云平台备份和容灾技术白皮书

胡玉斌 2021111054

摘要：当前，IT 信息系统已经渗透到各行各业的业务建设之中。用户业务系统的稳定可靠运行是用户业务发展的重要基础。本文作为一套完整的云平台的备份和容灾技术的设计方案，从数据备份，系统容灾，为多个典型场景构建解决方案。

关键词：备份，容灾，设计方案

1 技术概述

备份和容灾技术起源于人类的技术发展，在各种工程、系统建设过程中都有广泛应用。中国古代著名水利工程都江堰通过分水鱼嘴和宝瓶口等结构的联合运用，实现了抗洪容灾的功能。

由于 IT 信息系统在不受保护的情况下非常脆弱，比如断电即刻导致系统瘫痪，故 IT 信息系统是备份和容灾技术的重要应用领域。对于政府、组织和企业 用户，一旦重要 IT 信息系统停摆，业务体系将受到巨大冲击。据 University of Minnesota 的研究，当发生重大数据丢失事故后，半数以上的公司会在两三年内倒闭。因此，IT 信息系统的备份和容灾技术应用，越来越重要，也越来越被重视，国家和行业标准中规定了明确的技术要求。

备份和容灾在 IT 信息系统中主要指数据备份和系统容灾两项技术。数据备份技术是系统容灾技术的重要支撑，但数据备份技术也可以单独在系统中实施。最早在数据备份和系统容灾技术上有重大突破的是美国。早在 40 年前 SunGard 公司就在美国的费城建成了数据备份和系统容灾中心，用于保护金融业务系统。

1.1 数据中心灾备市场的普及和发展

随着云计算等新兴技术的成熟，数据中心灾备服务在行业的应用已经越来越广泛。结合以往有关数据中心的研究和本白皮书的调研，我们发现数据中心灾备服务正在快速普及和发展，并呈现出以下态势：

- 数据中心灾备服务已经在传统行业高度普及，如政府，金融，制造等行业，同时在新兴行业也在快速发展，特别是互联网行业企业尤为突出，该行业既是数据中心灾备服务的使用者，也是服务提供者。
- 原本具备一定规模和实力的企业才能使用的数据中心灾备服务，如今已经快速向中小企业客户渗透。本次调研中，超过 70%的受访企业是规模在百人以下的中小企业客户。这主要得益于云服务的普及使数据中心灾备服务的交付成本和难度大大降低。其中还有 26.8%的客户以全部或者部分外包的形式使用数据中心灾备服务。

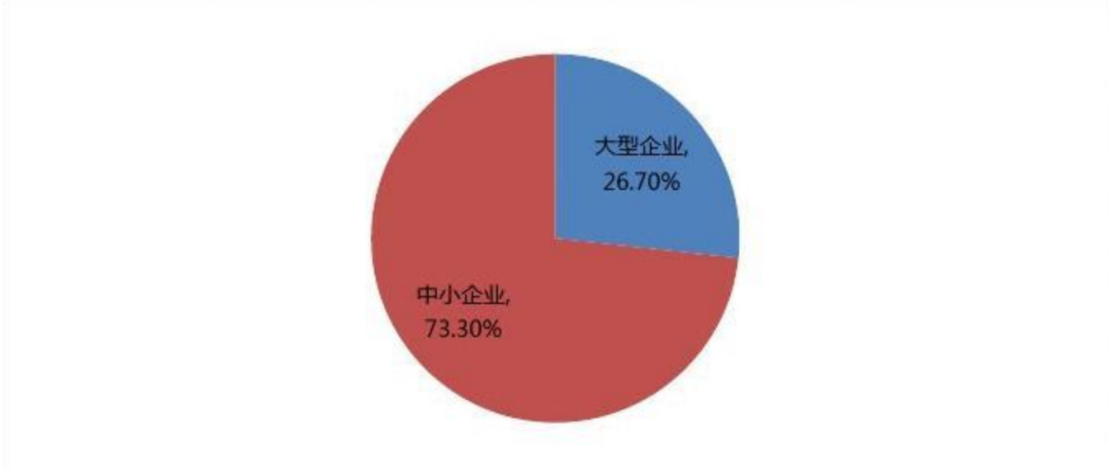

图 1 数据中心灾备用户比例

- 数据中心向新兴技术转型，特别是基于云计算建设已经是大势所趋。本次调研数据显示，超过 80%的企业在这方面有长期的发展规划，其中超过一半的企业已经在使用基于云的数据中心灾备服务，或者已经有计划向云计算转型。
- 不仅如此，在数据中心灾备服务应用方面比较领先的行业，如政府、金融、电信等行业，已经出台了严格的行业规范，甚至出台了相应的政策来促进和指导该市场的发展，包括鼓励和扶持、资金、税务、建设用地、监管等方面。

数据中心灾备服务市场的发展虽然是大势所趋，但也并非一帆风顺。本次调研的结果显示，当前企业在规划和使用数据中心灾备服务方面面临的挑战基本上在数据中心建设和使用的各个环节都有所体现，甚至覆盖了整个生命周期。比较突出的问题集中在建设、成本、利用率、管理、标准化等方面。另外，有些客户对数据中心灾备的信任度不高，技术方案的可行性不高，以及市场上众多复杂的技术方案缺乏标准化造成客户无从选择，也是客户反映的问题和制约该市场发展的因素。

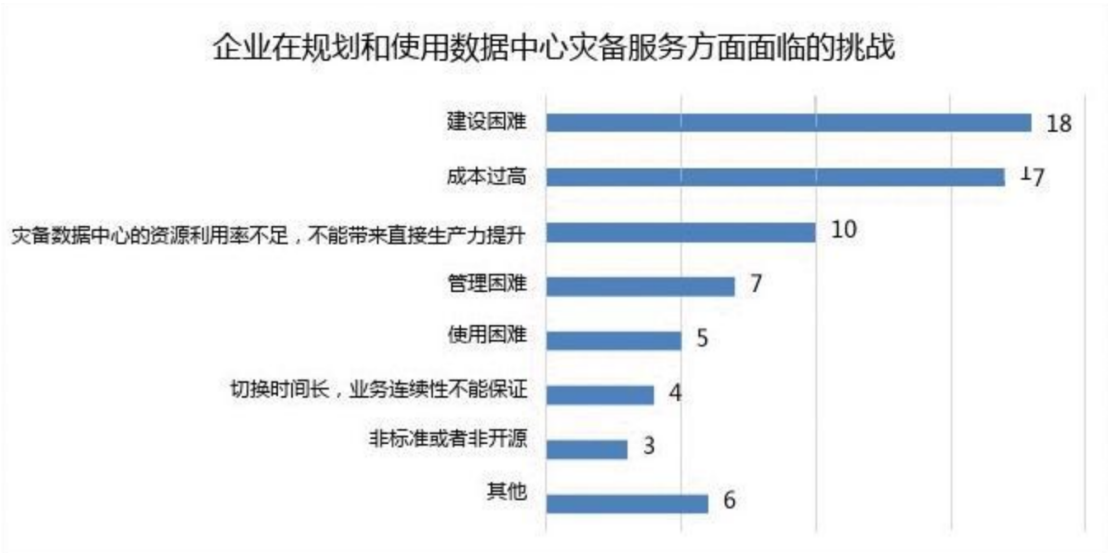

图 2 企业在规划和使用数据中心容灾服务方面面临的挑战

根据调研结果，我们的云平台备份和容灾的着力点也就确定了。

1.2 云平台数据备份技术

数据备份技术的核心是将生产环境中的在线数据通过技术方法备份到离线环境。当系统发生问题，则技术人员能够基于备份数据将数据恢复到理想的状态。备份数据并不用于业务生产，但保留关键版本的备份数据对业务系统的长期有效运行具有非常重要的意义。

根据业务场景和备份环境的不同，云平台提供两种主要的数据备份方式:一是支持在云平台上建立数据备份环境并将用户的业务系统核心数据安全可靠地备份到云平台上。二是支持将数据通过网络专线或 VPN 的方式备份到用户自有的数据中心。

云平台支持云平台或用户自建数据中心的数据库、文件、对象存储备份。通过网络专线或 VPN 在用户的业务生产环境和数据备份环境之间搭建安全可靠的网络数据传输通道。若用户的业务生产环境和数据备份环境都搭建在云平台公有云上，则能够在业务生产环境和数据备份环境之间搭建高带宽网络通道，实现数据安全高速传输。云平台通过部署数据备份服务或数据备份工具，使数据备份过程简单高效。并提供强大的资源监控工具，当系统出现问题，技术人员能够及时准确了解情况，并进行快速稳妥处理。

在数据备份技术方面，云平台支持数据库的迁移和复制、对象存储中数据的迁移和复制、文件系统中的文件迁移，并支持数据传输加密保护。利用云平台提供的快照功能，用户能够快速将数据恢复到所需的版本。云平台也提供完善的资源监控系统，使用户能够完全掌握数据备份过程中系统的运行情况，并在发生异常时发出报警提示。

1.3 云平台系统容灾技术

系统容灾技术的核心是当信息系统遭遇灾难并导致严重故障时能够保护客户数据安全和保持关键核心业务稳定。能够造成系统严重故障的灾难一般有地震、水灾、火灾、军事袭击、不当市政施工等，这些灾难在社会运行过程中均有一定发生的概率，因此在关键系统设计和建设时采取系统容灾技术进行有效保护非常重要。

云平台支持对系统的数据级容灾和应用级容灾。数据级容灾支持对客户的数据进行备份、同步复制或异步复制，维护客户数据安全，确保严重故障发生时关键数据可用和可恢复。应用级容灾支持建立与业务生产环境相匹配的备份系统，保证故障发生时及时将业务流量切换到备份环境，使业务系统持续对外提供服务。

云能够根据客户系统容灾需求并基于系统架构制定有效的容灾方案。通过丰富多样的系统容灾方案支持，提供多种系统容灾能力，满足客户的系统容灾需求。

- 冷备:支持数据的定期备份，并利用未运行的系统作为生产系统的备份环境，当大范围系统故障发生时启动备份系统支撑业务系统运行。
- 温备:支持数据的定期备份或周期性同步，利用周期性运行的系统作为生产系统的备份环境，备份环境中的系统定期开启并进行必要的系统同步操作。
- 热备:支持数据的定期备份或数据复制，在容灾环境建立最小化运行的热备份系统，当大范围系统故障发生时容灾环境接替原生产环境提供服务，并根据业务情况扩展资源。
- 双/多活:支持数据的同步复制，建立两个或多个相互隔离的业务生产环境，并保持各个业务生产环境的数据一致性。

利用云平台底层资源的容灾能力，支持多种系统容灾架构，充分满足不同行业客户的实际业务需求。

- 跨故障域容灾:云平台提供故障域支持，实现了在同一可用区内相互独立的供电、网络设施等基础设施建设。
- 跨可用区容灾/双活:利用云平台的负载均衡技术，客户能够便捷地实现跨可用区系统容灾，或实现两个可用区内双活系统架构。云平台在同一地域内的可用区之间相隔

数十千米，采用相互独立的双路供电系统，能够满足大多数客户的容灾架构需求。

- 两地三中心架构容灾:通过在不同的地域搭建业务系统，使系统获得极大的抗灾能力。
- 异地多活架构容灾:在多个可用区和多个地域建立同时运行的业务生产系统，在提升系统大范围抗灾能力的同时，能够保障系统最佳的灾后恢复速度。不同的容灾系统架构对应不同的系统容灾能力和灾难发生后的系统恢复效率，同时也会产生不同的系统建设和维护成本。云平台支持客户根据行业标准和实际需求选择最适合的容灾架构。

1.4 平台工具和服务

基础云服务。云平台根据安全性、数据规模、资源扩展性等客户需求，提供公有云、私有云、专有云、混合云等多种可选的备份容灾环境，通过专业的技术服务帮助客户高效合理的构建云计算环境下的业务系统和备份容灾系统，并提供可靠的后期技术保障支持。

网络支撑。云平台通过支持 VPN、网络专线、负载均衡、DNS 等多种网络技术，帮助客户在建设备份和容灾系统时获得可靠的网络技术保障，确保数据传输的安全和灾后数据流量切换的及时有效。

存储支撑。云平台通过支持多种 RDS(关系型云数据库服务)、海量对象存储 OSS 和大容量高性能云硬盘，为客户提供可靠的数据备份环境，并基于多副本机制确保客户数据不会丢失。

1.5 安全保障

云平台在实现数据备份功能的同时，还通过有效的技术手段确保备份过程和恢复过程安全可靠。

数据安全方面，系统通过网络安全、数据安全和数据可靠性保障等措施确保数据备份过程的安全。在网络传输过程中，支持建设网络专线保障数据安全快速传输，也支持搭建 VPN 实现数据加密传输，并通过 SSL 数字证书进行身份认证，有效保护数据在网络传输过程中的安全。在数据安全保护方面，利用有效的身份认证和访问控制机制，确保只有合法客户才能访问在权限范围内的数据。利用静态数据加密技术，保护在数据备份端落地存储的数据，满足在公有云等开放环境中也能确保客户数据安全。利用云平台提供的组合隔离技术，防止数据被非法访问。在数据的可靠性保障方面，支持数据库和对象存储的数据复制和多副本机制，并通过数据的完整性和一致性校验确保数据不会丢失。

在系统可用性保障方面，支持云主机热迁移、高可用组、跨可用区高可用、跨地域高可用，全面保障系统的长期稳定运行。

2 数据备份解决方案

2.1 适用场景

我国信息技术发展迅猛，IT 信息系统的应用领域极为广泛。但从各行业和部门信息系统建设和维护状况中，可发现仍然存在下面的诸多问题需要解决:

- 在互联网、游戏、传媒等行业，要不断根据新需求对系统进行快速迭代，会发生更新导致数据污染、数据损坏等异常。
- 由于产业发展迅猛，导致技术人才缺口增大，出现系统运维人员技术能力参差不齐的情况，易出现系统运维操作给系统数据带来负面影响的情况。
- 存储介质存在固有的故障率，在系统集群规模较大的情况下，发生存储硬件故障的概率较大，给系统中存储的数据带来丢失或不一致的风险。

云平台非常重视对数据的可靠性和一致性进行保护，为提升客数据的安全性，云平台提供的数据备份解决方案除能够较好地解决上述的几个主要问题，并能够适用于以下一些主要场景:

- 数据为核心资产之一。对某些客户，数据是核心资产，若失去数据则可能导致客户失去在市场中的竞争优势或失去业务运行的基础。云平台能够提供成熟的数据备份技术，并提供安全可靠的数据备份环境，帮助客户保护数据，维护客户核心利益。
- 标准、规范要求。数据备份已成为国家和行业针对重要业务系统提出的标准和规范的重要组成部分。云平台能够帮助客户实现满足标准和规范要求的 IT 支撑系统，使客户的业务系统满足监管机构的技术要求。
- 数据影响业务发展。在政府、组织、企业中，数据对其未来的发展起到越来越重要的作用。云平台能够帮助政府、组织、企业等重要客户实现可靠的数据备份系统，支撑系统快速迭代发展，保障数据的可靠性和一致性。
- 旧系统升级改造。由于技术发展历史原因，某些较老的信息系统的数据可能还存储在没有有效保障的环境，客户不希望投入过多经费对系统进行升级。云平台能够为客户提供高性价比的数据备份解决方案，利用云平台丰富的 IaaS 资源，帮助客户快速而又低成本地实现原有系统的改造，保障数据的安全。

2.2 技术方案

2.2.1 网络架构

- 线上业务数据备份到云硬盘或硬盘
- 线上业务数据备份到 OSS
- 线上业务数据备份到远程数据备份环境

2.2.2 产品数据备份与恢复

当系统遇到自然灾害或 人为灾难导致大范围故障时，云平台提供及时、专业的技术支持服务，帮助客 户快速恢复关键数据，降低系统损失。

2.2.2.1 数据库

云平台数据库备份工具和服务支持 MySQL、SQL Server 等关系型数据库，支持 MongoDB 等非关系型数据库，也支持 TiDB 等 NewSQL 数 据库。云平台通过数据库备份服务代理，将待备份的数据通过网络专线或 VPN 备份到云平台的 RDS、客户自建数据库和第三方云数据库。

云平台提供全量备份、增量备份、实时复制、数据库迁移等数据库备份服务，满足客户不同的数据安全性需求。当灾难发生并导致业务系统数据损坏时，备份环境中保存的数据确保客户关键业务数据不丢失，同时云平台将提供及时的技术支持服务，帮助客户快速恢复业务生产数据。

2.2.2.2 块存储和文件

云平台提供硬盘快照、数据多副本、数据实时复制、文件迁移等备份方式。当灾难发生并导致业务系统数据损坏时，备份环境中保存的文件确保客户关键数据不丢失，同时云平台将及时提供服务支持客户快速恢复关键数据。

2.2.2.3 对象存储 OSS

云平台对象存储产品 OSS 本身支持多副本机制，能够保障极高的数据可靠性。同时，云平台支持将客户存储在对象存储、文件存储、云硬盘或硬盘中的数据，通过备份服务代理，将文件备份到云平台的公有云、私有云、专有云、混合云的 OSS 中，也支持将文件备份到客户自有 IDC 或第三方云平台的对象存储中。

云平台提供 OSS 多副本机制、数据全量迁移、数据备份等备份方式。当灾难发生并导致业务系统数据损坏时，备份环境中保存的文件确保客户关键数据不丢失，同时云平台将及时提供服务支持客户快速恢复关键业务数据。

2.2.3 评估指标

- 数据库备份
  - RDS 备份配置
    - RPO < 1 小时
  - 备份工具增量备份
    - 可配置，可实现 RPO < 1 小时
  - 备份工具数据实时复制
    - RPO ≈ 0
- 块存储和文件备份
  - 云硬盘快照
    - 依赖手动执行频率，每天执行可实现 RPO < 24 小时
  - 备份工具数据实时复制
    - RPO ≈ 0
- 对象存储备份
  - 多副本机制
    - 支持 99.999999999%数据可靠性
  - 备份工具全量迁移
    - 依赖手动执行频率
  - 备份工具数据备份
    - 可实现 RPO < 1 小时

3 系统容灾解决方案

3.1 适用场景

IT 信息系统已经成为政府、各种组织和企业业务发展的关键，保障信息系统的稳定运行极为重要，但并非所有的系统都能满足长期稳定有效运行的要求。当系统没有依据客观情况进行合理的容灾设计的时候，会出现以下一些主 要问题:

- 当系统容灾的设计缺少或不规范时，一方面会导致系统不符合国家或行业的规范，另一方面当系统遭遇故障或灾难时会对业务带来巨大安全风险，轻则造成业务的停顿，重则造成企业的消亡。
- 当容灾设计与实际需求不匹配时，由于大量的资源投入和人员投入，会产生额外的巨大开销，造成资源和人力浪费。
- 设计不合理的系统容灾系统也可能造成在发生事故或灾难时无法按预定的 计划实现系统的恢复，对业务造成重大的冲击。
- 某些 IT 信息系统会承载多个客户的业务，不合理的容灾方案很可能在系统遭遇故

障或灾难时对系统上承载的业务造成损害，严重时产生法律纠纷。

3.2 技术方案

3.2.1 数据级容灾

在业务生产环境正常的情况下，系统主机中的应用系统访问业务生产环境中的数据库、块存储、对象存储等数据。同时，系统中的所有数据都同步或异步复制到系统容灾环境中。云平台通过提供稳定可靠、成本较低的数据库和存储资源，搭建理想的系统容灾环境。一旦在业务生产环境中的数据库、块存储设备、网络文件存储系统、对象存储系统等发生严重的故障而导致数据不可用时，支持将应用系统访问的数据地址切换到系统容灾环境，确保数据的一致和系统的稳定连续运行。

数据级容灾相比于下述的应用级容灾能够节省部署冗余的计算环境，因此可以大幅度降低整体系统的建设成本。

3.2.2 应用级容灾

建设应用级容灾系统时，需要在相隔一定距离的至少两个数据中心同时建设应用系统集群和数据库及存储系统。在数据库存储的数据和存储系统存储的文件层面，数据会在系统正常运行时实现两个或多个数据中心的同步，数据同步的频率依据客户的具体需求进行设定。同时，在系统容灾环境中，具有足够的数量的服务器集群，并能够在业务生产环境遭受重大灾难时接替业务生产环境的服务器集群进行工作，承接原有的用户业务流量。在灾难或重大故障发生时，云平台支持通过 DNS 切换或负载均衡切换的方式对网络进行调整，使业务流量能够顺利切换到系统容灾环境中。

应用级容灾相比于上述的数据级容灾能够承受更大的系统灾难和故障，通过冗余的计算资源承接用户的业务流量。而数据级容灾系统在服务器集群和数据库及存储系统同时遭受灾难时无法继续提供业务支撑，只能在服务器集群恢复运行后才能继续运行业务系统。

3.2.3 评估指标

- 主机容灾
    - 温备
        - RTO < 2 小时
    - 热备
        - RTO < 30 分钟
    - 双/多活
        - RTO < 2 分钟
- 数据库容灾
    - 冷备
        - RTO < 6 小时
    - 温备
        - RTO < 1 小时
    - 热备
        - RTO < 30 分钟
    - 双/多活
        - RTO < 2 分钟

4 典型场景和行业解决方案

4 .1 多级容灾解决方案

4.1.1 周级容灾

针对系统故障恢复能力要求不太高的客户(一般要求 RTO≤7 天)，云平台提供周级容灾解决方案，帮助客户在较少资源和人力投入的情况下实现系统的容灾保障。

在周级容灾方案中，重点针对用户客户的关键数据进行定时备份，并且支持在同地域或跨地域建立系统容灾环境。云平台支持通过在线传输或离线运输等方式实现关键数据的离线备份。

当业务生产环境发生故障时，云平台运维系统能够快速发现系统故障并发出预警信息。在系统容灾环境中启动作为冷备的服务器资源，或者在云平台上基于原有系统设计方案重新搭建可用的业务系统，而后管理员能够将业务流量切换至系统容灾环境，并对外提供有效的服务。当原业务生产环境的资源被修复后，再将全部数据恢复至业务生产环境。

周级容灾方案能够有效保护客户关键数据不会丢失，并一定程度上确保系统在短期内能够恢复服务，不但资源占用少，还能大幅降低容灾系统的建设和维护成本。

4.1.2 天级容灾

针对系统故障恢复能力要求一般的客户(一般要求 RTO≤1 天)，云平台提供天级容灾解决方案，帮助客户在一般资源和人力投入的情况下实现系统的容灾保障。

在天级系统容灾解决方案中，对客户系统中的数据进行定时备份，确保数据能够在系统容灾环境中有效保存。通过环境一致但处于长期休眠状态的冷备服务器，实现在系统容灾环境中保有能够替代业务生产环境中业务系统运行的服务器。云平台支持对业务生产环境和系统容灾环境的主机、数据库等系统进行实时的系统监控和定时的运维检查，及时发现大规模系统故障。

在业务生产环境发生大规模故障时，云平台运维系统能够第一时间检测到系统故障并对相关管理员发出预警信息。后续仅通过启动冷备服务器并进行系统自检之后，便可以将业务流量切换到系统容灾环境，使业务快速恢复运行。而后，当原有业务生产环境的资源恢复之后，在通过数据恢复和系统恢复技术使业务生产环境完全恢复。

天级系统容灾方案实现了对客户业务系统的有效保护，确保客户业务系统在遭受大规模灾难时不会长期停滞，满足长期的业务良好运转。

4.1.3 小时级容灾

针对业务系统停机会带来较大损失或造成较大社会影响的系统(一般客户灾难恢复容忍度 RTO≤4 小时，RPO≤1 小时)，为保障客户业务系统能够较快的恢复，云平台提供小时级容灾解决方案。

小时级系统容灾解决方案中，主要采用温备的方法对系统进行备份。在应用系统层，基于主机进行定期的状态同步。系统容灾环境中的云主机每隔一段时间(如小于 4 小时)启动运行，在完成主机的关键数据和系统状态同步之后再进入休眠状态。在数据层，对数据库进行实时复制或定时备份，确保数据在系统容灾环境中与业务生产环境中的差异控制在一定时间范围之内。基于云平台提供的系统资源监控服务，对业务生产环境和系统容灾环境中的主机和数据库进行实时监控，能够及时发现系统故障。

4.1.4 分钟级容灾

针对金融等重要行业对系统灾难恢复能力要求很高的客户，为保障快速在系统灾难中进行恢复，云平台提供分钟级系统容灾解决方案，能够实现 RTO≤ 30 分钟且 RPO≈0。

4.1.4.1 同城热备容灾解决方案

云平台为客户在同城或异地提供完整的系统容灾环境，承载用于容灾的云主机和数据库资源。为降低客户建设和维护成本，可采用最小模式运行用于热备的云主机集群。即，处于运行状态的云主机满足客户业务的最小需求，从而减少冗余资源的资源用量。利用云平台的数据复制技术，实现数据库之间的实时数据复制，保证系统容灾环境和业务生产环境中的数据一致，防止数据因故障丢失。

4.1.4.2 两地三中心容灾解决方案

在两地三中心容灾解决方案中，云平台支持在同一地域内建立跨数据中心的双活系统运行环境，并在第二个地域内建立异地系统容灾环境。在同一地域内的两个数据中心中的服务器集群实现同步的数据更新，保证当任一个数据中心发生故障时另一个数据中心都能承载全部业务流量。在业务生产环境两个中心和异地系统容灾环境中的数据库利用实时复制技术实现实时同步更新，确保数据不会丢失。

4.1.5 秒级容灾

针对系统灾难恢复能力要求最高的客户，云平台利用先进的负载均衡技术，提供秒级系统容灾解决方案。

- 同城双活容灾解决方案
- 异地多活容灾解决方案

4.2 行业解决方案

4.2.2 金融行业

根据重要性的不同，支持容灾 3 级标准到容灾 6 级标准。

4.2.2 政务行业

省级政务系统对业务连续性要求高，建议提供小时级和分钟级容灾解决方案。市县级政务系统相对规模较小，并且运维人员相对较少，建议提供天级容灾解决方案。

4.2.3 电商行业

需要根据电商的规模和种类，定制化不同的容灾系统。

5 总结

数据备份和系统容灾是保障客户业务长期有效运行的关键技术。作为一套完整的云平台的备份和容灾技术的设计方案，从数据备份，系统容灾，为多个典型场景构建解决方案。为客户基于云平台轻松构建安全、可靠的业务系统提供有价值的技术参考。

参考文献

[1] 《JR/T 0168-2018 云计算技术金融应用规范容灾》，中国人民银行

[2] 《重要信息系统灾难恢复指南》，国务院信息化工作办公室

[3] 《GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范》，国家质量监督检验检疫总 局

[4] 《华为云灾备白皮书》，IDC 华为