# 多次输错密码之后如何限制用户规定时间内禁止再次登录?

> 类似的问题：用户输入3次密码错误之后，如何限制用户10分钟内禁止登录?

我们首先要明确一下多次输错密码之后限制的是具体的用户还是 IP。

一般情况下我们建议以 IP 地址为单位来进行限制，而非具体的用户。这样可以避免影响到真实用户的使用，减少误伤其他用户的可能性。

例如，一个非法用户可能会拿别人的账号不断尝试登录，如果直接将其给限制登录了，那么该用户本人就无法登录自己的账号了。因此，以 IP 地址为单位进行限制相对更加合理。

同时，以 IP 地址为单位进行限制还可以避免其他攻击行为，比如黑客通过使用同一 IP 地址进行暴力破解等攻击行为。这样可以提高系统的安全性和稳定性。

需要注意的是，在实际的应用开发中，还需要考虑不同场景下的策略调整、粒度控制等因素，以达到最佳的用户体验和安全性能。

## 使用 Redis 的常见做法

后台使用 Redis 记录当前 ip 的尝试登录次数：

- key 为该 ip 请求登录的唯一标识。
- value 为当前 ip 的尝试登录次数。

我们需要给这个 key 设置一个过期时间，用来实现指定时间内无法再次登录的效果。并且，每次对 key 对应的 value 进行修改时，都需要重置过期时间。

整个逻辑也很简单（我们这里假设错误阈值为 3 ）：

1. 当用户提交用户名和密码登录时，先判断是否有对应的 key。
2. 如果没有对应 key 的话，说明是第一次登录，直接校验用户名和密码的正确性即可。用户名和密码校验通过，则返回“登录成功”；否则，就返回“登录失败，用户名/密码错误”，并创建对应的 key，key 对应的 value 值为 1，代表其已经请求尝试登录过 1 次了。
3. 如果有对应的 key，说明不是第一次登录了，需要判断 key 对应的 vaue 大小是否小于 3。
4. 如果小于 3 则代表还能继续尝试登录，重复密码校验这一步。用户名和密码校验通过，则返回“登录成功”；否则，就返回“登录失败，用户名/密码错误”，并将 key 对应的 value 值加 1（建议使用 Lua 脚本，涉及到 get、incr、expire 这三个操作）。
5. 如果 value 等于 3，则表明该 ip 已经尝试登录过 3 次，返回“输入密码错误次数达到 3 次，请 xx 分钟后再尝试”。

## 不使用 Redis 的常见做法

直接在用户表里增加两个字段：

1. 输错密码次数 num
2. 禁止登录的截至时间点 lock-time

我们需要记录输错密码的次数 num，当输入正确密码之后重置 num 和 lock-time 字段的值，当输错密码次数达到 3 次之后，修改 lock-time 为允许再次登录的时间。

整个逻辑也很简单（我们这里假设错误阈值为 3 ）：

1. 当用户提交用户名和密码登录时，先判断当前时间点是不是比 lock-time 小。
2. 如果比 lock-time 小的话，说明当提前用户暂时被限制登录，返回“输入密码错误次数达到 3 次，请 xx 分钟后再尝试”。
3. 如果大于等于 lock-time 的话，表明当前未被限制登录，进一步判断 num 的大小是否小于 3。
4. 如果小于 3 则代表还能继续尝试登录，用户名和密码校验通过，则返回“登录成功”，并重置 num 和 lock-time 字段的值；否则，就返回“登录失败，用户名/密码错误”，并将 num 的值加 1。

5. 如果 num 等于 3，则表明该 ip 已经尝试登录过 3 次，返回“输入密码错误次数达到 3 次，请 xx 分钟后再尝试”，并更新 lock-time 的值。

url=https%3A%2F%2Fwww.yuque.com%2Fsnailclimb%2Ftangw3%2Fbkag5r9o4frnoee3&pic=nu