



IaaS 资源池容灾关键技术及实施建议研究

姚文胜¹, 李 军², 叶何亮¹, 万 宁¹

(1. 中国电信股份有限公司广东研究院 广州 510630; 2. 中国电信集团公司 北京 100033)

摘要

研究了 IaaS 容灾关键技术的实现原理及其适用场景, 探讨了如何利用这些技术实现云计算 IaaS 资源池的容灾方式以及实现 IaaS 资源池容灾应该遵循的基本原则。

关键词 容灾; IaaS 资源池; 关键技术; 本地备份恢复; 容灾策略

1 前言

美国国家标准与技术研究院(NIST)对 IaaS(infrastructure as a service, 基础设施即服务)的定义为: IaaS 是对所有设施的利用, 包括处理、存储、网络和其他基本的计算资源, 用户能够部署和运行任意软件, 包括操作系统和应用程序。消费者不管理或控制任何云计算基础设施, 但能控制操作系统的选择、存储空间、部署的应用, 也有可能获得有限制的网络组件的控制^[1]。IaaS 资源池就是利用虚拟化技术, 实现服务器、网络、存储等企业的基础设施资源的抽象, 使其成为一个个可以被灵活生成、调度、管理的基础资源单位, 物理资源的管理和调度都按逻辑方式进行, 从而形成了一个可统一管理、灵活分配调度、动态迁移的基础服务设施资源池。

随着云计算技术快速发展和日渐成熟, 各大 IT 企业的一个典型应用就是: 利用虚拟化技术建设 IaaS 资源池, 并将业务系统向资源池环境进行改造和迁移, 以达到资源统一调度管理, 弹性应用, 提高资源利用率, 降低总体拥有

成本(total cost of ownership, TCO)的目的。IaaS 资源池作为企业云计算体系架构中的资源提供层, 承担着整个云计算架构的资源提供、业务部署、数据存储、服务提供和安全管理的重要责任。容灾系统建设的主要目的就是预防不可避免的、非计划性的意外灾害的发生, 如果用户不能预防或降低灾难, 灾难一旦发生, 用户所面临的损失将远不止构建容灾系统的成本。之所以越来越多的行业用户在 IT 基础架构建设的同时, 会投入大量的精力与财力做容灾, 就是要将宝贵的数据和信息保护起来, 并加以有效管理、应用^[2]。因此, 企业在建设 IaaS 资源池的同时, 从自身情况出发, 建设基于 IaaS 资源池的容灾系统, 才能最大限度地保证部署在资源池上的各项业务的连续性, IaaS 资源池容灾系统的建设势在必行。

2 IaaS 资源池的容灾关键技术选择

由于技术的发展, 云计算环境下的容灾备份较传统环境下的容灾更易于实现, 主要是采用重复数据删除(data deduplication)、数据镜像(mirror)、数据快照(snapshot)和持

续数据保护(continuous data protection, CDP)技术。

2.1 重复数据删除技术

IaaS 资源池与存储密不可分,随着企业的数据量不断增长,大量的重复数据给存储带来严峻的挑战。举例来说,现在有一个大小为 10 MB 的 PPT 文件,要把它发送给 100 个用户,这就需要邮件服务器有 1 GB 的可用存储空间。当每周都要备份 1 GB 的重复存储时,一年后,浪费的 1 GB 空间最终会导致需要 52 GB 的磁带备份或其他方式的备份存储。

重复数据删除正是为解决数据冗余问题应运而生的,如图 1 所示。基本而言,重复数据删除就是减小存储空间的一种方式,它通过“散列算法”(如 MD5 或 SHA-1)对数据进行分块处理,为每一个数据块产生一个特定的散列值,并将它保存在索引中。当处理另一个数据块时,其散列值将与已经编入索引中的其他散列值进行比较,如果该值已经存在于索引中,新的数据块将会进行重复删除处理,不被保存,但会插入一个指向已存在数据的“标号”。也就是说,当数据向备份、档案文件或者复制平台转移时,只有最初的数据实例会被保存到磁盘上。随后的实例会用小标号来简单地注明并指向已经保存的重复部分,它通过删除冗余数据,确保只有第一个单一的数据实例保存在存储介质中,而删除的冗余数据由一个指向元数据的指针所代替。

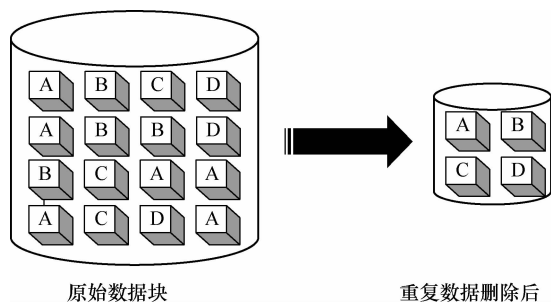


图 1 重复数据删除技术

重复数据删除带来了多种好处。目前最新的存储产品已经可以为用户提供 50:1 的压缩比,数据存储量的减少,极大地降低了存储成本。这意味着只需更少的磁盘和更低频率的磁盘采购。更少的数据同时也意味着备份更小。这些都将转化为较少的备份窗口占用时间和更快的恢复时间目标(recovery time objective, RTO)。更小的备份也延长了在虚拟磁带库(virtual tape library, VTL)或虚拟档案库的保存时间。

重复数据删除技术需要对数据产生一个可供重复删

除适用的全面索引,所以它适用于保存生命周期较长的数据,那些生命周期较短的数据(例如只需要保存一周的数据)对于重复删除来说是毫无意义的。

2.2 数据镜像技术

数据镜像技术适用于这种场合:数据一致性对于一个企业非常关键,并且对于恢复时间的目标要求为 0。

数据镜像在存储和 I/O 层面上有着多种实现方式,但其基本原理都在于系统在两个独立的存储单元上保存数据的两个副本,其中一个为主镜像,另一个为副镜像,如图 2 所示。对于主镜像中数据的变更,同步地反映在副镜像中,从而在主镜像发生故障而无法继续工作时,系统可以通过使用数据的副镜像继续运行而不会中断,直到修复发生故障的部件为止。

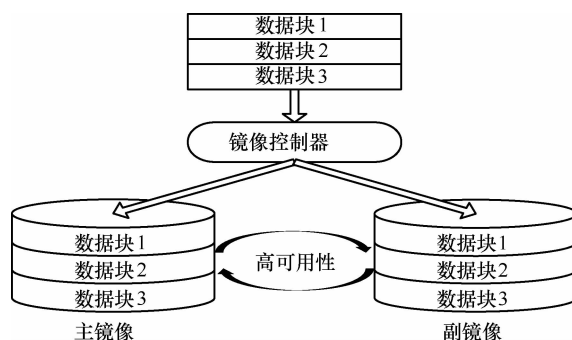


图 2 数据镜像技术

虚拟化管理软件中(如 VMware vCenter),虚拟机的高可用性(HA)功能和容错(FT)功能都是在数据镜像技术的基础上实现的。

2.3 数据快照技术

随着存储应用需求的提高,用户需要以在线方式进行实时的数据保护,快照就是在线存储设备防范数据丢失的有效方法之一。举个例子来说,一个企业的数据量很大,而且应用昼夜不停,做一次磁带备份需要 24 h。现要求备份某日 00:00 时间的数据,如果使用传统在线备份方式,备份下来的数据开始时是 00:00 的,最后的数据是 24:00 的,数据的前后一致性就无法保障了。利用数据快照技术,快照功能会自动寻找没有数据改变的時刻进行拷贝,只需几秒钟即可生成需要备份数据的索引,再对这些数据进行备份。当这个备份过程结束后,数据的一致性得到了保证。

数据快照是指对指定数据集合的一个完全可用拷贝,该拷贝包括相应数据在某个时间点(拷贝开始的时间点)的映像,可以是其所表示的数据的一个副本,也可以是数



据的一个复制品。快照技术的基本形式既包括完整卷复制,也称镜像、克隆或业务持续性卷;也包括部分复制,即只保存发生变化的数据或改变数据的指针。数据快照技术如图3所示。

快照技术最常见的用途是快速、简易恢复意外擦除或损坏的数据。除此之外,快照技术可以实现两项功能:整合资源、迁移数据。利用快照技术,能很容易地将数据迁移到新硬件中,替代现有硬件,重新安排数据的存储方法以及将多种设备整合为一种。

2.4 持续数据保护技术

持续数据保护是快照的逻辑扩展。在2.3节使用快照技术的例子中,如果在快照的开始时间00:00至备份完成时间点24:00之间发生故障,那么00:00到发生故障之间的数据就会丢失。而持续数据保护技术可以很好地解决这个问题。

持续数据保护是一套方法,它捕获或跟踪数据的变化,并将其独立存放在生产数据之外,以确保数据可以快速恢复到过去的任意时间点。持续数据保护系统可以基于

块、文件或应用实现,可以为恢复对象提供足够细的恢复粒度,实现几乎无限多的恢复时间点。持续数据保护技术可以连续不断地将本地变更的数据块或者字节增量复制到备份系统中,这从根本上改变了传统的对数据的全备份以及恢复过程。

持续数据保护技术通常用来避免时间以及频繁备份所遇到的一些问题。例如:持续数据保护技术可以保护终端用户或者远程系统通过相对的低速WAN连接。当一个终端用户遭受了数据损失或者文件损坏时,系统就会从数据中心的CDP中得到重建;CDP的部署通常也用来保护特定的应用,例如邮件和数据库服务器以及处理非常繁忙的网络事务的业务系统。持续数据保护技术如图4所示。

3 企业实施IaaS资源池备份和恢复方案的建议

3.1 传统的容灾解决方案不适用于IaaS资源池

在IaaS资源池中,计算、存储等资源统一进行管理和

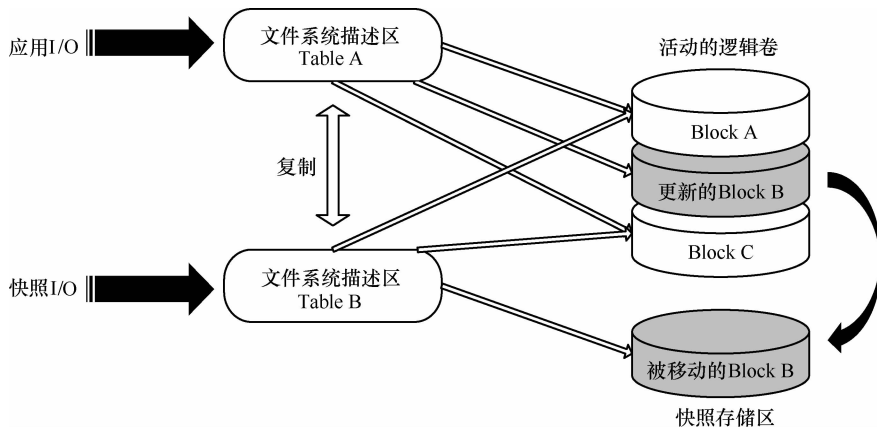


图3 数据快照技术

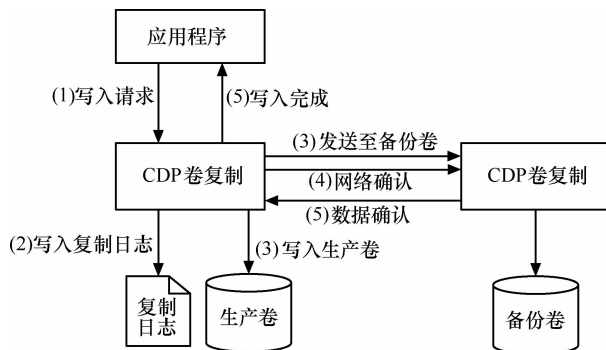


图4 持续数据保护技术

弹性调度,应用系统部署运行于虚拟机上,部署架构与旧有 IT 系统相比更为庞大和复杂,这就对容灾技术、产品的选择与方案的制定提出了新的要求。对于技术原理和实现方式而言,传统的容灾技术与云计算 IaaS 资源池的容灾技术基本上是一致的。但从解决方案的角度来看,传统的容灾产品和方案大多实现的是文件级或应用级的容灾,存在着对 IaaS 资源池中的大数据文件,特别是对部署了各种应用系统的虚拟机的备份力度不甚理想等问题;同时,因为传统容灾产品和方案与虚拟化技术的结合程度不高,也难以实现虚拟机的复制与动态迁移的基本要求。所以,传统的容灾产品和方案已经无法满足利用虚拟化技术,对部署于 IaaS 资源池虚拟机上的多系统统一进行备份和恢复的需求。

而利用虚拟化容灾产品和软件不仅简化了数据备份和恢复的过程,快速实现灾备目标,还降低了运维成本和灾备系统的总体拥有成本。前述的容灾关键技术已经成熟地应用在各主流厂商的软件和硬件产品当中,比如 VMware Consolidated Backup、VMware Site Recovery Manager、IBM Tivoli Storage Manager、EMC Avamar、Symantec NetBackup、FalconStor Software CDP 方案等。

3.2 IaaS 资源池容灾备份策略制定的基本原则

IaaS 资源池中实施灾难恢复与其他容灾的目的都是一样的,就是保证数据的零丢失和业务 7x24 h 的不中断。IaaS 资源池的容灾,实际上是对部署了业务系统的虚拟机以及存储在资源池中业务关键数据的容灾,制定合适的容灾备份策略,建立一个完备的 IaaS 资源池容灾体系应符合以下的基本原则。

(1)综合考虑各种因素,根据不同的灾备目标,灵活运用合适的灾备手段

IaaS 资源池的能力和带宽留有一定的冗余,确保部署于 IaaS 资源池上的业务系统的正常运作;明确 IaaS 资源池中各类数据的容灾等级划分,制定符合企业要求的 RTO 和 RPO 与备份恢复周期;根据容灾目标容量大小、更新频率、关键程度等特点选择合适的备份和恢复方式。

(2)制定详细的数据备份和灾难恢复计划,完善灾备流程的管理

明确企业业务连续性系统的建设目标,持续进行 IaaS 资源池数据集中与架构优化的工作;根据既定策略进行定期的演练和测试,确保灾备前后数据的完整性和一致性;

制定包括组织、人员以及执行步骤在内的详细的容灾管理流程。

4 企业构建 IaaS 资源池本地容灾系统的实施建议

虚拟化是 IaaS 资源池容灾的基础,利用不同的虚拟化软件建设虚拟化资源池,会在资源池的结构和数据类别的划分上有所不同。以 VMware 虚拟化软件建设虚拟化资源池为例,虽然资源池可以划分成不同级别的层次结构,每个资源池也可以包含子资源池,但若根据数据类别来划分,资源池中的数据主要可以划分成 3 类:虚拟机操作系统文件数据;用户数据;资源池及虚拟机配置文件数据。通过对上述 3 类数据的划分,能够实现虚拟服务器运行环境与物理部署环境的拆分、部署于虚拟服务器中应用系统与用户数据的拆分、用户配置文件和资源池环境的拆分,使得虚拟化资源池中的数据有更好的容灾目标性的划分。

资源池的使用过程中,对于不同的系统数据,可以采用不同的管理方法,从而降低复杂度和成本,提高管理效率。同时在数据备份恢复方面也可以有不同的思路和方法,主要包括以下几点。

- 基于备份介质的物理备份与恢复:通过备份软件将目标数据备份到其他离线的存储介质,如带库、VTL 等,当目标数据的使用或存储发生故障时,可从备份介质中恢复原有生产环境。基于备份介质的物理备份方式可以应对各种故障和误操作造成的数据丢失,但需要较长的恢复周期,而且数据的一致性得不到保证。
- 基于快照的逻辑备份与恢复:通过虚拟化软件的快照机制,可以实现数据的快速逻辑备份,当数据发生逻辑错误,比如虚拟机内数据的误删除等,能够从快照快速恢复。基于快照的备份方式可以提供虚拟机 OS 故障或丢失数据的快速恢复,但无法应对存储硬件故障等造成的数据丢失。
- 基于数据镜像技术的实时数据备份:通过备份软件将资源池的数据实时同步复制至另一台存储系统,在主系统存储设备出现故障时可切换至镜像存储系统迅速恢复业务。基于数据镜像的实时数据备份可以在零数据丢失的情况下迅速恢复故障系统数据访问,但无法恢复误操作或 OS 系统造成的数据变更。



表 1 虚拟化数据容灾方式的比较

数据容灾方式	技术特性	恢复速度	优缺点	实施成本
数据逻辑备份	备份软件定时备份至离线存储	慢	恢复慢,恢复后丢失备份时点至故障时点的数据更新	中
数据镜像备份	数据实时同步至镜像存储	快	恢复快,无法恢复误操作等造成的数据丢失	高
数据快照备份	虚拟化软件定时完成数据快照	较快	恢复快,无法恢复硬件故障的数据丢失,恢复后丢失备份时点至故障时点的数据更新	低
持续数据保护备份	快照技术的延伸和扩展	快	数据可恢复到可用时间的任何点,网络带宽需求很高,备份恢复的周期短	很高

- 基于持续数据保护技术的实时数据备份:提供了一个连续的、不断的系统存储的记录状态,可以使数据状态恢复到数据遭到破坏之前的任意一个时间点,从而有效规避了由人为的逻辑错误或病毒攻击所造成的数据丢失。但由于持续数据保护的存储库存储了所保护数据的同步副本,如果数据经常发生变化,日志就会快速增长,所以应设置较短的备份恢复周期。

虚拟化数据容灾方式的比较见表 1。

如表 1 所示,前 3 种备份方式各具特点,对于在本地构建容灾系统的需求来说,总体而言,建议采用快照与数据逻辑备份相结合的方式进行资源池数据的本地备份与恢复。

对于核心关键数据,例如部署于虚拟机上的关键应用以及应用所产生的关键数据等,可以考虑选用数据镜像的备份方式,建立专门的管理系统对其进行保存和管理,并对关键数据进行必要的冗余存储(数据镜像采用基于存储层面的方式实现),以尽量避免和降低系统出现故障时的数据丢失。

对于非核心数据,例如部署于虚拟机上的非核心应用系统、用户自定义数据等,在节省资产投入的基础上,采用快照与数据逻辑备份相结合的方式进行将虚拟服务器系统和应用的打包备份,而且在出现问题时可以用统一的数据备份进行恢复。

持续数据保护技术相较前 3 种备份恢复技术更为全面和高效。单从恢复时间目标的角度看,目前几乎没有比提供虚拟化恢复的 CDP 产品速度更快的产品了。相比其他的容灾技术,持续数据保护技术不但拥有较大的技术优势,而且仍在不断地发展和改进。同时也为实现 IaaS 资源池远程异地容灾提供了一个重要的选择。

5 结束语

IaaS 资源池容灾是云计算体系架构中的一种重要的灾难备份形式,本文介绍了 IaaS 资源池容灾的 4 个关键技术:重复数据删除、数据镜像、数据快照与持续数据保护技术,并浅析了这 4 种技术的应用场景与相互之间的比较,探讨了企业构建 IaaS 资源容灾系统的基本原则。

灾难备份的实施要求企业综合考虑其基础设施、数据存储及工作流程管理等多种因素,从本身的实际情况出发,合理利用各种灾备技术与产品,才能建设有效的、完善的灾备系统,从而达到最大限度保证企业业务连续性的目的。同时,随着云计算容灾关键技术的不断发展与成熟,以及各行业云计算数据中心、灾备中心建设的深入开展,构建在 IaaS 资源池基础上的云灾备系统必将成为灾难备份市场的主流方式。

参考文献

- 1 美国国家标准与技术研究院.<http://www.nist.gov/index.html>
 - 2 郝鹏. 居安思危认清容灾的重要性. 中国计算机用户, 2004(27)
 - 3 Halpert B. Auditing Cloud Computing: A Security and Privacy Guide. Wiley Corporate F&A, 2011
 - 4 Greg Schulz. Cloud and Virtual Data Storage Networking. CRC Press, 2011
 - 5 EC-Council. Disaster Recovery. Publisher: Course Technology, 2010
 - 6 Preston W Curtis. Backup & Recovery: Inexpensive Backup Solutions for Open Systems. O'Reilly Media, 2007
 - 7 肖达,刘建毅. 云灾备关键技术. 中兴通讯技术,2010(10)
 - 8 TT 存储技术专题. <http://www.techtarget.com.cn>
- 【作者简介】 姚文胜,硕士,毕业于中国科学院研究生院,高级工程师,具有 10 多年电信支撑系统研发经验,主要从事企业信

息化规划及相关技术研究;李军,硕士,毕业于北京理工大学,具有10多年电信IT支撑系统建设及管理经验,负责过多个电信BSS建设大型工程,目前负责IT服务管理及IT基础设施规划管

理等工作;叶何亮,本科,毕业于北京邮电大学,具有多年电信工作经验,长期从事规划研究;万宁,硕士,毕业于复旦大学,长期从事系统研发工作。

Research on Key Technology and Implementation of IaaS Resource Pool Disaster Recovery

Yao Wensheng¹, Li Jun², Ye Heliang¹, Wan Ning¹

(1.Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China;

2. China Telecom Corporation, Beijing 100033, China)

Abstract This paper describes the principle and application of key technologies of IaaS disaster recovery scene, explores how to build the disaster recovery system of the IaaS resource pool with these key technologies, and explores the basic principles should followed to realizing IaaS resource pool disaster recovery system.

Key words disaster recovery, IaaS resource pool, key technology, local backup and recovery, disaster recovery policy

(收稿日期:2012-06-21)

• 简讯 •

Check Point 利用虚拟化 功能简化私有云安全

Check Point 软件技术有限公司日前宣布推出 Check Point 虚拟系统,这样企业就能将安全网关整合到单个设备或开放服务器中,从而简化私有云环境的安全保护流程,降低成本并提高性能。通过 Check Point 虚拟系统,客户可选择利用 Check Point 软件刀片的任意组合保护多个网络段的安全,如防火墙、VPN、入侵防御(IPS)、应用控制、URL 过滤、反僵尸网络、防病毒及身份识别等,为客户提供最广泛的虚拟化安全保护。

通过 Check Point 虚拟系统,客户可在任意网关或开放服务器上构建安全的私有云服务,最多可将 250 个虚拟系统整合到一个网关上,因为每个虚拟系统都带有定制的软件刀片保护机制以及为满足特定业务需求量身定制的专用策略,可以降低复杂性。针对管理多个工作组或业务部门的企业或通过单个系统为多个客户提供服务的管理

服务提供商(MSP),Check Point 帮助客户通过虚拟化实现安全功能整合,同时让其 IT 部门通过专用虚拟系统保持 Web 安全、威胁防御、防火墙及远程接入等领域的职能独立。客户还可以使用 Check Point 获得专利的“虚拟系统负载分担(VSLS)”技术构建多达 8 个网关的集群,从而实现前所未有的最高扩展性能。随着客户业务需求的增长,Check Point 可帮助企业通过虚拟化安全的强大功能来降低成本和提高运营效率。

借助 Check Point 虚拟系统,客户将大大提高性能,并在 Check Point 新推出的 64 bit GAIa 操作系统上实现虚拟化安全,从而使同时连接的数量达到以往版本(VSX)的 8 倍以上。此外,该解决方案还采用 CoreXL 多核技术处理器,使客户能够实现更高的性能。

Check Point 虚拟系统帮助客户将多个网关整合到单个设备中,并通过基于 GAIa OS 及 VSLS 专利技术增强了安全性能与可扩展性。企业第一次能够通过虚拟系统真正实现虚拟化安全的强大功能,部署其所需的全部保护机制。