如何避免删库跑路黑天鹅事件？

---- 快狗打车数据库安全架构最佳实践

沈剑
快狗打车CTO

关于 - 我

- [now] “架构师之路”作者，深夜写写技术文章
- [now] **到家集团**技术委员会主席 & **快狗打车**(原58速运)CTO
- [ex] **58同城** - 高级架构师，技术委员会主席，技术学院优秀讲师
- [ex] **百度** - 高级工程师
- 技术人一枚，管理者一枚

关于 - 快狗打车

- 同城，短途货运，平台
- 拉货，搬家，运东西

关于 - 黑天鹅事件

- 今年年初，WM**删库事件**
- 去年年初，**云故障**
- 自建IDC，**机架故障**
- 不小心**drop错表**，不小心**delete错数据**
- 不小心**删除了根目录**
- 被**拖库**

- 内部恶意
- 外部不可抗力
- 内部架构缺陷
- 内部无意
- 外部恶意

这些问题，要不要解决？

资源有限，优先解决哪些问题？

目录

- 技术体系建设，主要矛盾寻找思路
- 删库黑天鹅，快狗打车最佳实践
- 总结

作为技术负责人，是否有这样的纠结?

资源有限，到底最优先做什么？

- 作为**架构部**负责人，如何规划内部研发框架，组件，技术平台？
- 作为**质量部**负责人，如何规划质量体系建设重点？
- 作为**运维部**负责人，如何规划运维体系建设的重点？
- 作为**DBA**负责人，如何规划数据库体系建设的重点？
- ...

以**运维侧**举例，哪些事情优先级最高?

- 服务器初始化自动化
- RDS申请工单自动化
- 域名申请工单自动化
- 站点与服务发布自动化
- 服务器资源监控，站点与服务进程端口监控，数据库连接监控
- 二进制与配置备份自动化
- ...

原则一：优先做“**最高频，最耗时，效率提升最大**”的事情

以**运维侧**举例，哪些事情优先级最高?

- 服务器初始化自动化
- RDS申请工单自动化
- 域名申请工单自动化
- **站点与服务发布自动化**
- 服务器资源监控，站点与服务进程端口监控，数据库连接监控
- 二进制与配置备份自动化
- ...

那如果是这样，黑天鹅事件发生概率低，岂不是永远轮不上？

- 今年年初，WM**删库事件**
- 不小心**drop错表**
- 不小心**delete错数据**
- 被**删除根目录**
- **...**

原则二：优先做“一旦发生，后果无法接受”的事情

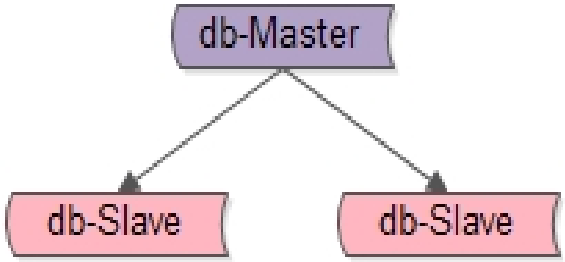
数据安全性无法保障，一旦发生，对公司来说是及其灾难性的！

（对我个人来说，也是），决不允许发生！

问题转化为，如何保证数据安全性?

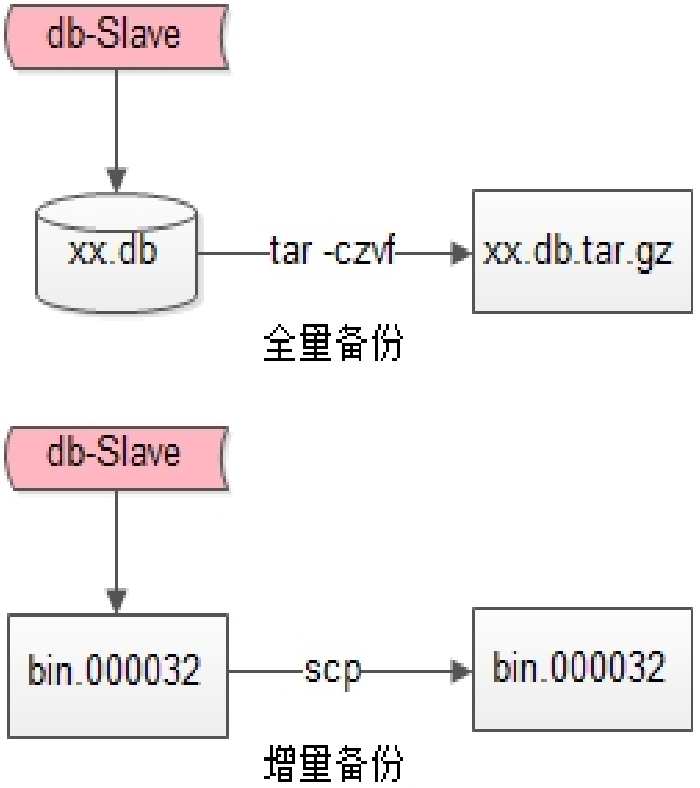
一、线上高可用：防机器故障，数据库故障，磁盘故障

- 主从
- 主主
- **潜在问题**
  - 无法防止无意误删



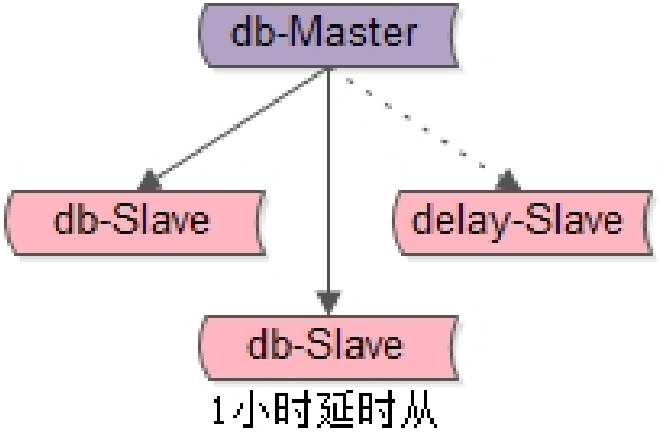
二、全量备份+增量备份：防止误删

- **全量备份**：定期库文件物理备份
- **增量备份**：定期binlog物理备份
- 如果误删，**如何恢复?**
- **潜在问题**
  - 恢复周期较长



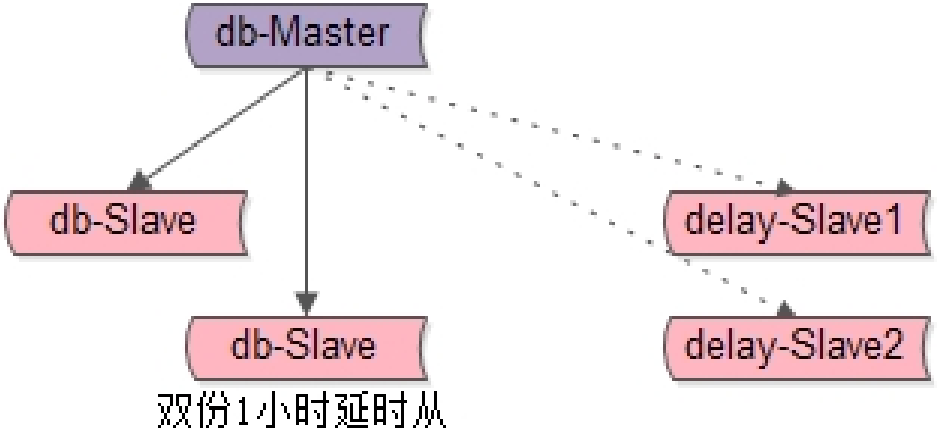
三、一小时延时从库：快速恢复

- 一小时延时从库
- 如果误删，**如何恢复?**
- **潜在问题**
  - 万一延时从刚连上，误删了呢?



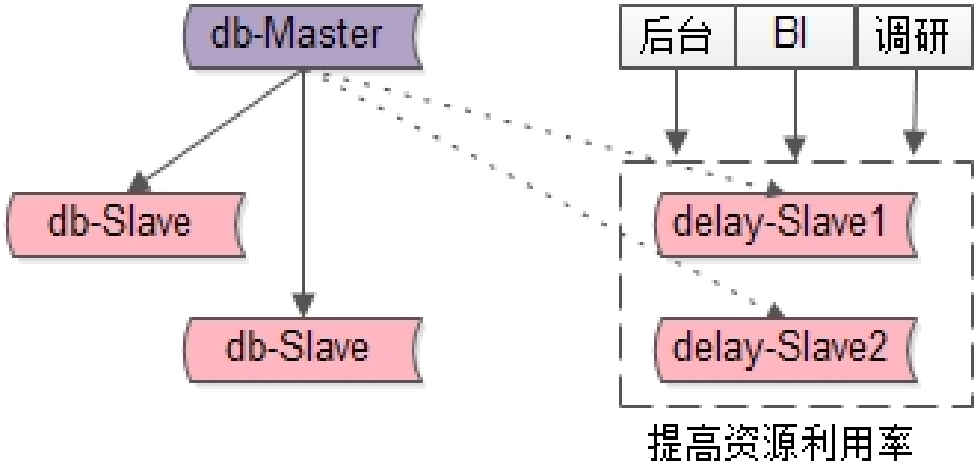
四、双一小时延时从库：无时间死角

- 双一小时延时从库
- 如果误删，**如何恢复?**
- **潜在问题**
  - 资源利用率较低



五、提高延时从库利用效率

- 允许延时的**只读**场景使用延时从
- **潜在问题**
  - 1个小时故障都没发现怎么办?
  - 云故障所有备份都丢了怎么办?
  - 内部恶意怎么办?



五、确保万无一失

- **个小时故障都没发现怎么办?**
  - 监控完善（一个小时数据全没了都没发现？太业余了吧？）
- **云故障所有备份都丢了怎么办?**
  - 异地备份（可以把数据拷贝到多个机房，或者内网备份机器）
- **内部恶意怎么办?**
  - 权限隔离（不能一个人干所有事：删实时库，删延时库，删增量+全量，删异地，删内网）

强调一点：**定期演练**

没有演练的预案 = 没有预案

删库的恢复，是技术难题吗？

如果不是，那为何，一而再再而三的发生？

重视，比怎么做更重要！

不要帅锅给实习生，技术负责人/运维负责人是第一责任人！

总结

- **快狗打车，数据安全实践：**
  - 线上高可用
  - 定期全量+增量备份：防止误删
  - 一小时延时从：加速恢复
  - 双一小时延时从：无时间死角
  - 只读场景使用延时从：提高利用率
  - 完善监控：及时发现
  - 异地备份（多机房，内网）：防止云故障
  - 权限隔离：避免内部恶意

- **什么事情，应该作为重点？**
  - “最高频，最耗时，效率提升最大”的事情
  - “一旦发生，后果无法接受”的事情

- **强调**：定期演练，没有演练的预案 = 没有预案

- **最重要的**：重视，一把手为结果负责！

THANKS