Go-SyncFlow 统一身份同步与管理平台 Unified Identity Sync & Management

Platform

文档版本 v3.0

更新日期 2026-02-09

文档状态 正式发布

本文档为系统自动生成，内容随版本迭代持续更新

目　录

Contents

1 Go-SyncFlow 统一身份同步与管理平台 - 技术架构文档

版本：v3.0 | 更新日期：2026-02-09

1.1 一、系统概述

Go-SyncFlow 是一套企业级统一身份同步与管理平台，提供用户全生命周期管理、多源身份同步、目录服务、消息通知和安全管控能力。

系统采用”上游同步 → 本地管理 → 下游同步”的三级架构：- **上游同步**：从 IM 平台（钉钉/企业微信/飞书/WeLink）、LDAP/AD、多种数据库同步用户到本地 - **本地管理**：统一的用户、群组、角色管理，配合密码策略和通知机制 - **下游同步**：将本地用户同步到 LDAP/AD、多种数据库

1.1.1 核心能力

能力	说明
上游同步	IM 平台（钉钉/企微/飞书/WeLink）、LDAP/AD、MySQL/PostgreSQL/Oracle/SQL Server/SQLite
下游同步	LDAP/AD、MySQL/PostgreSQL/Oracle/SQL Server 连接器，事件驱动 + 定时同步
统一认证	本地账号 + SSO 免登（钉钉/飞书/企微），JWT 令牌，AppID/AppKey 开放认证
统一授权	RBAC 权限模型，角色自动分配，角色布局定制（侧边栏/首页）
目录服务	内嵌 LDAP/LDAPS 服务器，默认支持 Samba 属性（兼容群晖 NAS）
消息通知	短信（12 家服务商）、邮件、Webhook、钉钉工作通知，消息策略路由
安全管理	密码策略、IP 黑白名单、账号/IP 锁定、会话管理、告警规则

能力	说明
日志管理	系统日志（登录 + 操作合并）、同步日志（区分上下游方向）、API 调用日志，可配置保留策略

1.2 二、技术栈

1.2.1 后端

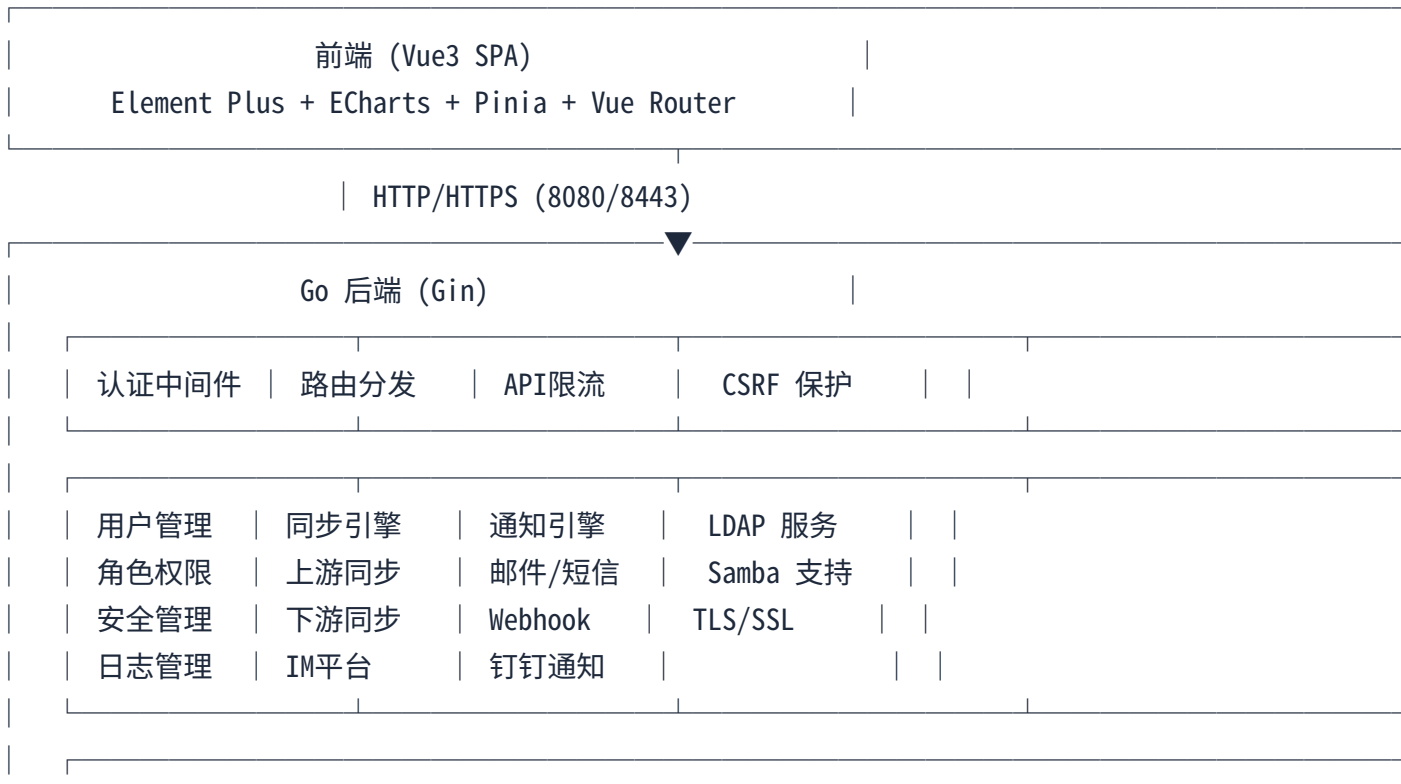
组件	技术	版本
编程语言	Go	1.22+
Web 框架	Gin	v1.10.0
ORM	GORM	v1.25.11
数据库	SQLite	via gorm sqlite driver v1.5.6
LDAP 服务端	gldap	v0.1.14
LDAP 客户端	go-ldap/ldap	v3.4.12
JWT	golang-jwt	v5.2.2
加密	golang.org/x/crypto	v0.45.0
系统监控	gopsutil	v3.24.5
MySQL 驱动	go-sql-driver/mysql	v1.9.3
PostgreSQL 驱动	lib/pq	v1.11.1
SQL Server 驱动	microsoft/go-mssqldb	v1.9.6
Oracle 驱动	sijms/go-ora	v2.9.0
中文拼音	mozillazg/go-pinyin	v0.21.0
WebSocket	gorilla/websocket	v1.5.3

1.2.2 前端

组件	技术	版本
框架	Vue 3	v3.4.38
构建	Vite	v5.4.1
UI 库	Element Plus	v2.7.8
图表	ECharts	v5.5.1
状态	Pinia	v2.2.2
路由	Vue Router	v4.4.3
HTTP	Axios	v1.7.9
PDF 导出	html2pdf.js	v0.14.0
语言	TypeScript	v5.5.4

1.3 三、系统架构

1.3.1 3.1 整体架构



1.3.2 3.2 上游同步架构

上游同步实现从外部数据源同步用户到本地系统：

1. **连接器（Connector）**：配置上游数据源的连接参数
   - IM 平台连接器：钉钉、企业微信、飞书、WeLink
   - LDAP/AD 连接器：标准 LDAP 和 Active Directory
   - 数据库连接器：MySQL、PostgreSQL、SQL Server、Oracle、SQLite
2. **同步规则（SyncRule）**：定义同步行为
   - 触发方式：手动 / 定点时间 / 固定间隔
   - 属性映射：源属性 → 本地属性，支持直接映射和转换规则
   - 用户匹配：根据配置的匹配字段识别已有用户
3. **属性映射（SyncAttributeMapping）**：精细控制字段转换
   - 直接映射：源字段直接对应目标字段
   - 转换规则：中文转拼音、邮箱前缀、手机号、IM UserID 等
4. **变更检测**：数据库上游支持基于时间戳字段的变更轮询

1.3.3 3.3 下游同步架构

下游同步将本地用户推送到外部目标系统：

1. **连接器**：配置下游目标的连接参数（LDAP/AD、数据库）
2. **同步规则**：事件驱动 + 定时同步
3. **属性映射**：本地属性 → 目标属性
   - 支持转换规则：中文姓氏/名字提取、密码转 Unicode（AD）、状态转 UAC 等

1.3.4 3.4 内嵌 LDAP 服务

- 协议支持：LDAP (389) + LDAPS (636)
- 目录结构：BaseDN → Groups/Users/Roles
- Samba 支持（默认启用）：
  - sambaSamAccount、sambaGroupMapping、sambaDomain objectClass
  - 自动生成 SID、NT Hash（MD4）
  - 支持群晖 NAS LDAP 认证对接
- 认证方式：管理员 Bind DN + 只读账号 Bind DN

1.4 四、目录结构

```
Go-SyncFlow/
├── backend/
│   ├── main.go                    # 入口
│   ├── go.mod / go.sum            # Go 依赖
│   ├── internal/
│   │   ├── handlers/               # HTTP 处理器
│   │   │   ├── router.go           # 路由定义
│   │   │   ├── auth.go             # 认证（登录/SSO/忘记密码）
│   │   │   ├── user.go             # 用户管理
│   │   │   ├── role.go             # 角色管理
│   │   │   ├── group.go            # 群组管理
│   │   │   ├── sync_upstream.go    # 上游同步
│   │   │   ├── sync_downstream.go  # 下游同步
│   │   │   ├── connector.go        # 连接器管理
│   │   │   ├── synchronizer.go     # 同步器管理
│   │   │   ├── ldap.go             # LDAP 设置
│   │   │   ├── notify.go           # 通知系统
│   │   │   ├── logs.go             # 日志管理
│   │   │   ├── settings.go         # 系统设置
│   │   │   ├── security.go         # 安全中心
│   │   │   ├── api_keys.go         # API 密钥
│   │   │   └── dingtalk.go         # 钉钉集成
│   │   ├── models/                 # 数据模型
│   │   │   ├── user.go             # User/Group 模型
│   │   │   ├── role.go             # Role/Permission 模型
│   │   │   ├── connector.go        # Connector/SyncRule/SyncAttributeMapping
```

```
│   │   │   ├── config.go            # 系统配置模型
│   │   │   ├── notify.go            # 通知模型
│   │   │   └── log.go               # 日志模型
│   │   ├── storage/                 # 数据存储
│   │   │   └── db.go                # 数据库初始化与迁移
│   │   ├── sync/                    # 同步引擎
│   │   │   └── engine.go            # 下游同步核心逻辑
│   │   ├── sms/                     # 短信服务商
│   │   │   ├── provider.go          # Provider 接口
│   │   │   ├── aliyun.go            # 阿里云短信
│   │   │   ├── tencent.go           # 腾讯云短信
│   │   │   └── ...                  # 其他12家服务商
│   │   ├── ldapserver/              # 内嵌 LDAP 服务
│   │   │   ├── server.go            # LDAP 服务主体
│   │   │   ├── schema.go            # 目录条目构建
│   │   │   └── samba.go             # Samba MD4/SID
│   │   ├── dingtalk/                # 钉钉 SDK
│   │   └── im/                      # IM 平台抽象
│   │       ├── client.go           # IMClient 接口
│   │       ├── dingtalk.go         # 钉钉实现
│   │       ├── wechatwork.go       # 企业微信实现
│   │       ├── feishu.go           # 飞书实现
│   │       └── welink.go           # WeLink 实现
│   ├── data/                        # 运行时数据（数据库/密钥）
│   ├── certs/                       # TLS 证书
│   └── static/                      # 前端静态文件
├── frontend/
│   ├── src/
│   │   ├── api/index.ts             # API 定义
│   │   ├── router/index.ts          # 路由配置
│   │   ├── store/user.ts            # Pinia 状态
│   │   ├── layouts/MainLayout.vue   # 主布局
│   │   └── views/
│   │       ├── Login.vue            # 登录页（含SSO）
│   │       └── admin/               # 管理页面
│   │           ├── Users.vue        # 用户管理
│   │           ├── Roles.vue        # 角色管理
│   │           ├── UpstreamSync.vue # 上游同步
│   │           ├── DownstreamSync.vue# 下游同步
```

```
│   │           ├──── Synchronizers.vue # 同步器
│   │           ├──── LDAPSettings.vue  # LDAP 设置
│   │           ├──── NotifyChannels.vue# 通知渠道
│   │           ├──── Security.vue      # 安全中心
│   │           ├──── ApiDocs.vue       # API 文档
│   │           └──── ...               # 其他页面
│   ├──── package.json
│   └──── vite.config.ts
├──── scripts/
│   ├──── start.sh                      # 一键启动
│   ├──── stop.sh                       # 停止服务
│   ├──── reset-admin.sh                # 重置管理员密码
│   └──── pack.sh                       # 打包脚本
├──── docs/                             # 系统文档
│   ├──── 技术架构文档.md / .pdf
│   ├──── 系统使用手册.md / .pdf
│   ├──── API接口文档.md / .pdf
│   └──── template.tex                  # PDF 生成模板
├──── tooling/                          # 部署工具包
└──── README.md
```

1.5 五、数据库设计

1.5.1 5.1 核心表

表名	说明	主要字段
users	用户表	id, username, password, nickname, email, phone, status, group_id, source, im_user_id, samba_nt_password
groups	群组/部门表	id, name, parent_id, remote_dept_id, source
roles	角色表	id, name, code, permissions, layout_config
user_roles	用户角色关联	user_id, role_id

表名	说明	主要字段
connectors	连接器	id, name, type, direction, host, port, im_* 字段, status
sync_rules	同步规则	id, name, connector_id, direction, schedule_type, schedule_time, enable_event
sync_attribute_mapping	属性映射	id, sync_rule_id, object_type, source_attribute, target_attribute, mapping_type, transform_rule

1.5.2 5.2 通知相关表

表名	说明
notify_channels	通知渠道（邮件/短信/Webhook/钉钉）
message_templates	消息模板
alert_rules	告警规则
message_policies	消息策略（消息类型 → 渠道映射）

1.5.3 5.3 日志表

表名	说明
login_logs	登录日志
operation_logs	操作日志
sync_logs	同步日志
security_events	安全事件
api_access_logs	API 调用日志

1.5.4 5.4 安全表

表名	说明
api_keys	API 密钥（AppID/AppKey/IP 白名单）
system_configs	系统配置键值对

1.6 六、API 架构

1.6.1 6.1 认证方式

方式	适用场景	请求头
JWT 令牌	Web 浏览器登录	`Authorization: Bearer <token>`
AppID/AppKey	第三方系统集成	`X-App-ID` + `X-App-Key`

1.6.2 6.2 路由分组

前缀	说明	认证方式
/api/auth/*	认证相关	无需认证
/api/*	管理 API	JWT
/api/open/*	开放 API	AppID/AppKey

1.6.3 6.3 中间件链

```
请求 → RateLimiter → CORSHandler → AuthMiddleware → PermissionCheck → Handler → Response
                                        ↓ (开放API)
                                  APIKeyAuthMiddleware
```

1.7 七、安全设计

1.7.1 7.1 密码安全

- 存储：bcrypt 哈希（cost=10）

- 传输：RSA 公钥加密（浏览器登录）
- 策略：可配置最小长度、复杂度要求、过期时间
- Samba：自动生成 NT Hash（MD4）用于 LDAP Samba 认证

1.7.2 7.2 会话管理

- JWT 令牌，可配置过期时间
- CSRF Token（一次性使用，用于登录）
- 单点登录：支持钉钉/飞书/企微 SSO

1.7.3 7.3 访问控制

- RBAC 权限模型
- 角色布局定制（隐藏侧边栏菜单、设定默认首页）
- IP 白名单/黑名单（全局 + API Key 级别）
- 登录失败锁定（账号/IP 锁定策略）

1.7.4 7.4 API 安全

- AppID/AppKey 认证，Key 以 SHA256 哈希存储
- 支持 IP 白名单/黑名单绑定
- API 调用日志记录

1.8 八、部署架构

1.8.1 8.1 运行环境

- 操作系统：Linux（Ubuntu 20.04+ / CentOS 7+）
- Go 1.22+（编译时需要）
- 内存：≥ 2GB
- 磁盘：≥ 10GB

1.8.2 8.2 服务端口

服务	端口	说明
HTTP	8080	Web 访问
HTTPS	8443	加密 Web 访问
LDAP	389	目录服务
LDAPS	636	加密目录服务

服务	端口	说明

1.8.3 8.3 一键部署

```
tar -xzf go-syncflow-XXXXXX.tar.gz -C /opt/
cd /opt/Go-SyncFlow
chmod +x scripts/*.sh
./scripts/start.sh          # 编译 + 部署 + 启动
./scripts/stop.sh           # 停止
./scripts/reset-admin.sh    # 重置管理员密码
```

1.8.4 8.4 systemd 管理

```
systemctl status go-syncflow
systemctl restart go-syncflow
journalctl -u go-syncflow -f
```

1.9 九、IM 平台对接

1.9.1 9.1 支持平台

平台	上游同步	SSO 免登	消息通知
钉钉	支持	支持	支持
企业微信	支持	支持	计划中
飞书	支持	支持	计划中
WeLink	支持	计划中	计划中

1.9.2 9.2 同步流程

1. 配置 IM 平台连接器（AppID/AppSecret/CorpID 等）
2. 创建上游同步规则，配置触发方式
3. 自定义属性映射（默认映射自动生成）
4. 执行同步：拉取 IM 平台用户/部门 → 创建/更新本地用户和群组
5. 同步完成后可自动触发下游同步（事件驱动）

1.9.3 9.3 用户名生成规则

规则	说明
pinyin	中文姓名转拼音（重名自动加数字后缀）
email_prefix	邮箱 @ 前的部分
mobile	手机号
email	完整邮箱
userid	IM 平台原始 UserID

1.10 十、通知系统

1.10.1 10.1 渠道类型

类型	说明
邮件	SMTP 协议，支持 TLS
短信	12 家服务商（阿里云、腾讯云、华为云、百度云等）
Webhook	HTTP POST，支持 HMAC-SHA256 签名
钉钉工作通知	钉钉 API 工作消息

1.10.2 10.2 消息策略

消息策略定义”消息类型 → 渠道”的映射关系，支持全局策略和群组级策略。

可用消息类型：密码重置验证码、安全告警、账号变更通知、新用户通知等。

1.11 十一、短信服务商

编号	服务商	Provider Key
1	阿里云	aliyun
2	腾讯云	tencent
3	华为云	huawei
4	百度云	baidu
5	中国移动	cmcc
6	容联云	rongcloud
7	云之讯	yunzhixun
8	网易云信	netease
9	螺丝帽	luosimao
10	Twilio	twilio
11	七牛云	qiniu
12	梦网科技	mengwang