银河麒麟迁移运维管理平台 V2.3
安全加固方案

麒麟软件有限公司

2026 年 1 月 8 日

目录

1 目的

本方案为银河麒麟迁移运维管理平台 V2.3 安全加固方案，目的在于提升平台安全性。

本文档适用范围为研发、产品、测试人员、售前技服等。未经书面许可，任何使用方不得随意扩大知悉范围，提供给上述规定对象以外的人员阅读或使用。

2 平台弱密码修改

2.1 redis 密码修改

Redis 服务默认密码修改：

1) 登录部署 redis 服务的机器，修改 redis 配置文件 redis.conf

vim /etc/redis/redis.conf //Qwer!234578 替换为自己所设密码

```
# The requirepass is not compatable with aclfile option and the ACL LOAD
# command, these will cause requirepass to be ignored.
#
# requirepass foobared
requirepass Qwer!234578
```

有下面的配置统一修改，两个密码保持一致

```
# replicaof <masterip> <masterport>

# If the master is password protected (using the "requirepass" configuration
# directive below) it is possible to tell the replica to authenticate before
# starting the replication synchronization process, otherwise the master will
# refuse the replica request.
#
# masterauth <master-password>
masterauth Qwer!234578
```

2) 修改 sentinel.conf 中密码

vim /etc/redis/redis-sentinel.conf

```
# sentinel auth-pass <master-name> <password>
sentinel auth-pass mymaster Qwer!234578
```

```
# format that is used inside redis.conf to describe users.
#
# aclfile /etc/redis/sentinel-users.acl

# requirepass <password>
requirepass Qwer!234578
#
```

3) 重启 redis 服务

systemctl restart redis

systemctl restart redis-sentinel

2.2 数据库密码修改

sudo -u postgres psql

SELECT rolname,rolpassword FROM pg_authid;

```
postgres=# SELECT rolname,rolpassword FROM pg_authid;
       rolname        |                                                   rolpassword
----------------------+------------------------------------------------------------------------------------------------------------------------------------------
 postgres             |
 pg_monitor           |
 pg_read_all_settings |
 pg_read_all_stats    |
 pg_stat_scan_tables  |
 pg_signal_backend    |
 kylin                | SCRAM-SHA-256$4096:9jbSqzT2kJOd8NfK3LVQVQ==$y9OyF/j4SANLAEM1//Cu2KAZs23vl3BTGh85AZqavr0=:iuVWSVXG7B1fPduxaqCIKhT+2SZFCiJyNT/uv3Kq+bI=
(7 rows)
```

kylin：用于后端连接数据库的账号，密码默认为 Qwer!234578

修改以下用户的密码信息：

#\password kylin

#SELECT rolname,rolpassword FROM pg_authid; //查看是否变更

```
postgres=# \password kylin
Enter new password:
Enter it again:
postgres=# SELECT rolname,rolpassword FROM pg_authid;
       rolname        |                                                   rolpassword
----------------------+------------------------------------------------------------------------------------------------------------------------------------------
 postgres             |
 pg_monitor           |
 pg_read_all_settings |
 pg_read_all_stats    |
 pg_stat_scan_tables  |
 pg_signal_backend    |
 kylin                | SCRAM-SHA-256$4096:T2znkxPrv9aYezioMih3iA==$CG9R0jGRNVZwbTBWpltn44tfeUt5zKIY+krDUGQX2+Q=:Doolz4chnj1OXgWVZJKNmgfb8sYRW+HixaJbFPbO6jQ=
(7 rows)
```

#postgres=# \q //退出

2.3 nacos 密码修改

2.3.1 nacos 访问密码修改

1) 登录部署 ismp-nacos 服务机器，修改/opt/ismp-nacos/conf/application.properties 中 db.password 为 2.2 中设置的数据库连接密码并重启 ismp-nacos 服务：

vim /opt/ismp-nacos/conf/application.properties

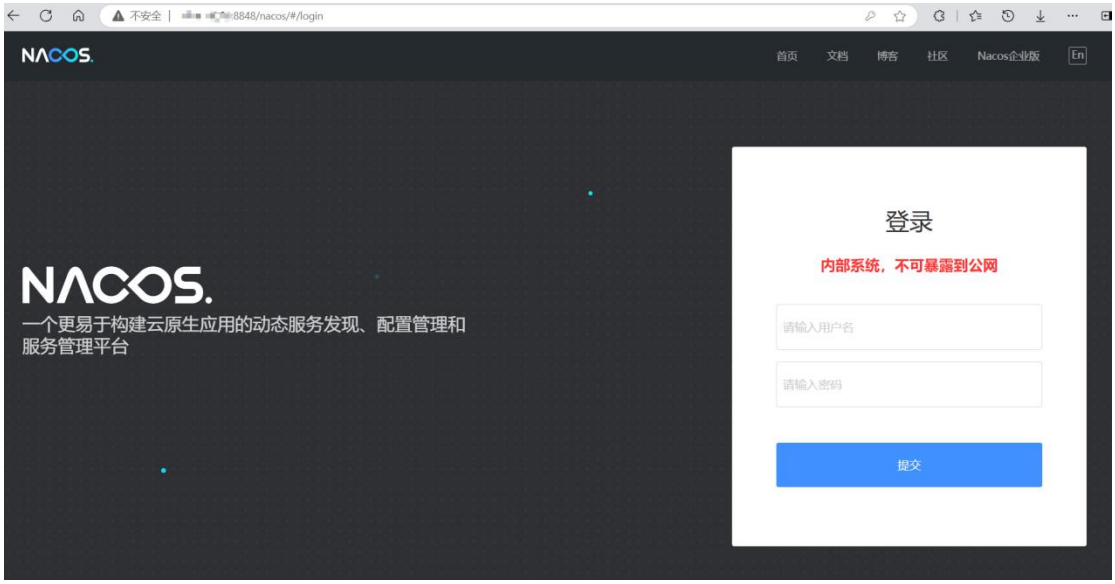
```
#*************** Config Module Related Configurations ***************#
### If use MySQL as datasource:
spring.datasource.platform=postgresql
### Count of DB:
db.num=1
### Connect URL of DB:
db.url.0=jdbc:postgresql://localhost:5432/nacos_config
db.user=kylin
db.password=Qwer!234578
```

systemctl restart ismp-nacos-standalone.service　//单机部署重启 nacos 服务

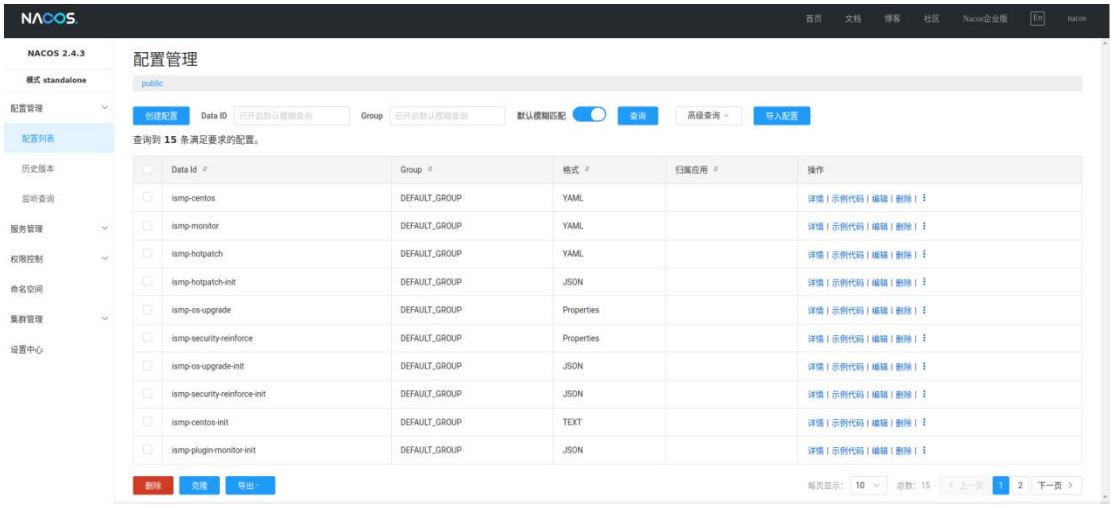
systemctl restart ismp-nacos-cluster.service　//高可用部署重启 nacos 服务

2)　登录 ismp-nacos 页面，登录方式如下：

浏览器输入：http://ip:8848/nacos，其中 ip 为部署 ismp-nacos 服务的机器的 ip，用户名为 nacos，默认密码为 Qwer!234578。



3)　登录进入 nacos 界面后，点击右上角 nacos，点击修改密码，如下图所示：

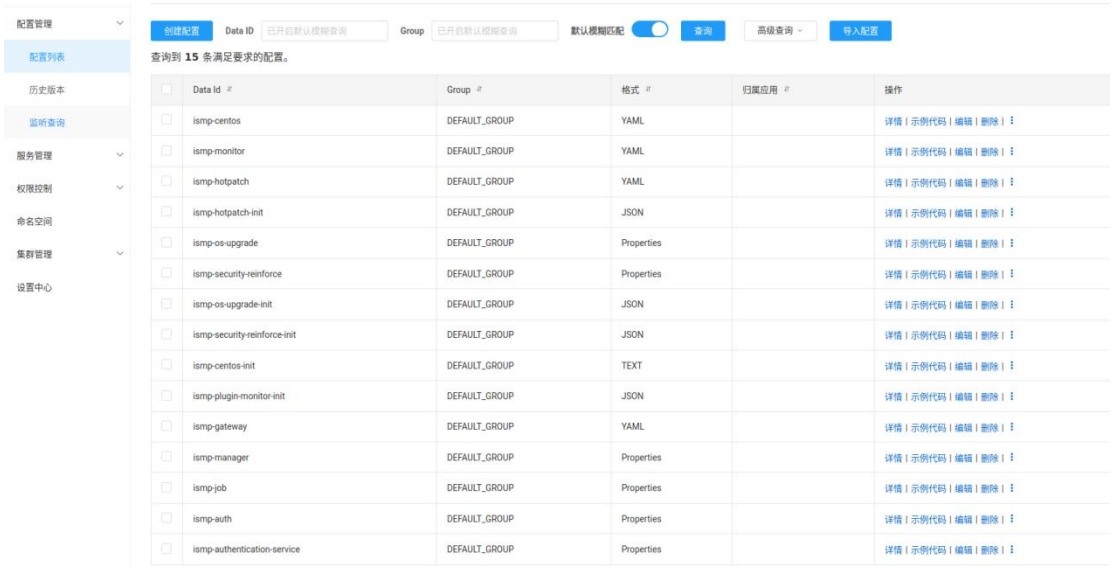


4) 在弹出窗口输入新密码并确认：

2.3.2 nacos 配置管理界面内的配置文件中密码修改

1) 通过 2.3.1 中方法登录 nacos 页面，如果已修改密码请使用新密码登录

2) 修改配置管理->配置列表下的配置(不包括 init 文件)，如下图所示：



以 ismp-manager 为例,修改密码为 2.1 或 2.2 章节修改的密码：

数据库密码配置项名称：

spring.datasource.password=Qwer!234578

spring.liquibase.password=Qwer!234578

缓存密码配置项名称：

spring.data.redis.password=Qwer!234578

注意：平台所有密码默认均为 Qwer!234578，修改时可通过 ctrl+f 搜索，然后根据配置项名称和上下行内容判断密码所属账号。

其他服务 ismp-gateway、ismp-auth、ismp-authentication-service、ismp-job、ismp-os-upgrade-service 、 ismp-centos 、 ismp-monitor 、 ismp-hotpatch 、 ismp-security-reinforce 等根据例子 ismp-manager 进行修改。最后 5 个为可选安装服务，如有安装部署则修改，反之略过。

2.4 本地连接 nacos 密码修改

以网关为例：

vim /opt/ismp-gateway/bootstrap.yml

```
server:
  port: 8888

spring:
  cloud:
    nacos:
      config:
        group: DEFAULT_GROUP
        file-extension: yaml
        #Nacos 地址
        server-addr: 127.0.0.1:8848
        enabled: true
        username: nacos
        password: Qwer!234578
      discovery:
        #Nacos 地址
        server-addr: 127.0.0.1:8848
        username: nacos
        password: Qwer!234578
  application:
    name: ismp-gateway
~
```

修改其中的 nacos 密码为 2.3 修改之后的，然后报错退出重启服务

systemctl restart ismp-gateway

systemctl status ismp-gateway

注：其他服务对应文件位置如下，且最后 5 个为可选安装服务，如有安装则修改，反之略过。

运维后端：/opt/ismp-manager/bootstrap.properties

用户：/opt/ismp-auth/bootstrap.properties

任务：/opt/ismp-job/bootstrap.properties

授权：/opt/ismp-authentication/bootstrap.properties

centos 迁移后端：/opt/ismp-centos/bootstrap.yml

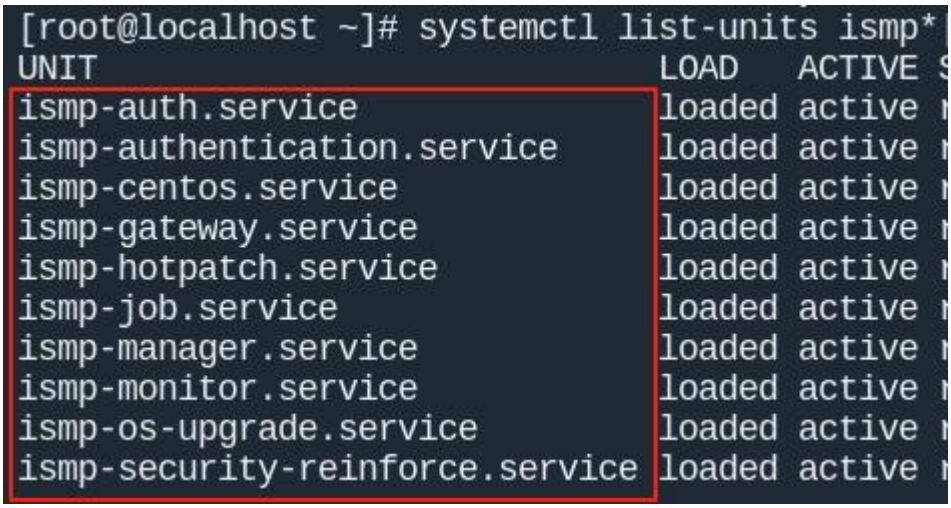
OS 升级后端：/opt/ismp-os-upgrade/bootstrap.properties

安全加固后端：/opt/ismp-security-reinforce/bootstrap.properties

监控后端：/opt/ismp-plugin-monitor/config.yaml

热补丁后端：/opt/ismp-hotpatch/config.yaml

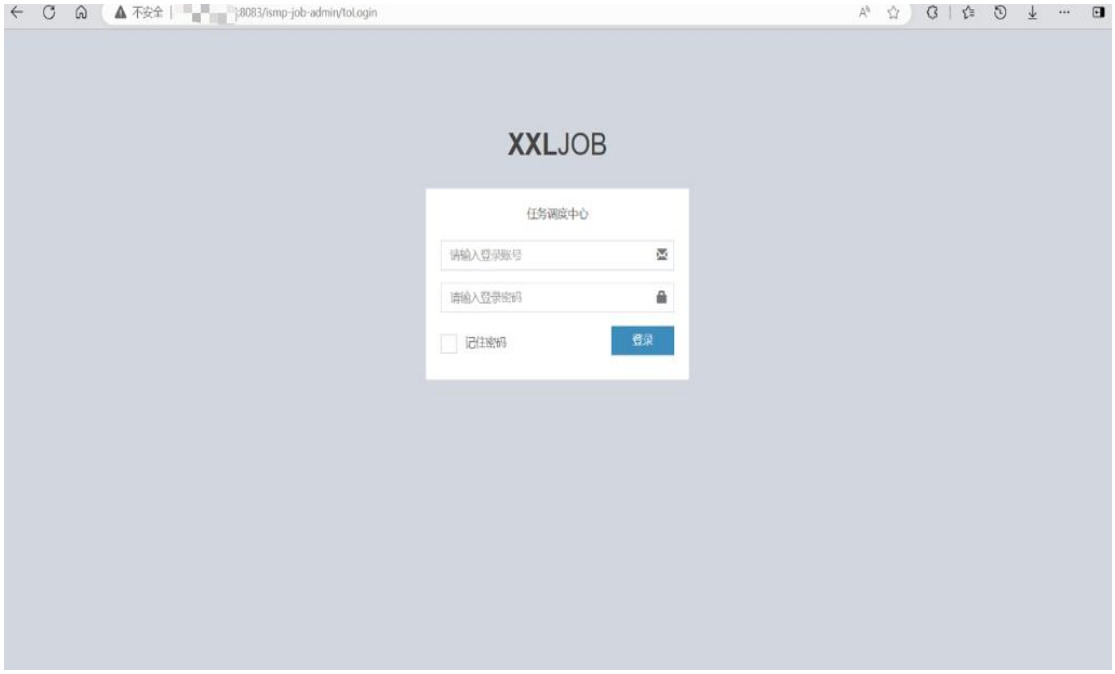
配置文件修改后需重启相应服务，下图为对应的 service 名称



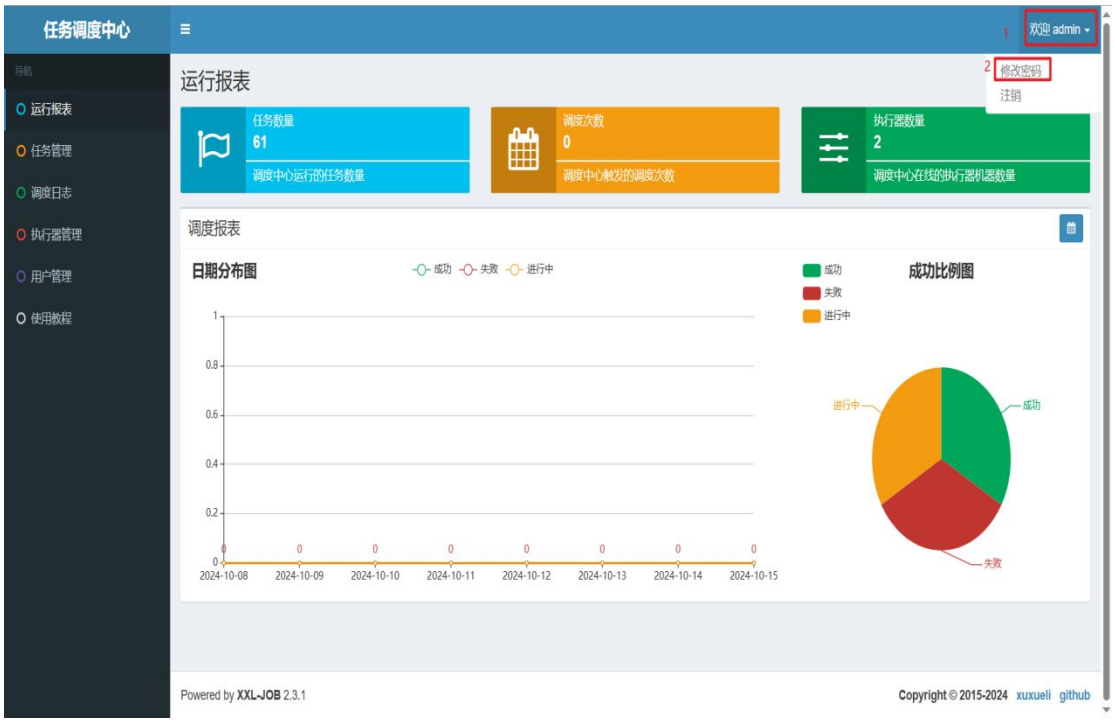
2.5 ismp-job 访问密码修改

1) 登录 job 页面，登录方式如下：

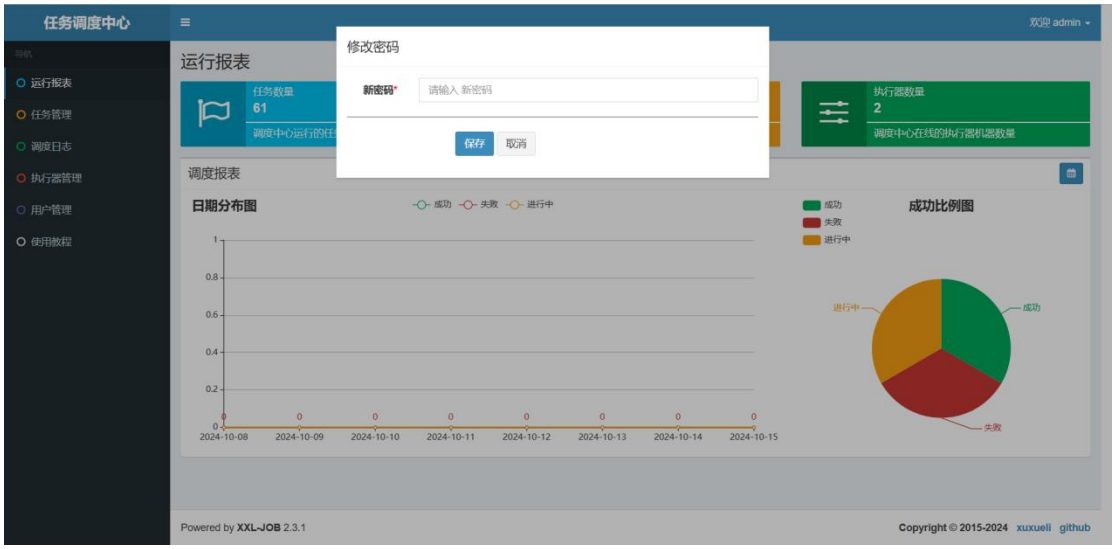
浏览器输入 http://ip:8083/ismp-job-admin，其中 ip 为部署 ismp-job 服务的机器的 ip，使用账号 admin，默认密码 Qwer!234578 登录：



2) 依次点击右上角“欢迎 admin”，“修改密码”：



3) 在弹出界面输入新密码并保存：



2.6 EMQX Dashboard 访问密码修改

管理控制台访问链接：http://emqx_ip:18083

默认账号 admin、密码 public，首次登录要求修改密码，如下图

也可以直接使用命令行修改管理控制台登录密码：

/opt/emqx/bin/emqx ctl admins passwd admin 'Qwer!234'

3 防火墙规则

3.1 打开机器防火墙服务

systemctl start firewalld.service　//登录服务端机器，打开防火墙

3.2 添加防火墙规则

单机环境：

服务器角色	开放端口	功能
服务端	9000	平台提供的软件源服务，用于补丁下发、软件包安装升级
	443	https 的端口，用于代理端安装注册
	8848	nacos 的反向代理
	1883	emqx 服务
	873	软件包仓库同步
	22	上传评估报告

分布式高可用环境：

服务端对外开放时，仅需将上面单机环境中的 1883 端口改为 8883 端口，其他配置保持不变。

如需同时开放内部及外部访问，请按下表端口进行配置。

服务器角色	开放端口	功能
前端服务	9000	平台提供的软件源服务，用于补丁下发、软件包安装升级
	22	用于上传迁移评估报告
	8883	emqx 反向代理端口
	443	https 的端口，用于代理端安装注册
	873	软件仓库同步
	8093	ismp-job 的反向代理端口
	8848、9848	六节点以上集群部署时 nacos 的反向代理、grpc 通信
	8847、9847	三节点集群部署时 nacos 反向代理 及 grpc 通信使用
	2049	nfs 共享存储
运维服务	8080	http 的端口，用于代理端安装注册
	8899	ismp-job 执行器

数据库服务	5432	数据库连接
缓存服务	6379	redis 连接
	26379	哨兵模式
消息队列服务	1883	mq 服务
注册与配置中心	8848	web 服务
	7848	Raft-rpc 通信
	9848、9849	grpc 通信
任务管理服务	8083	web 服务
网关	8888	web 服务
用户服务	8085 8086	用户服务
授权服务	8892 8893	授权服务
CentOS 迁移服务	9999 8889	Centos 迁移服务
热补丁服务	8188	热补丁服务
OS 升级服务	8890	OS 升级服务
安全加固服务	8886	安全加固服务
监控服务	8088 9010	监控服务

firewall-cmd --zone=public --add-port=443/tcp --permanent　//依次将 443 替换为上表中需要开放的端口，添加服务端需要开放的端口规则

firewall-cmd --reload　//重新加载防火墙

3.3 禁用 nacos 界面访问

nacos 中存储了平台各服务的 IP、端口和应用配置等信息，相关配置修改完成后，建议关闭 8848 端口的外部访问规则

firewall-cmd --zone=public --remove-port=8848/tcp --permanent

firewall-cmd --reload

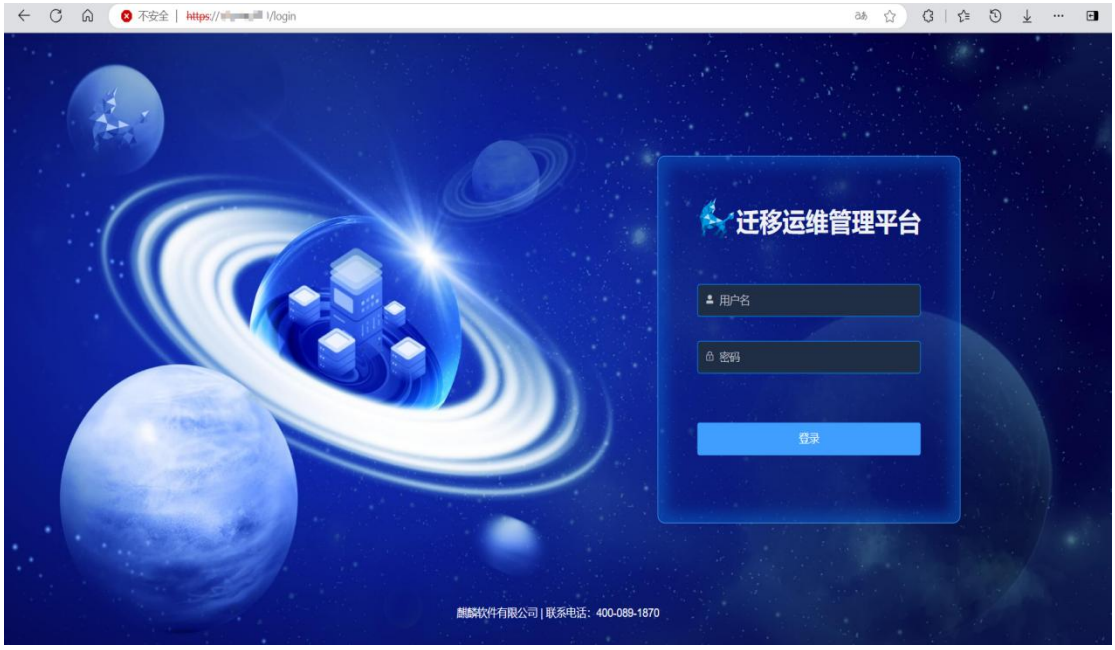
后续如需访问 nacos 界面，可以临时打开 8848 端口的访问规则

firewall-cmd --zone=public --add-port=8848/tcp

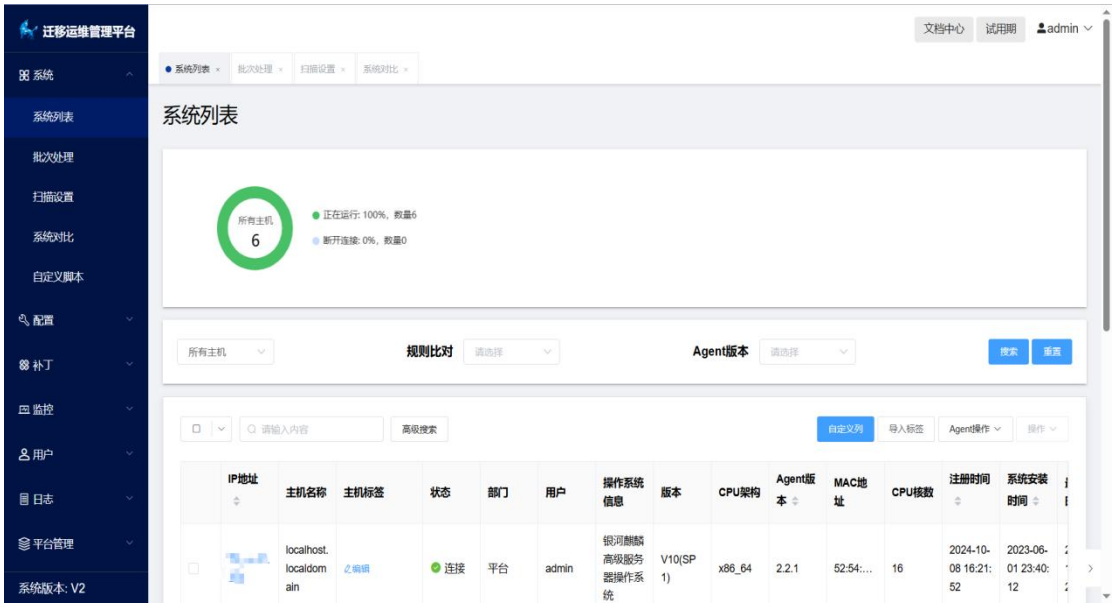
4 弱密码修改后验证平台服务是否正常

4.1 登录平台查看各功能是否正常运行

1) 浏览器输入 https://ip，其中 ip 为前端 ip，使用用户名 admin 登录平台，第一次登录，默认密码为 Easyclick123，登录后需要修改

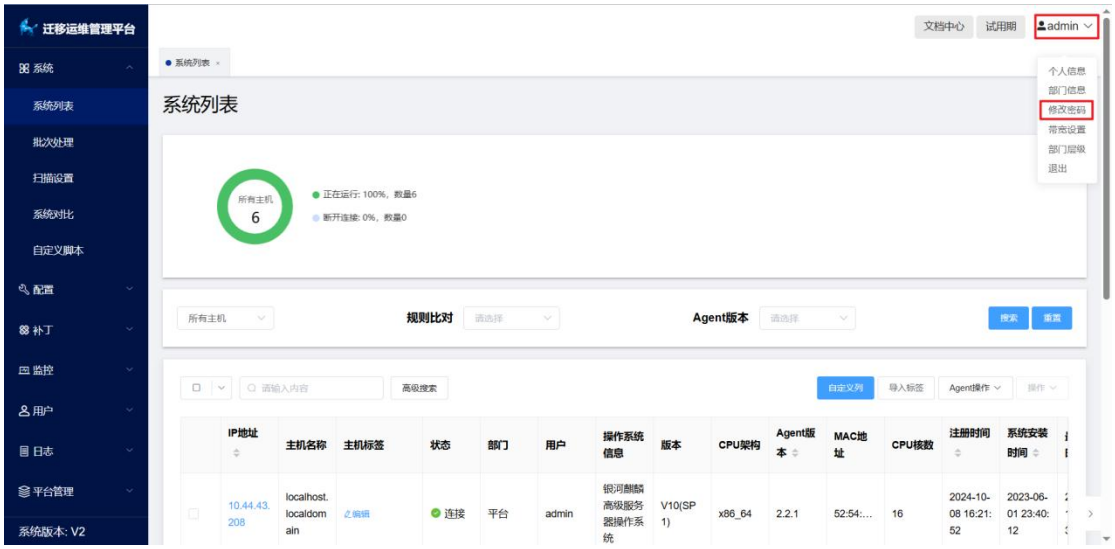


2) 进入平台，查看各功能运行是否报错



4.2 第一次登录修改默认密码

1) 依次点击右上角“admin”，“修改密码”：



2) 在弹出界面输入旧密码，新密码和确认新密码，最后确认：