

数 字 山 东 工 程 标 准

SZSD 0021—2024

灾备节点监管规范

Regulatory specifications 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 缩略语..... 1

5 监管框架..... 1

6 监管角色..... 2

 6.1 监管方..... 2

 6.2 监管对象..... 2

7 监管内容..... 2

 7.1 灾备服务商的监管..... 2

 7.2 灾备使用方的监管..... 3

参考文献..... 5

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：北京邮电大学、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、山东省大数据中心。

本文件主要起草人：辛阳、朱效民、马辉、张荣光、薛冰、赵硕、王传芳、刘云。

灾备节点监管规范

1 范围

本文件规定了灾备节点监管框架、监管角色和监管内容。

本文件适用于灾备节点的建设、管理和使用，也适用于对灾备服务商和使用方进行业务监督管理和绩效评价。

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 37972—2019 信息安全技术 云计算服务运行监管框架

SZSD 0020—2024 灾备节点技术要求

3 术语和定义

SZSD 0020—2024界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

CPU：互联网技术（Internet Technology）

5 监管框架

监管方对灾备服务商、灾备使用方进行监管。监管方应对监管指标数据进行分析审核、评估验证，形成监管结果，并向被监管方反馈意见和建议。监管框架见图1。

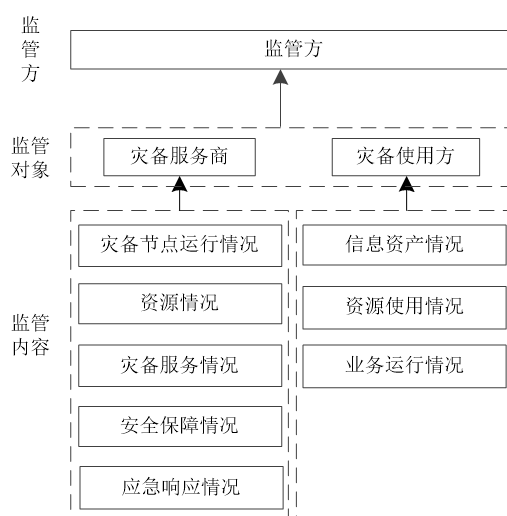


图1 监管框架

6 监管角色

6.1 监管方

- 6.1.1 应制定灾备节点监管要求，建立健全灾备服务监督管理机制，对灾备服务商和灾备使用方进行业务监管。
- 6.1.2 应对监管情况进行综合评估，并将评估结果反馈灾备服务商、灾备使用方。
- 6.1.3 根据监管情况等灾备服务商进行评估考核，并将考核结果作为费用结算的重要依据。

6.2 监管对象

6.2.1 灾备服务商

- 6.2.1.1 应按照监管方要求提供相关监管接口和技术材料，配合其做好灾备节点运行状态和资源情况的监管。
- 6.2.1.2 应根据监管评估结果采取相关措施及时整改，并上报监管方、灾备使用方整改情况。
- 6.2.1.3 应按照合同要求或与灾备使用方的约定，做好灾备服务的提供和日常运行保障工作，定期报送运行维护报告、灾备资源利用情况和优化建议等。

6.2.2 灾备使用方

- 6.2.2.1 应在职责范围内合理使用灾备资源，负责生产系统的运行管理，监控生产系统资源使用情况、日常运行状况等。
- 6.2.2.2 应根据资源利用情况及时采取相关措施，确保生产系统安全稳定运行。
- 6.2.2.3 应向监管方、灾备服务商提供资源使用监管账号，并对灾备服务商进行服务质量评价。

7 监管内容

7.1 灾备服务商的监管

7.1.1 灾备节点运行情况

灾备节点整体运行状态监管服务内容包括：

- a) 可用性：包括灾备节点的运行状态、运行异常告警信息等；
- b) 网络流量：包括灾备节点出口和入口的网络流量情况、网络流量变化情况、流量异常告警信息等；
- c) 安全接入：包括安全设备、网络设备等接入情况；
- d) 异常故障告警：包括物理服务器、存储设备、交换机等设备异常告警信息等；
- e) 机房环境：包括机房基础设施运行情况、能源消耗情况等。

7.1.2 资源情况

灾备节点资源监管服务内容包括：

- a) 灾备节点资源的配置、使用、负载等情况；
- b) 物理设备运行监管：包括灾备平台硬件、主机、网络、存储 CPU、内存等资源利用率，以及资源、设备利用率异常告警等；
- c) 资源总体情况：灾备节点的物理服务器总量、存储设备总量、已用存储空间、可用存储空间、双活应用总量等。

7.1.3 灾备服务情况

灾备服务监管内容包括：

- a) 数据级备份情况：监管数据级备份从生产中心到灾备中心的全流程，包括生产系统、所属单位、备份的数据元数据等信息，灾备中心对应的备份信息、数据量信息、更新信息、更新周期等，以及灾备节点离线数据备份总量、离线备份数据的增长情况、数据量增长趋势等；
- b) 灾备演练情况：对灾备演练计划、方案、演练过程、演练结果等进行记录并监管；
- c) 灾备恢复监管：在生产系统发生故障需要利用灾备数据恢复进行系统切换时，从故障发现、定位、恢复或切换启动、操作、验证等全流程监管。

7.1.4 安全保障情况

灾备节点安全保障情况监管内容包括但不限于：

- a) 安全管理制度制定及实施情况；
- b) 安全事件及安全事件响应情况；
- c) 安全防护措施提供情况：包括保障灾备中心基础环境、数据、网络、应用等采取的安全防护措施，具体监管内容和监管要求参见 GB/T 37972—2019 附录 B.1；
- d) 安全策略更新情况；
- e) 安全评估情况：包括灾备节点安全等级保护测评、商用密码应用安全性评估、安全检查、服务安全评估等。

7.1.5 应急响应情况

应急响应情况监管包括但不限于：

- a) 应急响应计划制定及更新情况；
- b) 应急演练开展情况；
- c) 应急响应处置机制、过程及结果的情况。

7.2 灾备使用方的监管

7.2.1 信息资产情况

信息资产情况监管内容包括但不限于：

- a) 资源使用情况：包括灾备设备量、资源数量、资源空间占用量；
- b) 系统清单：包括生产系统和应用清单；
- c) 数据项清单：包括生产系统和应用清单对应的数据项清单。

7.2.2 资源使用情况

系统资源使用情况监管内容包括但不限于物理设备、物理服务器、存储设备、存储空间、双活应用情况等资源分配和使用情况。

7.2.3 业务运行情况

业务运行情况监管内容包括设备运行状态、运行时长等情况。

参 考 文 献

- [1] 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
-