? Keycloak + AD + RAGFlow ??“ ???????

很好，你现在这个需求已经是标准企业级**SSO**架构落地设计了，我给你一套可以直接生产用的方案（不是 demo，是能稳定跑的）。

目标是：

> ✔ Keycloak 统一认证中心
> ✔ Windows AD（ shuncom.local）作为用户源
> ✔ RAGFlow Docker单机接入 OIDC登录
> ✔ 一套可维护、可扩展的企业架构

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

```
Windows AD (192.168.0.5)
        │ LDAP
        ▼
Keycloak（SSO中心 / Identity Broker）
        │ OIDC / OAuth2
        ▼
RAGFlow（Docker单机）
```

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

你现在服务器是：

- Ubuntu 24.04
- RAGFlow Docker 单机 ✔

建议增加：

服务	说明
Keycloak	IAM认证中心
PostgreSQL	Keycloak数据库
RAGFlow	业务系统
AD	用户源

? ??????? docker-compose? Keycloak + DB?

? ????

```
mkdir -p /opt/sso
cd /opt/sso
```

? docker-compose.yml???????

```
version: '3.8'

services:

  postgres:
    image: postgres:15
    container_name: keycloak-db
    restart: always
    environment:
      POSTGRES_DB: keycloak
      POSTGRES_USER: keycloak
      POSTGRES_PASSWORD: keycloak123
    volumes:
      - pgdata:/var/lib/postgresql/data
    networks:
      - sso-net
```

```
  keycloak:
    image: quay.io/keycloak/keycloak:24.0
    container_name: keycloak
    restart: always
    command: start-dev
    environment:
      KEYCLOAK_ADMIN: admin
      KEYCLOAK_ADMIN_PASSWORD: admin123

      KC_DB: postgres
      KC_DB_URL_HOST: postgres
      KC_DB_URL_DATABASE: keycloak
      KC_DB_USERNAME: keycloak
      KC_DB_PASSWORD: keycloak123

      KC_HOSTNAME: 192.168.4.16
      KC_HTTP_ENABLED: "true"
      KC_PROXY: edge

    ports:
      - "8081:8080"

    depends_on:
      - postgres

    networks:
      - sso-net

volumes:
  pgdata:

networks:
  sso-net:
```

? ??

```
docker compose up -d
```

? ??Keycloak?? AD? shuncom.local?

□□□

```
http://192.168.4.16:8081
```

? ?? LDAP

□□□

```
User Federation → LDAP
```

? ????????

□□	□
Vendor	Active Directory
Connection URL	ldap://192.168.0.5
Bind DN	CN=Administrator,CN=Users,DC=shuncom,DC=local
Bind Password	AD□□
Users DN	DC=shuncom,DC=local
Username LDAP attribute	sAMAccountName

? ??

- Import Users = ON
- Sync Registrations = ON
- Trust Email = ON□□□□

? ??

点击:

```
Test connection
Test authentication
```

必须全部 ✔

? ???? RAGFlow Client?OIDC?

Keycloak:

```
Clients → Create
```

? ??

项目	值
Client ID	ragflow
Protocol	openid-connect
Access Type	confidential

? Redirect URI??????

```
http://192.168.4.16:9380/*
```

? ?? Secret

```
Credentials → Client Secret
```

? ??RAGFlow Docker ??????

修改你的 `.env`:

```
AUTH_TYPE=oauth2

OAUTH_PROVIDER=keycloak
OAUTH_CLIENT_ID=ragflow
OAUTH_CLIENT_SECRET=xxxxxxxx

OAUTH_AUTH_URL=http://192.168.4.16:8081/realms/shuncom/protocol/openid-connect/auth
OAUTH_TOKEN_URL=http://192.168.4.16:8081/realms/shuncom/protocol/openid-connect/token
OAUTH_USERINFO_URL=http://192.168.4.16:8081/realms/shuncom/protocol/openid-connect/userinfo

OAUTH_REDIRECT_URI=http://192.168.4.16:9380/oauth/callback
```

? ????????

```
用户访问 RAGFlow
         ↓
跳转 Keycloak
         ↓
输入 AD账号密码
         ↓
Keycloak LDAP验证 AD
         ↓
返回 Token
         ↓
RAGFlow登录成功
```

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

? 1. ????????

```
timedatectl set-ntp true
```

? 2. Keycloak????hostname

```
KC_HOSTNAME=192.168.4.16
KC_PROXY=edge
```

? 3. ???????????

确认：

- 9380端口开放
- firewall关闭或放行

? 4. AD??????

建议：

AD字段	Keycloak
sAMAccountName	username
mail	email

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

如果你要企业级：

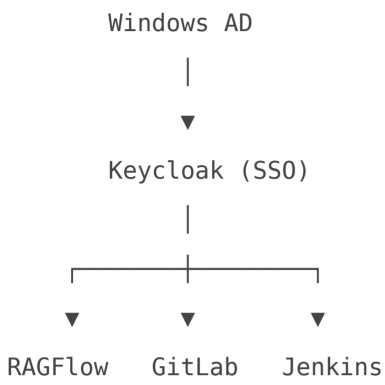
? 1. AD Group ? RAGFlow Role??

? 2. ???SSO?GitLab / Jenkins?

? 3. Keycloak HA????

? 4. LDAP Failover

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



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

1. □ Keycloak没数据库（你之前已经踩过）
2. □ □ start-dev
3. □ Redirect URI写错
4. □ AD LDAP Bind DN错误
5. □ □□□□□□□ token失败

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

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

? RAGFlow OIDC ??????

? Nginx HTTPS + SSO??

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

只要你说一句：

□□ “我要生产级 **SSO**完整落地”

我可以直接给你一套“复制就能跑”的最终版本。

Revision #1
Created 27 June 2026 11:33:40 by Admin
Updated 27 June 2026 11:35:35 by Admin