MySQL 触发器介绍

普通用户的密码和 `root` 密码在 Linux 和类 Unix 系统中有着不同的用途和权限控制。它们的区别主要体现在权限、用途以及安全性方面。

1. 权限区别：

- **普通用户密码**：
  - 用于验证普通用户身份，登录系统时需要提供这个密码。
  - 普通用户的权限受到系统的严格限制，通常只能访问自己拥有的文件和进程，不能进行系统级别的操作（如修改系统配置、安装软件、管理其他用户等）。
  - 普通用户可以通过输入自己密码来执行某些经过授权的命令（如通过 `sudo` 运行具有管理员权限的操作）。
- **`root` 密码**：
  - `root` 是系统的超级用户（管理员），拥有对整个系统的最高权限。`root` 用户可以访问和修改所有文件、管理所有进程、安装和删除软件、配置系统网络等。
  - `root` 密码用于直接登录 `root` 帐户或通过 `su` 切换到 `root` 身份。
  - 由于 `root` 的权限非常高，这个密码极其重要，需要高度保护，避免滥用。

2. 用途区别：

- **普通用户密码**：
  - 普通用户在登录系统、解锁屏幕、运行需要权限的操作时需要输入自己的密码。
  - 在使用 `sudo` 时，系统会提示输入普通用户的密码，以临时获取执行管理员任务的权限（前提是该用户有 `sudo` 权限）。
- **`root` 密码**：
  - `root` 密码直接用于登录 `root` 帐户或通过 `su` 切换到 `root` 用户，执行系统级的操作。
  - 某些系统禁止直接登录 `root`，但可以通过 `sudo` 或 `su` 切换到 `root`。

3. 安全性区别：

- **普通用户密码**：
  - 如果普通用户密码被泄露，攻击者通常只能获得普通用户的权限，不会对整个系统造成直接威胁。
  - 通过 `sudo` 限制，普通用户的能力被部分控制。
- **`root` 密码**：
  - `root` 密码如果被泄露，攻击者将获得对整个系统的完全控制，能够修改、删除任何文件，安装恶意软件，甚至破坏系统。因此 `root` 密码的安全至关重要。

4. 密码使用场景：

- **普通用户**：
  - 登录桌面系统或 SSH 远程访问系统。
  - 执行用户级别的操作，如编辑文件、运行应用程序等。
  - 使用 `sudo` 时会要求输入普通用户密码来获得临时权限。

- `root` **用户**：
  - `root` 密码用于执行高级操作，如修改系统配置、管理系统资源和用户等。
  - `root` 密码不应随意使用，直接登录 `root` 帐户也通常被视为不安全的做法，推荐使用 `sudo` 获得临时管理员权限。

总结：

- **普通用户密码**用于普通日常任务，具有受限权限，保护用户自己的文件和操作。
- `root` **密码**用于执行系统管理任务，具有最高权限，保护整个系统的安全。

通常情况下，建议通过 `sudo` 来执行需要管理员权限的任务，而不直接使用 `root` 密码，以减少系统遭受误操作或安全风险的可能性。