??? AD + Keycloak + RAGFlow ????

很好，这一步就是 企业级 **AD + Keycloak + RAGFlow** 完整闭环了，我给你一套可以直接落地的标准方案（生产可用）。

????????????

```
Windows AD (192.168.0.5)
        │ LDAP / LDAPS
        ▼
   Keycloak（身份中台）
        │ OIDC
        ▼
   RAGFlow（自动建用户 + 角色映射）
```

???????3???

必须同时完成：

? 1. AD??????

? 2. ????????RAGFlow??

? 3. AD Group ? RAGFlow Role ??

??Keycloak ??????

1?? LDAP ?? AD

进入:

```
User Federation → LDAP
```

配置:

参数	值
Vendor	Active Directory
Connection URL	ldap://192.168.0.5:389
Bind DN	CN=ldapbind,OU=ServiceAccounts,DC=shuncom,DC=local
Bind Credential	******
Users DN	DC=shuncom,DC=local
Import Users	✔ ON
Edit Mode	READ_ONLY

???????“???????”

在 LDAP 设置中:

? ?????

```
Import Users = ON
```

否则不会同步 AD 用户

??Keycloak Role / Group ????????

2?? ?? Mapper????

□□□

```
LDAP → Mappers
```

□□□

? Mapper 1????

Name	value
ldap attribute	sAMAccountName
user attribute	username

? Mapper 2???

| LDAP | mail |
| RAGFlow | email |

? Mapper 3?AD Group ? Keycloak Group

Mapper Type	group-ldap-mapper
Groups DN	OU=Groups,DC=shuncom,DC=local
Membership attribute	member

??Keycloak ? RAGFlow ????

3?? ? Keycloak ?? Realm Roles

例如:

- ragflow-admin
- ragflow-user
- ragflow-reader

4?? Group ? Role ??

Keycloak:

```
Group → Role Mapping
```

示例:

AD Group	RAGFlow Role
IT_Admin	ragflow-admin
AI_User	ragflow-user

??RAGFlow ????????

你现在 docker-compose 需要改这几个:

? 1. ???ID????????

```
OAUTH2_USER_ID_CLAIM=email
```

□□□ sub

? 2. ???????????

```
REGISTER_ENABLED=1
```

? 3. ?? OIDC

```
OAUTH2_ENABLE=True
OAUTH2_TYPE=oidc
```

? 4. ????????

```
OAUTH2_AUTO_CREATE_USER=true
```

（如果版本支持）

??RAGFlow ???????????

RAGFlow 本身是靠 OIDC claims:

你需要在 Keycloak 加:

5?? Client Mapper????

进入:

```
Client → ragflow → Mappers
```

添加:

? Mapper 1?roles

Name	roles
Mapper Type	User Realm Role

Name	roles
Token Claim Name	roles
Add to ID token	ON
Add to access token	ON

? Mapper 2?groups

Name	groups
Mapper Type	Group Membership
Token Claim	groups

??RAGFlow ?????

RAGFlow 会读取:

```
{
  "email": "8108@shuncom.local",
  "groups": ["AI_User"],
  "roles": ["ragflow-user"]
}
```

????????????????

当用户第一次登录:

```
Keycloak 登录成功
        ↓
RAGFlow 收到 email
        ↓
检查用户是否存在
        ↓
不存在 → 自动创建
        ↓
```

□□ role/group

??????????????????

docker-compose.yml??????

```
environment:
  - OAUTH2_ENABLE=True
  - OAUTH2_TYPE=oidc
  - OAUTH2_DISPLAY_NAME=AD□□□□□

  - OAUTH2_AUTHORIZATION_URL=http://192.168.4.16:8081/realms/shuncom/protocol/openid-connect/auth
  - OAUTH2_TOKEN_URL=http://192.168.4.16:8081/realms/shuncom/protocol/openid-connect/token
  - OAUTH2_USERINFO_URL=http://192.168.4.16:8081/realms/shuncom/protocol/openid-connect/userinfo

  - OAUTH2_CLIENT_ID=ragflow
  - OAUTH2_CLIENT_SECRET=xxxx

  - OAUTH2_REDIRECT_URI=http://192.168.4.16/oauth/callback

  - OAUTH2_USER_ID_CLAIM=email
  - REGISTER_ENABLED=1
```

????????????

? AD????RAGFlow

? ??????????

? AD???????

? Keycloak??????

? RAGFlow????????

??????????????????

我可以帮你再升级成：

? AD? ? RAGFlow??????

? ????????????

? ??????AD??

? LDAP????

? HTTPS + ??SSO????

只需要说一句：

> “升级成企业级 SSO完整方案 ”

我可以给你一套 生产环境标准架构（含 **Keycloak**导入模板 **+ LDAP**配置 **+ RAGFlow**最终 **docker-compose**）。

Revision #1
Created 29 June 2026 07:45:03 by Admin
Updated 29 June 2026 07:45:28 by Admin