

数 字 山 东 工 程 标 准

SZSD 0020—2024

灾备节点技术要求

Technical requirements for disaster recovery node

2024 - 04 - 15 发布

2024 - 06 - 01 实施

目 次

前言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 技术架构..... 1

5 基础设施..... 2

6 服务管理..... 2

 6.1 数据备份服务..... 2

 6.2 数据备份管理..... 2

 6.3 灾难恢复管理..... 2

 6.4 灾备服务门户..... 2

7 监控管理..... 3

8 运维要求..... 3

9 安全要求..... 3

 9.1 概述..... 3

 9.2 安全管理要求..... 3

 9.3 安全技术防护..... 3

参考文献..... 4

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。

本文件由山东省大数据局提出、归口并组织实施。

本文件起草单位：山东省大数据中心、山东省齐鲁大数据研究院、山东新一代标准化研究院有限公司、浪潮云信息技术股份公司、华为技术有限公司、上海爱数信息技术股份有限公司、上海英方软件股份有限公司。

本文件主要起草人：张荣光、朱效民、薛冰、赵硕、陈克磊、张继辉、谢枫、张浩秋。

灾备节点技术要求

1 范围

本文件规定了灾备节点的技术架构、基础设施、服务管理、监控管理、运维要求和安全要求。
本文件适用于灾备节点的建设、管理和使用。

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件必不可少的条款。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 30285—2013 信息安全技术灾难恢复中心建设与运维管理规范
SZSD 0019—2024 政务信息系统灾备指南
SZSD 0021—2024 灾备节点监管规范

3 术语和定义

GB/T 30285—2013界定的以及下列术语和定义适用于本文件。

3.1

生产系统 production system

正常情况下支持机构日常运作的信息系统。

[来源：GB/T 30285—2013，3.1]

3.2

灾备节点 disaster recovery node

满足政务部门关键业务运营连续性的要求，利用数据中心场地和环境承载备份数据，支撑灾难恢复系统运行，抵御导致生产系统（3.1）全部或部分不可用的灾难，对政务部门重要信息进行集中管理和处理的场所和组织。

4 技术架构

根据灾备需求建设三个省级灾备节点，各灾备节点基于本地基础设施搭建一套服务管理、监控管理、运维和安全保障体系，为全省提供灾备服务，技术架构见图1。

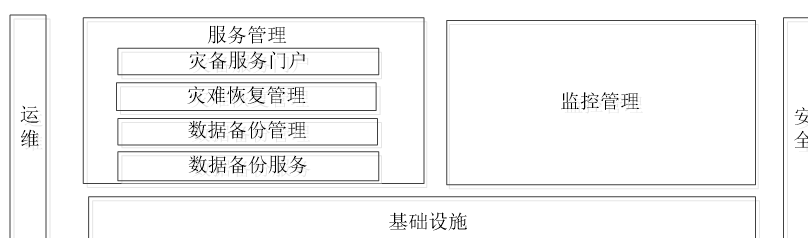


图1 技术架构

5 基础设施

各灾备节点提供灾备服务所需的基础设施资源，包括计算资源、存储资源、网络资源、支撑软件资源、安全保障资源等。

6 服务管理

6.1 数据备份服务

数据备份服务内容包括但不限于：

- 应支持本地备份，在生产系统部署备份相关的服务，对生产系统上的数据进行本地备份；
- 宜支持跨平台备份，在多平台架构中，将一个平台的数据备份到另一个平台并可恢复；
- 宜支持跨地域备份，在多地域架构中，将一个地域的数据备份到另一个地域并可恢复；
- 宜采用国密算法备份技术，对关键数据进行数据备份；
- 在生产系统侧进行数据备份时，宜提供识别并去除已备份数据块的服务。

6.2 数据备份管理

数据备份管理功能包括但不限于：

- 应支持生产系统、数据库等的数据备份恢复，包括全量备份、增量备份、差异备份等方式；
- 应提供实例的状态信息、健康运行状态信息，以及实例关联的备份计划信息的获取和分析等功能；
- 应提供备份记录的统计、日志等运维信息的管理；
- 应提供告警规则的设置，监控告警信息的查看等功能；
- 应支持备份作业、日志访问、策略管理、备份数据访问等涉及安全相关的所有操作进行访问控制策略设置。

6.3 灾难恢复管理

灾难恢复管理功能包括但不限于：

- 应提供灾备资源管理、预案管理、灾备配置等功能；
- 应提供灾备策略、灾备方案、灾备服务实施、灾备演练等所有服务的流程化管理功能；
- 应提供灾备切换过程自动化、可视化管理功能；
- 应提供对灾难恢复能力的评估功能。

6.4 灾备服务门户

灾备服务门户主要包括以下内容：

- a) 应提供灾备服务目录浏览、查询、申请功能；
- b) 应提供数据备份服务的申请、审批与分配、服务使用量统计等功能；
- c) 应提供用户查看所有下属子部门及系统资源使用情况、各类服务资源管理、考核统计等功能；
- d) 应提供灾备运行状态展示功能。

7 监控管理

通过对接灾备节点基础环境、设备运行、运维管理等系统数据，真实还原灾备节点实时的运行状态，对灾备节点各项异常数据进行告警和定位，实现灾备节点的可视化管理。监控管理服务内容应符合SZSD 0021—2024的相关要求。

8 运维要求

灾备节点的基础设施运维管理应满足GB/T 30285—2013的8.3.2节要求，灾备节点的相关系统运维管理应满足GB/T 30285—2013的8.3.3节要求。

9 安全要求

9.1 概述

灾备节点安全保障应满足GB/T 22239—2019中的网络安全等级保护三级要求，主要包括安全管理要求和安全技术防护两个方面。

9.2 安全管理要求

安全管理要求，包括但不限于：

- a) 建立安全应急保障机制，制定安全事件日常监测和应急处置流程，有效预防和应对安全事件的发生；
- b) 建立安全评估与审计机制，对灾备节点的安全状况进行深入全面完整的评估和审计，及时发现安全体系存在的问题和漏洞；
- c) 建立安全自查与演练机制，应符合SZSD 0019—2024的第7章规定，定期组织灾备节点安全自查工作，并组织对安全事件应急预案及处置措施进行实战演练，持续保持各项安全措施的完整有效，不断优化和完善应急预案；
- d) 建立信息安全保密机制，针对重要数据的使用、传递和保存应制定严格的管理制度，防止重要信息外泄；
- e) 定期组织安全知识和技能培训。

9.3 安全技术防护

安全技术防护要求，包括但不限于：

- a) 网络隔离要求：对于多个生产系统共享的灾备节点，建设时应针对不同生产系统的通信进行安全隔离，避免由于多个生产系统在灾备节点内部的通信互通导致的安全隐患；
- b) 存储安全要求：应根据有承载数据业务的安全需求，制定合理的存储策略，不同安全级别的数据应存放在不同的存储空间中；
- c) 数据安全要求：应采用加密或其他有效措施实现备份系统管理数据、重要业务数据、鉴别信息等传输过程中的保密性。

参 考 文 献

- [1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
 - [2] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范
 - [3] GB/T 30146—2013 公共安全 业务连续性管理体系要求
 - [4] YD/T 2850—2015 灾备系统性能测试方法
-