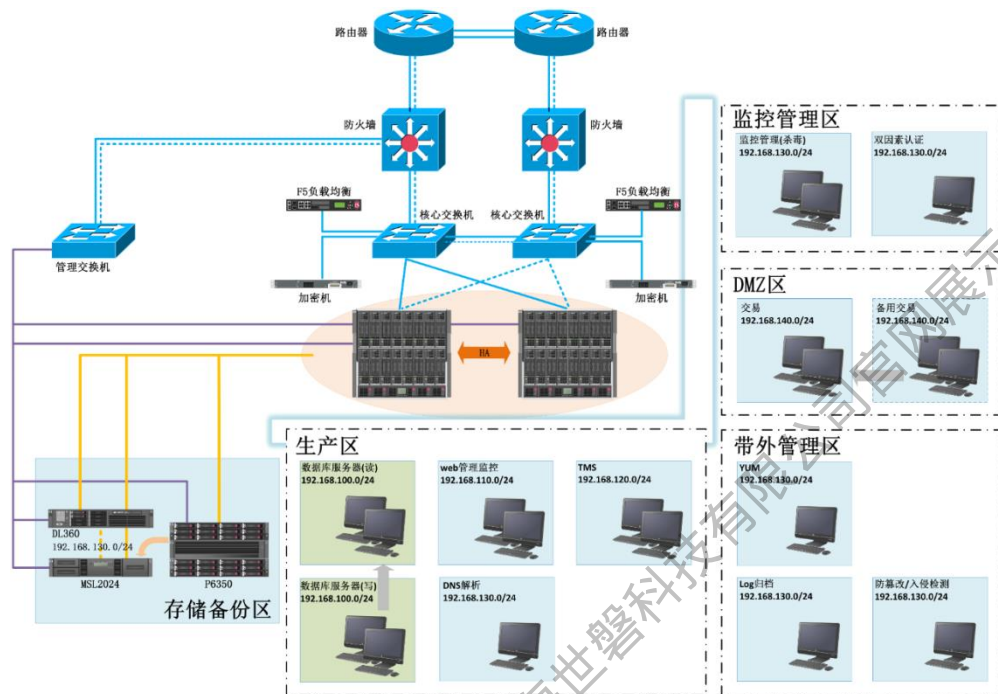


# 案例介绍 – 某零售商POS建设项目



项目介绍：  
某零售商为了建设新一代门店业务支持系统，提高IT运维水平和安全性，通过该项目能够实现从物理机到虚拟机的转换，部署开源系统和运维辅助软件。

- 1，以刀片服务器为核心的vsphere虚拟化基础架构
- 2，分隔不同区域系统，实现系统安全隔离管理
- 3，集中式备份DP，实现数据保护

项目时间及里程碑：

- 1，2016-02 项目Kick-Off
- 2，2016-03至2016-03 需求分析
- 3，2016-03至2016-04 设计和报告
- 4，2016-04至2016-05实施和部署
- 5，2016-05至2016-07 业务上线

# 案例介绍-某零售商POS建设项目



图1 OSSEC防篡改软件:

OSSEC是一款开源的多平台的入侵检测系统，可以运行于Windows, Linux, OpenBSD/FreeBSD, 以及 MacOS等操作系统中。包括了日志分析，全面检测，root-kit检测。采用客户端/服务器模式来运行。客户机通过客户端程序将数据发回到服务器端进行分析。

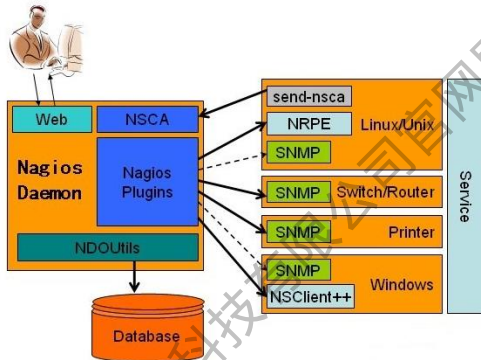


图2 Nagios监控软件:

Nagios是一款开源的免费网络监视工具，能有效监控Windows、Linux和Unix的主机状态，交换机路由器等网络设备，打印机等。在系统或服务状态异常时发出邮件或短信报警第一时间通知网站运维人员，在状态恢复后发出正常的邮件或短信通知。

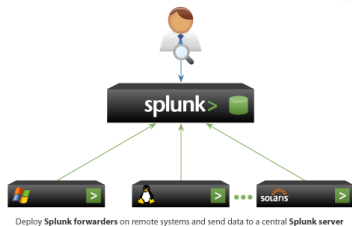


图3 splunk日志收集分析

Splunk 是机器数据的引擎。使用 Splunk 可收集、索引和利用所有应用程序、服务器和设备生成的快速移动型计算机数据。