# H4A融合登录模板设计文档

2023年1月31日

本文档旨在于描述H4A融合登录模板的设计方案，旨在于帮助相关专家老师们了解融合登录模板的开发设计思路。

## 整体流程

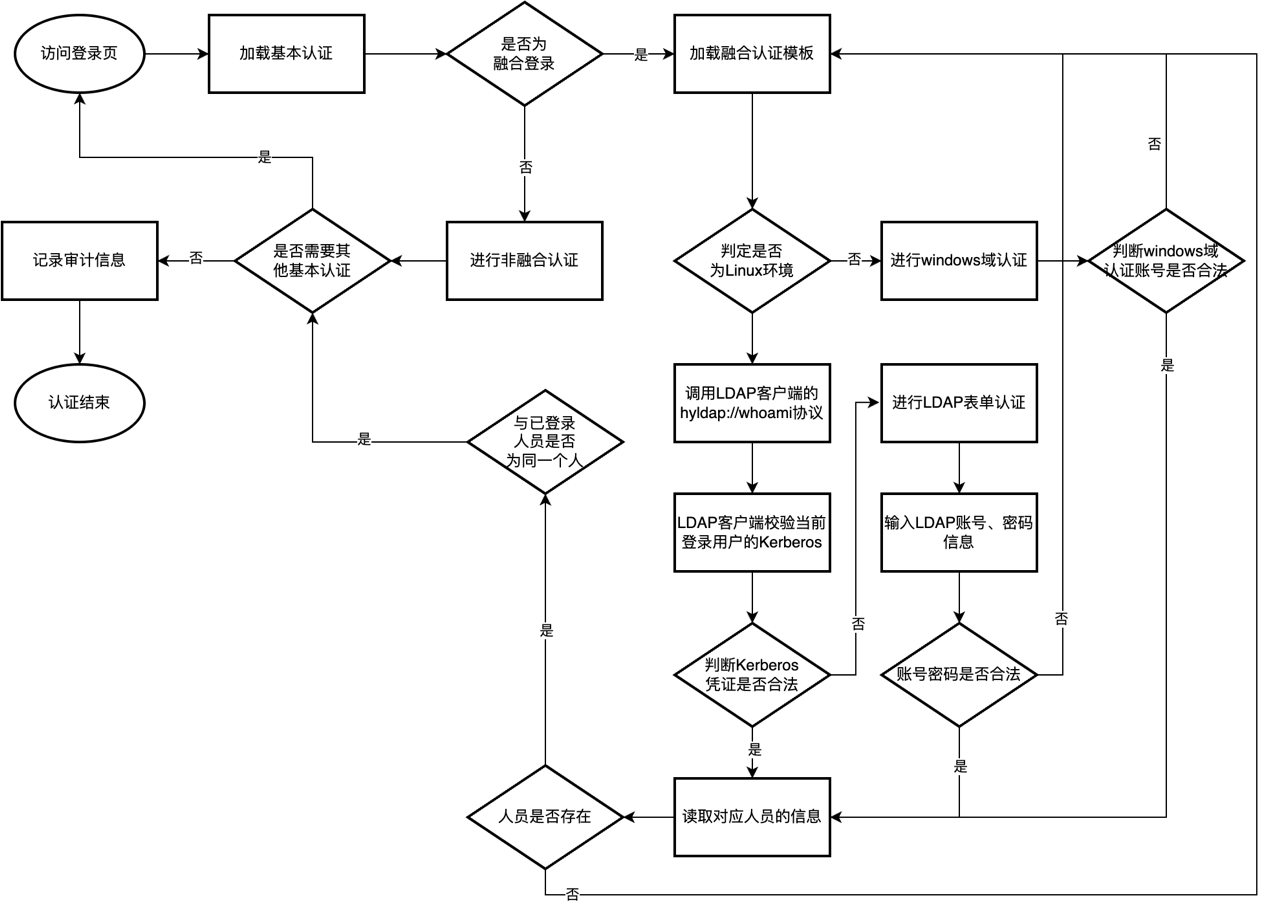


图 1整体流程

* 1. 业务系统访问登录页；
  2. 根据认证参数中的组合认证依次加载待认证的基本认证方式；
  3. 如果用户选择融合认证方式，或默认为融合认证方式，则加载融合认证模板；
  4. 融合认证模板会判断当前操作系统的类型，用以区分是Linux还是Windows；
  5. 如果是Linux系统，则会使用融合登录模板，模板页面会调用LDAP自定义协议：hyldap://whoami来获取当前登录的域用户信息。浏览器接收到此协议请求后，会启动LDAP本地客户端来处理此请求；
  6. 如果没有安装LDAP本地客户端或已卸载，则协议调用失败，模板页面显示“Kerberos登录失败”，并自动切换到表单登录页面；
  7. 在LDAP表单登录页面中，用户需要输入自己在H4A系统中的用户名和密码，融合登录模板会对账号进行非空校验，通过后向LDAP接口系统发送验证请求。
  8. LDAP接口系统收到验证请求后，会和LDAP域控服务器通信并执行用户有效性校验，要求必须为LDAP域用户，且账号正确。
  9. 如果验证通过，则读取并返回当前用户的标识，并记录审计日志后返回业务系统主页。
  10. 如果已安装LDAP客户端，则会唤醒客户端中的whomai程序，此时会在信创终端上校验当前登录系统的域账号的Kerberos凭证。此过程不会和LDAP服务器端交互，即便面临登录高峰，由于压力是分散在信创终端的，因此不存在性能瓶颈；
  11. 如果为本地用户，则因Kerberos而校验失败。如果为LDAP域用户或AD域用户，则Kerberos校验成功，并将当前登录用户的标识符使用Base64处理后返回给H4A融合登录页面。
  12. Kerberos认证成功后，则读取并返回当前用户的标识，并记录审计日志后返回业务系统主页。此过程中H4A融合登录模板不会在浏览器中存储任何信息。
  13. 如果Kerberos认证失败，则自动加载LDAP表单登录模板，输出“此用户非LDAP域用户，无法执行Kerberos自动登录”；
  14. 如果是Windows系统，则融合认证模板会自动切换到Windows域认证模板，执行Windows域认证。
  15. 切换到Windows域认证模板后执行的逻辑为原有Windows域认证的逻辑。
  16. 以上步骤完成后，认证结束。