

## 城市轨道交通云平台容灾方案研究\*

陈瑞军<sup>1</sup> 孟伟君<sup>1</sup> 胡晓伟<sup>1</sup> 刘楠<sup>1</sup> 牛昌平<sup>2</sup>

(1. 呼和浩特市城市轨道交通建设管理有限责任公司, 010010, 呼和浩特;

2. 交控科技股份有限公司, 100070, 北京//第一作者, 高级工程师)

**摘要** 介绍衡量容灾系统的评价指标和容灾能力的等级划分, 提出在城市轨道交通行业中数据类型分析和业务重要程度分析方法论, 用于指导当前城轨业务容灾保护方案选择。基于呼和浩特市城市轨道交通云平台项目实践经验, 介绍业务现有容灾实现, 并通过研究备份及容灾限制条件, 提出未来业务系统基于城轨云平台进行数据保护的实现方案。

**关键词** 城市轨道交通; 云平台; 容灾评估; 容灾恢复

**中图分类号** U29-39

**DOI**: 10.16037/j.1007-869x.2020.09.042

## Research on Disaster Recovery Solution of Urban Rail Cloud Platform

CHEN Ruijun, MENG Weijun, HU Xiaowei, LIU Nan, NIU Changping

**Abstract** Firstly, the evaluation index and the classification of disaster recovery capability are introduced, a method for data type and business importance analysis in urban rail industry is proposed, which is used to guide the selection of disaster recovery solutions for current rail transit business. Then, based on the practical experiences of urban rail transit cloud platform in Hohhot City, the application of disaster recovery solution is introduced, through studying the current backup and disaster recovery restrictive conditions, a future business system implementation scheme based on data protection solution of urban rail transit cloud platform is proposed.

**Key words** urban rail transit; cloud platform; disaster assessment; disaster recovery

**First-author's address** Hohhot Urban Rail Transit Construction Management Co., Ltd., 010010, Hohhot, China

随着 IT 技术的发展, IT 系统已成为组织开展各项运营生产、企业管理的核心平台。对于城市轨道交通(以下简称城轨)行业而言, IT 系统的稳定、可靠运行关乎大众出行安全与企业信誉, 不但要运

行稳健, 同时要求因灾难导致系统不可用时, 具备更快的恢复能力和更少的数据丢失。在传统 IT 架构下, 业务容灾存在着投资大、技术门槛高、维护复杂等诸多问题。随着云平台在城轨行业的应用, 以云平台为基础, 可简化容灾方案, 充分发挥“云”的便利性, 增强企业 IT 能力, 提升企业信息化水平。

## 1 容灾概念介绍

容灾系统是指在相隔较远的地点, 建立两套或多套功能相同的系统, 互相之间可以进行状态监视和功能切换。当一处系统因意外(如火灾、地震)停止工作时, 整个应用系统可以切换到另一处, 使得该系统功能可以继续提供服务<sup>[1]</sup>。容灾系统的建设成本会随其容灾能力的提升而增加。因此, 容灾方案的实现需要综合考虑业务系统重要程度、容灾等级要求、建设成本等多种因素。

### 1.1 容灾指标

衡量容灾系统的主要指标有 RPO(灾难发生时允许丢失的数据量)、RTO(系统恢复的时间)<sup>[2]</sup>。

衡量容灾系统指标需要从其技术实现、影响程度、建设成本等多方面考虑, 当业务要求 RPO、RTO 越低时, 其实现技术难度及实现成本越高。通过对影响因素分析, 建立容灾评估模型如图 1 所示。

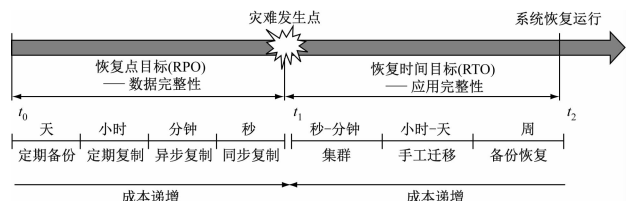


图 1 容灾评估模型

实际建设中受系统规模、实现技术及成本等方面的约束, 用户在选择容灾方案时应该综合考虑业

\* 呼和浩特市重大科技专项项目(2018-社-重-1)

务的重要性、实现技术及成本投入等多种因素,理性地做出选择。

### 1.2 容灾等级

《信息系统灾难恢复规范》(GB/T 20988—2007)通过对多方面综合分析,将容灾能力等级划分为6级<sup>[3]</sup>。不同的容灾能力等级对业务系统的保护效果可以通过RTO、RPO衡量,两者的对应关系如表1所示。

表1 容灾等级对应表

| 容灾等级 | 简介            | RPO      | RTO     |
|------|---------------|----------|---------|
| 第1级  | 备份基本支持        | 1~7 d    | 2 d以上   |
| 第2级  | 备用场地支持        | 1~7 d    | 24 h以上  |
| 第3级  | 电子传输和部分设备支持   | 数小时至1 d  | 12 h以上  |
| 第4级  | 电子传输级完整设备支持   | 数小时至1 d  | 数小时至2 d |
| 第5级  | 实时数据传输及完整设备支持 | 0~30 min | 数分钟至2 d |
| 第6级  | 数据零丢失和远程集群支持  | 0        | 数分钟     |

### 1.3 容灾与备份

容灾与备份是两种不同的实现,容灾的目的是保证数据和业务的“连续性”,备份是防止系统出现操作失误或系统故障导致数据丢失,而将全系统或部分数据集合从应用主机的硬盘或阵列复制到其他的存储介质的过程<sup>[4]</sup>。容灾系统通常基于存储层实现,会将数据完整的复制到容灾中心,包括错误数据,此时可以通过备份系统得以恢复被误删除的数据。简言之,备份是基础,是保护数据的最后手段,也是防止主动型信息攻击的最后一道防线<sup>[4]</sup>,而容灾可在备份基础上提供更高级别的保护能力,两者不可相互替代。

## 2 容灾需求分析

### 2.1 数据类型分析

对于信息系统而言,最重要的IT信息资产就是数据。按数据用途可以将数据分为程序文件、配置文件、业务数据、临时数据。对于这些文件的推荐保护机制如下:程序文件,一般通过软件介质或版本发布进行管理;配置文件,可作为系统档案进行保存;业务数据,主要指业务系统的所有带有业务属性的数据,其随着业务变化而发生变化,要求其

完整、准确应用数据为重点保护对象;临时数据,通常不做额外保护。

### 2.2 业务重要程度分析

根据业务系统处理的类型和服务对象,可分为核心业务、重要业务、一般业务。

核心业务:主要指涉及地铁运营生产的核心业务场景处理系统,集中处理业务数据,其状态将直接影响地铁运转,并可能造成人员安全事故或企业信誉受损,如信号系统。

重要业务:主要指地铁运营生产配套业务系统,或企业日常运营系统。发生业务中断,会造成部分服务受影响或中断,但不涉及经济损失或人员安全,如监控告警系统、企业邮箱等。

一般业务:主要指业务中断后对地铁运营或企业日常运营无重大影响,中断发生后能够接受在数天或数周内恢复,如考勤系统、人事档案系统等。

### 2.3 容灾保护矩阵

对数据类型和业务重要程度分析,可对地铁业务及数据进行分级处理,按照重要程度不同匹配不同的保护方案。对于第4级及以下容灾保护需求的业务,建议通过备份方案实现;对于重要业务、核心业务需要第5级保护的,建议采用容灾方案实现;对于核心业务系统中要求第6级保护的,建议采用由业务系统配置应用双活方案来实现。容灾保护实现如图2所示。

|        |     |      |      |      |
|--------|-----|------|------|------|
| 容灾能力等级 | 第6级 | —    | —    | 应用双活 |
|        | 第5级 | —    | 异地容灾 | 异地容灾 |
|        | 第4级 | 备份还原 | 备份还原 | 备份还原 |
|        | 第3级 | 备份还原 | 备份还原 | 备份还原 |
|        | 第2级 | 备份还原 | 备份还原 | 备份还原 |
|        | 第1级 | 备份还原 | 备份还原 | 备份还原 |
|        |     | 一般业务 | 重要业务 | 核心业务 |
| 业务重要程度 |     |      |      |      |

图2 容灾保护矩阵

## 3 云平台实现方案

城轨云平台作为多线路多专业融合的综合平台,提供承载运营生产系统、企业管理信息系统、乘客服务管理系统业务正常时的线网生产中心,同时提供线网级灾备中心,通过云平台统一管理。云平台除提供业务系统所必需的计算、存储、网络资源外,还应提供相应的数据保护功能,如备份服务、容

灾服务,使得传统 IT 模式下复杂的技术实现方案被封装为对用户更加友好的云服务。用户登录云平台提供的管理界面,通过申请云服务的方式,实现针对不同重要程度的业务系统的不同保护措施。同时云平台可为业务系统提供其实现应用双活所需的基础设施。

### 3.1 备份服务

生产中心和灾备中心分别建设备份系统,由云平台封装为备份服务,满足容灾等级为 4 级以下业务,如 PIS(乘客信息系统)、PBE(公务电话系统)、CAS(集中告警系统)等业务的本地备份需求,同时备份系统也可以作为第 5 级、第 6 级容灾方案的补充。

灾备中心设置异地备份系统,满足业务系统的异地备份需求,生产中心的业务系统数据在完成本地的数据备份后,由本地备份系统通过远程数据复制的方式,将本地备份完成的数据传送同步至灾备中心的备份系统进行远端的异地数据备份。

生产中心本地备份数据通过双中心互联的备份链路传输同步到灾备中心的备份系统中,完成异地备份的功能。备份流工作量如图 3 所示。备份数据可以通过备份系统本地还原,也可以跨中心还原,支持本机还原也支持异机还原,满足在病毒入侵、数据误删、系统故障等场景下的数据保护需求。备份服务与传统备份方式相比,无需在备份对象中安装插件,其缺点是需要更多存储容量支持,且不支持文件或目录级恢复。

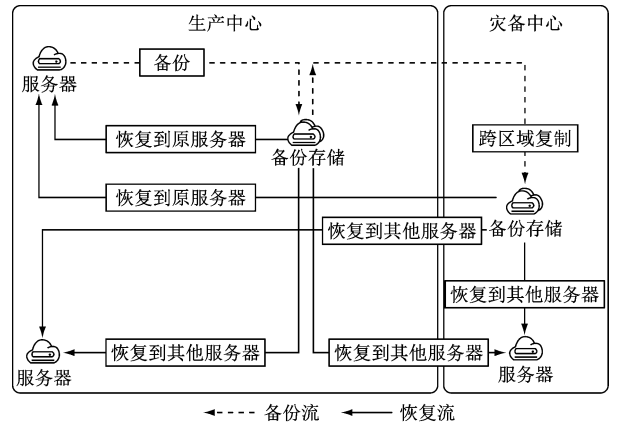


图 3 备份流工作量

### 3.2 容灾服务

对于自身无法实现容灾的业务系统,可在配置备份服务的基础上,进一步使用云平台提供的容灾服务。容灾服务是云平台在同城两个数据中心之间构建主备容灾场景,为业务系统提供第 5 级容灾

保护能力。

用户通过云平台申请容灾服务后,云平台会在主备双中心创建一对容灾保护实例,利用存储的远程复制功能,将生产中心需要保护的数据采用同步复制或异步复制的方式保护至灾备中心。同步远程复制工作模式下可实现数据零丢失,异步远程复制工作模式下会有分钟级数据丢失。灾备中心的容灾云服务器日常处于关机状态,仅当生产中心发生故障需要切换时,容灾管理员手工触发切换任务,将业务系统恢复至灾备中心。恢复期间业务会发生中断,业务恢复后可由灾备中心为车站提供服务。容灾服务情况如图 4 所示。

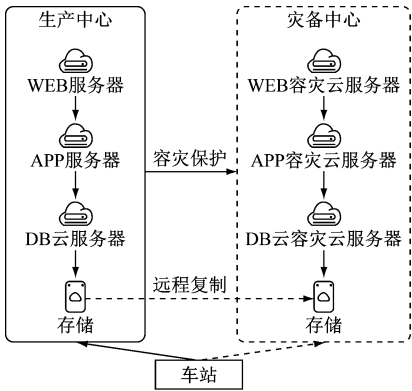


图 4 灾备服务

#### 3.2.1 应用案例

以综合监控业务部署为例,通过对中心区域实时服务器、区域实时服务器、通信前置机创建保护实例,实现对应用进行保护。云平台容灾服务要求主备双中心容灾实例计算类型一致,因此,除中心区域实时服务器使用数据库同步方式外,其他应用服务器使用云平台容灾服务实现。

表 2 灾备服务

| 保护对象      | 计算类型 |      | 容灾方式  |
|-----------|------|------|-------|
|           | 生产中心 | 灾备中心 |       |
| 中心历史服务器   | 裸金属  | 虚拟机  | 数据库同步 |
| 区域实时服务器 1 | 虚拟机  | 虚拟机  | 容灾服务  |
| 区域实时服务器 2 | 虚拟机  | 虚拟机  | 容灾服务  |
| 区域实时服务器 3 | 虚拟机  | 虚拟机  | 容灾服务  |
| 通信前置机     | 虚拟机  | 虚拟机  | 容灾服务  |

1) 服务创建:灾备中心创建容灾数据库虚拟机,通过配置 MySQL Replication 实现主备双中心数据同步;灾备中心使用与目标虚拟机相同镜像创建

容灾虚拟机;为适应业务 IP 不变,增加 VPC(虚拟私有云)内部子网,仅在灾备中心通信,避免 IP 冲突;创建容灾保护实例,添加生产中心及灾备中心对应虚拟机。

2) 容灾切换:登录管理平台,执行计划性迁移,模拟故障发生后资源切换,约 6 min 7 s 后完成测试切换。

3) 应用恢复:利用灾备中心 VPC 内部子网使各服务器按照原有 IP 地址进行通信;启动程序恢复应用;启动在线服务后,即可从中心的下装服务器中获取数据,通过 HMI 进行数据库相关的读写操作,可读取关系库中的历史趋势、事件、报表、应用配置,构造事件和点值变化,也可正常写入数据库,验证通过。

### 3.2.2 容灾限制

容灾服务相比传统模式下人工配置,可极大地简化底层配置,但在实践研究中由于容灾实现原理或业务系统本身配置问题,存在以下使用限制:①容灾服务要求主备中心主机类型一致,如生产中心为裸金属服务器,则要求灾备中心对应的容灾服务器也为裸金属服务器;②容灾服务器无法沿用生产中心 IP,切换后 IP 发生变化,对于将 IP 写进配置文件中的业务系统无法直接做到应用恢复。

## 3.3 应用双活方案

应用双活方案主要由业务系统实现,云平台可以为业务系统提供必要的基础设施环境。

对于 ATS(列车自动监控系统)业务与行车指挥相关,应做到双中心业务同时在线,生产中心与灾备中心可秒级切换,数据零丢失,实现对行车实时控制<sup>[5]</sup>。双中心同时部署应用服务器、数据库服务器、通信前置机,中心级应用与车站实时通信,业务人员可主动切换双中心 ATS 状态,也可在生产中心故障发生时,自动切换至灾备中心继续提供远程控制服务。

## 4 对未来云平台容灾的思考

云平台通过对底层技术的封装,降低业务系统容灾配置门槛,简化容灾配置。同时,云平台提供容灾方案,需要业务系统的应用架构相匹配,才能更好地发挥云平台的优势。基于此情况提出以下城轨业务容灾实现方案。

### 4.1 备份恢复

#### 4.1.1 备份

业务系统允许安装备份插件时,可以选择文件、目录或数据库级别的备份恢复,在满足细粒度备份需求的同时,减小存储容量,有利于降低成本<sup>[6]</sup>。业务系统对备份插件敏感时,可以使用云硬盘、云服务器整机备份恢复功能。

对文件、目录、数据库或云硬盘、云服务器的备份,应支持本地备份和远程复制功能。

#### 4.1.2 恢复

备份恢复时,本地备份介质应支持本地同机、异机恢复,也支持异地、异机恢复。远程备份介质支持异地异机恢复。

### 4.2 容灾恢复

#### 4.2.1 容灾需求

生产中心业务系统,如 AFC(自动售检票系统)、ISCS(综合监控系统)、ACS(门禁系统)等业务涉及运营生产,在备份服务的基础上需要实现容灾保护。当故障发生后,业务系统可将关键业务所在云服务器切换至灾备中心。利用灾备中心资源池、网络等重建业务系统,重建后的业务系统可恢复故障发生前全部数据且业务逻辑可继续执行。对车站可通过唯一入口访问主备双中心业务系统。

#### 4.2.2 容灾条件

为保障业务系统容灾方案能发挥其预期效果,应满足如下条件:①生产中心、灾备中心均有网络通道至车站,且双中心间网络通道互不依赖;②双中心业务切换引起 IP 更改后,业务主机可利用某种机制(如 DNS(域名系统)自动切换、基于全局负载均衡 GLSB(全局负载均衡)切换等),实现自动切换链路对接新 IP<sup>[7]</sup>;③双中心数据库计算资源类型一致。

#### 4.2.3 容灾切换

当生产中心发生故障导致大范围业务故障,需要切换至灾备中心时,容灾管理员可手动将目标业务系统切换至灾备中心,容器切换中涉及的内容大致包括:①维护人员判定符合容灾切换条件;②容灾管理员登录灾备云平台触发容灾切换;③业务系统云服务器在灾备中心完成重建;④ GLSB/DNS 映射自动更新;⑤车站与灾备中心连接恢复;⑥业务完成重建。容灾切换如图 5 所示。

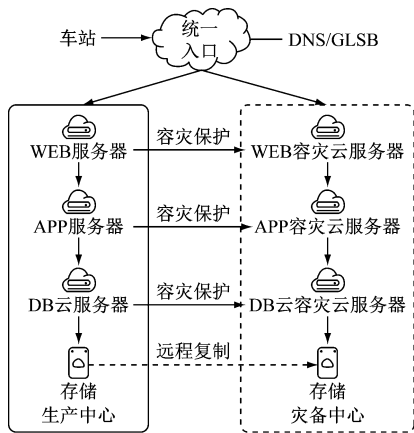


图5 容灾切换

## 5 结语

城轨云平台在为业务系统提供计算、存储、网络资源的同时,通过技术手段将备份还原、容灾保护等复杂的技术实现封装为简单易操作的服务,将业务人员从复杂的底层技术细节中解脱出来,使其更专注于业务本身。通过城轨云平台的引入,使传

(上接第183页)

互联互通特定应用测试阶段各承包商(集成商)/供应商需提交的文档及安全评估方所开展的安全评估活动,表2仅是测试阶段、提交文档和评估活动的建议,承包商(集成商)/供应商可根据实际情况调整测试阶段、提交文档和评估活动。

## 6 结语

目前,城市轨道交通逐步向互联互通的方向发展,国内各轨道交通信号系统厂商均在进行互联互通信号系统的开发研制,延伸线采用其他厂商互联互通信号系统,突破既有信号系统厂商捆绑,具备工程技术可行性和工程应用安全性。互联互通信号系统的安全认证也将成为其重要一环,而确定互联互通信号系统安全要求、互联互通安全接口、安全保证方法、测试验证范围和安全评估原则,是实现不同厂商信号系统互联互通关键技术之一。实践证明:本文提出的互联互通信号系统安全保证和安全认证方法能满足延伸线多厂商信号系统互联互通安全使用的要求,为延伸线采用互联互通不同信号厂商设备提供了良好的借鉴作用,推动了城

轨模式下除保护信号系统、综合监控、自动售检票等业务外,其他生产系统也可以较低成本实现更高等级保护。基于云平台架构的容灾保护有利于增强企业IT能力,提升企业信息化水平。

## 参考文献

- [1] 刘跃,宋兵.信息系统异地容灾技术探讨[J].中国传媒科技,2012(23):74.
- [2] 刘淑鹤,王芳.数据容灾技术研究[J].网络安全技术与应用,2013(9):45.
- [3] 张华,徐娟.灾备技术的现状与发展[J].宜宾学院学报,2012(6):88.
- [4] 周斌.浅谈数据备份技术与实践[J].通讯世界,2013(13):61.
- [5] 张赞,杨林曼,闫倩如.ATS系统双中心热备运行研究[J].自动化应用,2019(6):59.
- [6] 刘志宏.地铁综合监控系统的数据备份与恢复系统研究[J].通讯世界,2018(5):21.
- [7] 谢新标.IT系统应急容灾技术介绍与选型[J].通讯世界,2016(13):228.

(收稿日期:2020-05-21)

市轨道交通信号系统互联互通技术的开发和安全评估。

## 参考文献

- [1] IEC.轨道交通:城市自动化轨道交通运输(AUGT)安全性要求:IEC 62267—2009[S].Geneva:IEC,2009.
- [2] 张凯.轨道交通信号系统独立安全评估的原理和方法综述[J].城市轨道交通研究,2017(6):7.
- [3] 中国城市轨道交通协会.城市轨道交通 基于通信的列车运行控制系统(CBTC)互联互通工程规范:第2部分:安全评估:TCAME/T 040013.2—2018[S].北京:中国城市轨道交通协会,2018.
- [4] 中华人民共和国国家质量监督检验检疫总局.轨道交通:可靠性、可用性、可维修性和安全性规范及示例第2部分:安全性的应用指南:GB/T 21562.2—2015[S].北京:中国标准出版社,2015.
- [5] 中华人民共和国国家质量监督检验检疫总局.轨道交通:通信、信号和处理系统 控制和防护系统软件 GB/T 28808—2012[S].北京:中国标准出版社,2012.
- [6] 中华人民共和国国家质量监督检验检疫总局.轨道交通:通信、信号和处理系统 信号用安全相关电子系统:GB/T 28809—2012[S].北京:中国标准出版社,2012.

(收稿日期:2020-05-09)