然而，细心的读者可能会提出一个问题：如果用户拥有了 PROCESS 权限，他们会不会一不小心 KILL 掉一些关键的系统线程，比如主从复制线程（Replication Thread）或后台维护线程？这确实是一个合理的担忧，因为系统线程一旦被误杀，可能会导致数据库服务中断，甚至引发数据不一致的风险。

MySQL 8.0 的设计者显然也考虑到了这一点。为了保护系统线程，他们引入了 SYSTEM_USER 权限。这个权限的作用是区分普通用户线程和系统线程，并为后者提供额外的保护。具体规则如下：

- 如果某个线程是由具有 SYSTEM_USER 权限的用户创建的（通常是 MySQL 的内置系统账号，比如复制线程的执行用户），那么普通用户（没有 SYSTEM_USER 权限）无法通过 KILL 命令终止它。
- 只有当前会话也具备 SYSTEM_USER 权限的用户，才能 KILL 掉同样具备 SYSTEM_USER 权限的线程。

这意味着，即便业务用户拥有了 PROCESS 权限，他们也无法干扰数据库的后台线程，比如主从复制线程、事件调度线程（Event Scheduler）或管理员的命令行。这种设计极大地提升了系统的稳定性，避免了权限滥用带来的潜在风险。

这就保证了普通用户无法越界操作，系统的核心功能得到了保护。

## 五、实战演练：如何优雅地使用 KILL 权限