掌上办公服务器架构方案

沈阳普日软件技术有限公司

2017

目录

摘要

移动办公之风席卷而来，在这个移动信息的时代里，没有移动办公在手的医院，就显得很落后了。

移动办公实现完美的无缝式沟通与协作，顺理成章的成为了中小企业在激烈的市场竞争中力争上游的保障。

由于移动办公要经过开放的无线公网接入医院内部网以及信息在空中无线传播，因此移动办公使用和推广的首要问题就是移动办公的安全问题。

对于移动办公的安全问题，还是很多企业首先要关注的，因为保障企业内部数据安全有时比把握一次绝好的商机更为重要。

移动办公平台强大的扩展性和兼容性，可为用户提供随时随地的在线会议讨论、实时协作交流、数据留存等功能，降低了传统电话、会议、交通以及相关设备的维护成本等开支，而良好的易用性，为企业节省了庞大的培训费用，真正的实现了“低投入，高回报”。

移动办公平台采用灵活的部署方式，确保移动办公平台中涉及的所有数据安全，同时，移动安全办公在数据完整性、信息的保密性、网络的安全性以及信息处理的每一个步骤均作了周密的设计。

1. 系统架构

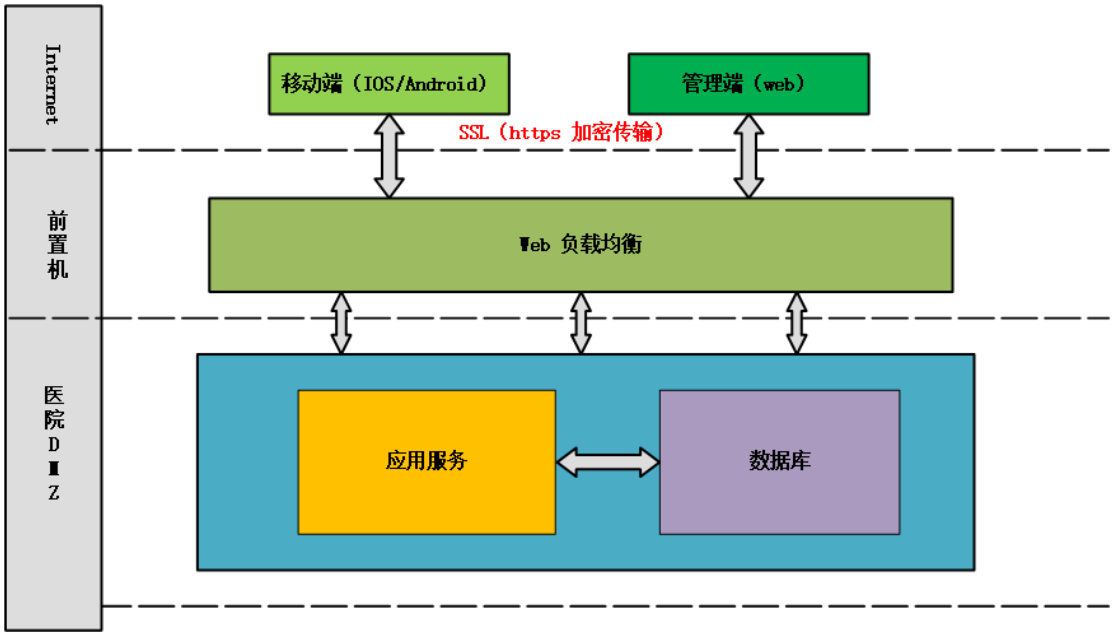
1.1 逻辑架构

我们运用“模块化设计”理念，将系统分为若干个功能子系统，再把每个功能子系统按业务性质具体划分若干个功能模块。

1.2 软件架构

参考 MVC 软件设计模式，采用数据、逻辑、表现分离架构核心应用，在保证软件健壮性、重用性和结构化的同时，通过封装和分离部署，更好的保护数据业务逻辑。

1.3 平台架构



客户端和医院服务端通过 HTTPS 协议进行数据交互，为了保障数据安全性，采用 SSL 安全套接加密技术，防止网络监听和数据窃取。为保证业务不间断运行，采用高可用机制，在发生特殊情况，其中如有一台服务器宕机或故障，服务可自动故障转移，因此在客户端和服务端间，设置了负载均衡层来分发并发请求。 负载均衡层链接着包含实际业务逻辑的应用服务器。

2. 系统安全

2.1 数据完整性

系统在数据的传输、存储、处理过程过程中，使用事务传输机制对数据完整性进行保证，使用数据质量管理工具对数据完整性进行校验，在监测到完整性错误时进行告警，并采用必要的恢复措施。

2.2 数据保密性

系统的身份鉴别信息、敏感的系统管理数据和敏感的业务数据在传输、存储、处理过程中，应进行加密或使用专用的协议或安全通信协议，负载均衡到应用系统和数据库系统之间设置访问控制，支持由授权主体设置对客体访问和操作的权限；支持特权用户的权限分离，权限分离采用最小授权原则，授予用户完成任务所需的最小权限；禁止默认用户的访问权限，重命名系统默认账户，并修改这些账户的默认口令；及时清除多余的、过期的账户，避免共享账户的存在；对重要信息资源和所有访问重要信息资源的用户设置敏感标记，统一强制设置严格的安全策略控制用户对有敏感标记重要信息资源的操作。

2.3 高可用

数据库拥有两个物理节点进行主从热备，主节点发生故障，切换至备节点。还可以通过数据同步方式，构建异地灾备数据库，双重保证数据的安全，让客户可以更多地专注业务实现，在基础设施

层面采用高可用、备份与恢复等机制保障系统安全可靠运行，在应用层面采用负载均衡、集群方式可扩展性。

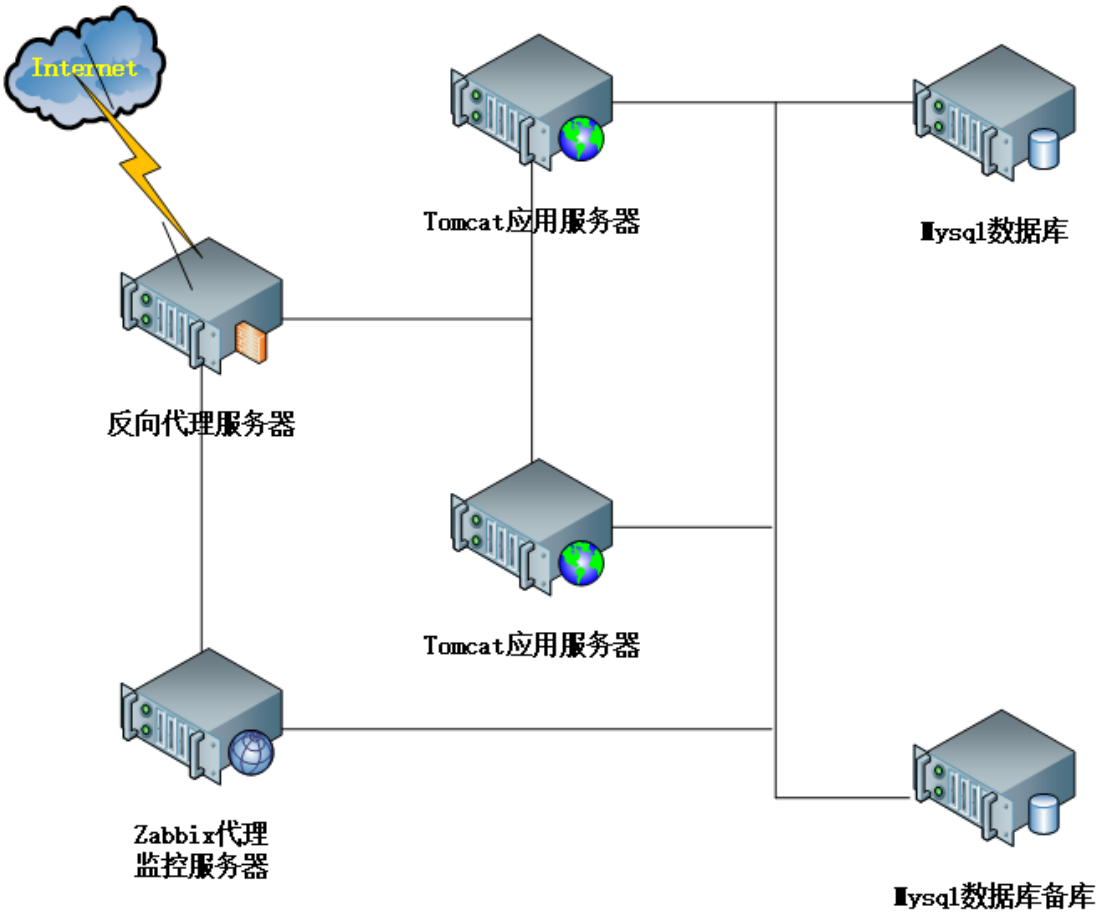
3. 硬件及软件环境要求

3.1 服务器配置要求

硬件及软件	
服务器数量	2
硬件配置	处理器：2 颗物理 CPU Intel Xeon E5645（志强六核，2.4 主频，12 线程） 内存：大于 32G（16G*2 或 8G*4，DDR3) 硬盘：大于 1TB
应用服务	操作系统：Ubuntu 16.04 LTS 64 位 运行环境：tomcat_7.0.82、jdk1.8.0、nginx1.13 数据库：MySQL 5.7.14

3.2 服务器拓扑图

掌上办公服务器拓扑图如下所示：



按照统一要求，与信息内网之间使用防火墙等逻辑访问控制设备进行访问控制，对于其他网络使用信息安全网络隔离装置进行访问控制；支持粒度至端口级的会话状态控制，支持对 HTTPS、TELNET 等应用层协议命令级的控制，支持对最大流量数和网络连接数的控制。