ICS 35.020
CCS L67

团　体　标　准

T/GZBD 10-2022

大数据容灾备份建设指南

Construction guidelines for big data disaster recovery and backup

2022-11-21 发布　　2022-12-21 实施

贵州省大数据发展促进会　发 布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由贵州省大数据发展促进会提出并归口。

本文件起草单位：贵州大学（省部共建公共大数据国家重点实验室）、贵州国卫信安科技有限公司、贵州数安汇大数据产业发展有限公司、贵州中云数据服务有限公司。

本文件主要起草人：陈玉玲、李少波、秦永彬、杨义先、胡建文、罗运、吕虓、钱晓斌、彭长根、龙洋洋、董森、李涛、张馨予、谭超月、张邦梅、丁会敏、杨国栋。

大数据容灾备份建设指南

1 范围

本文件提供了大数据容灾备份建设的建设原则、风险分析、模式确定、技术确定、项目建设等建议。

本文件适用于指导大数据容灾备份的建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 36957—2018 信息安全技术 灾难恢复服务要求

3 术语和定义

下列术语适用于本文件。

3.1

灾难 disaster

由于人为或自然的原因,造成信息系统严重故障或瘫痪，使信息系统的业务功能停顿或服务水平不可接受、达到特定的时间的突发性时间。通常导致信息系统需要切换到灾难备份中心运行。

[来源：GB/T 20988—2007，3.8]

3.2

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击，侵入、干扰,破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239-2019，3.1]

3.3

容灾 disaster recovery

一种降低灾难损失的系统部署方案。部署一套和生产系统相当的灾备系统作为生产系统的一个备用，以便在生产系统故障时能够保存生产数据，在生产系统恢复前将应用切换到灾备系统中运行，生产系统恢复后将应用重新切换到原生产系统中运行。

[来源：YD/T 3511-2019，2.3]

3.4

数据完整性 data integrity

数据的精确性和可靠性。它是防止数据库中存在不符合语义规定的数据和防止因错误信息的输入输出造成无效操作或错误信息而提出的。数据完整性分为四类:实体完整性、域完整性、参照完整性、用户自定义完整性。

[来源：YD/T 3511-2019，2.6]

3.5

去重 deduplication

一种可自动搜索重复数据，将相同数据只保留唯一的一个副本，并使用指向单一副本的指针替换掉其他重复副本，以达到消除冗余数据、降低存储容量需求的存储技术。

[来源：YD/T 3511-2019，2.1]

3.6

复时间目标　recovery time objective

灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。

[来源：GB/T 20988-2007，3.18]

3.7

恢复点目标　recovery goal

灾难发生后，系统和数据必须恢复到的时间点要求。

[来源：GB/T 20988-2007，3.19]

3.8

生产中心　production center

利用数据中心场地和环境支撑机构生产系统运行，对机构的重要信息进行集中管理和处理的场所和组织。

[来源：GB/T 30285-2013，3.4]

3.9

灾难恢复中心　disaster recovery center

满足机构关键业务运营连续性的要求，利用数据中心场地和环境支撑机构灾难备份系统运行，抵御导致生产系统全部或部分不可用的灾难，用以接替生产中心部分或全部职能，对机构重要信息进行集中管理和处理的场所和组织。

注：灾难恢复中心也称为容灾中心或灾备中心。灾难恢复中心按照其风险防范职能及与生产中心的距离，可分为同城灾难恢复中心和异地灾难恢复中心。

[来源：GB/T 30285-2013，3.5]

3.10

数据备份　data backup

利用备份软件将信息系统数据按照既定备份策略定期备份到磁带或磁盘等介质，或通过数据复制工具在本地建立一个数据的可用副本。

[来源：YC/Z 583-2019，3.6]

3.11

两地三中心　three centers of two places

在同城双中心的容灾备份模式下增加异地容灾备份模式，在两地构建三个数据中心的容灾备份模式种类。

4　建设原则

按需建设，经济实用，性能优越，安全可靠。

5　风险分析

5.1　风险种类

大数据容灾备份风险种类包括：

a）自然类灾害：泥石流、地震、台风、洪水等；

b）基地类灾害：供电故障、火灾、通信故障、雷击、人为盗窃；
c）系统类灾害：存储介质故障、黑客攻击、误操作等。

5.2 风险预防

按 GB/T 22239-2019 中 6.1 的规定执行。

5.3 风险等级

大数据容灾备份的风险等级由灾难发生后的恢复时间目标(RTO）及恢复点目标（RPO）综合决定，根据不同业务需求程度，大数据容灾备份风险等级评定表见表1。

表1 大数据灾难备份风险等级评定表

容灾备份风险等级	RTO	RPO
1	2天以上	1天至7天
2	24小时以上	1天至7天
3	12小时以上	数小时至1天
4	数小时至两天	数小时至1天
5	数分钟至两天	0至30分钟
6	数分钟	0

6 模式确定

6.1 两地三中心容灾备份

a） 具有配套的生产中心、同城大数据容灾备份中心、异地大数据容灾备份中心基础系统；
b） 异地容灾备份中心能独立承担生产工作；
c） 同城容灾备份中心与生产中心宜通过高速链路实时同步数据；
d） 同城容灾备份中心可分担生产中心的日常工作；
e） 同城容灾备份中心可与生产中心切换运行。

6.2 同城容灾备份

a） 容灾备份中心和生产中心建立在相近的区域内，距离≤300 km；
b） 容灾备份中心和生产中心应使用专用通信信道（光纤通信）；
c） 应使用同步容灾备份技术；
d） 在生产中心工作受阻时灾难备份中心应能及时接替生产中心的工作，立即恢复生产工作。

6.3 云端容灾备份

a） 云端拥有足够的存储资源；
b） 生产中心和云端始终保持链路连接；
c） 核心数据需加密后上传；
d） 云端数据时刻保持安全状态，定时与生产中心校准。

6.4 异地容灾备份

a) 灾难备份中心和生产中心建立在距离较远的区域，距离＞300 km；
b) 灾难备份中心应能防范火灾、建筑物破坏等可能遇到的风险隐患；
c) 灾难备份中心应能防范战争、地震、水灾等潜在的风险；
d) 在生产中心工作受阻时灾难备份中心能接替生产中心的工作，在相应时间内恢复生产工作。根据表 1 和大数据容灾备份模式特点，大数据容灾备份模式确定表见表 2。

表2 大数据容灾备份模式确定表

容灾备份模式	容灾备份风险等级					
	1	2	3	4	5	6
两地三中心模式	√	√	√	√	√	√
同城模式	√	√	√	√	√	
云端模式	√	√	√	√		
异地模式	√	√				
注：“√”表示该模式适用于相应的风险等级。						

7 技术确定

7.1 同步容灾备份

生产中心与大数据容灾备份中心的资源信息保持一致。生产中心生成的信息应及时传输至大数据容灾备份中心，生产中心接收到大数据容灾备份中心发出的同步信息后，进行下一步生产操作。大数据同步容灾备份示意图见图1。

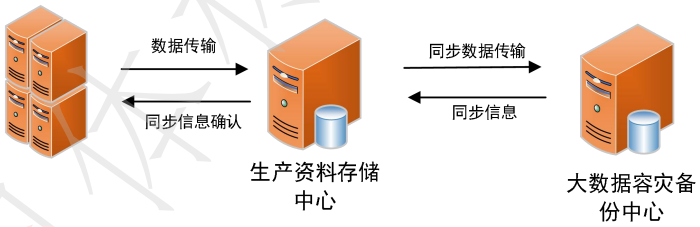

图1 大数据同步容灾备份示意图

7.2 半同步容灾备份

生产中心建立缓存中心，并在生产活动后将资源存放至缓存中心。待缓存中心刷新时，将缓存中心中存放的资源备份至大数据容灾备份中心，生产中心和大数据容灾备份中心不直接产生交互。大数据半同步容灾备份示意图见图2。

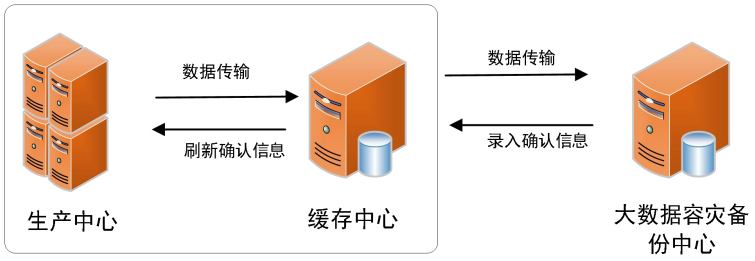

图2 大数据半同步容灾备份示意图

7.3 时间点容灾备份

生产中心和大数据容灾备份中心根据自身条件提前确定容灾备份时间段，根据约定的时间段生成资源快照，大数据容灾备份中心根据生产中心的资源快照进行容灾备份。大数据时间点同步容灾备份示意图见图3。

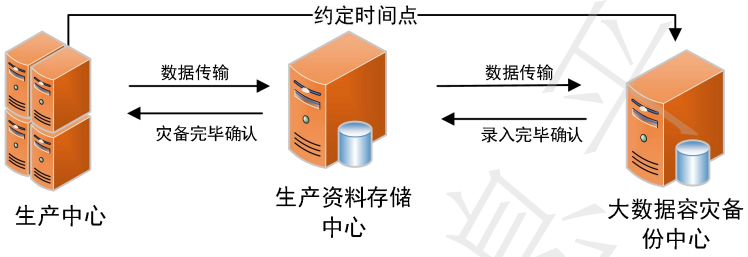

图3 大数据时间点容灾备份示意图

7.4 异步容灾备份

生产中心在生产活动后将生产资料备份至大数据容灾备份中心，大数据异步容灾备份示意图见图4。

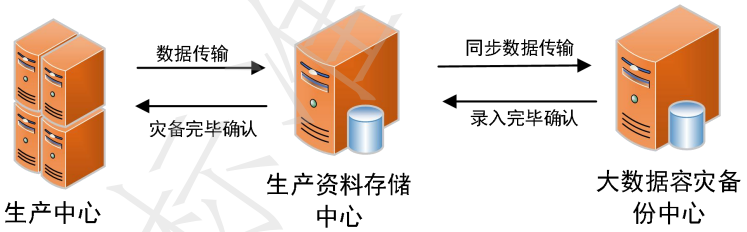

图4 大数据异步容灾备份示意图

根据大数据容灾备份模式和容灾备份性能需求，大数据容灾备份技术确定表见表3。

表3 大数据容灾备份技术确定表

容灾备份模式	容灾备份风险等级					
	1	2	3	4	5	6
两地三中心模式	异步备份	异步备份	时间点备份	半同步备份	半同步备份	同步备份
同城模式	异步备份	异步备份	时间点备份	半同步备份	同步备份	同步备份
云端模式	异步备份	时间点备份	半同步备份	同步备份	同步备份	同步备份
异地模式	时间点备份	半同步备份	半同步备份	同步备份	同步备份	同步备份

8 项目建设

8.1 资源配置

按GB/T 36957-2018中 5.1、5.2、5.3、5.4的规定执行。

8.2 恢复范围及目标

根据风险等级和模式技术选择的结果，确定大数据容灾备份的恢复范围及目标，包括：

a）关键业务功能恢复的先后顺序；
b）关键业务及数据的恢复范围；
c）灾难恢复的时间范围。

8.3 协议

a） 建立一致及规范的大数据容灾备份协议，明确大数据容灾备份安全要求（如传输通道加密、数据内容加密、签名验签、身份鉴别、数据传输接口安全等），确定大数据容灾备份的应用场景；
b） 现行协议将持续至此次容灾备份结束，不受更新的协议所干扰；
c） 在进行大数据容灾备份之前宜进行系统协议一致性测试。

参 考 文 献

[1] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
[2] GB/T 30285-2013 信息安全技术 灾难恢复中心建设与运维管理规范
[3] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[4] YC/Z 583-2019 烟草行业信息系统容灾备份建设指南
[5] YD/T 2916-2015 基于存储复制技术的数据灾备技术要求
[6] YD/T 3511-2019 灾备数据去重系统技术要求