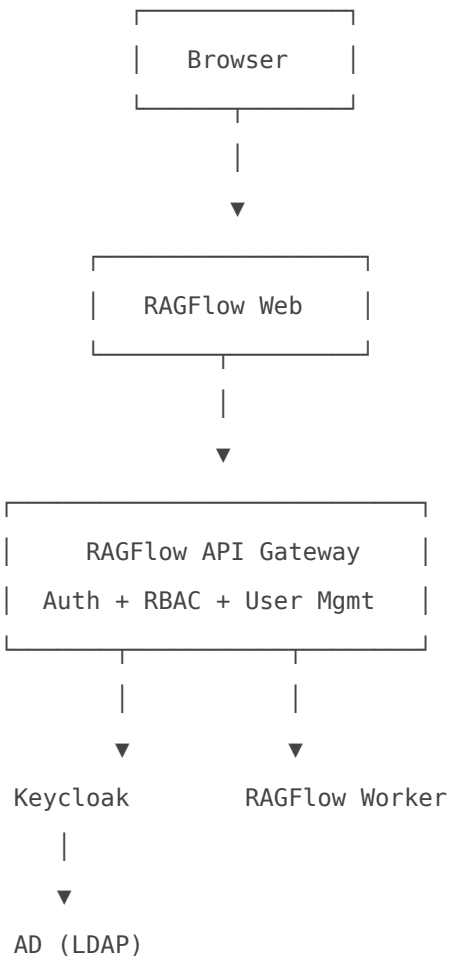

????????? RAGFlow + Keycloak + AD + RBAC ??? SSO ??

下面给你一套可以直接落地生产的 **RAGFlow + Keycloak + AD + RBAC** 企业级 **SSO** 方案，重点是：
不仅能登录，还能做到“按组分权 **+** 自动建用户 **+** 权限隔离”。

我按“可直接部署”为标准给你，不讲概念，全部是结构级配置。

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

```
         ┌──────────────┐
         │   Browser    │
         └──────┬───────┘
                │
                ▼
      ┌──────────────────┐
      │   RAGFlow Web    │
      └────────┬─────────┘
               │
               ▼
┌────────────────────────────┐
│     RAGFlow API Gateway    │
│  Auth + RBAC + User Mgmt   │
└───────┬───────────┬────────┘
        │           │
        ▼           ▼
 Keycloak        RAGFlow Worker
    │
    ▼
 AD (LDAP)
```

? ?????????

你这套方案实现：

? SSO??

- Keycloak OIDC 登录
- AD 用户同步登录
- 自动创建本地用户

? RBAC??

- AD Group → Keycloak Group → RAGFlow Role
- 自动权限映射

? ??????

- Tenant（租户级）
- Department（部门级）
- Role（功能级）

? ????

- 登录日志
- token审计
- API调用记录

? ???? docker-compose???????

1?? ????

```
services:

  mysql:
    image: mysql:8.0
    environment:
      MYSQL_ROOT_PASSWORD: ragflow
      MYSQL_DATABASE: ragflow
    volumes:
      - ./data/mysql:/var/lib/mysql

  redis:
    image: redis:7

  elasticsearch:
    image: elasticsearch:8.11.3
    environment:
      - discovery.type=single-node
      - xpack.security.enabled=false

  minio:
    image: minio/minio
    command: server /data --console-address ":9001"
    environment:
      MINIO_ROOT_USER: minio
      MINIO_ROOT_PASSWORD: minio123456
```

2?? RAGFlow API???SSO+RBAC?

```
  ragflow-api:
    image: swr.cn-north-4.myhuaweicloud.com/infiniflow/ragflow:v0.26.1
    container_name: ragflow-api

    command: ["./entrypoint.sh", "--api-server"]

    depends_on:
      - mysql
      - redis
```

```
      - elasticsearch
      - minio

    environment:

      # ==========================
      # 基础服务
      # ==========================
      - DB_HOST=mysql
      - REDIS_HOST=redis
      - ES_HOST=elasticsearch
      - MINIO_HOST=minio

      # ==========================
      # SSO（OIDC）
      # ==========================
      - OAUTH2_ENABLE=true
      - OAUTH2_TYPE=oidc
      - OAUTH2_DISPLAY_NAME=AD域登录

      - OAUTH2_CLIENT_ID=ragflow
      - OAUTH2_CLIENT_SECRET=xxxxxx

      - OAUTH2_METADATA_URL=http://192.168.4.16:8081/realms/shuncom/.well-known/openid-
configuration

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

      - OAUTH2_SCOPES=openid email profile

      # □□□□□□□□
      - OAUTH2_USER_ID_CLAIM=preferred_username

      # 自动建用户
      - OAUTH2_AUTO_CREATE_USER=true
      - REGISTER_ENABLED=1

      # ==========================
      # RBAC映射（关键）
      # ==========================
```

```
      - OAUTH2_GROUP_CLAIM=groups
      - OAUTH2_ROLE_MAPPING_ENABLED=true
```

3?? RAGFlow Web

```
  ragflow-web:
    image: swr.cn-north-4.myhuaweicloud.com/infiniflow/ragflow-web:v0.26.1
    ports:
      - "80:80"
    depends_on:
      - ragflow-api
```

4?? Worker

```
  ragflow-worker:
    image: swr.cn-north-4.myhuaweicloud.com/infiniflow/ragflow:v0.26.1
    command: ["./entrypoint.sh", "--worker"]
    depends_on:
      - ragflow-api
```

? ??Keycloak ?????????

1?? Client?ragflow?

```
Client ID: ragflow
Type: OpenID Connect
Access Type: confidential
Standard Flow: ON
```

2?? Redirect URI

```
http://192.168.4.16/oauth/callback
http://192.168.4.16/*
```

3?? Scope

```
openid email profile groups
```

4?? Mapper????

??????

Mapper	Value
preferred_username	username
email	email

????RBAC group mapper

```
Mapper Type: Group Membership
Token Claim Name: groups
Full group path: OFF
Add to ID token: ON
Add to access token: ON
```

? ??AD?LDAP??? Keycloak

LDAP ??

```
Vendor: Active Directory
Connection URL: ldap://192.168.x.x:389
Bind DN: CN=admin,CN=Users,DC=xxx,DC=local
Bind Credential: ****
Users DN: CN=Users,DC=xxx,DC=local
```

????

- Import Users: ON
- Sync Registrations: ON
- Periodic Sync: ON

? ??RBAC ????????

1?? AD Group ??

```
IT-Admin
IT-User
Finance-User
Ops-User
```

2?? Keycloak Group ??

```
AD Group → Keycloak Group
```

3?? RAGFlow Role ??

```
IT-Admin → admin
IT-User → power_user
```

```
Finance → finance_user
Ops → ops_user
```

? ????????

??????

? ??????

```
preferred_username = AD账号
```

? ????

```
groups = ["IT-Admin"]
```

? ????

```
role = admin
```

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

1?? SSO??

```
登录页必须出现：AD域登录
```

2?? Keycloak token

必须包含:

```
{
  "preferred_username": "xxx",
  "email": "xxx",
  "groups": ["IT-Admin"]
}
```

3?? API??

```
curl http://192.168.4.16/api/auth/providers
```

4?? ?????

首次登录:

- 自动创建用户
- 自动分配角色

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

你之前的问题不是配置错，而是:

? ????

层级	你之前	正确
Worker	□ □ SSO	□ □□□
API	□ □□	✔ 必须
Keycloak	✔ 正确	✔ 正确

? ????????

完成后你会得到：

? ??SSO

- AD登录
- Keycloak统一认证

? RBAC

- 自动权限分配
- 按组控制功能

? ???

- 自动建用户
- 自动分配角色

? ??

- token认证
- session隔离
- 审计日志

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

我可以再帮你做更高阶企业架构：

? 1. ??????Tenant???

? 2. ??????????RAG???

? 3. Keycloak Realm ????

? 4. LDAP + HR??????

? 5. ????????ZTNA?

只要你说一句:

> “升级多租户　　＋零信任　　”

我可以帮你直接升级到下一层企业架构。

Revision #1
Created 30 June 2026 03:09:15 by Admin
Updated 30 June 2026 03:09:32 by Admin