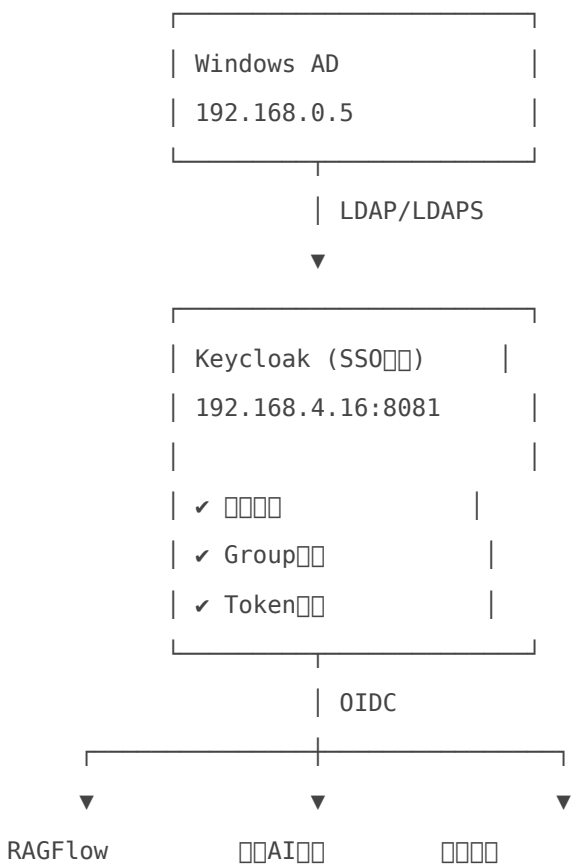


?? SSO?AD ? Keycloak ? RAGFlow???????

下面给你一套企业级 **SSO（AD → Keycloak → RAGFlow）**完整生产方案，目标是:

> ✔ AD账号即开即用登录
> ✔ 自动创建 RAGFlow用户
> ✔ AD组 → 角色 → 权限全映射
> ✔ 支持离职禁用、权限收敛
> ✔ 可扩展多系统统一 SSO

我按“可落地生产标准”给你拆 4 层架构。

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

```
        ┌──────────────────────┐
        │ Windows AD           │
        │ 192.168.0.5          │
        └─────────┬────────────┘
                  │ LDAP/LDAPS
                  ▼
        ┌──────────────────────┐
        │ Keycloak (SSO中台)    │
        │ 192.168.4.16:8081    │
        │                      │
        │ ✔ 用户同步            │
        │ ✔ Group管理          │
        │ ✔ Token签发          │
        └─────────┬────────────┘
                  │ OIDC
     ┌────────────┼───────────────┐
     ▼            ▼               ▼
  RAGFlow      其他AI系统        运维平台
```

（你的系统）

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

? ????Identity?

- AD 作为唯一身份源
- Keycloak 做统一身份中心

? ????Authentication?

- OIDC（标准　　OAuth2）
- Token JWT

? ????Authorization?

- AD Group → Keycloak Role
- Role → RAGFlow 权限

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

- 自动创建用户
- 自动禁用离职账号
- 自动同步组织架构

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

1?? LDAP ?? AD???????

```
User Federation → LDAP
```

????

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

2?? ??????????

```
Periodic Full Sync: 1h
Periodic Changed Users Sync: 10min
```

3?? ??????????

```
Import Users = ON
```

??AD Group ? ??????????

3?? AD??????

```
IT_Admins
AI_Users
AI_ReadOnly
Security_Team
```

4?? Keycloak Group ??

LDAP Mapper:

- group-ldap-mapper
- memberOf

5?? ??????

AD Group	Keycloak Role	RAGFlow权限
IT_Admins	ragflow-admin	全权限
AI_Users	ragflow-user	创建 /查询
AI_ReadOnly	ragflow-reader	只读

??Keycloak ? Token ????????

6?? Client Mapper??????

Client: ragflow

Mapper 1?email?????ID?

```
email → email
```

Mapper 2?groups????

```
groups → groups
```

Mapper 3?roles

```
realm roles → roles
```

Token?????

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

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

7?? docker-compose ????

□□□□□□□□□□

```
environment:
  - AUTH_TYPE=oauth2
  - OAUTH2_ENABLE=True
  - OAUTH2_TYPE=oidc

  - 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
  - AUTO_CREATE_USER=true
```

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

8?? ????

RAGFlow □□□

```
User
 ├── role
 │    ├── admin
 │    ├── user
 │    └── reader
 ├── group
 │    ├── AI_Users
 │    └── IT_Admins
```

9?? ????

Keycloak□□	**RAGFlow□□**
groups	role group
roles	permission
email	user identity

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

10?? ????

```
AD登录
 ↓
Keycloak认证
 ↓
返回JWT
 ↓
RAGFlow解析 email
 ↓
查用户表
 ↓
不存在 → 自动创建
 ↓
绑定 role/group
```

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

? 1. ??????

Keycloak LDAP:

```
User Disabled = AD disabled
```

? 2. ??????

用户离开 AD group → 自动降权

? 3. ???SSO??

同一 Keycloak:

- RAGFlow
- Jenkins
- GitLab

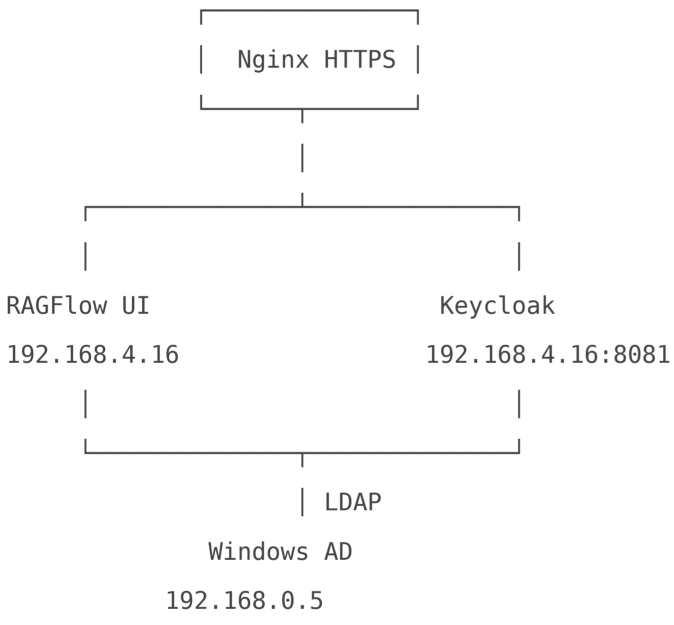
- 运维平台
- 内部 AI Agent

? 4. HTTPS????

生产必须加:

```
Nginx + SSL
```

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



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

你会得到:

? ????????

? AD??????

? ??????

? AD???????

? ???SSO??

? ???????

? ????????

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

我可以继续帮你做更高级企业能力：

? AD??????????RAGFlow??

? ?????????AI???

? API?RBAC????

? ???? + ????

? LDAP???????AD?

只要你说一句：

> “升级多租户 + 权限审计”

我可以帮你把这一套直接升级成完整企业 **AI** 平台身份体系。

Revision #1
Created 29 June 2026 07:45:53 by Admin
Updated 29 June 2026 07:46:08 by Admin