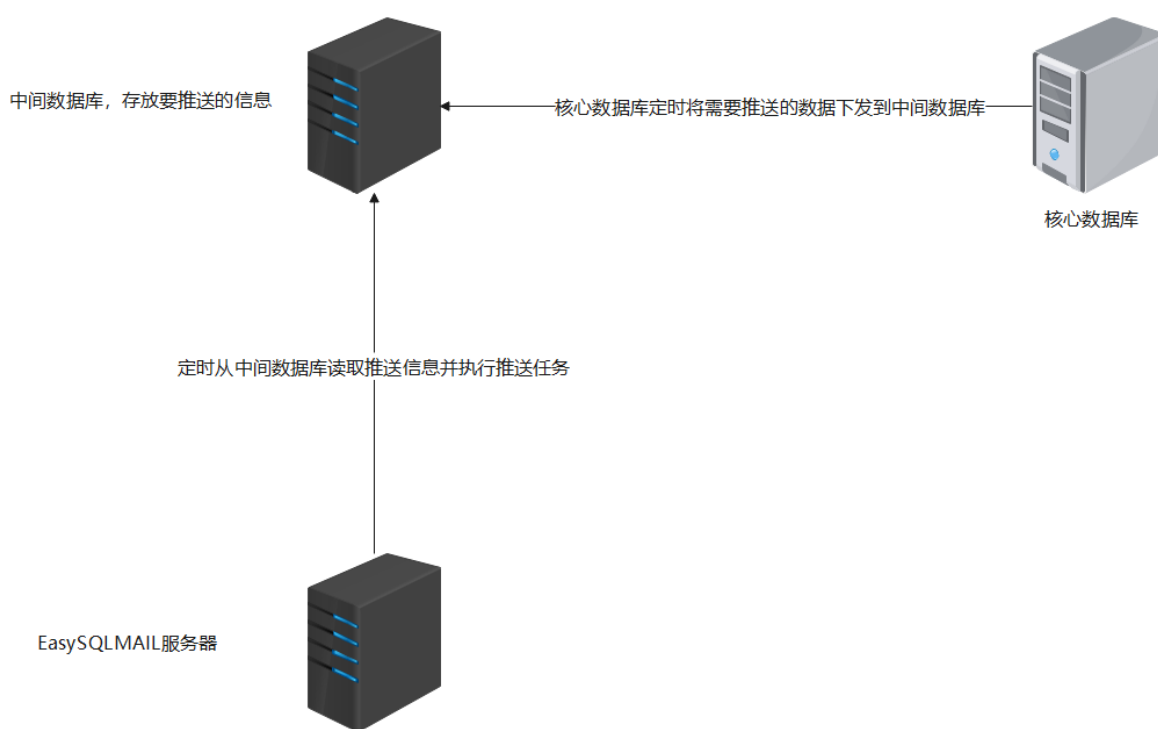


1 更安全地使用 EasySQLMAIL

1.1 数据源安全

EasySQLMAIL 中查询数据时需要连接数据源进行操作。为保证数据源的安全，建议在配置数据源时注意以下事项：

- (1) **不使用 EasySQLMAIL 直接连接关键的核心数据库**，以防止因为任务配置错误（例如任务执行频率过高或是查询语句效率太低，耗费大量数据库主机资源）而对核心数据库造成影响，干扰企业关键应用的工作。一种推荐的组网方式是，在企业中安装一个数据库作为中间数据库，由核心数据库定时将需要推送的数据下发到中间数据库上，EasySQLMAIL 再从中间数据库中读取推送数据进行推送。这种模式具有较好的隔离性，不会因为任务配置问题或是 SQL 语句的运行效率问题影响核心数据库的正常运行。



使用中间数据库存放推送信息

- (2) **不使用大权限数据库账号配置数据源**：在配置数据源时，不使用大权限的数据库账号(例如 sa、sys、root 等账号)，也不使用生产系统的数据库账号来连接数据源。应该专门创建一些权限小的查询账号供 EasySQLMAIL 使用，根据取数需要再赋予这些小权限账号 SELECT 或其它数据库操作权限。这样可以有效控制数据库访问权限。
- (3) **不将创建数据源权限开放给其他用户**：一般情况下，admin 不应将创建数据源的权限赋予其他用户。创建数据源时，应该由 admin 根据企业 IT 安全规定对取数需求进行评估后，再创建数据源，并将数据源的使用权限指派给相应用户。
- (4) **谨慎使用 DDL 及数据修改语句**：配置任务时，如果 SQL 语句中有 DDL 语句(例如 CREATE, DROP, ALTER, TRUNCATE 等)或是 INSERT、DELETE、UPDATE 语句时，应对语句和所配置的任务进行严格测试确认语句的正确性后再上线使用。

- (5) **在任务上线前仔细进行测试，确保查询和推送的正确性：**管理员在新配置的任务上线前应该对任务的执行结果进行仔细检查，确保任务生成的数据内容及推送方式、推送目标正确无误后再将任务正式上线运行。
- (6) **仔细检查导入任务的语句配置：**在导入任务后，应该对导入的任务内容进行检查、评估，确认导入的任务中的 SQL 语句不会与本地系统冲突，然后再进行测试、使用。这里的冲突主要是指 SQL 语句中涉及的表等数据库对象的 CREATE、UPDATE、INSERT、DELETE 和 DROP、TRUNCATE 等操作。例如，导入的任务中有一个 SQL 语句：“DROP TABLE T_BT” 这个表在任务的设计者那里仅仅是一个普通的临时表，但在本地，这个表是一个重要的数据表，那么这个任务导入后，如果对任务进行测试（预览）或运行，就会错误地将表 T_BT 删除，这会造成不可挽回的损失。所以，在预览和执行任务前，应仔细检查任务的 SQL 语句等内容，确认任务的安全性后再使用。

1.2 网络和密码安全

为保证各类密码的安全，EasySQLMAIL 在传输和存储密码时对密码进行了多层加密。但为进一步保证系统安全，在使用时还需要注意以下事项：

- (1) **不在公网或不安全的网络上暴露 EasySQLMAIL 系统的 WEB 控制台程序。** EasySQLMAIL 安装完成后，只能在安装的主机上通过访问 <http://127.0.0.1:9110> 访问 EasySQLMAIL 控制台。建议系统管理员使用此访问方式。
- (2) **只允许指定的 IP 地址访问 EasySQLMAIL 的 WEB 控制台。** EasySQLMAIL 中自带了 IP 访问限制策略。如果您的操作系统有网络防火墙，或是有其他类型的网络防火墙，也可以用这些网络防火墙实现 IP 访问限制。如果一定要对其它 IP 地址开放访问权限，建议在系统配置中启用“使用安全 HTTP 协议(HTTPS) 连接 WEB 控制台界面”选项。
- (3) **EasySQLMAIL 系统的用户应使用复杂的登录密码，并定期更换，**以避免密码被猜出而造成损失。
EasySQLMAIL 所在的服务器主机也应使用强密码进行保护。
- (4) **开启 EasySQLMAIL 的登录验证码功能，**在用户登录 EasySQLMAIL 的控制台和企业信息查询界面时，需要输入系统发送的数字验证码，可以增强系统的安全性，防止非法登录。
- (5) **使用强密码保护 EasySQLMAIL 所在的服务器主机，**防止无关人员登录主机后对系统进行非法操作。

1.3 根据企业 IT 安全要求对数据内容及推送方式进行评估

- (1) **评估推送方式是否符合企业 IT 安全管理制度的要求。**在配置信息推送任务前，应根据您的企业内部对信息安全管理的相关制度和要求，评估要推送的信息是否适合通过 EasySQLMAIL 系统进行推送。
- (2) **根据企业的 IT 信息管理制度及国家信息安全相关法律法规对推送信息进行脱敏处理。**例如，应该对推送信息中涉及到的公民个人信息的内容进行脱敏处理，以防止公民的个人信息泄露。

1.4 做好数据备份

EasySQLMAIL 系统管理员应定期对 EasySQLMAIL 系统所在的目录进行备份，并对备份数据进行加密后妥善保管，以便在主机发生故障时能够快速恢复 EasySQLMAIL 的运行。

1.5 信息推送的可靠性测试

EasySQLMAIL 系统在进行信息推送时会受到很多外部条件的约束。例如，公司的邮件服务器可能会将 EasySQLMAIL 系统发出的邮件误判为垃圾邮件而拒收，有一些邮件服务器可能会延迟一段时间后才能收到邮件。

为避免因这些情况导致您的工作事务被延误，在正式启用一个信息推送任务之前，管理员需要仔细对任务进行测试，确保任务发出的邮件或消息能在要求的时间内正确送达给指定收件人。