

# 以异地备份为途径解决数据安全问题

李 轩

( 中国国家博物馆 北京 100006 )

**摘 要:** 本文目内容是以国家博物馆为例, 探讨如何通过建设异地备份为途径, 保数据安全和预相关风险。

**关键词:** 博物馆; 异地备份; 数据安全

## 一. 项目背景

### 1.1 概述

中国国家博物馆是代表国家收藏、研究、阐释并充分反映社会主义先进文化、革命文化和中华优秀传统文化代表性物证的重要公共文化机构, 珍藏着中华民族集体记忆, 传承着国家文化基因, 是全世界唯一可以呈现中华文明五千年完整发展历程的博物馆。

国博生产和保存的文物数据是极其珍贵的电子资源, 数据量大且增长较快, 但尚未实现异地灾备, 一旦丢失或损毁, 对中华文明的守护和传承工作将造成无法估量和弥补的损失。具体情况如下:

一是数据量庞大。国博现有文物数据存量已超过 800TB, 数据增量每年约 150TB, 且数据增长速度越来越快。这些数据的生产、管理及保存花费了大量人力和物力成本, 一旦因灾害或事故造成丢失或损毁, 损失将十分惨重。

二是数据备份工作难度增加。随着“智慧国博”建设工程的全面铺开, 二维、三维文物影像数据采集工作也紧锣密鼓进行, 藏品大数据平台搭建完成并逐步完善, 业务运行数据库和藏品数据库集群也相继建立, 数据量大、文件类型多样且许多数据不可再生, 日常管理分类及数据备份工作难度较高。

三是数据存在无法规避的安全隐患。当前国博文物数据皆存储于同一本地机房, 如发生火灾、电路故障等险情, 很难保证所有数据的完整和安全, 面对人为误操作、病毒、网络攻击、软硬件故障、自然灾害等意外事件时缺少必要的安全保护, 一旦风险发生, 可能会严重影响到业务的正常开展, 带来无法估量和弥补的损失及负面影响。此外, 近年来我国网络安全事件层出不穷, 文物数据存在的网络安全风险不容忽视, 传统本地备份模式已难以满足现实需求。

### 1.2 现状分析

目前, 国家博物馆文物数据业务主要部署在内网, 内网业务部署在浪潮云平台, 后端采用宏杉存储, 主要为二维图片、三维模型等数据; 办公和系统采用华为私有云平台进行建设, 运行有 20+业务系统, 涉及操作系统主要是 CentOS 和 Windows, 数据库包括达梦、高斯等, 后端采用华为集中存储; 国家博物馆本地已采用一套备份系统进行了数据保护, 尚未建设异地灾备系统。

2018 年, 国博已开始筹备异地数据灾备中心的建设工作。当前应尽快开展异地数据灾备建设工作, 馆内机房现有设备可根据迁移工作的需要有序进行迁移, 保证设备的利用率, 异地灾备机房可以对现有数据提供有效的额外保护, 使数据安全更有保障。

## 二. 解决方案

中国国家博物馆异地数据灾备中心基础建设项目是为应对自然灾害、人为事故等各种突发事件, 保障国博信息系统业务连续性和

数据安全而建设的具备备份、容灾、恢复能力的信息系统基础设施。通过建设一个技术先进、可靠性高、可用性高、管理便利的异地数据灾备中心, 实现中国国家博物馆数据资源的备份及管理, 进一步完善数据资源安全存储机制, 保障国博各类数据资源安全。

国博信息系统总体结构相对复杂, 涉及的应用系统较多。在构建灾备系统时需要中心信息系统结构做深入调研和论证, 结合具体需求及相关法规、指南要求进行统一规划。

### 2.1 项目需求

根据国家相关法律法规, 异地灾备中心应与本地数据中心距离至少 100KM 以上, 同时还必须做到“三不”, 即不在同一地震带, 不在同一电网, 不在同一江河流域。当灾难发生时, 才可保证至少一个数据中心安全存活。经初步论证, 综合考虑了成本、距离等因素, 目前选定内贵州贵阳计算中心, 该灾备数据中心设施完善, 具备相应的安全供电、安防、消防系统, 供电稳定, 是三大电信运营商在内蒙古自治区“最先设计、最先开工、最先运营”的云计算基地, 建成后将是最大的云计算园区, 亚太地区最大的互联网数据交互中心, 同时也是“互联网+”生态圈的核心。

因灾备中心备份数据为国博文物影像数据和业务运行数据, 业务运行数据主要备份内容为各系统数据库, 文物影像数据内容为非结构化照片, 三维模型等, 因为灾备中心应具有数据库和非结构化数据每日自动化备份功能, 且对国博目前使用的数据库具有良好兼容性, 并且当灾难发生时, 可以通过快照、镜像等形式立即回滚前日数据至本地数据中心。

存储量方面, 国博文物数据量总计约 800TB, 考虑未来增量, 灾备中心应至少具有 1.2PB 的容量。建成后可对国博文物数据实现多方位保护, 包括每日定时备份当日新增数据, 每季度进行全量比较、备份, 实时统计存储量信息等。保证应用多种技术, 实现对数据安全的全面保障, 通过量化比对技术感知数据变化, 对重要数据进行永久保存。

### 2.2 建设内容

主要建设内容是异地灾备中心选址并开始建设, 并开始数据迁移与数据恢复实验。综合安全、使用等多方面因素, 为更好的解决数据保护的问题, 本次建设内容如下:

- (1) 部署一套数据集中备份系统, 接入现有网络环境, 用于实施备份策略并存储备份生产业务核心数据;
- (2) 针对数据业务数据建立快速数据恢复机制;
- (3) 支持各类主流数据类型业务系统备份保护;
- (4) 实现业务系统的系统级备份和恢复;
- (5) 实现对国产化系统环境的兼容适配;

(6) 满足等保合规建设要求, 避免法律风险。

其中, 基础环境的建设是本次建设的重点内容。基础环境建设指存储设备、网络设备及运营商数据中心机柜租赁等建设工作。

### 2.3 设备需求

部署在异地的灾备一体机需要配套相应设备, 才能够搭建起完整的网络, 实现数据传输。从配置考虑, 计算未来扩容后的数据量。所需设备参数如下:

#### (1) 数据交换机

序号	指标项	指标要求
1	容量	总可用容量: 1.2PB; 单台系统存储: 配置≥ 10块 SSD, 容量不小于 200TB 备份数据存储: 支持重复数据删除,且包含相应容量重复数据删除授权 支持去重数据复制至容灾端, 配置容灾复制授权。
2	CPU	支持国产或 X86 架构处理器, 主频不低于 2Ghz
3	内存	单台内存配置容量: ≥256GB
5	接口	单台配置: ≥4*GE 电口, ≥4个 10Gb 光口(含光模块)
6	授权	备份软件容量与硬件实配有效容量相同, 不限制备份客户端数量、重删、备份恢复功能等。

#### (4) 机柜租赁服务

待全部设备购置完成后, 我部门拟租赁运营商异地数据中心机柜, 用以放置设备, 因运营商数据中心已具备完整消防、电力、安防条件, 故只需定时巡检即可。

存放机柜的运营商机房应满足以下标准: 国际 TierIII 以上标准、工信部 A 级机房标准, 且结构安全等级一级, 满足 8 级抗震、9 级抗裂、一级耐火、一级防水抵、御强烈风暴和其他自然灾害的能力, 本项目出口带宽至少保证可达到 1000Mbps, 以供未来升级, 具备双路供电系统, 可保证 24 小时不断电, 网络丢包率应小于 5%。

目前, 采用爱数 AnyBackup Enterprise 8.0 AB9120 设备作为信息系统数据保护解决方案。整个方案涉及到的系统包含有: Windows 服务器, Linux 服务器, 虚拟化, 华为云环境。

### 三. 部署实施及应用

目前, 在北京本地数据中心和贵州数据中心各部署一套爱数备份与恢复系统 AnyBackup Enterprise 8.0, 设备型号均为 AB9120, 在北京数据中心备份虚拟机、文件系统、数据库等业务数据, 然后利用远程复制技术, 将已备份完成的数据复制到贵州的备份系统, 实现备份数据备份和异地数据备份。图示如下:



#### 3.1 系统组网规划

带外管理网络: 每台备份系统连接千兆以太网交换机, 用于备份设备带外管理, 用于设备维护。

交换容量应大于 2.56/25.6Tbps, 包转发率应大于 1000Mpps, 具备至少 24 个 10GE SFP+端口, 6 个 40GE/100GE QSFP28 端口。

#### (2) 带外网管理交换机

外网保障业务链路出现问题时, 也可以实现对设备的管理, 需要 1 台 48 口千兆交换机用于备份一体机的带外管理和维护。

设备配置建议: 48 个 10/100/1000BASE-T 电口, 支持 4 个 1000BASE-X SFP 端口, 满配光模块。

#### (3) 备份一体机

管理、备份网络: 使用两个万兆口绑定, 用于数据备份和恢复操作管理、备份系统内部数据交互以及备份恢复流量。

数据复制网络: 使用两个万兆网口绑定, 用于备份数据异地复制, 北京和贵州的备份系统之间互传备份数据。

#### 3.2 定时备份任务

在业务系统内安装备份客户端, 登录备份系统 admin 用户配置备份任务, 创建文件、数据库等备份任务。当本地备份作业运行后, 将北京数据中心的数据通过远程复制技术, 将备份数据复制到贵州的备份系统, 登录备份系统 admin 用户, 添加对端资源信息, 配置远程复制策略。

### 四. 结语

本项目目标是建设一个容量充足、每日定时备份、符合国家相关法规要求的异地数据灾备中心, 建设完成后可将国博所有数据, 包括结构化数据和非结构化数据, 安全备份到异地机房保存, 并在本地系统异常时, 可及时将备份数据恢复至本地, 以更好的保护文物和系统数据, 通过以上相关实施和部署, 可实现两地三中心多点备份要求, 充分保障了文物数据和业务数据的安全性。

#### 参考文献:

- [1]《“十四五”时期“智慧国博”建设专项战略规划》
- [2]《“智慧国博”2023 年实施方案》
- [3]《中华人民共和国网络安全法》
- [4]《信息安全技术—网络安全等级保护基本要求》(GB/T 22239-2019)
- [5]《中华人民共和国数据安全法》
- [6]《信息安全技术 信息安全风险评估规范》(GB/T 20984-2007)
- [7]《信息安全技术 信息系统灾难恢复规范》(GB/T 20988-2007)
- [8]《信息安全技术 信息安全事件分类分级指南》(GB/Z 20986-2007)

作者简介: 李轩 性别: 男、出生年月(1989.12-), 职称: 工程师、学历: 本科, 研究方向: 计算机软件与硬件。