??????????LDAP??

好嘞 □□
我帮你写一个开源版禅道登录时调用 **AD/LDAP** 验证的示例，直接可以插到 `module/user/control.php` 里的 `login` 方法开头。

? ????

1. 用户输入用户名和密码。
2. 先尝试用 LDAP 验证（比如绑定到 AD 域）。
3. 如果 AD 验证成功，就在禅道本地用户表 `zt_user` 中查找对应账号：
   - 如果已存在 → 直接登录。
   - 如果不存在 → 自动创建一个账号（避免重复维护）。
4. 如果 LDAP 验证失败 → 走禅道原有的本地认证逻辑。

? PHP ????

在 `module/user/control.php` 的 `login` 方法开头加：

```
<?php
// ===== LDAP 配置 =====
$ldapConfig = array(
    'host'       => '192.168.0.5',         // AD 域控IP (如 S-DNS6)
    'port'       => 389,                   // AD LDAP端口 (389/636 LDAPS)
    'base_dn'    => 'DC=shuncom,DC=local', // 域DN
    'domain'     => 'shuncom.local',       // 域名
    'admin_user' => 'administrator@shuncom.local', // 可选: AD管理用户
    'admin_pass' => '你的管理密码'              // 可选: 管理密码
);

// ===== 从表单获取用户名密码 =====
$username = trim($this->post->account);
$password = trim($this->post->password);

// ===== LDAP 验证 =====
```

```
if(!empty($username) && !empty($password))
{
    $ldapconn = ldap_connect($ldapConfig['host'], $ldapConfig['port']);
    ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, 3);
    ldap_set_option($ldapconn, LDAP_OPT_REFERRALS, 0);

    if($ldapconn)
    {
        // 拼接用户 UPN，如 user@domain
        $ldapUser = $username . '@' . $ldapConfig['domain'];

        if(@ldap_bind($ldapconn, $ldapUser, $password))
        {
            // LDAP 验证成功
            $filter = "(sAMAccountName={$username})";
            $search = ldap_search($ldapconn, $ldapConfig['base_dn'], $filter);
            $entries = ldap_get_entries($ldapconn, $search);

            if($entries['count'] > 0)
            {
                $displayName = $entries[0]['cn'][0];
                $email       = isset($entries[0]['mail'][0]) ? $entries[0]['mail'][0] :
$username.'@'.$ldapConfig['domain'];

                // 检查用户是否已存在禅道库
                $user = $this->dao->select('*')->from(TABLE_USER)->where('account')-
>eq($username)->fetch();

                if(!$user)
                {
                    // 自动创建禅道用户
                    $newUser = new stdclass();
                    $newUser->account  = $username;
                    $newUser->realname = $displayName;
                    $newUser->email    = $email;
                    $newUser->password = md5($password); // 禅道存本地密码(可随便填)
                    $newUser->role     = 'dev';
                    $newUser->dept     = 0;
                    $newUser->gender   = 'm';
```

```
                    $this->dao->insert(TABLE_USER)->data($newUser)->exec();
                }

                // 直接跳过禅道本地密码校验，构造登录态
                $user = $this->dao->select('*')->from(TABLE_USER)->where('account')->eq($username)->fetch();
                $this->session->set('user', $user);

                // 登录成功后跳转
                $this->locate($this->createLink('my', 'index'));
                exit;
            }
        }
    }
    @ldap_close($ldapconn);
}

// 如果LDAP失败，就继续走禅道原来的登录逻辑
```

? ????

1. `ldap_bind` 默认是明文，如果要走 **LDAPS (636)**，需要配置 SSL 证书。
2. 代码里是直接拼接 `$username@domain`，如果你的域用 `CN=user,CN=Users,DC=xx,DC=local` 形式，需要改 `binddn`。
3. 自动创建禅道用户时给了默认角色 `dev`，可以改成 `pm/test/admin`。
4. 这段代码最好放在原有 **`$this->user->identify()`** 之前，保证先走 LDAP。

要不要我帮你改一份完整的 **`login()`** 方法整合版（原有禅道逻辑 + 上面的 LDAP 插入好位置），这样你直接覆盖就能测试?

好的 □ 我帮你写一个完整的 `login()` 方法，把禅道开源版原有的逻辑和 **LDAP**（**AD** 域验证）逻辑融合在一起。这样你可以直接覆盖 `module/user/control.php` 里的 `login()` 方法来测试。

假设你的 AD 域控制器是 `192.168.0.5`，域名是 `shuncom.local`，管理员只需要验证账号密码，不需要复杂的组判断。

???? `login()` ???????

```
public function login($referer = 0)
{
    if(!empty($_POST))
    {
        $account  = trim($this->post->account);
        $password = $this->post->password;

        $user = null;
        $ldapSuccess = false;
        $ldapError   = '';

        /* === 第一步: 尝试 LDAP 验证 === */
        $ldapconn = @ldap_connect("ldap://192.168.0.5");
        if($ldapconn)
        {
            ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, 3);
            ldap_set_option($ldapconn, LDAP_OPT_REFERRALS, 0);

            $ldaprdn = $account . '@shuncom.local'; // UPN 格式
            $bind = @ldap_bind($ldapconn, $ldaprdn, $password);

            if($bind)
            {
                $ldapSuccess = true;

                // 查找用户在 AD 中的 displayName/mail 等信息
                $result = @ldap_search($ldapconn, "DC=shuncom,DC=local",
"(sAMAccountName={$account})");
                $entries = @ldap_get_entries($ldapconn, $result);

                if($entries["count"] > 0)
                {
                    $adName  = $entries[0]["displayname"][0] ?? $account;
                    $adEmail = $entries[0]["mail"][0] ?? "{$account}@shuncom.local";

                    // 检查禅道数据库是否已存在该用户
                    $user = $this->user->getByAccount($account);
                    if(!$user)
                    {
                        // 自动创建本地用户
```

```
                    $user = new stdClass();
                    $user->account  = $account;
                    $user->realname = $adName;
                    $user->email    = $adEmail;
                    $user->password = md5($password);
                    $this->dao->insert(TABLE_USER)->data($user)->exec();
                    $user->id = $this->dao->lastInsertID();
                }
            }
        }
        else
        {
            $ldapError = ldap_error($ldapconn);
        }
        @ldap_close($ldapconn);
    }

    /* === 第二步: 如果 LDAP 验证失败, 走禅道本地逻辑 === */
    if(!$ldapSuccess)
    {
        $user = $this->user->identify($account, $password);
    }

    /* === 第三步: 检查用户结果 === */
    if(!$user)
    {
        $this->view->reason = $ldapError ? "LDAP 验证失败: {$ldapError}" : $this->lang->user->loginFailed;
        return $this->display();
    }

    if($user->deleted == 1)
    {
        $this->view->reason = $this->lang->user->loginFailed;
        return $this->display();
    }

    /* === 第四步: 写入 session, 记录登录日志 === */
    $this->session->set('user', $user);
    $this->user->cleanLocked($account);
```

```
        $this->loadModel('action')->create('user', $user->id, 'login');

        /* === 第五步: 重定向 === */
        if($referer) $this->locate($referer);
        if($this->session->user->last) $this->locate($this->session->user->last);
        $this->locate($this->createLink('my', 'index'));
    }

    $this->display();
}
```

[illegible]

1. 优先调用 **LDAP** 验证，成功后自动同步用户到禅道数据库（不存在就创建）。
2. 如果 LDAP 验证失败，继续走 禅道本地数据库逻辑 。
3. 登录成功后，写入 session 并跳转。
4. 保留了禅道原有的 `$this->user->identify()`、`$this->session->set()`、`action->create()` 等逻辑。

要不要我帮你做一个 配置开关 （比如 `config->ldap->enable`），这样可以灵活选择走 AD 还是本地?

Revision #1
Created 30 September 2025 00:50:30 by Admin
Updated 30 September 2025 00:51:10 by Admin