ连接计算引擎，分析数据或者源数据实时高效写入到TSDB/HiStore/MaxCompute等。

图 3. 物联网应用场景

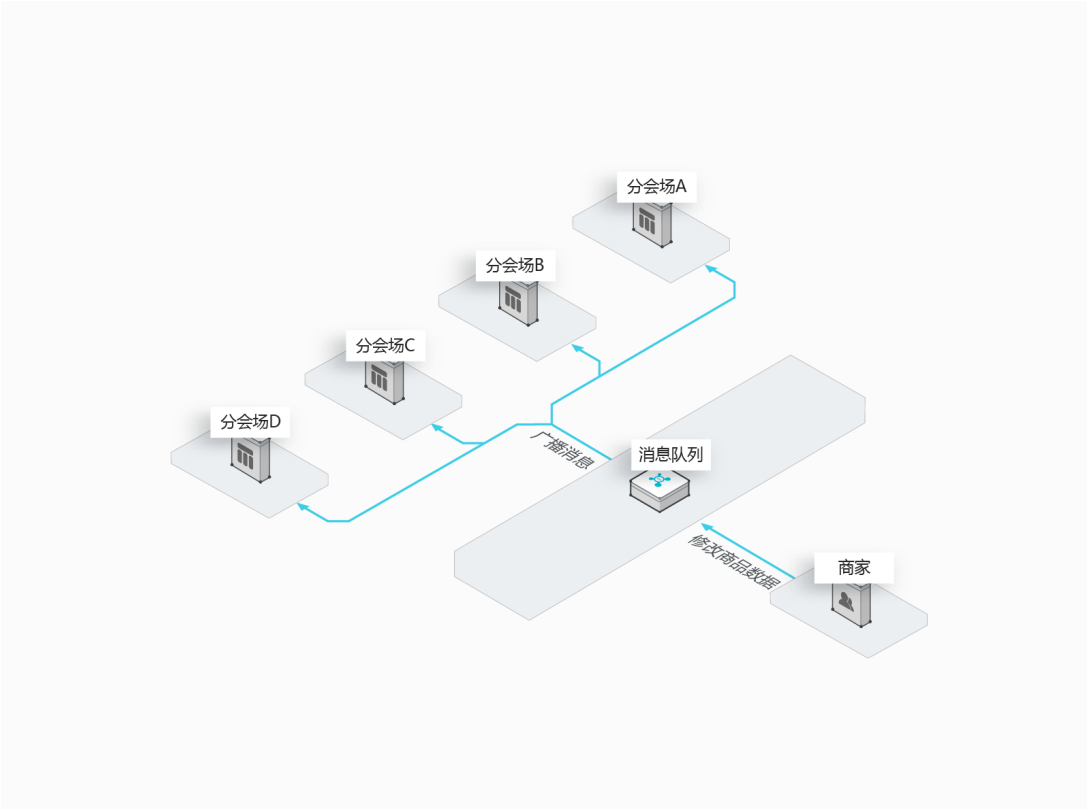


大规模缓存同步

在商业大促活动中，如“双11”大促，各个分会场会有琳琅满目的商品，每件商品的价格都会实时变化；同时，大量并发访问商品数据库，会场页面响应时间长。集中式缓存，带宽成瓶颈，无法满足对商品价格的访问需求。

RocketMQ能够通过大规模缓存同步，减少页面响应时间；针对分会场的多缓存设计，满足客户对商品价格的访问需求。

图 4. 大规模缓存同步场景



13.4. 微消息队列MQTT版

微消息队列MQTT版是阿里云推出的一款面向移动互联网以及物联网领域的轻量级消息中间件，广泛应用于移动互联网以及物联网领域，覆盖互动直播、车联网、金融支付、智能餐饮、即时聊天、移动Apps等多种应用场景；通过对MQTT、WebSocket等协议的全面支持，连接端和云之间的双向通信，可支撑千万级设备与消息并发，从而实现万物互联。

13.4.1. 产品详情

微消息队列MQTT版支持多语言的消息收发，同时针对不同的应用场景提供了一系列的高级功能。

收发消息功能

- 单独使用微消息队列MQTT版收发消息。
- 微消息队列MQTT版发送，消息队列RocketMQ版接收。
- 消息队列RocketMQ版发送，微消息队列MQTT版接收。
- 微消息队列MQTT版客户端使用签名模式。
- 微消息队列MQTT版客户端使用Token模式。
- 微消息队列MQTT版客户端使用SSL加密。
- 微消息队列MQTT版客户端发送顺序消息到消息队列RocketMQ版。
- 查询微消息队列MQTT版客户端在线数量。

高级功能

- 获取离线微消息队列MQTT版消息。
- 获取微消息队列MQTT版客户端在线状态。
- P2P消息收发模式（MQTT）。

13.4.2. 产品价值

作为一款面向移动互联网和物联网领域的消息中间件，微消息队列MQTT版可支持多种协议，能够覆盖绝大多数的移动端开发；并提供多种加密方式，为设备接入提供安全可靠的传输通道。

无缝迁移

兼容任何支持MQTT 3.1.1协议的SDK，支持WebSocket协议，覆盖绝大多数移动端开发平台及语言。

高性能

支撑千万级设备在线连接，消息百万级并发，万亿级流转，毫秒级推送；分布式架构设计，无单点瓶颈，各组件间均可水平扩展。

安全可靠

支持设备级权限控制，支持临时Token服务以及SSL/TLS传输加密通信，确保用户数据安全可靠。

天然互通

支持微消息队列MQTT版和消息队列RocketMQ版的消息互通，从而实现设备端和云端的双向打通，更高效、更可靠。

13.4.3. 应用场景

得益于微消息队列MQTT版的多协议、多语言和多平台的支持能力，目前广泛应用于移动互联网以及物联网领域，覆盖即时聊天、新零售、视频直播、智能餐饮等多种应用场景。

IM通讯

基于微消息队列MQTT版的基础功能消息收发，可实现即时通讯功能，包括一对一单聊、多对多群聊等。

新零售

微消息队列MQTT版与智能AP节点结合，可支持大量电子价签的接入和统一管理，实现商超、公共场所电子标签、多媒体屏幕的智能管理。

视频直播

在线教育直播场景中，用户使用手机、电脑等各种移动端设备接入直播间进行直播互动，通过微消息队列MQTT版可实现直播互动消息、管理员禁言、成员上下线通知等功能。

智能餐饮

随着物联网行业的快速发展，智能点餐服务已成为餐饮行业中的标配，消费者可通过手机在餐桌上扫码，通过微消息队列MQTT版连接商家的智能系统，从而实现自助下单与自助支付。

消费者、商家、后厨，全自助的智能设备端+云服务的双向通信能力，快速形成高效的智能点餐系统。

13.5. 消息队列Kafka版

消息队列Kafka版是阿里云提供的分布式、高吞吐、可扩展的消息队列服务。消息队列Kafka版广泛应用于日志收集、监控数据聚合、流式数据处理、在线和离线分析等大数据领域，已成为大数据生态中不可或缺的部分。

13.5.1. 产品详情

消息队列Kafka版针对Apache Kafka提供全托管服务，兼容Apache Kafka生态，解决开源产品长期以来的痛点，是大数据生态中不可或缺的产品之一。在底层技术实现上基于开源做了优化，用户只需专注于业务开发，更便捷、更稳定、更专业、更可靠。

兼容开源

消息队列Kafka版100%兼容开源Apache Kafka，可以直接使用开源Apache Kafka客户端与消息队列Kafka版通讯。消息队列Kafka版目前支持0.10.x~2.2.x的开源版本。

可靠性

- 采用分布式架构，支持多集群部署，支持双AZ间的同城容灾备份，业务无需改配或重启。
- 支持多副本复制，保障消息可靠性。
- 支持水平扩容，提升消息并发量与消息堆积。
- 采用健康巡检组件用于核心链路运行时巡检，针对不健康的状态进行告警。

可用性

消息队列Kafka版对消息存储做优化，解决磁盘过载导致的服务不可用问题。提供开源Metric数据监控告警能力，满足日常运维需要。

安全性

消息队列Kafka版支持ACL管控，支持SASL用户管理及用户对于Topic和Group的权限管控，确保数据安全传输。

13.5.2. 产品价值

消息队列Kafka版相比于自建开源Apache Kafka具备开箱即用、全托管、高可用、弹性计算等优势。

开箱即用

消息队列Kafka版100%兼容开源，支持企业无缝迁移上云。

- 兼容开源：消息队列Kafka版100%兼容开源Apache Kafka，企业可以直接使用开源Apache Kafka客户端与消息队列Kafka版通讯。消息队列Kafka版支持的客户端版本为0.10.x~2.2.0。
- 无缝迁移：消息队列Kafka版基于现有的开源Apache Kafka生态，企业无需额外代码改造，即可迁移上云。

全托管服务

消息队列Kafka版拥有专业且经验丰富的运维团队，以及成熟的运维体系。

监控报警：消息队列Kafka版提供完整的监控图表和报警，帮助用户及时发现问题。

高可用性

阿里云消息产品的研发与性能优化团队，进一步优化了开源产品的痛点，为用户提供更优质的服务。

- 数据持久化：专业团队保障更高可用性，消息持久化落盘到消息队列，数据高可靠，服务高可用。
- 高吞吐能力：在海量消息堆积的情况下，始终能保持消息队列Kafka版集群的高吞吐能力。

弹性计算

用户可以根据自身业务规模按需扩容，上层业务无感知。

- 集群扩容：支持横向扩容节点。
- 分区扩容：支持快速扩容分区。

13.5.3. 应用场景

消息队列Kafka版在网站活动跟踪、日志聚合、流计算处理和数据中转枢纽等方面都得到广泛的应用。

网站活动跟踪

成功的网站运营需要对站点的用户行为进行分析。通过消息队列Kafka版的发布/订阅模型，用户可以实时收集网站活动数据（例如注册、登录、充值、支付、购买），根据业务数据类型将消息发布到不同的Topic，然后利用订阅消息的实时投递，将消息流用于实时处理、实时监控或者加载到Hadoop、MaxCompute等离线数据仓库系统进行离线处理。

消息队列Kafka版用于网站活动跟踪具备以下优势：

- 高吞吐：网站用户产生的行为信息较为庞大，需要较高的吞吐量来支持。
- 弹性扩容：网站活动导致行为数据激增，云平台可以快速按需扩容。
- 大数据分析：可对接Storm、Spark等实时流计算引擎，亦可对接Hadoop等离线数据仓库系统。

日志聚合

许多公司，例如淘宝、天猫等，每天都会产生大量的日志（一般为流式数据，例如搜索引擎PV、查询等）。相较于以日志为中心的系统，例如Scribe和Flume，消息队列Kafka版在具备高性能的同时，可以实现更强的数据持久化以及更短的端到端响应时间。消息队列Kafka版的这种特性决定它适合作为日志收集中心。消息队列Kafka版忽略掉文件的细节，可以将多台主机或应用的日志数据抽象成一个个日志或事件的消息流，异步发送到消息队列Kafka版集群，从而实现非常低的RT。消息队列Kafka版客户端可批量提交消息和压缩消息，对生产者而言几乎感觉不到性能的开支。消费者可以使用Hadoop、ODPS等离线仓库存储和Strom、Spark等实时在线分析系统对日志进行统计分析。

消息队列Kafka版用于数据聚合具备以下优势：

- 应用与分析解耦：构建应用系统和分析系统的桥梁，并将它们之间的关联解耦。
- 高可扩展性：具有高可扩展性，即当数据量增加时可通过增加节点快速水平扩展。
- 在线或离线分析系统：支持实时在线分析系统和类似于Hadoop的离线分析系统。

流计算处理

在很多领域，如股市走向分析、气象数据测控、网站用户行为分析，由于数据产生快、实时性强且量大，用户很难统一采集这些数据并将其入库存储后再做处理，这便导致传统的数据处理架构不能满足需求。与传统架构不同，消息队列Kafka版以及Storm、Samza、Spark等流计算引擎的出现，就是为了更好地解决这类数据在处理过程中遇到的问题，流计算模型能实现在数据流动的过程中对数据进行实时地捕捉和处理，并根据业务需求进行计算分析，最终把结果保存或者分发给需要的组件。

消息队列Kafka版用于流计算处理具备以下优势：

- 流动的数据：构建应用系统和分析系统的桥梁，并将它们之间的关联解耦。
- 高可扩展性：由于数据产生的速度快且数据量大，需要高可扩展性。
- 流计算引擎：可对接开源Storm、Samza、Spark以及EMR、Blink、StreamCompute等阿里云产品。

数据中转枢纽

十多年来，诸如KV存储（HBase）、搜索（Elasticsearch）、流式处理（Storm、Spark、Samza）、时序数据库（OpenTSDB）等专用系统应运而生。这些系统是为单一的目标而产生的，因其简单性使得在商业硬件上构建分布式系统变得更加容易且性价比更高。通常，同一份数据集需要被注入到多个专用系统内。例如，当应用日志用于离线日志分析时，搜索单个日志记录同样不可或缺，而构建各自独立的工作流来采集每种类型的数据再导入到各自的专用系统显然不切实际，利用消息队列Kafka版作为数据中转枢纽，同份数据可以被导入到不同专用系统中。

消息队列Kafka版作为数据中转枢纽具备以下优势：

- 高容量存储：能在商业硬件上存储高容量的数据，实现可横向扩展的分布式系统。
- 一对多消费模型：发布/订阅模型，支持同份数据集能同时被消费多次。
- 同时支持实时和批处理：支持本地数据持久化和Page Cache，在无性能损耗的情况下能同时传送消息到实时和批处理的消费者。

13.6. 应用实时监控ARMS

ARMS应用监控是一款应用性能管理（APM）产品。无需修改代码，只需为应用安装一个探针，ARMS就能够对应用进行全方位监控，帮助开发人员自动生成应用拓扑，快速定位出错误接口和慢接口（慢SQL）、重现调用参数、发现系统瓶颈，从而大幅提升线上问题诊断的效率。

13.6.1. 产品详情

ARMS应用监控提供一键接入、主动诊断、无损统计等能力。

一键接入

通过与EDAS集成，在EDAS中部署的应用可以一键接入到ARMS，无需下载部署探针。

应用主动诊断能力

ARMS应用实时监控支持慢调用、慢SQL、异常、CPU使用率过高、内存溢出、线程Dump等多种典型问题的根因定位能力。

无损统计

通过Agent端预聚合以及链路数据和指标数据分路上报机制，ARMS应用性能监控指标相对同类产品更加精确。

动态配置下发

ARMS Agent支持采样率、自定义慢阈值、URL收敛等多种参数进行白屏配置，配置自动下发到Agent端，无需重启应用即可生效。

丰富的性能分析指标

ARMS应用实时监控以应用为中心，包含应用、JVM、主机、异常分析、错误分析、SQL分析、接口快照等多种维度的性能分析和监控能力。

13.6.2. 产品价值

应用监控面向分布式架构，监控Java应用，支持查看应用拓扑、接口调用、异常事务、慢事务等。

自动生成全局拓扑

- 所有应用拓扑纵览。
- 主要调用健康统计。
- 各类组件调用分类统计。

代码级根因定位

当故障发生后，传统的APM产品往往只能定位应用的某一个具体接口或某一个SQL语句，然后再结合日志和Review代码定位到具体的代码上。但在ARMS中通过接口快照可以直接定位到方法栈级别，自动分析出接口调用的方法栈耗时，解决最后一公里问题定位的问题。

捕获慢调用

- 动态设置慢调用阈值
- 自动捕获慢接口和慢方法
- 慢SQL分析

异常诊断、调用链分析和错误分析

对于传统AMP产品，没有历史数据对比，不知哪些是新增和突增的异常，只能通过异常日志逐条检查。

ARMS的异常诊断功能可以通过以下方式迅速定位问题：

- 提供今日和昨日对比，迅速发现新增和突增异常。

- 异常与请求关联，能查看是哪些请求发生了异常，平均每个请求抛出多少异常，重要异常不遗漏。
- 提供按照异常名，异常信息，异常接口三大维度观察异常，快速定位系统最核心异常问题。

ARMS错误分析功能的错误列表能够显示该应用在指定时间段的所有错误。

消息队列MQ性能分析

- 拓扑展示：实时展示应用与MQ数据源之间的消息发布和订阅关系。
- 性能指标：发布端和消费端请求数、响应时间、错误统计。
- 接口快照：提供关于消息发布和订阅的接口快照，开发人员可以通过Trace ID链接查看完整调用链以及诊断问题原因。

配置动态下发

- 采样率动态配置。
- 插件动态开关。
- 慢阈值自定义配置。
- URL收敛配置。

13.6.3. 应用场景

ARMS应用监控能够通过发现应用拓扑、捕获异常和慢接口等能力诊断应用问题。

应用拓扑发现

ARMS应用监控探针能够自动发现应用的上下游依赖关系，有效捕获、智能计算、自动展示不同应用之间通过RPC框架组成的调用链。

捕获应用异常和慢接口、慢SQL

开发人员可以进一步获取接口的慢SQL、MQ堆积分析报表或者异常分类报表，对错、慢等常见问题进行更细致的分析。

自动发现并监控接口

ARMS应用监控能够自动发现和监控应用代码中常见的Web框架和RPC框架，并统计接口的调用量、响应时间、错误数等指标。

应用问题诊断

通过调用链下钻、线程分析、异常分析等能力，对应用的性能、可用性、错误等问题进行分析，帮助用户进行根因定位。

13.7. 链路追踪Tracing Analysis

链路追踪Tracing Analysis为分布式应用的开发者提供了完整的调用链路还原、调用请求量统计、链路拓扑、应用依赖分析等工具，可以帮助开发者快速分析和诊断分布式应用架构下的性能瓶颈，提高微服务时代下的开发诊断效率。

13.7.1. 产品详情

链路追踪基于OpenTracing标准，能够接入多语言应用，并还原完整的调用链路。

分布式调用链查询和诊断

追踪分布式架构中的所有微服务用户请求，并将它们汇总成分布式调用链。

应用性能实时汇总

通过追踪整个应用程序的用户请求，来实时汇总组成应用程序的单个服务和资源。

分布式拓扑动态发现

用户的所有分布式微服务应用和相关PaaS产品可以通过链路追踪收集到分布式调用信息。

多语言开发程序接入

基于OpenTracing标准，兼容开源社区，例如Jaeger、Zipkin。

丰富的下游对接场景

收集的链路可直接用于日志分析，且可对接到MaxCompute等下游分析平台。

13.8. Prometheus监控

阿里云Prometheus监控全面对接开源Prometheus生态，支持类型丰富的组件监控，提供多种开箱即用的预置监控大盘，且提供全面托管的Prometheus服务。

13.8.1. 产品详情

Prometheus监控提供服务发现、指标采集、大盘展示、Agent水平扩容等功能。

ServiceMonitor服务发现

支持使用CRD ServiceMonitor的方式来满足用户自定义服务发现的采集需求。通过使用ServiceMonitor，用户可以自行定义Pod发现的Namespace范围以及通过MatchLabel来选择监听的Service。

容器集群Metrics采集

兼容标准Prometheus监控的数据采集能力，支持容器Node、GPU、Kube State等数据采集。

支持查看Targets采集的Metrics指标信息。

Grafana大盘展示

默认支持K8s DaemonSet、K8s State、K8s StatefulSet、Kubernetes容器副本、Kubernetes概览、Kubernetes部署、Node Summary、Node TopN、Physical Resources、Pod TopN、Prometheus主机详情等大盘。

Prometheus监控通过Grafana大盘展示监控数据。

Prometheus Agent安装及水平伸缩（HPA）

支持通过Helm2和Helm3方式安装Prometheus Agent，同时支持对基于持久化的关键状态的采集器Agent自动扩容。

13.8.2. 产品价值

与开源Prometheus监控相比，阿里云Prometheus监控具有稳定、省时、资源占用小等优势。

落地更快，比开源节省快50倍时间

阿里云Prometheus监控无需部署，默认完成对Grafana和Alertmanager的集成，提供预置监控大盘，能够一体化Agent，自动完成部署和采集配置，10分钟完成对K8s集群的监控。

架构更稳定，支持水平扩展，采用高可用架构

阿里云Prometheus监控数据处理支持水平扩展，数据存储采用高可用架构，Agent端使用自动重传机制，并引入消息队列应对高流量。

业务侵入性更小，Agent资源占用整体比开源少50%

阿里云Prometheus监控使用一体化Agent，单进程运行，能够限制Agent资源占用，优化了内存和CPU的消耗。

13.8.3. 应用场景

Prometheus监控适用于阿里云容器服务、自检Kubernetes集群以及自建Prometheus的一体化监控的场景。

阿里云容器服务ACK和ASK集群

适合需要对容器服务集群及其上面运行的应用进行一体化监控场景。

自建的Kubernetes集群

适合需要对自建Kubernetes集群及其上面运行的应用的一体化监控场景。

自建的Prometheus

适合已自建了Prometheus Server，但是需要通过Remote Write的方式来解决Prometheus存储的可用性和可扩展性的场景。

13.9. CSB开放平台

CSB开放平台OP（Open Platform），即原版云服务总线CSB，具有服务协议适配和开放管控能力，可以实现跨环境、跨协议的服务互通，主要针对应用系统能力对外开放和服务互相访问的场景，提供统一的安全授权、流量限制等管理和控制。

13.9.1. 产品详情

CSB开放平台基于API服务总线、API组织管理和API运维监控提供了诸多功能。

API服务总线

提供高可用、稳定高效、可线性扩容的服务能力以及丰富全面的访问控制功能。

- 协议转换：支持常用协议服务的接入和开放，支持复杂类型和结构的出入参数定义，以及高度定制化、灵活的数据变换。
- 认证鉴权：支持服务访问签名，检查请求是否合法，是否已授权，可对接企业自有账号认证系统（非公共云）。
- 服务控制：提供服务访问流量限制、设置黑白名单、服务路由、响应过滤等访问控制，支持定制化实现的验签、请求校验、后端服务预请求和响应处理逻辑。

API管理组织

提供可灵活定制的API全环节管理和组织功能。

- 服务发布：提供发布后端已有服务、生命周期管理、服务组管理、服务发布审批、服务订阅审批、服务导入和导出，以及适应复杂多环境连通场景，例如混合云的跨CSB实例联动发布机制。
- 服务授权：提供灵活的服务授权方式。
- 服务消费：提供SDK，支持编程使用以及命令行调试调用；支持JWT Token调用服务。

API运维监控

提供多样的运维管控工具用以获取及时详尽的系统状态信息，使得系统维护更加方便、快捷。

- 日志监控：提供系统管控、服务消费与管理审计日志，提供服务调用统计、链路分析，以及系统的监控和巡检。
- 平台配置：提供实例管理、用户管理、灵活的系统角色权限定制能力。

13.9.2. 产品价值

CSB开放平台具有高性能稳定可靠，轻量级简便易用，跨协议开放互联，一站式服务管理等特点。

高性能稳定可靠

稳定可靠地支持大规模请求，基于阿里巴巴内部长期使用与沉淀的高可用高性能分布式集群技术产品构建。

轻量级简便易用

实现企业业务能力的高效数字化输出和迅捷变更。

- 服务发布、配置变更便捷灵活。
- 服务调用简单方便。
- 处理能力按需简便扩容。

跨协议开放互联

实现从简单的应用间调用，到新建与遗留系统之间，以及企业组织间的能力互通。

- 支持不同系统、协议服务安全可控的互联，对接企业原有系统和账号体系。
- 支持复杂结构参数转换以及多种常用协议的服务 API 发布和消费。

一站式服务管理

整体把握控制跨平台、跨系统、跨企业组织的能力开放，实现能力的统一管理、组织和互动。

- 完整的API生命周期管理，服务目录，服务授权，用户管理。
- 角色化的服务发布者、消费者、管理者，以及灵活的权限管理。
- 及时详细的服务质量监控和服务消费报告。

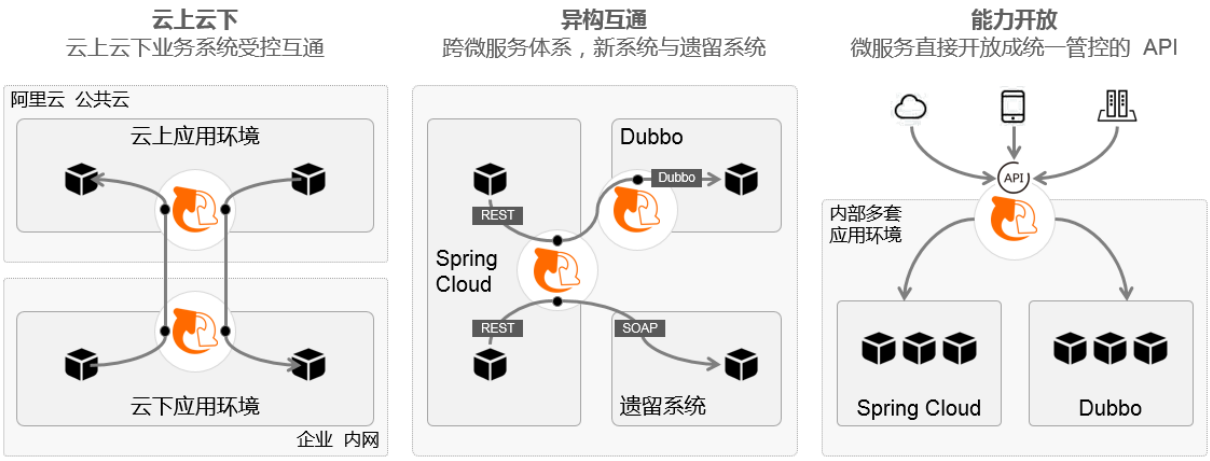
13.9.3. 应用场景

CSB开放平台可以应用于专有云、公共云，以及混合云场景，实现跨系统跨协议的服务互通。主要针对需要进行管理和控制（包括安全授权、流量限制）的系统间服务访问和对外开放场景。

CSB开放平台注重互联网场景下的开放性。企业以服务API的方式开放自身的业务能力，提供给已有的和潜在的合作伙伴，以及第三方开发者，来共同满足多变多样的需求。由于服务开放的对象广泛且多变，需要强调服务开放管理以及线性扩容能力，而不是一次性的给定两个系统之间的接口适配对接。

CSB开放平台注重解决复杂多环境多归属的系统间的互通与管控。不同的企业组织，企业组织内不同的地区，同一地区内不同的分部机构，在连通形态和管理关系上可能大不相同，需要有灵活的服务访问打通能力和管控策略适应能力。

CSB开放平台具有的跨环境服务体系互通和API开放能力，有下图所示的三种典型应用场景，即云上云下互通，不同架构协议的应用系统互通，以及多套应用环境的统一API开放，甚至可以是多种方式综合的复杂场景。



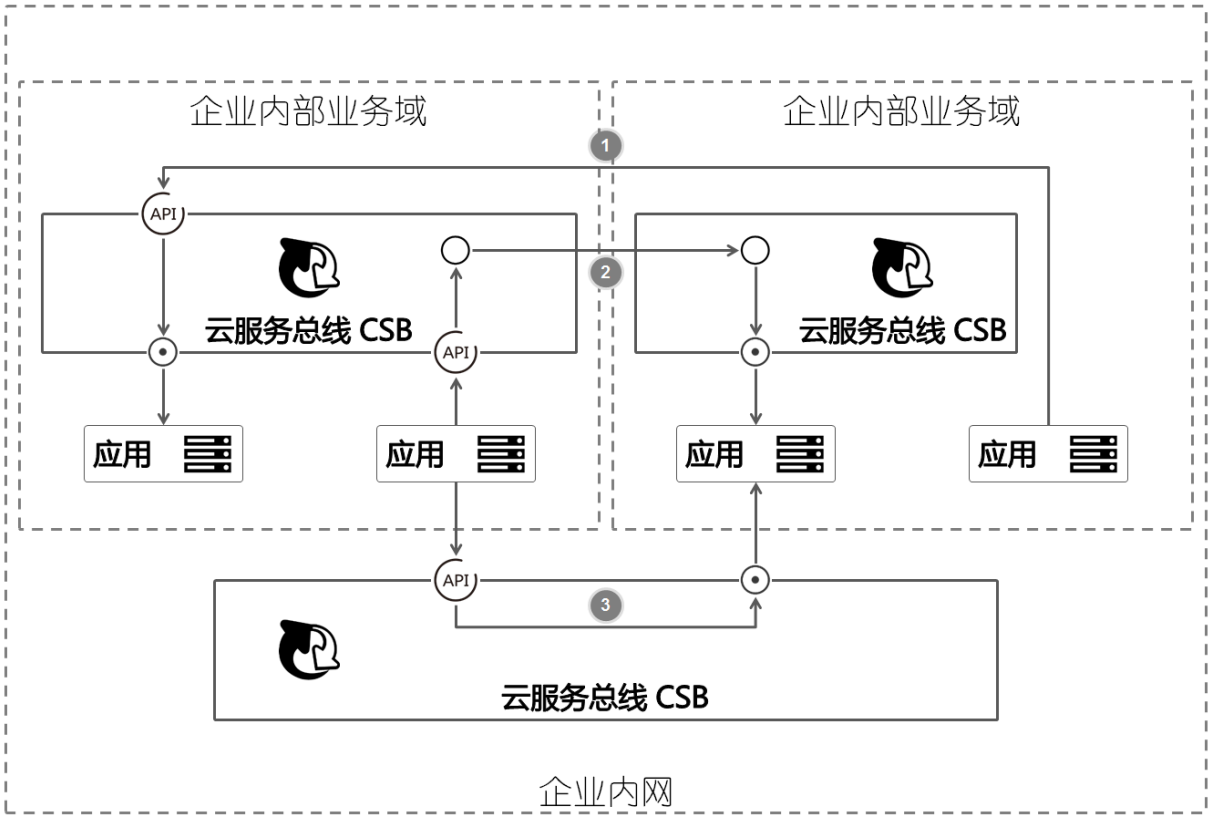
从互通的多个环境的归属和类型上分为内部互通、内外互通和混合云、云上VPC互通三个典型场景。

内部互通

企业内部服务能力通过CSB开放平台可管可控地开放互通。

- 一个域的应用通过另一个域的CSB实例访问其内部应用服务。
- 两个域的CSB实例构成的桥接通道实现互通。
- 各个域之间通过企业统一的CSB实例实现互通。

以业务能力API化规范企业业务，促进复用创新。



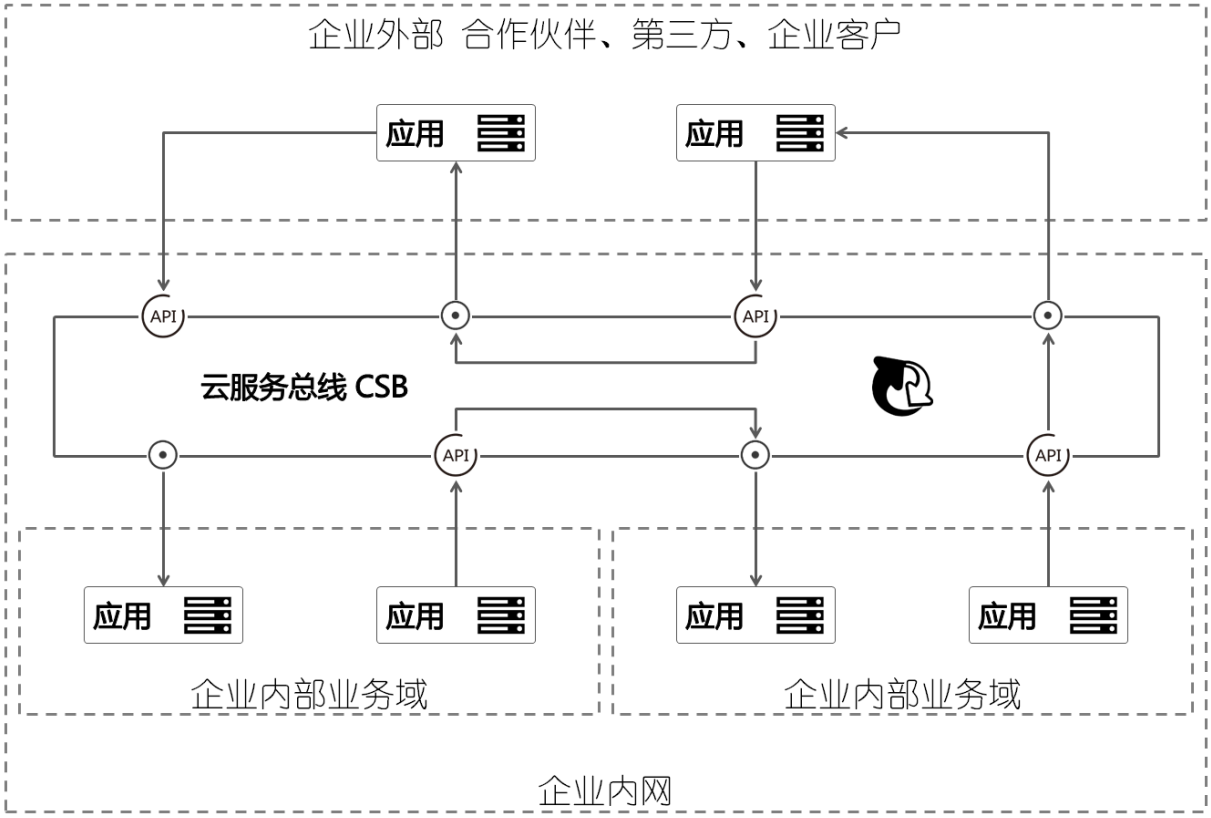
内外互通

企业内部以及与合作伙伴和第三方的系统通过CSB构建的能力开放平台，可管可控地开放互通。

- 企业内部以及合作伙伴和第三方都可以在CSB开放平台上发布和订阅服务。
- 各自的服务通过授权做访问控制（包括流量控制、黑白名单等）。

- 所有发布的服务在CSB开放平台上形成由企业自主管理的能力开放平台。

以API方式进行业务协作，高效互补业务能力、延伸服务领域，满足多样需求。

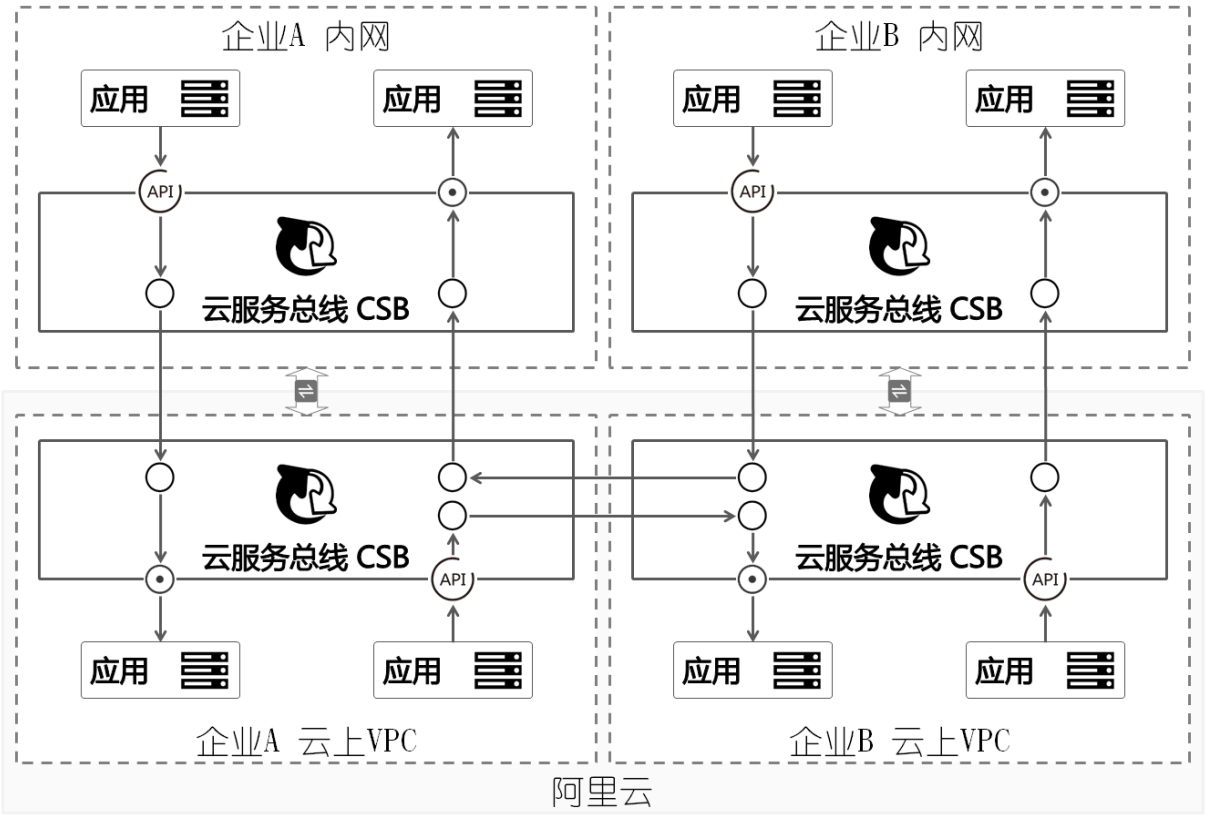


混合云、云上VPC互通

企业内部云上混合云互通，公共云上不同企业VPC之间互通。

- 企业内部CSB与其在公共云上VPC内的CSB通过专线互通。
- 公共云上的多个企业VPC之间通过各自的CSB互通。
- 每个CSB（实例）上的用户和服务由CSB实例拥有者自主管理。

解决复杂多环境多归属互通问题，提供灵活的，可自由对接和定义链路规则的联动管理。



13.10. 应用高可用服务AHAS

应用高可用服务AHAS包括性能压测、流量防护、故障演练三大功能模块，其核心功能是流量防护，分应用防护和网关防护。应用防护以流量为切入点，从流量控制、熔断降级、系统保护等多个维度来保障服务稳定性。而网关防护是从流量入口处拦截激增的流量，防止下游服务被冲垮。

13.10.1. 产品详情

AHAS提供性能压测、流量防护、故障演练的功能。

性能压测

性能测试PTS（Performance Testing Service）是具备强大的分布式压测能力的SaaS压测平台，可模拟海量用户的真实业务场景，全方位验证业务站点的性能、容量和稳定性。

流量防护

流量防护是应用高可用服务AHAS的主要功能，包括应用防护、网关防护、Nginx防护。

- 应用防护

  AHAS应用防护以流量为切入点，从流量控制、熔断降级、系统负载保护等多个维度来保障业务的稳定性，提供更专业稳定的流量防护手段、秒级的流量水位分布分析功能，是阿里巴巴双十一技术体系中的核心组件，同时也是开源框架Sentinel的商业化产品。

- 网关防护

  AHAS可以对网关进行流量控制，从流量入口处拦截骤增的流量，防止下游服务被压垮。

- Nginx防护

  Nginx为目前比较流行的高性能开源服务器，Ingress则为实际的K8s流量入口。Ingress/Nginx防护作为应用侧的上游，可以提前对业务流量做控制，从而有效地保证下游服务不会因流量激增而导致系统瘫痪。

故障演练

故障演练是一款遵循混沌工程实验原理并融合了阿里巴巴内部实践的产品，提供丰富故障场景，能够帮助分布式系统提升容错性和可恢复性。

13.10.2. 产品价值

AHAS一体化平台的性能压测、流量防护、故障演练各模块都具有诸多优势。

性能压测

- 平台稳定可靠：
  - PTS是基于支持阿里巴巴全生态多达五年的单链路、全链路压测平台的再加强版本。
  - PTS支持了多个行业，涉及电商、多媒体、金融保险、物流快递、广告营销、社交等等。
- 功能多：
  - 全SaaS化形态，无需额外安装和部署。
  - 数据工厂功能，简单编码实现压测的API、URL的请求参数格式化。
  - 复杂场景的全可视化编排，支持登录态共享、参数传递、业务断言，同时可扩展的指令功能支持多形态的思考时间、流量蓄洪等。
  - 支持RPS并发多压测模式。
  - 流量支持动态秒级调整，百万QPS亦可瞬时脉冲。
  - 强大的报表功能，将压测客户端的实时数据做多维度细分展示和统计，同时自动生成报告供查阅和导出。
  - 压测API、场景均可调试，压测过程提供日志明细查询。
- 流量真实：
  - 真实模拟最终用户的流量来源，相应的报表、数据更接近用户真实体感。
  - 施压能力强，支持千万RPS的压测流量。

流量防护

- 丰富的应用场景：流量防护承接了阿里巴巴近10年的双十一大促流量的核心场景，例如秒杀（即突发流量控制在系统容量可以承受的范围）、消息削峰填谷、集群流量控制、实时熔断下游不可用应用等。
- 完备的实时监控：流量防护同时提供实时的监控功能。用户可以在控制台中看到接入应用的单台机器秒级数据，甚至500台以下规模的集群的汇总运行情况。
- 广泛的开源生态：流量防护提供开箱即用的与其它开源框架、库的整合模块，例如与Spring Cloud、Dubbo、gRPC的整合。用户只需要引入相应的依赖并进行简单的配置即可快速地接入流量防护。
- 完善的SPI扩展点：流量防护提供简单易用、完善的SPI扩展接口。用户可以通过实现扩展接口来快速地定制逻辑。例如定制规则管理、适配动态数据源等。

故障演练

- 灵活的流程编排：
  - 故障演练将故障演练的环节分为了准备、注入、检查以及恢复四个阶段，每个阶段除了系统初始化完成的必要节点之外，用户也可以根据需要添加所需的流程节点。
  - 故障演练支持一次演练包含多个定义的故障场景，同时用户可以定制这些场景的运行方式，选择依次进行故障注入或同时注入多个场景，通过不同的策略配置来达到不同的故障注入效果。
- 丰富的故障场景：
  - 常见的基础设施资源例如CPU、内存、磁盘等故障演练。
  - 应用级别的故障注入。
  - 云原生领域的演练场景。
- 多样的专家经验：

- 专家经验都来自于阿里内部经常演练的场景，保证了演练场景的真实性以及实用性。
- 专家经验不但包括了可执行的演练流程，而且还描述了专家经验试图解决的问题以及针对的系统架构弱点。
- 专家经验极大的提升了演练创建的效率，用户可以基于专家经验配置好的流程一键生成自己的演练。

- 安全的演练防护：
  - 在演练的任意一个环节，用户都可以随时终止演练，每一个终止操作都会自动恢复注入的场景。
  - 用户可以一键终止所有正在运行当中的演练。
  - 用户可以配置演练自动的恢复时间，防止因演练时间过长而忘记恢复演练引发的不必要问题。
  - 用户可以通过全局恢复功能来配置自动恢复的策略，当某个指标符合某个要求时自动恢复演练。
- 深度集成的阿里云产品：
  - 对依赖的阿里云组件进行故障注入。
  - 通过RAM服务来授权不同账号的演练权限，提升演练的安全性。

13.10.3. 应用场景

高可用服务AHAS的性能压测、流量防护、故障演练功能适用于多业务场景且适用行业广泛。

性能压测

性能压测适用于用户新系统上线、技术升级验证、业务峰值稳定性、站点容量规划、性能瓶颈探测等场景。

流量防护

AHAS流量防护广泛用于秒杀场景、消息削峰填谷、集群流量控制、实时熔断等场景，从多个维度保障用户业务的稳定性。

故障演练

- 衡量微服务的容错能力

  通过模拟调用延迟、服务不可用、机器资源满载等，查看发生故障的节点或实例是否被自动隔离、下线，流量调度是否正确，预案是否有效，同时观察系统整体的QPS或RT是否受影响。在此基础上可以缓慢增加故障节点范围，验证上游服务限流降级、熔断等是否有效。最终故障节点增加到请求服务超时，估算系统容错红线，衡量系统容错能力。

- 验证容器编排配置是否合理

  通过模拟杀服务Pod、杀节点、增大Pod资源负载，观察系统服务可用性，验证副本配置、资源限制配置以及Pod下部署的容器是否合理。

- 测试PaaS层是否健壮

  通过模拟上层资源负载，验证调度系统的有效性；模拟依赖的分布式存储不可用，验证系统的容错能力；模拟调度节点不可用，测试调度任务是否自动迁移到可用节点；模拟主备节点故障，测试主备切换是否正常。

- 验证监控告警的时效性

  通过对系统注入故障，验证监控指标是否准确，监控维度是否完善，告警阈值是否合理，告警是否快速，告警接收人是否正确，通知渠道是否可用等，提升监控告警的准确和时效性。

- 定位与解决问题的应急能力

  通过故障突袭，随机对系统注入故障，考察相关人员对问题的应急能力，以及问题上报、处理流程是否合理，达到以战养战，锻炼人定位与解决问题的能力。

13.11. 多活容灾MSHA

多活容灾MSHA（Multi-Site High Availability），是在阿里巴巴电商业务环境演进出来的多活容灾架构解决方案，核心是面向业务应用的多活容灾。可以将业务恢复和故障恢复解耦，有基于灵活的规则调度、跨域跨云管控、数据保护等能力，保障故障场景下的业务快速恢复，助力企业的容灾稳定性建设。

13.11.1. 产品详情

MSHA支持三种容灾解决方案，包括同城多活、异地双活以及异地应用双活。

同城多活

同个城市部署多个数据中心，并行地为业务访问提供服务。

- 同城机房间的物理距离通常<50 km，跨机房的网络延迟较小（RT<2 ms）。
- 应用跨机房冗余部署，同时对外提供服务。
- 中间件、数据库跨机房主备部署，数据单点写避免考虑数据一致性问题。

异地双活

不同城市部署多个数据中心。

- 两个数据中心间的距离没有限制。
- 应用、中间件、数据库多地域冗余部署，同时对外提供服务。
- 业务流量带标，按路由规则分流，流量在数据中心（RPC、MQ、DB）内闭环。
- 多个数据中心数据异步复制。

异地应用双活

不同城市部署多个应用。

- 两个数据中心的物理距离通常≤100 km，存在跨地域的网络延迟（RT≤7 ms）。
- 应用、中间件两地冗余部署，同时对外提供服务。
- 数据库两地冗余部署，两地应用单点写数据库，无需考虑数据一致性问题，数据异步复制。

13.11.2. 产品价值

多活容灾MSHA可以保障业务连续性，是业务高速发展的架构支撑，拥有演进式容灾架构、业务大规模实践沉淀、一站式容灾管控等多种优势。

演进式容灾架构

MSHA为客户提供了从单地域到多地域，从单元到多云，从主备到多活的丰富的容灾架构，针对不同发展阶段的客户，可以基于实际的物理环境、业务规模、容灾诉求、容灾成本，选择当下最合适的容灾架构，并为后续的架构平滑演进升级打好基础。MSHA在底层云平台的基础上，构建可演进的业务容灾架构，真正为客户的业务连续性负责。

业内大规模实践沉淀

阿里巴巴集团容灾实践自2012年开始持续发展，由同城容灾到异地多活，多年的积累和沉淀在MSHA。MSHA赋能云上客户，覆盖公共云、专有云、混合云等多家头部客户，客户在各自领域的复杂容灾场景沉淀在MSHA上，共享MSHA持续实践沉淀的容灾能力。

一站式容灾管控

MSHA是一站式的容灾管控平台。横向上包括业务架构的全生命周期，从容灾架构的上线、运维、演练、升级，最后到下线。纵向上包括业务流量的完整路径，从流量接入、到服务化调用、异步化消息，再到最终数据落库。在纵向上，MSHA将持续增加对云产品及开源技术栈的支持，提升全栈的管控能力。

高可用容灾切换

作为容灾管控平台，MSHA必须保证在灾难场景下的自身高可用。MSHA围绕切流场景，梳理强弱依赖，降级DB依赖，并通过常态化演练保障自身容灾能力。

MSHA通过自上而下精细地管控每个节点的流量，以及高可用自动化切流流程，保证切流操作的可用性。同时通过常态化的巡检、监控可视化，提前暴露风险，保障客户业务随时可切、敢切。

分钟级容灾切换

MSHA基于确定性的容灾切换流程编排和统一规则控制特性，在灾难发生时，对纳管的复杂业务及组件进行统一的容灾切换，在复杂的多活场景下可具备分钟级恢复业务的能力。

自动化多活运维

多活容灾是管控加各层技术栈组件的解决方案，对各层数据面组件或集群，MSHA提供全自动化运维产品化能力，让客户没有运维后顾之忧。

13.11.3. 应用场景

MSHA通过自上而下的全域流量隔离来解决数据同步的延时无法突破物理限制的问题。

业务容灾

现实运行过程中，容灾不只用于应对地震、挖光纤等低概率事件，同样还用于应对人为原因等高概率事件。

- 人为操作失误，例如配置错误、应用发布失败等。
- 硬件故障，例如网络设备故障导致机房或者集群内多台服务器受影响。
- 网络攻击，例如DDoS等网络攻击。
- 断网或断电，例如支付宝光缆被挖断。
- 自然灾害，例如青云雷击导致机房电力故障。

基于MSHA提供的多个多活架构，当以上这些场景出现时，秉承“先恢复，再定位”的原则，可以有效提升业务的连续性，做到让“业务恢复时间”和“故障恢复时间”解耦。

容量拓展

基于MSHA提供的异地多活架构，当机房或者地域容量遇到限制时，可以在其它机房或者其它地域快速扩建业务单元，实现快速水平扩容的目的。

新技术实验田

基于MSHA构建的同城多活和异地多活等架构，本质上是提供了一种自上而下的流量隔离能力。基于这种能力，可以做到单元之间的隔离，进而完成一个技术上需要的场景：

- 基础设施的升级（数据库升级、网络升级、应用变更、配置变更等）
- 大规模的技术架构升级
- 新技术验证

14.大数据服务

14.1. 大数据管家

大数据管家ABM（Apsara Big Data Manager，原名BCC）是为大数据产品量身定做的运维管理平台，支持业务、服务、集群和主机等多个维度的监控、管理和运维。客户运维团队或驻场人员通过大数据管家的产品能力，可以轻松完成对大数据产品的统一运维管理。

14.1.1. 产品详情

大数据管家对所有大数据产品提供监控、运维和管理三大功能模块，支持客户监控大数据产品的实时运行状况，并通过图形化界面进行业务、服务、集群、主机等多个维度的运维和管理操作。

监控

- **仪表盘**：支持查看MaxCompute、DataWorks、RealtimeCompute和DataHub产品的关键运行指标概览。
- **资源库**：支持查看MaxCompute、DataWorks和DataHub的资源使用情况。
- **健康度**：支持查看各个大数据产品的监控项以及不同紧急程度的报警，并提供详情查看和修复后的再次检查。
- **报表**：支持查看每个大数据产品的巡检结果。

运维

- **业务运维**：提供对每个大数据产品的专有定制运维功能：
  - MaxCompute的业务运维用于对MaxCompue进行项目管理、作业管理和业务治理。
  - DataHub的业务运维用于展示DataHub集群中项目和日志源信息。
  - RealtimeCompute的业务运维用于展示RealtimeCompute集群中项目、作业和队列信息。
  - Elasticsearch的业务运维用于对Elasticsearch集群进行集群配置和系统配置。
  - ABM的业务运维用于对MaxCompute和DataWorks进行异地容灾配置和管理，包括配置中心、保护组管理、演练计划和故障计划。
- **服务运维**：支持从服务层面对大数据产品进行的运维，展示了集群中所有的服务角色及每个服务角色的资源使用趋势，部分大数据产品进行单独定制。
  - MaxCompute的服务运维包括控制服务、伏羲服务、盘古服务和通道服务。
  -
  - DataWorks的服务运维包括数据工场和数据集成。
  - DataHub的服务运维包括控制服务、伏羲服务和盘古服务。
  - RealtimeCompute的服务运维包括RealtimeCompute、Yarn和HDFS。
- **集群运维**：从集群层面对大数据产品的运维，包括集群概览和集群健康。
- **主机运维**：从主机层面对大数据产品进行的运维，包括主机概览。

管理

- **作业服务**：通过执行作业对大数据产品进行运维。作业分为定时作业和普通作业，定时作业可根据设置的时间自动执行，也可手动来执行，而普通作业只能通过手动来执行。
- **健康管理**：主要包括监控配置和巡检管理。

- 监控配置为每个产品内置了丰富的调度项和监控项，用于检查产品的故障并产生报警，并支持用户自定义调度间隔、启用状态等，能够及时发现产品故障并修复。
- 巡检管理提供巡检项和巡检场景的管理，并支持用户手动或定期巡检，在发生重大问题甚至故障前规避非预期的风险问题。

- **流程服务**：提供人工任务处理、流程定义和流程实例查看。
- **操作审计**：提供大数据管家中所有运维操作的历史记录及每个操作的详细信息，支持用户在事后查看历史和定位故障。

14.1.2. 产品价值

大数据管家帮助客户统一运维与管理大数据产品，增强大数据产品稳定性，降低运维成本并与提升运维效率，尤其在集群健康状况监控、数据化分析资源变化趋势与图形化界面等方面具有客户价值。

集群健康状况监控

支持对大数据产品集群的设备、资源、服务进行状态监控和配置管理，收集与展现集群的实时运行状态信息。

数据化分析资源变化趋势

支持收集集群的设备、资源与服务的实时运行状态和历史数据，并对收集的信息进行聚合分析，以分析和评估集群的健康状态。如果分析和评估结果存在风险，还可以实时推送给相关责任人。

图形化界面运维操作管理

可视化展现系统的各类运行信息，以及常见的运维操作。

14.1.3. 应用场景

在阿里云专有云相关场景中，如果客户部署了任一大数据产品，都需要通过大数据管家对部署的大数据产品进行运维管理。

专有云企业版+大数据产品

如果客户部署了阿里云专有云企业版，并且同时部署了任一大数据产品（例如，MaxCompute或DataWorks等），则需要使用大数据管家对已部署的大数据产品进行运维管理。

14.2. 大数据计算服务

大数据计算服务（MaxCompute）是阿里巴巴内部发展的一个高效能、低成本，高可用的**EB级**大数据计算服务，在集团内部每天处理超过EB级的数据量。MaxCompute是面向大数据处理的分布式系统，主要提供结构化数据的存储和计算，是阿里巴巴云计算整体解决方案中最核心的主力产品之一。

多租户、数据安全、水平扩展等特性是MaxCompute的核心设计目标，采用抽象的作业处理框架为不同用户对各种数据处理任务提供统一的编程接口和界面。

MaxCompute主要服务于批量结构化数据的存储和计算，可以提供海量数据仓库的解决方案以及针对大数据的分析建模服务。MaxCompute的目的是为用户提供一种便捷的分析处理海量数据的手段 。用户可以不必关心分布式计算细节，从而达到分析大数据的目的。

14.2.1. 产品详情

大数据计算服务（MaxCompute）是阿里巴巴自主研发的海量数据处理平台，主要提供数据上传和下载通道，提供SQL及MapReduce等多种计算分析服务，同时还提供完善的安全解决方案。

数据通道

- Tunnel：提供高并发的离线数据上传和下载服务。使用Tunnel服务向MaxCompute批量上传数据，或

者将数据从MaxCompute下载到本地。目前，Tunnel仅提供Java编程接口。

- DataHub：提供数据的实时上传和下载的功能。与Tunnel服务不同，通过DataHub上传的数据会实时体现在数据中。

计算及分析任务

- SQL：MaxCompute只能以表的形式存储数据，并且对外提供了SQL查询功能。可以将MaxCompute作为传统的数据库软件操作，但其却能处理TB、PB级别的海量数据。需要注意，MaxCompute SQL不支持事务、索引及Update/Delete等操作。同时MaxCompute的SQL语法与Oracle、MySQL有一定差别，无法将其他数据库中的SQL语句无缝迁移到MaxCompute上来。此外，在使用方式上，MaxCompute SQL最快可以在分钟或者秒级别完成查询，无法在毫秒级别返回查询结果。MaxCompute SQL的优点体现在学习成本低，不需要了解分布式概念，只要具备数据库操作经验就可以快速熟悉MaxCompute SQL的使用。
- MapReduce：MapReduce最早是由Google提出的分布式数据处理模型，随后受到了业内的广泛关注，并被大量应用到各种商业场景中。使用MapReduce需要对分布式概念有基本了解，并有对应的编程经验。MapReduce提供Java编程接口。
- Graph：MaxCompute提供的Graph功能是一套面向迭代的图计算处理框架。图计算作业使用图进行建模，图由点（Vertex）和边（Edge）组成，点和边包含权值（Value）。通过迭代对图进行编辑、演化，最终求解出结果。
- 访问并处理非结构化数据（融合计算场景）：MaxCompute团队依托MaxCompute系统架构，引入非结构化数据处理框架，解决了MaxCompute SQL面对MaxCompute表外的各种用户数据时（例如OSS上的数据）需要先通过各种工具导入MaxCompute表才能进行计算，无法直接处理的问题。
  目前，MaxCompute支持通过创建外部表，对如下九种数据源进行处理：
  - 内部数据源：OSS、TableStore、AnalyticDB、RDS、HDFS（内部）、TDDL。
  - 外部数据源：HDFS（开源）、MongoDB、Hbase。
- 访问并处理非结构化数据（内部）：通过支持读写Volume，建立了MaxCompute对非结构化数据的存储和处理能力，解决了非结构化数据只能存储在外部存储系统的问题。

Spark on MaxCompute

Spark on MaxCompute是阿里云开发的大数据分析引擎，为用户提供大数据处理能力。

SDK

MaxCompute提供给开发者的工具包。

安全解决方案

MaxCompute提供了功能强大的安全服务，为用户的数据安全提供保护。

14.2.2. 产品优势

国内优秀的大数据云服务平台，真正的数据分享平台

- 能够同时做到数据仓库、数据挖掘、数据分析、数据分享。
- 阿里巴巴集团内部使用的统一数据处理平台，支持阿里巴巴贷款、数据魔方、DMP（阿里巴巴广告联盟）、余额宝等多款产品。

MaxCompute支持的集群及用户规模极大，同时能够支持极高的作业并发数

- 单一集群规模可以达到10000+服务器（保持80%线性扩展）。
- 单个MaxCompute可以多集群部署100万服务器以上，无限制（线性扩展略差），支持同城多数据中心模式。
- 10000+用户数，1000+项目应用，100+部门（多租户）。
- 100万以上作业（目前单日平均提交任务），20000以上并发作业。

海量运算触手可得

您不必关心数据规模增长带来的存储困难、运算时间延长等烦恼，MaxCompute根据您的数据规模自动扩展集群的存储和计算能力，使您专心于数据分析和挖掘，最大化发挥数据的价值。

服务“开箱即用”

您不必关心集群的搭建、配置和运维工作，仅需简单的几步操作，您便可以在MaxCompute中上传数据、分析数据并得到分析结果。

数据存储安全可靠

采用多副本技术、读写请求鉴权、应用沙箱、系统沙箱等多层次数据存储和访问安全机制来保护您的数据，使其不丢失、不泄露、不被窃取。

管理节点可靠性

采用多节点集群架构，各组件管理节点具备高可用机制，运维管理节点故障不影响业务正常运行。

强大的容错能力

支持对集群内服务器硬盘故障自动容错处理，支持硬盘热插拔，故障硬盘的业务恢复时间小于2分钟。

完善的存储空间管理能力

支持查询分布式文件系统的存储容量、存储使用量等信息；支持数据生命周期管理；同时根据数据价值或标签可实现数据存储在不同的存储位置，包括支持Tempfile写SSD盘加快IO，提高集群资料使用效率。同时提供自优化的最佳压缩比的zstd存储压缩算法。

完善的数据备份机制

- 支持对数据进行备份，支持全量或增量备份，并支持从存储中恢复数据。
- 支持数据中心间的数据集群备份，满足多中心之间的数据互备需求，可通过大数据管家对备份过程可视化管理。
- 支持对关键组件元数据、文件及表进行备份和恢复。

安全可靠的权限控制机制

- 支持数据访问权限管理，包括登录权限、创建表权限、读写权限、白名单控制权限等。
- 支持通过云管平台管理权限控制，包括管理员分级等。
- 通过云管平台，提供集中统一的用户权限管理功能，将系统中各组件零散的权限管理功能集中呈现和管理，对普通用户屏蔽掉内部的权限管理细节，对管理员简化权限管理的操作方法，提升权限管理的易用性和用户体验。

多用户协作的多租户机制

通过配置不同的数据访问策略，您可以让组织中的多名数据分析师协同工作，并且每人仅能访问自己权限许可内的数据，在保障数据安全的前提下最大化工作效率。

- **隔离**：支持多租户（项目空间）并行执行，租户任务提交到不同的队列执行，租户间资源隔离。
- **权限**：支持对不同租户统一管理，实现租户资源的动态配置和管理、资源隔离、资源使用统计等功能，支持多级租户的管理功能。
- **调度**：支持多集群和多资源池的多租户调度。

多设备支持

在不影响运行性能的前提下，支持单组件集群中使用的CPU、硬盘、内存、网卡规格不一致，可以最大限度的兼容已有设备。

14.2.3. 应用场景

MaxCompute适用于100 GB以上规模的存储及计算需求，最大可达EB级别，并且MaxCompute已经在阿里巴巴集团内部得到大规模应用。MaxCompute适用于大型互联网企业的数据仓库和BI分析、网站的日志分析、电子商务网站的交易分析、用户特征和兴趣挖掘等。

使用成本低，数据上云周期短

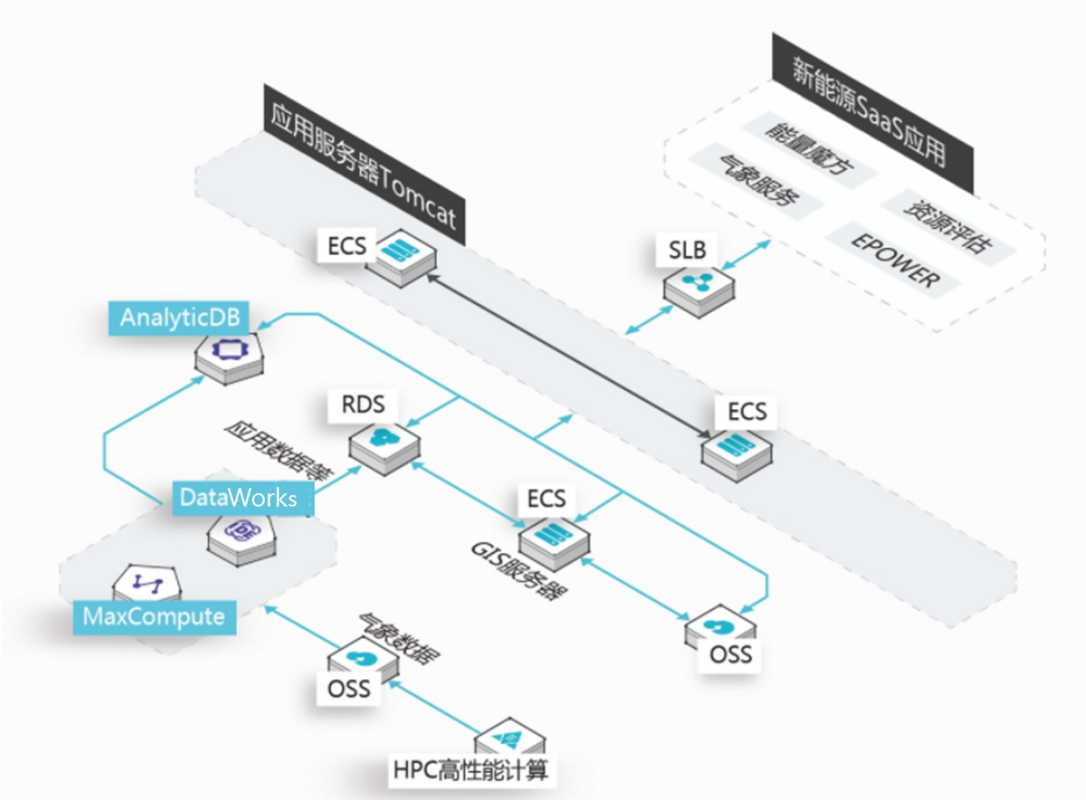
使用场景：针对某从事新能源电力领域的数据信息服务公司的业务需求，搭建新能源产业互联网大数据应用服务云平台。

目标达成：3个月内业务全面交付云端，数据处理时间不到原来自建方式的1/3，并确保云上新能源电力数据安全无忧。

客户收益：

- **让企业更专注于业务**：用了不到3个月时间，就将业务全面的交付云端，让云端的海量资源真正为业务服务。
- **降低投资、运维成本**：极大减少了自建大数据平台的物力投入、人力运维投入和研发投入。
- **安全稳定**：全方位服务能力及其稳定安全的表现确保数据上云万无一失。

应用架构图：



架构解读：使用MaxCompute、分析型数据库、DataWorks、SLB、ECS、OSS、RDS及HPC搭建云端平台。

- 使用MaxCompute进行大数据计算和分析。
- 使用分析型数据库（AnalyticDB，原名ADS）存放上亿条记录级数据，支持业务实时数据访问及展示。
- 使用DataWorks进行数据同步、数据开发、离线任务调度运维等。
- 使用阿里云SLB负载均衡，实现用户终端实时高性能接入。
- 使用阿里云ECS部署Web应用、地图服务等应用。
- 使用阿里云OSS对象存储进行海量气象数据、地图文件存储。
- 使用阿里云RDS数据库存储业务应用、地图应用数据。
- 使用阿里云HPC高性能计算进行气象数据计算。

提升开发效率，降低存储和计算成本

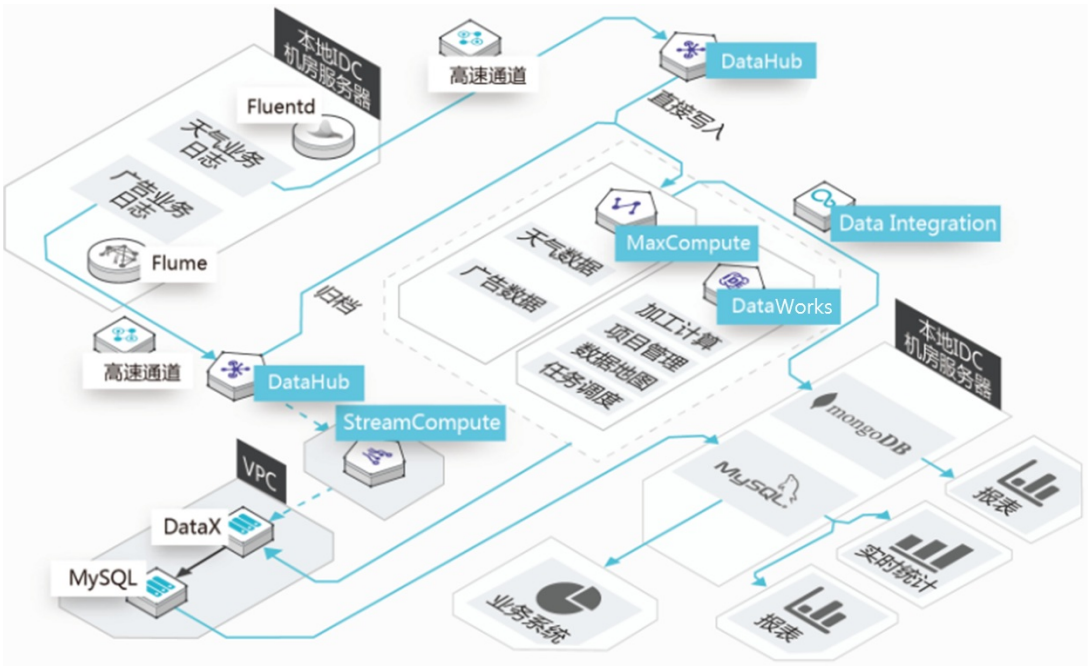
使用场景：针对某以“做卓越的天气服务公司”为目标的新兴移动互联网公司的业务需求，提供天气查询业务和广告业务的海量日志分析服务。

目标达成：该互联网公司日志分析业务迁移到MaxCompute后，开发效率提升了超过5倍，存储和计算费用节省了70%，每天处理分析2TB的日志数据，更高效的赋能其个性化运营策略。

客户收益：

- **提高工作效率**：日志数据全部通过SQL进行分析，工作效率提升了5倍以上。
- **提升存储利用率**：整体存储和计算的费用比之前节省70%，性能和稳定性也有提升。
- **个性化的服务**：可以借助MaxCompute上的机器学习算法，对数据进行深度挖掘，为用户提供个性化的服务。
- **降低大数据使用门槛**：MaxCompute提供多种开源软件的插件，轻松完成数据上云。

应用架构图：



架构解读：利用MaxCompute存储天气业务和广告业务日志数据并通过DataWorks进行计算、调度和分析，利用数据库实现数据的实时查询和计算处理，展示数据报表和实时统计结果。

- 使用MaxCompute进行大数据存储、计算和分析。
- 使用DataWorks进行数据加工计算、项目管理、任务调度运维等。
- 使用数据库（MySQL、MongoDB）存放数据，支持业务实时数据访问及展示。

盘活海量数据，实现百万用户精细化运营

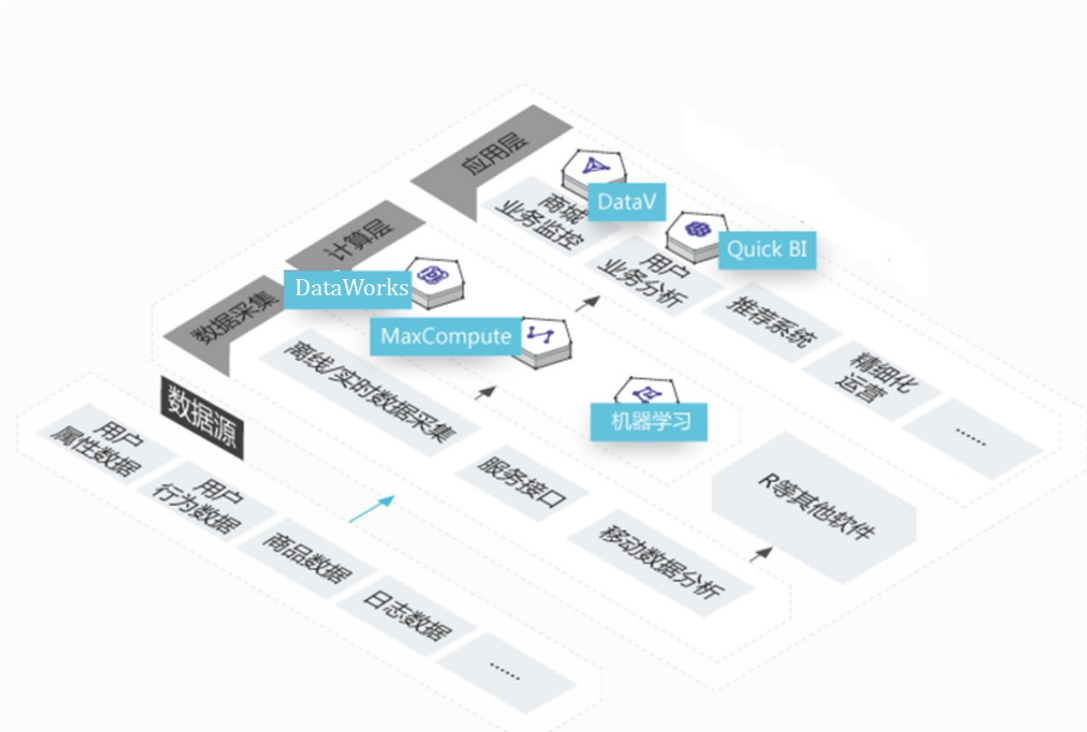
使用场景：针对某专注美甲行业的社区型垂直电商APP的业务需求，使用MaxCompute为其搭建大数据平台，主要应用在其业务监控、业务分析、精细化运营和推荐四个方面。

目标达成：该电商APP使用MaxCompute搭建的大数据平台后，通过MaxCompute的计算能力实现了针对百万用户的精细运营，业务上做到了更敏捷、更智能、更具洞察力，并且能够快速响应新业务的数据及分析需求。

客户收益：

- **提升业务洞察能力**：通过MaxCompute计算能力实现了针对百万用户的精细化运营。
- **业务数据化**：对业务数据分析能力提升并有效监控，更好的业务赋能。
- **快速响应业务需求**：MaxCompute生态满足新业务数据分析需求的“随机应变”能力。

应用架构图：



架构解读：整体架构分为数据采集层、计算层以及应用层。

- 数据采集层-数据采集、清洗、处理：数据源主要包括云数据库RDS、移动数据分析（Mobile Analytics）日志、服务接口调用的数据。以精细化运营为例，用户属性数据存放于RDS，用户行为数据来源于移动数据分析的日志数据。使用大数据开发套件DataWorks把分布在多个数据源的数据集合一起，进行清洗和加工。
- 计算层-数据分析挖掘：使用大数据开发套件DataWorks的定时任务调度功能，自动完成计算任务并将结果同步回传到数据库；IDE、机器学习以及R等工具主要解决具体的业务分析；MaxCompute用于海量数据的存储和计算引擎。
- 应用层-实际应用：使用DataV制作业务看板进行实时业务监控；推荐系统用于其个性化业务的个性化推荐；Quick BI用于业务分析；精细化运营用于用户洞察及精准营销。

大数据精准营销

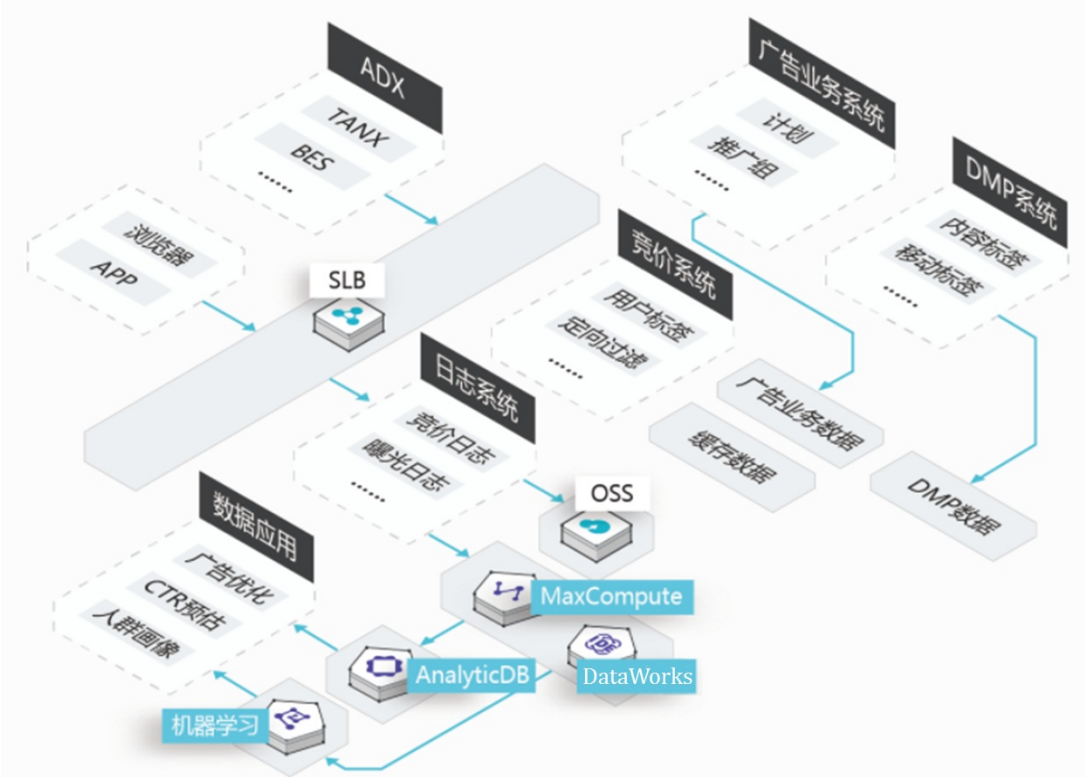
使用场景：针对某以精准营销广告技术与服务为长的互联网企业的业务需求，为其搭建核心的大数据精准营销平台。

目标达成：该企业基于MaxCompute，搭建了核心的大数据精准营销平台，所有的日志数据存储在MaxCompute并通过DataWorks进行离线调度和分析。

客户收益：

- **高效低成本的海量数据分析**：对海量日志数据进行统计分析，在满足同等业务需求基础上能够减少一半的支出，有效地节约了成本开支，帮助创业型企业快速成长。
- **数据查询分析的实时性**：MaxCompute帮助该企业确立技术优势，打破了海量数据处理分析和实时查询分析的技术瓶颈，每天通过MaxCompute收集、分析和存储20多亿条的访客行为；同时，还会根据用户需求在亿级日志表中做毫秒级查询。
- **低门槛的机器学习平台**：作为精准营销广告提供商，算法模型的好坏直接与最终收益挂钩，因此选择具有低门槛、易上手特点的MaxCompute的机器学习平台可以起到事半功倍的效果。

应用架构图：



架构解读：利用MaxCompute存储日志数据并通过DataWorks进行离线调度和分析，利用分析型数据库实现数据的实时查询和计算处理，同时通过学习机器完成开源到MaxCompute的迁移。

- 日志数据全部存储在大数据计算服务MaxCompute中。
- 大部分离线统计需求都在大数据开发套件DataWorks中开发，将数据使用做到极简，只要使用者会写SQL，就可以制作并导出自己需要的报表，满足了公司大部分的业务需求。
- 分析型数据库能够满足在亿级数据中做毫秒级查询，在即席查询及数据分析方面，能够满足数据实时计算处理的需求。
- 通过机器学习组件，逐步将开源大数据平台中的机器学习相关业务应用迁移到基于MaxCompute的机器学习平台之上。

14.3. DataWorks

DataWorks数据工场是基于MaxCompute、E-MapReduce等计算引擎，从工作室、车间到工具集都齐备的一站式大数据智能研发与治理平台，助力企业快速完成数据集成、开发、治理、服务、质量、安全等全套数据研发治理工作。

14.3.1. 产品详情

DataWorks不仅具备海量数据的离线加工分析、数据挖掘的能力，也集成了数据集成、数据开发、生产运维、实时分析、资产管理、数据质量、数据安全、数据共享等核心数据工艺，同时还提供了数据服务、机器学习（PAI）在线研发平台，承上启下，让数据从采集到展现、从分析到驱动应用得以一站式解决。

数据集成

数据集成是DataWorks提供的稳定高效、弹性伸缩的数据同步平台。致力于提供复杂网络环境下、丰富的异构数据源之间数据高速稳定的数据移动及同步能力。

数据集成提供对业务方数据库进行抽取监控功能，能够对数据源头的数据资源进行统一清点，并能够在复杂网络情况下对异构的数据源进行数据同步与集成，包括对关系型数据库、NoSQL数据库、大数据数据库、文本存储（FTP）等数据库类型支持，支持离线数据的批量、全量、增量同步，支持分钟、小时、天、周、月来自定义同步时间。

支持多种数据通道

- 元数据信息同步：元数据信息是整个平台数据的基础，数据集成系统可以从各个业务系统完成MySQL、SQLServer、Oracle、MaxCompute等20多种常见数据库的元数据信息的收集，避免对整体数据资产的情况不清楚，帮助数据管理者直接通过元数据进行后续资产的盘点及重点数据的同步。
- 关系型数据库同步服务：支持MySQL、SQLServer、Oracle、PostgreSQL、DB2、云原生分布式数据库PolarDB-X 1.0等关系型数据库的读写操作。
- NoSQL数据库同步服务：支持HBase、MongoDB、Table Store等NoSQL数据库的读写操作。
- MPP数据库同步服务：支持HybridDB for MySQL、HybridDB for PostgreSQL等MPP数据库的读写操作。
- 大数据数据库同步服务：支持MaxCompute、HDFS的读写操作，并支持AnalyticDB的写操作。
- 非结构化存储同步服务：支持OSS、FTP的读写操作。

实时同步

支持实时读取MySQL、Oracle、DB2、SQL Server、OceanBase、Datahub、Loghub、Kafka等数据并写入至MaxCompute、Hologres、Kafka、Datahub中。

数据流入管控

支持各种数据类型的转换，精确识别脏数据，进行过滤、采集、展示，提供可靠的脏数据处理，让用户准确把控数据流入内容，提供作业全链路的流量、数据量、脏数据探测和运行时汇报。

传输速度快

数据集成充分利用单机网卡能力，并使用分布式模型架构，保障数据吞吐量水平扩展，能够提供GB级、TB级的数据流量。

控制友好

数据集成提供精准流控保证，支持通道、记录流、字节流三种流控模式，并提供完备的容错处理，支持线程级别、进程级别、作业级别多层次局部或全局的重跑。

同步插件

支持以插件的方式部署采集工具至数据源端的服务器，完成数据信息的同步采集工作。

跨网络传输

支持各种复杂网络环境下的数据传输。例如，本地跨私网环境、VPC环境等。

数据模型

DataWorks联合建模工具DDM（Datablau Data Modeler）提供一体化的数据建模解决方案（DATABLAU），将数据模型设计管控、引标落标等能力融入DataWorks规范化开发流程，助力用户实现数据资产价值化输出，在数据全生命周期上夯实数据基础，为客户的数据价值化提供有力支撑。

- 模型的可视化设计：提供专业化的本地客户端与在线轻量级的客户端，供用户在不同工作场景下进行可视化建模。
- 协同设计：支持多人同时登录协同进行模型设计。
- 数据标准：管理者可以定义数据标准、代码规范及命名规范。
- 智能引标：提供模型设计人员在构建模型时，引用预先设定好的标准的能力，实现事前落标。
- 正向与逆向DDL：不仅支持将工具中设计好的模型直接下发至引擎，而且支持将引擎中已存在的模型提取至工具中进行再编辑、再下发，告别传统模型工具手工导入、导出的繁琐操作。
- 模型库：支持用户将模型迁入、迁出至模型库统一管理的模式。
- 模型落标监控：支持对已落到引擎中的模型进行基线检查，帮助用户轻松发现表结构与物理模型结构的不一致。

- 与DataWorks开发体系完美结合：支持将模型的发布与DataWorks已有开发流程关联，实现更加规范化的从模型设计到模型发布上线的流程。

数据开发

数据开发为数据使用者提供一站式的集成开发环境，可满足数据资源平台下，数据开发者进行ETL开发、数据挖掘算法开发、数据主题库建设等需求。

当底层数据进行聚合后，数据仍然处于零散的状态，数据是无法直接为上层智能算法和DI应用提供对应数据的，此时需要对数据进行汇聚加工。数据管理和开发人员需要在数据资源平台建立对应的数据中心，进行对应数据的加工。

业务流程设计器

业务流程设计器可以实现将不同类型业务节点组织在一起的开发方式，让用户能以业务流程为中心组织数据开发逻辑。该功能通过各种类型开发节点的容器看板，将相关的工具和管理操作围绕数据看板中的对象来组织，使得开发的管理更加方便和智能化。

业务流程设计器支持ODPS_SQL、ODPS_MR、Shell、机器学习、数据同步、虚拟节点、PyODPS、SQL组件节点之间的组合使用，不仅每个业务流程内的节点可以相互依赖，不同业务流程之间的节点也能跨流程依赖，同时所有节点均能根据业务需要设置个性化调度时间以便适时运行。

- 节点任务：节点任务包含ODPS_SQL、ODPS_MR、Shell、机器学习、数据同步、虚拟节点、PyODPS、SQL组件任务，可以被本业务流程内的节点及其他流程内的节点依赖，并能够被调度系统调度。
- 节点属性：双击节点展开节点任务设计器，可以对节点进行基本业务配置（如对SQL节点编写SQL、对数据集成节点配置数据传输规则），并可以在页面右侧查看或配置节点的调度属性、血缘关系、版本和结构。
- 历史版本：支持查看任意版本的节点代码（仅限ODPS_SQL、ODPS_MR、Shell等节点类型），回滚节点的历史版本。
- 任务发布：提供简单易用的发布功能，在标准模式的项目内，可以发布已测试通过的业务流程至生产环境。

解决方案设计器

用户可以通过项目>解决方案>业务流程的模式进行数据开发工作。通过解决方案设计器将不同类型的业务流程节点组合在一起，站在更高视角横跨多个业务流程做开发。同时，业务流程可以被多个解决方案复用，用户只需要从解决方案视角来考量业务。

代码开发编辑器

代码开发编辑器支持SQL编程、MR编程、Resource资源文件、注册UDF函数和Shell脚本编程。

- SQL编程：提供基于Web端的SQL编程，包括辅助编程（自动SQL提示、格式化、代码高亮等）、代码调试运行等编程功能。
- MR编程：支持将MR编译的JAR包以资源的形式上传并在ODPS_MR节点中引用的形式来使用。
- Resource资源文件：支持上传JAR包、Python程序、自定义参数的Shell脚本、xml配置文件、txt配置文件等资源文件。支持通过资源名称中的后缀识别压缩类型，包括.zip/.tgz/.tar.gz/.tar/.jar等压缩文件类型。
- 注册UDF函数：支持Java UDF和Python UDF两种UDF函数，上传JAR包和Python程序后注册UDF函数，即可使用自定义函数进行数据开发。
- Shell脚本编程：提供在线的Shell脚本编程与调试环境。

代码管理与团队协作

代码管理与协作功能让数据开发可以多人同时进行编辑协作，提高开发效率。

代码管理提供工作流任务和代码的锁机制，保证同一个工作流任务或代码在同一时间内只能被一个用户编辑。用户也可以通过获取锁的方式来得到编辑权限，并实时发送系统提示信息给对应用户。

同时数据开发也提供代码版本管理，每一次提交的节点或工作流任务的版本都会被系统记录保存下来，支持查看任意两个版本的对比。

监控运维

监控运维为数据开发者和维护者提供一站式的数据运维管控能力，用户可以自主管理作业的部署、作业优先级、以及生产监控运维。

DataWorks上数据量庞大、数据类型多样、数据业务复杂，数据处理任务也非常多，数据处理环节和流程周期长，需要支持高并发、多周期、支持多种数据处理环节的统一数据任务调度机制，按照策略进行数据任务调度。

DataWorks提供数据监控运维、任务运行情况监控、异常情况告警、日常运维数据统计等功能。

运维概览

主要用于展示调度任务的指标数据情况，包含任务完成情况、任务运行情况、任务执行时长排行、调度任务数量趋势、近一月出错排行、任务类型分布和30天基线破线次数排行。

任务运维

可视化展示调度任务DAG图，极大地方便用户对线上任务进行运维管理。

- 支持任务运行状态监控告警，支持单任务重跑、多任务重跑、Kill、置成功、暂停等操作。
- 支持两种模式选择：包括列表、DAG模式。
- 可以针对周期运行、测试运行、手动运行任务查看任务运行状态。
- 可以针对任务进行重跑、停止、查看运行日志、查看节点代码、查看节点属性。

智能监控

智能监控是DataWorks任务运行的监控及分析系统。根据监控规则和任务运行情况，智能监控决策是否报警、何时报警、如何报警以及给谁报警。智能监控会自动选择最合理的报警时间、报警方式以及报警对象。

智能监控拥有一整套的监控报警逻辑，用户只需要提供所关注业务的重要任务名称，即可监控整体任务的产出过程，并生成对应的标准统一的报警机制。智能监控还提供轻量级的自助配置监控功能，用户可以根据自己的需求定义报警规则。

引擎运维

DataWork提供一站式的计算引擎资源管理视图，如计算、存储资源使用详情，作业占用资源详情等。使用引擎运维功能，可以查看各个作业的详细信息，及时查找并清理运行有误的作业，避免该类作业阻塞下游任务，影响实例任务的正常运行。

实时分析

实时数据分提供临时查询和个人表两个核心功能，通过MaxCompute取数工具的准实时模式来加快分析速度。

数据地图

数据地图是在元数据基础上提供的企业数据资产管理模块，涵盖全局数据检索、元数据详情查看、数据预览、数据血缘和数据类目管理等功能。数据地图可以帮助用户更好地查找、理解和使用数据。

安全中心

安全中心提供便捷的权限管控功能和可视化的申请、审批流程，用户可以进行权限的审计和管理。

- 权限自助申请：用户可以选择自己需要权限的数据表，在线上快速发起申请，改变原有线下联系管理员的模式，提高工作效率。
- 权限审计及交还：管理员可以快速方便地查看数据库表权限对应人员，进行审计管理，用户也可以主动交还不再需要的权限。
- 权限审批管理：将以前管理员直接授权的模式改为审批授权模式，提供可视化、流程化的管理授权机制，并可以对审批流程进行事后追溯。

数据服务

数据服务提供快速将数据表生成数据API的能力，同时支持将现有的API快速注册到数据服务平台以统一管理和发布。同时，数据服务与API网关产品打通，支持将API服务一键发布至API网关，为用户提供安全稳定、低成本、易上手的数据共享与开放服务。数据服务采用Serverless架构，客户只需关注API本身的查询逻辑，无需关心运行环境等基础设施，数据服务会准备好计算资源，并支持弹性扩展，零运维成本。

数据服务是数据交换的核心组件。数据交换包含数据共享服务和数据开放服务。数据服务为数据交换构建了安全、灵活、可靠的服务总线，可以支撑政务系统内部实现跨部门、跨层级、跨网络的数据共享，也可以支撑政务数据对社会公众开放的政务数据开放服务。

API生成

数据服务支持将关系型数据库、NoSQL数据库（例如OTS）、分析型数据库（例如AnalyticDB）的表通过可视化配置的向导模式快速生成数据API，用户无需具备编码能力，即可在几分钟之内生成好一个数据API，并且立即可以调用。同时为了满足高阶用户的个性化查询需求，数据服务也提供了自定义SQL的脚本模式，允许用户自行编写API的查询SQL，并支持多表关联、复杂查询条件以及聚合函数等能力。

API注册

数据服务也支持注册客户已有的API服务，与通过数据表生成的API统一管理。目前支持Restful风格的API注册，包含GET、POST、PUT和DELETE四类常见请求方式，支持表单、JSON和XML三种数据格式。

API网关

提供API托管服务，涵盖API发布、管理、运维、售卖的全生命周期管理。辅助用户简单、快速、低成本、低风险的实现微服务聚合、前后端分离、系统集成，向合作伙伴、开发者开放功能和数据。数据服务与API网关产品一键打通，在数据服务中配置生成以及注册的API都可以一键发布到API网关，并通过API网关来管理API的授权鉴权、流量控制、计量等服务。

迁移助手

迁移助手可以帮助用户快速复制DataWorks上不同的版本、主账号、地域和工作空间中的开发成果。支持对DataWorks的周期任务、手动任务、资源、函数、数据源、组件、临时查询、表元数据（DDL）、数据服务等开发成果，进行跨集群迁移、跨版本迁移以及自定义迁移。

平台管理

平台管理从系统层面为管理者对参与数据资源平台使用的用户进行对应管控。项目空间作为代码管理、成员管理、角色和权限分配的基本单元，每个团队都可具有独立的项目空间。用户加入项目空间并被分配相关权限后，才可查看或编辑代码。

组织管理

显示组织详情信息以及组织Owner账号、AccessKey和AccessSecret信息，并可以对组织对应人员进行成员管控。

项目管理

支持将项目空间以列表形式进行展示提供创建、配置、激活、禁用项目空间的对应管理功能，方便数据资源层管理员对项目空间进行整体管控。

成员管理

以列表的形式显示本工作空间的成员名称、登录名称、成员角色等信息。

权限管理

用于平台用户、角色、权限等的统一管理。

数据资产管理

数据资产管理有独立的权限点控制，由于数据资产管理属于组织级别的模块，需要在组织管理中添加权限。

业务系统及DataWorks中有大量的数据表、API等各类数据资产，数据管理者通过数据集成工具同步数据、通过数据开发加工数据后，需要对整个平台数据进行统一管控，了解平台的核心数据资产，提供对应数据资产管理规范。

数据保护伞

数据保护伞平台是一款数据安全管理产品，提供数据资产识别、敏感数据发现、数据分类分级、脱敏、访问监控、风险发现预警与审计能力。

规则配置

数据安全管理员可以在配置监控规则，定义敏感数据。

数据发现

数据安全管理员在完成敏感数据规则配置T+1后，即可在识别数据分布中查看数据分布情况，分整体、按等级分布以及字段明细。

数据访问

数据访问包括访问行为和导出行为，数据安全管理员在完成敏感数据规则配置T+1后，即可在数据访问行为、数据导出中查看数据使用情况和用户自MaxCompute将数据导出至外部的情况。

数据脱敏管理

数据脱敏配置页面提供新建、修改、删除和测试脱敏规则的功能，用户可以对每一条数据识别规则，自定义配置相应的脱敏方式，并可以对相应的数据脱敏规则配置不需脱敏的白名单。

分级信息管理

如果规则配置中的分级选择无法满足需求时，用户可以在分级页面管理中进行设置。

手动修正数据

在规则识别的敏感数据不准确的情况下，可以在修正数据页面手动修正，包括删除识别错误数据、更改识别数据类型以及批量处理。

数据风险

提供通过手工进行风险数据识别、风险识别管理（风险规则配置识别、AI识别）产生的风险数据清单，同事可以对风险数据进行审计备注。

风险识别管理

通过配置风险数据的规则，识别日常访问中的风险以及启动AI识别自动识别数据风险。识别后的风险数据统一在数据风险页面进行展示和审计操作，同时也会在数据访问页面的相应数据后打上识别标志

数据审计

数据审计多维度展示风险处理结果和风险分布情况。

数安链

数安链实现数据转移但控制权不转移的功能，极大地解决数据交易及数据共享中的数据安全问题，促进数据共享及数据开放行业的健康发展。

- 提供安全的数据转移过程，保证数据使用方获得的数据，是按照数据属主方的要求进行加密后的数据。
- 基于密文访问控制机制，使每份加密的数据仅能由被授权者使用，避免数据被转卖的风险。
- 基于密文访问控制机制，让数据属主方保有撤销数据授权的能力，授权被撤销后，已转移给数据使用方的加密数据无法再被使用。
- 向数据使用方提供密文使用的组件，对密文的所有计算、查询操作都必须经过该组件，组件输出的计算或查询结果均会按照数据属主方制定的策略进行脱敏后输出。
- 基于数据使用组件，数据使用方会记录被转移数据的所有使用记录，并提供给数据属主方进行数据使用的审计。

- 所有的数据共享、数据申请、审批、使用记录都将在区块链上存证，保证数据源的可追溯并且不可篡改。

数安链产品构建数据共享目录管理、数据审批流程管理、数据共享后的使用权控制、数据共享后的保护策略管理和控制、数据共享后的数据使用审计五大功能，保障数据共享及开放的全流程的数据安全。

14.3.2. 产品价值

DataWorks具有超大规模计算处理能力、异构数据源快速集成能力、多租户权限模型、一站式、智能、易用、完备、便捷、安全等产品优势。

超大规模计算处理能力

DataWorks与底层计算平台集成，能够轻松处理海量数据，

- 万亿级数据JOIN，百万级并发Job，作业I/O可达PB级/天。
- 离线调度支持百万级任务量，实时监控告警。
- 提供功能强大易用的SQL、MR引擎，兼容大部分标准SQL语法。
- 采用三重备份、读写请求鉴权、应用沙箱、系统沙箱等多层次数据存储和访问安全机制保护用户数据，确保不丢失、不泄露、不被窃取。

一站式的数据工场

DataWorks提供可视化的操作界面，支持多人协同作业。

- 提供数据从集成、加工、管理、监控、输出服务的全流程所有功能。
- 提供可视化工作流程设计器功能。
- 多人协同作业机制，分角色进行任务开发、线上调度、运维、数据权限管理等功能，数据及任务无需落地即可完成复杂的操作流程。

海量异构数据源快速集成能力

支持400对异构数据源的离线同步，支持分钟、小时、天、周和月多种调度周期配置。

Web化的软件服务

支持在互联网/内部网络环境下直接使用，无需安装部署，拎包入驻，开箱即用。

多租户权限模型

确保用户数据安全隔离，以租户为单位进行统一的权限管控、数据管理、调度资源管理和成员管理工作。

智能的监控报警

通过设置监控基线，不仅可以从宏观把控整体任务链路的完成时间，也可以从微观对每一个节点任务状态进行全方位监控。

易用的智能SQL编辑器

通过智能代码提示功能、表Meta信息提示功能、代码格式化和折叠功能、预编译功能、炫酷皮肤切换功能来获得全新的SQL代码编辑体验。

完备的数据质量监控体系

支持多种异构数据源、离线数据、实时数据的质量校验、通知、管理。

便捷的数据服务开发接口

API网关服务、交互式数据服务引擎，只需两步操作，即可将已有API和数据以服务的形式发布到数据共享与开放平台。

安全的数据共享机制

提供受保护空间，让详细数据以不可见、不落地的形式共享给其他租户，让数据真正安全地发挥大数据共享价值。

14.3.3. 应用场景

DataWorks广泛应用于云上数仓构建、数据化运营等场景。

云上数仓

支持大型企业在专有云环境使用DataWorks来构建超大型的数据仓库。

- 海量存储：可支持PB、EB级别的数据仓库，存储规模可线性扩展。
- 数据集成：支持多种异构数据源的数据同步和整合，消除数据孤岛。
- 数据开发：基于MaxCompute的大数据开发，支持SQL、MR等编程框架，以及贴近业务场景的白屏化工作流设计器。
- 数据管理：基于统一的元数据服务来提供数据资源管理视图，以及数据权限审批流程。
- 离线调度：可以提供多时间维度的周期性调度能力，支持每天百万级的调度并发，并对任务调度实时监控，对错误及时告警。

数据化运营

- 创新业务：通过数据挖掘建模和实时决策系统，将大数据加工结果直接应用于业务系统。
- 中小企业：基于DataWorks可快速使用和分析数据，助力企业的经营决策。

14.4. 交互式分析Hologres

阿里云交互式分析是一款兼容PostgreSQL生态的实时交互产品，与大数据生态无缝打通，支持对PB级数据进行高并发、低延时的分析处理，轻松而经济地使用现有BI工具对数据进行多维分析透视和业务探索。

Hologres致力于高性能、高可靠、低成本、可扩展的实时计算引擎研发，为用户提供海量数据的实时数据仓库解决方案和亚秒级交互式查询服务，广泛应用在实时数据中台建设、精细化分析、自助式分析等场景。

14.4.1. 产品详情

Hologres是阿里巴巴自主研发的一站式实时数仓引擎，支持海量数据实时写入、实时更新、实时分析，支持标准SQL，支持PB级数据多维分析（OLAP）与即席分析（Ad Hoc），支持高并发低延迟的在线数据服务（Serving），提供企业级离在线一体化全栈数仓解决方案。

多场景查询分析

Hologres支持行存、列存等存储模式和多种索引类型，同时满足简单查询、复杂查询、即席查询等多样化的分析查询需求。Hologres使用大规模并行处理架构，分布式处理SQL，提高资源利用率，实现海量数据极速分析。

- 支持实时数据

  与阿里云实时计算深度合作，支持高并发实时写入与更新，写入速度可达亿级TPS，数据写入即可查。

- 海量数据复杂查询

  全并行计算，实现PB级数据关联分析亚秒级响应。

- 联邦查询

  无缝对接MaxCompute，无需移动数据，直接交互式分析，快速获取查询结果。可以直接单独查询MaxCompute表数据，也可以与实时数据结合进行联合计算。

生态与可扩展性

兼容PostgreSQL生态，与大数据计算引擎及大数据智能研发平台DataWorks无缝打通。无需额外学习，即

可上手开发。

- 兼容PostgreSQL生态

  Hologres兼容PostgreSQL生态，提供JDBC/ODBC接口，轻松对接第三方ETL和BI工具，包括Quick BI、DataV、Tableau、帆软等。

- DataWorks开发集成

  Hologres与DataWorks深度集成，提供图形化、智能化、一站式的数仓搭建和交互式分析服务工具，支持数据资产、数据血缘、数据实时同步、数据服务等企业级能力。

- 达摩院Proxima向量检索

  Hologres与机器学习平台PAI紧密结合，内置达摩院Proxima向量检索插件，支持在线实时特征存储、实时召回、向量检索。

14.4.2. 产品价值

交互式分析Hologres兼容PostgreSQL生态、支持MaxCompute数据直接查询分析，支持实时写入实时查询，实时离线联邦分析，低成本、高时效、快速构筑企业实时数据仓库。

极速响应

PB级数据亚秒级查询响应，满足用户实时多维分析透视和业务探索需求。支持向量化计算及列存储智能索引，性能大幅优于于开源系统。

MaxCompute无缝打通

无缝对接MaxCompute，无需移动数据，直接交互式分析，快速获取查询结果。可以单独查询MaxCompute，也可以与实时数据结合进行联合计算。

高并发实时写入和查询

支持高并发实时数据的实时写入和实时查询，写入速度可达数亿TPS，写入即可查。

统一引擎架构

采用统一的引擎架构，支持行存和列存两种存储模式，同时满足点查询、即席查询及OLAP场景。

简单易用

兼容PostgreSQL生态，与大数据计算引擎及智能云研发平台DataWorks无缝链接。

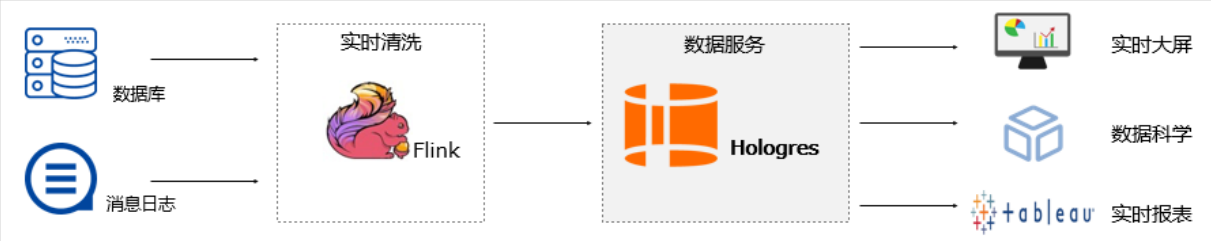
14.4.3. 应用场景

Hologres是一款实时交互引擎，与大数据生态无缝打通，支持海量实时和离线数据的实时分析，并兼容PostgreSQL生态，提供JDBC/ODBC接口，对接第三方BI工具，轻松实现数据的可视化分析。Hologres适用于实时数仓、MaxCompute加速查询和实时离线联邦分析等场景。

实时数仓场景

业务数据实时写入实时计算，并将数据进行ETL处理，再由Hologres实时查询，最终输出到第三方分析工具，实现实时数据的实时分析。

- 数据部门的实时数仓、实时大屏、实时Reporting报表分析。
- 运维和数据应用的实时监控、实时异常检测预警、实时Debug。
- 业务部门的实时风控、实时推荐、实时效果分析、实时训练等。



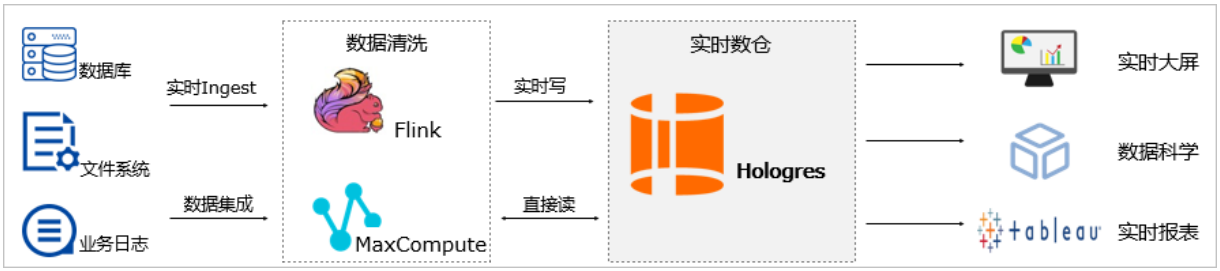
MaxCompute加速查询场景

业务数据写入离线数仓MaxCompute，由Hologres直接加速查询/导入查询，再对接BI分析工具，轻松实现离线数据的实时分析。

- MaxCompute离线数据的实时查询。
- MaxCompute 离线数据报表分析。
- MaxCompute离线数据的在线应用输出（例如RESTful API）。

实时离线联邦分析场景

业务数据按冷热分开存储，冷数据存储在离线数仓MaxCompute，热数据存储在Hologres，通过Hologres实现实时离线数据联邦分析，再对接BI分析工具，快速响应简单查询与复杂多维分析的业务要求。



14.5. 实时计算（Flink）

阿里云实时计算Flink版是一套基于Apache Flink构建的第三代一站式实时大数据分析平台，有效地缩短全链路数据流的时延、实时化计算业务逻辑和平摊计算成本，最终有效满足实时处理大数据的业务需求。实时计算Flink版提供端到端亚秒级实时数据分析能力，并通过标准SQL降低业务开发门槛，助力企业向实时化、智能化大数据计算升级转型。

14.5.1. 产品详情

阿里云实时计算Flink支持的功能特性包括数据采集和存储、数据开发、数据运维和自动性能调优。

数据采集和存储

大数据分析系统的前提是数据需要被采集进入大数据系统。为了最大化运用客户现有的流式存储系统，阿里云实时计算Flink对接了多种上游的流式存储，例如DataHub、LogService、TableStore和MQ等。客户无需进行数据采集、数据集成，即可享受现有的数据流式存储。

数据开发

- 集成SQL辅助功能
  - Flink SQL语法检查

    在修改IDE文本后，单击验证会触发SQL语法检查功能。语法校验出错误后，将在IDE界面提示出错行数、列数以及错误原因。
  - Flink SQL智能提示

    在输入Flink SQL过程中，IDE提供包括关键字、内置函数、SQL智能记忆等提示功能。
  - Flink SQL语法高亮

    针对Flink SQL关键字，提供不同颜色的语法高亮功能，以区分Flink SQL的不同结构。
- 提供DDL辅助生成

  实时计算DDL生成工作大部分均属于比较机械的翻译工作，即将需要映射的数据存储DDL语句人工翻译为实时计算的DDL语句。实时计算提供辅助生成DDL工作，进一步减少手工编写流式作业的复杂度，有效降低人工编写SQL的错误率，并最终提供实时计算业务产出效率。用户可以在开发页面选择模板，即可自动生成DDL语句，选择运行便可生成表结构存储展示在Schema中。
- 支持标准SQL

  支持使用标准SQL进行实时数据清洗、统计汇总、数据分析，支持通用的聚合函数，支持流数据和静态数据关联查询。

数据运维

阿里云实时计算提供作业状态、数据曲线、FailOver、CheckPoints、JobManager、TaskExecutor、血缘关系和属性参数等运维监控功能。

自动性能调优

该功能可以在各个算子和流作业上下游性能达标和稳定的前提下，帮助用户更合理的调整作业并行度和资源配置，全局优化作业性能，解决作业吞吐量不足、全链路存在反压和资源浪费等各种性能调优问题。

14.5.2. 产品价值

相较于其他实时计算产品，阿里云实时计算Flink极具竞争力，客户可以充分利用以下这些优势，解决自身业务实时化大数据分析的问题。

强大的实时处理能力

阿里云实时计算集成多种全链路功能，方便用户进行全链路实时计算开发：

- 强大的实时计算引擎：
  - 阿里云实时计算提供标准的Flink SQL，支持各类失败场景的自动恢复，保证故障情况下数据处理的准确性。
  - 支持多种内建的字符串、时间、统计等类型函数。
  - 精确的计算资源控制，彻底保证作业的隔离性。
- 关键性能指标超越开源Flink达3到4倍，数据计算延迟优化到秒级乃至毫秒级，单个作业吞吐量可达到百万级别，单集群规模达数千台。
- 深度整合各类云数据存储，包括DataHub、日志服务（Log Service）、云数据库RDS版、表格存储（Table Store）、分析型数据库MySQL版等各类数据存储系统，无需额外的数据集成工作，阿里云实时计算Flink可以直接读写上述产品数据。

良好的流式开发体验

- 支持标准的Flink SQL。

  实时计算使用内建的字符串、时间、统计等各类计算函数，将低效且复杂的Flink Java API替换为简单的Flink SQL，让更多的BI与运营人员使用简单的Flink SQL就能完成实时化大数据分析和处理，让实时大数据处理普适化。

当前实时计算对外接口定义为Flink SQL/UDF，提供服务于流式数据分析、统计、处理的一站式开发工具，面向的用户人群更多是数仓开发人员、数据分析师，这类用户不希望更多参与底层代码开发，而希望简单的编写实时计算SQL完成自身流式数据分析业务。

- 提供全流程的流式数据处理方案

  包括数据开发、数据运维、监控告警等不同阶段辅助套件。

- 支持对集群内服务器硬盘故障自动容错处理

  支持硬盘热插拔，故障硬盘的业务恢复时间小于2分钟。

- 平台采用多节点集群架构

  平台内管理节点支持高可用机制，日常运维管理节点故障不影响业务正常运行。

低廉的人力和集群成本

大量优化的SQL执行引擎，会产生比手写原生Storm任务更高效且更廉价的计算任务，无论开发成本还是运行成本，阿里云实时计算均要远低于开源流式框架。使用阿里云实时计算服务，用户可以完全聚焦业务，快速实现市场目标，无需考虑编写复杂业务逻辑下Storm任务Java代码行。因为针对这个任务的调试、测试、调优、上线及后续对于Storm、Zookeeper等开源软件的运维成本，均由阿里云平台承担。

在不影响运行性能的前提下，支持单组件集群中使用的CPU，硬盘、内存、网卡规格不一致，可以最大限度地兼容已有设备。

14.5.3. 应用场景

阿里云实时计算Flink适用于实时ETL&索引构建、实时统计&分析、实时机器学习平台和实时事件处理类等场景。

实时ETL&索引构建

集成实时计算现有的诸多数据通道和SQL灵活的加工能力，对流式数据进行实时清洗、归并和结构化。实时计算是离线数仓有效的补充和优化，数据实时传输的计算通道。

实时统计&分析

实时化采集和加工流式数据源，实时监控和展现各类指标，让数据化运营实时化。例如：

- 实时的网络点击PV、UV统计。
- 统计某交通卡口平均5分钟通过车流量。
- 水利大坝的压力数据统计和展现。

实时机器学习平台

帮助数据分析和应用开发人员能够从数据处理、特征工程、模型训练、预测，端到端地完成整个流程。

实时事件处理类

对系统和用户行为、业务和系统进行实时地检测和分析，发现危险行为。例如：

- 交易大屏、用户大屏等一系列用户行为大屏展示。
- 全站交易时段曲线图，可以协助运营或者技术人员了解当前时间点全站交易情况。如果交易出现不正常波动（如突然下跌），应该立刻触发报警机制以方便相关人员介入排查问题，以减少交易波动对于公司业务的影响。
- 针对双十一、618等大促活动的实时监控。运营人员需要实时获取到各类指标信息，用以迅速决定是否需要更换大促运营方案。
- 针对网络支付涉及金融盗窃固定行为，设置规则告警。

14.6. 机器学习PAI

机器学习PAI（Platform of Artificial Intelligence）是阿里云人工智能平台，是一套基于分布式计算引擎MaxCompute（原ODPS）的数据挖掘、建模、预测的工具，提供一站式的机器学习解决方案。机器学习PAI分为有监督学习、无监督学习和增强学习，通过机器学习PAI，对大量的历史数据进行学习从而生成经验模型，利用经验模型指导业务，主要在营销类、金融类、SNS关系挖掘、文本分类场景等方面发挥作用。

14.6.1. 产品详情

机器学习PAI提供一站式解决方案，客户只需要准备好训练数据，通过机器学习PAI提供的服务即可实现一站式机器学习。

可视化建模

机器学习PAI提供了可视化建模的能力，操作简单并且可以清晰地梳理流程逻辑。可视化建模包含丰富的算法组件，封装好了适用于商品推荐、文本分析、金融风控、天气预测等场景的一系列实验模板。通过提供基本的组件，客户可以直接将数据导入平台，通过算法组件灵活地拼装实验流程，搭建各个垂直场景下的解决方案，解决自身的业务场景，节省了很多切换环境的损耗。对于每个输出型组件，都可以通过右键组件来查看可视化输出模型，一目了然。

交互式建模（DSW）

除了可视化建模外，机器学习PAI也为客户提供了Notebook建模和在线IDE的方式，可以使用原生代码进行更加定制化的模型构建。客户可以在实例列表中选择自己喜欢的编程环境，进行模型的构建与训练。DSW支持：

- 实例随时停止和启动、镜像一键保存、开发环境恢复及VPC访问。
- 提供集成式AI开发环境。
- 预装常用大数据开发包和算法包，且开放Sudo权限，从而允许安装第三方库。
- 提供官方镜像，可以覆盖多版本主流计算框架。例如TensorFlow及PyTorch。
- 嵌入WebIDE，可以安装任意插件。

云原生深度学习训练（DLC）

DLC（Deep Learning Containers）是基于阿里巴巴容器服务ACK（Alibaba Cloud Container Service for Kubernetes）的深度学习训练平台，为客户提供灵活、稳定、易用和最佳性能的深度学习训练环境。

DLC支持任务生命周期管理、多机多卡分布式任务及自定义镜像。通过DLC，算法科学家们可以方便快速地提交深度学习任务、监控任务进度，并便捷地查看结果，从而有效降低算法开发人员在离线任务上的工程成本，提升建模训练效率。

模型在线服务（EAS）

EAS支持客户将机器学习模型（PMML、PAI-OfflineModel、Tensorflow和Caffe等）一键部署成服务，同时也支持客户根据EAS制定的接口规范开发自定义的在线服务。部署服务时，仅需通过一个JSON文件描述服务相关的信息（模型位置、服务区域、使用的资源等），即可通过客户端工具eascmd或Java SDK将模型一键部署成在线服务，并同时提供生产网和公网的访问。此外，EAS在不同地域提供服务，支持异构硬件（CPU和GPU）。

14.6.2. 产品价值

机器学习PAI平台具有一站式可视化体验、优质和丰富的机器学习算法、与阿里产品完美配合、优质的技术保障等优势。

一站式可视化体验

- Web界面，客户可通过拖、拉、拽的方式，搭积木般即可完成整个数据挖掘过程，不需要进行编程。
- 提供了数据模型的可视化功能，数据分析、算法评估都可以通过直观的图表一览无余。
- 从数据处理、模型训练、预测、评估到模型部署、服务化、定时调度等，都可一站式完成。
- 除了web界面，阿里云机器学习PAI也提供了命令行工具，客户可以方便地将算法嵌入到自身的工程中。

优质、丰富的机器学习算法

- 机器学习算法种类丰富，机器学习PAI平台提供了数据预处理、聚类、回归、文本分析、特征处理等近百种机器学习算法，适用于不同的业务场景。
- 集成业界较新较优的算法，与传统软件相比，大大提升了计算能力和精准度。
- 支持深度学习，提供GPU作业调度能力，机器学习PAI平台集成并深度优化了业界最受关注的Tensorflow框架，客户可以轻松掌握Tensorflow的使用并体验到更快速的训练速度。
- 在兼容开源的基础上，机器学习PAI平台的各类算法都汇聚了阿里云大数据挖掘和应用的经验沉淀，可以显著缩短数据建模、部署和应用的周期。

与阿里产品完美配合

- 阿里云已经建立了包括机器学习PAI平台在内的丰富的大数据生态。
- 机器学习PAI平台依托于MaxCompute计算平台，并与数加DataWorks平台进行了深度整合，合力帮客户解决数据挖掘以及其上下游的数据采集、实验调度、数据应用等一系列问题。
- 基于MPI、PS、图算法、MapReduce等计算框架，全分布式算法，让客户轻松处理海量数据。

14.6.3. 应用场景

机器学习PAI主要在营销类、金融类、文本类、非结构化数据处理及其他各类预测场景中得到广泛应用。

营销类场景

- 具体场景：商品推荐、用户群体画像、广告精准投放。
- 实例：通过用户的购物行为数据，使用机器学习平台获取商品的关联关系，对用户之后的购买形成推荐，并评估结果。

金融类场景

- 具体场景：贷款发放预测、金融风险控制、股票走势预测、黄金价格预测。
- 实例一：农业贷款发放问题是一个典型的数据挖掘问题。贷款发放人通过往年的数据，包括贷款人的年收入、种植的作物种类、历史借贷信息等特征，使用机器学习构建经验模型，通过这个模型来预测受贷人的还款能力。
- 实例二：基于用户的信用卡消费记录，使用机器学习算法，将原始数据通过分箱后进行特征工程变换，继而应用于线性模型进行建模。再通过评分卡预测得到每个用户的最终信用评分，这个评分可以应用到各种贷款或者金融相关的征信领域中。

文本类场景

- 具体场景：新闻分类、关键词提取、文章摘要、文本内容分析。
- 实例：使用机器学习平台的文本分析功能，实现简单的商品标签自动归类系统。

  以网购为例，一般一件商品会通过多维度的标签来展示。例如，一双鞋的商品描述可能是“韩都少女英伦风系带马丁靴女磨砂真皮厚底休闲短靴”，一款包的商品描述可能是“天天特价包包2016新款秋冬斜挎包韩版手提包流苏贝壳包女包单肩包”。

  每个产品的描述都包含非常多的维度，可能是时间、产地、款式等，如何按照特定的维度将数以万计的产品进行归类，往往是电商平台最头痛的问题。其中最大的挑战是如何判断每种商品的维度由哪些标签组成。如果可以通过机器学习算法自动学习标签词语，例如“日本”、“福建”、“韩国”等与地点相关的标签，那么就可以快速地构建标签归类体系。

非结构化数据处理场景

- 具体场景：图片分类、图片文本内容提取OCR。
- 实例：使用Tensorflow深度学习框架，快速搭建了图像识别的预测模型。整个流程只需要半小时，就可以实现对图片的识别，系统会返回图片的分类结果。这种使用深度学习实现图片识别的案例也可以用在图片鉴黄、人脸识别、物体检测等各个领域。

其他各类预测场景

- 具体场景：降雨预测、足球比赛结果预测、微博粉丝领袖分析、社交关系链分析。
- 实例：根据历年的空气指标数据，例如PM2.5指标、一氧化碳的指标、二氧化氮的指标等，使用机器学习平台预测雾霾天气。并根据预测结果来分析哪种空气指标对于PM2.5影响最大。

14.7. 数据总线DataHub

阿里云数据总线（DataHub）是流式数据（Streaming Data）的处理平台，提供对流式数据的发布（Publish）、订阅（Subscribe）及分发功能，让用户可以轻松构建基于流式数据的分析和应用。

DataHub与阿里云实时计算引擎Realtime Compute无缝连接，用户可以轻松使用SQL进行流数据分析。

14.7.1. 产品详情

DataHub服务可以对各种移动设备、应用软件、网站服务、传感器等产生的大量流式数据进行持续不断的采集、存储和处理。用户可以编写应用程序或者使用流计算引擎来处理写入到DataHub的流式数据（例如实时web访问日志、应用日志、各种事件等），并且能够产出各种实时的数据处理结果（例如实时图表、报警信息、实时统计等）。

数据队列

支持单shard内数据保序；单topic的性能以shard数为单位水平扩展。

点位存储

支持消费应用将消费点位保存到DataHub服务，保证消费应用在Failover后可以从保存的点位进行消费。

数据同步

DataHub中的数据支持自动同步到阿里云其它服务。DataConnector是将DataHub服务中的流式数据同步到其他云产品中的功能，目前支持将Topic中的数据实时/准实时同步到MaxCompute、OSS、ElasticSearch、RDS、AnalyticDB、TableStore中。

用户只需要向DataHub中写入一次数据，并在DataHub服务中配置好同步功能，即可以在各个云产品中使用这份数据。数据同步支持at least once语义，在网络服务异常等小概率场景下可能会导致目的端的数据产生重复。

扩容缩容

Datahub具有服务弹性伸缩功能，用户可根据实时的流量调整Shard数量，来应对突发性的流量增长或达到节约资源的目的。

例如，在双11大促期间，大部分Topic数据流量会激增，平时的Shard数量可能完全无法满足这样的流量增长。此时可以对其中一些Shard进行SplitShard扩容操作，最大可扩容至256个Shard，按目前的流控限制足以达到256MB/s的流量，用以应对数据流量的激增；而在双11大促后，数据流量下降，多余的Shard会占用没有必要的quota，此时可以进行MergeShard缩容操作，每两个Shard合并为一个，直至合适为止。

14.7.2. 产品价值

DataHub服务基于阿里云自研的飞天操作平台，具有高可用、低延迟、高可扩展、高吞吐的特点。

高吞吐

单主题（Topic）最高支持每日TB级别的数据量写入；每个分片（Shard）最高支持每日8000万Record级别的数据量写入。

实时性

通过DataHub ，用户可以实时的收集通过各种方式生成的数据并进行实时的处理，对用户的业务产生快速的响应。

易用性

- DataHub提供丰富的SDK包，包括C++、Java、Pyhon、Ruby、Go等语言。
- DataHub服务也提供Restful API规范，用户可以使用自己的方式实现接口访问。
- 除了SDK以外，DataHub还提供一些常用的客户端插件，包括Fluentd、LogStash、Oracle GoldenGate等，用户可以使用这些客户端工具向DataHub中写入流式数据。
- DataHub同时支持强Schema的结构化数据和无类型的非结构化数据，用户可以自由选择。

高可用

- 规模自动扩展，不影响对外服务。
- 数据自动多重冗余备份。

动态伸缩

每个主题（Topic）的数据流吞吐能力可以动态扩展和减少，最高可达到每主题256000 Records/s的吞吐量。

高安全性

- 提供企业级多层次安全防护，多用户资源隔离机制。
- 提供多种鉴权和授权机制及白名单、主子账号功能。

14.7.3. 应用场景

DataHub作为一个流式数据处理服务平台，结合阿里云众多云产品，可以构建一站式的数据处理服务。

数据上云入口

DataHub做为数据上云的入口，可以简化用户将数据上传到阿里云的接口，让用户做到一次写入多处使用，无需对接多种云服务的接口。

数据采集通道

DataHub提供丰富的采集端插件，支持多种业务数据的采集，让用户可以方便的将现有的业务数据采集到DataHub，在云端进行更多的处理和使用。目前DataHub支持的采集端包括日志采集（Logstash/Fluntd）、数据库binlog采集（DTS/Oracle GoldenGate）、视频采集（GB28181协议的监控/安防视频）。

流处理应用

用户可以编写应用订阅DataHub中的数据，并进行实时的加工，并且将加工后的结果输出。

用户还可以将应用计算产生的结果输出到DataHub中，并使用另外一个应用来处理上一个应用生成的流式数据，来构建数据处理流程的DAG。

流式数据归档

用户的流式数据可以归档到MaxCompute中，通过创建DataHub Connector，指定相关配置，即可创建将Datahub中流式数据定期归档的同步任务。

14.8. 智能数据构建与管理Dataphin

智能数据构建与管理Dataphin是智能的大数据平台建设引擎，旨在面向各行各业大数据建设、管理及应用诉求，集产品、技术、方法论于一体，一站式为您提供集数据引入、规范定义、数据建模研发、数据资产管理、数据服务等的全链路智能数据构建及管理服务。

Dataphin致力于屏蔽不同计算与存储环境差异，帮助您快速引入数据、标准规范化构建数据、通过建模化方式自动开发数据、萃取以实体对象为中心的标签数据体系、沉淀业务数据知识与数据资产、治理数据问题。同时还支持数据表查询、智能语音查询等多种类型数据服务。

14.8.1. 产品详情

智能数据构建与管理Dataphin提供数据引入、规范定义、数据建模研发、数据萃取、数据资产管理、数据服务等全链路智能数据构建及管理服务。

平台管理

支持对整个产品系统全局化功能设置，帮助学习使用产品功能、快速开始工作，以及进行必要的系统管理与控制、保障各模块正常运转。

全局设计

支持从业务全局出发，拆解并设计对应的业务数据总线，从顶层进行数据中心的命名空间划分、主题域及相关名词定义、管理单元（即项目）划分、数据源定义。

数据引入

基于全局设计定义的项目空间与物理数据源，支持将各业务系统、各类型的数据抽取加载至数据库，完成数据的同步与集成，并通过各种清洗策略等，完成基础数据中心的建设。

规范定义

基于全局设计定义的业务总线、数据引入构建的基础数据中心，支持根据业务数据需求，结构化地定义、组件化地构建标签与统计指标等，以保证业务数据无二义性地标准化、规范化生产。

建模研发

基于规范定义的数据元素，支持可视化地设计与构建数据模型，提交发布后由系统智能自动化地生成代码与调度任务，完成公共数据中心的全托管生产。

编码研发

基于通用的代码编辑界面，支持自由灵活地进行个性化的数据编码研发，并完成对应任务发布。

资源及函数管理

支持各种资源包（如JAR、文档文件）管理以满足部分数据处理需求，支持原生的系统函数查找与使用，支持自定义函数以满足数据研发特殊的函数加工需求。

数据萃取

在基础数据中心及公共数据中心基础上，支持以**目标对象**为中心，用参数选配的方式可视化地识别与连接业务中的对象ID，并提取对象行为与标签，智能地完成数据打通与深度挖掘，并生成代码与调度任务，完成萃取数据中心的全托管生产。

调度运维

支持基于策略对建模研发、编码研发、数据萃取生成的代码任务进行调度与运维管控，包括数据生产任务部署、任务运行及依赖情况查看以及管理维护，以确保所有任务正确有序地生产数据。

元数据中心

支持采集、解析、管理基础数据中心、公共数据中心、萃取数据中心的元数据。

资产分析

在元数据中心基础上，支持元数据深度分析并实现资产化管理数据，以可视化地呈现资产分布、元数据详情等，以便查找及深度了解数据资产。

安全管理

支持从质量管理、安全管理等角度进行标准定义、分析呈现、流程管理、监控报警、从数据源到数据应用端的全链路追踪等，发现资产优化空间并提供治理建议。

即席查询

支持自定义SQL等方式查询数据资产中的数据，并通过查询分析引擎快速实现物理表及面向主题的逻辑表（也即数据模型，或逻辑模型）数据查询及结果获取。

14.8.2. 产品价值

智能数据构建与管理Dataphin提供全链路、一站式、智能化的数据构建与管理工具，降低数据建设门槛，且通过数据资产全链路分析追踪与优化，降低数据生产及消费成本。

数据规范统一

采用维度事实建模理论，对维度、维度属性、业务过程、指标字段等进行严格的标准化、规范化定义，保障数据质量，避免数据指标定义的二义性。

高效且自动化的编码

基于函数化理念，对通用数据计算逻辑组件化定义并可自由组建统计指标，从而自助地实现建模研发、系统自动生成代码执行生产数据。

智能计算优化

支持从业务视角进行逻辑建模。逻辑模型发布后，系统自动化进行物理建模、编码，从而降低对开发人员的技术能力依赖。

一站式研发体验

数据引入、建模、研发、运维、数据查找及探查等过程一站式研发，链路统一高效。

系统化构建数据目录

基于规范化建模、高效自动化的元数据抽取，以标准的技术框架系统构建规范可读的业务化数据目录，形成数据资产地图，方便业务查找及应用。

高效数据检索

基于元数据及数据构建数据图谱，实现数据表及数据，简单且快速的智能检索。

可视化数据资产

系统化构建业务数据资产大图，数据视角还原业务系统、提取业务数据知识，并可快速提炼业务关键环节及数据。

数据使用简单可依赖

定义即服务，研发构建的业务主题式数据逻辑表可被直接、快速地查询和访问，可简化约80%的查询代码。

提升效率

提供全链路、一站式、智能化的数据构建与管理工具，降低数据建设门槛，不同背景的开发人员可自助ETL并快速完成数据需求。其中贯穿的OneData、OneEntity、OneService思想与方法论（已申请专利）可完成模型&指标抽象与自助定义、代码自动化生产、主题数据自动聚合并输出服务。

降低成本

以元数据为基础、算法智能为驱动，实现物理和逻辑分层的智能自动化生产、数据资产全链路分析追踪与优化，优化计算及存储资源分配，从而降低数据生产及消费成本。

14.8.3. 应用场景

智能构建与管理Dataphin典型应用场景包括智能构建云上数仓、输出主题式数据服务等。

智能构建云上数仓，提高战略决策效率

某集团在全国经营多家连锁超市，线上线下零售渠道及形态众多，通过Dataphin智能构建云上数仓，提供战略决策效率。

- 数据融合：通过数据引入功能，将业务系统数据集成、融合一体，统一基础数据。
- 数据建模：通过规范建模功能，结合业务发展需求，自顶向下设计标准的数据模型，统一公共数据。
- 数据生产：基于建模后系统代码自动化托管生产功能，快速响应业务需求。模型设计输出后，自动化生成代码、周期性调度产出任务。

输出主题式数据服务，提高数据化运营效率

某公司是一家大型跨省直营餐饮品牌公司，具有线上线下多个客户触达渠道，以爆款思维策划公司品牌，可通过Dataphin输出主题式数据服务，提高数据化运营效率。

- 数据融合：通过数据引入功能，将各渠道数据沉淀至数据仓库内，丰富基础数据。
- 数据建模：通过数据建模及代码自动化生成功能，以会员为中心，构建完整的会员数据模型，集成会员属性、统计指标等数据。
- 主题服务：通过数仓即席查询功能，面向应用，自动输出会员主题的汇总数据模型，高效完成会员日报分析、门户搭建等。

14.9. Quick BI

Quick BI是一个基于云计算的灵活的轻量级的自助BI工具服务平台。

Quick BI秉承**全场景消费数据，让业务决策触手可及**的使命，通过智能的数据分析和可视化能力帮助企业构建数据分析系统，用户可以使用Quick BI制作漂亮的仪表板、格式复杂的电子表格、有分析思路的数据门户。也可以通过Quick BI提供智能化的数据建模工具，极大地降低数据的获取成本和使用门槛；通过拖拽式的操作和丰富的可视化图表控件，帮助用户轻松自如地完成数据透视分析、自助取数、业务数据探查、报表制作和搭建数据门户等工作。

Quick BI不止是业务人员查看数据的工具，更能让每个人都成为数据分析师，帮助企业实现数据化运营。

14.9.1. 产品详情

Quick BI提供丰富的数据源接入，内置高速数据云计算引擎，亿级数据可实现秒级计算和响应；提供丰富的可视化组件、灵活智能的分析能力和电子表格，推出数据门户、自助取数和数据填报等数据分享体系，降低数据使用门槛；提供组织及权限、数据行列权限等，精细化数据权限管控。

数据源

负责适配各种云数据源，包括MaxCompute、HybirdDB for MySQL、AnalyticDB for PostgreSQL、AnalyticDB等，封装数据源的元数据或者数据的标准查询接口。

数据建模

负责数据源的OLAP建模过程，将数据源转化为多维分析模型，支持维度（包括日期型维度、地理位置型维度）、度量、星型拓扑模型等标准语义，并支持计算字段功能，允许用户使用当前数据源的SQL语法对维度和度量进行二次加工。

数据分析

- **仪表板**

负责将可视化图表控件组装为仪表板。支持线图、饼图、柱状图、漏斗图、树图、气泡地图、色彩地图、指标看板等多种图表，支持查询条件、TAB、内嵌页面、图片和文本框5种基本控件，支持图表间数据联动效果。

- **电子表格**

  负责在线电子表格（Workbook）的相关操作功能，涵盖行列筛选、普通或高级过滤、分类汇总、自动求和、条件格式等数据分析功能，并支持数据导出，以及文本处理、表格处理等功能。

- **即席分析**
  面向一线业务人员，以表格形式提供拖拽式的表格分析能力，让懂业务的人自助实现数据分析。

> **说明** 在专有云环境下即席分析属于增值模块，需要额外购买，您可根据业务需求按需购买。

数据应用

- **数据门户**

  负责将仪表板组装为数据门户，支持内嵌链接（仪表板）和外嵌链接（第三方URL），支持模板和菜单栏的基本设置。

- **自助取数**

  负责下载报表的数据，可将数据下载到本地或者服务器上后再进行进一步的数据加工或分析。IT支撑人员可以基于Quick BI的数据集进行指标定义，其他业务人员基于自助取数功能进行拖拽式取数，可以减少IT人员后台数据抽取及数据加工过程从而提升临时取数支撑效率。

> **说明** 在专有云环境下自助取数属于增值模块，需要额外购买，并且需要额外的机器资源。您可根据业务需求按需购买。

- **数据填报**

  负责在线数据收集，助力企业一站式完成数据收集上报，提供丰富的表单组件、批量上传能力、数据管理和审核、灵活的拖拽式布局和安全的数据权限管控体系。例如，仓库进销管理，可以通过数据填报录入每一单进销信息，以便仓库货品盘点和追溯历史进销记录等。

> **说明** 在专有云环境下数据填报属于增值模块，需要额外购买，您可根据业务需求按需购买。

组织及权限管控

- **组织权限管理**

  负责组织管理和工作空间管理的两级权限架构体系管控，以及工作空间下的用户角色体系管控，实现基本的权限管理，实现对同一份报表，不同的人可以看不同的内容。

- **行级权限管理**

  负责数据的行级粒度权限管控，实现对同一张报表，不同的人可以查看不同的数据。

- **分享和公开**

  支持将电子表格、仪表板、数据门户分享给其他的用户，支持将仪表板公开到互联网供非登录用户查看。

14.9.2. 产品价值

Quick BI帮助客户轻松自如地完成数据分析、业务数据探查、报表制作等工作，帮助企业构建自上而下的决策分析体系，让企业的数据资产快速的流动起来，通过BI和AI结合挖掘数据背后的价值，加深并加速在企业内部各种场景的数据消费。

IT部门价值

- 融合数据
- 建设平台

- 统一口径
- 减少重复工作
- 缩短响应时间
- 聚焦底层数据建模

业务部门价值

- 业务灵活自助分析
- 更多时间洞察业务问题
- 快速迭代响应业务变化
- 搭建商业分析体系
- 数据支撑业务快速运转

企业管理价值

- 掌握企业经营状态
- 及时调整战略执行
- 赋能企业效率升级
- 塑造核心竞争力
- 挖掘持续增长可能性

14.9.3. 应用场景

在中国和海外拥有众多Quick BI用户，丰富的功能特性满足了用户不同的场景需求。

人人都是数据分析师

自助分析对标IBM cognos，支持亿级数据的低门槛拖拽式探索分析，让业务实现任意行列级别的合并与拆分实现组装式分析，提供极大的自助灵活性；应用于不确定性问题的探索分析，会议讨论时的灵活统计分析，快速多变业务场景的报表快速制作与变更。

构建商业分析体系&数据产品化

通过丰富的可视化组建、门户功能、交互能力等，制作数据产品，让分析体系化、自动化、产品化。

从人找数据到数据找人

快速构建企业数据分析体系，对接丰富数据源、构建分析模型、仪表板，通过数据门户分享至业务端。

14.10. DataV数据可视化

DataV数据可视化平台旨在让更多的人看到数据可视化的魅力，帮助非专业的工程师通过图形化的界面轻松搭建专业水准的可视化应用，满足会议展览、业务监控、风险预警、地理信息分析等多种业务的展示需求。此外，DataV提供高性能三维渲染组件DataV.GL、天猫双11大屏同款可视化工具等将三维渲染能力，引入地理场景。借助GPU算力实现海量数据渲染，提供低成本、可复用的三维可视化方案，适用于智慧城市、智慧交通、安全监控、商业智能等场景。

14.10.1. 产品详情

DataV数据可视化平台是大屏应用的开发工具和运行环境，平台提供多种布局、组件，能够在模板的基础上通过配置的方式实现可视化前端应用，并能够和各类常见数据库连接，实现多种数据可视化展示场景的需求。

连接数据源

数据可视化平台目前支持接入数据库类、文件类、API类和数据代理等数据源。

- 数据库类：支持RDS for MySQL、RDS for PostgreSQL、RDS for SQLServer、TableStore、兼容MySQL数据库等。
- 文件类：支持CSV文件和静态JSON。
- API类：支持POP API、阿里云API网关和自定义HTTP API。
- 数据代理：提供开源数据库代理服务，支持在ECS上进行部署。通过数据代理服务，可降低数据库暴露IP带来的风险。

创建可视化应用

创建可视化应用时，可以选择直接使用模版创建，也可以使用空白画布从零开始设计。

设计可视化应用

可视化模版

数据可视化的设计难点在于，如何能在简单的一页之内读懂数据之间的层次与关联，这就关系到色彩、布局、图表的综合运用。DataV提供多种精美的模板，对应指挥中心、地理分析、实时监控、汇报展示等多种场景常见设计，直接套用使可视化作品显现出高设计水准。

组件种类

DataV数据可视化平台在常规组件上再进行了设计，优化过的条、饼、柱、线等传统图在视觉呈现上更加新颖、多样，相比一般的图表更适合在大屏幕上呈现。组件包括常规图表、地图、指标、关系网络、文字以及其他更多第三方组件，还能绘制出包括海量数据的地理轨迹、地理飞线、热力分布、地域区块、3D地图、3D地球，以及地理数据的多层叠加、拓扑关系、树图等异形图表组件，此外还提供ECharts和AntV-G2等第三方开源图表库。

组件设置

任何一个组件都可设置其配置、数据和交互。配置设置因组件不同有差异化，可设置全局样式、图表位置等外观上的显示；数据默认使用静态数据，可设置数据源和具体数值；交互数值即参数变量，可以用于控制组件之间参数的传递，从而达到组件之间数据交互的目的。

组件异常提示

在缺少数据、数据连接失败、数据获取错误等情况下会发生数据异常，此时在数据设置页面会出现提示，该组件不能正常工作。

编辑可视化应用

编辑可视化应用，支持快速修改可视化应用的内容和配置。

复制可视化应用

支持复制可视化应用，复制后，会生成一个名为“xxx_副本”的应用（复制功能只会将应用复制给自己）。复制的应用继承原应用的配置和数据，可稍作修改，生成一个符合要求的大屏。

删除可视化应用

支持整体删除可视化应用，删除后应用不可恢复。

拷贝可视化应用

拷贝功能是指将“xxx”应用，通过用户识别码拷贝给其他用户，实现大屏协作与共享（拷贝功能是将应用拷贝给其他用户，区别于复制可视化应用）。

重命名可视化应用

支持修改可视化应用的名称，名称允许重复。

预览可视化应用

应用创建完成后，使用预览功能可预览应用，展示动态效果。

发布可视化应用

可视化应用发布功能提供公开分享、密码访问、TOKEN验证免登和IP白名单访问分享四种方式。

- 公开分享：通过URL链接，即可访问大屏应用。
- 密码访问：可设置大屏访问密码，通过URL访问大屏时，需要输入密码。
- TOKEN验证免登：需要进行TOKEN验证，通常用来实现权限体系集成。
- IP白名单访问分享：设置启用IP白名单后，发布后的可视化应用仅允许在设置范围内的白名单IP下访问。

14.10.2. 产品价值

相比于传统图表与数据仪表盘，如今的数据可视化致力于用更生动、友好的形式，即时呈现隐藏在瞬息万变且庞杂数据背后的业务洞察。无论在零售、物流、电力、水利、环保、还是交通领域，通过交互式实时数据可视化大屏来帮助业务人员发现并诊断业务问题，越来越成为大数据解决方案中不可或缺的一环。

“一站式”开箱即用数据可视化解决方案

DataV数据可视化平台致力于提供“一站式”开箱即用数据可视化解决方案，帮助非专业的数据工程师通过图形化的界面轻松搭建专业水准的可视化应用。

专业级大数据可视化

专精于地理信息与业务数据融合的可视化，提供丰富的行业模版和图表组件，处理与展示百万级的复杂数据。

图形化编辑界面

拖拉拽的图形化配置方式，通过简单拖拽即可完成样式和数据配置，无需编程就能轻松搭建大屏。

智能主题配色

数据可视化可以通过智能主题功能，无需专业的大屏设计师，也能对大屏进行合理的配色，快速解决在设计大屏时遇到的配色困难的问题。

一键美化样式

数据可视化可以通过一键美化功能，快速调整可视化应用的布局，并通过内置样式丰富可视化应用的内容，快速解决在设计可视化应用时遇到的整体样式配置困难的问题。

工具箱滤镜功能

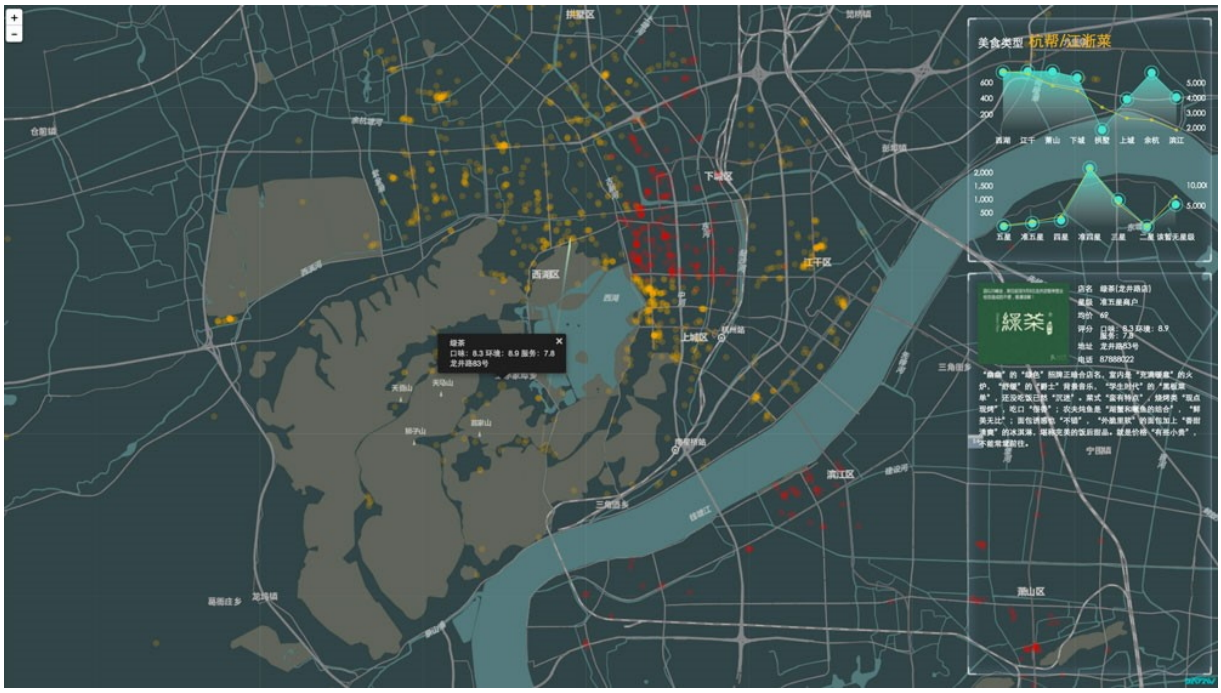
DataV工具箱提供滤镜配置的功能。通过滤镜配置，可以对大屏中组件的色相、饱和度、亮度、对比度以及透明度等颜色属性进行配置。

14.10.3. 应用场景

DataV数据可视化借助GPU算力实现海量数据渲染，提供低成本、可复用的三维可视化方案，适用于智慧城市、智慧交通、安全监控、商业智能等场景。

智慧城市-美食大屏

DataV数据可视化平台创建美食大屏，通过美食大屏可以直接观察到菜系的分布。



汇报展示-业绩大屏

经营状况实时数据可以通过大屏直接动态展示，可实时监控当日交易支付金额，成交会员分析、热销商品排行等品牌全域核心数据。

14.11. 数据资源平台

阿里云数据资源平台是数据资产定义、加工、管理、服务的全流程平台，提供数据同步、数据查询、数据标准、数据建模、数据加工、质量评估、标签构建、业务模型构建、资产管理、数据服务、画像分析等功能，为智能数据应用持续稳定供给全量、标准、干净、智能的数据资源。

依托数据资源平台，可设计高质量的标准化数据模型，减少重复开发工作，用户可全面了解数据质量、数据使用情况和系统运行情况，并从业务视角更直观的使用并探索数据，更高效地从数据中获取业务价值。

14.11.1. 产品详情

数据资源平台需覆盖数据同步、数据标准建模及数据质量检查、数据开发、数据标签体系构建，基于标签数据的群体分析、专家业务模型构建、全流程任务监控告警、数据服务化、数据资产管理等核心能力，提供标准化程度高、易用性强的一站式大数据管理平台。

研发工作台

- **数据同步**：数据同步可实现离线、实时多源异构数据的便捷同步或接入，系统可提供完善的数据接入配置、 数据模板配置、数据同步任务运行监控等功能，有效保障数据接入的稳定性和可控性，满足各类平台、数据源及应用系统间的数据汇聚需求。
- **数据探查**：提供对云计算资源中物理表的探查，快速了解物理表详情及分布情况。支持面向多种云计算资源中的表及字段进行预览和表数据自动探查，提供表级别、字段级别探查结果图表化展示。
- **空间数管**：空间数据管理支持单文件、多文件、数据库等多种形态，矢量、栅格、瓦片、倾斜摄影等多种类型，不同格式的多源异构空间数据的接入和管理；支持本地上传、从OSS导入等多种方式添加数据；添加数据的同时支持各类型空间数据的元信息自动解析，支持按空间对平台所有空间数据进行统一检索、统计和管理。
- **数据标准**：提供逻辑表标准、字段标准（数据元、指标、维度、数据字典等）管理能力。帮助用户通过设计标准数据元素，定义关键业务对象、业务对象属性及值域定义，并规范标准数据字典，制定并管理平台遵循的统一数据标准，帮助平台管理者和数据管理者管控治理后数据的一致性和数据质量。
- **数据建模**：帮助用户在数据标准的约束下构建数据模型，将数据标准贯彻到数据质量分析、保障及检查的全过程中，将散乱的多源异构数据加工成标准、干净的数据资产，确保数据的完整性、一致性、准确性、可用性，通过客观量化评估指标帮助客户了解数据治理工作进程，指引数据治理工作的螺旋式上升过程。为了完成在云上积累可运营数据资源的目标，提供数据充分融合、数据高质量可用的必要保障。
- **数据开发**：支持对计算节点中的脚本、自定义函数、节点输入、节点输出、参数等进行配置和管理，同时提供数据加工、算法服务任务流程开发、编排与调试、上线、部署、维护等功能。支持流式计算、批量离线计算等类型的计算节点在一个工作流中统一编排，通过可视化操作界面，通过拖拉拽的方式连接计算节点迅速实现数据加工流程编辑。支持通过空间算子编辑器零代码实现对空间数据的处理，包括地址空间化（依赖达摩院地址标准化产品）、坐标转换、矢量分析和计算、栅格分析和计算等。空间计算节点可作为节点任务统一编排到工作流，实现空间数据和非空间数据的融合治理及治理链路固化。
- **智能标签**：可将治理后的数据以业务化视角进行建模、查看、管理及使用，并提供业务衍生标签的自定义功能，为上层应用提供统一的标签数据目录和标签调用接口，沉淀上层应用制作的模型标签，实现高价值标签共享复用，形成标签运营生态。
- **统一服务**：是一款数据中台建设过程中的数据服务化组件，面向数据开发者提供覆盖各个加工阶段统一体验的、便捷的数据查询转服务、服务管理、服务运维能力；面向数据资产管理者提供服务的统计分析、服务用量统计分析、热门数据统计分析能力，实现数据中台建设后半场“数据应用”的有效落地，支撑数据智能应用的高效开发。
- **空间服务**：通过空间服务发布将空间数管中的各类型空间数据发布成行业标准的空间服务，支持发布OGC WMTS、WMS、WFS服务；TMS（MVT）矢量瓦片服务；S3M、3DTiles等标准的三维服务。
- **运维监控**：对数据资源平台中的数据同步、数据开发、标签加工等任务进行运维管理。按业务链路配置监控场景，支持自定义监控链路和告警消息配置，可快速实现从数据生产到业务应用的全链路编排及溯源。
- **质量评估**：对数据模型中建立的逻辑表进行质量规则配置和管理，支持根据配置的质量规则在数据开发环节自动生成质量检测节点和设置自定义质量检查计划。提供面向不同计算资源多种类型质量规则，可通过数据质量监控报告展现系统整体数据质量概览，和多维度细分数据的质量情况。

- **解决方案**：对数据资源平台中已沉淀的数据标准、数据模型、数据加工场景、数据服务API配置、云计算资源配置等数据资产进行导入导出，便于在不同环境中快速搭建数据治理工作的初始化。

运营工作台

- **资产注册**：支持平台侧需管理的数据资产注册功能，用户可选择需要管理的数据资产来源作为管理输入，支持对多个数据源端进行展现订阅；可定期自动订阅数据表、标签、API资产的信息。
- **资产目录**：支持按资产类型分别维护资产，帮助资产目录内容提供者对各类资产进行管理维护，并针对资产进行编目分类及发布上下线管控。

数据资产中心

- **资产概览**：提供统一的数据资源视图，以可视化的方式体现数据表、标签、API等数据资产的总量与增量的指标信息。
- **资产目录**：对已接入上线的数据资产，可在资源目录对资产进行搜索、目录列表查看及资产详情信息展示。

画像分析

可基于标签的多维度分析，按照业务需求圈定特定群体范围，实现对复杂群体数据的智能化统计、筛选、加工、沉淀，建立单实体360度全方位个性化档案，通过关系图谱展示、可视化线索分析、相似人员智能化推荐等功能实现用户对于目标群体的精准定位。

数据探索

数据探索面向行业客户/业务人员，提供工具内容一体化的业务模型构建平台，实现低代码、可视化构建全场景专家模型，重塑大数据服务创新模式。平台通过将业务数据沉淀为智能数据或智能算子，以可视化拖拉拽和简单图形化条件设定进行模型编排，支持离线、在线、实时全场景，采用简化建模过程、提高模型运行效能、融合智能化算法等方式帮助用户将数据与业务结合起来，不断积累和沉淀专家业务模型，服务于日常事件挖掘、实时预警事件、在线风险识别。

我的资产

支持我可使用的、我可管理的、我已授权的数据资产及资产信息进行展示、管理。

系统设置

数据资产平台的基础功能，包含账号管理、系统设置。该功能帮助用户快速、便捷完成用户角色及相应权限等基础配置，并实现必要的系统管理与控制，保障模块正常运转。

14.11.2. 产品价值

数据资源平台为用户提供了一站式数据资产定义、生产、管理与服务平台，提供企业级数据资产构建能力和一致性使用体验，助力客户快速构建数据智能平台，实现数据资源统一管理，挖掘潜在规律，优化业务决策，让大数据真正的驱动客户业务。

数据开发更简单

- 平台提供的各种工具产品能够极大的简化数据开发过程，缩短数据治理周期，降低数据治理成本。
- 通过标准化、精细化、规格化的智能数据生产流程，完成流水线式的数据生产作业，提升数据资源生产效率、消除数据供应品质差异。

数据服务更便捷

能够赋予数据以业务价值，让各级用户能够直观的理解数据，并以此为基础向应用输出多样、便捷的数据服务，不断提升数据面向业务的价值。

数据应用更智能

提供面向业务人员的无代码业务模型构建能力和数据分析能力，大大降低数据获取和分析门槛，让业务人员可以直接使用数据，积累沉淀业务模型，能够向上层应用提供更加智能的数据。

数据资产更清晰

从宏观到微观助力数据管理方全面盘点数据资产，通过智能化全链资产血缘分析，理清战略数据资源，做到让管理者心中有数。

数据运营更高效

遵循应用先行、以用带存、由存而通、因通促用的理念，实现城市数据运营，驱动客户业务创新。

14.11.3. 应用场景

数据资源平台可用于构建数据中台，快速沉淀行业领域数据模型资产；面向业务沉淀的数据模型资产，客户画像分析助力精准营销。

构建数据中台，行业领域模型快速沉淀

场景： 快速构建数据仓库，有效治理数据质量，实现政企客户各部门数据的业务协同和共享。

痛点： 以政务服务为例，政务服务部门众多，业务系统复杂、流程长，数据来源多且更新频率高；数据口径标准、数据准确性难以保障，传统政务服务需要老百姓多次递交多份纸质材料提供给不同服务部门，服务效率低。

解决方案：

- 数据同步：通过数据同步功能，将不同业务系统数据汇聚到统一的存储计算引擎，实现数据的初步融合。
- 数据标准：管理数据标准和构建数据模型，将数据标准贯彻到数据质量分析、保障及检查的全过程中，将散乱的多源异构数据加工成标准、干净的数据资产，确保数据的完整性、一致性、准确性和可用性。
- 数据建模：通过数据建模模块提供的各种数据开发工具，实现数据的清洗、加工和转换。
- 资产管理：通过资产运营功能实现资产的注册、编目、上架，在资产中心方便各个部门的使用人员搜索数据资源并申请数据权限。

价值：

- 数据标准一致：沉淀行业数据设计规范，保障数据质量。
- 高效资产管理：快捷数据资产搜索，全360度资产盘点，高效管理数据资产。

面向业务沉淀数据资产，客户画像分析助力精准营销

场景： 传统金融行业客户寻求数字化转型，从产品销售导向逐渐转变为面向客户金融需求的服务导向，需要全面了解客户需求进行更精准的营销推广。

痛点：

- 运营人员获取高净值客群强依赖IT部门，相似指标IT重复开发，无法有效沉淀数据资产，提高开发效率。
- 多部门数据隔离，无法获得全面客户画像，重复营销成本高。
- 各网点数据无法进行行列权限隔离，安全风险高，数据共享难。

解决方案：

- 智能标签：通过智能标签实现面向业务的数据内容编排，搭建主题标签库，实现标签的闭环运营，沉淀业务经验。
- 标签加速配置：通过创建标签加速计划将各种不同数据源的标签数据进行同步，提升数据运维效率。
- 权限控制：依托智能标签及画像分析的工作组，实现信息中心数据面向各网点安全有序开放。

价值：

- 语义化的数据集市，大大降低数据获取和分析门槛，解耦IT人员和运营人员的工作，保证高频运营需求，提升运营效率。

- 高净值客群数据获取时间降低至小时级，灵活的圈群和分析工具，赋能精准营销；由手工EXCEL表获取目标用户列表的方式升级为系统接口实时获取。
- 通过交叉运营，利用不同部门之间的数据资产，降低拉新成本，提升拉新成功率。
- 实现仅信息中心IT人员可查看，到多网点运营及业务人员独立查看，实现行内数据普惠。

14.12. 阿里云Elasticsearch

Elasticsearch是一个基于Lucene的实时分布式的搜索与分析引擎，是遵从Apache开源条款的一款开源产品，是当前主流的企业级搜索引擎。它提供了一个分布式服务，可以使用户快速地、近乎于实时地存储、查询和分析超大数据集，通常被用来作为构建复杂查询特性和满足庞大需求应用的基础引擎或技术。

Elasticsearch集群通常是由多个节点组成的分布式集群，所有节点共同存储数据，并提供集群内所有节点的联合索引和搜索能力。因此，在Elasticsearch集群中，系统会根据设定，将数据量较大的索引切分成若干个“分片”，再分配到各个节点上，以提高水平扩展能力。除此之外，Elasticsearch集群还支持对分片进行备份，以副本分片的形式，存在不同的节点中，以提升集群的高可用性能，并且能够在检索场景下分担集群压力，提升集群的并发性能。

阿里云Elasticsearch提供100%兼容开源Elasticsearch的服务，支持多版本开源Elasticsearch，并针对性地优化内核性能。支持多租户、高可用服务和弹性伸缩。同时，在开源产品的基础上，提供自研中文分词、向量检索等插件，支持企业级安全认证，支持可视化创建集群及插件管理，并能够通过插件支持SQL查询、快照备份等能力。

14.12.1. 产品详情

本文为您详细介绍阿里云Elasticsearch的产品能力。

多租户

阿里云Elasticsearch支持多租户，可实现在云平台多个业务共用Elasticsearch服务，并且确保各业务间数据的独立性。租户可创建和使用多个Elasticsearch集群，并可根据自己的业务需求配置集群节点个数、节点规格和相关参数。每个Elasticsearch需要独立设置密码，用户数据隔离级别高、安全性好。

权限和安全管理

- 分别提供用户控制台和运维控制台，实现用户角色和运维角色账号独立，并支持权限控制。
- 遵循阿里云三网分离规范。用户可在控制台直观查看各域名IP，可避免非预期的网络透出。
- 支持为每个实例单独设置密码，保障数据安全。并支持通过自账号设置，更细粒度拆分集群数据的读写权限。

Elasticsearch搜索引擎

- 提供原生Elasticsearch的API编程接口，用于大数据搜索服务的数据导入、索引建立和数据检索。能够完全兼容Elasticsearch生态组件，包括Kibana、Logstash、Beats和Grafana等。
- Elasticsearch海量数据分布式存储和索引检索技术，支持PB级别数据量近实时分析和检索、数据导入后近实时分析和检索、数据导入后毫秒级别内可查询和毫秒级别响应。
- 针对海量全文数据库的结构化和文本关键词信息存储，进行多维度信息匹配及筛选过滤、倒排索引以及全文检索。支持关键字搜索和综合搜索毫秒级响应，支持模糊搜索和批量搜索秒级响应。
- 支持聚合算子下推，提升搜索聚合分析性能。支持按相关度排序，支持按时间等字段排序。

管控平台能力

- 弹性伸缩

  支持集群规模平行扩展。服务器扩容及缩容过程不影响业务查询，不会停止服务。

- 可视化监控

  提供界面友好的海量信息索引库及全文检索集群可视化平台，实现Elasticsearch集群指标分析，可实时查看索引库及集群状态，支持基础指标的Web化展示。

- 自定义插件和词库扩展

  支持第三方或用户自定义插件上传，支持分词、同义词、纠错词和屏蔽词等多种自定义配置，提升搜索效果，满足个性化全文检索需求。

- 容灾部署

  支持跨可用区部署Elasticsearch集群，以应对业务容灾场景。

- 数据备份

  基于分布式文件系统的数据快照技术，能够进行数据备份和快速恢复，确保数据可靠性。支持通过阿里云OSS进行快照备份和还原。

内核增强

- 引擎特性优化

  部分版本在开源基础上引入阿里自研内核引擎特性，修复部分开源漏洞或缺陷，可针对性优化读写性能及稳定性。

- NLP分词器

  集成阿里达摩院自研NLP分词插件，支持中文的自然语义理解和切词。

- 向量检索

  适配图像和声纹等非结构化数据向量的相似度匹配，支持以图搜图、视频匹配和声音识别等场景化应用。

14.12.2. 产品价值

阿里云Elasticsearch提供100%兼容开源Elasticsearch的服务，支持多版本开源Elasticsearch，并针对性地优化内核性能。在开源产品的基础上，提供自研中文分词、向量检索等插件，支持企业级安全认证，支持可视化创建集群及插件管理，并能够通过插件支持SQL查询、快照备份等能力。

近实时检索和分析

支持海量数据分布式存储和索引检索技术、PB级别数据量实时分析和检索、毫秒级快速响应。

弹性扩容

集群规模可平行扩展。扩容过程平滑，不影响集群正常查询（在有副本的情况下），不需要停服务。

可视化检索分析

提供海量信息索引库及全文检索集群运维管理工具，Web化展示、界面友好。

数据查询

- SQL查询：数据入库后，支持通过插件兼容SQL查询。
- 地理信息查询：支持通过插件兼容地理信息查询。

权限管控

- 支持进行权限配置，支持变更操作权限和只读权限分离。
- 支持在一个账号下创建并管理多个身份，并允许给不同身份分配不同的权限，从而实现不同用户拥有不同资源访问权限的目的。
- 支持对不同集群统一管理，支持集群资源的动态配置及管理、资源隔离等功能。

数据安全

- 支持通过密码保护，阻止未经授权的访问，避免信息和数据泄露。
- 支持同时创建多个集群并独立管理集群密码及配置，实现业务级权限分割和管理。
- 支持通过操作日志记录变更操作。

- 支持业务侧灵活管控Elasticsearch集群内索引、字段级别的数据读写权限。
- 遵循阿里云三网分离规范。且用户可在控制台直观查看各域名IP，可避免非预期的网络透出。

数据备份

- 支持通过自定义插件使用阿里云OSS进行快照备份和还原，基于分布式文件系统的数据快照技术，能够进行数据备份和快速恢复，确保数据可靠性。
- 支持对数据进行全量或增量备份。
- 支持数据中心间的数据集群备份，满足多中心之间的数据互备需求。
- 支持可视化管理集群内备份。

数据同步

支持通过自研跨集群索引同步插件实现集群间的数据同步。

部署维护简单

支持通过自研管控平台一键创建Elasticsearch集群和Kibana可视化工具等，操作灵活便捷。

业务监控

将实例维度的监控数据与云监控对接，默认提供丰富的监控项，可实现用户角度对业务集群的指标分析和监控告警配置。

中文分词

默认整合主流中文分词插件，包括第三方IK中文分词、自研达摩院中文分词插件。

向量检索

默认整合阿里云自研向量检索插件，支持图像搜索、视频指纹采样、人脸识别和语音识别等向量检索场景。

内核增强

部分版本提供阿里内核引擎特性，在开源Elasticsearch的基础上大幅增强了产品性能。例如阿里云提供的Elasticsearch 7.10版本在海量分片下集群的调度速度、带主键文档写入性能、时序查询性能均有较大提升。

容灾部署

具备业务容灾能力，支持跨可用区部署的容灾架构。

服务稳定性

通过管控调度设计针对性优化部署结构，最大程度避免索引数据主副本分配在同一台服务器的节点上，有效提升Elasticsearch集群的高可用性。

Opendistro生态支持

新增对开源Opendistro生态的支持，可实现开源Elasticsearch中不包含的商业X-Pack场景能力，包括但不限于：

- 通过集成ISM插件，支持索引级别的生命周期管理。
- 通过集成Security插件实现LDAP（Lightweight Directory Access Protocol）能力。

14.12.3. 应用场景

阿里云Elasticsearch具有广泛的应用场景，包括日志分析与运维全观测、信息检索、数据智能等。

日志分析与全观测

在复杂业务场景下，海量服务器、物理机、Docker容器、移动设备和IoT传感器等设备中，往往存在着结构分散、种类多样、规模庞大的各类指标、日志和APM数据，对全链路的异常问题定位、业务分析与运维带来了巨大的挑战。用户往往很难从繁杂的日志中获取价值，却要承担其高昂的存储成本。

阿里云Elasticsearch支持通过Beats、Logstash等开源生态组件，快速对接各种常见数据源。借助Kibana仪表盘，能够高效地构建数据可视化运维看板，并在看板中灵活地配置主机名称、IP地址、部署情况、显示颜色等信息。最终帮助用户在海量数据中快速定位和发现问题，提高解决问题的效率，从而让日志数据产生价值。

信息检索

每一个生活在移动互联网中的用户，每天都在查询各种各样的信息。例如查询信用卡账单、电子发票、附近的餐厅酒店、媒体咨询、购物订单、交通物流等。为了帮助用户高效获取信息，广大企业需要实现面向海量数据的信息检索服务。

相对于传统关系型数据库，Elasticsearch拥有强大的全文检索能力，并提供了简单易用的RESTful API 和各种语言客户端。只需要几毫秒的时间，即可在PB级结构化和非结构化的数据中找到匹配信息。用户可以使用阿里云Elasticsearch的高可用性、易用性以及自研的各类插件，实现复杂组合、条件和模糊查询，轻松应对各类文本、数字、日期、IP地理数据，乃至图像、音视频数据的高性能读写。从而快速搭建电商商品或订单检索、App搜索、企业CRM（Customer Relationship Management）系统等检索服务，并整合到已有业务框架中。

数据智能

随着游戏、教育、零售等各个行业的快速发展，除了底层系统的日志指标数据外，往往还存在着规模庞大的业务数据，例如用户行为、行车轨迹、交易记录等。在数据驱动运营的行业背景下，深入统计分析和挖掘业务数据，为上层业务发现问题与机会并辅助商业决策，才能真正让数据产生价值。

阿里云Elasticsearch拥有结构化查询能力，并支持复杂过滤和聚合统计功能。不仅可以快速、高效地分析用户行为、属性、标签等各类数据，实现目标人群的精准触达；还能借助Kibana，完成业务数据的统计分类以及大盘的搭建，从而在电子商务、移动应用、广告媒体等多个场景下，高效统计并分析海量数据，深入挖掘业务的数据价值。

14.13. 关系网络分析

关系网络分析（Graph Analytics）是基于关系网络的大数据可视化分析平台，在阿里巴巴、蚂蚁金服集团内广泛应用于反欺诈、反作弊、反洗钱等风控业务，面向公安、税务、海关、银行、保险、互联网等提供行业解决方案。

Graph Analytics是围绕大数据多源融合、计算应用、可视分析、业务智能来设计和实现的，它可结合关系网络来建立可视化表征以及揭示对象间的关联。

14.13.1. 产品详情

Graph Analytics提供关联网络、搜索网络、智能网络、信息立方、智能研判、协作共享和动态建模等功能，以可视化的方式有效融合了机器的计算能力和人的认知能力，从而使用户获得对海量数据的洞察力，帮助用户更为直观和高效的获取信息和知识。

搜索

搜索是Graph Analytics两大独立模块之一，提供对象信息检索的功能，可帮助用户快速定位信息。同时搜索还是关系网络的入口，可将检索到的对象信息引入到图谱中进行拓展分析。

在Graph Analytics中，搜索分为简单搜索和高级搜索：

- 简单搜索：用于快速搜索包含某一类型的关键字的对象，支持模糊查询。在进行简单搜索时，只要选择一个关键字类型，然后输入一个或多个关键字即可。
- 高级搜索：是一种多条件组合查询方式，支持模糊查询。除了简单搜索中指定的搜索项，高级搜索还支持指定所选搜索项的高级关联项（相当于多类型关键字组合查询），同时还支持指定搜索的数据源项（相当于指定搜索范围）。

图谱

图谱是Graph Analytics进行关系网络分析的场景画布，提供多种关系网络分析方式，可让用户方便快捷的从复杂的关系网络中挖掘出有用的情报。图谱的主要功能包括关系扩展、群体分析、共同邻居、骨干分析、血缘分析、信息立方、群体统计、标签统计和协作共享等。

- 关系扩展：支持以任意单个或一批对象为起点，无限进行关系拓展分析，实现信息的无限关联。情报分析工作的核心是从大量的、无关联的信息中发现少量的关联性线索和情报，即将信息转换为可操作情报的过程。关系扩展有简单和高级两种方式。
- 群体分析：支持分析一批相同或不同类型的对象内部之间的关联关系，包含直接关系和间接关系。
- 共同邻居：支持分析一批相同或不同类型的对象所共同关联的对象。
- 路径分析：支持分析两个对象之间的关系路径。
- 骨干分析：支持针对团伙网络，通过智能业务算法，探索关系网络中核心骨干节点。
- 血缘分析：支持以家族户号为血缘脉络，展示所有人之间的血缘关联。
- 信息立方：包括行为分析、时序分析、行为明细、对象信息、统计信息。
  - 行为分析：展示事件在时间维度上发生的分布频率情况。
  - 时序分析：在时间维度上详细展示每个事件的发生细节。
  - 行为明细：展示事件的明细信息（原数据记录按规则筛选）。
  - 对象信息：汇总关系网络中的实体，并按实体类型分类。
  - 统计信息：统计关系网络中的关系和实体，包含总体分布、对象属性和关系属性。
- 群体统计：用于统计关系网络分析中的群集分布，其中群集是指一群对象节点。在群体统计分析结果中，任意两两对象节点在拓扑上均拥有联通路径，其中合并节点可作为一个联通桥，在拓扑上认为其内部全部联通。
- 标签统计：用于统计关系网络中的对象节点的标签信息。在Graph Analytics系统中，标签分为系统标签和用户标签两类。系统标签是指业务系统给节点定义的标签，例如红黑名单等。用户标签是指每个Graph Analytics用户给节点定义的标签。
- 图区布局：图谱中的节点支持以多种布局方式来显示，包括矩阵布局、圆环布局、横直线布局、竖直线布局、力导向布局和层次布局。
- 协作共享：允许用户将自己的分析文件共享给其他用户，实现了多人协作进行网络分析。通过协作共享功能，用户可在一个分析中融合多人的智慧和经验，使分析结果更精准和完善，也可将团队融合成一个整体。

文件中心

文件中心是Graph Analytics的研判大厅，用于管理所有与当前用户有关的分析文件，支持以全部、个人文件、我的分享和收到的分享等类别查看分析文件。

- 全部：按照创建时间顺序展示与当前用户有关的所有的分析文件，包括个人文件和收到的分享文件。个人文件可分为未分享和已分享两类，未分享是指当前用户创建的但未分享给其他任何用户，已分享是指当前用户创建并且已分享给了其他用户（即我的分享的中文件）。
- 个人文件：按照创建时间顺序展示所有的个人目录和个人分析文件。在个人文件页面，用户可对个人目录和个人分析文件进行增、删、改、查等操作。
- 我的分享：按照创建时间顺序展示当前用户已分享的分析文件。用户分享一个分析文件后，系统均会在我的分享中建立一个与源分析同名的分享文件，该文件默认有初始文件和自动合并两个版本。
- 收到的分享：按时间顺序展示其他用户共享给自己的分析文件。每个共享成员的在收到共享分析后，系统均会在收到的分享中建立一个与源分析同名的分享文件，该文件默认有初始文件和自动合并两个版本。

智能网络

以预定义的模式来查询数据源中与任务具有相同图结构的子图数据。模式是智能网络中预定义的关系图结构模型。任务是基于模式创建的，用于查询数据源中与任务具有相同图结构的数据。

- 模式：模式是智能网络中预定义的关系图结构模型，可分为私有模式和公共模式。
- 任务：任务是基于模式创建的，用于查询数据源中与任务具有相同图结构的数据。基于模式创建的任务，初始与模式完全相同，后续可对任务的图结构、过滤条件等进行修改。

14.13.2. 产品价值

关系网络分析具有实时挖掘、万物相连、灵活赋能、高效体验、以人为本等产品优势。

海量数据实时挖掘

在百亿节点、千亿边和万亿记录的PB量级数据中，Graph Analytics能够按照用户的业务指令进行关系挖掘和时空计算，并且可实时交互响应。

模型认知万物相连

Graph Analytics通过OLEP模型认知世界万物以及万物间的关联，以实体（Object）、关联（Link）和事件（Event）显像表征，以属性（Property）实现异构数据的理解和整合。

业务场景灵活赋能

Graph Analytics自带以OLEP为核心的中枢控制，通过业务配置和感知实现人机交互学习，可灵活的应用于公安、金融和税务等行业的研判分析。

可视分析高效体验

Graph Analytics全面分析潜在用户体验要素和业务痛点，沉淀出了分析可视化和协作共享功能，使得有证可查，有据可说。

智能深入以人为本

Graph Analytics可精准和智能的帮助业务员思考学习，解决常见的业务难题。目前Graph Analytics已有涉恐指数、亲密度和涉毒指数等深度训练模型。

重大项目深度考验

Graph Analytics已经作为亮点应用参与多个国家级重点项目，在安保、反恐和关税等领域让客户耳目一新，业务价值经住了深度考验并得到了认可。

14.13.3. 应用场景

关系网络分析主要面向海关、工商、交通、税务、金融、风控和大安全等提供行业解决方案。

智能关系网络

Graph Analytics提供智能的关系网络分析，可以方便快捷的帮您分析出各对象之间的关系。本节以团伙关系分析和转账交易分析的为例进行介绍。

行业风控

Graph Analytics广泛应用于反欺诈、反作弊、反洗钱等风控业务。

- 关系模型：建立自然人、账户、设备和环境间的联系，通过数据挖掘算法识别关系属性（例如，强弱、影响力和类型等），挖掘关键人物及其子群并进行研究。
- 关系引擎：将关系数据转化成标准化的引擎和接口服务，以使更多的业务场景享受关系网络带来的价值。
- 可视化产品：更友好、直观的展示对象之间的关联，更易于使用。
- 应用方案：通过风险控制以及关系网络推荐等场景中的业务应用方案，使得关系网络可以不断有业务上的驱动。

15.安全服务

15.1. 云盾

专有云云盾是专有云的安全解决方案，从安全运营、主机安全、应用安全、网络安全、数据安全、内容安全、运维审计和安全服务等多方面保护云上资产安全。

15.1.1. 产品详情

专有云云盾主要包括云盾标准版和可选安全产品两部分。本文介绍云盾标准版和可选安全产品的详情。

概述

- 标准版的专有云云盾包含如下产品：网络流量监测与响应、漏洞扫描、安骑士、安全审计、Web应用防火墙、态势感知、云安全管理中心SOC和安全运营驻场服务。
- 除标准版包含的产品外，专有云云盾提供如下可选安全产品：DDoS流量清洗、云防火墙、堡垒机、敏感数据保护、数据梳理、数据库审计、数据发现与脱敏、加密服务、密码服务、安全编排自动化响应、容器防护、云平台安全风险巡检和应用身份服务IDaaS。

网络流量检测与响应

通过多种威胁检测引擎和威胁情报，检测互联网边界和内网边界流量中的网络攻击行为，并对攻击行为进行响应。

功能项	功能说明
流量统计分析	支持查看从互联网边界和内网边界到云VPC内的流量统计和流量列表。
威胁检测	支持对Web攻击、远程代码执行、注入、扫描行为、暴力破解、WebShell上传等网络入侵行为进行检测。
威胁告警	针对检测到的攻击行为生成攻击告警，并通过告警详情查看攻击的IP、类型、威胁等级等基本信息、攻击payload和请求响应报文，支持下载原始pcap包进行进一步分析。
威胁响应	支持一键封禁、一键加白等操作，可快速处理告警。
攻击者画像	从攻击者的视图对入侵者的基础信息、威胁情报、攻击手法、攻击目标、攻击过程进行统一的分析展示。
策略管理	支持对网络层、应用防护策略进行管理。
行为分析	支持DGA域名、DNS隧道、加密流量行为分析。
日志检索	支持对指定时间段的流量日志和安全事件日志进行查看和检索。

漏洞扫描

结合人工智能技术帮助企业及时发现安全风险的智能安全产品。

功能项	功能说明
资产发现	系统内置资产学习模型，根据用户提供的已知资产，准确分辨资产来源，定期进行资产巡检以发现更多的未知资产，并添加至资产库中。
资产管理	系统支持资产导入、删除、分组及导出管理，资产归属及负责人管理，资产检索及监控管理。
资产监测	系统利用HTTP和ping方式对资产进行监测，通过自定义告警策略后，可查看该监控网站在被监控期间的可用性详情及监控基础信息。
漏洞扫描	系统支持基础漏洞扫描、弱口令扫描、安全漏洞扫描、漏洞自动化巡检、基线检测及CVE漏洞扫描。
漏洞管理	系统支持扫描后的漏洞与资产进行自动关联，使资产风险可视化，帮助企业及时发现和管理风险。
外部风险监测	外部风险监测基于员工行为特征和企业关键信息进行外部巡检。

安骑士

通过安骑士服务实现对ECS的入侵防范和恶意代码防范。

功能项	功能说明
基线检查	对云服务器ECS中的安全基线进行检查，包括账户安全检测、弱口令检查、以及配置项风险检测等，以达到企业级服务器安全准入标准。
漏洞管理	• 对云服务器ECS进行扫描，发现主机软件漏洞并提供漏洞修复方案。 • 对云服务器ECS中的应用和操作系统的高危漏洞提供一键修复，包括Web应用漏洞修复、系统文件修复等。
网站后门查杀	通过规则匹配对云服务器中存在的脚本后门进行精准查杀，并可手动对脚本后门进行隔离。
暴力破解攻击检测	对黑客进行暴力破解的行为进行实时检测。
异常登录告警	通过分析和比对用户常用登录设置，对疑似的非常用登录行为进行告警。
主机异常检测	检测诸如反弹Shell、JAVA进程执行CMD命令、Bash异常文件下载等进程异常行为。

资产指纹	对云服务器主机的端口、账号、进程、应用软件等进行清点，全面了解主机资产的运行状态并有效进行回溯分析。
日志检索	将散落的云服务器主机的进程、网络、系统登录等日志集中管理，帮助在主机出现问题时一站式搜索相关日志，快速定位问题根源。

安全审计

通过安全审计服务汇总和分析日志，以便安全审计员及时发现并消除安全隐患。

功能项	功能说明
原始日志采集	支持采集以下日志： • 数据库日志、主机日志。 • 用户侧控制台操作日志、运维侧控制台操作日志。 • 网络设备日志。
审计查询	根据审计类型、审计对象、操作类型、操作风险级别、是否告警和创建时间进行审计日志查询。同时，支持审计日志的全文检索。
策略设置	支持根据发起者、目标、命令、结果和原因参数设置审计规则，对原始日志进行高危操作识别并告警。

Web应用防火墙

通过Web应用防火墙防护恶意应用攻击，保障移动、PC等互联网用户的接入安全。

功能项	功能说明
防护总览	防护总览提供以下功能： • 防护总览：提供最近24小时，以及最近30天的防护统计信息。 • 监控访问状态：实时展示Top 100请求访问信息。 • 导出防护报告：支持导出日报、周报以及定时任务报告。 • 统计攻击检测：提供攻击检测相关的数据统计信息。
防护日志	防护日志提供以下功能： • 攻击检测日志：提供攻击检测日志。攻击检测日志列表显示攻击的处理结果、被攻击地址、攻击类型、攻击者IP及攻击时间针对每条攻击日志，可进一步查看日志详情。 • CC防护日志：提供CC防护日志。日志列表显示匹配中CC规则的日志记录，包括请求URL，命中的CC规则名称及命中时间，提供CC防护日志的条件查询功能，可根据事件生成时间和CC规则名称进行日志筛选。 • 系统操作日志：提供系统的操作日志，内容包括用户名、具体操作行为以及IP等信息。 • 访问日志：提供业务的访问日志，包括请求访问地址、目的IP、源IP、请求方法、响应码等信息。

防护配置	防护配置支持以下功能： • 防护站点管理：支持添加、删除、修改、启用、禁用防护站点的功能转发代理。 • 自定义规则：支持新增、删除、启用、禁用自定义规则，可对站点进行HTTP细粒度的访问控制。 • 攻击防护策略： ◦ 支持URL解码、JSON解析、Base64解码、十六进制转换、斜杠反转义、XML解析、PHP序列化对象解析、UTF-7解码等多种解码方式。 ◦ 支持SQL注入检测、XSS检测、情报、CSRF检测、SSRF检测、PHP反序列化检测、Java反序列化检测、ASP代码注入检测、文件包含攻击检测、文件上传攻击检测、PHP代码注入检测、命令注入检测，机器人爬虫检测和服务器响应检测模块。 ◦ 内置5种模式防护模板（默认防护策略、观察模式、高防模式、金融类客户、互联网客户），针对模板中的解码算法可自定义，攻击检测模块可单独开关或设置检测粒度支持自定义拦截响应状态码。 ◦ 支持开启HTTP响应检测并设置响应BODY检测长度。 ◦ 支持设置HTTP请求BODY的检测长度。 ◦ 支持开启、关闭检测超时限制。 • CC防护：支持设定针对域名和URL的访问频次控制规则，实现对违规IP、Session的访问控制，对满足条件的IP、Session进行访问频率限制或者封禁。对已知的IP、Session进行访问频率限制或者封禁，支持CC白名单功能，CC白名单中的用户（IP或Session）不能通过CC防护规则。
系统管理	支持展示节点的负载、网络、检测等多种状态。日志支持以Syslog发送，可以配置业务以及系统相关的告警阈值。

态势感知

通过态势感知服务实现流量监控、整体安全监控，实现安全审计与集中管控。

功能项		功能说明
态势监控		展示云租户的安全态势，应用于云环境网络安全的监控。
风险分析	安全监控	集中展示网络攻击、异常行为、脆弱性风险三个维度的安全告警数据，应用云租户的安全监控。
	云产品检查	检查云产品服务的安全配置是否存在安全隐患，应用于云产品的安全合规性扫描检查及管理。
	流量分析	展示网络流量统计信息，应用于网络流量风险分析。
资产管理		集中展示云主机资产或虚拟化资产信息列表，以及资产基础信息、网络攻击、异常行为、脆弱性风险，应用于资产风险管理。

云安全管理中心SOC

云原生的一体化安全运营中心，适用于云环境的整体安全运营管理，可以构建云环境风险预测发现、防御控制、检测分析、响应管理的闭环安全运营体系。

功能项		功能说明
运营中心		针对云盾各个安全产品的实时安全告警进行集中统计呈现，支撑安全巡检、安全监控、攻防对抗等场景的安全运营。
态势监控		集中呈现云平台和所有云租户的全局安全态势、资产风险态势、风险威胁态势，应用于云环境网络安全的监控。
风险分析	威胁事件	基于预定义或自定义安全分析规则，针对标准化日志进行关联分析，生成IOC威胁事件，还原完整攻击路径，提炼关键性证据信息，定位攻击源。
	威胁溯源	基于主机异常行为、网络攻击、威胁事件，自动化智能威胁溯源，以图形化的方式还原攻击路径，定位攻击源及攻击目标。
	弱点分析	云平台及租户云主机资产或虚拟化资产的安全漏洞、安全配置基线的集中监控和检索分析。
	云产品检查	云租户产品服务的安全配置检查，检查云产品的安全配置是否存在安全隐患，应用于云产品的安全合规性扫描检查及管理。
	流量分析	云平台及租户全局网络流量信息统计呈现，应用于网络流量风险分析。
威胁情报	情报概览	集中呈现阿里云高度活跃的IP、域名、URL等威胁情报概览统计数据，应用于威胁情报管理。
	情报查询	通过IP、域名或文件MD5进行威胁情报的查询确认，应用于恶意IOC指标的识别和发现。
	情报管理	集中呈现威胁情报使用授权和情报数据应用统计概览，应用于威胁情报数据的消费配置管理。
资产管理	平台资产	集中呈现平台侧云主机资产信息列表，以及资产基础信息和异常行为，应用于云平台资产风险管理。
	租户资产	集中呈现租户侧云主机资产或虚拟化资产信息列表，以及资产基础信息、网络攻击、异常行为、脆弱性风险，应用于租户侧资产风险管理。
处置任务		处置任务管理，提供全局安全风险分析及处置的流程化跟踪管理，应用于安全运营管理工作的辅助支撑。

日志管理	日志概览	集中呈现接入日志的预定义及自定义统计视图，应用于接入日志统计分析。
	日志查询	支持标准化日志全局关联检索查询及查询结果导出。
	平台日志	支持查询云平台侧日志源日志。
	租户日志	支持查询租户侧日志源日志。
	日志配置	• 支持云盾安全网元及第三方网元日志源接入配置管理。 • 支持标准化日志解析模板管理，及接入日志解析、标准化处理配置。 • 支持日志转发到第三方服务器配置。
报表管理		报表管理是面向云安全运营管理者提供的自动化报表导出能力，可创建日报、周报、月报三种周期的报表任务，当周期报表生成以后，自动发送到指定邮箱。
规则管理	分析规则	支持内置和自定义关联分析规则管理，通过分析计算引擎调用，应用于高级威胁检测。
	告警规则	支持自定义安全告警规则管理，提供半自动化的安全告警推送能力，应用于安全运营工作。
	封禁规则	支持安全告警一键IP封禁处置管理。
运营管理	安全审计	支持专有云主机、网络设备、数据库、用户操作、运维操作的日志管理、日志审计、日志查询、及审计策略管理。
	存储管理	支持存储空间占用率统计及管理。
	IP地址库	支持IP地址自定义地理位置管理。
	组织授权	支持全局组织及单组织的SLR授权管理。

安全运营驻场服务

以驻场形式对租户业务系统安全进行专业的运营管理，保障租户系统的安全性。

服务类别	服务项	服务内容
	租户资产调研	在租户授权的前提下，定期调研、整理云上租户业务清单，包括业务系统名称、ECS、RDS、IP地址、域名、责任人等信息。

租户安全运营	租户准入安全检测	• 在租户新业务迁移上云前，通过自动化工具及人工方式对目标业务系统的系统漏洞、应用漏洞进行检测。 • 提供漏洞修复指导及漏洞修复后的验证服务。
	周期性租户业务安全检测	• 周期性通过自动化工具对租户已上线业务的系统漏洞、应用层漏洞及安全风险进行评估，确定存在的风险和漏洞。 • 针对安全检测结果提供风险处置建议，包括但不限于安全策略的设置、安全补丁更新、应用层漏洞改进建议等。
	准入访问控制管理	租户新业务上云时，提供网络访问控制策略实施检测及指导。
	访问控制巡检	周期性对租户业务的访问控制风险进行巡检。
	租户日常安全风险巡检	监控、巡检专有云云盾中出现的安全事件，核实安全事件后，通知并指导用户进行修复。
云盾安全运营	云盾规则更新	负责定期更新云盾产品规则库。
	云盾接入服务	• 提供用户应用系统接入云盾产品的技术支持。 • 协助用户定制、优化云盾安全策略。
应急响应	安全通告	同步阿里云的安全应急通告，并指导用户进行相关修复工作。
	安全事件处理	发生类似于黑客入侵等紧急安全事件时，及时提供安全应急响应服务。

DDoS流量清洗

通过DDoS防护服务提供网络链路可用性保证，提升业务连续性。

功能项	功能说明
DDoS攻击清洗能力	检测并防御SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood、DNS Flood、HTTP Flood攻击。
DDoS攻击查看	可通过IP地址、状态、事件信息搜索到对应的DDoS攻击事件。
DDoS流量分析	针对某DDoS攻击进行流量分析，可查看DDoS攻击的流量协议，并展示该事件的Top10主机IP。

云防火墙

通过云防火墙服务，统一管理互联网到业务以及业务之间的访问控制策略（东西向和南北向）。

功能项	功能说明
网络边界访问控制	支持互联网边界防火墙，包括从云内对互联网、互联网对云内的网络访问控制策略配置。
	支持VPC到VPC防火墙，实现两个不同的VPC之间的网络访问控制策略配置。
	支持VPC到IDC防火墙，实现从云VPC到企业内网之间的网络访问控制策略配置。
网络边界入侵防御	支持阻断异常连接、命令执行、暴力破解、扫描、信息泄露、DOS攻击、溢出攻击、Web攻击等网络攻击行为。
虚拟补丁	支持虚拟补丁功能，热门高危漏洞主机无法更新补丁时，也能通过云防火墙提供虚拟补丁防护。
日志检索	支持查看防火墙访问控制和入侵防御的安全事件日志，支持按多个维度对日志进行检索。

堡垒机

通过堡垒机管理运维ECS，实现云上服务器的操作运维审计和账号权限管理。

功能项	功能说明
主机资产管理	支持对云内ECS主机资产进行运维管理，支持主机/主机组的管理。
访问授权管理	支持基于时间、用户/用户组、设备/设备组、设备账号、命令关键等组合访问控制策略，授权用户可访问的目标设备。
运维命令审核	支持对重要命令进行实时审核。运维人员执行命令后，系统响应动作包括：实时审批、忽略指令、断开会话、实时告警。
运维方式	支持使用浏览器直接调用H5控件实现运维操作。
在线监控	支持对运维操作会话进行在线监控、实时阻断、会话回放。
回话回放	支持会话录像在线回放、定位回放及下载后使用官方专用客户端离线回放。
审计报表	内置根据运维人员和组织生成各种维度的分析报表。
运维管理	支持按设备、账号、计划执行时间、改密周期、密码策略生成详细的改密计划，到期自动执行。

敏感数据保护

通过敏感数据保护服务帮助用户防止数据泄露和满足合规要求。

功能项	功能说明
数据安全态势总览	支持敏感数据的整体安全情况查看。
异常检测与事件处理	检测敏感数据异常事件，人工核查后确认事件处理结果。
敏感数据识别	识别MaxCompute、OTS、OSS、ADS、RDS等产品的敏感数据。
静态脱敏	通过脱敏算法，为敏感数据进行静态脱敏。
智能审计	通过创建审计规则，智能审计OSS、MaxCompute和RDS等产品。
数据权限管理	支持层次化展示部门、人员关系；支持人员、账号的分类展示；支持账号级别的详细权限查询和管理。
数据流转监控	支持DataHub和CDP的数据流转详情展示。
规则配置	配置敏感数据识别规则、风险等级、异常产出规则，通过规则发现敏感数据。
访问授权	基于部门实现授权，敏感数据保护能够保护已授权部门所属的数据资产。

数据梳理

通过数据梳理服务帮助用户发现敏感数据，防止数据泄露和满足合规要求。

功能项	功能说明
数据库自动嗅探	系统提供自动搜索网内数据库的功能，也可以指定IP段和端口的范围进行搜索。
自动识别敏感数据	能够按照用户指定的一部分敏感数据或预定义的敏感数据特征，在执行任务过程中对抽取的数据进行自动的识别，发现敏感数据，并可以根据规则对发现的敏感数据进行导出清单。
权限梳理	能够对数据库中不同用户，不同对象的权限进行梳理并监控权限变化。如果权限发生了变更，能够及时向用户反馈。
资产使用分析	支持数据源访问分析、访问行为分析、资产访问热度分析，并给出分析结果。

任务管理	针对目标数据库，可以创建授权任务对该库进行敏感数据发现和权限梳理。
资产周期统计与对比分析	将数据资产梳理按日、周、月三个周期进行统计，用户可以看该周期内发现数据源分布、敏感数据、权限梳理以及资产使用情况。同时也支持将任意两个周期资产梳理结果对比分析，通过对比分析发现资产差异性。
丰富的报表与技术报告呈现	能够提供给用户丰富的专项报表供用户分析审核，管理员还可以利用报表自定义功能生成定制化的报告。

数据库审计

通过数据库审计服务实现对数据库的审计功能。

功能项	功能说明
审计内容	数据库审计的审计内容包括会话的终端信息、会话的主机信息、会话的其他信息、操作信息等。
审计过滤规则	数据库审计的审计过滤规则包含用户名、实例、字段、执行时长、客户端工具、查询的行数、返回结果集等审计策略要素。
审计信息展示	支持从会话、语句类型、风险三个维度进行导航展示，支持基于时间、客户端IP、数据库服务器IP、用户名、数据库操作命令、数据库表名/字段名等多种丰富的查询检索条件。
审计报表	• 支持系统级多数据库聚合报表展现和单数据库综合性报表展现。 • 基于总体概况、性能、会话、语句、风险多层面展现报表。 • 支持图表结合展现，支持柱形图、饼状图、条形图、双轴折线图等多种统计图展现形式。 • 支持报表定时推送功能，自定义推送周期以邮件形式推送报表文档。 • 支持日、周、月等综合性报表和自定义分析型报表功能。

数据发现与脱敏

通过数据发现与脱敏服务帮助用户对敏感数据进行脱敏，防止数据泄露和满足合规要求。

功能项	功能说明
自动识别敏感数据	按照指定的部分敏感数据特征或预定义的敏感数据特征，自动识别姓名、证件号、银行账户、金额、日期、住址、电话号码、Email地址、车牌号、车架号、企业名称、工商注册号、组织机构代码、纳税人识别号等敏感信息自动识别。
敏感数据管理	提供全面的敏感数据管理功能，实现有序、一致的可视化脱敏数据管理。

脱敏算法	通过屏蔽、变形、替换、随机、格式保留加密（FPE）和强加密算法（如AES），针对不同数据类型进行数据掩码扰乱。
数据子集管理	提供多种数据子集抽取方式对目标数据库中一部分数据进行脱敏，以适应不同场景下脱敏需求。
脱敏策略和方案管理	针对不同脱敏项目，可以配置定制化的脱敏策略，或实现脱敏算法的扩展；支持脱敏策略的导入导出，以实现策略复用。对于同一类应用场景，可将若干脱敏策略组合成为适用于该场景的脱敏方案。脱敏方案制定后，可被重复利用于该场景下不同批次数据的脱敏需求。
脱敏任务管理	可对脱敏任务进行停止、启动、重启、暂停、继续操作，支持任务并发。脱敏过程中可跳过异常数据，持续执行任务；并支持脱敏任务的中断续延。
脱敏数据验证	支持对脱敏后的数据进行“验证”，确定哪些数据是“漏网”的真实数据。

加密服务

通过加密服务满足金融、互联网等行业加密需求，保障业务数据隐私安全。

功能项	功能说明
密码算法支持	全面支持国产算法以及主要国际通用密码算法，满足用户各种加密的算法需求。
金融支付支持	符合中国人民银行标准和规范的金融行业定制加密需求，全面支持金融支付领域的加解密需求。

安全编排自动化响应

通过SOAR安全自动化编排，将安全事件运营自动化、流程化，提升安全响应速度。

功能项	功能说明
案件管理	用户可以在案件中执行调查指令获取安全事件在主机、网络、用户侧的相关数据，用于辅助用户进行安全分析。也可以在案件中执行封禁遏制动作，对恶意指标进行封禁，防止危害扩大。
联合作战室	通过联合作战室快速溯源分析、共享事件数据、下发响应指令、持续跟踪恶意指标。
任务列表	支持查看和SOAR执行的定期任务。查看任务执行记录和输出的数据。
响应动作	支持自定义作战室中的响应动作，并在作战室中调用，扩容事件响应的场景。
剧本响应	内置多种安全运营剧本，并可以自定添加和编辑剧本，实现自动化管理。

组件列表	可以扩展剧本支持组件。
情报管理	持续对恶意指标进行跟踪，并对封禁策略进行管理，实现云内安全防护体系的情报层面的信息共享和联动防御。
知识管理	安全事件处置过程中积累的经验和知识，以及在后续事件中重复利用，提升工作效率。

容器防护

通过容器防护实现对阿里云上容器及其运行环境的入侵防范。

功能项	功能说明
容器资产管理	容器防护为贴合不同用户的使用习惯，在集群视角中提供多种容器资产安全管理方案。
镜像资产管理	容器防护在资产管理功能中提供基于镜像的风险追溯和防护能力。
镜像安全扫描	镜像安全扫描功能支持对镜像中存在的高危系统漏洞、应用漏洞、恶意样本、配置风险和敏感数据进行检测和识别。
入侵事件告警	支持实时检测资产中的安全告警事件，覆盖网页防篡改、进程异常、网站后门、异常登录、恶意进程等安全告警类型。
日志快速检索	提供登录流水、暴力破解、进程快照、网络连接、端口监听快照、账号快照、进程启动的日志查询，支持前缀模糊匹配查询。

密码服务

应用系统通过使用密码服务提供的管理、API等功能完成密码应用。

功能项	功能说明
密码服务平台	支持组织密码机、密码服务资源数量、使用情况等信息统计。
	支持用户一键开通密码服务，支持自定义服务实例数及使用密码机资源配置。
	支持在控制台一键添加实例数（增加云资源）的方式动态扩容密码服务，升级对应用无感，不影响应用可用性。
	支持在控制台一键升级密码服务软件版本，升级过程完全自动化，升级失败支持自动回滚。
	支持按使用密码服务实例类型、数量为租户计量，为运营方提供计量数据。

	支持平台及密码服务管理操作日志审计。
	支持密码服务实例CPU、内存、网络和磁盘使用监控。
	支持与加密服务对接，直接开通、删除密码机实例。
	支持动态扩容或缩容密码机分组，灵活调整密码服务调用密码机实例数量。
	支持新加入密码机分组的密码机实例自动获得与其他密码机同样的数据状态。
密钥管理服务	支持对称密钥、非对称密钥全生命周期管理。
	支持密钥随机产生方式。
	支持密钥授权，密钥授权给某个应用。
数据加解密服务	支持XML、INI、数据库连接串等多种配置文件加密。
	支持手机号、身份证号、银行卡号、口令等多种隐私数据加密。
	支持信封加密功能。
签名密码服务	支持证书管理功能，包括根证书和用户证书管理。
	支持生成证书请求并导入外部签发的证书和导入PFX证书。
	支持Raw签名和验证，国密签名格式符合GM/T0009定义。
	支持PKCS#7Attach和Dettach方式签名和验证，数字信封编制和解密功能。
	支持SM2、RSA非对称加密解密。
	支持XML文件签名的编制及核验。
	支持时间戳证书管理，包括根证书管理和时间戳密钥证书管理。
	支持数据和哈希数据的时间戳生成和验证，支持标准RFC3161时间戳协议规范。

时间戳密码服务	支持通过OID方式调用时间戳。
	时间戳格式遵循GM/T0033时间戳接口规范定义格式。
	支持生成证书请求并导入外部签发的证书和导入PFX证书。
	支持RFC3161、GM/T0033等标准规范。
电子签章服务	支持证书管理，主要包括根证书管理和签章证书管理。
	支持PDF普通签章、骑缝签章编制或核验功能。
	支持OFD版式文档文件的签章、骑缝章签编制或核验。
	支持V1、V4版本的电子印章制作或验证功能、电子签章编制或核验功能。
	支持生成证书请求并导入外部签发的证书；支持导入PFX证书。
	系统兼容海关、金融、公安、财政、税务等重要行业CA证书，并支持中国内地主流CA厂商证书。
SSL网关服务	遵循GM/T0024规范要求，支持国密SSL卸载。
	支持国密双证双向HTTPS应用交付功能。
	支持正向SSL加载安全代理模式，将HTTP协议转换为HTTPS协议。
	支持证书管理功能，包括国密X509数字双证书、国际标准的X509数字证书。
	支持一个服务中可同时配置多条证书链，验证不同CA的用户证书。
	兼容密信安全浏览器。
	支持服务器上的文件夹可指定密钥进行加解密。
	支持ext2、ext3、vfat、ntfs、iso9660、jffs等Linux多种文件系统，支持NAS、NFS等网络存储。
	支持同一台服务器上设置多个加密文件夹，文件夹数量没有限制。

文件加密服务	支持自动根据服务器的操作系统和版本，推送和安装文件加密插件。
	支持不同的加密文件夹，设置独立的加密密钥。
	通过密码插件对文件进行自动加密，无需对现有系统进行改造。
	支持SM2、SM3、SM4算法。
	支持把非空的文件夹设置为加密模式，原有文件被自动加密。
数据库加密服务	支持MYSQL、达梦、神通数据库等数据库透明加密。
	支持数据库加密密钥统一管理。
	支持不同数据源配置独立的加密密钥。
	支持存量数据自动加密。
	支持表加密，支持数据库后置扩展列加密模式。
	通过密码插件对数据库进行自动加密，无需对现有系统进行改造。
	所有数据库类型和加密模式支持SM4算法。

应用身份服务IDaaS

通过统一的账户、认证、授权、审计管理，实现应用单点登录、访问权限管控，以保障应用的身份安全。

功能项	功能说明
应用管理	对应用进行认证配置管理实现应用单点登录，以及开启应用二次认证、开启和禁用应用接口、查看应用操作记录。支持JWT、SAML、OAuth2、CAS、OIDC认证协议。
用户管理	对用户、组织机构进行统一管理，可以手动添加和Excel导入账户、组织，以及人员对入职、转岗、离职、返聘管理。
认证管理	对平台的身份联邦进行管理，配置开启后可使用三方身份源登录到IDaaS平台。
授权管理	对账户、组、组织机构、分类和应用的访问权限进行统一管理。

安全审计	对用户使用行为进行统计记录，包括时间、IP、认证方式、登录应用等。

云平台安全风险巡检

平台安全风险巡检是用于巡检专有云平台底座产品及设备存在的安全风险。

功能项		功能说明
eScan巡检管理	平台安全运营指引	平台安全运营指引将平台存在的安全风险分成6个模块进行展示，包括紧急安全风险、网络风险、配置不当、应用漏洞、三方组件漏洞、合规风险。每个模块中将展示具体的安全风险，并提供风险信息及修复方案，支持导出风险报告。
	巡检任务	用于管理每日巡检任务的状态，可以重启任务、查看任务中各插件的执行状态、查看插件执行返回内容、结果下载、查看任务报错，并支持任务删除。
	文件下载	部分插件支持文件导出功能，可在此入口统一下载。
云平台资产		支持查看云平台相关资产。 • 查看Apsara Uni-manager运维控制台账号：包含账号信息、最近登录时间、是否存在出厂口令、是否开启双因素。 • 集群版本：查询所有云产品集群的版本信息（commitId、commitTag）。 • 资产查询：包含域名、物理机、容器、云平台SLB等资产的查询能力。
便利工具	IP定位	用于全面检索云平台IP资产，定位到对应IP类型。
	资产匹配	支持上传Excel文件，根据IP信息匹配资产类型、归属产品（例如漏洞扫描报告的产品、SR定位）。
插件管理	插件集列表	用于管理每日巡检任务中需要执行的插件列表。
	全量插件	展示全量插件信息，包括插件名、插件描述、插件类型、风险等级等。并提供单插件执行能力。
	白名单列表	云平台风险管理过程中，因各种原因需要进行风险加白处理，此入口将展示白名单列表，支持白名单删除。
系统配置	升级	支持插件包的上传升级，以逐步更新云平台风险插件能力。升级包进行了压缩加密，并通过非对称加密算法校验插件包md5签名。
	日志查看	可查看巡检插件执行过程中的日志信息、本系统访问日志等。

15.1.2. 产品价值

作为云上安全先行者，阿里云云盾拥有多项权威认证，通过成熟的安全体系和安全技术，帮助专有云用户全面保障专有云环境的安全。

云上安全先行者

阿里云安全团队从2005年起护航阿里巴巴集团内部所有业务系统的信息安全，不断积累安全经验。自2011年推出云盾产品，全方位保障云上安全，成为云上安全先行者。

体系完整，技术领先

十年攻防，一朝成盾。在经历了为阿里巴巴集团自身业务十年来的安全护航后，阿里巴巴积累了大量的安全研究成果、安全数据、安全运营和安全管理方法，形成了一支专业的云安全专家团队。 云盾是集合这些安全专家多年攻防经验开发出来的面向云计算平台安全最佳实现的成熟体系，可有效保护专有云用户云平台、云网络环境和云业务系统的安全。

与传统安全产品对比

特点	传统安全产品	云盾
互联网企业安全能力完整输出	传统安全厂商都有各自擅长的产品，但在其他产品上存在短板，无法形成整体安全防护体系。	阿里巴巴集团在与黑客攻击对抗过程中沉淀了大量的情报能力，及时发现流行的互联网攻击行为以及0 Day攻击手段，为用户提供完整的安全能力。
提前研判、预知风险爆发	传统安全厂商缺少完整的监控业务场景，无法准确研判风险的爆发。	对于重大漏洞、重大安全事件能够进行分析并及时响应，避免安全问题的爆发。
安全大数据建模分析	传统安全厂商使用单一的特征检测方式无法发现未知威胁；日志分析展现仍停留在数据统计、报表展现，无法实现真正的安全数据建模分析。	通过大数据建模分析方式，发现全网安全威胁，并全量展示安全态势。模型包含30多种算法模型，结合历史数据、网络数据、主机数据，实现真正的态势感知能力。
弹性扩容，与硬件解耦合	基于自身定制的硬件设备实现；软件化后的安全产品，也是基于虚拟化平台上的虚拟主机实现。	• 硬件解耦合：采用云架构设计，所有功能模块都基于通用的X86硬件平台，对硬件无依赖性。 • 弹性扩容：在性能不足时，无需改造网络结构，直接平滑地扩展硬件数量即可。
体系化建设，联合检测响应	通过设备的堆叠来实现安全能力覆盖。各设备之间不能有效的联动，一般只能通过管理平台将各个设备的日志、状态进行统一收集、展现。	提供完整的网络、主机、应用、数据、身份防护能力，各防护组件通过自动化的运营方式实现联动响应、情报共享。
兼容所有的IDC环境，和云平台解耦合	大部分的传统安全厂商仍然基于硬件盒子的形态提供安全产品。在SDN技术越来越普及的情况下，这样的形态无法与云环境兼容。	采用“网络出口检测 + 服务器操作系统联动”架构；采用数据分析方式发现安全威胁。通过这种架构及方式，避开了IDC内部复杂的网络结构，完全兼容所有的IDC环境。

15.1.3. 应用场景

专有云云盾为不同规模、不同行业的用户提供灵活的、可扩展的安全解决方案，主要用于工业、农业、交通、政务、金融、交通、教育等各个方面。

专有云等保

阿里云专有云通过帮助用户在计算资源平台部署专有云云盾主机安全、网络安全、应用安全、数据安全、运维审计和统一管理安全体系，实现纵深防御，实时掌握平台和业务安全风险，满足等保三级和四级合规安全技术要求。同时通过安全运营驻场服务和等保咨询服务，保障客户业务安全和稳定运行，满足等保2.0三级和四级合规安全管理和测评要求。

政务专有云

政务专有云通过构建专有云政务统一服务平台，建设智能便民服务和智能政务办公，大幅提升内部工作效率和便捷为民服务。客户部署云端DDoS和Web防护形成最外侧第一道防线，并通过专有云云盾安全产品保障政务云业务系统的运行安全、数据安全、运维安全，通过安全服务帮助用户构建安全管理组织结构、管理制度和安全工作意识。

金融专有云

金融专有云建设安全纵深防护体系，在专有云出口部署Beaver、Aliguard、云防火墙进行网络层攻击的深度检测及防护；在应用层，部署WAF对应用层攻击进行过滤；在主机上部署安骑士主机防护客户端，对端终安全进行防护。在此基础上，收集全网安全日志，进行统一安全大数据建模分析，打通安全孤岛。安全防护系统基于X86架构进行云化部署，告别传统安全专用硬件。

15.2. 密钥管理服务

密钥管理服务KMS（Key Management Service）是一站式密钥管理和数据加密服务平台，提供简单、可靠、安全、合规的数据加密保护能力。KMS帮助用户降低在密码基础设施和数据加解密产品上的采购、运维、研发开销，以便用户关注业务本身。

15.2.1. 产品详情

密钥管理服务KMS（Key Management Service）包含用户主密钥、自带密钥（BYOK）、全托管密码机、加密密钥轮转、主密钥别名、资源标签功能。

用户主密钥

密钥服务是KMS的核心组件，加密密钥为用户主密钥CMK（Customer Master Key）。用户主密钥包括：

- 对称密钥：主要用于数据的加密保护场景。如果不指定具体的密钥规格（KeySpec），则KMS默认创建的是对称密钥。通过使用KMS加解密的接口，无需获得密钥的明文材料就可以完成对数据的加密操作和解密操作。
- 非对称密钥：主要用于数据加密和数字签名。用户在KMS创建的非对称用户主密钥（CMK），由一对关联的公钥和私钥构成。公钥可以被分发给任何人，而私钥必须被安全的保护起来。KMS保证私钥的安全性，不提供任何接口导出非对称密钥的私钥，可通过私钥运算的接口来使用私钥进行数据解密或者数字签名。任何获得公钥的人，都可以使用公钥进行数据加密或者验证私钥产生的签名。

自带密钥（BYOK）

为了满足更高的安全合规要求，KMS支持使用自带密钥（BYOK）用于云上数据的加密保护。对于自带密钥的情形，推荐用户使用托管密码机对密钥进行保护，将密钥导入到保护级别为HSM的CMK中。导入到托管密码机中的密钥只能被销毁，其明文无法被导出。

全托管密码机

KMS使用具有合规资质的托管密码机，可安全生成密钥、存储密钥、执行密码计算。通过将外部密钥导入托管密码机，实现对密钥的启用或禁用、生命周期管理、密钥别名或标签设置和运算接口调用，保护最敏感的计算任务和资产。

> **说明** 全托管密码机需要额外购买硬件安全模块（HSM），并且购买KMS高级版本的License。

加密密钥轮转

用户可通过密钥版本化和定期轮转来加强密钥使用的安全性，实现数据保护的安全策略和最佳实践。加密密钥轮转包括自动轮转、人工轮转。

- 自动轮转密钥：KMS支持同一个CMK有多个密钥版本，每个版本为一个独立的密钥，各个版本互不相关。在多版本的基础上，KMS内建了加密密钥的自动轮转能力，帮助用户实现安全最佳实践并满足合规审计要求。
- 人工轮转密钥：如果用户使用的密钥类型不支持基于密钥版本的自动轮转，可以基于使用场景，直接轮转使用的用户主密钥 （CMK），通过人工的方式实现密钥轮转。

主密钥别名

KMS支持为主密钥创建别名，通过别名可以更方便的使用主密钥。

别名是用户主密钥的可选标识，在一个组织账号、一个地域中具有唯一性。同一个组织账号在不同地域下可以拥有相同的别名。 每个别名只能指向同地域的一个用户主密钥，但是每个用户主密钥可以拥有多个别名。

资源标签

通过资源标签用户可以更方便的管理KMS中的密钥资源。

15.2.2. 产品价值

与传统密钥管理设施（KMI）相比，密钥管理服务KMS（Key Management Service）具有多集成、易使用等优势。

多集成

KMS和ECS、RDS、OSS等多个产品无缝集成。通过一方集成，用户可以轻松地使用KMS主密钥加密，控制存储在服务中的数据，管理云上计算和存储环境。

易使用

产品价值	说明
轻松实现加密	KMS提供简单的密码运算API，简化了密码学概念，让用户轻松使用API完成数据的加解密。对于需要密钥层次结构的应用，KMS提供了方便的信封加密能力，快速实现密钥层次结构。例如：生成一个数据密钥，并将主密钥（CMK）用作密钥加密密钥KEK（Key Encryption Key）来保护数据密钥。
集中密钥托管	密钥管理服务提供对密钥的集中化托管与控制。 用户可以从线下密钥管理基础设施（KMI）或在加密服务中创建的HSM中将密钥导入到KMS。无论在KMS内创建的密钥还是外部导入的密钥，密钥中的机密信息或者敏感数据都会被阿里云上的其他云产品用于加密保护。
支持自带密钥（BYOK）	KMS支持自带密钥BYOK（Bring Your Own Key）。用户可以将密钥租借给KMS用作云上数据的加密保护，从而更好地管理密钥。
自定义密钥轮转策略	KMS允许用户根据所需的安全策略来自动轮转对称加密密钥。通过密钥轮转，可达成如下目标： • 减少每个密钥加密的数据量 • 提前具备响应安全事件的能力 • 对数据形成逻辑上的隔离 • 减小破解密钥的时间窗口 • 满足合规规范

15.2.3. 应用场景

用户可以使用密钥管理服务KMS（Key Management Service）对云上数据进行加密，保护云上的敏感数据安全。例如，KMS可为应用开发者提供加密密钥保护功能，从而保障应用系统中敏感数据的安全。

信封加密

使用信封加密技术将主密钥存放在KMS服务中，只部署加密后的数据密钥。仅在需要使用数据密钥时，调用KMS服务获取数据密钥的明文，用于本地加解密业务数据。

直接加密

直接调用KMS的加解密API，使用主密钥直接加密或解密敏感数据。

服务端加密

使用云产品的服务端加密功能，更简单有效的对数据进行加密保护。例如：通过对象存储服务端加密，保护存储敏感数据的OSS桶或通过数据库透明数据加密（TDE），保护存储敏感数据的表。

16.应用服务

16.1. API网关

API网关帮助企业快速构建以API为核心的系统架构，满足新技术引入、系统集成、业务中台等诸多场景需要。同时，提供防攻击、防重放、请求加密、身份认证、权限管理、流量控制等多重手段保证API安全，降低API开放风险。支持自动生成SDK、API说明文档，提升API管理、迭代的效率。API网关提高能力复用率，加速企业内部业务创新。

16.1.1. 产品详情

API网关提供完整的API托管服务，覆盖设计、开发、测试、发布、运维监测、安全管控、下线等API各个生命周期阶段。

API生命周期管理

- 支持包括API发布、API测试、API下线等生命周期管理功能。
- 支持API日常管理、API版本管理、API快速回滚等维护功能。
- 发布管理，通过不同域名或header方式访问到不同环境的API。
- 支持API Diff功能，API发布时，可以与历史版本进行对比，了解API版本间细节差异。

全面的安全防护

- 支持多种认证方式，包括匿名访问、简单身份认证、摘要签名认证、JWT认证方式。
- 支持HTTPS协议，支持SSL加密。
- 防攻击、防注入、请求防重放、请求防篡改。
- 支持后端签名认证，提供网关和后端服务之间的认证。

灵活的权限控制

- 以APP作为请求API的身份，网关支持针对APP的权限控制。
- 只有已经获得授权的APP才能请求相应的API。
- API提供者可以主动授权某个APP调用某个API的权限。

丰富的插件功能

- 通过插件功能，使API具备插拔式的功能扩展。
- 网关提供流量控制、IP访问控制、后端签名、JWT鉴权、跨域资源访问（CORS）、缓存、后端路由、访问控制、断路器、错误码映射等丰富的插件种类。

请求校验

支持参数类型、参数值（范围、枚举、正则）校验，无效校验直接会被API网关拒绝，减少无效请求对后端造成的资源浪费，大大降低后端服务的处理成本。

数据转换

支持前端请求的数据转换。通过配置映射规则，实现前、后端数据翻译。

集成

支持集成大数据平台作为后端服务，以API形式对外提供数据服务。

自动化工具

- 自动生成API文档。
- 提供多种语言的SDK示例。
- 提供可视化界面调试工具，快速测试，快速上线。

监控报警

- 提供可视化的API实时监控，包括调用量、响应时间、错误率等。
- 配置API报警，以便实时掌握API运行情况。
- 结合日志服务SLS，提供API全量日志查询，支持将API的HTTP请求应答日志记录到日志中。

16.1.2. 产品价值

API网关具有解放生产力、高性能、稳定、安全等产品优势。

解放生产力

完成API录入后，即可告别API管理的一切繁杂，API网关为客户解决API文档维护、SDK维护、API版本管理等繁琐事务，大幅降低日常开发维护成本。

高性能

支持高效率的HTTP2协议接入，同时支持使用二进制长连接通信的WebSocket协议接入，提高良好的客户端接入性能。采用分布式部署，自动扩展，能够承载大规模的API访问；同时还能保证较低的延时，为后端服务提供高保障高效率的网关功能。

稳定

API网关自2016年在阿里云公共云正式商业化发布，历经数年公共云、专有云用户的考验，能在各种情况下都保持平稳的运行状态，如大报文、后端服务不稳定返回时间不确定的各种特殊情况。

安全

API网关具备全链路SSL通信的能力，保证所有数据在传输过程中不被窃听。API网关具备全链路签名验证的能力，保证所有数据在传输过程中不被篡改。API 网关还提供严格的权限管理功能、防重放、参数清洗、IP访问控制、精准的流量控制功能，并且能够与阿里云WAF组合使用，提供全套API安全保障，让您的服务安全、稳定、可控。

16.1.3. 应用场景

API网关在中台API枢纽、多端兼容、系统集成等场景中都发挥着重要作用。

中台API枢纽

API网关可作为各系统的API统一管控工具、快速实现互通互联和系统间集成对接，对API进行统一API管理，统一流控，统一权限，统一监控。方便运维操作，避免重复接入，一次接入全部共享，极大提高运营效率。

多端兼容

随着移动、物联网的普及，API需要支持更多的终端设备，以扩充业务规模，但同时也带来系统复杂性的提升。

- 通过API托管可以使API适配多端，企业只需维护一个服务体系，面向多端输出；只需调整API定义，即可实现对App、设备、web端等多种终端的支持，无需做额外工作。
- 降低运维成本，多个场景、多个终端、多种用户、多级服务，仅需要运维一套 API，降低运维复杂度。

系统集成

- 通过API网关对系统间接口进行规范统一，用标准化的接口实现系统集成。

- 快速完成资源整合和管理，消除快速发展造成的冗余和浪费，聚力发展业务。

16.2. 无影云桌面

无影云桌面是一款面向数字经济时代的生产力工具，可实现随时随地云上办公、海量算力触手可得、多种应用一网打尽，依托阿里云安全防护体系，全面保障企业业务和数据安全。无影云桌面为客户提供一整套易用、安全、高效的云上办公体系，带来便捷、流畅的办公体验。无影云桌面具有弹性配置、购买灵活；集中管理、高效运维；网络便捷、数据安全等优势，适用于远程办公、多分支机构、安全OA、专业制图和短期使用等多种场景。

16.2.1. 产品详情

阿里云无影是依托阿里云专有云打造的云管端一体化安全防护体系，借助多个功能模块共同为客户提供强大算力、 海量应用和便捷办公体验。

阿里云无影主要的功能模块主要有：

- 终端：支持超轻量零终端，同时提供SDK用于生态扩展。
- 零终端：阿里云自主研发超轻量级终端设备，支持自主协议，主要用于连接用户终端外设和服务接入。
- 外设与企业IT设施：支持主流外设与IT环境。
- 轻空间：提供给终端办公用户的一个智能办公空间。
- 云流自适应流媒体技术：自主研发的ASP协议，是阿里云无影产品中自主研发的面向应用流的新型端云协同协议，用于终端与云端交互。
- 云应用：部署在云平台的各操作系统平台的应用。
- 云管控：面向客户运维管理人员一站式控制台，可对云桌面、云资源及零终端进行安全有效的管控。
- 云安全：依托阿里云强大安全能力打造的端到端安全。

零终端

零终端是阿里云无影产品中的用户使用的超轻量级终端设备。零终端基于阿里云自研的StreamingDocker方案及自适应流化协议，将从网络接收到的加密数据流，在本地进行解密及解码，并通过零终端连接的显示设备将图像输出给用户。

ASP协议

ASP（Adaptive Streaming Protocol）是阿里云自主研发的面向应用流的一种新型端云协同协议，旨在为无影产品提供端云一体的协议支撑，为终端用户提供低时延高画质的实时交互体验。通过ASP协议用户在不同服务器和客户端配置需求中、不同的工作场景下以及不同的网络条件时均能得到最佳的用户体验。

轻空间

轻空间是在云端运行面向企业办公人员的一个智能办公空间，集成办公协作、文档管理、跨系统应用、云桌面等服务。保障了办公数据在云端的安全且易于管理，便利了应用服务的使用，从而实现高效办公。

云管控

云管控是为阿里云无影产品管理运维人员提供的一站式控制台。是无影产品的“中枢管理站”，可实现云应用发放管理、云桌面管理、用户管理、相关云资源管理、终端管理、系统运维管理、策略管理等简单、高效的管理运维。

云资源

阿里云无影产品根据用户可能使用客服、办事大厅或呼叫中心等对计算资源要求不高的业务，给出多用户共享桌面的方案。在使用共享桌面进行办公时，在同一时刻一个虚拟机资源可以给多个用户同时使用。从而减少虚拟机资源的占用，将更多的计算资源给专有桌面的用户使用，实现虚拟机粒度的资源弹性使用。

16.2.2. 产品价值

无影云桌面与阿里云上其他服务和IT设施打通，实现高效创建和维护桌面办公系统。无影云桌面的价值体现在：云上的桌面服务，可随时随地访问；数据保存在云端，高可靠存储，安全无忧；无需投资基础硬件设施，即用即买，灵活弹性，节约成本；云上集中管理，运维简单高效。

产品安全

- 终端安全：终端采用自研终端，避免病毒和木马侵害。
- 外设安全：终端外设端口的使用支持灵活管控。
- 数据安全：用户数据均在云端，终端上不留业务数据，保证数据不泄露、不丢失。
- 行为安全：通过云管控平台全链路监控数据流转，保证用户行为可追溯。
- 环境安全：采用阿里云专有云安全基础设施，支持配置安全策略、云盾DDoS防护系统、多用户隔离、防密码破解等安全措施。

数据可靠

- 数据存放于高可靠的云端存储。
- 桌面运行于阿里云全托管的基础设施之上，用户无需关心设施运维。
- 可灵活配置安全策略，提供剪贴板、本地磁盘等基础策略和客户端登录方式管控策略。从而减少数据泄漏的风险，实现精细化的安全管控。
- 支持查看远程命令和用户操作日志，操作可审计可溯源，提高安全性。

访问便捷

- 支持通过公网、内网、专线等网络连接。
- 安全网关实现网络隔离，保障访问安全。
- 支持Windows客户端、macOS客户端、Web客户端和硬件终端（卡片式、盒式和一体机。）连接云桌面，可随时随地访问云桌面。

运维高效

- 集中式管理：软件、桌面、云资源、用户、终端和外设在管控平台中心化部署、发放和授权，大幅提升管理设备的效率。
- 可利用资源充足：充沛的算力资源，根据应用即时按需调度，轻松满足日常办公或大型软件研发等不同需求。
- 迁移便捷：用户数据保存在云端，支持随时迁移。
- 平台易用：采用云管控运维平台，高效、可靠、简单、易用，无学习成本。
- 容灾备份：环境和数据具备多份副本，单份损坏可在短时间内快速恢复。
- 云主机简化运维：软件、系统升级均在云上完成，配合分时、迁移设置，用户无需关注。主机数据与计算分离，如果主机运维操作故障，无需担心主机数据丢失。

降低成本

- 购买成本：无需投资基础硬件设施，即用即买，灵活弹性。
- 终端成本：零终端超低成本，硬件购买便捷安装简单。
- 运维成本：大幅减少运维人力支出及安全管控方案采购需求。
- 应用管理成本：可统一购买、分配和授权应用，便于企业统一管理。

16.2.3. 应用场景

针对不同规模和不同行业的用户，无影云桌面为客户提供合适的行业解决方案。无影云桌面可应用于具有较高数据安全管控和较高计算性能的领域，广泛适用于远程办公、多分支机构、安全OA、专业制图和短期使用等多种办公场景。

远程办公

政务办公场景中，政府对办公地点、资源和设备的灵活性具有一定的要求，无影云桌面产品针对性地为客户提供多种CPU、GPU规格，多地域覆盖，同时支持多种客户端。客户可不受时间、地点、资源和设备的限制，根据业务需求弹性配置、快速购买，下单后简单安装即可使用，满足客户按需弹性购买或释放桌面的要求。适用于有出差需求和办公地点灵活的员工。

多分支机构

政务办公场景中，企业可能会面临以下问题：数据管控较为分散，资源利用率相对较低，运维成本过高，无影云桌面企业办公方案可有效解决上述问题。采用无影云桌面通过管控平台轻松实现在线管理多地多分支机构，满足大型企业的IT管理需求，提高协同办公效率，适用于同一地域多机构分散或者跨地域多分支机构协同办公场景。

安全OA场景

采用无影云桌面企业数据不落地，高可靠保存在云端；通过安全网关隔离公共网络和云桌面所在的VPC网络，保证数据安全可靠；辅以水印、磁盘映射等基础策略和多种安全策略保证数据可溯可审，防止数据外泄；同时借助RAM权限管控，确保权限最小化。适用于对安全性和保密性要求较高的办公场景。

专业制图

无影云桌面提供高性能桌面，兼容市场主流设计软件，满足客户高计算机性能需求的使用场景，例如：在线设计和渲染图纸、在线制作动画视频或需要较高配置独立显卡的大型软件。

短期使用

采用无影云桌面客户可以根据使用需求弹性购买或释放资源，使用灵活，节约成本。适用于政务办公中短期实习生和临时培训等办公时间较短的场景。

17.应用运维服务

17.1. 应用运维平台

应用运维平台（Application Operation Platform，简称AOP），是一款面向混合云的应用运维平台，提供以稳定高效为本的“云+应用”一体化运维产品解决方案。面向应用提供“云+应用”全生命周期管理，面向业务提供“云+应用”监管控一体化运维，保障业务稳定运行，让企业稳定用云。

17.1.1. 产品详情

应用运维平台提供应用蓝图、全景监控、自动化运维、统一事件管理、统一配置管理、安全风控六大核心产品特性。

应用蓝图

提供“云+应用”全生命周期管理能力。构建从应用逻辑态、应用部署态到应用运行态“三态”纳管能力，即从“应用逻辑态管理”的应用架构设计与管理、应用运行环境规划；到“应用部署态管理”的部署架构管理、资源管理、发布部署管理；到“应用运行态管理”的全景监控、统一事件管理、自动化运维，统一配置，统一风控，实现“云+应用”全生命周期管理。

功能模块	功能描述
应用等级定义	支持应用等级定义（高可用等级、重要性等级、连续性等级、安全性等级等）
应用环境规划	• 支持应用生产环境规划与管理 • 支持应用预发布环境规划与管理 • 支持应用测试环境规划规划与管理
应用逻辑态管理	• 支持应用系统架构管理 • 支持应用访问关系管理 • 支持资源模版管理
应用部署态管理	• 支持应用部署架构管理 • 支持灵活的资源编排 • 支持部署集群管理 • 支持资源一键部署
应用运行态管理	• 支持全景应用监控关联与管理 • 支持应用自动化运维关联与管理 • 支持统一事件管理关联与管理

全景监控

提供“云+应用”租户侧全景监控能力，即提供统一的监控入口，支持从业务、应用到云服务实例三层上卷下钻、层层监控。提供业务全链路、业务关键指标智能分析的业务监控；提供应用自身关键指标、上下游调用链智能关联分析的应用监控；提供服务可用性的服务拨测；提供声明式、低代码的监控自助服务；提供云服务实例运行状态监控、分析、应用关系自动挖掘的云服务实例监控；实现故障的快速发现与定位。

功能模块	功能描述
业务监控	• 支持业务全链路关键指标监控 • 支持业务全链路关键指标分析 • 支持下钻应用指标分析
应用监控	• 支持应用关键指标监控 • 支持上下游调用链分析
云服务实例监控	• 支持云服务实例运行状态监控 • 支持云服务实例运行状态分析
逐层下钻与关联分析	• 支持从业务到到应用下钻与关联分析 • 支持从应用到云服务实例下钻与关联分析
监控告警与事件关联	• 支持控告警与事件关联与分析 • 支持不同人群不同渠道告警

自动化运维

提供“云+应用”自动化运维，实现“看管控”一体化的自动化运维。

- 支持“看”-统一运营体系：即从统一编排入口、服务目录、资源调度、到统一配置管理等
- 支持“管“-高效的应用管理：即从自定义服务目录、灵活运维编排、可视化的资源交付、流程化的在线审批、到多平台多策略发布等
- 支持”控“-稳定的应用运行：即从安全策略管理、变更窗口管理、变更实时检测、到高危风险拦截等

功能模块	功能描述
统一编排入口	支持统一流程中心、统一待办中心、统一消息中心、统一权限中心、统一模版中心
灵活运维编排	支持结合客户场景，自定义运维服务内容。包含应用扩容、服务重启、集群扩缩、应用巡检、服务下线等各种运维服务

多策略多平台发布	• 支持一键部署、一键回滚 • 支持多策略发布。支持发布批次、批次内滚动发布、蓝绿发布、灰度发布、金丝雀发布、无人值守等发布策略 • 支持多平台发布。支持裸金属、虚机、标准容器平台、EDAS、SOFA、ACK等多平台发布 • 支持发布过程中插入作业执行等复杂的自动化发布流程 • 支持发布模版管理功能。通过标准的发布模版将策略、依赖关系规内嵌并规范化，应用发版时不需要重复构建发布内容，只需关注动态变化的版本参数等变量，提升发布效率
全方位变更管控	• 支持事前风险识别、检测。应用变更前风险检测包含封网管控、变更窗口管控、变更管控策略、高危脚本检测等 • 支持事中风险拦截 • 支持事后风险追溯

统一事件管理

提供“云+应用”统一事件管理能力。提供从业务、应用、云服务实例、云平台资源到硬件基础设施五层的“一体化事件定级”能力，即从业务定级、应用定级到云平台定级；提供五层的“一体化事件管理”能力，即从事态采集定级管理到事件监控定级关联处理，进行统一技术运营分析；提供五层的“事件智能联动”能力，即从事件归集到智能关联；实现故障的快速定级与定界。

功能模块	功能描述
业务定级	• 业务指标定级是评价一个“业务”运行稳定性的量化标准，一旦业务指标超过【策略】设定的阈值就会产生对应级别（P1-P5）的业务故障事件 • 支持对“业务交易指标”设置不同的策略（同比、环比、基线、阈值），产生不同等级的“业务交易异常事件 • 支持事件等级与触发规则关联与管理 • 支持“自顶向下”安全生产体系的顶层设计，发现应用系统的业务运行健康状态，即从网络延迟、DB抖动、系统故障、市场行情暴涨、到渠道堵塞等各种类型问题引起的业务故障
应用定级	• 一整套应用相关事件的丰富、关联、定级策略模板，可以将应用下所有的告警事件关联合并成一个以应用为对象的事件 • 支持多场景定级，即从交易系统、服务可用性、部署集群、部署实例到云服务实例等 • 支持根据异常实例比例、应用重要性等级综合判定事件的等级
云平台定级	• 一整套云平台相关事件的丰富、关联、定级策略模板，可以按云产品下所有的告警事件关联合并成一个事件 • 支持多场景定级，即从云产品监控、Service监控、云服务实例集群到工作集群等
事件智能联动	• 支持事件从采集、分析、关联到归集 • 支持事件上下关联与分析 • 支持构建特定的诊断场景，用户可以在该类故障发生时通过触发“诊断”场景自动排查和缩小故障范围，实现故障的智能定界

故障告警分级	支持根据客户业务情况来进行告警分级定义与管理，从P1-P7的分级和对应运维规则定义与管理
全局展现	• 支持业务视图、应用视图、云平台视图和整体统一盯屏试图展现 • 支持从“全局视图”下钻到“二级详细视图” • 支持从“业务视图”下钻到“应用视图”
事件管理	• 支持统一查询所有接入的事件信息，支持用户根据不同筛选条件进行事件筛选 • 支持提供事情详情，事情轨迹，事件处理（响应、转交、结单） • 支持原始告警信息的查询
事件通知	• 支持定制事件的通知规则，支持按事件对象、类型、等级、来源筛选特定事件，支持在事件发送和恢复时通知，通知生效时间可配置 • 支持将用户指定为通知对象，当通知策略筛选规则被触发时，系统会向服务组中的联系人发送通知。 • 支持指定通知频率、最小和最大间隔时间，对于未恢复的事件通知的频率会被抑制 • 支持通知模板为每个通知渠道提供自定义通知格式能力

统一配置管理

统一配置管理（即CMDB），作为企业ITIL规范中的核心，提供储存与管理信息系统的各种配置数据。提供从团队协作、企业主数据、IT资产管理等核心模块的数据交换服务；自动化和智能化监控运维的基础服务；提供业务维度、应用维度、云服务实例、云平台资源、硬件基础设施的视角展现；提供灵活的建模以及查询能力；在大流量、高并发的情况下，提供实时、准确的数据操作能力，支撑各种运维业务的需求。

功能模块	功能描述
故障Attach	• 支持业务维度、应用维度、云服务实例、云平台资源、硬件基础设施的视角展现 • 支持故障逐层下钻，即上卷看影响、自身看状态、横向找源头、下钻找根因
主动运维	支持平台侧运维人员从硬件视角看到全景视图，精准分析基础设施影响链路，实现主动运维
资源管理	• 支持快速查看模型里下所有实例信息 • 支持展示当前实例的所有CI属性值 • 支持查看与当前实例存在关联关系所有实例信息 • 支持查看当前实例的变更历史（变更类型、变更系统、变更项、变更前后值）

拓扑查询	• 支持多维度、深度的复杂拓扑查询，复杂关联表数量可以达10+，常见查询也有3到5跳查询 • 支持查询平均RT在5毫秒以内，95%的查询在20毫秒以内，99%的查询在150毫秒以内 • 支持定时数据对外写入/导出报表 • 支持多达8种检索条件（等于/不等于、关联/未关联、包含/不包含、匹配/不匹配）
模型管理	• 支持模型分类的管理 • 支持模型的新增、编辑和删除，其中平台内置模型不支持编辑和删除 • 支持模型字段分组管理 • 支持模型关联关系维护 • 支持模型唯一校验维护
业务管理	• 支持单CI模型千万级实例信息的存储，查询平均RT在5毫秒以内，用于响应应用运维平台、监控系统、应急平台等系统的大量查询 • 支持以产品树+应用系统的维度，灵活化展示各节点的主机信息，并对内存、CPU、存储、机器数量方面对资源进行汇总
运营分析	• 支持CMDB全量信息进行多维度统计分析，可视化展示模型数量、模型关系、实例变更趋势、上游系统写入频率分析 • 支持自定义配置相关规则的能力，方便用户定时查看不符合规则的CI信息并支持定时导出

安全风控

提供“云+应用”安全变更风险管控能力。依据数字化业务安全生产《基于云计算的数字化业务安全工程要求》标准，提供事前变更操作风险的识别和评估，事中有效拦截风险，并给出合理的决策措施，最大限度减少由于变更操作导致的系统故障导致的损失，并在事后可审计。

功能模块	功能描述
风险防护策略	• 支持内置高危风险的专家策略 • 支持用户自定义风险防护策略 • 支持防护策略的调试、禁用、克隆、编辑和删除
高危脚本检测	• 支持高危风险的Shell脚本命令的检测 • 支持伪装命令识别检测 • 支持高危语义检测 • 支持恶意脚本混淆检测
封网管控	• 支持自定义封网窗口的新建、编辑、关闭和删除 • 支持封网窗口内的一键放行

风险防护记录	支持风险防护策略检测及高危脚本检测的记录和追溯

17.1.2. 产品价值

应用运维平台具有稳定、高效、智能、开放、降本等产品优势。

稳定

与混合云紧密结合，提供从业务、应用、云服务实例、云平台资源到硬件基础设施5层的“云+应用”一体化运维能力，实现保障业务稳定运行，让企业稳定用云。

高效

与混合云管理平台紧密结合，提供统一入口、统一配置、统一事件管理能力，构建“云+应用”监管控一体化运维能力，实现故障快速发现、定位定界和恢复，让企业高效用云。

智能

贴合运维场景，提供用户维度“云+应用”自动化运维，让企业智能用云。实现应用变更时，无人值守发布异常检测；实现应用运行时，智能异常检测、配置自动推荐、事件智能收敛、容量预测分析、故障根因诊断。

开放

贴合用户视角，基于应用三态模型，提供与行业运维监控产品集成与被集成能力，实现让企业生态用云。

降本

贴合用户视角，提供用户维度“云+应用”一体化数字化运维，实现让企业低成本用云。

17.1.3. 应用场景

应用运维平台致力于“云+应用一体化运维“的用好云场景，即面向应用提供“云+应用”全生命周期管理，面向业务提供“云+应用”监管控一体化运维，让企业管理好云上应用、运维好云上应用。

面向应用“云+应用”全生命周期管理

核心能力

构建应用“逻辑态”、‘部署态“、“运行态“三态纳管能力，实现面向应用“云+应用”全生命周期应用管理。

应用场景

- 传统应用上云管理
- 应用云上架构管理
- 多云场景下应用管理

客户价值

以应用为视角和入口，打通应用运维和云平台运维，实现”云+应用“全生命周期管理，从根源上解决客户应用运维管理体验（稳定、高效、低成本）。

面向业务“云+应用”监管控一体化运维

核心能力

从业务视角，构建从业务、应用、云服务实例、云平台资源到硬件基础设施的“云+应用”监管控一体化运维，保障业务稳定运行。

应用场景

- 专有云场景下，从业务、应用、云服务实例、云平台资源到硬件基础设施的监管控一体化运维
- 行业云多租户场景下，从业务、应用、到云服务实例的监管控一体化运维

客户价值

以应用为视角和入口，打通应用运维和云平台运维，实现”云+应用“监管控一体化运维，实现故障快速发现、快速定位定界、快速恢复，保障业务稳定运行。

18.物联网服务

18.1. 物联网平台

阿里云物联网平台是一个集成了设备管理、数据安全通信和消息订阅等能力的一体化平台。向下支持连接海量设备，采集设备数据上云；向上提供云端API，服务端可通过调用云端API将指令下发至设备端，实现远程控制。

使用物联网平台实现设备完整的通信链接，需要用户自行完成设备端的设备开发、云端服务器的开发（云端SDK的配置）、数据库的创建、手机App的开发。在设备和服务器开发中，用户需完成设备消息的定义和处理逻辑。

18.1.1. 产品详情

物联网平台主要提供设备接入、设备管理、规则引擎等能力，为各类IoT场景和行业开发者赋能。

设备接入

物联网平台支持海量设备连接上云，设备与云端通过IoT Hub进行稳定可靠地双向通信。

- 提供设备端SDK、驱动、软件包等帮助不同设备、网关轻松接入阿里云。
- 提供2G/3G/4G/5G、NB-IoT、LoRaWAN、Wi-Fi等不同网络设备接入方案，解决企业异构网络设备接入管理痛点。
- 提供MQTT、CoAP等多种协议的设备端SDK，既满足长连接的实时性需求，也满足短连接的低功耗需求。
- 开源多种平台设备端代码，提供跨平台移植指导，赋能企业基于多种平台做设备接入。

设备管理

提供完整的设备生命周期管理功能，支持设备注册、功能定义、数据解析、在线调试、远程配置、固件升级、远程维护、实时监控、分组管理、设备删除等功能。

- 提供设备物模型，简化应用开发。
- 提供设备上下线变更通知服务，方便实时获取设备状态。
- 提供数据存储能力，方便用户海量设备数据的存储及实时访问。
- 支持OTA升级，赋能设备远程升级。
- 提供设备影子缓存机制，将设备与应用解耦，解决不稳定无线网络下的通信不可靠痛点。

安全能力

阿里云物联网平台提供多重防护，有效保障设备云端安全。

- 身份认证
  - 提供芯片级安全存储方案（ID²）及设备密钥安全管理机制，防止设备密钥被破解。安全级别很高。
  - 提供一机一密的设备认证机制，降低设备被攻破的安全风险。适合有能力批量预分配设备证书（ProductKey、DeviceName和DeviceSecret），将设备证书信息烧入到每个芯片的设备。安全级别高。
  - 提供一型一密的设备认证机制。设备预烧产品证书（ProductKey和ProductSecret），认证时动态获取设备证书（包括ProductKey、DeviceName和DeviceSecret）。适合批量生产时无法将设备证书烧入每个设备的情况。安全级别普通。
- 通信安全
  - 支持TLS（MQTT\CoAP）数据传输通道，保证数据的机密性和完整性，适用于硬件资源充足、对功耗不是很敏感的设备。安全级别高。
  - 支持设备权限管理机制，保障设备与云端安全通信。

- 支持设备级别的通信资源（Topic等）隔离，防止设备越权等问题。

规则引擎

规则引擎提供数据流转功能，配置简单规则，即可将设备数据无缝流转至其他设备，实现设备联动。

使用规则引擎，用户可以：

- 将数据转发至另一个设备的Topic中，实现设备与设备之间的通信。
- 将数据转发到消息队列（Kafka）中，实现消息的高可靠流转。
- 将数据转发到AMQP服务端订阅消费组，您的服务器可以通过AMQP客户端监听消费组中的消息。

18.1.2. 产品优势

企业基于物联网，通过运营设备数据实现效益提升已是行业趋势和业内共识。然而，物联网转型或物联网平台建设过程中往往存在各类阻碍。针对此类严重制约企业物联网发展的问题，阿里云物联网平台提供了一系列解决方案。

以下是传统开发与基于阿里云物联网平台开发的对比表。

-	传统开发	基于阿里云物联网平台的开发
设备接入	需要搭建基础设施，联合嵌入式开发人员与云端开发人员共同开发。 开发工作量大、效率低。	提供设备端SDK，快速连接设备上云，效率高。 同时支持全球设备接入、异构网络设备接入、多环境下设备接入和多协议设备接入。
性能	自行实现扩展性架构，极难做到从设备粒度调度服务器、负载均衡等基础设施。	具有亿级设备的长连接能力、百万级并发处理能力，架构支撑水平性扩展。
安全	需要额外开发、部署各种安全措施，保障设备数据安全是个极大挑战。	提供多重防护，保障设备数据安全。 • 设备认证保障设备安全与唯一性。 • 传输加密保障数据不被篡改。 • 云盾护航和权限校验保障云端安全。
稳定	需自行发现宕机，并完成迁移。迁移时服务会中断。稳定性无法保障。	服务可用性高达99.9%。去中心化，无单点依赖。拥有多数据中心支持。
简单易用	需要购买服务器搭建负载均衡分布式架构，需要花费大量人力物力开发”接入 + 计算 + 存储”一整套物联网系统。	一站式设备管理、实时监控设备场景、无缝连接阿里云产品。可灵活简便地搭建复杂物联网应用。

18.1.3. 应用场景

物联网平台支持海量设备稳定连接、实时在线，支持云端调用API低延时下发指令，提升各场景中用户体验。

智能家居

物联网平台广泛应用于智能家居电器，以智能插座为例，用户可远程查看插座使用情况，并控制其开关，避免因大功率电器过热，发生危险。

智能音箱

播报音箱接入物联网平台后，用户扫码完成支付后，将支付金额实时通过音箱，向用户和商家进行语音播报。

农业设备

使用各种传感器设备和通信网络，实时监控采集农业大棚中数据。传感器设备可通过RS485总线连接网关，再通过网关将其连接到物联网平台，实现在云端展示和管理数据。

智能媒体屏

媒体屏连接物联网平台后，云上实时感知设备状态，媒体屏实时更新内容，实现媒体屏的智能精细化运营，起到降本增效的作用。

- 云上可管理所有媒体屏，实现新媒体的智能化内容运营。
- 企业服务实例可远程下发媒体内容，大大节省传统媒体屏人工维护成本。
- 实例规格支持灵活扩展，能够支持业务的快速发展。

18.2. 物联网边缘计算

物联网边缘计算，又名Link IoT Edge，是阿里云能力在边缘端的拓展。它继承了阿里云安全、存储、计算、人工智能的能力，可部署于不同量级的智能设备和计算节点中，通过定义物模型连接不同协议、不同数据格式的设备，提供安全可靠、低延时、低成本、易扩展、弱依赖的本地计算服务。

物联网边缘计算，提供的物联网信息一体化解决方案，它囊括了开展边缘端业务所需要的服务器、算法、应用、设备接入能力等。

18.2.1. 产品详情

物联网边缘计算可以结合阿里云的大数据、AI学习、语音等能力，打造出云边端三位一体的计算体系。

边缘实例

边缘实例提供一种类似文件夹的管理功能，用户可以通过实例的方式管理边缘端相关的网关、子设备，同时也可以管理场景联动、函数计算、流数据分析和消息路由内容。通过部署实例，将边缘实例中的资源部署至网关中。

设备接入

物联网边缘计算提供多语言设备接入SDK，让设备轻松接入边缘计算节点。

场景联动

场景联动是规则引擎中，一种开发自动化业务逻辑的可视化编程方式，用户可以通过可视化的方式定义设备之间联动规则，将规则部署至云端或者边缘端。

拖拽可视化组件即可实现多设备的本地管理、联动及控制，每个人都可以成为面向设备不用编程的程序员。

例如，用户可以将“开门”、“开灯”两个操作串联起来，并设置时间区间在18：00至19:00之间，实现在固定时间段，门开灯亮。

边缘应用

边缘应用是一种运行时框架，遵循事件驱动模型，当前产品支持函数计算类型的边缘应用。函数计算是一种运行时（Runtime）框架，可完成设备接入到边缘网关的开发以及基于设备数据、事件的业务逻辑开发。

用户可以使用本地函数计算框架，完成设备接入到边缘网关的开发以及基于设备数据、事件的业务逻辑开发。如：

- 在本地对设备数据做单位换算。
- 在本地对数据进行过滤。
- 在本地将数据转发至本地存储或应用。
- 在本地访问其他服务接口。

消息路由

物联网边缘计算提供消息路由的能力。用户可以设置消息路由路径，控制本地数据在边缘计算节点中的流转，从而实现数据的安全可控。

提供的路由路径如下：

- 设备至IoT Hub
- 设备至函数计算
- 函数计算至函数计算
- 函数计算至IoT Hub
- IoT Hub至函数计算

断网续传

边缘计算节点在断网或弱网情况下提供数据恢复能力。用户可以在配置消息路由时设置服务质量（QoS），从而在断网情况下将设备数据保存在本地存储区，网络恢复后，再将缓存数据同步至云端。

18.2.2. 产品价值

物联网边缘计算平台在接入、成本、安全等各方面具备极大优势。

速接入

通过边缘提供的快速设备接入方案，用户可以通过自己熟悉的语言连接不同协议、不同数据格式的设备。

低延迟

可以在设备所处的本地网络中完成设备数据采集，实现控制策略，在本地对设备数据进行清洗、计算、分析，更实时，更可靠。

低成本

本地数据清洗、计算、过滤可将最优价值的数据上传至云进行存储，减少计算、存储及带宽带来的成本。

高安全

提供云到边缘的安全连接，提供数据加密及安全存储。

弱依赖

可在断网或者弱网环境下运行本地计算、存储、分析。

高智能

提供AI学习、语音识别、视频识别能力，与云能力做结合，提高本地智能化。

18.2.3. 应用场景

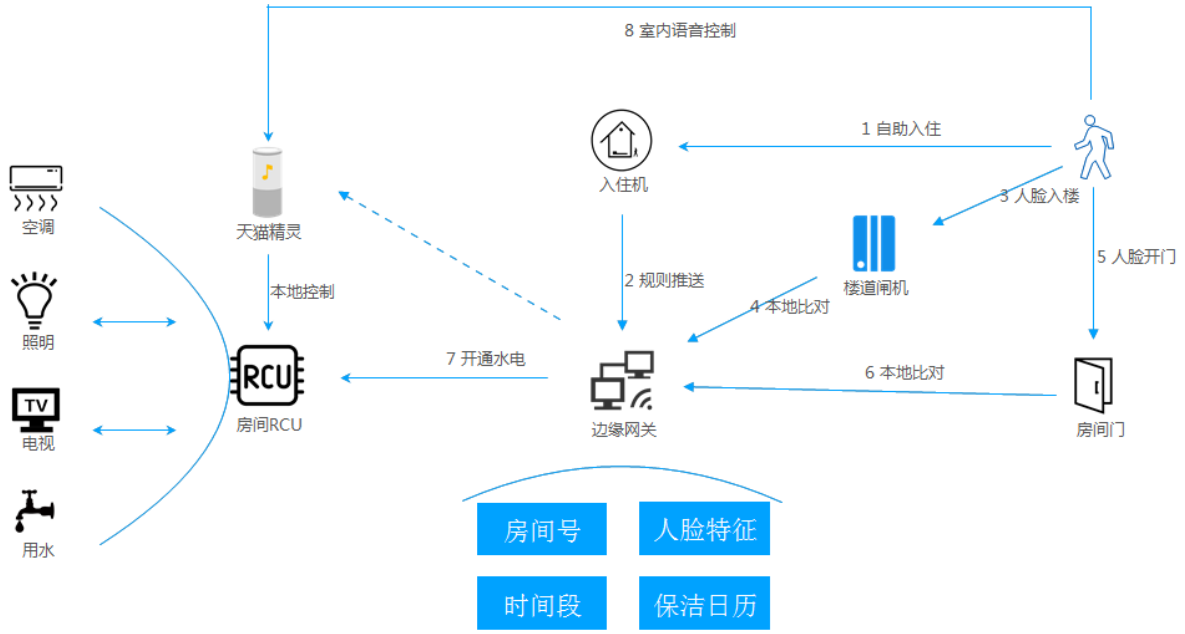
物联网边缘计算平台的典型应用场景有：未来酒店、工业生产、风力发电效率提升等。

未来酒店

通过边缘网关快速集成本地设备后，边缘网关作为本地节点快速响应本地事件，实现本地M2M的智能联动，实现室内室外一体化的语音智能。

特点：

- 设备联动：入楼闸机、房间门、空调、照明、水电等智能联动。
- 边缘计算：人脸信息、房间号、保洁日历、时间段等全部由边缘网关计算处理。
- 语音智能：入住后，天猫精灵成为私人管家，接收住户指令，管理多端设备。



整个场景的运转流程是：

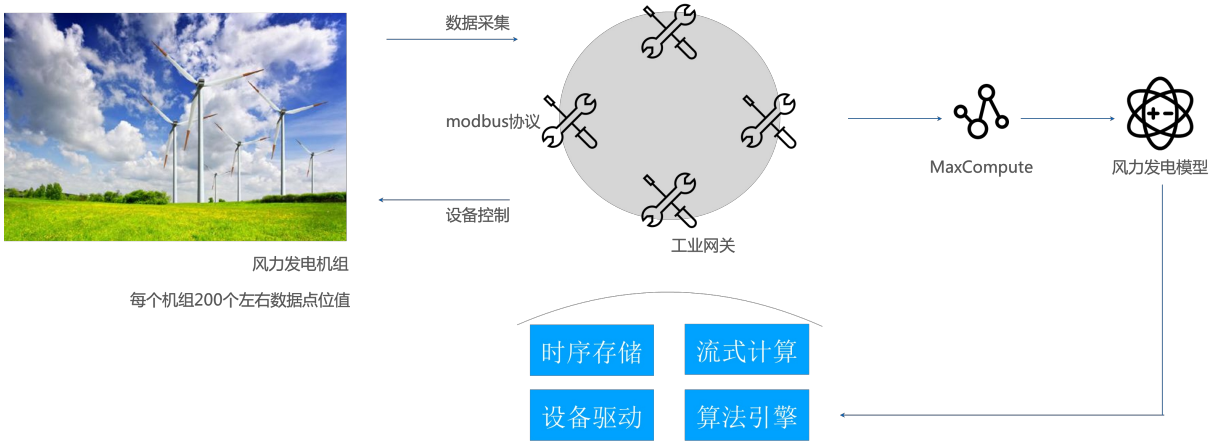
1. 住户自助办理入住，入住机将信息等规则推送给边缘网关。
2. 住户在入楼闸机处刷脸，闸机与边缘网关核对身份信息。
3. 信息核对成功后，闸机打开，住户被允许进入大楼。
4. 住户来到房间门口，刷脸。房间门与边缘网关核对身份信息。
5. 信息核对成功后，房间门打开，住户被允许进入房间。
6. 房间门打开的同时，房间水电、空调、照明、电视等根据环境设置自动开启，天猫精灵开始工作。
7. 住户入住后有其他需求，可以语音将指令需求告知天猫精灵，实现进一步智能联动。

风力发电

在风力发电机组本地网络中，部署边缘计算网关，实时采集机组数据。在本地处理采集的数据后，先将数据上传至阿里云MaxCompute，再使用大数据训练模型后，对发电参数，如风向灵敏度、启动延时参数等做优化。将模型转化为算法或者规则导入本地边缘节点，自动调整风电机组参数，提高机组发电性能。

特点：

- 数据实时采集：多机组多数据点同时采集。
- 大数据处理：数据上传至阿里云后，使用大数据训练模型。
- 即时反馈：算法或规则导入本地边缘节点后，实时自动调整机组参数，实现最优化生产。



18.3. 物联网络管理平台

物联网络管理平台（Alibaba Cloud Link WAN，简称Link WAN），是阿里云面向物联网企业所推出的网管平台，旨在帮助开发者搭建企业物联网络，实现企业级、大容量、高并发的网络专网服务。

Link WAN可与阿里云物联网平台搭配使用，确保物联网平台每个环节的开发者都能轻松实现各自功能，并且拥有可自主管理的物联网无线覆盖区。

18.3.1. 产品详情

物联网络管理平台Link WAN支持LoRaWAN协议的网关与设备接入。

网络管理

用户可将网关关联于自主账号内，实现网络覆盖的服务，Link WAN提供网关管理功能。

网络分享

透过入网凭证的分发，用户可分享自己搭建的网络给其他的阿里云用户，使其设备接入网络上云。

数据出口

可实现对凭证数据的出口统一配置，支持阿里云物联网平台（IoT Platform）配置。

18.3.2. 产品价值

相比自建LoRa平台，物联网络管理平台在各方面都具有优势。

能力	其他LoRa平台	Link WAN (LoRaWAN)
LoRaWAN 国际标准	标准混乱，彼此互不相通，系统维护成本高。	遵循LoRaWAN国际标准协议。
技术领先性	普偏采用开源Demo版本NS自行迭代，对于新协议能力开发，被动演进。	阿里云自主迭代，跟随联盟定义标准，目前支持LoRaWAN 1.0/1.0.2/1.1，Class A/B/C。
性能	自行实现扩展性架构，极难做到从设备粒度调度服务器、负载均衡等基础设施。	具有亿级设备的长连接能力、百万级并发的能力，架构支撑水平性扩展。
安全	需要额外开发、部署各种安全措施，保障设备数据安全是个极大挑战。	基于LoRaWAN AES与阿里云物联网安全通道，双重链路保障。
稳定	需自行发现宕机并完成迁移，迁移时服务会中断。稳定性无法保障。	服务可用性高。发生单点故障，系统自动迁移。

能力	其他LoRa平台	Link WAN (LoRaWAN)
简单易用	需要购买服务器搭建负载均衡分布式架构，需要花费大量人力物力开发“接入 + 计算 + 存储”，自己组建复杂网络管理系统。	一站式网络管理、实时管理覆盖区、无缝连接阿里云产品与物联网平台，用户搭建灵活简便。

18.3.3. 应用场景

物联网络管理平台广泛应用于智能抄表、智能生活、智慧园区等场景。

表计数据采集

随着经济的快速发展，人力成本显著提升，远程智能“水”“电”“煤”表类抄写业务急需升级。基于低功耗广域（LPWA）的物联网连接技术，与抄表应用完美契合，满足垂直行业需求。

低耗设备控制

适合低功耗、低流量的智能生活设备使用，如智能灯泡、智能开关、人体红外(PIR)与呼叫按钮设备，可实现高穿透力、设备长待机、覆盖范围大等等的双向通讯能力。

基础设施控制

物联网络管理平台提供双向通讯与组播能力，适合智能路灯与基础设施的群组管理，借由灯控的电流、电压、与流明参数回传至管理平台，可实现实时控制、能源管理与预测性维修等解决方案。

18.4. IoT设备身份认证

IoT设备身份认证ID²（Internet Device ID），是一种物联网设备的可信身份标识，具备不可篡改、不可伪造、全球唯一的安全属性，是实现万物互联、服务流转的关键基础设施。

18.4.1. 产品详情

ID²为IoT设备在身份标识、认证、数据加密等方面提供诸多核心能力。

设备身份标识

为每个IoT设备提供唯一的身份标识，基于ID²提供双向身份认证服务，防止设备被篡改或仿冒。

安全连接

提供兼容TLS和DTLS的轻量级安全协议，iTLS/iDTLS。这些安全协议更适合物联网设备，在保障安全性的同时大幅减少IoT设备的资源消耗。

业务数据保护

基于设备可信根派生的密钥支持多种加密算法，为设备固件、业务数据、应用授权等敏感数据提供安全防护。

密钥管理

为IoT系统中的设备、应用、业务所使用的密钥提供集中管理，包括密钥生成、密钥销毁、端到端的密钥安全分发。

18.4.2. 产品价值

ID²具有轻量化、高安全、广覆盖的特点，适合在低功耗的物联网设备中使用。

轻量化

使用ID²代替CA证书，即节省存储空间又节省网络资源的消耗。仅连接握手阶段就可以节省70%的网络资源消耗。

高安全

为IoT设备提供云端可信根，基于可信根为上层业务提供可信服务，从源头确保IoT设备的合法性和数据的安全性。

广覆盖

适用于多种安全等级的IoT应用场景，支持不同安全等级的载体（SE、SIM、TEE、secure MCU、软件沙箱）。

18.4.3. 应用场景

ID²在智能门锁、充电桩等场景中都得到充分的应用。

智能门锁的安全认证

帮助智能门锁实现安全的密钥分享、远程开门、关键数据加密、用户身份认证、代码安全升级等高安全等级业务。

充电桩设备的安全认证

帮助智能充电桩设备完成认证和消费前的数据加密。

18.5. IoT安全运营中心

IoT安全运营中心（Link SOC）是立足于终端安全、借鉴成熟的传统安全方案、借助大数据和云计算而产生的，旨在适应物联网环境的、一站式管控、可持续运营的安全管理平台。在设备上可以理解为基于大数据的一种HIPS（Hosted Intrusion Prevention System）实现；在服务上可以理解为一种综合借鉴EDR（Endpoint Detectionand Response）、NTA（Network Traffic Analytics）、MDR（Managed Detection and Response）等安全服务特点，针对物联网场景优化的面向持续运营的安全服务。

18.5.1. 产品详情

阿里云IoT安全运营中心-Link SOC（Security Operations Center）通过对终端行为的持续分析、威胁模型检测等多种方式识别物联网系统中潜在的安全风险，帮助管理员自动处置/响应/修复物联网安全风险，保障物联网系统的安全性，提升设备安全管理效率。

安全检测与告警

评估物联网设备安全管理措施的合规性，提供诊断结果和改进建议，提高物联网设备安全防护水平。

- 常见威胁检测：支持20多项常见威胁的检测
- 等保合规检测：支持基于等保-物联网扩展的专项检测
- 风险告警：支持自定义检测关注的风险，设置告警通知

漏洞扫描和修复

扫描和追踪组系统组件的漏洞，提醒用户漏洞的风险，提供关键漏洞的修复方案，尽可能减少物联网设备面临的安全风险。

- 漏洞扫描：识别潜在的风险漏洞
- 漏洞修复：通过升级组件，完成漏洞修复

威胁感知和阻断

结合安全基线的防护策略实现设备安全管理，通过事件关联分析识别网络层、系统层、应用层的潜在威胁，为管理员提供威胁预警和应急防护措施阻止威胁事件的发生和扩散。

- 持续性监测：提供持续性的安全检测和防护
- 异常感知：支持根据历史行为和群体行为识别风险行为
- 自动处置策略：针对风险进行安全策略自动响应

安全运营托管

通过智能化的安全基线构建、安全风险检测、安全风险评估、动态安全策略防护服务，实现对安全事件的自动响应。

- 自动化安全运营管理：一键完成安全托管，全自动化处理
- 托管报告：定期推送托管运营报告

18.5.2. 产品价值

IoT安全运营中心具有全景掌控、规范发布、持续运营、高质量威胁情报四大产品优势。

全景掌控

统计物联网系统中所有设备安全管理的数据（漏洞、异常、威胁），综合评估物联网安全等级。

规范发布

将安全检测融入到物联网设备安全管理流程，只允许达到安全要求的设备发布。

持续运营

安全运营中心通过持续性的安全监测和防护，大幅缩短从“事件发生—监测异常—响应和处置”的周期。及时遏制风险的扩散，控制风险事件对物联网安全的影响。

高质量威胁情报

安全运营中心为物联网系统提供高质量的安全威胁情报数据，提升安全风险识别的精准度提高物联网设备安全管理的效率。

18.5.3. 应用场景

IoT安全运营中心广泛应用于智能制造、智能城市、智能消费品等场景。

安全基线锁定，智能风险预警

在新制造领域，借助实时数据流计算模型，监控工厂生产的全过程，根据既定的规则给出及时的告警；通过综合的数据分析，提供针对不同业务场景的实时决策能力；辅助工厂生产流程的优化和生产效率的提高。在这些场景中，即使最简单的设备开关机数据落入竞争者手中，都会损害企业的利益。您可以使用Link SOC安全运营中心规定设备安全行为，任何超出规定的异常行为都会触发告警，运营方可以通过相应的操作降低危害。

持续性监测，实时风险处置

随着智能城市的建设，各种各样的传感器和IoT设备信息汇聚到城市平台，大大降低了城市管理者响应突发事件的时间，提升了城市管理质量。但是由于IoT设备的品类繁多，接入地点分散在城市的各个角落，IoT设备安全运营的问题尤其突出。例如空气质量监控设备被侵入，伪造上传的数据有可能造成严重的公共安全事件。Link SOC可以帮助城市运营者管理IoT设备，通过技术手段确认数据来源的合法性，为IoT系统的安全性提供保障，保证了公共安全的同时又为政府的决策提供了可靠的依据。

设备运营托管，智能风险处置

各种智能消费品越来越普及，但普遍缺失安全功能的设计，容易造成使用者的个人数据泄露侵害隐私安全。针对这种情况，设备商可以在Link SOC安全运营中心中定义相关的安全模型，比如当有设备向异常IP地址发送数据时，这个行为会被感知并阻拦，从而保护用户的个人数据。