RAGFlow + Keycloak ??? HTTPS ??????

下面给你一套 **RAGFlow + Keycloak** 生产级 **HTTPS** 标准接入方案（可落地）。我按“正确架构 → Keycloak → Nginx → RAGFlow → 验证步骤”完整给你一步一步拆开。

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

推荐结构：

```
Browser
   ↓ HTTPS (443)
Nginx (TLS终止)
   ↓ HTTP 内网
RAGFlow (9380)
Keycloak (8081)
PostgreSQL
```

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

必须统一三点：

? 1. ???? HTTPS

? 2. ???? HTTP

? 3. Keycloak ???? X-Forwarded headers

???????? HTTPS?Nginx?

1. ???????????

```
cd /home/shuncom/ragflow-main/docker

mkdir -p /nginx/ssl

openssl req -x509 -nodes -days 365 \
  -newkey rsa:2048 \
  -keyout ./nginx/ssl/key.pem \
  -out ./nginx/ssl/cert.pem \
  -subj "/CN=192.168.4.16"
```

---

2. Nginx HTTPS ??????

```
server {
    listen 80;
    server_name 192.168.4.16;
    return 301 https://$host$request_uri;
}

server {
    listen 443 ssl;
    server_name 192.168.4.16;

    ssl_certificate     /etc/nginx/ssl/cert.pem;
    ssl_certificate_key /etc/nginx/ssl/key.pem;

    # ========================
    # RAGFlow □□
    # ========================
    root /ragflow/web/dist;

    location / {
```

```
        try_files $uri $uri/ /index.html;
    }

    # ========================
    # RAGFlow API
    # ========================
    location ^~ /api/ {
        proxy_pass http://127.0.0.1:9380;
        include proxy.conf;

        proxy_set_header X-Forwarded-Proto https;
    }

    location ^~ /v1/ {
        proxy_pass http://127.0.0.1:9380;
        include proxy.conf;

        proxy_set_header X-Forwarded-Proto https;
    }

    location ^~ /api/v1/admin {
        proxy_pass http://127.0.0.1:9381;
        include proxy.conf;
    }

    # ========================
    # Keycloak □□□□□□
    # ========================
    location /auth/ {
        proxy_pass http://127.0.0.1:8081/;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-Proto https;
        proxy_set_header X-Forwarded-Port 443;
    }
}
```

??????Keycloak HTTPS ????????

□□ docker-compose□

```
keycloak:
  image: quay.io/keycloak/keycloak:24.0
  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

    # =========================
    # □□HTTPS/□□□□
    # =========================
    KC_PROXY: edge
    KC_PROXY_HEADERS: xforwarded

    KC_HTTP_ENABLED: "true"
    KC_HOSTNAME: 192.168.4.16
    KC_HOSTNAME_STRICT: "false"
    KC_HOSTNAME_STRICT_HTTPS: "false"

    KC_HOSTNAME_PORT: 443

  ports:
    - "8081:8080"
```

??????RAGFlow OIDC ??

 `service_conf.yaml.template`

```
oauth:
  oidc:
    display_name: "SSO Login"
    client_id: "ragflow"
    client_secret: "xxx"

    issuer: "https://192.168.4.16/auth/realms/shuncom"

    scope: "openid email profile"

    redirect_uri: "https://192.168.4.16/api/v1/auth/login/oidc"
```

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

 Keycloak □□□□

Client ???

? Valid Redirect URIs????

```
https://192.168.4.16/api/v1/auth/login/oidc
```

□□□□□□□

```
https://192.168.4.16/*
```

? Web Origins

```
https://192.168.4.16
```

? Access Type

```
confidential
```

? Standard Flow

```
ON
```

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

? ?1???? HTTP / HTTPS

必须统一:

- □ http://192.168.4.16
- ✔ https://192.168.4.16

? ?2?Keycloak ???? X-Forwarded-Proto

否则 cookie 会错:

```
Secure cookie rejected
```

? ?3?redirect_uri ?? HTTPS

??????????

1. ?? HTTPS

```
curl -k https://192.168.4.16
```

2. ?? Keycloak

```
https://192.168.4.16/auth
```

3. ?? OIDC

登录:

```
https://192.168.4.16
```

??????????

你之前的问题全部来自:

> “ Keycloak + Nginx 没统– HTTPS scheme（ X-Forwarded-Proto错误）

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

```
Nginx（HTTPS）
   ↓
Keycloak（HTTP 内网）
   ↓
RAGFlow（HTTP 内网）
```

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

我可以帮你直接升级成：

? ???SSO??????

包含：

- HTTPS + Nginx标准配置
- Keycloak OIDC 完整修复
- RAGFlow 登录不循环
- AD/LDAP自动同步
- 角色映射
- 多域名 SSO

只要你说一句：

> “做企业级 SSO最终生产架构”

我可以直接给你一套 可以上线用的完整配置（避免你现在所有坑）。

Revision #3
Created 1 July 2026 09:41:04 by Admin
Updated 1 July 2026 09:58:51 by Admin