**五邑大学大作业设计报告**



**课程名称：数据安全技术**

|  |  |
| --- | --- |
| **姓名：** | **陈子龙** |
| **学号：** | **3116003896** |
| **院系：** | **智能制造学部** |
| **专业：** | **信息安全** |
| **指导老师：** | **温强** |
| **题目：** | **数据机房设计方案** |

**GitHub：**

**https://github.com/Longoing/study/tree/Longoing-patch-1**

要求：

数据机房背景（XXX电视台新媒体机房），需要考虑数据存储安全性、稳定性和可用性。内容包括数据存储架构设计、磁盘规格选择、Raid存储阵列（文字说明使用哪种Raid及该基于什么原因）、任意一种数据存储技术（例如SAN）、数据备份方案。

背景：

YD电视台新媒体机房，占地面积300平方米，可容纳50个机柜架构和存储介质库，配备计算机设备,服务器，网络设备；基础环境：供电系统，制冷系统，机柜系统，机柜系统，消防系统，监控系统等物理设施。

YD电视台业务广泛，需要存储的数据繁杂，需要考虑数据存储安全性、稳定性和可用性。运用现有知识，搭建数据存储中心，建立共享灾备中心。

## SAN存储架构设计

开放系统的存储分为：内置存储和外挂存储

外挂存储根据连接的方式分为：直连式存储（Direct-Attached Storage，简称DAS）和网络化存储（Fabric-Attached Storage，简称FAS）；网络化存储根据传输协议又分为：网络接入存储（Network-Attached Storage，简称NAS）和存储区域网络（Storage Area Network，简称SAN）

SAN提供了一种与现有LAN连接的简易方法，并且通过同一物理通道支持广泛使用的SCSI和IP协议。SAN不受现今主流的、基于SCSI存储结构的布局限制。特别重要的是，随着存储容量的爆炸性增长，SAN允许企业独立地增加它们的存储容量。SAN的结构允许任何服务器连接到任何存储阵列，这样不管数据置放在那里，服务器都可直接存取所需的数据。因为采用了光纤接口，SAN还具有更高的带宽。

SAN真正的综合了DAS和NAS两种存储解决方案的优势，利用SAN解决方案，你还可以实现存储的集中管理，从而能够充分利用那些处于空闲状态的空间。可以将服务器配置为没有内部存储空间的服务器，要求所有的系统都直接从SAN引导。这也是一种即插即用技术。

存储区域网络（Storage Area Network，简称[SAN](https://baike.baidu.com/item/SAN" \t "https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%8C%BA%E5%9F%9F%E7%BD%91%E7%BB%9C/_blank)）采用网状通道（Fibre Channel ，简称[FC](https://baike.baidu.com/item/FC" \t "https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%8C%BA%E5%9F%9F%E7%BD%91%E7%BB%9C/_blank)，区别与Fiber Channel光纤通道）技术，通过FC交换机连接[存储阵列](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E9%98%B5%E5%88%97/1496275" \t "https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%8C%BA%E5%9F%9F%E7%BD%91%E7%BB%9C/_blank)和服务器[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151" \t "https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%8C%BA%E5%9F%9F%E7%BD%91%E7%BB%9C/_blank)，FC-SAN。建立专用于[数据存储](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AD%98%E5%82%A8/9827490" \t "https://baike.baidu.com/item/%E5%AD%98%E5%82%A8%E5%8C%BA%E5%9F%9F%E7%BD%91%E7%BB%9C/_blank)的区域网络，一方面可以传输大块数据，另一方面可以实现远距离传输。

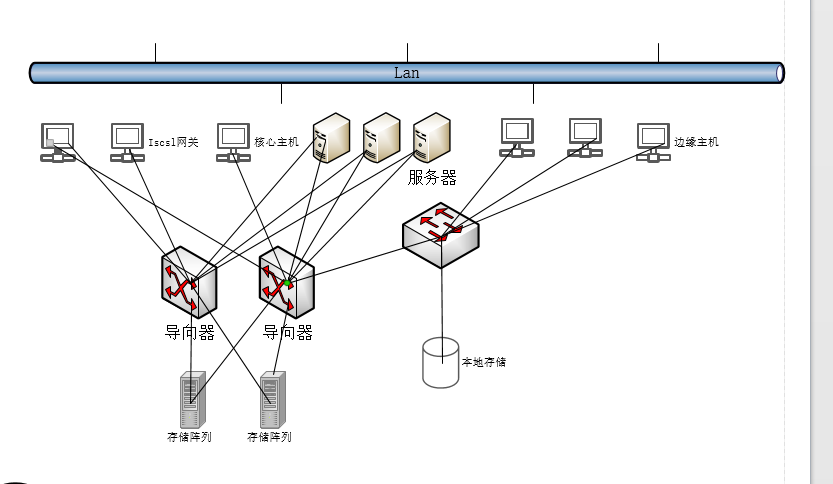
### 初步SAN存储设计

在机房核心区部署核心导向器，SAN网络架构采用“核心-边缘结构”（core-edge）利用Firbre Channel protocol（光纤通道协议）通过FC交换机建立与服务器和存储设备的直接连接；SAN组网采用“双交换”连接，确保扩展性。FC采用双Fabric架构

核心主机与存储系统间采用scsi协议

优点：核心-边缘结构一般由一到两台核心交换机与多台接入交换机所组成，每台接入交换机，都与核心交换机进行互联，而服务器和存储设备则需要按照不同的性能、用途和重要性而接入不同的交换机。这种设计允许路径上不同级别服务器进行连接，很好的满足了不同应用的带宽需求，而且在成本、扩展性与性能

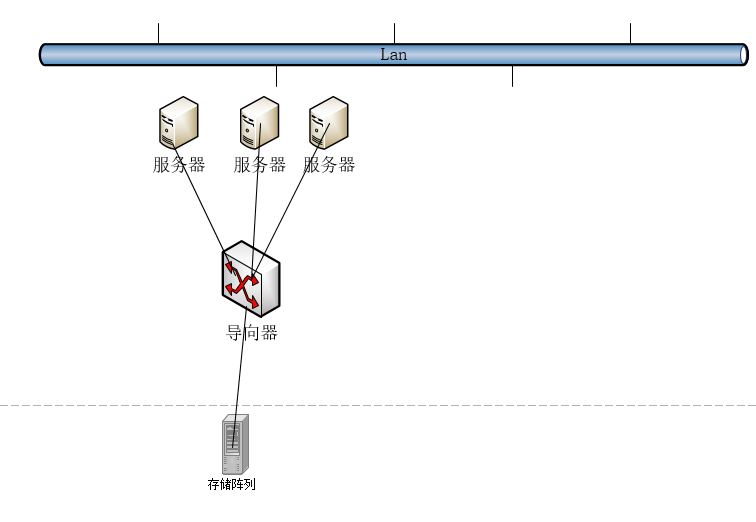
之间得到最大的平衡。



### 备份SAN存储设计

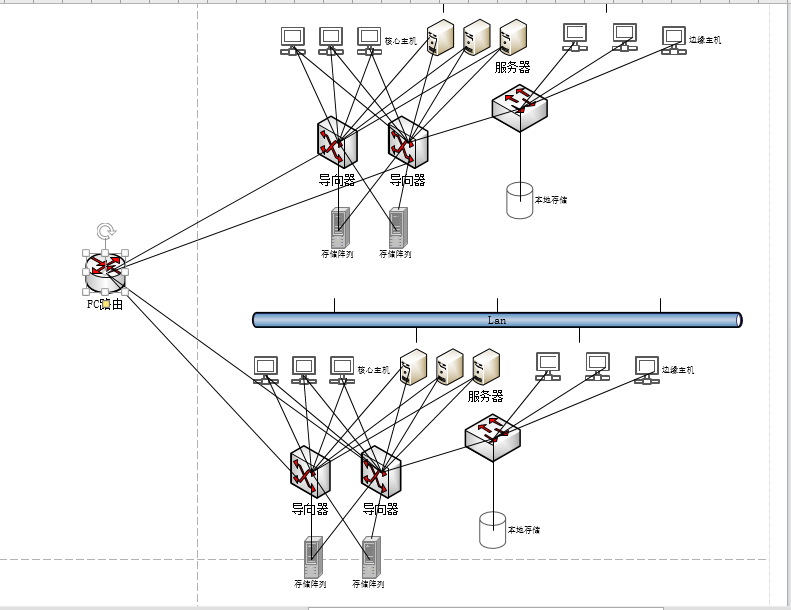
在机房备份区搭建单独的SAN存储区域网络，建立单独的fabric，连接到备份的存储库

优点：独立的备份fabric，避免与直接存储数据的影响，保障了数据备份的正确，安全性



### 机房不同区域资源共享设计

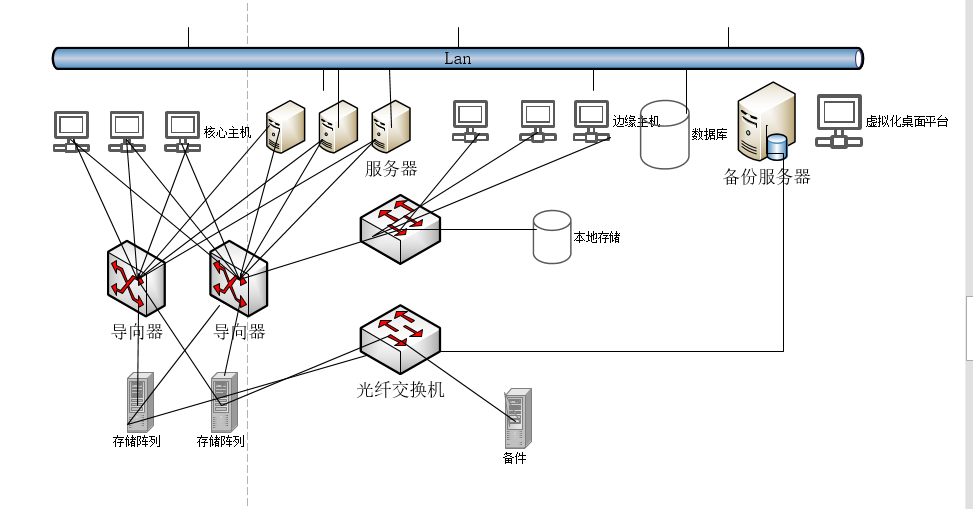
在机房内的不同区域内需要部署资源共享，在不同区域间通过FC Router建立连接，联通fabric，使区域的主机和存储设备进行访问，实现资源共享

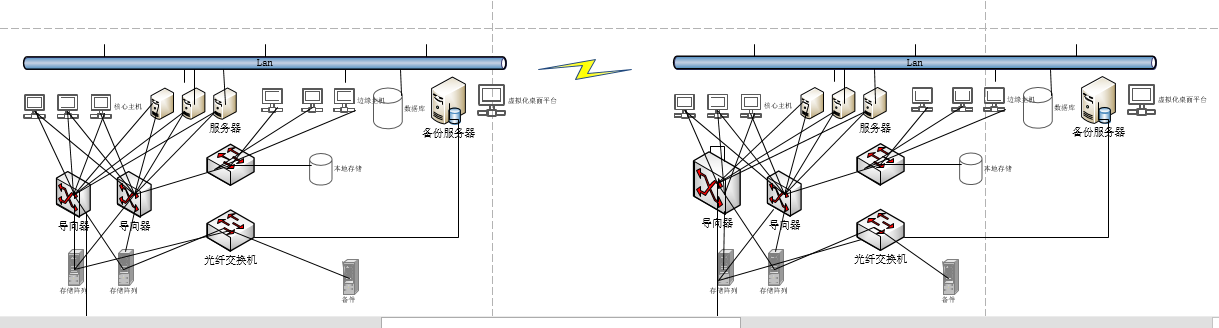


### 数据灾备规划设计

（1）本地机房内采用“虚拟云桌面备份”的方式。对虚拟化桌面平台进行虚拟桌面备份。通过虚拟缓存技术，提升整体访问性能通过虚拟存储之间的复制技术，并且通过虚拟存储之间的复制技术实现远程灾备；

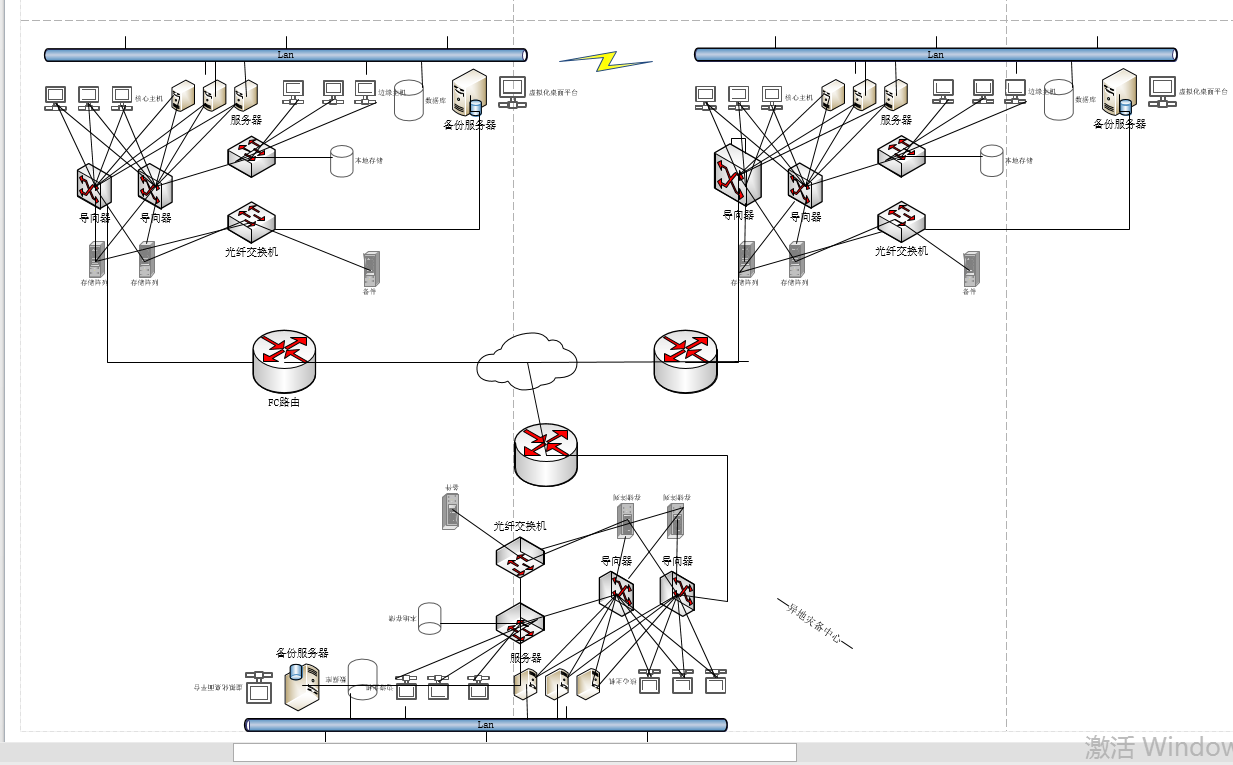
使用虚拟桌面创建数据，数据类型不一，个人操作习惯，时间，文件类型不同。每日查看目录，进行数据备份。



1. 本地灾备中心建设，在本地另一机房建立灾备机房，将服务器实时接管到灾备中心做到数据的实时复制
2. 搭建两地三中心灾备，为排除不可抗力因素，导致本地机房无法使用，需要在异地建立灾备中心

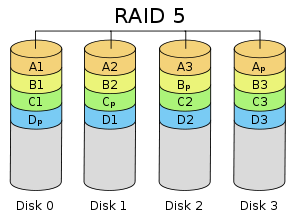
在本地灾备中心的基础上，在异地建立灾备中心，通过路由通信实现数据同步

优点：两地三中心架构是灾备中心和双活动中心的结合体，机油冗余系统架构，也有异地灾备效果



### Raid存储阵列设计

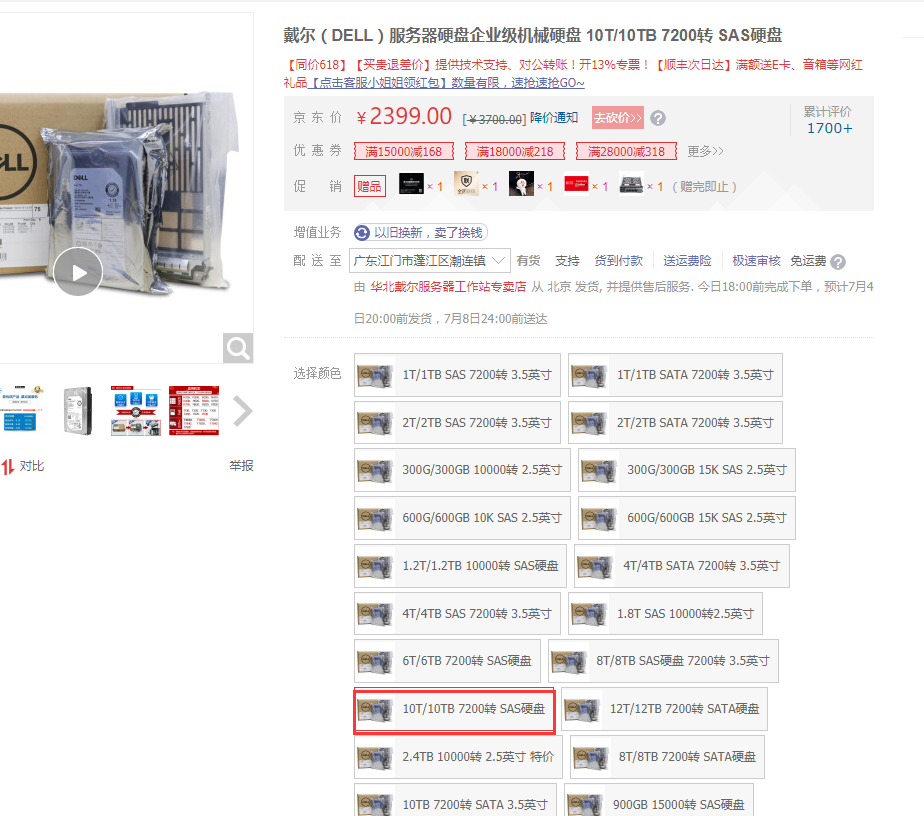
Raid存储阵列选择raid5等级，RAID 5 是一种存储性能、[数据安全](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AE%89%E5%85%A8/3204964" \t "https://baike.baidu.com/item/_blank)和存储成本兼顾的存储解决方案。 RAID 5可以理解为是RAID 0和RAID 1的折中方案。RAID 5可以为系统提供[数据安全](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AE%89%E5%85%A8/3204964" \t "https://baike.baidu.com/item/_blank)保障，但保障程度要比Mirror低而磁盘空间利用率要比Mirror高，，RAID 5的磁盘空间利用率要比[RAID 1](https://baike.baidu.com/item/RAID 1" \t "https://baike.baidu.com/item/_blank)高，存储成本相对较低，是目前运用较多的一种解决方案。



Raid5把数据和相对应的[奇偶校验](https://www.baidu.com/s?wd=%E5%A5%87%E5%81%B6%E6%A0%A1%E9%AA%8C&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)信息存储到组成RAID5的各个磁盘上，并且奇偶校验信息和相对应的数据分别存储于不同的磁盘上。当RAID5的一个磁盘数据发生损坏后，利用剩下的数据和相应的奇偶校验信息去恢复被损坏的数据

优点：容错性：奇偶校验冗余类型，读性能高，可用容量：（n-1）\*n的总磁盘容量（n为磁盘数）

磁盘规格

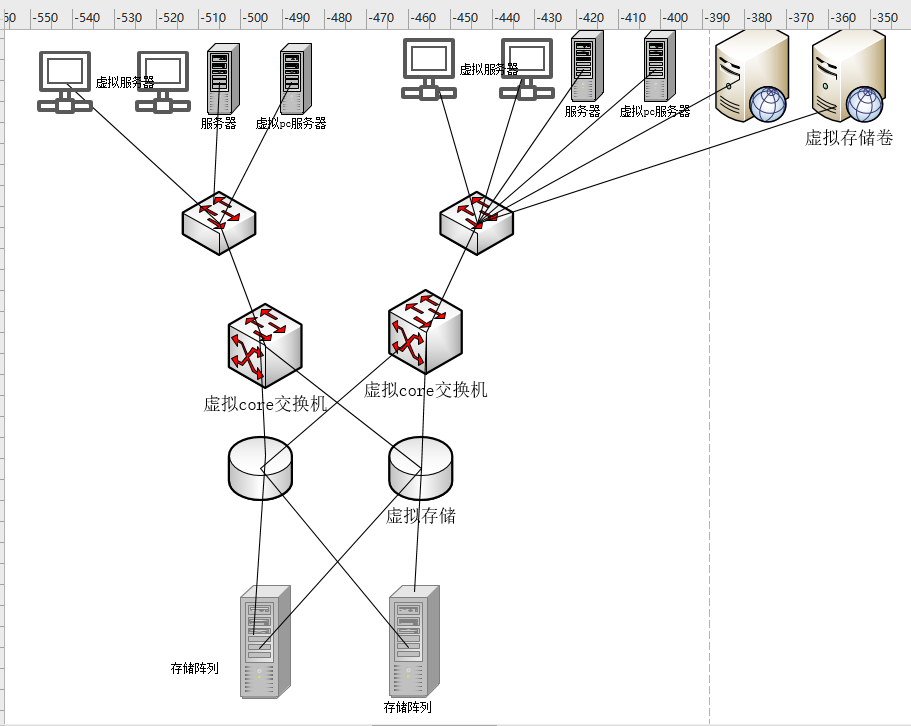




[SAS接口](https://www.baidu.com/s?wd=SAS%E6%8E%A5%E5%8F%A3&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)将延续[SCSI硬盘](https://www.baidu.com/s?wd=SCSI%E7%A1%AC%E7%9B%98&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)上诸如命令排序之类的功能，这个功能让[硬盘控制器](https://www.baidu.com/s?wd=%E7%A1%AC%E7%9B%98%E6%8E%A7%E5%88%B6%E5%99%A8&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)能够按照最有效率的顺序执行命令，从而提高性能。而相同的功能若要在[SATA硬盘](https://www.baidu.com/s?wd=SATA%E7%A1%AC%E7%9B%98&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)中实现的话，在很大程度上将依赖于处理器的计算。SAS是一个完全的双向系统，而SATA则继承了IDE的特性，是半双向通信的系统。因此SAS的数据吞吐量可以是SATA系统的两倍，它采用串行技术实现更高的传输速度，缩短连接线。

### 存储架构规划设计

主机房部署物理磁盘阵列，物理存储的上层通过虚拟存储设备，建立虚拟存储池。物理主机，虚拟主机通过IP-SAN网络和FC-SAN网络访问虚拟存储池中的虚拟存储卷。通过存储虚拟化整合，可以提升数据的安全性，虚拟化技术具备众多的存储服务功能，能够通过多种手段提升存储数据的可恢复性和存储设备故障的可恢复性



### 数据库规划

HBase分布式数据库，HBase – Hadoop Database，是一个高[可靠](https://baike.baidu.com/item/%E5%8F%AF%E9%9D%A0" \t "https://baike.baidu.com/item/HBase/_blank)性、高性能、面向列、可伸缩的[分布式存储系统](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F%E5%AD%98%E5%82%A8%E7%B3%BB%E7%BB%9F" \t "https://baike.baidu.com/item/HBase/_blank)，利用HBase技术可在廉价PC Server上搭建起大规模[结构](https://baike.baidu.com/item/%E7%BB%93%E6%9E%84" \t "https://baike.baidu.com/item/HBase/_blank)化[存储](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8" \t "https://baike.baidu.com/item/HBase/_blank)集群。

DDBMS分布式数据库管理系统

### IMG_256

### 心得体会

经过本课程学习，学习到很多数据安全方面的知识，raid存储阵列，数据存储技术，数据备份方案，体验了一次靶机数据窃取渗透的过程，动手进行信息收集，漏洞分析，sql注入练习等；大作业选择做了数据机房的设计方案，自己参考资料设计SAN“核心-边缘”数据存储架构，加入综合数据灾备方案，用到了书本的“虚拟云桌面备份”和“两地三中心”和本地灾备中心等知识，还有许多不懂得知识通过学习博客的资源得以掌握。总的来说，本次大作业所用的知识还是比较多，数据机房设计或多或少存在一定的缺陷，在之后的学习过程中要进行完善。最后，感谢老师的教导。

参考文献：《数据安全与灾备管理》清华大学出版社

参考文章：<https://blog.csdn.net/shipeng1022/article/details/72862367>

https://www.docin.com/p-638138218.html