银河麒麟迁移运维管理平台 V2.2.1

安全加固方案

麒麟软件有限公司

2024 年 10 月 15 日

目录

1 目的

本方案为银河麒麟迁移运维管理平台 V2.2.1 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/sentinel.conf

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

3) 重启 redis 服务

systemctl restart redis

systemctl restart redis-sentinel

2.2 数据库密码修改

1) 修改配置文件

vim /data/pgsql/data/postgresql.conf

取消 88 行对应的注释，修改 scarm 为 scram-sha-256

```
87 #ssl_crl_file = ''
88 password_encryption = scram-sha-256            # md5 or scram-sha-256
89 #db_user_namespace = off
```

vim /data/pgsql/data/pg_hba.conf

根据下图内容将 trust 改为 peer 或者 scram-sha-256

```
# "local" is for Unix domain socket connections only
local   postgres             all                                     peer
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            scram-sha-256
host    all             all             0.0.0.0/0               scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     scram-sha-256
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
[root@localhost data]#
```

2) 重启服务

systemctl restart postgresql

3) 更新密码

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                | md58ce5e7b755ceddc13940ffbd50f2f70e
(7 行记录)
```

kylin：用于后端连接数据库的账号，密码默认为 Qwer!234578。

ismp：单机或分布式部署不用关注，该用户为高可用部署时主从复制的用户，密码可在/data/pgsql/data/recovery.conf 文件中查看。

修改以下用户的密码信息：

#\password ismp　　　//高可用部署时修改

#\password kylin

#SELECT rolname,rolpassword FROM pg_authid;　　//查看是否变更为 sha256 算法

```
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$4096:8qYv3eja8VLLLtxFQ/T08Q==$pjvepQf4M+GFNv/xk2v5TJvsMFStTFUEeojYwfTYc1A=:yB/rNT1mk4X5pdkPyHGLP9S1T8X7QIxm7LVRJrRE
jHs=
(7 rows)

postgres=#
```

#postgres=# \q　　　//退出

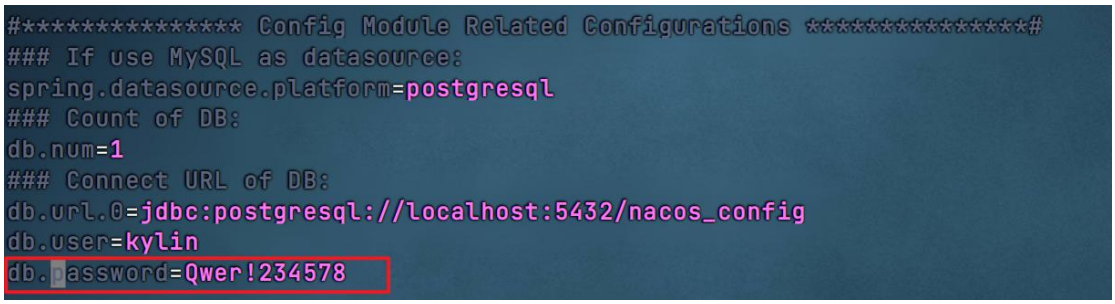
2.3 nacos 密码修改

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

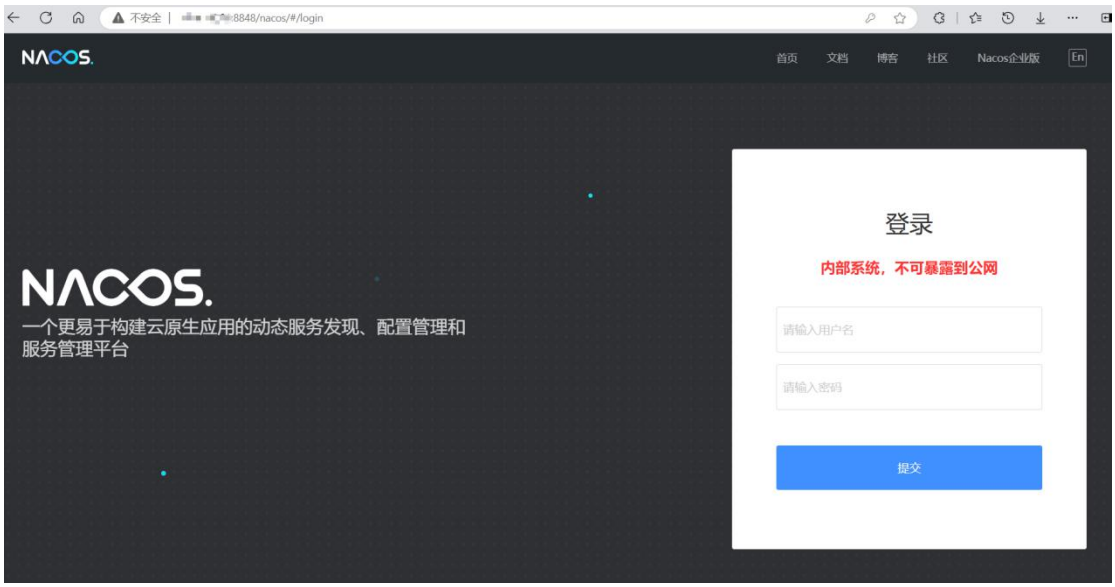


systemctl restart ismp-nacos-standalone.service //单机部署重启 nacos 服务

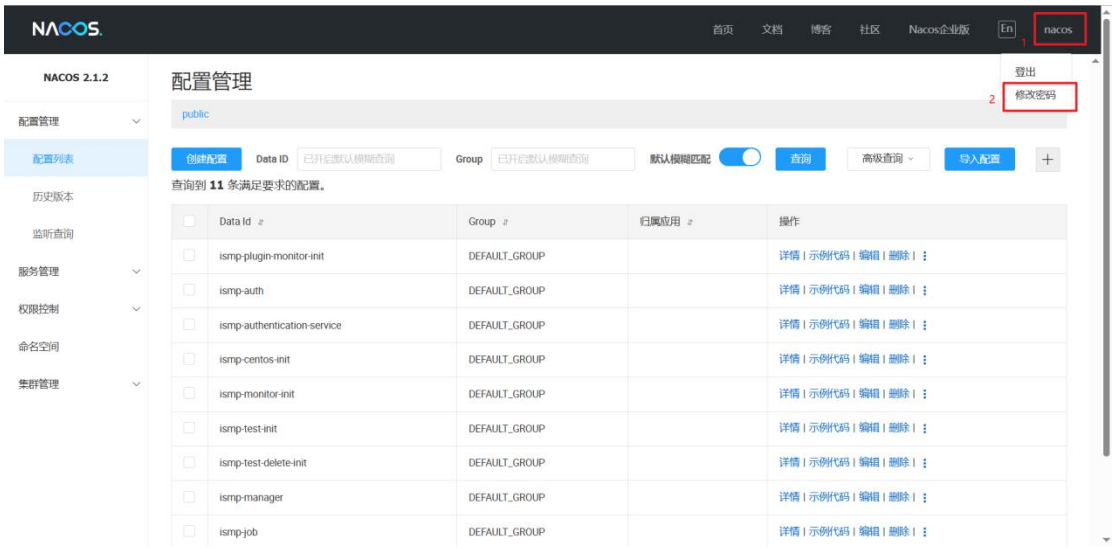
systemctl restart ismp-nacos-cluster.service //高可用部署重启 nacos 服务

2) 登录 ismp-nacos 页面，登录方式如下：

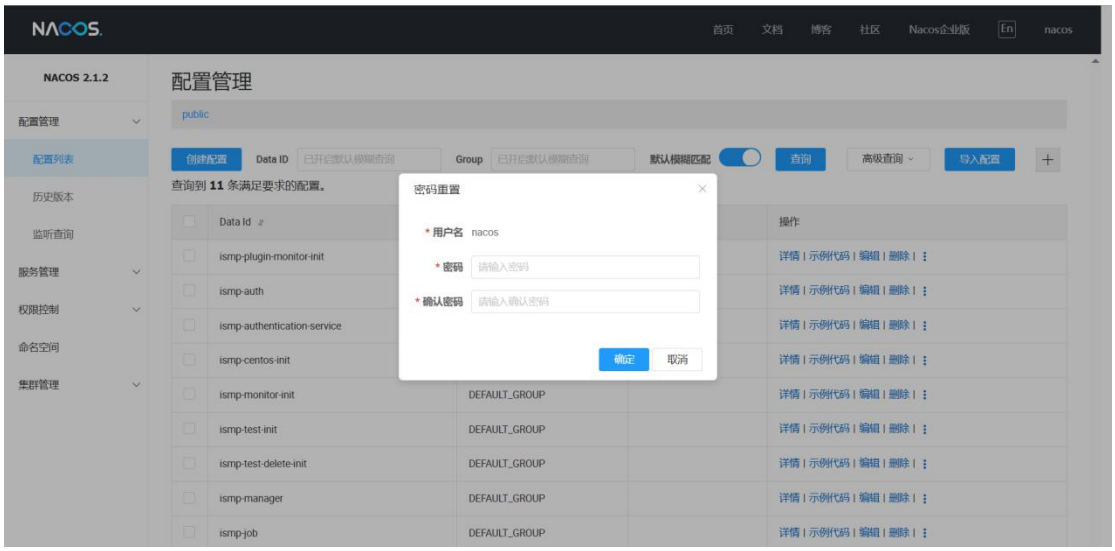
浏览器输入：http://ip:8848/nacos，其中 ip 为部署 ismp-nacos 服务的机器的 ip，用户名为 nacos，默认密码为 Qwer!234578。



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：



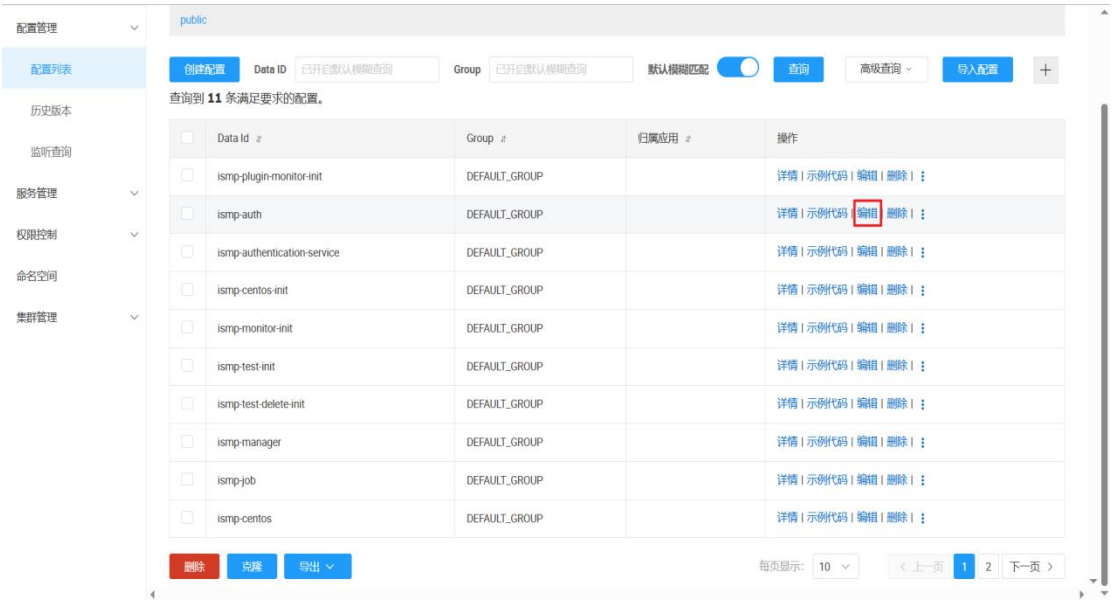
4） 在弹出窗口输入新密码并确认：



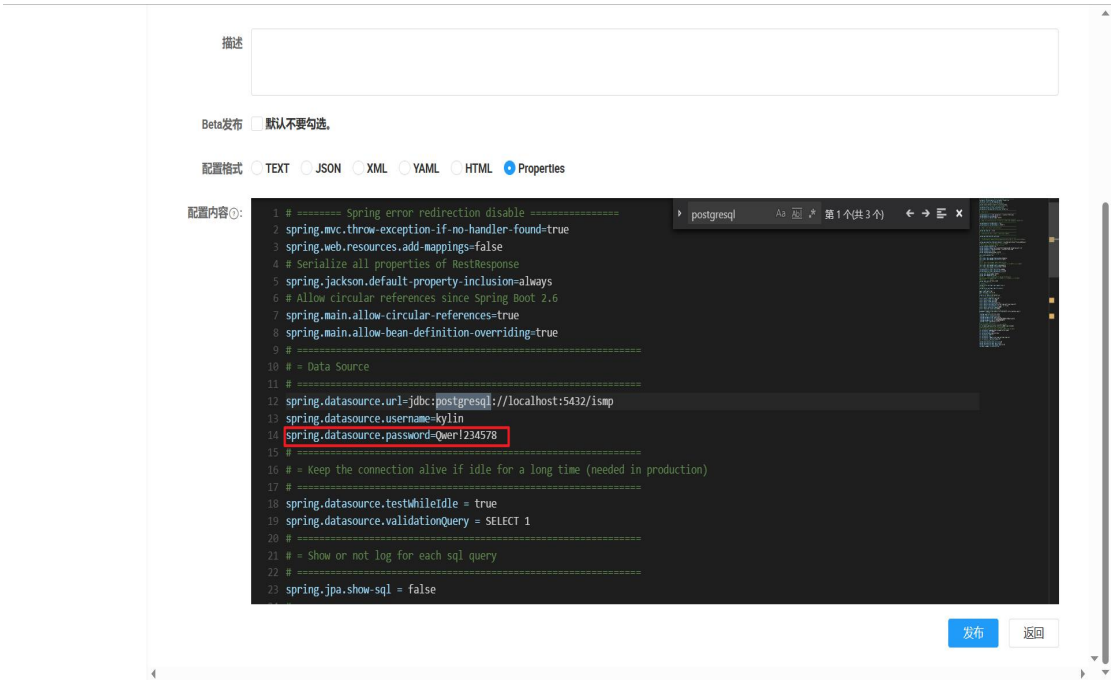
2.3.2 nacos 配置管理界面内的配置文件中密码修改

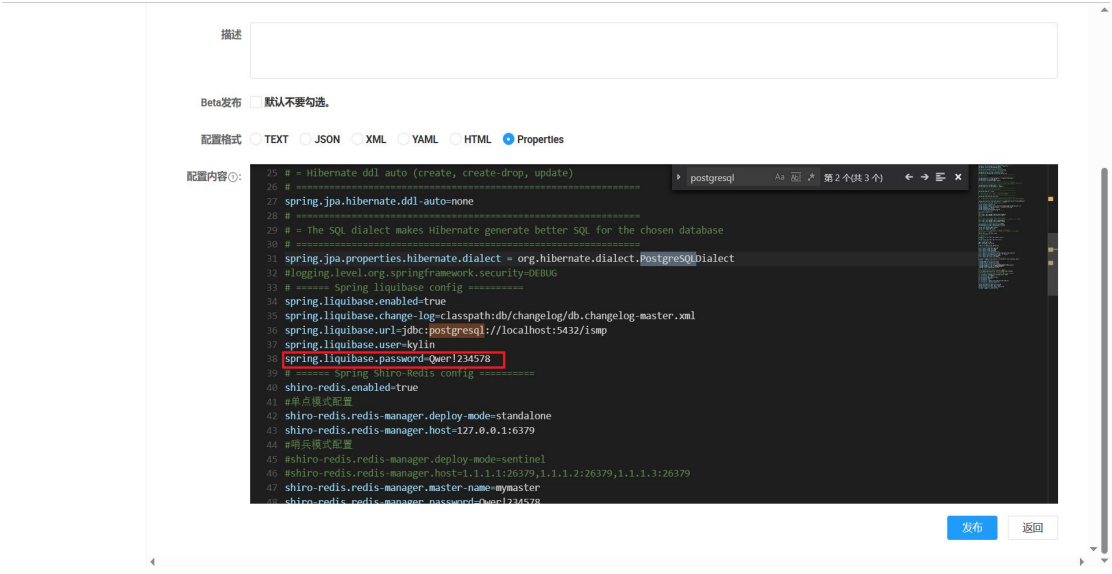
1） 通过 2.3.1 中方法登录 nacos 页面，如果已修改密码请使用新密码登录

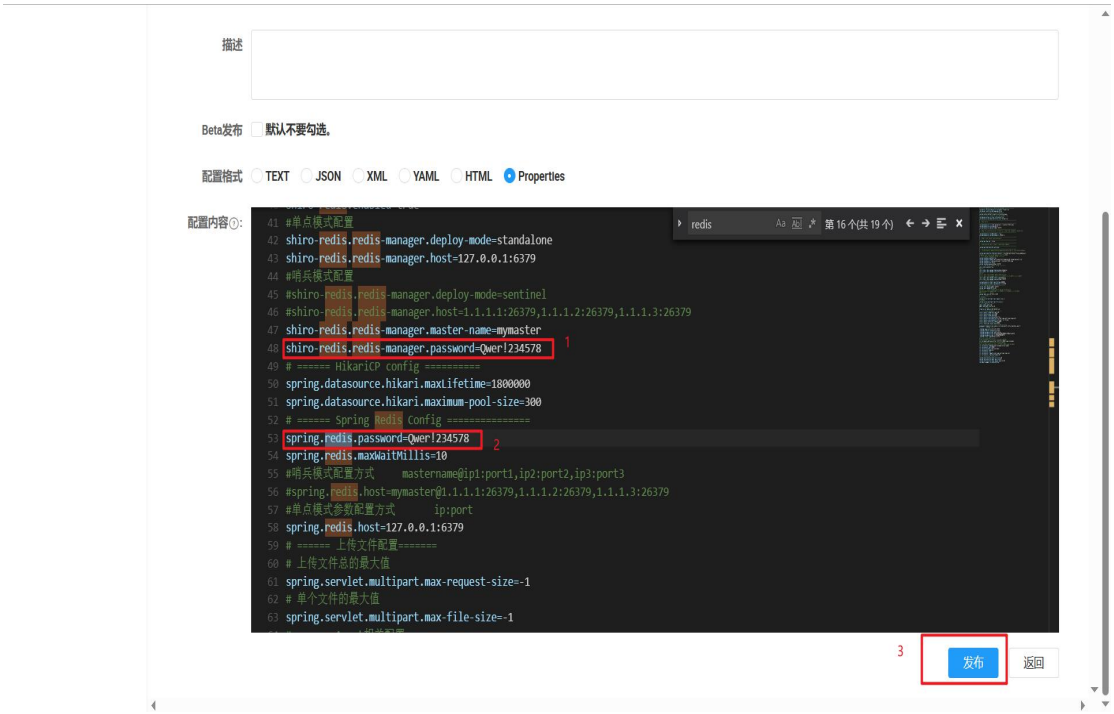
2） 在配置管理界面编辑 ismp-auth，如下图所示：



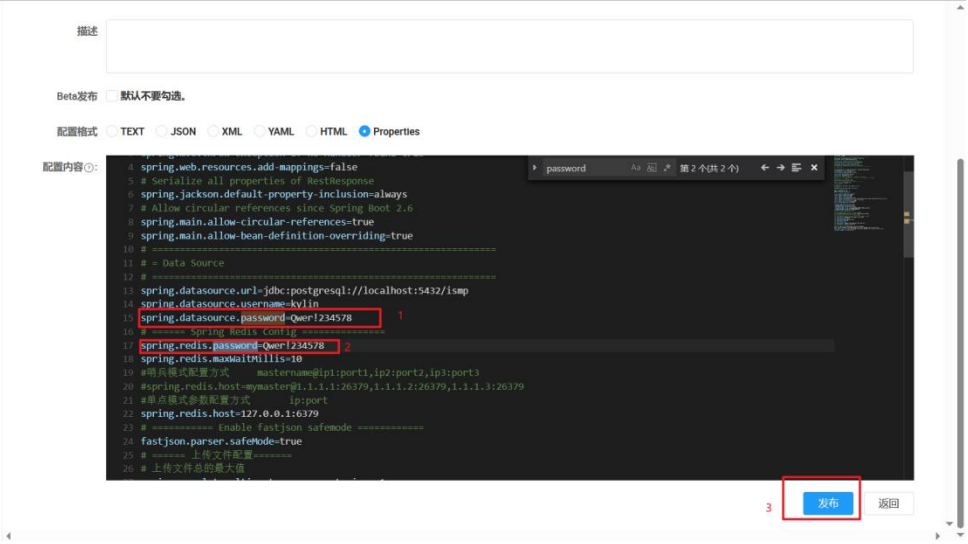
3) 在 ismp-auth 配置界面通过 ctrl+F 搜索 password，修改 shiro-redis.redis-manager.password 和 spring.redis.password 为 2.1 中设置的 redis 密码，修改 spring.datasource.password 和 spring.liquibase.password 为 2.2 中设置的数据库 kylin 用户密码，修改完成后点击发布修改后点击发布：



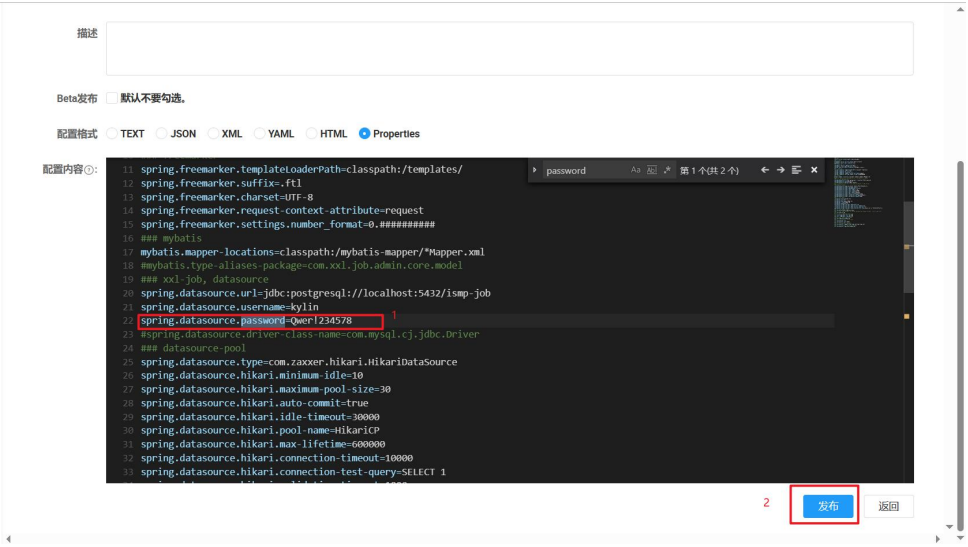




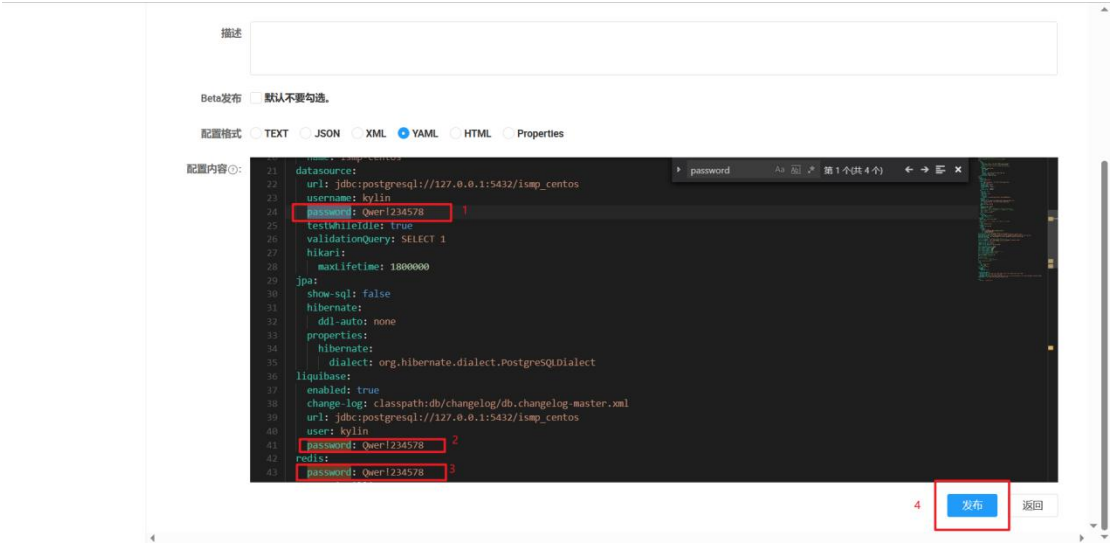
4) 在 nacos 配置管理界面点击编辑 ismp-authentication-service 文件，通过 Ctrl+F 搜索 password，修改 spring.datasource.password 为 2.2 中设置的数据库 kylin 用户的密码，修改 spring.redis.password 为 2.1 中设置的 redis 密码，修改完成后点击发布：



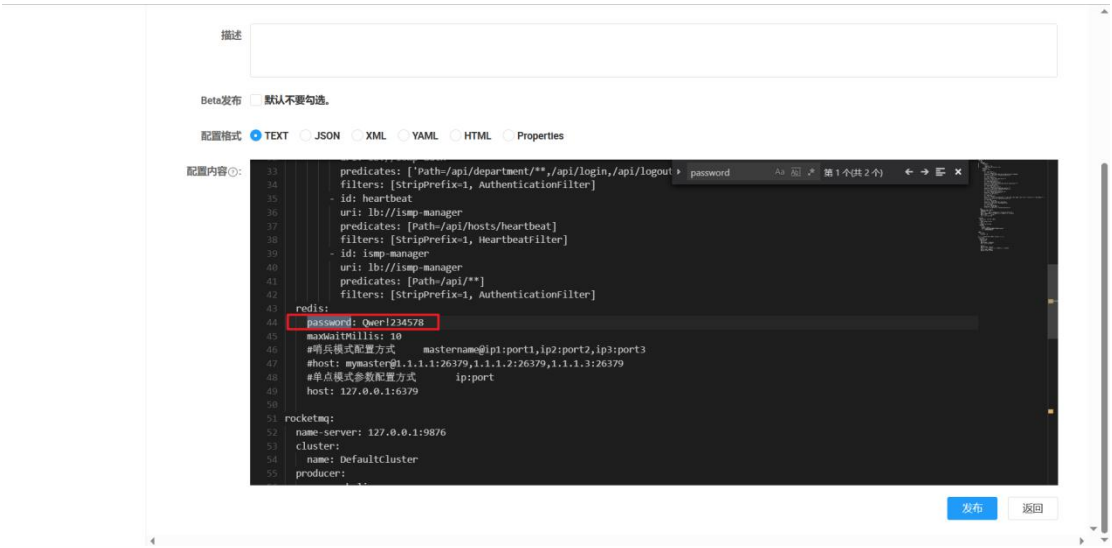
5) 在 nacos 配置管理界面点击编辑 ismp-job 文件，通过 Ctrl+F 搜索 password，修改 spring.datasource.password 为 2.2 中设置的数据库 kylin 用户密码，修改后点击发布：

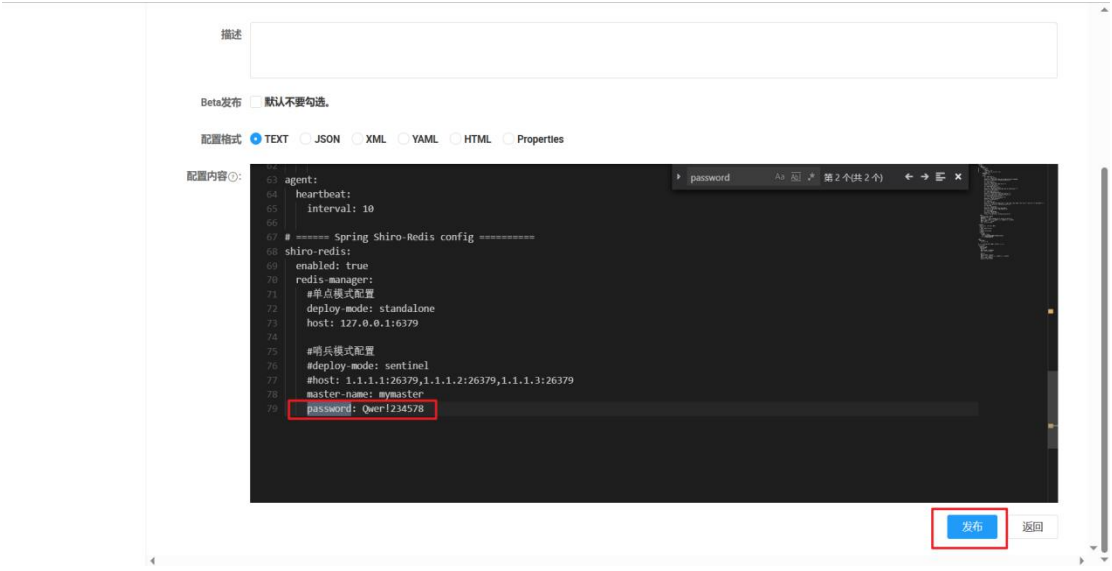


6) 在 nacos 配置管理界面点击编辑 ismp-centos 文件，通过 Ctrl+F 搜索 password，修改 datasource 下的 password 为 2.2 中设置的数据库 kylin 用户密码，修改 liquibase 下的 password 为 2.2 中设置的数据库 kylin 用户密码，修改 redis 下的 password 为 2.1 中设置的 redis 密码，修改后点击发布，如下图所示：

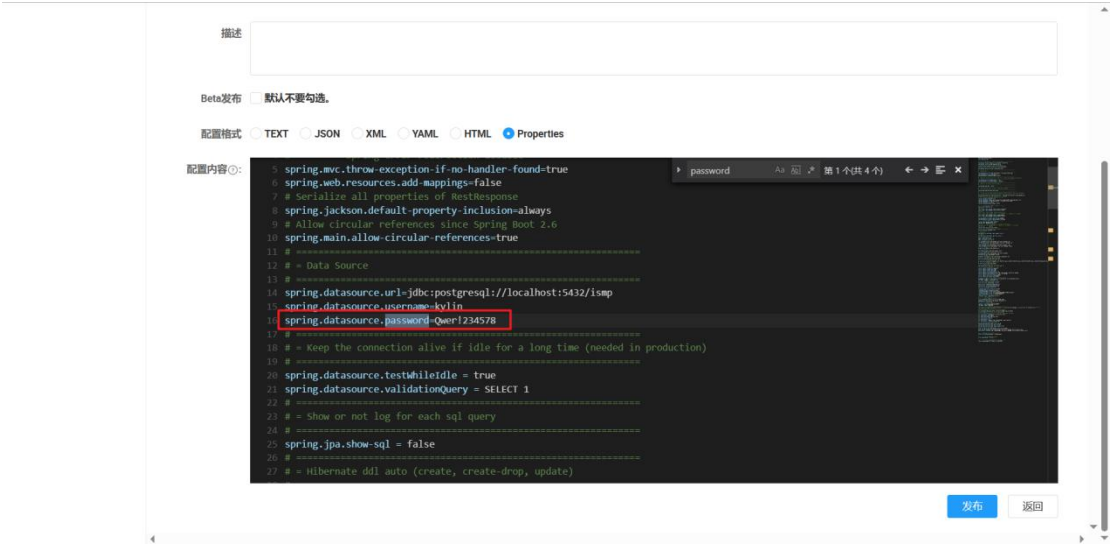


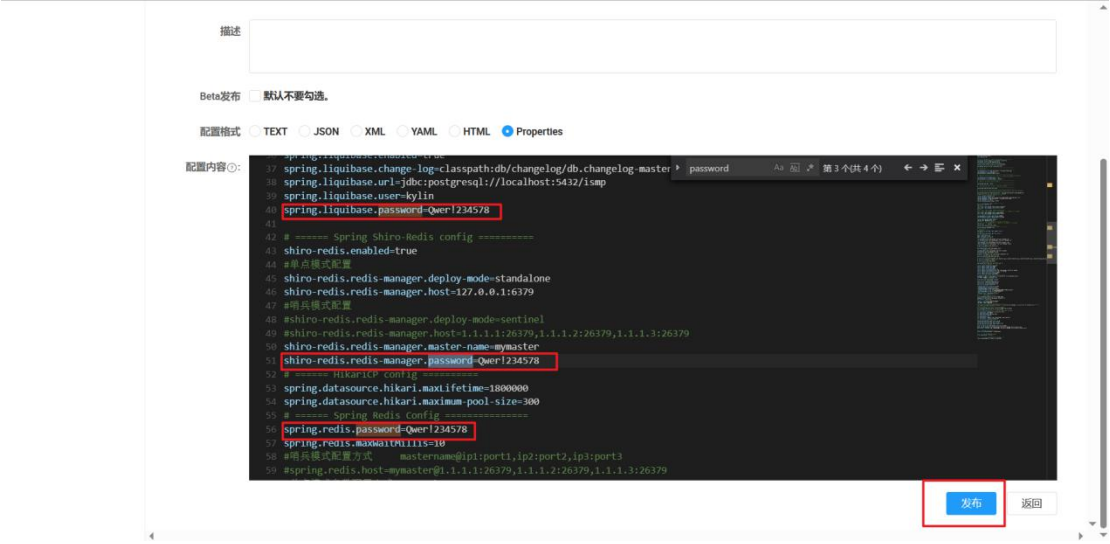
7) 在 nacos 配置管理界面点击编辑 ismp-gateway 文件，通过 Ctrl+F 搜索 password，修改 redis 和 shiro-redis 下的 password 为 2.1 中设置的 redis 密码，修改后点击发布，如下图所示：





8) 在 nacos 配置管理界面点击编辑 ismp-manager 文件，通过 Ctrl+F 搜索 password，修改 spring.datasource.password 和 spring.liquibase.password 为 2.2 中设置的数据库 kylin 用户密码，修改 shiro-redis.redis-manager.password 和 spring.redis.password 为 2.1 中设置的 redis 密码，修改后点击发布：





9) 登录部署 ismp-nacos 服务机器，重启 nacos 服务

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

2.4 ismp-gateway，ismp-auth，ismp-authentication，ismp-job，ismp-centos，ismp-monitor，ismp-manager 连接 ismp-nacos 服务的密码修改：

1) 登录部署 ismp-gateway 机器，修改 /opt/ismp-gateway/bootstrap.yml 文件中 password 为 2.3.1 中设置的 nacos 平台访问密码，修改后重启服务：

vim /opt/ismp-gateway/bootstrap.yml

```yaml
server:
  port: 8888

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

systemctl restart ismp-gateway // 修改完后重启 ismp-gateway 服务

2) 登录部署 ismp-job 服务的机器，修改/opt/ismp-job/bootstrap.properties 文件中 password 为 2.3.1 中设置的 nacos 平台访问密码，修改后重启服务：

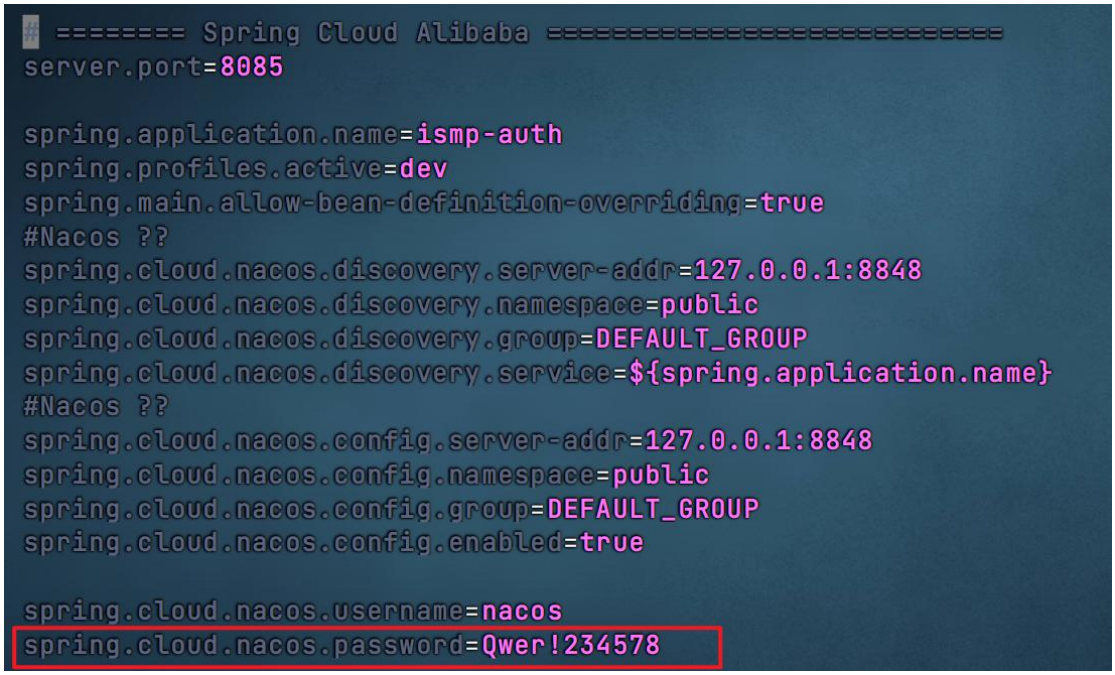
vim /opt/ismp-job/bootstrap.properties

```properties
server.port=8083
spring.application.name=ismp-job
spring.profiles.active=dev
spring.cloud.nacos.discovery.server-addr=127.0.0.1:8848
spring.cloud.nacos.discovery.namespace=public
spring.cloud.nacos.discovery.group=DEFAULT_GROUP
spring.cloud.nacos.discovery.service=${spring.application.name}
spring.cloud.nacos.config.server-addr=127.0.0.1:8848
spring.cloud.nacos.config.namespace=public
spring.cloud.nacos.config.group=DEFAULT_GROUP
spring.cloud.nacos.config.enabled=true
spring.cloud.nacos.config.file-extension=properties
spring.cloud.nacos.username=nacos
spring.cloud.nacos.password=Qwer!234578
```

systemctl restart ismp-job //修改完后重启 ismp-job 服务

3) 登录部署 ismp-auth 服务的机器，修改/opt/ismp-auth/bootstrap.properties 文件中 password 为 2.3.1 中设置的 nacos 平台访问密码，修改后重启服务：

vim /opt/ismp-auth/bootstrap.properties



systemctl restart ismp-auth　　//修改完后重启 ismp-auth 服务

4) 登录部署 ismp-authentication 服务的机器，修改/opt/ismp-authentication/bootstrap.properties 文件中 password 为 2.3.1 中设置的 nacos 平台访问密码，修改后重启服务：

vim /opt/ismp-authentication/bootstrap.properties

```
# ======== Spring Cloud Alibaba ============================
server.port=8891

spring.application.name=ismp-authentication-service
spring.profiles.active=dev
spring.main.allow-bean-definition-overriding=true
#Nacos ??
spring.cloud.nacos.discovery.server-addr=127.0.0.1:8848
spring.cloud.nacos.discovery.namespace=public
spring.cloud.nacos.discovery.group=DEFAULT_GROUP
spring.cloud.nacos.discovery.service=${spring.application.name}
#Nacos ??
spring.cloud.nacos.config.server-addr=127.0.0.1:8848
spring.cloud.nacos.config.namespace=public
spring.cloud.nacos.config.group=DEFAULT_GROUP
spring.cloud.nacos.config.enabled=true

spring.cloud.nacos.username=nacos
spring.cloud.nacos.password=Qwer!234578
~
```

systemctl restart ismp-authentication // 修改完后重启 ismp-authentication 服务

5) 登录部署 ismp-centos 服务的机器，修改 /opt/ismp-centos/bootstrap.yml 文件中 password 为 2.3.1 中设置的 nacos 平台访问密码，修改后重启服务：

vim /opt/ismp-centos/bootstrap.yml

```yaml
server:
  port: 8889

spring:
  cloud:
    nacos:
      username: nacos
      password: Qwer!234578
      config:
        namespace: public
        group: DEFAULT_GROUP
        file-extension: yaml
        #Nacos 地址
        server-addr: 127.0.0.1:8848
        enabled: true
      discovery:
        namespace: public
        group: DEFAULT_GROUP
        server-addr: 127.0.0.1:8848
        service: ${spring.application.name}
  main:
    allow-bean-definition-overriding: true
  application:
    name: ismp-centos
```

systemctl restart ismp-centos //修改完后重启 ismp-centos 服务

6) 登录部署 ismp-monitor 服务的机器，修改/opt/ismp-plugin-monitor/config.yaml 文件中 redis_server 下的 password 为 2.1 中设置的 redis 密码，nacos 下的 password 为 2.3.1 中设置的 nacos 平台访问密码，psql_server 下的 password 为 2.2 中设置的数据库 kylin 用户密码，修改后重启服务：

vim /opt/ismp-plugin-monitor/config.yaml

```
psql_server:
  db_addr: localhost
  port: 5432  #postgresql默认端口是5432
  user_name: kylin
  password: Qwer!234578
  data_base: ismp_plugin_monitor #数据库名字
redis_server:
  deploy_mode: standalone #分为单机模式和哨兵模式：standalone、sentinel
  host: 127.0.0.1:6379
  sentinel_hosts: 1.1.1.1:26379,1.1.1.2:26379,1.1.1.3:26379
  master_name: mymaster
  password: Qwer!234578
  defaultDB: 0
  dialTimeout: 5s #redis连接超时时间.默认5s
nacos:
  user_name: nacos
  password: Qwer!234578
  ip: localhost
  port: 8848
```

systemctl restart ismp-monitor//修改完后重启 ismp-monitor 服务

7) 登录部署 ismp-manager 服务的机器，修改/opt/ismp-manager/bootstrap.properties 文件中 password 为 2.3.1 中设置的 nacos 平台访问密码，修改后重启服务：

vim /opt/ismp-manager/bootstrap.properties

```
server.port=8080
# ======== Spring Cloud Alibaba ==============================
spring.application.name=ismp-manager
spring.profiles.active=dev
spring.main.allow-bean-definition-overriding=true
#Nacos registry
spring.cloud.nacos.discovery.server-addr=127.0.0.1:8848
spring.cloud.nacos.discovery.namespace=public
spring.cloud.nacos.discovery.group=DEFAULT_GROUP
spring.cloud.nacos.discovery.service=${spring.application.name}
#Nacos config
spring.cloud.nacos.config.server-addr=127.0.0.1:8848
spring.cloud.nacos.config.namespace=public
spring.cloud.nacos.config.group=DEFAULT_GROUP
spring.cloud.nacos.config.enabled=true

spring.cloud.nacos.username=nacos
spring.cloud.nacos.password=Qwer!234578

redis.savemessageinfo.timeout.config=1800
```

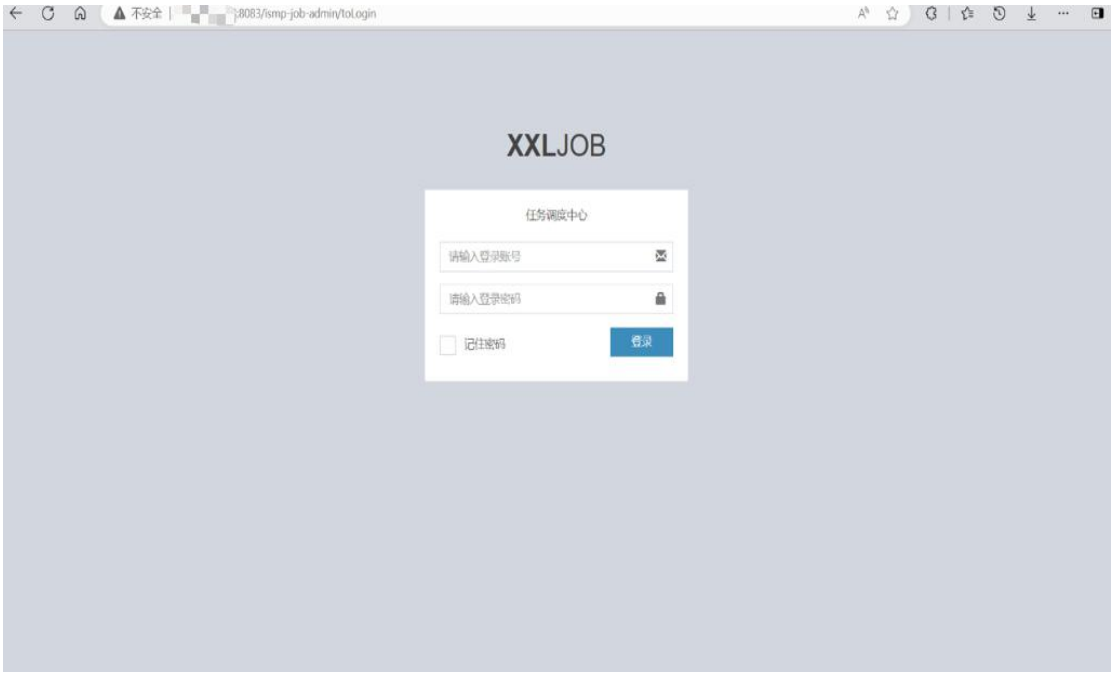
systemctl restart ismp-manager //修改完后重启 ismp-manager

服务

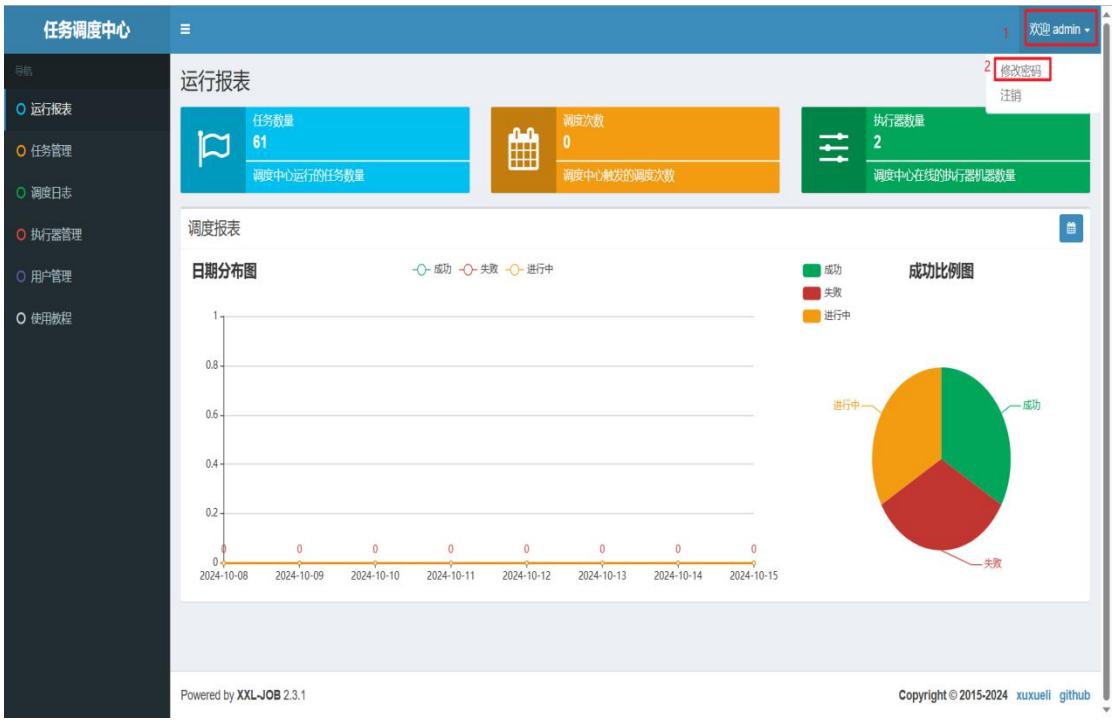
2.5 ismp-job 访问密码修改

1) 登录 job 页面，登录方式如下：

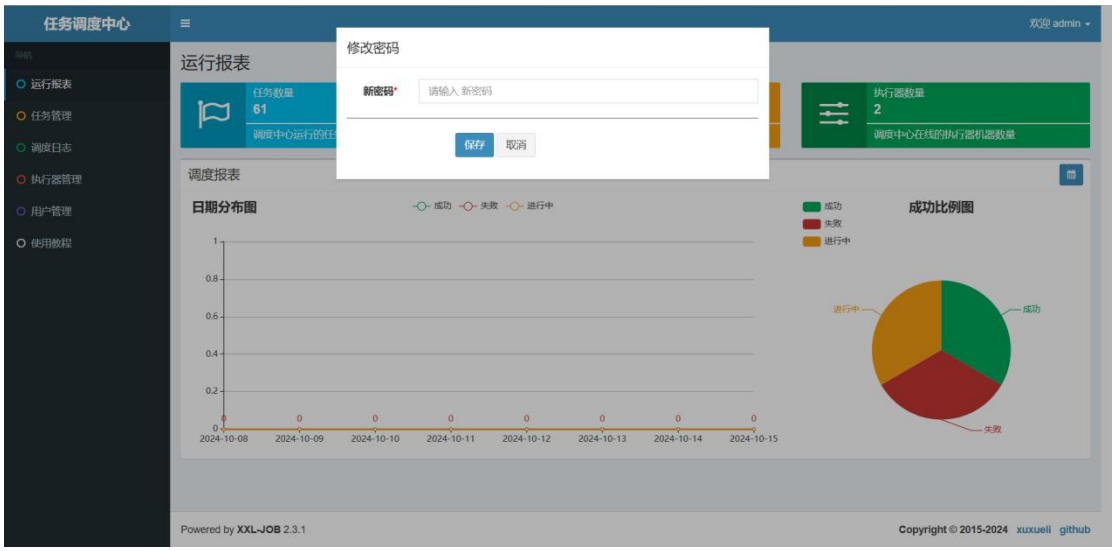
浏览器输入 http://ip:8083/ismp-job-admin，其中 ip 为部署 ismp-job 服务的机器的 ip，使用账号 admin，默认密码 123456 登录：



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：



3 单机部署防火墙规则

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

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、SP 升级操作
	443	https 的端口，用于代理端安装注册
	8848	nacos 的反向代理
	10911 10912 10909 9876	mq 服务
	22	上传评估报告

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

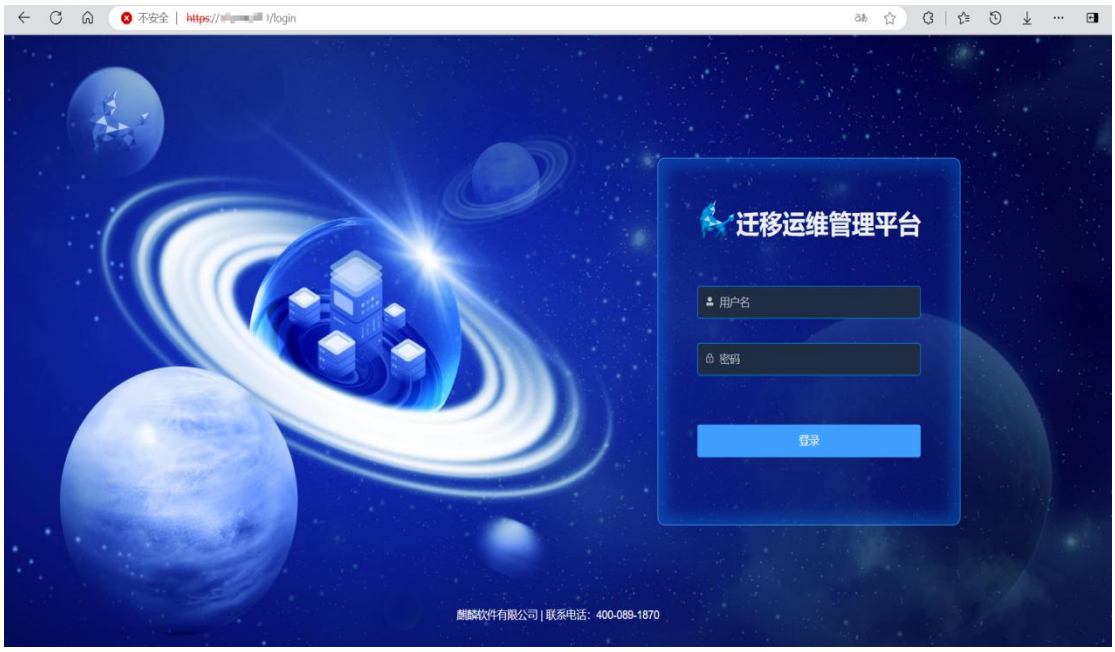
firewall-cmd --zone=public --add-port=8848/tcp

4 弱密码修改后验证平台服务是否正常

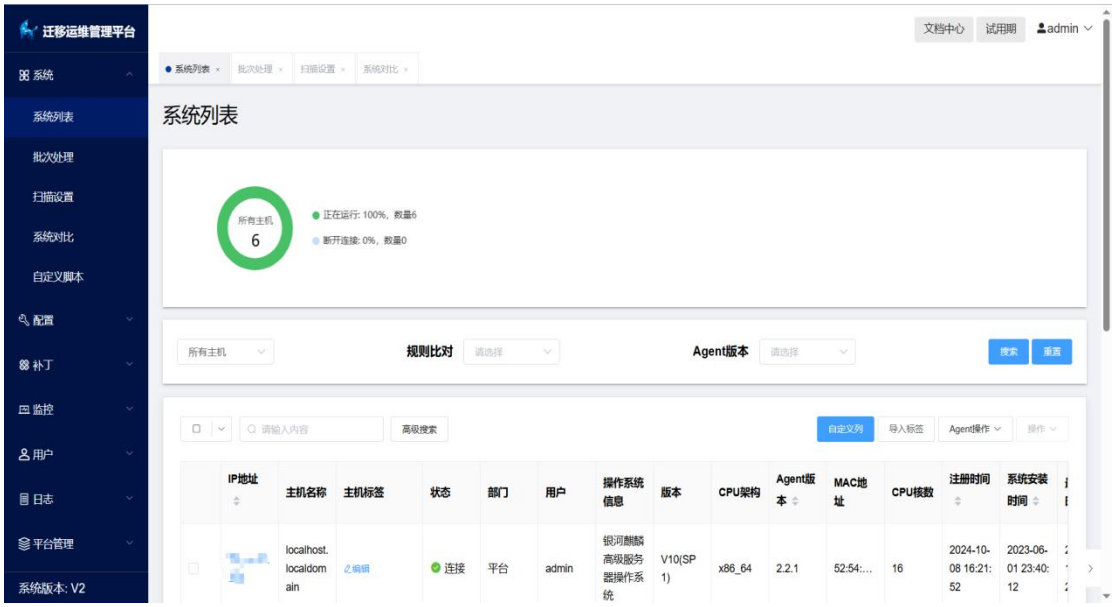
4.1 登录平台查看各功能是否正常运行

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

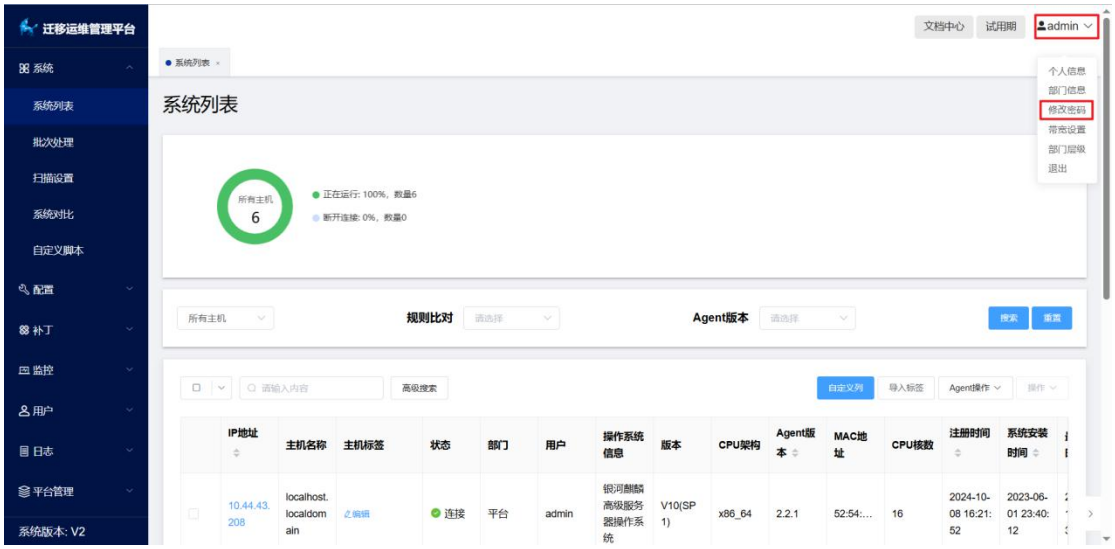


2） 进入平台，查看各功能运行是否报错



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：