# 宿州市立医院容灾备份系统需求

## 现状及问题分析

我院目前的核心数据库采用物理服务器集群承载,应用服务器及其他次核心业务采用虚拟化/超融合平台承载，可以在一定程度上防止因单个硬件故障导致的业务中断和数据丢失。为防止逻辑错误风险，采用定时备份方式对关键数据进行定时备份，可保证部分重要数据丢失量不大于24小时。已经具备一定的风险防护能力，但仍然存在诸多问题，具体表现在以下几个方面：

1. 发生故障后，数据丢失量大

数据备份覆盖不全面，仅保护了部分关键数据，同时定时备份方式一旦发生数据丢失，数据丢失量为1天。

1. 发生故障时，业务停机时间长

以目前的保护手段，发生系统故障时（包括人为误操作、病毒、勒索病毒等、超融合平台故障任何情况），需要修复平台、恢复数据、补录数据等多种手段结合处理完成后，方可恢复业务运行。总计停机时间需1~3天，而我院正常运营完全依赖于信息化系统，这将导致医院医疗秩序失控。

1. 灾难恢复演练困难

根据电子病历等级评审要求及日常运维需求，灾备系统需定期完成灾难恢复演练（一般是每个季度一次）。目的是验证灾难恢复系统的运行可靠性，同时对工程师进行强化培训。已目前的保护方案，每次灾难恢复演练所需时间超过一周，对医院信息中心造成极大的工作负担。

## 系统需求分析

根据医院业务级别，我们对医院业务系统重要性进行分级分类(可根据实际情况调整)：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 业务系统 | 重要程度 | 规划建议 |
| 1 | HIS、EMR、LIS | A+ | RPO≈0min/RTO≤15min |
| 2 | HRP、RIS、PACS | A | RPO≈0min/RTO≤20min |

结合我院信息化系统业务功能和业务中断影响分析的结论，总结当前对于容灾备份系统的需求如下：

1. 核心业务系统（A+/A）通过CDP连续数据保护和应急接管，可以在数据不丢失的情况下，实现分钟级应急接管；
2. 次核心和一般业务的保护通过NBP定时备份系统，实现虚拟化无代理备份，并支持瞬时挂载恢复，即将备份数据副本挂载至虚拟化平台即可直接恢复应用；

## 关键业务系统统计（预估）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | CPU | 内存 | 数据量 | 级别 |
| HIS | 48 | 512 | 3T | A+ |
| EMR | 48 | 512 | 3T | A+ |
| HRP | 16 | 64 | 0.5 | A+ |
| PACS | 16 | 64 | 0.5T | A |
| LIS | 8 | 64 | 0.5T | A |
| RIS | 8 | 64 | 0.5T | A |
| 合计 | 144 | 1280 | 8T |  |

1. 以上为预估空间

注：HIS为IRIS库。

## 建设目标

本次项目建设对标《电子病历系统应用水平分级评价管理办法及评价标准》，达到七级标准要求，即：

* 具备异地灾备能力
* 数据与系统的恢复时间不大于15分钟，数据丢失时间不超过30分钟。
* 数据与系统的恢复时间不大于2小时，数据丢失时间不超过24小时（五级标准）

同时对标《医院信息系统互联互通成熟度测评方案》，达到五级乙等要求，即：

* RTO≤15分钟，RPO≤15分钟；
* 具备异地灾备能力；
* 具备离线数据备份能力；

通过建设本异地容灾备份系统，提高核心业务的连续性。即：

* 正常情况下，由原生产平台提供业务，容灾备份系统提供灾难恢复演练、测试等任务；
* 发生逻辑错误，导致数据丢失时，可通过容灾备份系统在15分钟内恢复业务，并保证数据丢失量趋于零；
* 生产系统因病毒或勒索病毒等故障，可通过容灾备份系统在15分钟内接管业务；
* 生产平台发生重大硬件故障时，可通过容灾备份系统台在15分钟内接管核心业务，保证业务不中断；
* 生产机房发生灾难事故时，可由异地容灾备份系统在15分钟内接管核心业务，保证业务不中断，数据不丢失。