

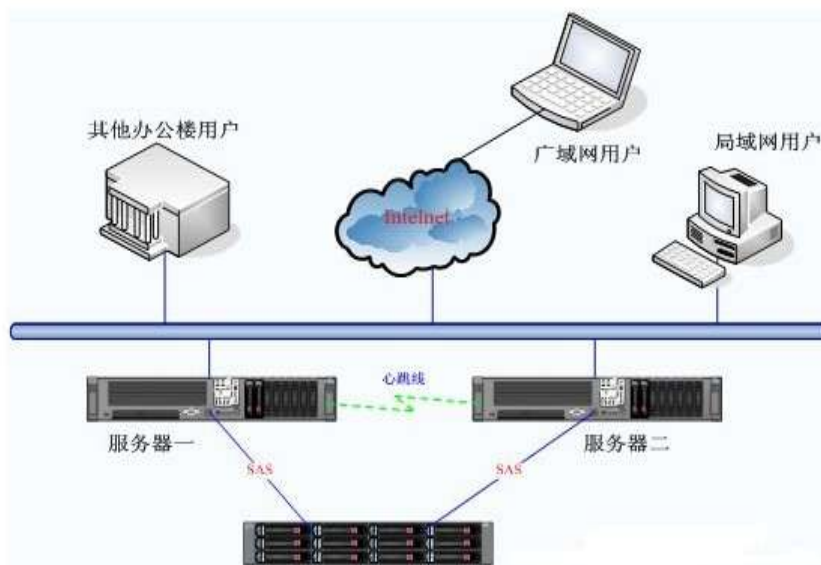
TurboMail 双机热备方案

双机热备针对的是服务器的临时故障所做的一种备份技术，通过双机热备，来避免长时间的服务中断，保证系统长期、可靠的服务。企业为了避免服务器故障产生数据丢失等现象，旧的技术是利用 RAID 技术和数据备份技术，但是数据备份只能解决系统出现问题后的恢复。无论是硬件还是软件问题，都可能会造成邮件服务的中断，而 RAID 及数据备份技术恰恰就不能解决避免服务中断的问题。

发生宕机事故后到恢复服务器运行，再轻微的问题或者强悍的技术支持，服务器也会中断一段时间，可能会造成邮件的丢失，对于一些需要不间断在线的用户，丢失邮件就等于丢失金钱，损失可大可小，这类用户是很难忍受服务中断的。因此，就需要通过双机热备，来避免服务中断，保证系统长期、可靠的服务。

双机热备模式

1) 基于存储阵列的双机热备

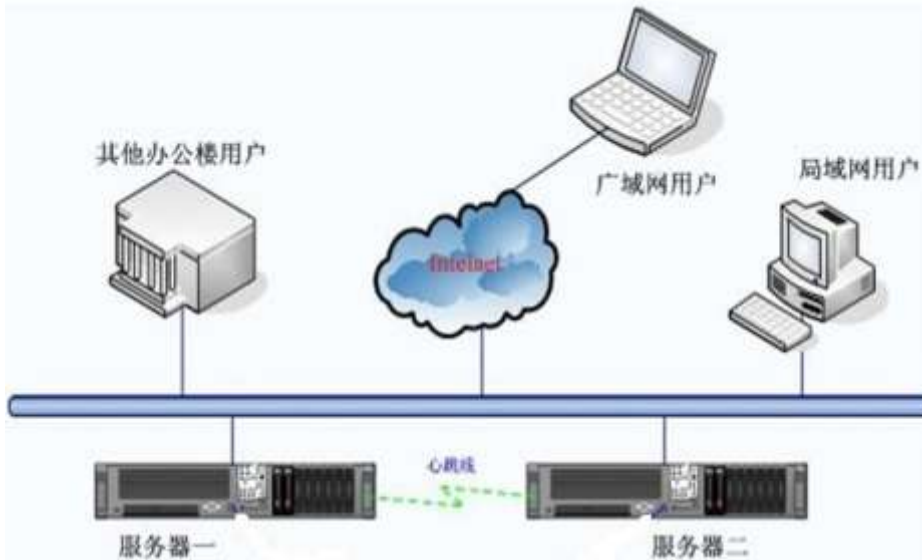


基于存储共享的双机热备是双机热备中最标准的方案。对于这种方式，采用两台服务器（邮件系统同时运行在两台服务器上），使用共享的存储设备磁盘阵列（邮件系统的数据都存放在该磁盘阵列中）。两台服务器可以采用互备、主从、并行等不同的方式。在工作过程中，两台服务器将以一个虚拟的 IP 地址对外提供服务，依工作方式的不同，将服务请求发送给其中一台服务器承担。同时，服务器通过心跳线（目前往往采用建立私有网络的方式）侦测另一台服务器的工作状况。当一台服务器出现故障时，另一台服务器根据心跳侦测的情况做出判断，并进行切换，接管服务。对于用户而言，这一过程是全自动的，在很短时间内完成，从而对业务不会造成影响。由于使用共享的存储设备，因此两台服务器使用的实际上是一样的数据，由双机或集群软件对其进行管理。

优点：对于共享方式，数据库放在共享的存储设备上。当一台服务器提供服务时，直接在存储设备上读写。而当系统切换后，另一台服务器也同样读取该存储设备上的数据。它可以在无人值守的情况下提供快速的切换，保证不会有数据丢失现象。

缺点：增加了存储设备的投资，对于有实力的企业，可优先考虑该方式。

2) 基于软件管理的双机热备



纯软件的方式，通过镜像软件，将数据可以实时复制到另一台服务器上，这样同样的数据就在两台服务器上各存在一份，如果一台服务器出现故障，可以及时切换到另一台服务器。

优点：

- ① 节约投资。
- ② 不受距离的限制：两台服务器不需受 SCSI 电缆的长度限制（光纤通道的磁盘阵列也不受距离限制，但投资会大得多）。这样，可以更灵活地部署服务器，包括通过物理位置的距离来提高安全性。

缺点：

- ① 可靠性相对较差，两服务器间的数据实时复制是一个比较脆弱的环节。
- ② 一旦某台服务器出现中断，恢复后还要进行比较复杂的数据同步恢复。并且，这个时段系统处于无保护状态。
- ③ 没有事务机制，由于其复制是在文件和磁盘层进行的，复制是否成功不会影响数据库事务操作，因此有出现数据不完整变化的情况，这个存在着相当的风险。

软件存在维护和未知 BUG 等因素，所以我们并不建议客户采取这种方式进行双机热备。目前 TurboMail 的客户中需要采用双机热备的使用者绝大多数都是利用“磁盘阵列”这种基于共享存储设备的方式，而且截止现在，尚未发现报修或者需要维护的情况。

TurboMail 双机热备方案使您能够在失败切换的基础上，或者在可伸缩的基础上执行应用程序。失败切换 和可伸缩应用程序也可以同时在一群集上运行。一般来说，失败切换应用

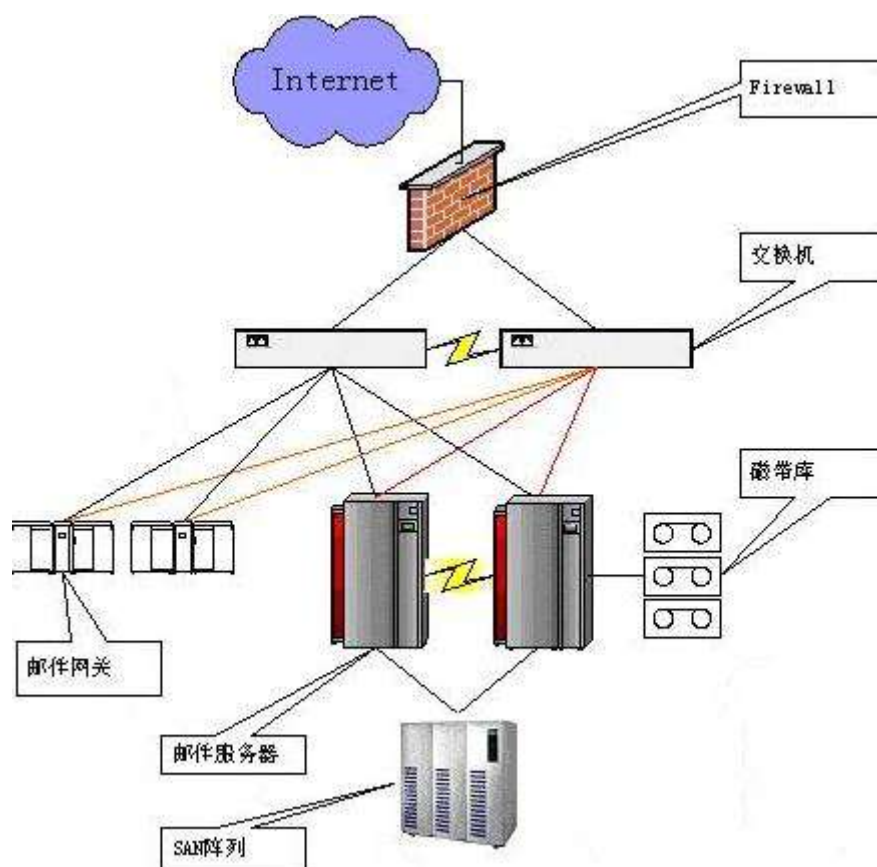
程序提供高可用性（冗余），而可伸缩应用程序除了具有高可用性之外，还具有更高的性能。单一群集既可以支持失败切换应用程序，也可以支持可伸缩应用程序。

系统失败切换

失败切换就是群集自动将应用程序从一个故障主节点重新定位到指定的辅助节点的进程。有了失败切换功能，Cluster 就具备了高可用性。当失败切换发生时，客户可能会看到一个短暂的服务中断，并可能需要在失败切换结束后重新连接。然而，客户并不需要知道哪一个物理服务器向他们提供应用程序和数据。

系统可伸缩性

当失败切换忙于冗余时，可伸缩性提供持续的响应时间或吞吐量，而不用去关心负荷。可伸缩应用程序利用群集中的多个节点来同时运行一个应用程序，从而增强了性能。在可伸缩配置中，群集中的每一个节点都可以提供数据和处理客户请求。配置两台主机，每一台主机都能够独自支撑系统所有用户的正常访问。两台主机接入一台可支持两台主机同时连接的磁盘阵列设备。系统通过 Cluster 软件进行管理。两台主机均安装相同的软件，其中一台作为主节点，系统服务正常运行。另外一台作为从节点，系统服务处于停止状态。如果主节点发生故障，Cluster 软件会及时发现并将从节点启动，保持用户服务不中断。另外如果采用异地容灾方案，需要另外配置一台服务器作为远程容灾服务器即可。



双机实施案例

客户需求：

- ◆ 支持 POP3、IMAP4 和 HTTP 等邮件访问协议和方式，支持 SSL 等安全访问。
- ◆ 能够进行用户邮件存储空间限额设置，能够独立设置分配域空间大小、每个邮箱大小、每个用户邮件附件大小。
- ◆ 拒收超过存储空间的邮件，用户不会因邮件空间原因造成无法访问邮件帐户。
- ◆ 系统管理员可以根据 IP、发信人等过滤垃圾邮件。
- ◆ 支持简单邮件传输协议中继（SMTP Relay）认证（ESMTP）。
- ◆ SPECmail 2001 \geq 350 msgs/min。
- ◆ 支持流量监控和运行监控。

其它需求：

- ◆ 高可靠性：系统稳定可靠，能够提供 7X24 X365 不间断服务。
- ◆ 高安全性：系统要求具有较强的防垃圾邮件、防病毒、防黑客攻击能力。
- ◆ 多域名支持：系统应提供无数量限制的多域名支持。（企业邮箱应用系统）
- ◆ 手机短信支持：系统提供邮件短信到达提醒、短信回复邮件等支持。在发送邮件的同时，可以同时发送短消息，将邮件主题、发信人、发信时间、正文摘要组成一个 SMS 通知到用户手机上。

系统容量需求：

- ◆ 电子邮件双机系统最多可支持 10 万用户。

功能扩展需求：

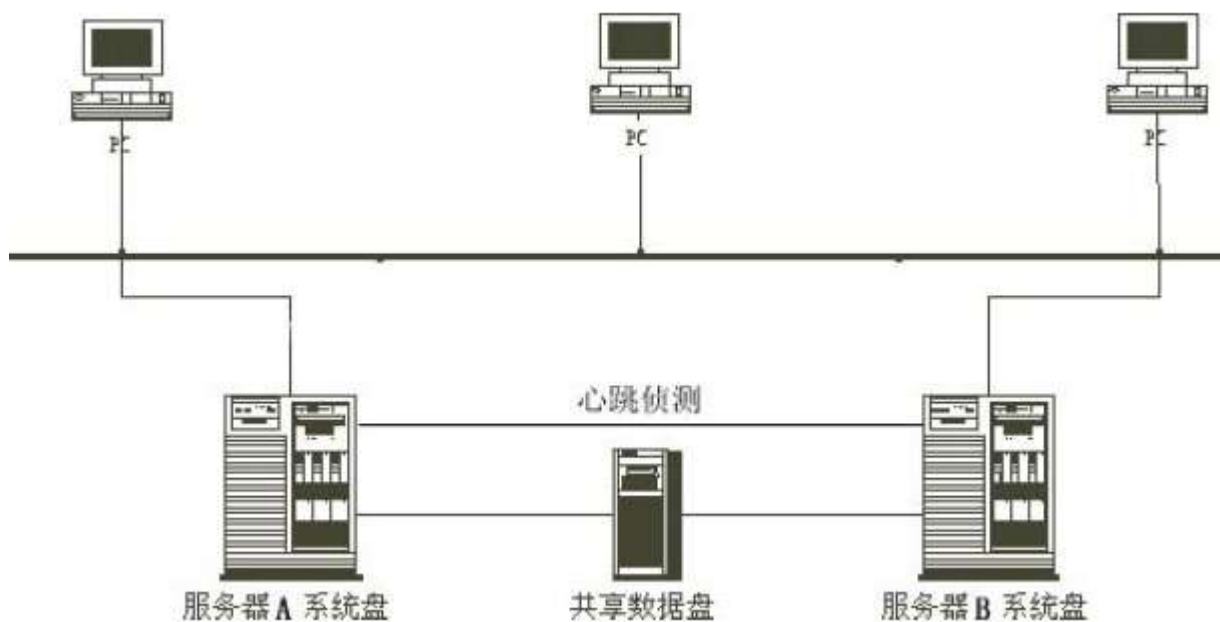
根据客户需求，系统在提供基本的邮件系统功能的基础之上，随着业务的发展需要，还可以实现多种功能的扩展：电话/传真邮件：用户可以通过电话/传实现邮件的收发。

- ◆ Mail to SMS：用户可以邮件到达通知。
- ◆ Mail to WinCE：用户可以通过 WinCE 掌上电脑收发邮件。
- ◆ Mail to BP/PDA：用户邮件（到达通知）可以发送到 BP 或 PDA。

基于以上需求分析，拓波建议以双邮件服务器系统构成高可用 HA 系统，从而满足系统的大容量、高性能、高可靠性以及系统平台与功能的扩展性。以二台服务器为基础，二台服务器共同工作，当一台服务器的系统出现故障时，另一台服务器可确保系统正常运行，从而将系统风险降低到最低限度，保障了整个系统的高可靠性、高安全性和高可用性。

双机热备的硬件系统结构：双机系统是由两台服务器和共享存储子系统组成的。

下图是双机热备系统的硬件示意图



- ◆ 每台主机都有自己的系统盘，安装操作系统和应用程序。
- ◆ 每台主机至少安装两块网卡，一块对外工作，另一块相互侦测对方的工作状态。
- ◆ 每台主机都连接在共享磁盘子系统上，共享磁盘子系统通常均为有容错的磁盘阵列。
- ◆ 各种应用所需的数据均储存在磁盘阵列子系统上。

硬件系统基本需求 (Hardware Requirements)

- ◆ 两台相对应的服务器，CPU P4 Xeon 2.8G
- ◆ 服务器内装 DDR 512MB ECC 内存
- ◆ 每台服务器内装两片以太网卡 (Network Card)
- ◆ 服务器内装一组 SCSI 接口或光纤通道 Host 卡 (Ultra 160, Fibre Channel)
- ◆ 一台磁盘阵列 (如 DzStor3000 系列) 内有四个 Ultra 160 or 2 个 Fibre Channel 通道，可接两台服务器 (Dual Host Channel)，一般采用 PowerPC 控制器，背板的传输速度为 320MB/S，单柜的容量在 1.4 个 TB 左右

软件系统基本需求 (Software Requirements)

- ◆ linux 系统
- ◆ 双机控制软件，如 Rose HA, KeeperLife, Cluster 等
- ◆ DataBase 系统如: MySQL3.23
- ◆ 拓波邮件系统软件

切换时机 (Take Over)

- ◆ 系统软件或应用软件造成服务器宕机
- ◆ 服务器没有宕机，但系统软件或应用软件工作不正常
- ◆ SCSI 卡损坏，造成服务器与磁盘阵列无法存取数据
- ◆ 服务器内硬件损坏，造成服务器宕机
- ◆ 服务器不正常关机

双机软件简介

在双机热备系统的工作中，双机软件是必不可少的。一切故障的诊断，服务的切换，硬件的控制都由双机软件来控制实现。同时为了使双机系统对外像一个单主机系统一样，双机软件还可以为双机系统生成系统虚拟 IP 对外工作，客户机通过虚拟 IP 访问双机系统。这样就避免了服务切换后主机 IP 地址改变导致客户机无法连通的问题。并且双机软件还可以控制两台服务器对共享磁盘子系统的访问同一时刻只能有一台主机可以对其访问，避免了同时访问可能造成的数据破坏。双机软件通过侦测网卡或两台服务器之间互连的串口线进行两台主机的状态诊断，一旦工作的主机出现问题，如数据库服务器出现操作系统挂起、死机、网卡坏、硬盘控制器坏等等，双机软件控制备份机接管系统的虚拟 IP 和共享磁盘子系统的控制权并启动备份机上的服务对外工作，保证系统的实时性和可靠性。