



新一代电信 IT 系统容灾技术方案研究与策略分析

龚德志, 石屹嵘

(中国电信股份有限公司上海研究院 上海 200122)

摘要:对最新容灾相关技术的发展进行了分析,对关键业务和系统的等级划分原则进行了阐述,并以中国某电信公司为例,进行具体分析和设计,同时按照不同的保护等级要求,进行了新一代容灾方案的技术架构分析。

关键词:新一代;容灾;方案

doi: 10.3969/j.issn.1000-0801.2013.06.025

Research and Strategic Analysis of New Generation Telecom IT System Disaster Recovery System

Gong Dezhi, Shi Yirong

(Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: The latest disaster recovery technology was stated and classification principles into critical business systems was elaborated. Also, the architecture of a new generation of disaster recovery technology program was analyzed by taking one branch of China Telecom as an example.

Key words: new generation, disaster recovery, plan

1 引言

经过几年的企业信息化建设和不断完善,中国电信各分公司的 MBOSS 所涵盖的各个系统已经在市场拓展、客户服务等工作中发挥了重要的支撑作用。日益激烈的市场竞争和不断提高的客户服务质量需求对 MBOSS 业务支撑能力和可靠稳定运行的要求越来越高,从面向客户服务的角度而言,无论何时出现何种情况,都需要提供不间断的业务支撑服务,以保证客户满意度、客户服务质量和企业信誉等不受影响,并避免财务损失,增强企业竞争力。

集中化在带来实现业务快速响应和管理高效等众多优势的同时,也存在着系统故障点集中、风险集中的危险,如系统故障、人为误操作、火灾、水灾、传输中断、电网停电等系统风险。因此,适时、合理地规划和开展支撑系统容灾建设,已经成为电信公司的重要任务。

容灾相关技术也在不断地发展,如 CDP(连续数据保护)技术,基于虚拟存储网络的远程复制技术的引入,给容灾技术方案的设计带来新的考虑。同时基于 X86 的虚拟化技术、小型机虚拟化技术的引入,也给容灾站点建设带来新的思路。本文将就如何采用上述新的容灾相关技术进行新一代电信 IT 系统容灾技术方案设计和建设进行讨论。

2 技术发展

容灾实现技术自下而上,按实现层次划分,可以分为 5 种,分别是:

- 基于存储的远程数据复制容灾技术;
- 基于虚拟存储网络的远程数据复制的容灾技术;
- 基于连续数据保护的容灾技术;
- 基于服务器虚拟化的容灾技术;
- 基于主机卷管理的远程数据复制的容灾技术;



- 基于数据库复制的远程容灾技术;
- 基于应用程序远程容灾技术。

最近几年虚拟化相关技术发展迅速,特别是基于连续数据保护的容灾技术、X86 平台虚拟化技术、存储虚拟化技术和服务器虚拟化容灾技术(SRM)。上述技术的应用为实现不同等级的容灾保护要求提供了另外一种解决方案,同时也能降低容灾站点的建设成本。表 1 对其中几种新的技术特点和实现方式进行简要阐述。

2.1 资源虚拟化和复用技术

(1) 服务器虚拟化技术

服务器虚拟化也称系统虚拟化,它把一台物理计算机虚拟化成一台或多台虚拟计算机,各虚拟机间通过被称为虚拟机监控器(virtual machine monitor, VMM)的虚拟化层共享 CPU、网络、内存、硬盘等物理资源,每台虚拟机都有独立的运行环境。虚拟机可以看成是对物理机的一种高效隔离复制,要求同质、高效和资源受控。同质说明虚拟机的运行环境与物理机的环境本质上是相同的;高效指虚拟机中运行的软件需要有接近在物理机上运行的性能;资源受

控指 VMM 对系统资源具有完全的控制能力和管理权限。一般来说,虚拟环境由 3 个部分组成:硬件、VMM 和虚拟机。VMM 取代了操作系统的位置,管理着真实的硬件。

(2) 存储虚拟化技术

存储虚拟化是对存储硬件资源进行抽象化表现,通过将一个(或多个)目标服务或功能与其他附加的功能集成,统一提供有用的全面功能服务。存储虚拟化是一种贯穿于整个 IT 环境、用于简化本来可能会相对复杂的底层基础架构的技术。实现思想是将资源的逻辑映像与物理存储分开,从而为系统和管理员提供一幅简化、无缝的资源虚拟视图。对于用户来说,虚拟化的存储资源就像是一个巨大的“存储池”,用户不会看到具体的磁盘、磁带,也不必关心自己的数据经过哪一条路径通往哪一个具体的存储设备。从管理的角度看,虚拟存储池采取集中化的管理,并根据具体的需求把存储资源动态地分配给各个应用。

存储虚拟化技术包括基于主机层存储虚拟化技术、基于网络层存储虚拟化技术和基于阵列控制器的存储虚拟化技术。

表 1 主流容灾技术对比

	基于存储的远程数据复制容灾技术	基于虚拟存储网络的远程数据复制的容灾技术	基于连续数据保护的容灾技术	基于服务器虚拟化的容灾技术	基于主机卷管理的远程数据复制的容灾技术	基于数据库复制的远程容灾技术	基于应用程序远程容灾技术
投资内容	容灾中心:新增同型号存储 两地:存储互联	容灾中心:新增异构存储 两地:新增虚拟存储设备	容灾中心:新增异构存储 两地:新增连续数据保护容灾设备	容灾中心:新增异构存储,新增主机 两地:安装服务器虚拟化软件	容灾中心:新增异构存储,新增主机 两地:主机安装软件	容灾中心:新增异构存储,新增主机 两地:数据库同步软件	容灾中心:新增异构存储,新增主机 两地:应用改造
主机依赖性	不一定需要主机	不一定需要主机	不一定需要主机	一定需要主机	一定需要主机	一定需要主机	一定需要主机
是否影响生产系统	不影响,旁路连接	影响,切入生产系统	不影响,旁路连接	不影响(如主站点已实现虚拟化)	不影响,旁路连接	不影响,旁路连接	不影响,旁路连接
适应范围和约束条件	数据级容灾 应用级容灾 业务级容灾	数据级容灾 应用级容灾 业务级容灾	数据级容灾 应用级容灾 业务级容灾	应用级容灾 业务级容灾	应用级容灾 业务级容灾	应用级容灾 业务级容灾	应用级容灾 业务级容灾
实施难度	低	中	中	中	中	中	高
技术成熟度	成熟	成熟	成熟	较成熟	成熟	成熟	成熟
对系统性能的影响	同步影响大 异步无影响	同步影响大 异步无影响	同步影响大 异步无影响	同步无影响 异步无影响	同步影响大 异步影响主机性能	同步影响大 异步影响主机性能	同步影响大 异步影响主机性能
灾难情况下的数据丢失量	同步:没有丢失 异步:1 min 以内	同步:没有丢失 异步:1 min 以内	同步:没有丢失 异步:1min 以内	同步:没有丢失	同步:没有丢失 异步:1 min 以内	同步:没有丢失 异步:1 min 以内	同步:没有丢失 异步:1 min 以内
存储是否需要同构	需要	不需要	不需要	不需要	不需要	不需要	不需要
数据库是否需要相同	不需要	不需要	不需要	不需要	不需要	需要	不需要

2.2 数据复制和备份技术

(1)基于虚拟存储网络的远程复制技术

基于虚拟存储网络的远程复制技术,是在存储虚拟化技术的基础上实现的一种远程复制技术。采用虚拟存储技术进行数据复制同样也可以有同步复制方案和异步复制方案,需要根据具体的需求选择合适的实现方式。采用虚拟存储化技术建设容灾方案生产中心和容灾中心的存储阵列可以是不同厂商的产品,存储平台选择不受现有存储平台厂商的限制,对不同厂商的存储阵列提供统一的管理界面。存储虚拟化技术可以在不同层面实现,如在智能交换机层面、存储层面或增加第三方设备来实现。

目前各存储厂商分别有不同的存储虚拟化技术,利用各厂商的存储虚拟化技术能够实现异构存储平台之间的数据复制(同步或异步方式)。应用该技术时,主生产中心和容灾中心的存储阵列可以是不同厂商的产品,存储平台选择不受现有存储平台厂商的厂商限制,并为不同厂商的存储阵列提供统一的管理界面。

(2)基于连续数据保护的容灾技术

基于连续数据保护的容灾技术,也是基于虚拟化存储技术,是在前端应用服务器与后端存储系统之间的存储区域网络(SAN)旁边加入一层数据复制器,这个数据复制器会含有一定的数据空间,它的角色就是持续不断地获取生产数据,不仅可以实现本地的数据冗余而且可以实现异地数据的复制,其优点是灾备功能强大。由于数据复制是通过数据复制器执行,它对主机的性能影响非常低,而且,通过持续不断地数据获取,不仅能对现有数据做完整的无损备份,而且还具备了对于历史数据的任何时间点的历史轨迹备份(在现有数据丢失或被破坏时发挥作用,如同照片等记录历史一刻的功能,这是唯一的一种具备历史数据恢复的灾备技术。

(3)基于服务器虚拟化的容灾恢复技术

服务器虚拟化技术可以提供一些传统的灾难恢复方

式所不具备的解决方案,可以降低容灾的部署成本,提供更大的灵活性,并且确保目标恢复时间(RTO)的达成。利用虚拟化灾难恢复技术,可以方便管理从生产数据中心到灾难恢复站点的故障切换;同时,还可以管理两个互为恢复站点且具有活动工作负载的站点之间的故障切换。服务器虚拟化技术还可以自动执行及简化故障切换至新数据中心的过程,从而让所计划的数据中心故障切换(如数据中心迁移)变得更加顺畅。

3 关键业务和系统

按照业务服务对象,将关键业务分为 3 类业务,下面分别研究这 3 类业务中对公司的关键业务的中断是否会对企业的收入、客户满意度、社会影响度产生直接或间接的影响。

(1)直接对外提供服务

指如果此项业务无法开展,将无法为客户提供服务,对客户感知造成直接影响,造成服务质量、客户满意度、客户忠诚度的下降,如充值等业务。

(2)通过人员对外提供服务

指如果此项业务无法开展,业务受理人员将无法为客户提供业务办理等服务,如业务受理等业务。

(3)提供企业内部管理服务

指如果此项业务无法开展,电信企业内部管理平台将无法为员工提供内部管理业务,如综合办公等业务。

以某电信公司 A 为例,将关键业务和系统分类,见表 2。

4 保护等级

业务保护等级的制定需要参考主要风险、关键业务需求、国家和行业标准来制定。通过对某电信公司 A 关键业务的业务需求分析,同时参照 GB/T 20988,对容灾保护等级和容灾保护要求进行定义,如表 3 所示。

表 2 关键业务和系统

关键业务	业务类型	业务功能	相关 IT 系统
A 类业务	直接对外提供服务的业务	A1: 通话类业务	OCS; 融合计费账务系统
		A2: 停复机业务	自动激活系统; 服务开通系统; 网上营业厅; EAI; 统一认证(内部)
		A3: 充值类业务	统一充值平台; 统一认证(外部); CRM 系统
B 类业务	通过人员对外提供服务的业务	业务受理; 客户服务; 计费、开账类业务	综合资源管理系统; 智能交换平台; 营销实物系统
C 类业务	提供企业内部管理服务	内部办公; 预算、决算; 采购需求、采购方案; 供应商管理; 生产经营报表	ERP; 综合办公服务系统; ODS



表 3 保护等级说明

保护等级定义	容灾保护要求定义	参考 GB/T 20988
1 级	双活中心, $RTO=0$; 零数据丢失, $RPO=0$	6 级: 数据零丢失和远程集群支持(双活)
2 级	2 h 内完成切换, $RTO \leq 2$ h; 零数据丢失, $RPO=0$	6 级: 数据零丢失和远程集群支持
3 级	4 h 内完成切换, $RTO \leq 4$ h; 秒级丢失量, $RPO \leq 1$ min	5 级: 实时数据传输及完整设备支持
4 级	切换时间未定义 2 h; 数据丢失, $RPO \leq 2$ h	3 级: 电子传输和部分设备支持

5 容灾策略

容灾策略设计应该考虑在确保数据安全的基础上提高业务连续运行能力,降低企业运营风险,将业务损失降低到可接受的程度,提升服务质量和水平,增强企业竞争力。在容灾策略设计过程中,应该考虑以下 3 个原则。

- 成熟方案原则: 尽量利用现有的技术架构功能满足业务需求,或者是购买成套成熟软件产品。
- 方便使用原则: 容灾备份系统对使用和维护有非常高的要求。不恰当容灾技术的选择,会给各使用人员的培训、监督、管理、演练、维护等工作造成非常大的工作压力,甚至导致因人为失误造成的不必要损失,所以容灾备份系统必须便于使用、维护和演练。
- 平战结合原则: 在不影响灾难备份与恢复的前提下,本着平战结合的原则,充分利用灾备中心的各类资源,开展培训、灾备演练、测试和完善、信息系统应用开发、数据应用等业务。

以某电信公司 A 为例,制定以下容灾策略,如表 4 所示。

6 技术方案

6.1 方案一

在为 A 类关键业务实现 2 级容灾保护要求时候,采用连续数据保护的容灾技术实现(如图 1 所示),技术方案如下。

(1)主机层

在生产中心的业务系统中,主机下接生产存储和通过 CDP 本地设备挂接的生产中心备份存储,并在主机上安装卷管理软件,实现卷镜像,创建一个逻辑卷(volume)供业务主机使用。该卷实际上是由两个完全对等的、容量相同的磁盘片构成,两个磁盘片上的数据完全一样,业务主机对该逻辑卷的任意修改,都将同时被写到位于生产中心的

生产磁盘系统和本地备份磁盘系统上。

(2)网络层

在 SAN 设计中,需要采用冗余的网络设计,生产中心和容灾中心各需要配置高端光纤通道交换机进行互连,为主机和存储系统提供冗余的连接路径。IP 网络在本阶段作为 SAN 的冗余方案考虑,本地和异地的 CDP 设备在 SAN 中断情况下,可以基于 IP 网络进行数据异步复制,并可以实现数据的压缩传输。

(3)存储层

在生产中心可以设置一套同等性能存储,或者对原有存储进行扩容。实现所有数据在生产中心的备份。主机在进行数据写入时,同时写入生产存储和挂接在存储虚拟化设备之后的备份存储。生产中心存储虚拟化设备的配置数量需要进行 IOPS 评估。

在备份中心设置一套低端存储,通过存储虚拟化设备将生产中心的备份数据复制到容灾中心。容灾中心存储虚拟化设备按照生产中心配置数量的一半进行配置。

6.2 方案二

在为 B 类关键业务实现 3 级容灾保护要求时,采用虚拟存储网络的远程复制技术实现(如图 2 所示),技术方案如下。

(1)主机层

在生产中心的业务系统中,在主机上对卷进行卸载,将卷通过虚拟存储设备进行映射,再分配给主机,主机重新进行挂载。

(2)网络层

在 SAN 设计中,需要采用冗余的网络设计,生产中心和容灾中心各需要配置高端光纤通道交换机进行互连,为主机和存储系统提供冗余的连接路径。IP 网络在本阶段作为 SAN 的冗余方案考虑,本地和异地的 CDP 设备在 SAN

表 4 3 类业务的容灾策略

业务级别	保护要求建议	切换方式	容灾规模	容灾层次	数据复制方式
A 类业务	2 级	人工切换,不采用远程集群	存储同级、数据库主机同级、其他主机降级	应用级,主备	同步复制
B 类业务	3 级	人工切换,不采用远程集群	存储同级、主机降级	应用级,主备	异步复制
C 类业务	4 级		存储降级,无主机	数据级,主备	异步复制

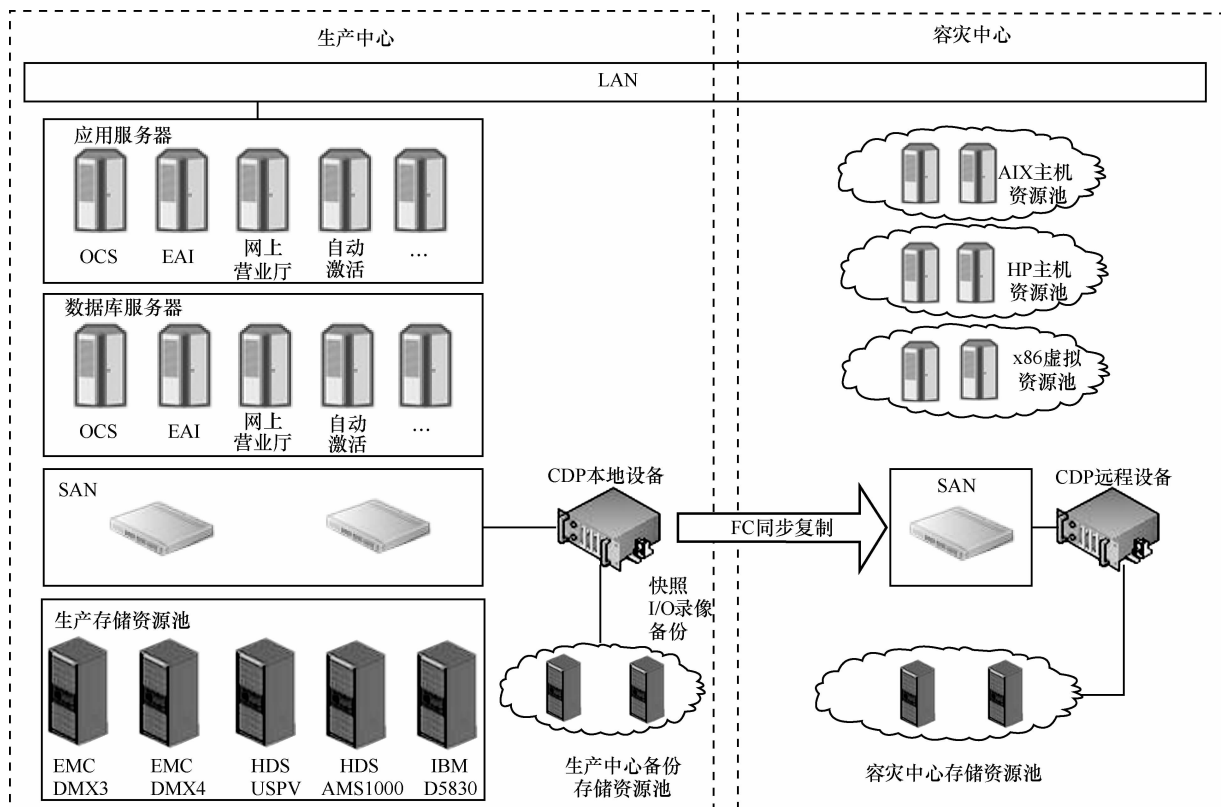


图1 连续数据保护容灾技术方案

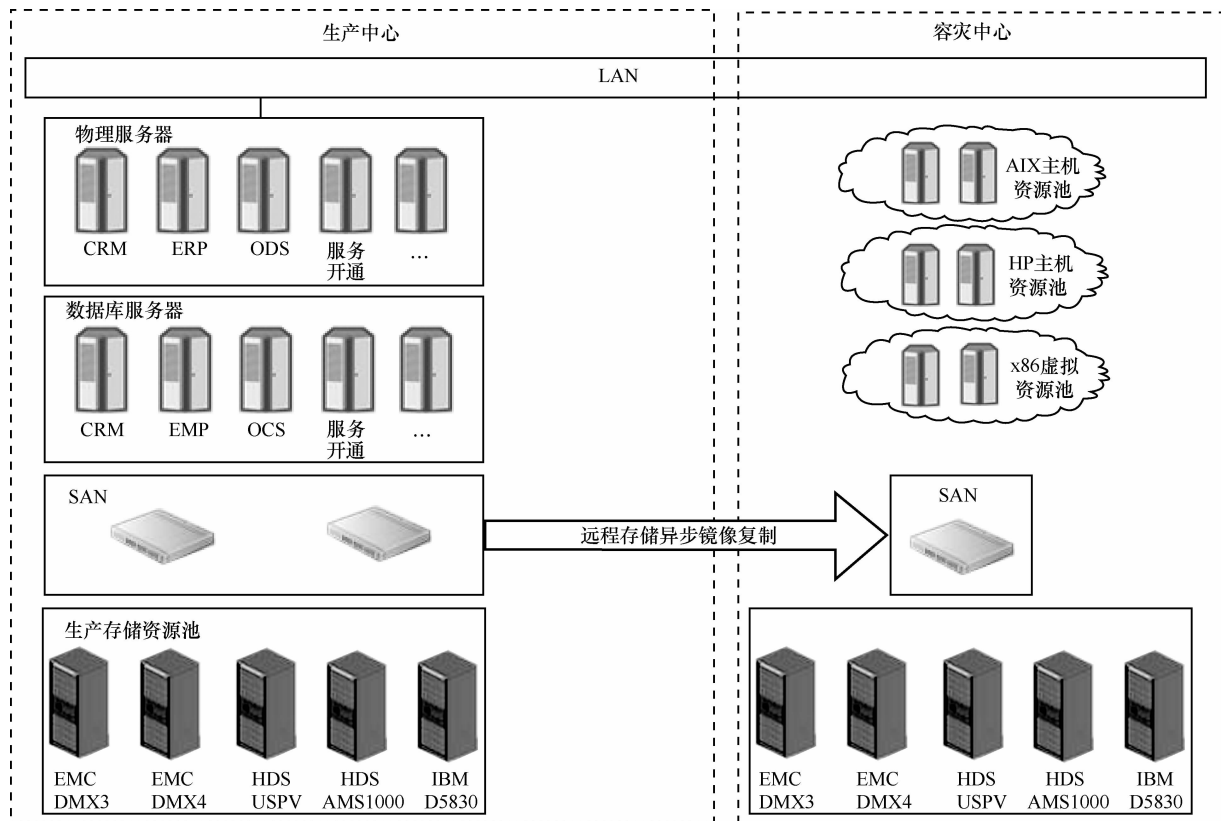


图2 虚拟存储网络的远程复制技术方案



中断情况下,可以基于 IP 网络进行数据异步复制,并可以实现数据的压缩传输。

(3)存储层

在备份中心设置一套低端存储,通过存储虚拟化设备将生产中心的备份数据复制到容灾中心。容灾中心存储虚拟化设备按照生产中心配置数量的一半进行配置。

6.3 方案三

在为 C 类关键业务实现 4 级容灾保护要求时候,采用虚拟带库技术实现,技术方案如下。

(1)主机层

采用虚拟化技术,为部分系统配备数据库主机。

(2)存储层

存储设备降级,采用虚拟带库技术,将存储设备虚拟成带库进行远程数据备份。

7 技术验证

在研究过程中,重点针对基于虚拟存储网络的远程复制技术以及其衍生的基于连续数据保护的容灾技术进行实验室验证,验证对象见表 5。

表 5 验证对象

编号	厂商	产品
1	富士通	DX8000V
2	惠普	P9500
3	HDS	VSP
4	飞康	NSS
5	EMC	VPLEX
6	IBM	SVC

验证内容包括设备管理能力、存储整合能力、数据备份与恢复、设备自身及使用安全性、灵活性、扩展性、兼容性等性能。其中,性能包括读写加速性能、数据远程传输性能、数据压缩性能、切换效率等。

验证结果表明:基于虚拟存储网络的远程复制技术以及其衍生的基于连续数据保护的容灾技术能实现异构存储环境的容灾,能实现生产系统出现逻辑故障后在本地快速恢复,并在主站点出现故障或链路出现故障后能将应用快速切换到容灾站点。

8 实现步骤

容灾环境的建设需要逐步完成,不可能一步就实现整个环境的建设,以某电信公司 A 为例,可以按照二期实现。

(1)第一期

1~3 年内,实现 A 类业务应用级容灾,B 类、C 类业务

数据级容灾,目标如下:

- A 类业务实现 2 级保护要求(实施过程中,可以按照 A1、A2 和 A3 逐步实施);
- B 类业务实现 3 级保护中 RPO 要求;
- C 类业务实现 4 级保护要求。

(2)第二期

4~5 年内,在第一期基础上,实现 B 类应用容灾。目标如下:

- B 类业务实现 3 级保护要求的目标。

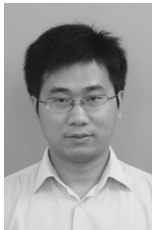
9 结束语

资源虚拟化和复用技术以及虚拟存储网络技术的引入,为新一代电信 IT 系统容灾技术方案的设计提供了新的技术支撑点。新技术的引入提高了容灾方案的技术先进性,提高了容灾和备份的便捷性和可管理性,同时降低了容灾站点的建设成本。

参考文献

- 1 闻剑峰,龚德志.虚拟化技术在电信灾难恢复计划中的应用研究.电信科学,2009,25(9)
- 2 徐娟.企业信息中心容灾建设.科技管理研究,2010,30(7)
- 3 龚德志,闻剑峰.虚拟化技术在电信服务器资源整合中的应用研究.电信科学,2009,25(9)
- 4 马锡坤,于京杰,杨国斌.存储虚拟化技术在医院信息系统平台中的作用.中国医疗设备,2011,26(10)
- 5 谭生龙.存储虚拟化技术的研究.微计算机应用,2010,31(1)

[作者简介]



龚德志,男,学士,中国电信股份有限公司上海研究院工程师,中国电信企业信息化验证实验室主管,主要研究方向为云计算、大数据、信息系统评测和容灾。



石屹嵘,男,硕士,中国电信股份有限公司上海研究院高级工程师,信息技术部主任工程师,主要研究方向为系统架构、云计算、系统审计和信息安全等。

(收稿日期:2013-03-05)