上交所技术有限责任公司
证通云产品服务白皮书

2020 年 7 月

目 录

一、证通云介绍

1、公司介绍

上交所技术有限责任公司成立于2016年1月4日，为上海证券交易所控股子公司。公司始终秉持“用户至上、赋能行业、技术领先”的价值观念，致力于服务证券交易、服务资本市场，为上交所成为世界领先交易所的核心战略目标服务。主要职能包括：负责上交所信息技术系统及重要技术基础设施的规划、建设和运行保障，维护市场安全平稳高效运行；围绕上交所功能定位，为会员等市场参与者提供技术服务和创新产品服务。

公司前身为上海证券通信有限责任公司。自1997年6月证通公司成立以来，历经20余年的发展，公司向组织架构合理、基础设施先进、制度流程科学、产品技术架构完善的目标逐步迈进。目前公司下设15个管理部门，拥有500人的员工队伍（技术人员占比近80%），向500余家行业用户提供技术服务，累计获得上海市高新技术企业、中国卫星应用产业十佳运营商、上海市科技进步二等奖、自贸区经济贡献百强企业等荣誉、资质，“证通”商标被评为“上海市著名商标”。公司还参股了上证所信息网络有限公司、上海上证数据服务有限责任公司、证通股份有限公司三家公司。

证券市场业务创新的蓬勃发展和信息技术的持续更新换代，对行业技术支持能力不断提出新的要求。公司始终坚持专业、严谨、务实、创新的态度，厚积薄发、精益求精，以更安全可靠的信息网络承载证券市场业务数据传输，以更高效灵活的技术架构支持证券市场转型与发展，以更丰富优质的产品和服务满足证券市场用户成长的深度需求，以更进取向上的社会责任感降低整个证券行业运营成本，推动行业技术进步。

图 1-1-1 上交所技术官网

2、服务介绍

证通云是上交所技术有限责任公司（简称“上交所技术公司”）面向证券、基金等金融机构推出的云服务平台，依托上交所技术公司 T3+数据中心，拥有成熟稳定的云平台技术、完善的用户服务体系及丰富的安全运营管理经验，严格遵循国家相关部门监管政策，为金融机构提供技术领先、稳定可靠、安全合规的云计算服务。通过汇集产业链合作伙伴，证通云发挥“云+”聚合能力，实现产业链深度聚合，为客户提供多维度、多应用、全方位的云产品服务。

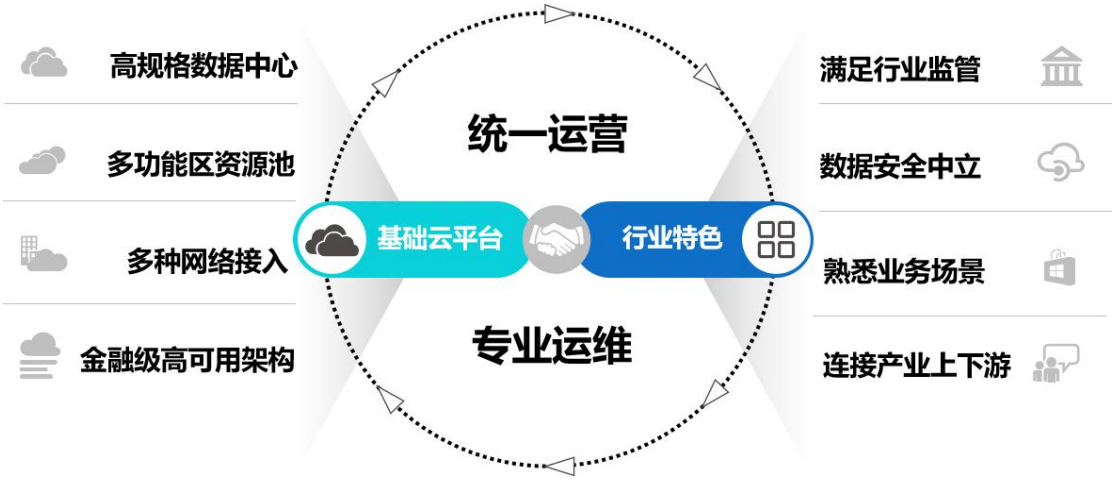


图 1-1-2 证通云-打造证券行业金融云

（1）服务价值

证通云以丰富的产品和服务为依托，以阿里云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，能够帮助企业级用户完成数字化转型。使用证通云服务所带来的服务价值也体现弹性、敏捷、数据和智能四个方面。

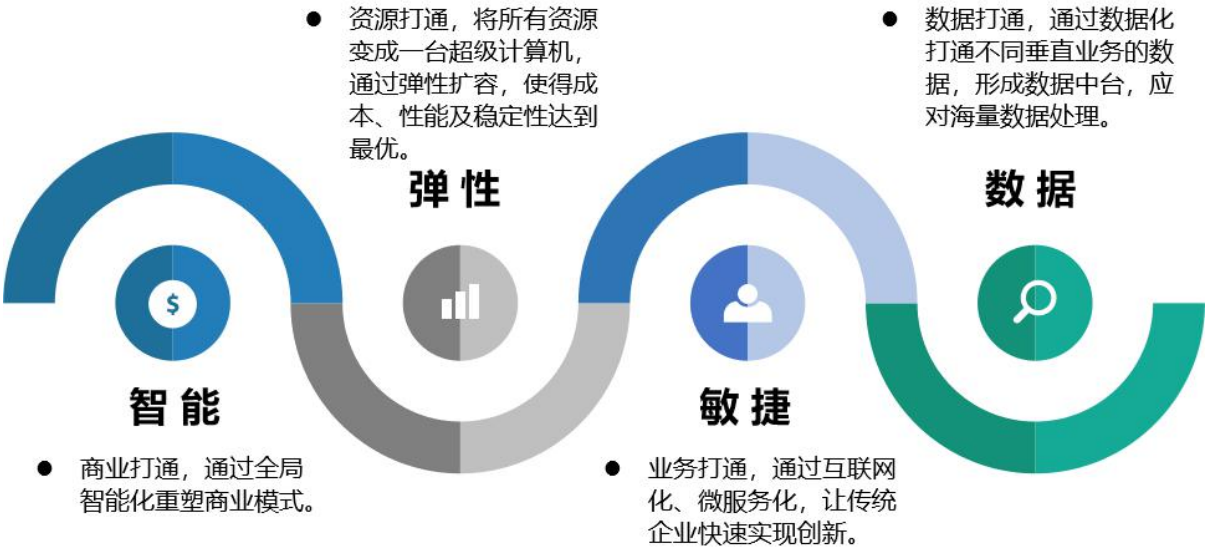


图 1-1-3 证通云服务价值

（2）服务特点

低成本、高弹性、高可用、安全合规，帮助金融客户实现从传统 IT 向云计算的转型。

能够更为便捷的为客户实现与核心机构的对接。

在提供高性能、高可靠、高可用、高弹性的计算能力之外，还能助力金融客户进行业务创新，提升业务竞争力。

证通云可以为金融客户提供优质网络带宽资源，提升互联网用户覆盖范围和用户体验。

能为金融客户提供大规模离线数据处理服务，让客户深入挖掘数据价值。

（3）服务项目

服务项目	产品	资源配置	服务内容
计算类	云服务器（ECS）	计算型虚拟机	具有强大、稳定的计算能力，适用于计算密集型业务需求
		通用型虚拟机	性能均衡，适用于企业通用类业务场景
		组播型虚拟机	具有强大、稳定的计算能力支持组播传输，主要用于组播行情接收、转发场景
		GPU 型虚拟机	适用于深度学习、科学计算、专业图像处理等场景
		普通云盘	分布式文件系 性能均衡。适用于企业通用类业务场景 适用场景：开发与测试业务、系统盘（不支持组播型虚拟机） IOPS：3000 、吞吐量：100 MBps、容量：32768 GiB
		高效云盘	分布式文件系统 性能均衡，适用于计算密集型业务需求 适用场景：开发与测试业务、系统盘、弹性扩容，快照备份 IOPS：5000 、吞吐量：140 MBps、容量：32768 GiB
		SSD 云盘	分布式文件系统和高性能存储，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 适合场景：I/O 密集型应用，中小型关系数据库等使用场景 IOPS：25000、吞吐量：300 MBps 容量：32768 GiB
	服务器（Server）	裸金属	提供用户对功能、性能等相对于虚机有特殊要求的物理主机（PC 服务器），对云内虚机形成补充
存储类	存储服务（Store）	对象存储	提供海量、安全、低成本、高可靠的云存储服务，和极高的数据可靠性，容量和处理能力弹性扩展，多种存储类型供选择全面优化存储成本
		NAS 存储	面向证通云 ECS 实例、容器服务等计算节点的文件存储服务，提供标准的文件访问协议，用户无需对现有应用做任何修改，即可使用具备一定容量及性能扩展、单一命名空间、多共享、高可靠和高可用等特性的分布式文件系统
网络类	云上网络	弹性公网 IP	为用户提供云服务器访问互联网或互联网访问的功能，用户可在申请时选择需要的带宽，获取弹性公网 IP 后可直接绑定 ECS 或结合 NAT 网关使用
		专有网络（VPC）	专有网络（Virtual Private Cloud，简称 VPC），能够帮助用户基于证通云构建出一个隔离的网络环境。用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、划分网段、配置路由表和网关等。此外用户可以通过专线/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，实现应用的平滑迁移上云
		负载均衡 SLB	为用户提供对多台云服务器进行流量分发的负载均衡功能，可提高应用系统对外的服务能力，并消除单点故障
		NAT 网关	是一款 VPC 公网网关，在 VPC 环境下构建一个公网流量的出入口，通过自定义 SNAT，DNAT 规则灵活使用网络资源，支持多 IP，支持共享公网带宽

		异地站点传输	异地站点接入产品是为证通云用户在证通云不通城市站点间传输提供的网络传输
	混合云网络	专线代收代付	与三大电信运营商合作，为云内用户提供高速、稳定的电信、联通、移动线路服务。云内用户点对点专线从外部接入上交所技术证通云，用户可委托我公司向运营商申请线路
		VSEP 接入	通过数据中心内部网络，满足云内用户与数据中心用户、广域网线路间的数据传输需求
		FDEP 接入	提供云内用户与深证 FDEP 系统的接入通道
		证联网接入	提供证联网的接入通道
		沪深报盘、行情	提供上交所委托报单、接收 level-1 行情数据 、接收成交回报、清算数据及接入中登 PROP 系统的网络接入。提供深交所交易行情业务的备用传输通道
		B 转 H 报盘、行情	为云内用户提供千兆局域网接入点，开通深交所 B 转 H 股业务，实现与特定（多个）市场核心机构之间的网络路由，满足用户相关业务需求
安全服务	云安全	运维审计	堡垒机软件授权：为用户提供堡垒机，基于协议正向代理实现，通过正向代理的方式实现对 SSH 、Windows 远程桌面、及 SFTP 等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维审计的目的
		云盾	云盾是集合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，可有效保护证通云用户云平台、云网络环境和云业务系统的安全
		镜像站	YUM 源服务：提供 Yum 源镜像站服务，方便云内用户更新 Linux 系统补丁
		补丁更新	Windows 补丁：提供 Windows 补丁更新服务，方便云内用户更新 Windows 系统补丁,提升用户体验
	数据安全	加密	加密服务基于国家密码局认证的硬件加密机，提供了云上数据加解密解决方案，用户能够对密钥进行安全可靠的管理，也能使用多种加密算法来对云上业务的数据进行可靠的加解密运算
数据库	RDS	MySQL 版	数据库 MySQL 版支持直接挂载只读实例，分担主实例读取的压力。MySQL 版数据库的主实例和只读实例都具有独立的连接地址，当您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，实现了自动的读写分离
		Redis 版	Redis 是基于开源的 Redis 二次开发，兼容开源 Redis 协议的在线 Key-Value 存 储服务。其硬件和数据部署在云端，有完善的基础设施、网络安全保障和系统维护服务
		MongoDB 版	MongoDB:基于天分布式系统和高可靠存储引擎的在线数据库服务，可提供多节点副本集高可用架构、弹性扩容、容灾、备份回滚、性能优化等解决方案
		Hbase 版	Hbase 面向大数据领域的一站式 NoSQL 服务，适用于 GB 至 PB 级的大规模吞吐、检索、分析工作负载

大数据	大数据计算	实时计算	大数据离线计算称为 E-MapReduce，是运行在云平台上的一种大数据处理的系统解决方案。E-MapReduce 构建于云服务器 ECS 上，基于开源的 Apache Hadoop 和 Apache Spark，可以方便地使用 Hadoop 和 Spark 生态系统中的其他周边系统来分析和处理自己的数据。不仅如此，E-MapReduce 还可以与其他的云数据存储系统和数据库系统进行数据传输
		数据总线	云流数据处理平台 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）和分发功能，可以轻松构建基于流式数据的分析和应用。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实时计算引擎来处理写入到 DataHub 的流式数据，并产出各种实时的数据处理结果。DataHub 服务也提供分发流式数据到各种云产品的功能，目前支持分发到 MaxCompute（原 ODPS），OSS 等
		数据中台	数据中台称为 DataWorks，为用户提供数据集成、数据开发、数据地图、数据质量和数据服务等全方位的产品服务，一站式开发管理的界面，帮助企业专注于数据价值的挖掘和探索。其支持多种计算和存储引擎服务，并且支持用户自定义接入计算和存储服务，可为用户提供全链路智能大数据及 AI 开发和治理服务。用户可以使用数据中台，对数据进行传输、转换和集成等操作，从不同的数据存储引入数据，并进行转化和开发，最后将处理好的数据同步至其它数据系统
		搜索与分析	Elasticsearch 简称 ES，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，可以使用户快速的近乎于准实时的存储、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需求强大应用的基础引擎或技术
增值类服务	其他设施类	混合云部署	满足用户灵活放置私有设备的需求，使整个系统的设备相对集中，方便运维管理
		USB key	提供客户 USB Key 设备接入服务,满足虚机应用系统访问 USB Key 硬件设备的需求
		呼叫中心	满足用户对呼叫中心网关设备的需求，使整个系统的设备相对集中，方便运维管理
	VPN 服务	深信服	提供用户云内 VPN 服务，以镜像方式提供 VPN 服务（深信服、华耀、山石），基于 internet，通过加密通道的方式实现用户数据中心与云内资源互通
		华耀	
		山石	

（4）服务合规

证通云按照证监会和银保监会的合规标准建设，在安全性、服务可用性和数据可靠性等方面作了大幅增强。

建设和管理参照的行业标准有：

- 《中华人民共和国金融行业标准 JR/T 0167-2018 云计算技术金融应用规范安全技术要求》
- 《中华人民共和国金融行业标准 JR/T 0166-2018 云计算技术金融应用规范技术架构》
- 《中华人民共和国金融行业标准 JR/T 0168-2018 云计算技术金融应用规范-容灾》
- 《证券公司网上证券信息系统技术指引》
- 《证券期货业信息系统安全等级保护测评要求》
- 《金融业信息系统机房动力系统测评规范》
- 《金融行业信息系统信息安全等级保护测评指南》
- 《银行业信息系统灾难恢复管理规范》
- 《网上银行系统信息安全通用规范》
- 《商业银行业务连续性监管指引》
- 《银行业金融机构信息科技外包风险监管指引》
- 《保险信息安全风险评估指标体系规范》
- 《保险公司信息系统安全管理指引（试行）》

……

3、整体架构

证通云为金融用户提供可以实现同城双中心与异地三中心的高等级绿色数据中心，数据中心位于上海（金桥、宁桥、外高桥）和北京（安外）

两个地域，作为整个平台的基础设施。其中上海地域有三个可用区，北京有一个可用区。

证通云面向中大型企业客户的全栈云平台，基于证通云产品的分布式架构，针对企业级市场的使用特点，为客户提供一个开放、统一、可信的企业级云平台。部署包括：虚拟化 VM、数据库、存储、中间件、大数据等金融云产品。赋能证券交易行业 IT 体系平稳、有序地切换到新技术体系。金融级别的合规集群保障了容灾能力和稳定性；多运营商 BGP 优质网络接入为全国客户提供了流畅的网络体验，规避了运营商网络之间的互联互通风险。

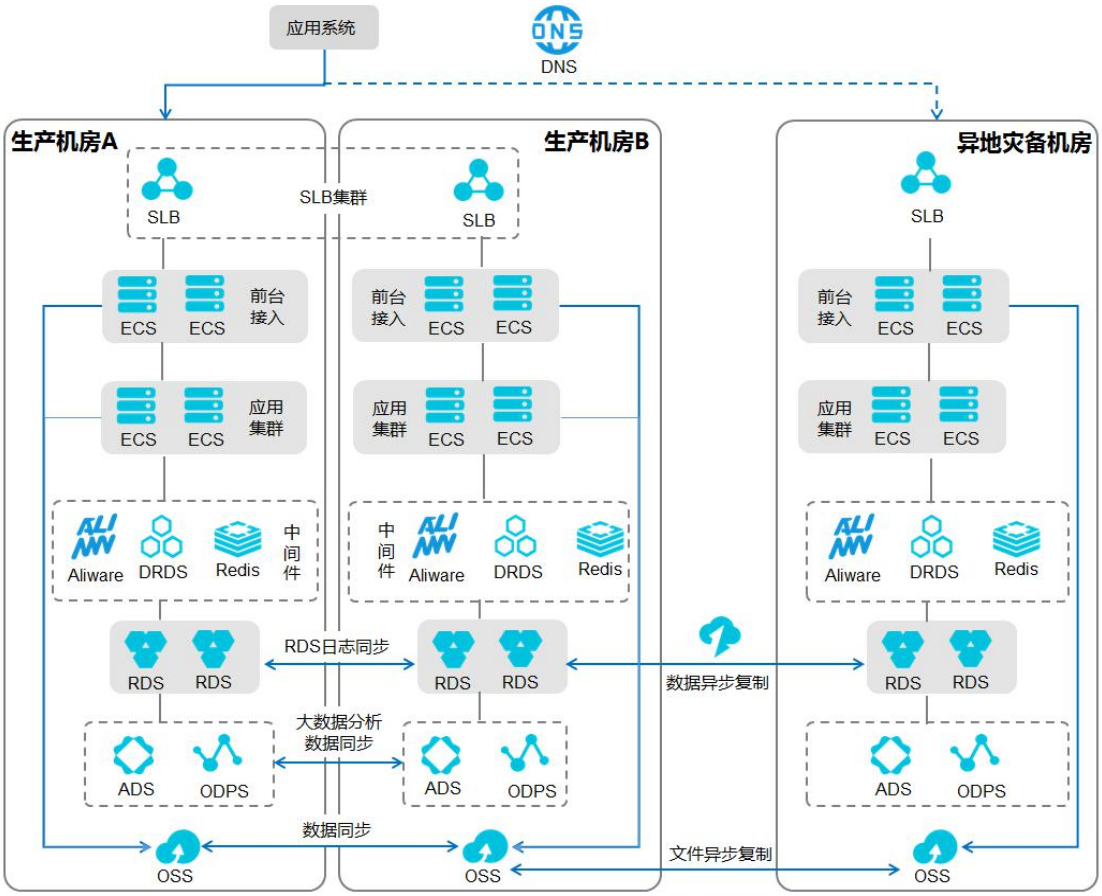


图 1-3-1 证通云技术架构

（1）架构说明

ECS 和 RDS 支持实时弹性扩展，以应对预期或突发的业务爆发及性能压力。

云上方案优化企业资金分配，根据业务量支出费用，且计算、存储成本低，让企业大胆开拓不易预测的创新业务。新业务试错成本小，成功时架构扩展方便。

通过证通云骨干网络分发，降低访问延时，增加访问稳定性。

（2）架构优势

① 证通云上海金桥站点、上海宁桥路站点与行情同站点

② 多高等级机房部署，服务多地域，支持同城容灾与两地三中心

③ 简化系统结构

④ 支持快速扩容

⑤ 系统开发周期短

⑥ 优质多线 BGP 保障网络服务

⑦ 中间件和数据库稳定可靠

4、产品优势

证通云计算是将一些可以自我维护和管理的虚拟计算资源整合在平台集群中，包括计算服务器、存储服务器和宽带资源等，并通过自动化运维方式实现任务调度、自动管理、无人介入生产等。用户可以动态申请部分资源以支持各种应用程序的运转，省去了购买网络设备和服务器、租用机柜等烦恼，从而集中精力开拓业务，有利于提高效率、降低成本和技术创新。 证通云计算对比传统自建 IT 基础设施和托管有如下优势：

超大的集群规模。证通云计算集群具有能够适应海量计算的服务器规模，最大的集群服务器数量达到 5000 台，并可以提供多集群的计算资源，能够为用户提供前所未有的计算能力。

强大的弹性扩展能力。证通云支持客户业务动态伸缩，满足应用和用户规模增长的需要。业务增长时计算、存储资源随之增长，反之则随之下降，让资源使用效率最大化。

按需服务。证通云是一个庞大的资源池，用户购买计算、数据、存储资源可以按需购买，如同使用自来水、电和煤气那样按量计费，不会造成计算资源的闲置和浪费。

成本低廉。证通云的计算架构和特殊容错措施使其可以采用极其廉价的节点来构成云。证通云的自动化管理使数据中心管理成本大幅降低。证通云的公用性和通用性使资源的利用率大幅提升。依托优质的数据中心和网络带宽资源，证通云可以为客户提供极高性价比和极低总体拥有成本的计算服务。

安全稳定。证通云主机、数据库等产品采用了证通云分布式技术，在数据方面对每一份数据分散存储同时保留三份或三份以上镜像，大幅降低数据丢失的可能性。在服务器资源方面，一台云服务器宕机会在 10 分钟内迁移到其他物理服务器启动起来，从而保证系统的可用性。并且提供给用户两地三中心的基础设施来部署有更高可用性和连续性要求的业务系统。

5、与公共云的差异

	项目	公有云	证通云
合规	ISO27001	★	★
	等保级别	等保三级	等保三级
	金融行业合规		★
	ISO20000	★	★
	ISO22301	★	★
安全	DDOS防护	★	★
	堡垒机	★	★
	云防火墙	★	★
产业聚合	核心机构互联		★
	高性能物理区		★

	多运营商专线接入	★	★
	BGP互联网线路	★	★
	组播业务支持		★
可用性	两地三中心	★	★
	同城容灾	★	★
	ECS（SLA）	99.95%	99.97%
	RDS（SLA）	99.95%	99.97%
	SLB（SLA）	99.95%	99.97%
其他	金融监管风险评估调查		★
	金融行业监管报告提交		★
	专线	★	★
	特殊设备混合云		★
	客户准入	开放注册	行业客户
	售后服务	标准	金融商用

6、上云须知

证通云基础资源外包服务主要服务于金融用户，出于合规需求及安全考虑，证通云与公共云在使用和功能上有部分区别，请在使用证通云基础资源外包服务之前仔细阅读本文档。

（1）开放地域

证通云基础资源外包服务是服务于银行、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。

证通云为金融用户提供可以实现两地三中心的高等级绿色数据中心，数据中心位于上海（金桥、宁桥、外高桥）和北京（安外）两个地域，作为整个平台的基础设施。其中上海地域有三个可用区，北京有一个可用区。支持同城双活/灾备架构。

图 1-6-1 证通云站点概览

上海、北京为 VPC 网络环境，用户之间网络隔离。用户 VPC 地址由证通云统一分配，用户可根据自身网络需求规划网络，划分多个 VPC 或 Vswitch。

（2）网络访问限制

在互联网访问上，证通云做了严密的符合金融行业规范的风控措施。

（3）访问控制台

用户访问证通云管理平台需先申请管理 VPN 账号，获取 VPN 访问权限后通过拨入 VPN 访问证通云管理平台进行资源申请，网络创建等操作。

（4）远程运维操作

对 ECS 进行简单运维操作时，用户可拨入 VPN 登陆云管平台通过 VNC 登陆 ECS 进行系统设置等操作，用户如需远程传输文件至 ECS 需通过开通互联网访问功能，通过互联网映射相关端口进行访问。用户也可购买证通云的云内 VPN 产品，部署在用户自己 VPC 中，通过该产品远程管理自己的 ECS。

（5）互联网访问云产品

目前证通云互联网访问带宽可在 EIP 上选取，但是为了安全控制，EIP 地址并非真实的互联网地址，用户 ECS 向互联网提供访问需向证通云提交需求说明，由证通云分配互联网地址并开通互联网访问策略。目前仅用户的 ECS 可开通互联网访问功能，RDS，OSS 等产品不对互联网开放。

二、站点服务

证通云站点位于上海与北京两地，分别为上海金桥站点、上海外高桥站点、上海宁桥路站点与北京安定门站点。

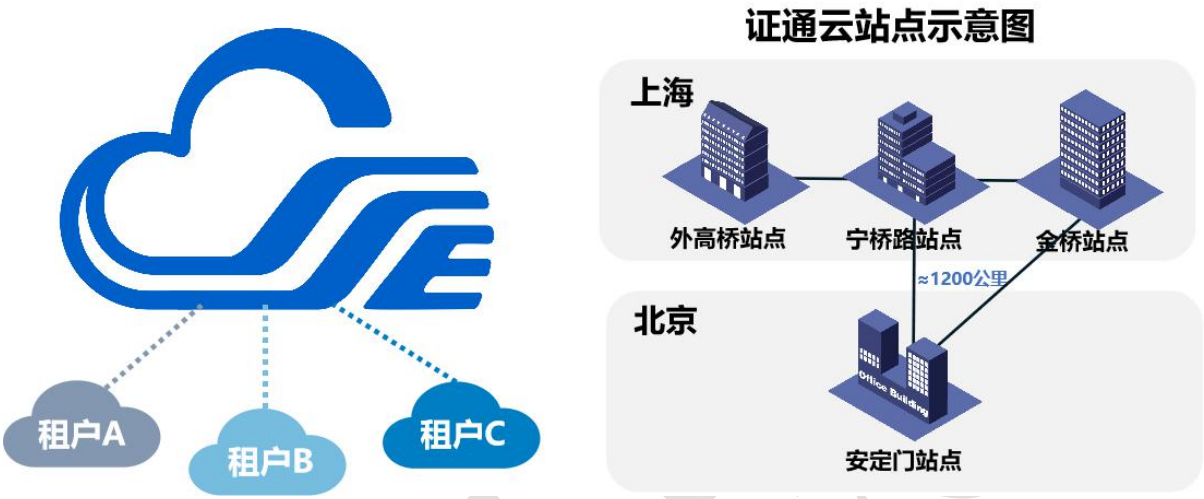


图 2-0-1 证通云站点示意图

1、上海金桥站点

证通云（上海金桥站点）位于上交所技术公司自建数据中心金桥数据中心，园区占地 9.6 万平方米，总建筑面积 22.4 万平方米，其中地上建筑面积 19.2 万平方米，地下建筑面积 3.2 万平方米。数据中心总建筑面积 14 万平方米，净机房面积为 4.7 万平方米，可容纳约 2 万个标准机柜。证通云部署于 D2 机房占有 500 个高密度机柜。为证通云提供基础资源保障。

（1）设计指标

整个数据中心采用三路独立的 110kV 市政电源作为常用电源，分布式冗余架构，以并列运行的模式供电，任意一路市电故障由另外两路分摊故障回路下的用电负荷。项目配备了 N+1 满负荷容量的应急电源柴油发电机系统，采用双母线输出、双回路供油，实现物理隔离。项目采用热通道封

闭、免费制冷及双温双盘管精密空调技术。数据中心配备双冷源、双路管道和双盘管精密空调的 2N 系统架构，确保无单点故障。

金桥数据中心是国内金融业大规模、高标准的行业数据中心，是行业汇聚、国内领先、国际一流的新一代数据中心。GB50174-2017 等级 A 级，UPTIME 等级 Tier Ⅳ（D1-D2）/Tier Ⅲ+（D3-D8），安防等级一级，设计 PUE 不超过 1.6。

（2）功能定位

上交所主运行中心：待交易所主机房迁移金桥后，将提供核心交易、业务操作、交易所网站等功能。

核心机构托管中心：包括中国结算和深交所等，与深交所合作实现链路互备和机房互备。

市场机构托管中心：承担市场机构交易托管及市场机构综合托管两类职能。

行业增值服务中心：提供上证信息公司 LEVEL-2 行情、证联网、核心机构接入网等服务。

（3）地理位置

上海金桥站点位于上海金桥进出口加工区（南区）海关封关区 WH2-3 地块，毗邻川沙路和龙沪路，地址为龙沪路 399 号。

专线接总头编号：

电信：3500-15646 6.1

联通：01T318169

2、上海外高桥站点

证通云（上海外高桥站点）位于上交所技术公司自建数据中心证券技术大厦，占地面积 15,600 平米，总建筑面积 28,800 平方米,于 2004 年 12

月奠基，2007 年 1 月正式启用。目前有全国各地 90 余家用户的中心或灾备机房入驻其中，已成为名副其实的证券业数据中心和灾备中心。

（1）设计指标

数据中心大厦场地标准均符合国家 A 级机房标准及国家等保三级要求，其主要参数如下：

供电系统：两路合计上限每平米 2KW，UPS 持续供电时间大于 10 分钟，并备有柴油发电机。

暖通系统：相对湿度为 45%—65%，温度夏季控制在 23℃±2℃、冬季控制在 20℃±2℃。

（2）功能定位

核心机构托管中心：包括中国结算和深交所等，与深交所合作实现链路互备和机房互备。

行业增值服务中心：提供上证信息公司 LEVEL-2 行情、证联网、核心机构接入网等服务。

（3）地理位置

上海外高桥站点位于上海市浦东新区华京路 1 号证券技术大厦，坐落于上海市外高桥保税区内。

专线接入机柜：技术大厦 312 级房 C01 机柜，提供电信、联通、移动三家运营商的广域网专线接入。

3、上海宁桥路站点

证通云（上海宁桥路站点）位于上交所技术有限公司与中国联通合作数据中心。宁桥路数据中心位于上海市宁桥路 801 号，目前位于园区内二期、三期两栋大厦中，分别处于二期 3 楼、二期 6 楼以及三期 6 楼，机柜

总量为 762 个；并在二期 6 楼、三期 6 楼配有用户坐席区，可供用户在其办公。

（1）设计指标

市电容量充沛，能满足整栋大楼 IDC 业务需求，为扩展业务提供有力保障；

非同路由 2 路市电从附近不同变电站引入，安全系数高，为安全生产提供有力保障；

配电系统：10KV 到各楼层。35KV 至 10KV、10KV 至 0.4KV、二级配电柜至三级配电柜等各级变电、配电设备均使用 2N 系统配置；

柴油发电机 N+1 台备份。满足国标 50174 中 A 级要求，满足 TIA942 中 TIA942 中 T4 等级要求；

UPS 系统：机房按照 2N、2（N+1）系统配置 UPS，满足 TIA942 中 T4 等级机房需求。

电力系统持续供电可用性达 99.995%

（2）功能定位

行业增值服务中心：提供上证信息公司 LEVEL-2 行情（待定）、证联网、核心机构接入网等服务，与深交所合作实现链路互备和机房互备。

（3）地理位置

上海宁桥路站点位于上海市宁桥路 801 号中国联通金桥数据中心园区内上海市宁桥路 801 号。

专线接入机柜：宁桥路 3 期 5C 机房 03-23 机柜，提供电信、联通的广域网专线接入。

4、北京安定门站点

安定门联通 IDC 机房由网聚无限完全独立自主运营，是中国联通北京分公司按照 TIER3 国际标准倾力打造，于 2013 年 9 月建成的全新数据中心，内部等级四星级+，优质硬件基础设施，配套休息区、检验区、调测区，集结完美运营为一体的大型运营商数据中安定门联通 IDC 机房地理位置优越。

（1）设计指标

机房总面积达 2000 余平方米；总计 380 个机架，标准 42U 机架，机房架高地板的承重为 1000kg/sqm，整体抗地震级别达 8 级，采用大小模块组设计，具备单独隔离功能，VIP 独享区域。

安定门联通 BGP 机房供电由华北、华中、东北三大电网分别接入，总电量为 5000KVA，每机柜最高电力容量为 13A，为保障分配给用户的电力不间断的供应，数据中心电力机房安装了智能 UPS 系统及容量充足的电池，可以保证持续供电；配电系统的敷设方式为通过机柜上方的开放式桥架走线，每机柜的电缆线径不小于 4mm。此外，数据中心还配备 3 台应急发电机组，当电力中断时使用，可为用户提供 99.99%的电力供应保障。

（2）功能定位

行业增值服务中心：提供上证信息公司 LEVEL-2 行情（待定）、证联网、核心机构接入网等服务，与深交所合作实现链路互备和机房互备。

（3）地理位置

北京安外站点位于北京北二环安定门外大街 59-1，机房处于北京安定门外大街，北二环至北三环之间位于北京城区绝佳的地理位置。

专线接入机柜：5 楼数据中心 K01 机柜和 L01 机柜，提供电信和联通的广域网专线接入。

三、计算类服务

1、云服务器 ECS

云服务器 ECS（Elastic Compute Service）是一种弹性可伸缩的计算服务，助用户降低 IT 成本，提升运维效率，使用户更专注于核心业务创新。现分为以下几种类型服务。

（1）功能特性

云主机租用：用户可根据需要租用不同配置的云主机，操作系统支持主流的 Linux、Windows 系统，也可以使用自定义镜像创建云主机。用户申请的云主机可部署在不同的数据中心可用区。

快照管理：支持云主机快照和快照恢复功能，为云主机做重大业务变更或定期做快照，方便回滚。

自定义镜像：支持自定义镜像创建、并根据自定义镜像创建新主机。

用户完全管控：可通过 web 服务控制台对云主机做开机、关机、重启、查询初始密码、快照、远程 VNC、挂载/解挂弹性块/文件存储、绑定公网。

多网卡管理：云主机可配置多块网卡。

安全组管理：复用安全组，每次创建新云主机时可选择已创建的安全组，安全组规则修改不影响正在使用该安全组的云主机，快捷方便；用户亦可创建自定义安全组规则。

云主机监控：用户可实时查看云主机的 CPU、内存、磁盘 IO、网络 IO 情况。

（2）产品优势

与普通的 IDC 机房或服务器厂商相比，云服务器 ECS 具有以下优势：

① 高可用性

相较于普通的 IDC 机房以及服务器厂商，使用更严格的 IDC 标准、服务器准入标准以及运维标准，以保证云计算整个基础框架的高可用性、数

据的可靠性以及云服务器的高可用性。当需要更高的可用性时，可以利用多可用区搭建自己的主备服务或者双活服务。对于面向金融领域的两地三中心的解决方案，也可以通过多地域和多可用区搭建出更高的可用性服务。其中包括容灾、备份等服务，证通云都有非常成熟的解决方案。

② 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。证通云近期通过了信息安全等保三级认证在安全合规上对于用户数据的私密性、用户信息的私密性以及用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。只需进行简单配置，就可在自己的业务环境下，与全球所有机房进行联接，从而提高了业务的灵活性、稳定性以及可扩展性。对于原来拥有自建的 IDC 机房，也不会产生问题。

证通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。证通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，让业务更加灵活。结合证通云的生态，可以在云上发展出意想不到的业务生态。

专有网络更加稳定和安全。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。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，它们将获得云计算所带来的技术红利。

③ 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。传统 IDC 模式下，很难做到对单个服务器进行快速变更配置。而对于证通云，云服务器或者存储的容量可以根据业务量的增长或者减少自由变更自己的配置。横向的弹性，即对于业务的高峰期，若在传统的 IDC 模式下，将无法立即准备资源；而云计算却可以使用快速弹性的方式帮助客户度过这样的高峰。当业务高峰消失时，可以将多余的资源释放掉，以减少业务成本的开支。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：证通云拥有很强的存储弹性。当存储量增多时，对于传统的 IDC 方案，只能不断去增加服务器，而这样扩展的服务器数量是有限的。在云计算模式下，将提供海量的存储，当需要时可以直接创建，为存储需求提供最大保障。

网络弹性：云上的网络也具有非常大的灵活性。当选择了证通云的专有网络，所有的网络配置策略与线下 IDC 机房配置策略可以是完全一致的，并且可以拥有更多的灵活性。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便捷。

总之，对于证通云的弹性而言，是计算的弹性、存储的弹性、网络的弹性以及对于业务架构重新规划的弹性。可以使用任意方式去组合自己的业务，证通云都能够满足需求 。

（3）产品规格

① 计算型虚拟机

计算型虚拟机具有强大、稳定的计算能力，主要适用于计算密集型业务需求。

② 通用型虚拟机

通用型虚拟机性能均衡，适用于企业通用类业务场景。

③ 组播型虚拟机

组播型虚拟机主要用于组播行情接收、转发场景。

④ GPU 型虚拟机（仅金桥站点支持）

支持 GPU 计算，适用于深度学习、科学计算、专业图像处理等场景。

（4）应用场景

ECS 应用非常广泛，既可以作为简单的 Web 服务器单独使用，也可以与其他证通云产品（如 OSS、RDS 等）搭配提供强大的多媒体解决方案。以下是云服务器 ECS 的典型应用场景。

① 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 即可运行应用程序、数据库、存储文件等。随着网站发展，您可以随时提高 ECS 的配置，增加 ECS 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。

② 多媒体、大流量的 app 或网站

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

③ 访问量波动大的 app 或网站

某些应用访问量可能会在短时间内产生巨大的波动。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。

④ 数据库

支持对 I/O 要求较高的数据库。使用较高配置的 I/O 优化型 云服务器 ECS，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 服务器，搭配负载均衡，实现高可用架构。

⑤ 行情接收

组播型虚拟机支持接收组播行情数据，包括上交所的高速行情网和深交所的新一代交易系统发送的组播行情。接收上游组播行情后只需和原来系统内部的交易服务器打通路由即可。

⑥ GPU 场景

GPU 型虚拟机是基于 GPU 应用的计算服务，多适用于视频解码，图形渲染，深度学习，科学计算等应用场景，该产品具有实时高速，并行计算跟浮点计算能力强等特点。

2、块存储

（1）功能特性

查询：查询用户申请的弹性块存储信息；查询弹性块操作记录。

创建：弹性块创建；计费扣费。

基本操作：名称修改；加载到主机；从主机卸载。

销毁、续订：块存储销毁；块存储续订。

（2）产品优势

① 节约成本

无需采购存储设备，存储空间可自由定制，产生的费用按弹性块存储的使用时间和使用容量来计算。

② 灵活部署

创建后即可对弹性块存储进行挂载实现快速部署，每块弹性块存储可以挂载到任意一台云主机上，两者具有不同的生命周期。当云主机被删除时，弹性块存储数据仍然存在，并可以挂载到其它的云主机上继续使用。

③ 按需使用

客户可申请多个弹性块存储，客户可以随着业务的增大对块存储弹性扩展存储空间，也可以为云主机挂载更多的弹性块存储，不再使用时可通过简单的 web 操作进行删除。

（3）产品规格

① 普通云盘

分布式文件系 性能均衡。适用于企业通用类业务场景。

适用场景：开发与测试业务、系统盘。

最大 IOPS:3000、吞吐量：最大 100 MBps。

② 高效云盘

分布式文件系统 性能均衡，适用于计算密集型业务需求。

适用场景：开发与测试业务、系统盘、弹性扩容，快照备份。

最大 IOPS:5000、最大吞吐量:140 MBps。

③ SSD 云盘

分布式文件系统和高性能存储，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。

适合场景：I/O 密集型应用，中小型关系数据库等使用场景。

最大 IOPS:25000、最大吞吐量:300 MBps 。

	普通云盘	高效云盘	SSD 云盘
最大 IOPS	3000	5000	25000
最大吞吐量	100Mbps	140Mbps	300Mbps

3、云服务器功能服务

① 弹性网卡

为用户提供云服务器 ECS 除默认网卡外新增网卡的功能，用户可创建弹性网卡，与 ECS 实例绑定或从实例中分离。

② 快照

快照是云盘数据在某个时刻完整的只读拷贝，是一种便捷高效的数据容灾手段，常用于数据备份、制作自定义镜像、应用容灾等。

③ 镜像

ECS 镜像提供了创建 ECS 实例所需的信息。创建 ECS 实例时，必须选择镜像。镜像文件相当于副本文件，该副本文件包含了一块或多块云盘中的所有数据，对于 ECS 而言，这些云盘可以是单块系统盘，也可以是系统盘加数据盘的组合。

④ 安全组

安全组规则，可以允许或者禁止，ECS 实例的外网和内网的出入方向的访问。可以随时授权或取消安全组规则。您的变更安全组规则会自动应用于与安全组相关联的 ECS 实例上。

在设置安全组规则时，安全组的规则务必简洁。如果您给一个实例分配多个安全组，则该实例可能会应用多达数百条规则。访问该实例时，可能会出现网络不通的问题。

4、服务器（Server）

（1）物理机

提供用户对功能、性能等相对于虚机有特殊要求的物理主机（PC 服务器），提供较高的物理安全隔离，对云内虚机形成补充。

使用场景：用户上云可能会存在多种形态的计算资源，某些情况下虚拟机无法满足复杂的应用场景，这时候可能就需要需要虚拟机和物理机相结合的场景，如数据库及高性能应用服务器。

（2）集中式存储

满足用户高性能、高安全性存储的需求，集中式存储系统性能相对稳定，性能抖动较小，适合数据库等对性能、安全性要求较高的应用场景。采用双控结构、SSD 分层技术以提升系统整体可靠性和性能。

四、存储类服务

1、对象存储

对象存储提供海量、安全、低成本、高可靠的云存储服务，和极高的数据可靠性。容量和处理能力弹性扩展，多种存储类型供选择全面优化存储成本。

对象存储服务（Object Storage Service，简称 OSS）提供的海量、安全、低成本、高可靠的云存储服务。

OSS 可以被理解成一个即开即用，无限大空间的存储集群。相比传统自建服务器存储，OSS 在可靠性、安全性、成本和数据处理能力方面都有着突出的优势。使用 OSS，您可以通过网络随时存储和调用包括文本、图片、音频和视频等在内的各种非结构化数据文件。

OSS 将数据文件以对象/文件（Object）的形式上传到存储空间（Bucket）中。OSS 提供的是一个 Key-Value 键值对形式的对象存储服务。用户可以根据 Object 的名称（Key）唯一地获取该 Object 的内容。

对象存储提供海量、安全、低成本、高可靠的云存储服务，和极高的数据可靠性。容量和处理能力弹性扩展，多种存储类型供选择全面优化存储成本。

（1）功能特性

类别	功能	描述
存储空间	创建存储空间	在上传任何文件到 OSS 之前，您需要首先创建存储空间来存储文件
	删除存储空间	如果您不再需要存储空间，请将其删除以免进一步产生费用
	修改存储空间读写权限	OSS 提供权限控制 ACL（Access Control List），您可以在创建存储空间的时候设置相应的 ACL 权限控制，也可以在创建之后修改 ACL
	设置静态网站托管	将存储空间配置成静态网站托管模式，并通过存储空间域名访问该静态网站
	设置防盗链	为了减少您存储于 OSS 的数据被其他人盗链而产生额外费用，OSS 支持设置基于 HTTP header

		中表头字段 referer 的防盗链方法
	管理跨域资源共享	OSS 提供 HTML5 协议中的跨域资源共享 CORS 设置，帮助您实现跨域访问
生命周期	设置生命周期	定义和管理存储空间内所有对象或对象的某个子集的生命周期。设置生命周期一般用于文件的批量管理和自动碎片删除等操作
对象（文件）	上传文件	您可以上传任意类型文件到存储空间中
	新建文件夹	您可以像管理 Windows 文件夹一样管理 OSS 文件夹
	搜索文件	在存储空间或文件夹中搜索具有相同的名称前缀的文件
	获取文件访问地址	通过获取已上传文件的地址进行文件的分享和下载
	删除文件	删除单个文件或批量删除文件
	删除文件夹	删除单个文件夹或批量删除文件夹
	修改文件读写权限	您可以在上传文件的时候设置相应的 ACL 权限控制，也可以在上传之后修改 ACL
	管理碎片	删除存储空间内的全部或部分碎片文件

（2）产品优势

OSS 与自建存储对比的优势

对比	对象存储 OSS	自建服务器存储
可靠性	• 规模自动扩展，不影响对外服务 • 数据自动多重冗余备份	• 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，支持同城容灾 • 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 具备的其他各项优势

① 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。

- 不限文件数量和大小。您可以根据所需存储量无限扩展存储空间，解决了传统硬件存储扩容问题。

- 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。

② 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。

③ 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。

（3）使用限制

限制项	说明
存储空间（bucket）	• 同一用户创建的存储空间总数不能超过10个 • 存储空间一旦创建成功，名称和区域不能修改
上传文件	• 通过控制台上传、简单上传、表单上传、追加上传的文件大小不能超过5GB，要上传大小超过5GB的文件必须使用分片上传(Multipart Upload）上传方式。分片上传方式上传的文件大小不能超过48.8TB • OSS支持上传同名文件，但会覆盖已有文件
删除文件	• 文件删除后无法恢复 • 控制台批量删除文件的上限为50个，更大批量的删除必须
生命周期	每个存储空间的生命周期配置最多可容纳1000条规则
图片处理	• 对于原图： - 图片格式只能是：jpg、png、bmp、gif、webp、tiff。 - 文件大小不能超过20MB - 使用图片旋转或裁剪时图片的宽或者高不能超过4096PX。 • 对于缩略后的图： - 宽与高的乘积不能超过4096x4096 - 单边长度不能超过4096 PX

（4）应用场景

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

依靠低成本、高可用的 OSS 对象存储，可以将企业内部长期需要离线归档的数据转存至 OSS。

2、NAS 存储

面向证通云 ECS 实例、容器服务等计算节点的文件存储服务，提供标准的文件访问协议，用户无需对现有应用做任何修改，即可使用具备一定容量及性能扩展、单一命名空间、多共享、高可靠和高可用等特性的分布式文件系统。

NAS 后端基于分布式存储，数据三副本分布存储于多台盘古节点上。前端访问节点接受 NFS 客户端的连接请求和提供 Cache 功能，自身是无状态和分布式部署，保证前端的高可用。

NAS 的 Metadata 数据保存在 MetaServer 上，前端机的 I/O 请求在用 MetaServer 获得 NAS 的 Metadata 后，User Data 的读写直接到后端盘古数据节点。

架构上前后端可以单独弹性扩展，在保证高可用的前提下，做到吞吐的高并发和低时延。

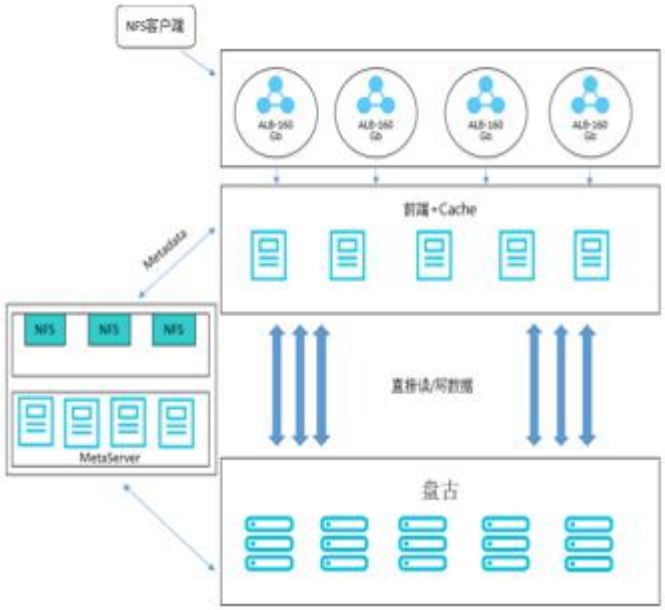


图 4-2-1 NAS 存储示意图

（1）功能特性

① 无缝集成

NAS 支持 NFSv3 及 NFSv4 协议，并使用标准的文件系统语义访问数据。主流的应用程序及工作负载无需任何修改即可无缝配合使用。

② 共享访问

一个 NAS 文件系统实例可以被多个计算节点同时访问，非常适合跨多个 ECS、容器服务实例部署的应用程序访问相同数据来源的应用场景。

③ 安全控制

NAS 具有网络隔离（专有网络）/用户隔离（经典网络）、文件系统标准权限控制、权限组访问控制和 RAM 主子账号授权等多种安全机制，从而保证文件系统数据安全。

④ 线性扩展的性能

NAS 能够为应用工作负载提供高吞吐量与高 IOPS、低时延的存储性能，同时，其性能与容量成线性关系，可满足业务增长时对更高容量与存储性能的诉求。

（2）产品优势

① 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。

② 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。

③ 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。

④ 高性能

单个文件系统吞吐性能随存储量线性扩展，相比购买高端 NAS 存储设备，大幅降低成本。

⑤ 易用性

支持 NFSv3 和 NFSv4 协议，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。

（3）使用限制

文件存储 NAS目前支持 NFSv3 和 NFSv4 协议。

NFSv4.0 和 NFSv4.1 不支持的 Attribute 及客户端上显示的错误如下表所示：

协议	不支持的Attribute	显示错误
NFSv4.0	FATTR4_MIMETYPE, FATTR4_QUO TA_AVAIL_HARD, FATTR4_QUOTA_AVAIL_SOFT, FATTR4_QUOTA_USED, FATTR4_TIM E_BACKUP, FATTR4_TIME_CREATE	NFS4ERR_AT TRNOTSUPP
NFSv4.1	FATTR4_DIR_NOTIF_DELAY, FATTR4_DIR ENT_NOTIF_DELAY, FATTR4_DACL, FATTR4_SACL, FATTR4_CHANGE_POLICY, FATTR4_FS_STATUS, FATTR4_LAYOUT_HINT, FATTR4_LAYOUT_TYPES , FATTR4_LAYOUT_ALIGNMENT, FATTR4_FS_LOCATIONS_INFO, FATTR4_MDS THRESHOLD, FATTR4_RETENTION_GET,	NFS4ERR_AT TRNOTSUPP

	FATTR4_RETENTION_SET，FATTR4_RETENTEVT_GET， FATTR4_RETENTEVT_SET，FATTR4_RETENTION_HOLD， FATTR4_MODE_SET_MASKED，FATTR4_FS_CHARSET_CAP	

此外，NFSv4 不支持的 OP 包括：OP_DELEGPURGE，OP_DELEGRETURN，NFS4_OP_OPENATTR，客户端将显示 NFS4ERR_NOTSUPP 错误。

NFSv4 暂不支持 Delegation 功能。

（4）应用场景

场景一：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。

场景二：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。

场景三：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。

场景四：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。

五、网络类服务

1、BGP 互联网服务

① 产品规格

证通云提供用户互联网访问服务，包括上海宁桥路站点，金桥站点及北京站点，各站点使用独立的互联网出口，且都为三线 BGP 互联网线路（兼容电信，联通，移动）。

② 功能特性

用户在云管平台申请 EIP 后可开通互联网相关服务。北京站点 EIP 即互联网地址，用户可直接访问互联网或提供互联网访问权限。上海同城双站点申请 EIP 后，由运维人员开通互联网访问策略。

③ 使用限制

目前证通云平台互联网服务仅在虚拟区提供，其他区域（云外区域）不提供互联网访问服务。

2、云上网络

（1）弹性公网 IP（EIP 实例）

① 产品规格

弹性外网 IP（Elastic IP Address，简称 EIP），是用户需访问互联网或提供互联网访问必须绑定的，能动态绑定到不同的专有网络的 ECS 实例上，绑定和解绑时无需停机。

② 功能特性

用户可以申请、绑定、解绑定、删除弹性外网 IP。为了便于管理控制，弹性外网 IP 并非真实的互联网地址，如用户 ECS 需访问互联网，直接绑定 EIP 并配置公网 DNS 即可。如需对互联网开放服务端口，需向运维人员申请，由运维人员分配互联网地址及完成相关策略开通。

③ 使用限制

单个 EIP 只可绑定一台 ECS，无法绑定多台 ECS。如需多台 ECS 共享一个 EIP 访问互联网，可使用 NAT 网关产品。用户实际访问互联网的公网地址并非 EIP，由证通云指定。

④ 产品优势

独立购买与持有：用户可以单独持有一个 EIP，作为您账户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，将之解绑并释放，避免不必要的计费。

可配置的网络能力：用户可以根据需要随时调整 EIP 的带宽值，带宽的修改即时生效。

（2）专有网络（VPC）

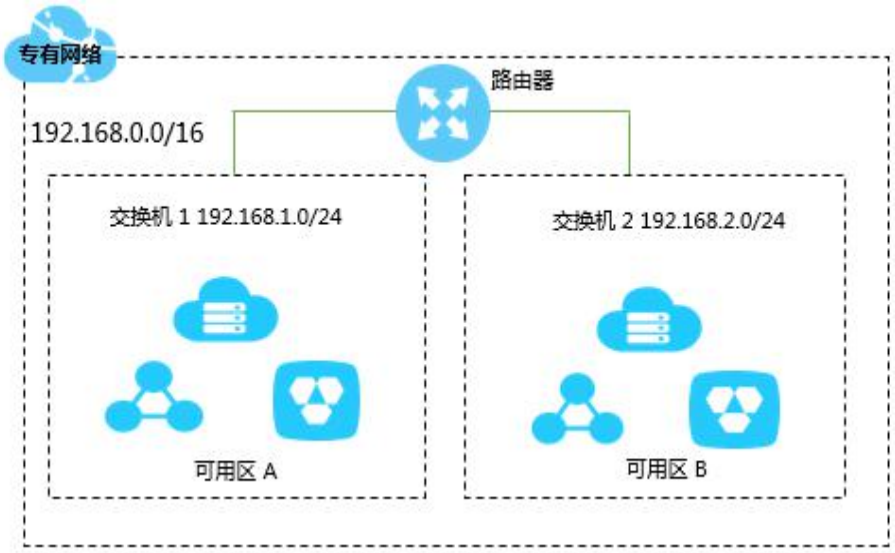


图 5-2-1 专有网络 VPC 示意图

① 产品规格

VPC 为用户创建出一个隔离的网络环境，并可以根据分配到的 IP 地址段划分多个网段、路由表和网关等。

② 功能特性

自定义私有网络：用户可以规划自己的专有网络。当创建 VPC 和交换机时，用户可以根据业务规划创建多个子网，将不同的服务部署到不同的子网以提高服务的可用性。

自定义路由：用户可以在 VPC 的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。

多种连接方式：证通云提供多种连接方式，用户可以将 VPC 连接到 Internet、您的数据中心或其他 VPC：

连接到 Internet：用户可以通过绑定弹性外网 IP、配置 NAT 网关方式，将 VPC 与 Internet 连接，使 VPC 内的云服务可以和 Internet 通信。

连接到其他 VPC：用户可以通过创建一对路由器接口连接到其他 VPC，建立高速、安全地内网通信。

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 VPC 连接起来，将本地应用平滑迁移到云上。

③ 使用限制

用户 VPC 的地址必须由证通云运维人员分配，用户配置自己定义的 IP 地址将无法与云外网络通信。

④ 产品优势

安全：每个 VPC 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，VPC 之间完全隔离。另外，您可以通过安全组、白名单等方式控制专有网络内的云资源访问。

易用：用户可以通过专有网络控制台快速创建、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路由表。

可扩展：用户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 VPC 和本地数据中心或其他 VPC 相连，扩展网络架构。

（3）负载均衡 SLB

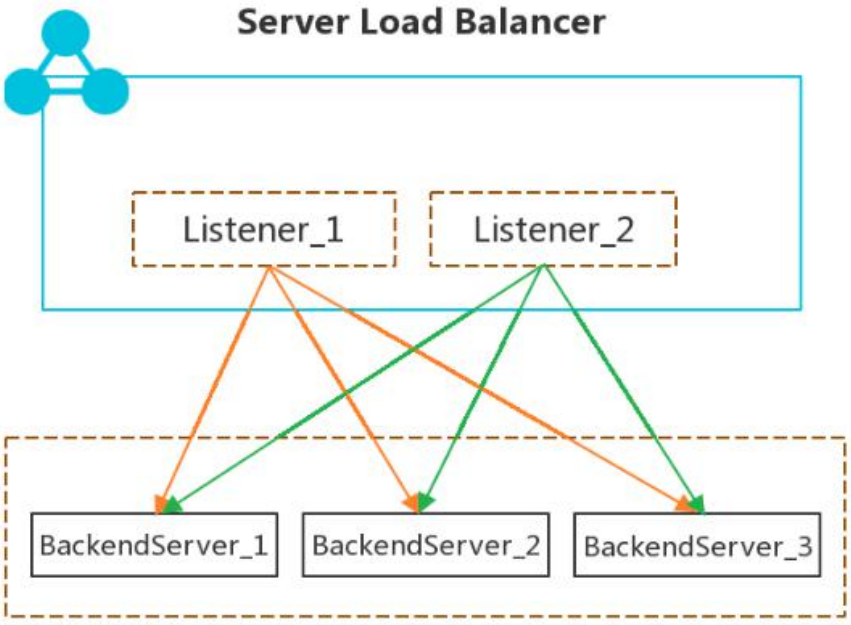


图 5-2-2 负载均衡 SLB 示意图

① 产品规格

为用户提供对多台云服务器进行流量分发的负载均衡功能，可提高应用系统对外的服务能力，并消除单点故障。

② 功能特性

本地和全局负载均衡：对分别放置在不同的地理位置、有不同网络结构的服务器群间作负载均衡。

L4-L7 负载均衡：根据 L4-7 的数据包头分析流量类型，按照不同类型导向对应的服务器。

健康检查：负载均衡设备定期对真实服务器或链路服务状态进行探测，收集相应信息，及时隔离工作异常的服务器或链路。

③ 使用限制

证通云平台用户申请 SLB 时，需统一选择专有网络 SLB。该 SLB 不对公网开放，如用户 SLB 需对公网开放，可使用 NAT 网关功能，将 SLB 绑定 EIP 并配置映射端口。

④ 产品优势

维护方便：支持基于全 B/S 架构的运维管理系统。在同一个管理系统中实现：资源管理、逻辑拓扑监控、告警与事件管理、系统监控、虚拟资源管理、系统配置、用户管理、操作日志查询等。

算法灵活：调度算法支持以源 IP 地址为粒度，新建连接会话负载均衡到服务器地址池中的 IP 地址，支持使用同源同宿，支持静态算法和动态算法。

易扩展：负载均衡产品具有良好的系统和软件升级能力。支持以软件的方式按照流量升级而不需要更换硬件。

冗余设置：负载均衡设备采用冗余设计，在设备发生故障或链路中断时系统能迅速切换，保证系统的正常运营。

（4）NAT 网关服务

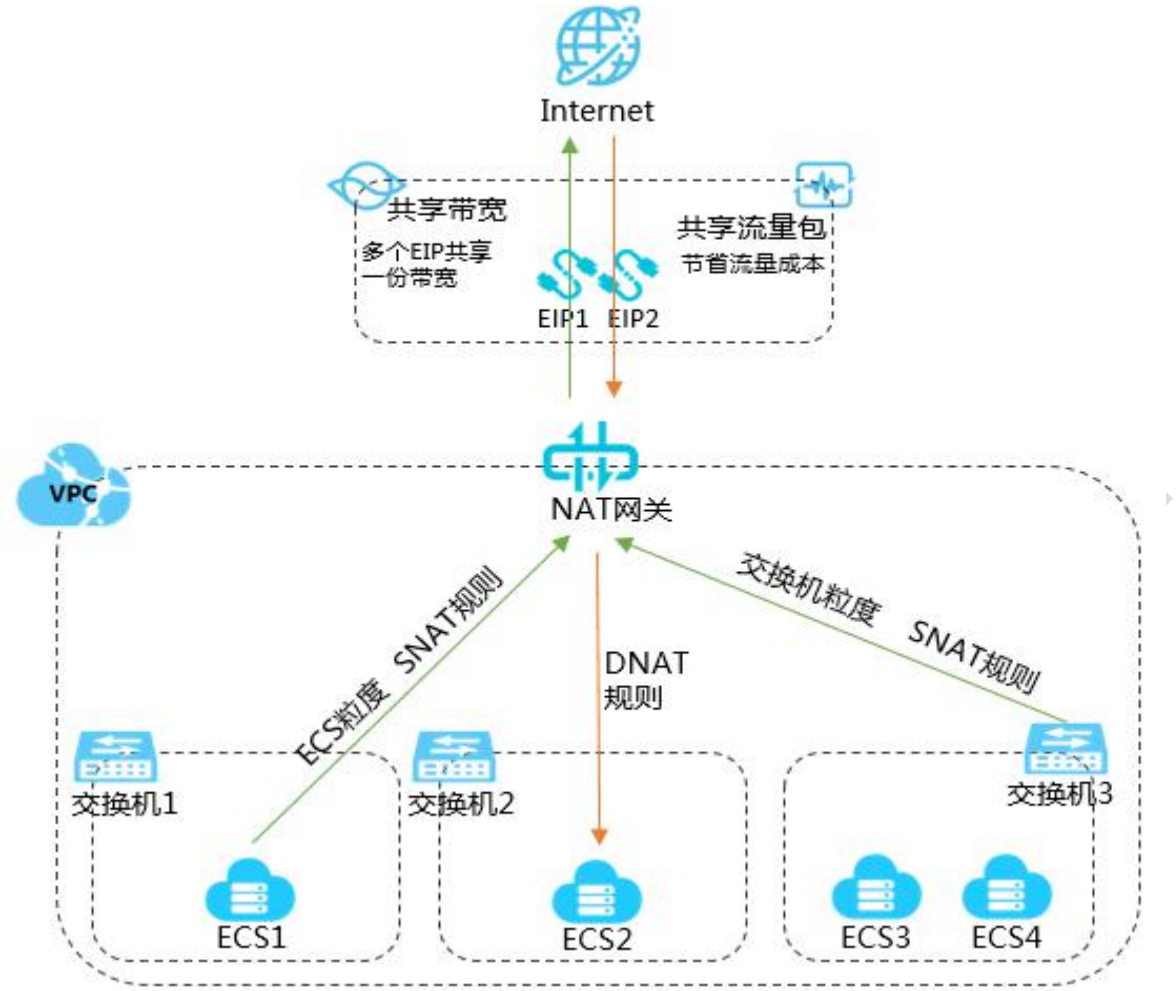


图 5-2-3 NAT 网关服务示意图

① 产品规格

NAT 网关是一款 VPC 公网网关，在 VPC 环境下构建一个公网流量的出入口，通过自定义 SNAT、DNAT 规则灵活使用网络资源，支持多 IP，支持共享公网带宽。

② 功能特性

SNAT：NAT 网关提供 SNAT 功能，为 VPC 内无公网 IP 的 ECS 实例提供访问互联网的代理服务。

DNAT：NAT 网关支持 DNAT 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。

宽带共享：通过为 NAT 网关绑定 EIP，可实现 NAT 网关下多机器共享 EIP 的带宽。

③ 使用限制

SNAT 与 DNAT 需使用不同的 EIP。

④ 产品优势

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。

高性能：NAT 网关是基于证通云自研分布式网关，使用 SDN 技术推出的一款虚拟网络硬件。NAT 网关支持 10Gbps 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。

按需购买：NAT 网关的规格、EIP 的规格和个数，均可以随时升降，轻松应对业务变化。

（5）异地站点传输

① 产品规格

异地站点接入产品是为证通云用户在证通云不通城市站点间传输提供的网络传输产品。（北京-上海-东莞）

② 功能特性

用户可通过接入本地金融云机房，通过该产品与异地金融云站点内的资源进行数据传输及开展相关业务。

③ 使用限制

用户必须在两站点申请云内资源进行网络通信。带宽规格如下：2M，5M,10M，20M，50M，100M，200M。

④ 产品优势

低成本：正常情况下用户需接入异地金融云站点开展业务时需向运营商申请异地长途专线，售价为本地线路的 4 倍左右。通过该产品，用户只需拉本地专线到本地金融云站点，通过该产品即可与异地站点的金融云资源进行数据传输开展业务。该产品售价参照本地运营商专线售价（电信或联通），总体可为用户节省 40%-50%费用。

周期短，流程简单：通过该产品用户实现异地站点访问只需申请一根本地专线到本地金融云站点，周期相比申请异地专线短很多。本地专线接入后，用户提交访问需求工单，后台运维人员进行配置后即可完成网络互通。

（6）高速通道

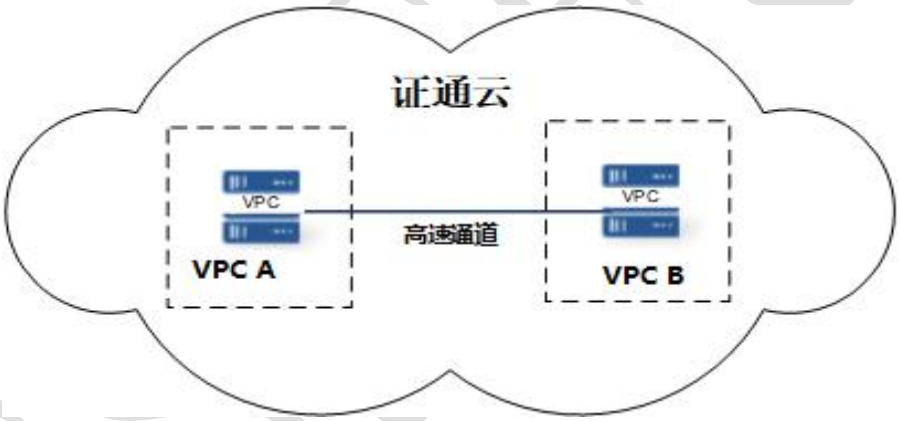


图 5-2-4 高速通道示意图

① 产品规格

高速通道为云内不同 VPC 之间互相通信的一种方式，主要通过创建路由器接口，配置路由的方式实现不同帐户 VPC 之间的互相通信。

② 功能特性

用户可通过高速通道实现自己账户下不同 VPC 之间，与其他用户帐户的 VPC 之间网络的互相通信。支持同站点，同城站点间间不同 VPC 之间的网络互通。

③ 使用限制

不同用户 VPC 之间互通需协商部分参数。一条高速通道只可以打通两个 VPC，如多个 VPC 需互通要创建多条高速通道。

④ 产品优势

配置简单：用户只需创建路由器接口，并在创建的路由器下配置路由即可完成。

无需平台运维人员干预：所有配置用户在云管平台即可完成，无需运维人员操作。

安全可控：用户可通过配置精确的路由条目控制可互访的 ECS，也可通过配置安全组精确控制互访的 ECS 及端口。

3、云内通信服务混合

（1）平台接入服务

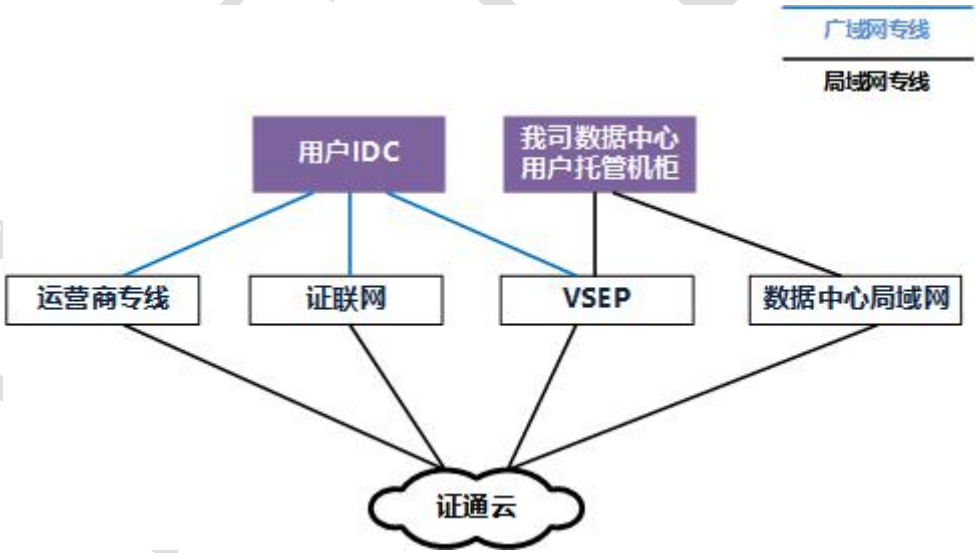


图 5-3-1 平台接入服务示意图

① 专线代收代付接入服务

与三大电信运营商合作，为云内用户提供高速、稳定的电信、联通、移动广域网线路服务。云内用户点对点专线从外部接入上交所技术证通云，

用户可委托我公司向运营商申请线路，并享受我公司与运营商间的优惠结算价格。

站点名称	宁桥路	金桥	外高桥	北京
可接入运营商	电信、联通	电信、联通、移动	电信、联通、移动	电信、联通

特别强调：因云内用户的广域网线路是通过汇聚方式接入，不论是用户自行申请还是代收代付方式，所有广域网线路开通时必须使用证通云统一规划的线路汇聚总头编号，VLAN 编号和网间网地址，否则会影响线路的连通性及延长线路开通的周期。

② 数据中心用户的局域网接入服务

用户如在我司数据中心有托管机柜，需与其云内资源互通，证通云提供专有局域网接入服务，用户托管机柜设备接入数据中心相关专有网络（VSEP 网或租户网），即可通过局域网高速接入云内资源。

③ VSEP 网接入平台

通过数据中心内部网络，满足云内用户与上证技术已有数据中心用户、广域网线路间的数据传输需求。

④ 证联网接入平台

用户可向中证信息申请通过证联网接入云内相关资源。

（2）平台上行业务接入服务

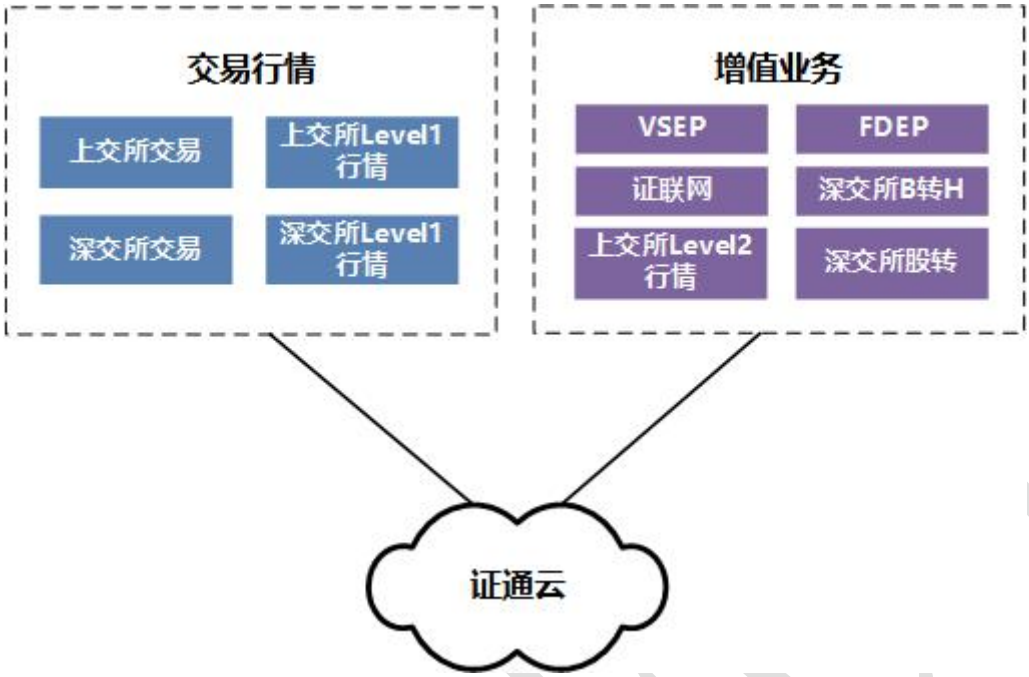


图 5-3-2 平台上行业务接入服务示意图

① 沪深报盘、行情

提供上交所委托报单、接收 level-1 行情数据 、接收成交回报、清算数据及接入中登 PROP 系统的网络接入。提供深交所交易行情业务的备用传输通道。

② VSEP 接入

提供上交所 VESP 网接入服务。

③ 深证 FDEP 链路接入

提供云内用户与深证 FDEP 系统的接入通道

④ 证联网接入

提供证联网的接入通道

站点名称	宁桥路	金桥	外高桥	北京
证联网接入	提供内部网络通道连接至证联网外高桥节点	已开通	已开通	已开通

（5）其他增值业务接入

为云内用户提供千兆局域网接入点，实现与特定（多个）市场核心机构之间的网络路由，满足用户相关业务需求。已开通深交所 B 转 H 股业务，股转业务，上交所信息公司的 Level-2 非展示行情业务。

六、安全服务

1、云安全

（1）运维审计

堡垒机软件授权：为用户提供堡垒机，基于协议正向代理实现，通过正向代理的方式实现对 SSH 、Windows 远程桌面、及 SFTP 等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维审计的目的。

① 功能特性

堡垒机具备操作审计、职权管控、安全认证、高效运维等功能。

操作审计：多面记录运维人员的操作行为，作为事件追溯的保障和事故分析的依据。运维操作记录包括操作失误、恶意操作、越权操作详细记录。Linux 命令审计包可提取命令符审计，支持命令定点回放。Windows 操作录像包括远程桌面的操作，支持全程录像，包括键盘操作、鼠标操作、窗口打开等。文件传输审计包括支持远程桌面文件传输、FTP/SFTP 的原文件审计。

职权管控：通过账号管控和权限组管理，实现分职权进行人员和资产的管理。账号管控确保运维账号唯一，解决共享账号、临时账号、滥用权限等问题。权组管理包括按照人员、部门组织、资源组，建立人员职责与资源分配的授权管理。

② 产品优势

审计合规：满足《萨班斯法案》、金融监管、《等级保护》的审计要求。

高效易用：管理界面简洁易用。

多协议支持：支持 SSH、Windows 远程桌面、SFTP 等常见运维协议。

追溯回放：追溯运维操作的故障，支持在线回放操作记录。

③ 应用场景

堡垒机常用于审计合规要求严格和高效运维管理等场景。

（2）云盾

云盾--WEB 应用防火墙：对网站或者 APP 的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。

云盾--态势感知：实时识别、分析、预警安全威胁的统一安全管理系统，通过防勒索、防病毒、防篡改、合规检查等安全能力，帮助用户实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产满足监管合规要求。

云盾--流量安全监控：基于网络流量旁路镜像的实时海量数据采集、计算分析产品。能对网络流量进行检测分析、异常流量检测、Web 应用攻击防护。

云盾--主机入侵检测：对云上主机检测达到：关键目录完整性检测、异常进程告警、异常端口告警、异常网络连接警。

云盾—数据库审计：可针对数据库 SQL 注入，风险操作等数据库风险操作进行记录与告警。支持 RDS 与云上自建数据库，为云上数据库提供安全诊断、维护、管理的能力。

云盾--资产漏洞扫描：为用户提供自动化漏洞渗透测试和敏感内容监测等。

① 功能特性

证通云云盾不同于传统的软硬件安全产品，它采用纵深防御、多点联动的云安全架构，完全基于专有云的云计算环境研发，从网络层、应用层、主机层等多个层面为用户提供全面的、一体化的云安全防护能力。

② 产品优势

云盾是集合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，可有效保护证通云用户云平台、云网络环境和云业务系统的安全。

安全域	服务名称	解决方案
安全管理	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。
应用安全	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等互联用用户的接入安全。
	DDOS流量防护	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。
网络安全	流量安全监控	基于网络流量旁路镜像的实时海量数据采集、计算分析产品。能对网络流量进行检测分析、异常流量检测、Web应用攻击防护。
主机安全	主机入侵检测	对云上主机检测达到：关键目录完整性检测、异常进程告警、异常端口告警、异常网络连接警。
资产安全	资产漏洞扫描	根据用户设置的已知资产结合内置的资产学习模型，对资产进行分析，准确分辨资产来源，帮助企业自动发现未知资产。同时根据漏洞检测覆盖能力，帮助企业及时发现未知的安全风险。

③ 互联网应用场景

如果部署的应用平台需要面向互联网并对外提供服务，建议参考图面向互联网场景结合安全产品进行配置，从网络安全、服务器安全、数据安全和安全管理等方面防护证通云。

网络安全：DDoS 流量清洗、WEB 应用防火墙

数据安全：数据库审计、敏感数据保护

安全管理：堡垒机

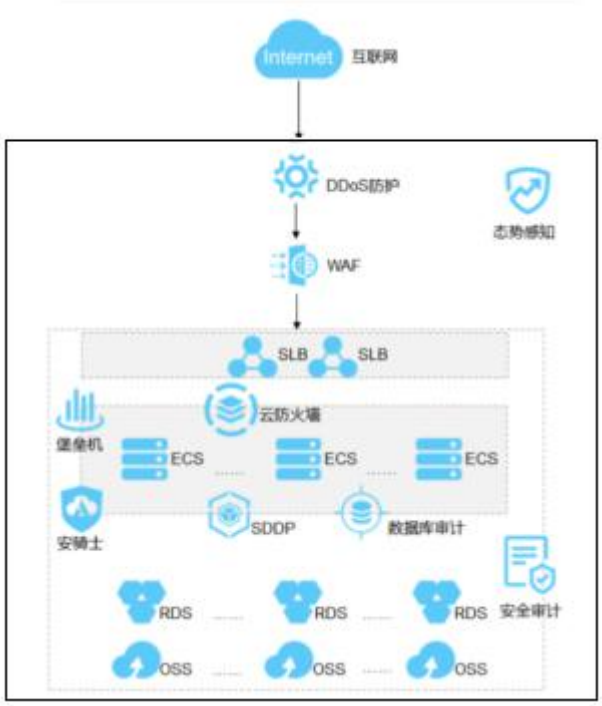


图 6-1-1 面向互联网的云盾应用场景

④非互联网应用场景

如果仅在专网环境中部署证通云平台，不面向互联网提供服务，建议在云盾标准版的基础上参考非互联网场景结合安全产品进行配置，从内部网络安全、服务器安全、数据安全和安全管理等方面防护您的证通云环境。

内部网络安全：WEB 应用防火墙

数据安全：数据库审计、敏感数据保护

安全管理：堡垒机

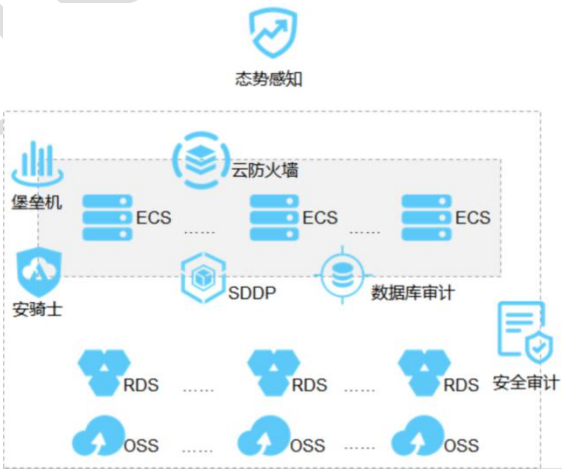


图 6-1-2 面向非互联网的云盾应用场景

（3）镜像站

YUM 源服务：提供 Yum 源镜像站服务，方便云内用户更新 Linux 系统补丁。

使用场景：在某些生产环境是断网操作无法联网，例如我们服务对象是内部生产服务，要求全部是断网操作，所以在部署某些东西的时候就不能用 Yum 进行在线下载，为了能在内网环境中使用 Yum 安装相关的软件，就需要配置本地 Yum 源仓库。内部如果使用自己的 Yum 服务器，不但占用带宽少、速度更快，而且可以更加灵活方便的自定义配置，能有效提升日常工作效率。

（4）补丁更新

Windows 补丁:提供 Windows 补丁更新服务,方便云内用户更新 Windows 系统补丁,提升用户体验。

使用场景：用户内网通过补丁服务器更新微软补丁。

2、数据安全

（1）加密服务

加密服务基于国家密码局认证的硬件加密机，提供了云上数据加解密解决方案，用户能够对密钥进行安全可靠的管理，也能使用多种加密算法来对云上业务的数据进行可靠的加解密运算。

① 功能特性

数据加密：数据是企业的核心资产，每个企业都有自己的核心敏感数据。包括企业自身的敏感数据，如合同、交易、流水等，企业用户的敏感数据，如身份证、银行卡等。这些数据都需要加密服务来保护不会被他人获取。

加密算法支持：全面支持国产算法以及部分国际通用密码算法，满足用户各种加密算法需求。其中对称密码算法支持 SM1、SM4、DES、3DES、AES；非对称密码算法支持 SM2、RSA（1024-2048）；摘要算法支持 SM3、SHA1、SHA256、SHA384。

金融行业支持：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，包括：

PIN 码的产生/加密/转加密/验证等；

ARQC 的生成/验证、脚本加密、脚本 MAC 等；

MAC1、MAC2 计算及验证、TAC 验证等；

外部认证、更新密钥、内部认证等；

敏感数据加密、转加密、报文 MAC 计算及验证等；

CVV/CVN、PVV/PVN 的产生及校验。

② 产品优势

加密服务产品包含以下优势。

安全的密钥存储：使用硬件密码机保护客户密钥，且密码机符合国家密码管理局（GM/T 0029-2014）和中国人民银行（PBOC1.0/2.0/3.0）等多项要求。

安全的密钥管理：设备管理和密钥管理权限分离。证通云只能管理密码机硬件设备，主要包括监控设备可用性指标，开通、停止服务等。密钥完全由客户管理，证通云没有任何方法可以获取客户密钥。密钥管理体系通过国家密码管理局的安全检测和认证。

方便的云上使用：加密服务实例部署在客户的 VPC 专有网络中，通过客户指定的私网 IP 地址进行管理和调用，很方便地与云服务器实例上的业务配合使用。

弹性扩展：您可以根据实际情况，灵活地调整租用的加密服务实例数量，通过负载均衡来满足不同的加解密运算要求。

满足监管合规要求：加密服务使用通过国家密码管理局检测认证的密码机，让客户安全地生成、存储和管理用于数据加密的加密密钥，在不牺牲应用程序性能的情况下符合严格的密钥管理要求。

③ 使用场景

加密服务适用于证通云上所有客户，主要使用场景包括云上金融业务系统、政务系统、企业财务系统等敏感数据保护。

金融业务系统：主要包括银行卡号、身份证、PIN 码等敏感信息的存储。

政务系统：主要包括涉密业务的敏感信息存储。

企业财务系统：主要包括合同、财务等敏感信息存储。

七、数据库缓存服务

1、RDS 关系型数据库

（1）产品优势

易于使用：云数据库 RDS 拥有即开即用、按需升级、透明兼容和管理便捷的优点。

即开即用：您可以通过 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，您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，您无需二次学习，上手即用。另外 RDS 兼容您现有的程序和工具。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。

高性能：云数据库 RDS 通过参数优化、SQL 优化、高端硬件来实现高性能。

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，我们持续对其进行优化，确保 RDS 一直基于最佳实践在运行。

SQL 优化：针对您的应用场景特点，RDS 会锁定效率低下的 SQL 语句并提出优化建议，以便您优化业务代码。

高端硬件投入：RDS 所使用的服务器硬件经过多方评测，保证服务器运行稳定性。

用安全性：云数据库 RDS 通过防 DDoS 攻击、访问控制策略、系统安全和 TDE 加密实现用安全性。

（2）使用限制

为保障实例的稳定及安全，云数据库 MySQL 版有部分使用上的约束。

操作	使用限制
修改数据库参数设置	大部分数据库参数须使用RDS控制台或API进行修改，同时出于安全和稳定
数据库的root	不提供root或者sa权限。
数据库备份	可使用命令行或图形界面进行逻辑备份。仅限通过RDS控制台或API进行物理备份
数据库还原	可使用命令行或图形界面进行逻辑数据还原。仅限通过RDS控制台或API进行物理还原。
数据迁入	可以使用命令行或图形界面进行逻辑导入。可以使用MySQL命令行工具、数据传输服务等方式迁入数据。
MySQL 存储引擎	目前支持InnoDB、TokuDB两种引擎（MyISAM引擎由于自身缺陷，存在数据丢失的风险，因此仅部分存量实例暂时支持，新创建实例的MyISAM引擎表会自动转换为InnoDB引擎表）。出于性能和安全性考虑建议尽量采用InnoDB存储引擎。不支持Memory引擎。如果您创建Memory引擎的表，我们将自动为您转换成InnoDB引擎的表。
搭建数据库复制	云数据库MySQL版本身提供主备复制架构的双节点集群，无需用户手动搭建。其中主备复制架构集群的备（slave）实例不对用户开放，用户应用不可直接访问。
重启RDS 实例	必须通过RDS控制台或API操作重启实例。
用户、密码管理和数据库管理	云数据库MySQL版默认需要通过RDS控制台进行用户、密码和数据库管理（包括创建、删除、修改权限、修改密码）。

通常，从创建实例到可以开始使用实例，您需要完成如下操作：

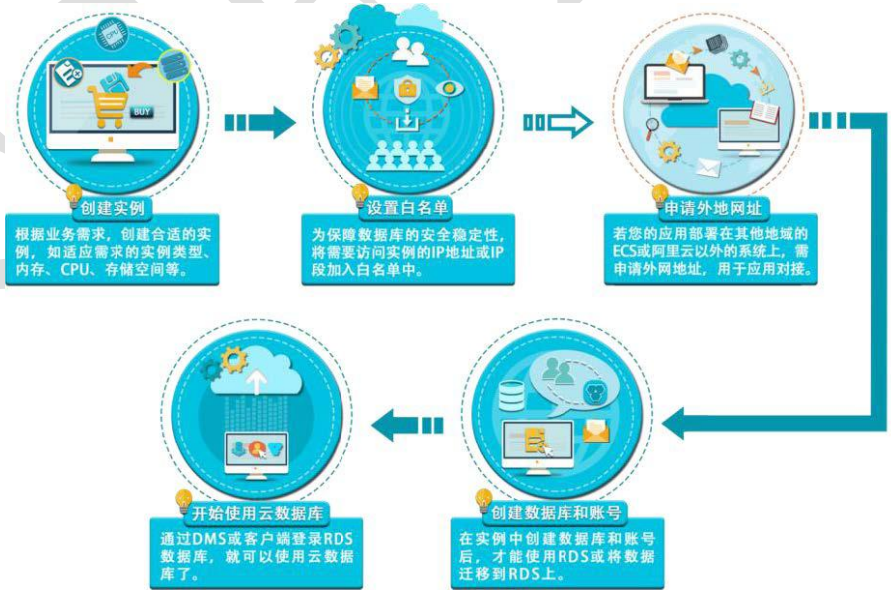


图 7-1-1 RDS 实例的创建到使用步骤

（3）应用场景

① 数据多样化存储

云数据库 RDS 提供缓存数据持久化和多结构数据存储。

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

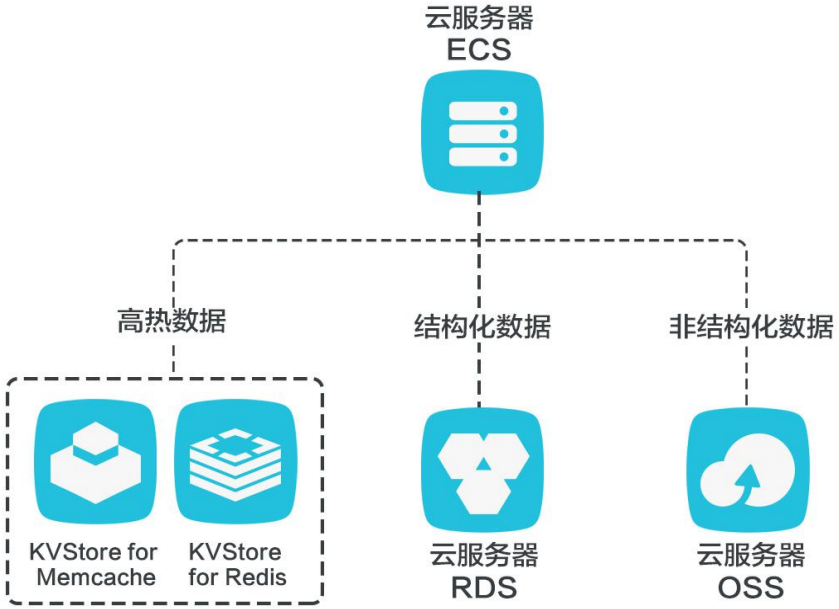


图 7-1-2 数据多样化存储示意图

② 缓存数据持久化

RDS 可以和 KVStore for Memcache、KVStore for Redis 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，KVStore for Memcache 和 KVStore for Redis 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）。

③ 多结构数据存储

OSS 是证通云对外提供的海量、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。

④ 读写分离

通过读写分离功能可以实现数据读取和写入入作的分离，扩展系统的处理能力。

数据库 MySQL 版支持直接挂载只读实例，分担主实例读取的压力。MySQL 版数据库的主实例和只读实例都具有独立的连接地址，当您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，实现了自动的读写分离。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，而将读取请求按照您设置的权重发往各个只读实例。您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，如读写分离示意图所示。

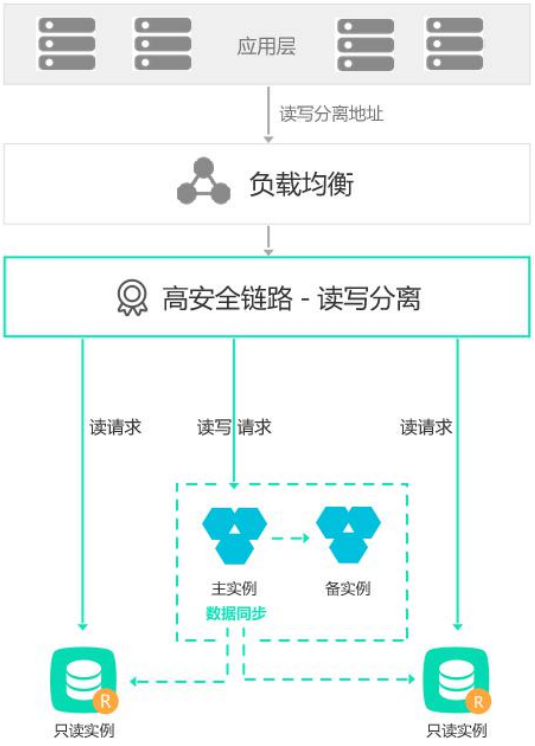


图 7-1-3 读写分离示意图

⑤ 大数据分析

将 RDS 数据导入大数据计算服务，可以实现大规模的数据计算。

大数据计算服务（MaxCompute），可服务于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，如大数据分析示意图所示。

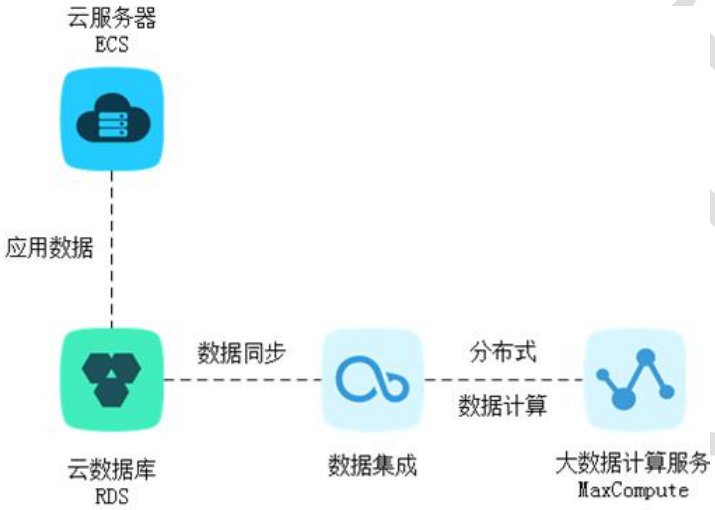


图 7-1-4 大数据分析示意图

2、Redis 缓存

（1）Redis 缓存（主从版）

Redis 是基于开源的 Redis 二次开发，兼容开源 Redis 协议的在线 Key-Value 存 储服务。其硬件和数据部署在云端，有完善的基础设施、网络安全保障和系统维护服务。

（2）Redis 缓存（主从同城容灾版）

同主从同城容灾版 Redis 不仅有主从双节点，而且在部署上是分布在不同机房。保证部署在物理上隔离，避免单点故障对系统的影响，提升 Redis 服务的稳定性。

3、MongoDB 版

云数据库 MongoDB 是金融云基于 MongoDB 专业打造的高性能分布式数据存储服务，100%完全兼容 MongoDB 协议，提供稳定可靠、弹性伸缩的数据库服务。同时提供容灾、备份、恢复、监控、报警等方面的全套数据库解决方案。

（1）产品规格

规格类型	规格信息	规格代码	最大连接数	最大IOPS
通用规格	1核2G	dds.mongo.mid	500	1000
	2核4G	dds.mongo.standard	1000	2000
	4核8G	dds.mongo.large	2000	4000
	8核16G	dds.mongo.xlarge	4000	8000
	8核32G	dds.mongo.2xlarge	8000	14000
	16核64G	dds.mongo.4xlarge	16000	16000
独享规格	2核16G	mongo.x8.medium	2500	4500
	4核32G	mongo.x8.large	5000	9000
	8核64G	mongo.x8.xlarge	10000	18000
	16核128G	mongo.x8.2xlarge	20000	36000
	32核256G	mongo.x8.4xlarge	40000	72000
独占物理机	60核440G	dds.mongo.2xmonopolize	100000	100000

（2）功能特性

① 架构灵活

云数据库 MongoDB 版自动搭建好三节点的副本集供您使用，您可以直接操作 Primary 节点和一个 Secondary 节点。如果判断主节点实例不可用，进行主备节点的切换操作，保证 MongoDB 实例的高可用。

② 弹性扩容

存储容量一键扩容：您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：在线调整实例存容量，无需停止服务，不影响您的业务。

③ 数据安全

自动备份：云数据库 MongoDB 版支持您自行设置备份周期。备份开始时间可根据您的业务低峰灵活配置；所有备份文件免费保留 7 天。

临时备份：您在需要时可以临时性发起备份操作；备份文件免费保留 7 天。

数据恢复：利用备份文件，您可以直接覆盖型恢复至现有实例。

备份文件下载：云数据库会将您的备份文件免费保留 7 天，在此期间您可以登录管理控制台，将备份文件下载至本地。

根据备份集创建实例：根据备份文件在控制台上一键式地创建一个实例，实现快速部署的需求。

IP 访问白名单：提供对实例进行 IP 访问过滤功能，您可以登录云数据库 MongoDB 版管理控制台进行 IP 访问白名单设置，设置后便可实现最高级的访问安全保护，IP 白名单最多可配置 1000 条。

多层网络安全防护 VPC 私有网络在 TCP 层直接进行网络隔离保护；DDOS 防护实时监测并清除大流量攻击；支持 1000 个以下 IP 白名单配置。

④ 智能运维

监控平台：提供 CPU 利用率、连接数、磁盘空间利用率等实例信息实时监控及报警，随时随地了解实例动态。

可视化管理平台：管理控制平台对实例克隆、备份、数据恢复等高频高危操作可便捷地进行一键式操作。

数据库内核版本管理主动升级，快速修复缺陷，免去日常版本管理苦恼；优化 MongoDB 参数配置，最大化利用系统资源。

（3）使用限制

操作	约束
搭建数据库复制	系统自动搭建了三节点的副本集。其中对您提供了两个节点（Primary和Secondary），另外一个备份节点隐藏对您不可见。您暂时无法自行搭建Secondary节点。
重启数据库	必须通过控制台进行重启实例的操作。

（4）产品优势

① 高可用

三节点副本集高可用架构，提供极高的业务可用性保障。云数据库 MongoDB 服务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 和 Secondary 节点提供服务，当 Primary 节点出现故障，系统自动选举新的 Primary 节点，当 Secondary 节点不可用，由备用节点接管服务。

自动备份，一键式数据恢复。每天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。

② 高安全

- 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触发黑洞机制。

- IP 白名单配置：最多支持配置 1000 个允许连接 MongoDB 实例 IP 地址，从访问源进行直接的风险控制。

③ 易用性

完善的性能监控。提供 CPU 利用率、IOPS、连接数、磁盘空间等实例信息，实时监控及报警，随时随地了解实例动态。

④ 扩展性

副本集模式弹性扩容，云数据库 MongoDB 支持三节点的副本集模式，支持弹性扩容。当前实例配置无法满足应用的性能要求，或者当前实例的配置过高，您可以变更实例的配置。变更过程完全透明，对业务无影响。

4、HBASE

HBase 是低成本、高扩展、云智能的大数据 NoSQL，兼容标准 HBase 访问协议，提供低成本存储、高扩展吞吐、智能数据处理等核心优势.具备 PB 规模、千万级并发、秒级伸缩、毫秒响应、跨机房高可用、全托管、全球分布等企业能力。HBase 全面提供海量半结构/非结构化数据下的实时存储、高并发吞吐、轻 SQL 分析(集成 Phoenix)、全文检索(集成 Solr)等能力， 结合完备的工具服务，丰富的生态融合，一站式高效满足企业在大数据量场景下的的存储、检索、分析需求。

（1）产品规格

规格	适用角色	带宽	SIZE	数据空间
hbase.sn1.8xlarge	Master	6.0 Gbit/s	32C 64G	/
hbase.d1.6xlarge	Core for Hitsdb	8.0 Gbit/s	24C 96G	12 *5.5TB*0.7
hbase.d1-c14d3.14xlarge	Core for HBase	17.0 Gbit/s	56C 160G	12*5.5TB*0.7

（2）功能特性

① 产品内核及架构深度优化

架构高可用 Master 为两节点，互为主备模式，且 HA 实时检测，保障业务高可靠；Core 节点故障时，Region 可秒级切换。

集群弹性扩展单 Core 节点提供最高 10 万 QPS、最高 8T 存储空间；磁盘及节点可灵活扩容，可轻松扩展到千台规模，满足千万级 QPS 及数 PB 存储空间。

内核深度优化对原生 HBase 内核源码深度优化，云数据库 HBase 读写性能比社区版本提升更快。

② 多重防护机制

权限控制账号密码验证，ACL 权限控制，抵御恶意数据损毁，保障数据高安全。

VPC 私有网络实例部署在利用 OverLay 技术在物理网络基础上构建的专有 VPC 虚拟网络上，在 TCP 层直接进行网络隔离保护。

DDoS 防护在网络入口实时监控，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恶意 IP 拉进黑洞。

IP 白名单配置最多支持配置 1000 条白名单规则，直接从访问源进行风险控制。

③ 完整数据生态

数据生态闭环：支持 MaxCompute 以及 EMR Hadoop/Spark/storm/Flink 等各类开源组件访问云数据库 HBase。

数据集成平台：提供可跨异构数据存储系统的、安全、可靠、低成本、可弹性扩展的数据同步能力，打通 HBase 与多种数据源之间的离线（全量/增量）数据进出通道，以应对复杂应用场景。

开源组件 UI 访问：HBase UI 查看 HBase 的基本信息，节点资源使用情况等；HDFS UI 查看存储空间的使用情况；Ganglia UI 查看系统进行时的状态信息，入 JVM 信息等。

④ 便捷运维

云监控平台：提供 CPU 利用率、IOPS、连接数、磁盘空间等实例信息实时监控及报警，随时随地了解集群动态。

可视化管理平台：管理控制平台对实例进行扩容，修改配置参数，重启等。

数据库内核版本管理主动升级，快速修复缺陷，免去日常版本管理麻烦；优化 HBase 参数配置，最大化利用系统资源大幅提升效率。

（3）使用限制

限制项	限制范围	限制说明
单集群规模	单集群规模最大100；单次最大5台	超过限制联系运维人员处理

（4）产品优势

性能可靠：基于 HBase 1.1 改造，性能不断提升。自动负载均衡、默认 HA、对集群服务进程自动守护、单节点故障时可秒级故障迁移。独占资源，可靠稳定，不受其它用户干扰。

生态完整易运维：完全兼容开源、与 Hadoop 生态完美融合、内部支持 Phoenix 组件。支持不同规格不同场景的需求，支持本地实例。支持可视化 web 控制台，全指标监控预警，修改配置等。

数据访问安全：支持网络白名单，VPC 网络隔离，数据可靠性高。

扩展性良好：支持在线增加节点，且可以平滑增加资源。

使用便捷高效：支持通过 SQL 访问数据库数据，高效的二级索引方案让您查询数据更加便捷高效。支持关系型、MaxCompute、EMR 等数据源与 ApsaraDB HBase 导入导出。支持与位于同一VPC 的产品互通。

八、大数据服务

1、实时计算

E-MapReduce 大数据离线计算：大数据离线计算称为 E-MapReduce，是运行在云平台上的一种大数据处理的系统解决方案。E-MapReduce 构建于云服务器 ECS 上，基于开源的 Apache Hadoop 和 Apache Spark，可以方便地使用 Hadoop 和 Spark 生态系统中的其他周边系统来分析和处理自己的数据。不仅如此，E-MapReduce 还可以与其他的云数据存储系统和数据库系统进行数据传输。

（1）产品规格

以 CU 数为单位。

（2）功能特性

E-MapReduce 具有以下功能：

支持创建丰富的作业类型，例如 Spark、Hadoop、Hive、Pig、Sqoop、SparkSQL 和 Shell 等等，实现用户的日志分析、数据仓库、商业智能、机器学习和科学模拟等业务需求。

用户根据实际情况选择作业类型后，可定义要执行的命令以及执行失败后的策略。同时，您还可以克隆、修改和删除作业。

支持创建灵活的执行计划。执行计划是一组作业的集合，支持在一个现有的 E-MapReduce 集群上运行，也支持动态的按需创建出一个临时集群来运行作业。通过配置调度策略，可以被一次性或者周期性的执行。执行计划最大的优势就是执行多少作业就用多少资源，最大化的节省资源。其灵活性体现在以下方面：

用户可以将作业（包括 Hadoop/Spark/Hive/Pig）任意组合成执行计划。

执行计划的执行策略有两种，包括立即执行和定时周期执行。

提供交互式工作台：交互式工作台提供在 E-MapReduce 管理控制台直接编写并运行 Spark、SparkSQL、HiveSQL 任务的能力，您可以在工作台直接看到运行结果。交互式工作台适合处理运行时间较短、想要直接看到数据结果、调试性质的任务，对于运行时间很长、需要定期执行的任务应使用作业和执行计划功能。

支持报警管理：E-MapReduce 支持将执行计划和报警接收组进行关联。在执行计划管理页面打开“报警通知”后，当执行计划执行完成时，关联的报警接收组中的联系人，都将会接收到短信通知。

短信内容包含执行计划名、作业的执行情况（成功多少、失败多少）、对应的执行集群名以及具体的执行时长信息。

（3）使用限制

无

（4）产品优势

与自建集群相比，E-MapReduce 能给您提供相对方便可控的手段，从各方面管理自己的集群。此外，它还具有以下优势：

深度整合与金融云其它产品如 OSS、MNS、RDS、MaxCompute 等深度整合，使其可作为 E-MapReduce 产品中 Hadoop/Spark 计算引擎的输入源或者输出目的地。

安全：MapReduce 整合了金融云 RAM 资源权限管理系统，通过主子账号对服务权限进行隔离。

2、数据总线 DataHub

云流数据处理平台 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）和分发功能，可以轻松构建基于流式数据的分析和应用。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实时计算引擎来处理写入到 DataHub 的流式数据，并产出各种实时的数据处理结果。DataHub 服务也提供分发流式数据到各种云产品的功能，目前支持分发到 MaxCompute（原 ODPS），OSS 等。

(1) 产品规格

按套为数量。

(2) 功能特性

数据队列：DataHub 的基本功能，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 中的数据自动同步到金融云其它服务。

流式数据同步 DataConnector：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。

DataConnector 支持的系统下面是 DataConnector 支持数据同步的各系统的相关描述。

DataConnector 支持的系统如下：

目标系统	时效性	描述
MaxCompute	准实时，通常情况有5分钟延迟	同步Topic中流式数据到离线MaxCompute表，字段类型名称需一一对应，且DataHub中必须包含一列（或多列）MaxCompute表中分区列对应的字段。
OSS	实时	同步数据到对象存储OSS指定Bucket的文件中，将以csv格式保存。
ElasticSearch	实时	同步数据到ElasticSearch指定Index中，Shard之间数据同步不保证时序，所以需将同样ID的数据写入相同的Shard中。
RDS	实时	同步数据到指定的RDS表中。
AnalyticDB	实时	同步数据到指定的AnalyticDB表中。
TableStore	实时	同步数据到指定的TableStore表中。

扩容缩容：DataHub 支持为 Topic 动态扩容/缩容，一般通过 SplitShard/MergeShard 来实现。

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。

(3) 使用限制

限制项	限制范围	限制说明
活跃shard数	(0,10]	每个topic中活跃shard数量最大不超过10个。
总shard数	(0,512]	每个topic中总shard数量最大不超过512个。

限制项	限制范围	限制说明
Http BodySize	最大不超过4MB	Http请求中body大小最大不超过4MB。
单个String长度	最大不超过1MB	数据中单个String字段长度最大不超过1MB。
Merge/Split频率限制	5s	每个新产生的shard在5s内不允许进行Merge/Split操作。
QPS限制	最多不超过1000次	每个shard写入QPS限制（非Record/s，Batch写入同一shard仅计算为1次）最大不超过1000次。
Throughput限制	最大不超过1MB	每个shard写入每秒吞吐最大不超过1MB。
Project限制	最多不超过5个	每个云账号能够创建的Project上限最多不超过5个。
Topic限制	最多不超过20个	每个Project内能创建的Topic上限最多不超过20个，例如有特殊请求请联系管理员。
Topic Lifecycle限制	[1,7]	每个Topic中数据保存的最大时长为7天，最小时长为1天。

(4) 产品优势

① 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。

② 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。

③ 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。

④ 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。

⑤ 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。

3、数据中台 DataWorks

数据中台称为 DataWorks，为用户提供数据集成、数据开发、数据地图、数据质量和数据服务等全方位的产品服务，一站式开发管理的界面，帮助企业专注于数据价值的挖掘和探索。其支持多种计算和存储引擎服务，并且支持用户自定义接入计算和存储服务，可为用户提供全链路智能大数据及 AI 开发和治理服务。用户可以使用数据中台，对数据进行传输、转换和集成等操作，从不同的数据存储引入数据，并进行转化和开发，最后将处理好的数据同步至其它数据系统。

（1）产品规格

以套为数量单位。

（2）功能特性

数据集成：数据集成提供对业务方数据库进行抽取监控功能，能对数据源头的数据资源能够进行统一清点，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。

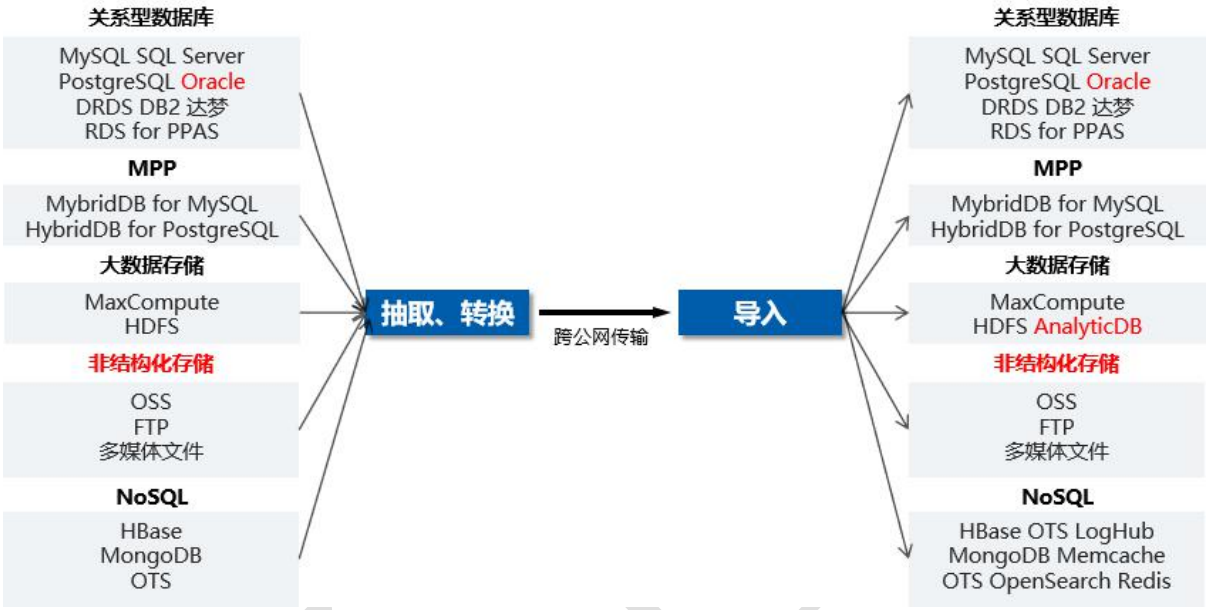


图 8-3-1 数据集成示意图

（3）使用限制

无

（4）产品优势

① 超大规模计算处理能力

DataWorks 与底层计算平台天然集成，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您的数据，确保不丢失、不泄露、不被窃。

② 一站式的数据工厂

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。

③ 海量异构数据源快速集成能力

DataWorks 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。

④ Web 化的软件

DataWorks 可在互联网/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。

⑤ 多租户权限

多租户模型确保您的数据被安全隔离，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。

⑥ 更智能的监控报警

通过设置监控基线，您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。

⑦ 更易用的智能 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。

⑧ 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。

⑨ 便捷的数据服务开发

API 网关服务、交互式数据服务引擎让您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。

⑩ 安全的数据共享机制

数据共享服务提供受保护空间，让详细数据以不见、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。

4、搜索与分析 Elasticsearch

Elasticsearch 简称 ES，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，可以使用户快速的近乎于准实时的存储、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需求强大应用的基础引擎或技术。

(1) 产品规格

按套为数量。

(2) 功能特性

① 分布式的搜索引擎和数据分析引擎

搜索：比如百度网站的站内搜索，IT 系统的检索。

数据分析：比如电商网站，分析最近 7 天销量排名前 10 的商家有哪些。分析新闻网站最近 1 个月访问量排名前 3 的新闻版块是哪些。

② 全文检索，结构化检索，数据分析

全文检索：比如想搜索商品名称包含牙膏的商品。

结构化检索：比如想搜索商品分类为日化用品的商品都有哪些。

数据分析：比如分析每一个商品分类下有多少个商品。

③ 对海量数据进行近实时的处理分布式：Elasticsearch 可以自动将海量数据分散到多台服务器上去存储和检索。

海量数据的处理：分布式完成后，便可采用大量的服务器去存储和检索数据，实现海量数据的处理。

近实时：在秒级别对数据进行搜索和分析。

(3) 使用限制

参考列表：

规格	最大节点数	单节点最大磁盘（查询）	单节点最大磁盘（日志）	单节点最大磁盘（通常）
2C 4G	10	40 GB	200 GB	100 GB
2C 8G	10	80 GB	400 GB	200 GB
4C 16G	20	160 GB	800 GB	512 GB
8C 32G	40	320 GB	1.5 TB	1 TB
16C 64G	50	640 GB	2 TB	2 TB

(4) 产品优势

金融云 Elasticsearch 具有以下特点和优势：

实时检索和分析支持 PB 级数据实时搜索和分析，支持毫秒级快速响应。

商业版 X-pack 插件提供企业级权限管控、实时系统监控等强大服务。

稳定可靠金融云 IaaS 支持灾备和容错机制，数据存储稳定可靠。

部署维护简单自动化部署，0 成本运维，提供完善的系统监控模块。

可视化分析集成 Kibana 模块，可视化数据分析、后台管理。

中文分词默认整合主流插件，包括第三方 IK 中文分词插件。

弹性扩展支持弹性扩展到上百台服务器，服务器硬件配置可以伸缩。

技术支持，提供完善的产品文档。

九、增值类服务

1、其他设施类

（1）混合云部署（4U+0.5KW 机柜）

满足用户灵活放置私有设备的需求，使整个系统的设备相对集中，方便运维管理。

使用场景：配合物理机使用，用户自行对空间进行使用。

（2）USB 虚拟化服务

提供客户 USB Key 设备接入服务，满足虚机应用系统访问 USB Key 硬件设备的需求。

使用场景：配合物理机使用，上交所技术负责集中存储相关配置工作，物理机能识别到对应存储空间，用户自行对空间进行使用。

（3）呼叫中心网关（30B+D）

呼叫中心网关（30B+D）：满足用户对呼叫中心网关设备的需求，使整个系统的设备相对集中，方便运维管理。

使用场景：办公使用，用户负责线路申请，上交所技术配合接入并协助用户网络打通，用户负责线路申请，上交所技术配合接入并协助用户网络打通。

2、VPN 服务

提供用户云内 VPN 服务，以镜像方式提供 VPN 服务（深信服、华耀、山石），基于 internet，通过加密通道的方式实现用户数据中心与云内资源互通。

① 使用场景

VPN 网关是一款基于 Internet 的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或 Internet 终端与证通云专有网络（VPC）安全可靠的连接。

VPN 网关配置灵活，可满足不同的应用场景。

VPC 到本地数据中心的连接：您可以通过 IPsec-VPN 将本地数据中心和 VPC 快速连接起来，构建混合云。

图 9-2-1 VPC 到本地数据中心的连接

VPC 到 VPC 的连接：您可以通过 IPsec-VPN 将两个 VPC 快速连接起来，实现云上资源共享。

图 9-2-2 VPC 到 VPC 的连接

VPC 到移动客户端的连接：您可以通过建立 SSL-VPN 隧道将单个移动客户端和 VPC 连接起来，满足远程办公的需要。无论何时何地，只要有 Internet 就可以安全地接入 VPC。

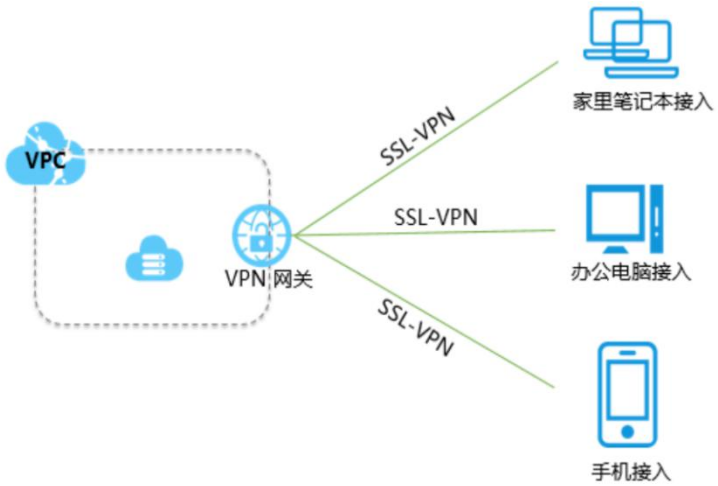


图 9-2-3 VPC 到移动客户端的连接

IPsec-VPN 和 SSL-VPN 组合使用：您可以组合使用 IPsec-VPN 和 SSL-VPN，扩展网络拓扑。客户端接入后，不仅可以访问 VPC，还可以访问接入的办公网络。

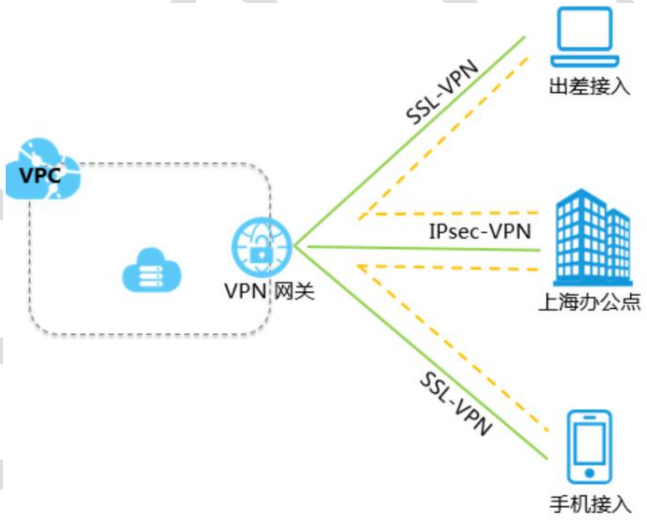


图 9-2-4 IPsec-VPN 和 SSL-VPN 组合使用

② 使用限制

在使用 VPN 网关前，您需要了解以下限制。

SSL 服务端端口 不能使用如下端口：22，2222，22222，9000，9001，9002，7505，80，443，53，68，123，4510，4560，500，4500。

SSL、IPSEC 授权购买周期为 1 年、2 年、3 年，不允许中途退出。

华耀 VPN 暂不支持 IPSEC 模块

因云内 VPN 以镜像方式提供服务，购买 VPN 产品会产生 ECS 费用，具体规格计费会在订单确认中体现。

授权并发 5 表示最多在线 5 个 VPN 用户，创建用户数不受限制。

3、桌面云服务

桌面云服务旨在满足不同证通云用户对托管环境多样化的需求。通过桌面云服务，证通云用户通过互联网或专线方式访问其在证通云上的 VPC 环境，提供安全、便捷、高效的工作方式。

（1）功能特性

兼容常用的运维工具、办公软件；

支持 USB 存储设备、USB 键盘鼠标等；

支持集中管理能力，如：对操作系统镜像统一管理、软件统一分发、终端统一管理等；

支持对重要用户的虚拟机进行备份和恢复；

系统具有完善的安全防护能力；

系统支持高可用性、动态迁移等可靠性设计；

系统支持通过扩容存储与计算资源实现用户平滑扩容。

（2）产品优势

采用业界主流云技术改造办公桌面，即将用户桌面集中在数据中心，通过虚拟化技术组建资源池，提供业务用户使用软终端、智能终端等移动接入，打造一种全新的、安全、便捷、高效的工作方式。

通过数据与用户隔离提升安全性：将原本分散在各 PC 上的用户桌面数据集中到数据中心，实现统一的安全管控，用户可访问的仅仅是桌面图像变化量，数据无法带出数据中心。

通过资源大集中提升运维效率：从分散的运维向集中化运维过渡，管理员通过后台便可处理用户的大多数问题，降低运维工作量并提升维护效率。

采用先进架构支撑未来演进：建立一个高效优化的、易管理的桌面云架构，同时未来能方便地扩展为企业私有云架构。

（3）产品规格

提供的虚拟桌面终端为 4C8G、200G 硬盘，操作系统为 Windows7。

十、服务能力

1、服务指标

证通云 IAAS 平台指标概述如下：

云计算平台总体可用性≧99.9%，一年内中断时间累计不超过 9 小时(不计计划内停机时间)；

云计算平台 7*24 小时普通服务，5*8 小时专家服务；

云计算平台服务响应时间 15 分钟；

虚拟机故障恢复时间 15 分钟。

2、安全保障

（1）物理与环境安全

① 机房安全保障

机房标准：满足《计算机场地技术要求<GB2887-89）》、《电子计算机机房工程施工及验收规范(SJ/T30003-93)》、《电子计算机场地通用规范（GB/T 2887-2000）》的要求。

机柜要求：19 英寸标准机柜，高度 42U，机柜深度 800mm 至 1000mm，机柜采用全钢材料，承重 300Kg。

供电保障系统：提供两路市电+UPS+油机供电系统，保证 99.99%以上的持续供电率。每个机柜提供 1000W 的功率。

空调系统：机房温度 22±2 0C（夏季），20±2 0C（冬季）；相对湿度始终保持在 45%与 65%之间，温度变化率小于 5 0C/h,要求不凝露。

安全保障系统：实时 CCD 摄像监控。

门禁系统：感应式门禁、联机管理。

消防系统：高灵敏度火灾自动报警系统；环保型气体灭火系统。

防雷系统：满足执行 10/350us 波形，可防护雷电流 150KA。

漏水检测系统：可提供各类液体泄漏的实时检测、报警。

综合布线：采用超五类布线系统。

接地系统：包括交流工作地、安全防护地和防雷保护地。

荷载要求：机房地板承重达 600Kg/ m2 以上，结构稳固。

抗震要求:按 8 度抗震能力设防。

清洁：高度洁净环境。

② 供电保障

两路一类市电采用 10KV 三相线路，互为主备用；

双路冗余大功率智能 UPS 系统，保证持续供电；

双备份柴油发电机组,外加一台柴油发电机作为后备电源,保证 99.99%持续电力供应；

交流电 220V50HZ（16A 或者 25A）标准 19 英寸机架，每个机柜采用两路完全独立 UPS 电源直接供电；机架内设置足够多电源插座，能够根据用户需求，提供足够的电力供应。

③ 空调保障

配置 2 个制冷站，包含高压离心冷水机组和螺杆冷水机组；

N+2 模式的机房模块精密空调设计；

冷冻水主干管环网，不间断供应冷冻水。

④ 网络保障

支持 SSCCNET 接入，接入速率为 1G；

SSCCNET 可用性为 99.99%；

SSCCNET 实施 7*24 小时监控，响应时间为 5 分钟；

支持中国电信、中国联通、中国移动等运营商网络。

⑤ 消防保障

机房配备七氟丙烷气体灭火系统；

监控室采用配置消防水喷淋系统；

全覆盖的极早期消防报警系统，充分保障火灾报警的及时性和灵敏性。

⑥ 安全保障

实时高清摄像监控系统，全程摄录机房所有进出口与通道，视频数据保留三个月。

感应式+密码锁双重认证门禁系统，各门禁读卡信息联网至监控中心，所有刷卡日志信息永久保留。

园区由专业保安 24 小时值守，有严谨的进出机房人员验证登记制度，及设备进出管理制度。

（2）灾难恢复和业务连续性

为确保运行于证通云的业务活动的连续性，保护业务流程不会受信息系统重大失效或自然灾害的影响，并确保他们的及时修复，证通云严格执行灾难恢复与业务连续性管理要求，主要包括：备份管理与数据恢复、制定和实施业务连续性计划、灾难恢复演练。

① 审计安全

云安全审计系统是证通云平台进行可信云认证、信息安全等级保护制度第三级要求认证不可或缺的一部分。相对于传统 IT 系统，云平台中服务组件众多、通信结构复杂，收集云平台日志信息、监控网络流量、记录用户操作，在运行维护、安全责任追究、事后查证等方面具有重要利用价值。将安全审计系统应用到云平台中，能有效的对云平台管理员和用户的行为进行监控与记录，对云平台各服务组件的日志进行汇聚、挖掘和分析，然后根据审计规则识别异常行为，进行自动告警和处理，能够进一步保障云平台的安全。

② 应用安全

证通云为各类证通云应用提供基础设施服务（IaaS），各租户承担各自应用系统的安装、调试、维护、运维、安全、合规的全部责任。证通云可为租户提供应用安全方面的技术支持和服务包括：

身份鉴别：租户用户 ID 及密码的分配和维护，在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护；

访问控制：租户用户的访问权限分配和维护；

安全审计：可根据租户要求记录并保存用户的登录及操作，审计记录包括安全事件的主体、客体、时间、类型和结果等内容。提供审计记录查询、分类、分析和存储保护；确保对特定安全事件进行报警；确保审计记录不被破坏或非授权访问；

应用安全防护：针对 WEB 类应用部署 WAF、WEB 漏扫系统、木马防治等专业的安全防护设备。

③ 数据安全

提供数据存管产品，用户可以根据需要将数据存放在数据存管平台中，实施数据的异地备份。数据存管平台存放证券、基金、期货等客户的交易、账户等核心数据。数据可靠性和安全性得到足够保证。数据存储形式主要包括虚拟机镜像和存储卷，原则上数据库数据存放在专业存储上，其他应用主机操作系统及应用数据可选择分布式存储方案。

（3）产品服务 SLA

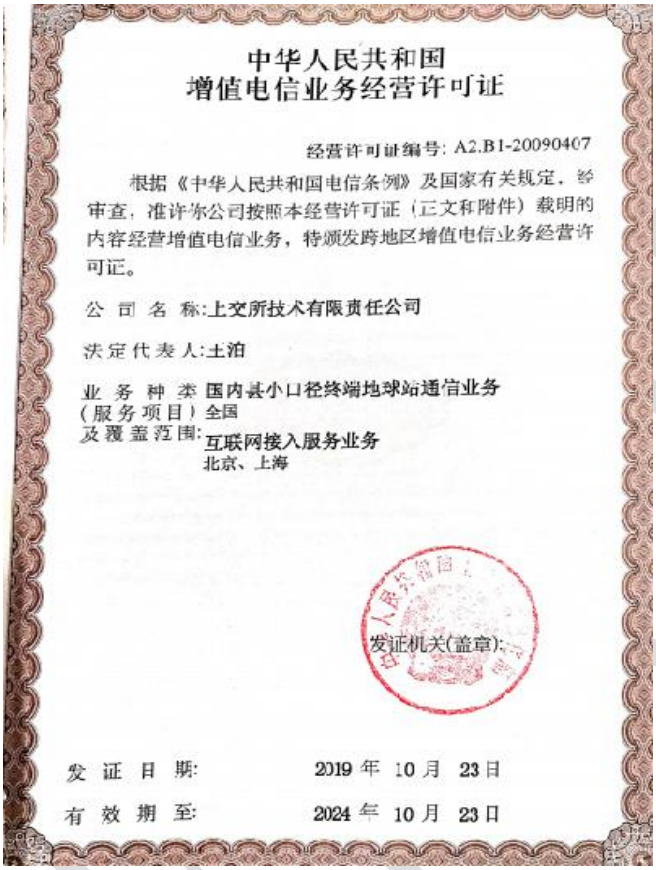
产品	SLA 承诺	服务可用性计算公式
ECS	对于单实例维度， 证通云承诺一个服务周期内 ECS 的服务可用性不低于 99.9%	服务可用性=（单实例服务周期总分钟数 - 单实例服务不可用分钟数）/单实例服务周期总分钟数×100%
ECS	对于单地域多可用区维度，证通	服务可用性=（单实例服务周期总分钟数

	云承诺一个服务周期内ECS的服务可用性不低于99.95%	- 单实例单地域多可用区服务不可用分钟数）/单实例服务周期总分钟数×100%
OSS	对于对象存储服务维度，证通云承诺一个服务周期内OSS的服务可用性不低于99.90%	服务可用性=（1 - 服务周期内5分钟错误率总和/（12*24*服务周期的天数））×100%　　每5分钟错误率=每5分钟失败请求数/每5分钟有效总请求数×100%
RDS	对于单实例维度，云数据库RDS Mysql服务可用性不低于99.9%	服务可用性=（单实例服务周期总分钟数 - 单实例服务不可用分钟数）/单实例服务周期总分钟数×100%
Redis	对于单实例维度，云数据库Redis服务可用性不低于99.9%	服务可用性=（单实例服务周期总分钟数 - 单实例服务不可用分钟数）/单实例服务周期总分钟数×100%
排除条款： 不包括以下原因所导致的服务不可用： （1）证通云预先通知客户后进行系统维护所引起的，包括割接、维修、升级和模拟故障演练； （2）任何证通云所属设备以外的网络、设备故障或配置调整引起的； （3）客户的应用程序受到黑客攻击而引起的； （4）客户维护不当或保密不当致使数据、口令、密码等丢失或泄漏所引起的； （5）客户的疏忽或由客户授权的操作所引起的； （6）客户未遵循证通云产品使用文档或使用建议引起的； （7）云数据库实例在进行日志重放（即redo或recovery）操作过程中所消耗的时间； （8）本地盘出现宕机数据会被擦除，依赖本地盘及本地盘中数据作为启动依赖项而导致的不可用； （9）由于客户所安装软件或者其他非证通云直接运营的第三方软件或者配置引起的ECS实例出现错误； （10）由于客户违反《云服务器（ECS）服务条款》导致的服务被暂停或终止，包括但竞价实例因为客户的出价低于交割价格而被释放；由于欠费导致ECS实例被暂停服务或被释放等； （11）《云服务器服务（ECS）服务条款》中所描述的证通云对ECS正常维护、升级所引起的短时服务中断； （12）不可抗力引起的。		

（4）资质证书

证通云面向行业，熟悉行业监管政策，可辅助监管，进行风控，快速协同应急。同时更加熟悉场检标准，助力客户快速通关。另外证通云具备金融级别的安全防护措施，例如数据加密机制，同时证通云客户群集中（都

是金融机构），数据封闭。目前，证通云平台通过信息系统三级评测并具备增值电信业务经营许可证。



中华人民共和国
增值电信业务经营许可证

经营许可证编号：A2.B1-20090407

根据《中华人民共和国电信条例》及国家有关规定，经审查，准许本公司按照本经营许可证（正文和附件）载明的内容经营增值电信业务，特颁发跨地区增值电信业务经营许可证。

公 司 名 称：上交所技术有限责任公司

法 定 代 表 人：王泊

业 务 种 类（服务项目）及覆盖范围：国内最小口径终端地球站通信业务 全国
互联网接入服务业务 北京、上海

发证机关（盖章）：

发 证 日 期：2019 年 10 月 23 日

有 效 期 至：2024 年 10 月 23 日

图 10-2-1 证通云增值电信业务经营许可证

图 10-2-2 证通云通过信息系统三级评测

证通云提供一对一的快速响应渠道，即时响应您的合作需求、疑问解答需求、技术支持需求等，我们的服务团队为您提供全天候的专业支持与服务。

7*24 小时的客服为您即时解答有关证通云的所有非技术类疑问，即时响应客户的业务需求。

十一、解决方案

针对云上服务的用户制定四大类解决方案，包括新筹基金 IT 系统上云、证券/基金灾备系统上云、券商/基金互金系统上云以及托管云解决方案。

1、新筹基金 IT 系统上云

（1）客户需求

在有限的时间内，经济快速地完成基础设施、服务器、核心系统的搭建及调测，具备上线条件。

（2）解决方案

上交所技术公司根据《证券基金经营机构信息技术管理办法》和新筹基金 IT 系统场检要求，联合 ISV 一起为新筹基金提供包括基础设施、硬件设备、核心业务系统的“一站式”云化解决方案，帮助新筹基金快速完成 IT 系统建设。

图 11-1-1 新筹基金 IT 系统上云解决方案

（3）方案价值

云资源快速提供，业务系统适配证通云，缩短 IT 系统建设周期。

按照使用量付费，大大降低新筹基金初期投入及后续运维成本。

证通云安全合规，提高场检通过率，避免多次场检带来的开业延期。

资源弹性扩容，快速应对业务增长带来的压力。

2、券商/基金灾备系统上云

（1）客户需求

建立同城或异地灾备中心，保障业务连续性，满足业务系统 RPO/RTO 要求。

有效控制资金投入，降低使用成本，业务快速上线。

（2）解决方案

根据《证券基金经营机构信息技术管理办法》要求，重要信息系统应当具备灾难及重大灾难应对能力。上交所技术公司基于证通云平台，联合 ISV 一起为券商、基金提供低成本、高效率的云化灾备系统解决方案。

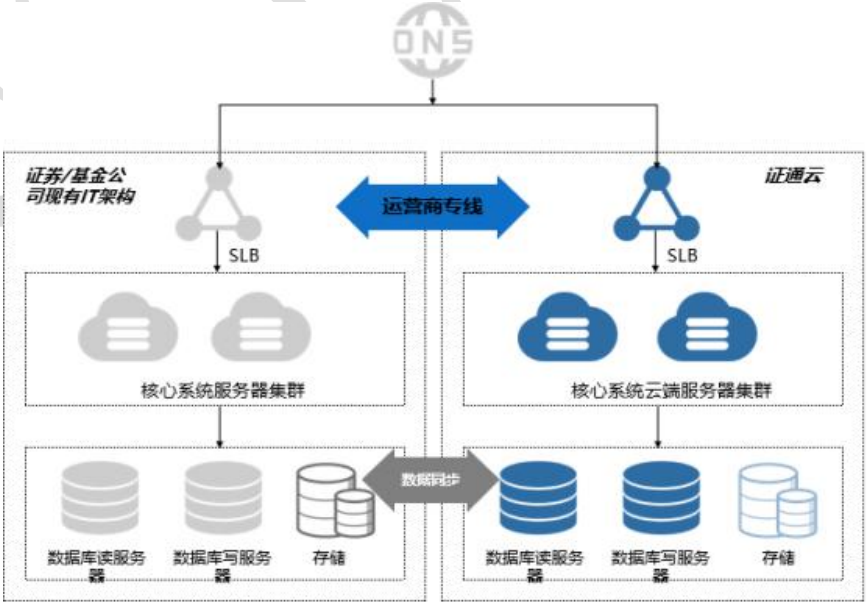


图 11-2-1 券商/基金灾备系统上云解决方案

（3）方案价值

方案满足监管机构关于 RPO/RTO 要求。

基础资源快速提供，高效实现灾备系统建设。

按照使用量付费，大大降低灾备系统建设和运维成本。

采用“小火种”模式，降低灾备系统日常运行费用。

3、券商/基金互金系统上云

（1）客户需求

满足券商、基金互金业务快速上线及快速扩展需求。

（2）解决方案

满足金融行业监管要求，提供券商、基金互金业务快速上云解决方案，通过统一的基础设施监控，配合券商、基金日常运维。

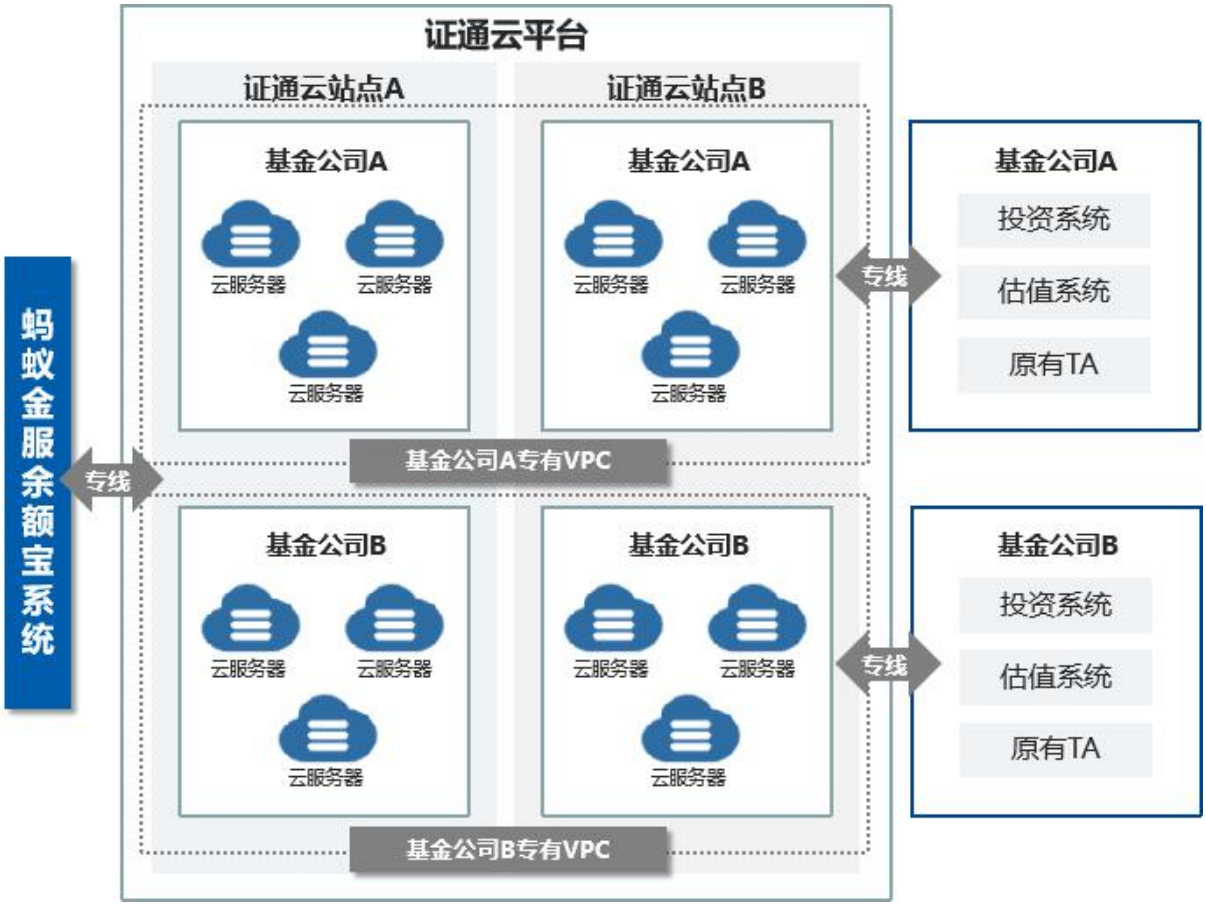


图 11-3-1 券商/基金互金系统上云解决方案

（3）方案价值

证通云同城双活站点部署，7*24 小时保障业务连续性。

基础资源弹性扩展，保障业务量激增情况下的资源快速平滑扩容。

基于统一架构部署，大幅缩短业务上线周期。

4、托管云

（1）客户需求

满足用户对云资源自主控制及高效率建设私有云的需求。

（2）解决方案

基于上交所技术公司高等级托管机房及专业的云建设和运维团队，根据用户需求提供定制化的私有云解决方案。

根据用户实际上云需求提供托管云解决方案，用户无需自行建设机房，无需采购服务器、网络、存储等硬件设备，可直接购买证通云服务提供商的计算、存储和网络资源，同时也无需花费设备的维护费用。

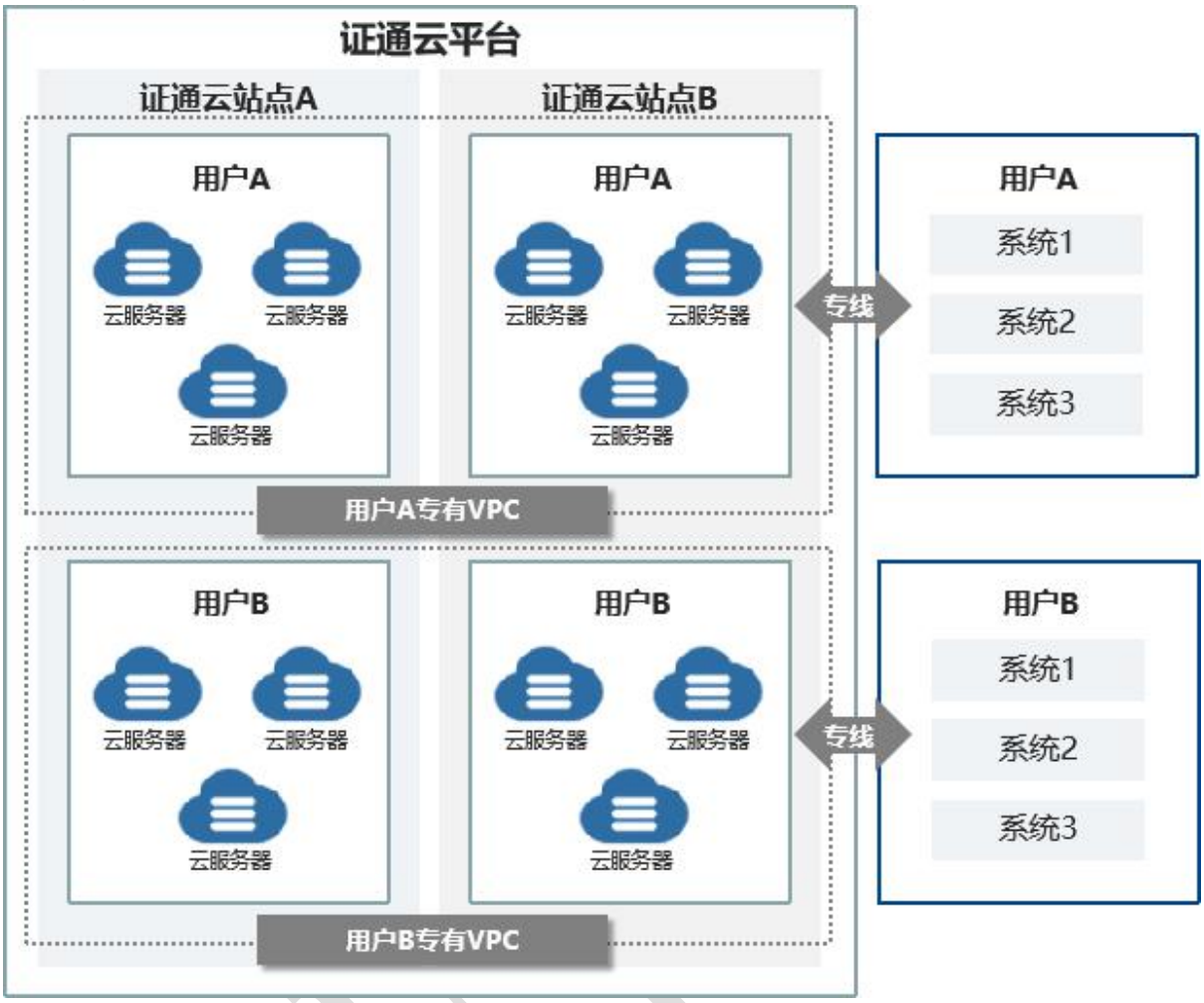


图 11-4-1 托管云解决方案

（3）方案价值

单独隔离的私有云资源池，满足用户对云资源自主掌控及更高安全性的需求。

可与行业云资源一起构建混合云，并通过云管系统统一管理。

用户无需自行采购机房、硬件设备、网络、系统，降低了建设及运维成本。

上交所技术有限责任公司
地址：上海市浦东新区外高桥保税区台中北路 8 号
邮编：200131
电话：021-58656238
网址：https://www.ssetech.com.cn/statics/