

数据中心容灾与高可用性架构设计与实现

黄伟灵

联通(广东)产业互联网有限公司

DOI:10.12238/jmsr.v2i2.6392

[摘要] 本文旨在介绍数据中心容灾与高可用性架构设计的原理、实现方法以及实践效果,以提高数据中心的稳定性和可靠性,确保业务运行的正常。首先介绍了数据中心容灾与高可用性架构设计的方法,包括数据备份、恢复、安全管理等方面,展示了数据中心容灾与高可用性架构设计的实践效果,包括数据中心的稳定性、可靠性和响应速度等方面的评估,以及对业务流程的影响和提升。研究表明,数据中心容灾与高可用性架构设计对于提高数据安全和业务可靠性具有重要意义和实用性。

[关键词] 数据中心; 容灾; 高性

中图分类号: N37 **文献标识码:** A

Design and Implementation of Data Center Disaster Recovery and High Availability Architecture

Weiling Huang

China Unicom (Guangdong) Industrial Internet Co., Ltd

[Abstract] This article aims to introduce the principles, implementation methods, and practical effects of disaster recovery and high availability architecture design in data centers, in order to improve the stability and reliability of data centers and ensure normal business operations. Firstly, the methods of data center disaster recovery and high availability architecture design were introduced, including data backup, recovery, security management, and other aspects. The practical effects of data center disaster recovery and high availability architecture design were demonstrated, including the evaluation of data center stability, reliability, and response speed, as well as the impact and improvement on business processes. Research has shown that disaster recovery and high availability architecture design in data centers are of great significance and practicality for improving data security and business reliability.

[Key words] data center; disaster recovery; high availability

引言

随着信息技术的快速发展,数据中心已经成为各种应用和服务的核心承载平台。为了保证数据中心的稳定和安全,容灾与高可用性架构设计变得至关重要。容灾是指提前制定好应急预案,以应对可能出现的灾难事件,确保业务数据的完整性和可用性。高可用性是指通过技术手段提高系统的稳定性和可靠性,减少系统故障对业务的影响。数据中心容灾与高可用性是确保数据安全和可靠的重要手段。在灾难发生时,容灾和高可用性措施可以快速恢复数据和应用程序,确保业务的连续性和数据一致性;在灾难发生时,容灾和高可用性措施可以快速恢复数据和应用程序,避免业务中断和数据丢失,保证业务的连续性。在某些行业和地区,数据中心的容灾和高可用性是法规和规定要求,容灾和高可用性措施可以避免数据丢失和损坏,在灾难发生时,容灾和高可用性措施可以快速恢复数据和应用程序,避免数据丢失和损坏;在灾难发生时,容灾和高可用性措施可以快速恢复

数据和应用程序,避免用户访问中断和数据不一致,提高用户体验^[1-6]。数据中心容灾与高可用性的重要性和必要性在于确保数据安全、业务连续性、遵守法规和规定、避免数据丢失和损坏,以及提高用户体验。

1 数据中心容灾架构设计

1.1 基本原理

数据中心容灾的基本原理包括备份、恢复和故障转移。这些步骤确保了在数据中心发生故障或灾难时数据和应用程序的可用性和可靠性。

(1) 备份是容灾过程的第一步。备份是指将数据和应用程序复制到另一个存储设备或位置,以防止数据丢失或损坏。备份可以是在线的或离线的,也可以是冷备份或热备份。在线备份是指备份数据可以实时更新,而离线备份是指备份数据不会实时更新。冷备份是指备份数据不会经常备份,而热备份是指备份数据会实时备份。

(2)恢复是容灾过程的第二步。恢复是指在数据中心发生故障或灾难时,使用备份数据将数据和应用程序恢复到正常运作状态。恢复点目标是确定需要恢复的数据和应用程序的状态。恢复程序是详细地说明如何恢复数据和应用程序的流程。恢复人员是负责恢复数据和应用程序的人员^[1]。

1.2设计思路

(1)地理位置:容灾架构需要考虑数据中心的地理位置。在灾难发生时,需要确保业务可以在另一个地理位置的数据中心继续运行。因此,容灾架构需要包括多个数据中心的备份和故障转移方案。

(2)数据备份:数据是容灾架构的核心。数据备份是指将数据复制到另一个存储设备或位置,以防止数据丢失或损坏。数据备份可以是实时的或非实时的,也可以是冷备份或热备份。

(3)应用程序备份:应用程序是容灾架构的重要组成部分。应用程序备份是指将应用程序复制到另一个服务器或虚拟机上,以防止应用程序失效。应用程序备份可以是实时的或非实时的,也可以是冷备份或热备份。

(4)网络备份:网络是容灾架构的重要基础设施。网络备份是指将网络设备、网络线路和网络协议备份到另一个数据中心或网络设备上,以防止网络失效。网络备份可以是实时的或非实时的,也可以是冷备份或热备份。

1.3技术方案

(1)备份服务器:备份服务器是容灾架构的重要组成部分。备份服务器可以是物理服务器或虚拟机,用于存储备份数据和应用程序。备份服务器需要具备高性能、高可靠性和数据保护功能^[2]。

(2)备份软件:备份软件是容灾架构的核心。备份软件是指将数据和应用程序复制到备份服务器上的软件。备份软件需要具备自动化、可配置和可管理的功能。

(3)备份存储设备:备份存储设备是容灾架构的重要组成部分。备份存储设备用于存储备份数据和应用程序。备份存储设备需要具备高性能、高可靠性和数据保护功能。

(4)备份网络:备份网络是容灾架构的重要基础设施。备份网络是指将数据中心之间的网络设备、网络线路和网络协议备份到另一个数据中心或网络设备上。备份网络需要具备高性能、高可靠性和数据保护功能^[3]。

1.4设计原则

(1)多样性:在设计容灾高可用性架构时,需要确保多样性,即采用不同的技术、设备和线路,以防止单一故障点。

(2)可靠性:容灾高可用性架构需要具备高可靠性,即备份数据和应用程序必须可靠,能够在短时间内恢复。

(3)实时性:容灾高可用性架构需要具备实时性,即能够实时备份和恢复数据和应用程序,以避免数据丢失和业务中断。

(4)可扩展性:容灾高可用性架构需要具备可扩展性,即能够随着业务的发展而扩展,以满足未来的需求。

(5)安全性:容灾高可用性架构需要具备安全性,即能够保

护数据和应用程序的安全,防止数据泄露和攻击。

1.5实现细节

在此基础上,提出了基于“双活型数据中心”的新型容灾模型,并从网络层、应用层、数据库层、云平台与存储层四个层面展开研究。

在网络层面上,为了确保数据传输的可靠性,提出了一种采用多个通信设备的备份方案。在节点出现故障时,采用 Smart DNS/Global 负载均衡等交换策略,使节点能够迅速地完成交换^[4]。

在一个应用层面上,在一个数据中心上建立一个应用程序簇。在B/S架构下,在局部数据中心和灾备中心,各自建立了一个应用服务器,各数据中心的应用服务器平台构成了一个高可用集群,并分别与相应的数据库平台相连接。在C/S体系结构下,若C/S系统不能实现分散配置,则主路由仅能在单一的数据中心上分发,导致系统仅能在单一的数据中心上正常工作,并可实现系统的失效后自适应转移。若C/S应用程序是分散的,且分别在各个数据中心(外部IP地址不一致),则需要人工设置相应的服务端IP,并在出现错误时进行访问切换。

针对其核心服务所需的数据库,利用扩展型分簇技术实现同一城市两个数据中心间的数据库级高可用性;采用数据库扩展簇技术,可以在存储空间上实现对数据库的双重访问,但在数据中心失效的时候,也会影响到数据库的其他数据,从而影响到整个应用系统的正常运转,而采用数据库的数据镜像技术,则可以确保数据的高可用性,在同一城市的两个数据中心中,任何一个数据中心失效,都可以做到零损失。在备份数据中,为确保数据的完整性,本项目提出在备份数据中使用数据库备份技术,在发生区域灾害时,可以将备份的数据转移到备份中心,以确保备份数据的完整性和完整性^[5]。

另外,对于应用运行所需要的其他数据,可以灵活地使用基于存储或者存储网关等数据复制技术实现多中心间的复制。

2 数据中心容灾备份策略

2.1备份策略设计

不同类型的数据的备份目标、备份频率和备份保留时间。不同的数据类型根据其重要性和恢复时间要求不同,采取了不同的备份策略。比如,数据库每天备份,并保留30天;文件系统每周备份,并保留3个月;系统状态每月备份,并保留6个月;应用软件每季度备份,并保留1年;用户数据每月备份,并保留90天;系统镜像每半年备份,并保留1年半^[6]。

2.2恢复策略设计

不同恢复目标的恢复方式、恢复时间和相应的恢复人员。不同的恢复目标根据其重要性和恢复难度不同,采取了不同的恢复策略和人员。比如,数据库恢复由DBA团队从云端存储恢复,需要在1小时内完成;文件系统恢复由系统管理员团队从本地磁盘恢复,需要在2小时内完成;系统状态恢复由系统管理员团队从云端存储恢复,需要在3小时内完成;应用软件恢复由应用软件支持团队从本地磁盘恢复,需要在4小时内完成;用户数据恢

复由用户数据管理团队从云端存储恢复,需要在5小时内完成;系统镜像恢复由系统安装和支持团队从云端存储恢复,需要在6小时内完成。

2.3高可用性监控

2.3.1系统监控

不同监控对象的监控指标、监控频率、监控阈值和相应的监控人员。不同的监控对象根据其重要性和资源使用情况不同,采取了不同的监控指标和监控阈值。比如,数据库的CPU使用率和内存使用率需要每分钟监控,并在使用率达到80%和90%时触发警报;文件系统的磁盘空间使用率需要每小时监控,并在使用率达到80%时触发警报;网络连接的连接数需要每分钟监控,并在连接数达到500时触发警报;系统状态的CPU使用率和内存使用率需要每分钟监控,并在使用率达到70%和80%时触发警报;应用软件的CPU使用率和内存使用率需要每分钟监控,并在使用率达到60%和70%时触发警报^[7]。

2.3.2故障诊断

表1 故障类型

序号	故障类型	故障症状	可能的原因	故障处理人员
1	网络故障	网络连接中断	路由器故障、交换机故障、光纤通道故障等	系统管理员团队
2	数据库故障	数据库无法连接或异常退出	数据库服务器故障、数据库软件故障、存储设备故障等	DBA团队
3	文件系统故障	文件系统损坏或无法挂载	磁盘故障、文件系统配置错误、操作系统故障等	系统管理员团队
4	系统状态故障	系统无法启动或异常停止	系统软件故障、硬件故障、操作系统故障等	系统管理员团队
5	应用软件故障	应用软件无法启动或异常退出	应用软件本身故障、系统环境问题、数据库连接问题等	应用软件支持团队

不同故障类型、故障症状、可能的原因和相应的故障处理人员。不同的故障类型根据其特点和影响不同,采取了不同的

故障症状和可能的原因。比如,网络故障可能是由路由器、交换机或光纤通道故障引起的;数据库故障可能是由数据库服务器、数据库软件或存储设备故障引起的;文件系统故障可能是由磁盘、文件系统配置或操作系统故障引起的;系统状态故障可能是由系统软件、硬件或操作系统故障引起的;应用软件故障可能是由应用软件本身、系统环境或数据库连接问题引起的。

3 总结

数据中心容灾与高可用性架构设计是保证数据中心稳定和安全的关键技术。通过合理的架构设计和实践案例,我们可以看到容灾与高可用性架构设计的实际应用和效果。然而,随着技术的不断发展和业务需求的不断变化,新的挑战和问题也将会出现。未来,数据中心容灾与高可用性架构设计需要更加智能、自动化和灵活。随着云计算、大数据和人工智能等新技术的应用,数据中心的规模和复杂性也将不断增加,因此,需要进一步研究和探索新的技术手段和方法,以应对未来的挑战。

[参考文献]

- [1]王猛,王霞,万成威.基于云的容灾双活数据中心构建技术研究[J].网络安全技术与应用,2023,(03):62-65.
- [2]翁文炳.医院数据中心容灾备份策略研究[J].科技资讯,2022,20(17):5-7.
- [3]许海清.区域教育城域网数据中心容灾机制的建设与应用[J].江苏教育,2022,(12):16-21.
- [4]李小林.基于CDP技术建设同城数据容灾中心——设计与实践[J].中国信息化,2021,(11):85-87+84.
- [5]廖峰.基于EVPN实现云数据中心异地容灾[J].电脑与电信,2021,(11):60-64.
- [6]许上鉴.建设灾备中心保障企业信息化[J].电脑知识与技术,2021,17(31):65-67.
- [7]阮春海.广梅数据容灾备份中心电气设计重难点分析[J].低碳世界,2021,11(08):114-115.