堡垒机 V2.0 版系统手册

Author：wangsong

一 功能说明：

堡垒机 v2.0 是基于 paramiko 与 sqlalchemy 模块进行开发,系统设计采用三层架构模式。

开发环境: Ubuntu + python3.4 + mysql

功能模块包括：

1 系统数据库初始化模块

2 管理员后台模块：添加主机组、添加主机、添加系统登录用户、添加主机用户

(修改及查询功能暂未实现)

3 普通用户登录并访问远程机器

4 系统审计(日志模块),记录用户登录/登出、访问服务器、执行命令日志

二 目录结构：

```
├─── bin                          程序主文件目录
│    ├─── initdb.py                  初始化数据库模块
│    └─── main.py                    程序引导文件
├─── bll                          业务逻辑处理层
│    ├─── groups.py                  主机组处理模块
│    ├─── hosts.py                   主机处理模块
│    ├─── login_user.py              系统登录用户处理模块
│    ├─── op_log.py                  日志操作模块
│    └─── ssh_user.py                主机登录用户处理模块
├─── conf                         系统配置目录
│    └─── settings.py                主配置文件
├─── dalhelper                    数据库访问层目录
│    └─── mysqlhelper.py             数据库访问模块
├─── doc                          文档目录
```

```
|   └── 数据字典.xlsx          数据字典表
├── logs                     系统日志目录
|   └── sys.log                系统异常日志文件
├── module                   系统模块目录
|   ├── admin.py               管理员后台管理模块
|   ├── common.py              公共函数模块
|   ├── interactive.py         主机 SSH 登录模块
|   ├── myexception.py         自定义异常类模块
|   └── tables.py              Sqlalchemy 数据表定义模块
├── raskey                   密钥保存目录
├── start.py                 主程序文件
└── template                 模板文件目录
    └── templates.py           模板文件
```

三 使用方法

1 系统执行方法

Python3 start.py

2 初始化数据库

1) 登录 mysql 数据库，手工创建一个数据库 baolei(自定义),字符集 utf-8,
2) 如果程序目录 conf 下存在 .dblck 文件，先删除该文件
3) 修改配置文件 conf/setting.py 修改数据库连接地址、端口、数据库名
4) 启动程序: python3 start.py
5) 系统提示初始化数据库,选择 y 系统自动创建所需数据表并初始化一个管理用户 admin
6) 用 admin / admin 登录系统

3 创建基础信息

用管理员登录后台，依次创建主机组、主机、主机 SSH 用户、系统登录用户

4 普通用户登录

普通用户登录系统后，能够查看到自己所能操作的所有主机信息，选择主机编号登录系统，如果该主机对应多个用户，选择一个登录

四 数据字典

bl_login_user （系统登录用户表）

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长ID
username	varchar(50)			Y	非空	登录用户名
password	varchar(50)				非空	密码(sha2加密)
name	varchar(50)					名字
role	varchar(50)	"user"			非空	角色(管理员or普通用户): admin / user
isdel	bool	0			非空	删除标识: 已删除 1/ 正常 0
expired	datetime				非空	用户过期时间(默认: 创建日期+1天)

bl_groups （ 主机组表）

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长组ID
groupname	varchar(20)				非空	组名

bl_hosts (主机表)

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长ID
hostname	varchar(20)			Y	非空	主机名
ipaddr	varchar(20)				非空	主机IP
sshport	int	22			非空	远程访问ssh端口

bl_ssh_users (主机SSH登录用户列表)

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长ID
hid	int		bl_hosts.id	Y		主机id
auth_type	int	1			非空	ssh方式：1 passwd登录 / 2 key登录
auth_user	varchar(50)			Y	非空	ssh登录用户
auth_key	varchar(50)				非空	ssh登录密码 or 密钥key文件(默认文件存放在程序sshkey目录下)

bl_r_host_group（主机及主机组关联关系表）

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长ID
hid	int		bl_hosts.id	Y	非空	对应主机id
gid	int		bl_groups.id	Y	非空	对应主机组id

bl_r_user_group (系统用户 及 主机组关联关系表)

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长ID
uid	int		bl_login_user.id	Y	非空	系统登录用户id
gid	int		bl_groups.id	Y	非空	主机组id

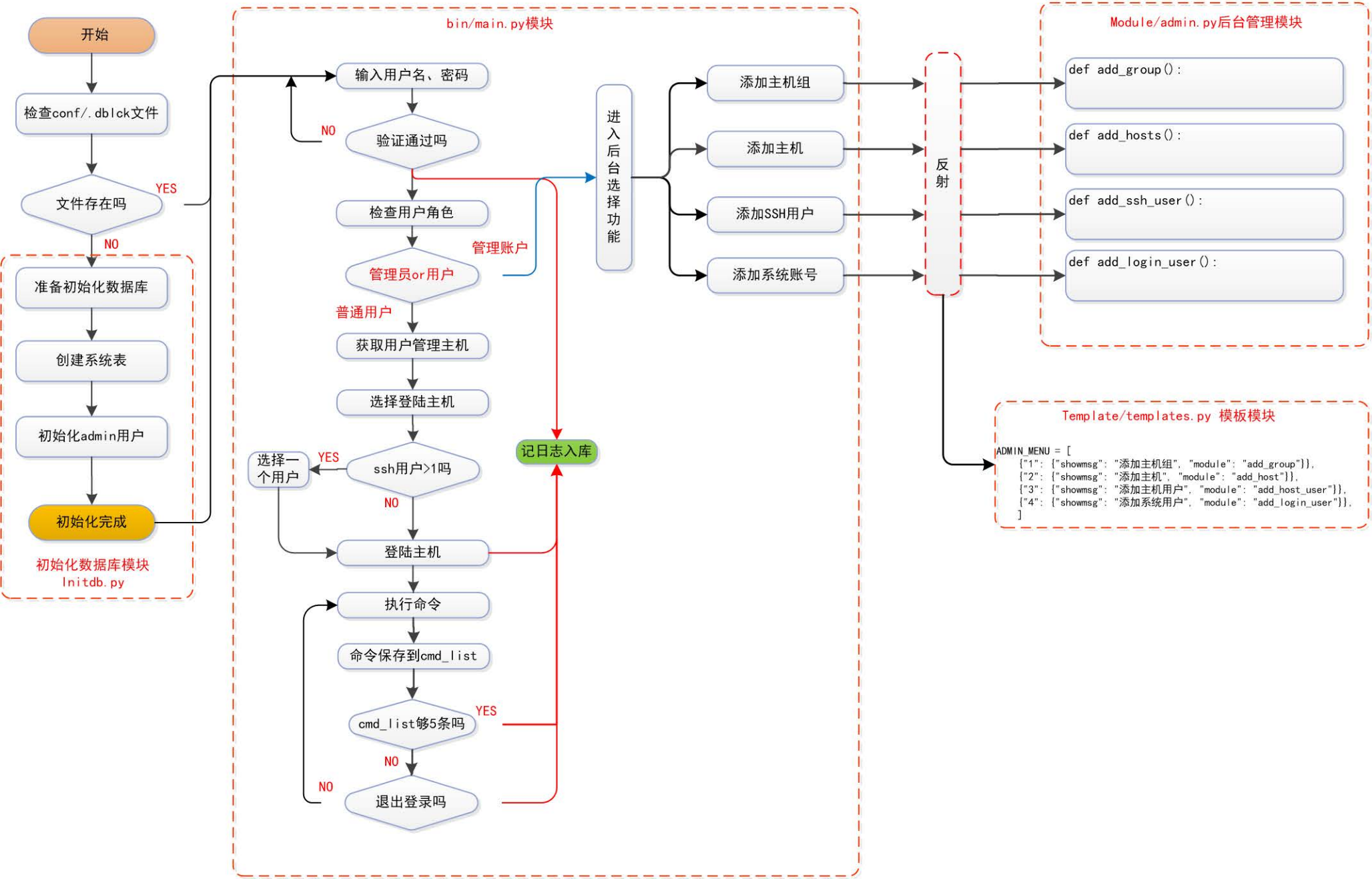
bl_r_user_sshuser (系统用户 及 主机组关联关系表)

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长ID
uid	int		bl_login_user.id	Y	非空	登录系统用户id
sid	int		bl_ssh_user.id	Y	非空	主机SSH用户id

bl_op_logs （用户操作日志表)

字段名	类型	默认值	外键	主键	Null	备注
id	int					自增长ID
uid	int		bl_login_user.id	Y	非空	登录用户id
opdate	datetime				非空	操作时间
optype	int				非空	操作类型：1 登入登出操作 2 执行命令
opmsg	varchar(500)					操作信息

五 系统功能图


开始
检查conf/.dblck文件
文件存在吗
YES
NO
准备初始化数据库
创建系统表
初始化admin用户
初始化完成
初始化数据库模块
Initdb.py
bin/main.py模块
输入用户名、密码
NO
验证通过吗
检查用户角色
管理账户
管理员or用户
普通用户
获取用户管理主机
选择登陆主机
选择一个用户
YES
ssh用户>1吗
NO
登陆主机
执行命令
命令保存到cmd_list
cmd_list够5条吗
YES
NO
退出登录吗
NO
记日志入库
进入后台选择功能
添加主机组
添加主机
添加SSH用户
添加系统账号
反射
Module/admin.py后台管理模块
def add_group():
def add_hosts():
def add_ssh_user():
def add_login_user():
Template/templates.py 模板模块
ADMIN_MENU = [
{"1": {"showmsg": "添加主机组", "module": "add_group"}},
{"2": {"showmsg": "添加主机", "module": "add_host"}},
{"3": {"showmsg": "添加主机用户", "module": "add_host_user"}},
{"4": {"showmsg": "添加系统用户", "module": "add_login_user"}},
]