Apusic 金蝶天燕

生成时间：2026-05-19

管理员使用手册

金蝶Apusic应用服务器软件V10.0

版权声明

本文档所涉及的软件著作权、版权等知识产权已依法进行了注册，由金蝶天燕云计算股份有限公司合法拥有。受《中华人民共和国著作权法》《计算机软件保护条例》《知识产权保护条例》和相关国际版权条约、法律、法规以及其它知识产权法律和条约的保护。未经授权许可，不得非法使用。

免责声明

本文档包含的版权信息由金蝶天燕云计算股份有限公司合法拥有，受法律的保护，金蝶天燕云计算股份有限公司对本文档可能涉及到的非金蝶天燕云计算股份有限公司的信息不承担任何责任。在法律允许的范围内，您可以查阅并仅能够在《中华人民共和国著作权法》规定的合法范围内复制和打印本文档。任何单位和个人未经金蝶天燕云计算股份有限公司书面授权许可，不得使用、修改、再发布本文档的任何部分和内容，否则将被视为侵权，金蝶天燕云计算股份有限公司有依法追究其责任的权利。

本文档如有更新，不另行通知。对本文档中的问题您可向金蝶天燕云计算股份有限公司告知或查询。未经本公司明确授予的任何权利均予保留。

商标声明

Apusic是深圳市金蝶天燕云计算股份有限公司向中华人民共和国国家商标局申请注册的注册商标，注册商标专用权由金蝶天燕合法拥有，受法律保护。未经金蝶天燕的书面许可，任何单位及个人不得以任何方式或理由对该商标的任何部分进行使用、复制、修改、传播、抄录或与其它产品捆绑使用销售。凡侵犯金蝶天燕商标权的，金蝶天燕将依法追究其法律责任。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

目录

1 版本变更说明

本手册根据产品实际更新情况同步更新，最新版本将会包括历史版本内容或作出对应的修改说明。

日期	手册版本	适用产品	更新说明
2023年12月	V10E02F01	AAS V10.0	调整目录

2 前言

本文档是金蝶Apusic应用服务器V10.0的管理员使用手册，介绍管理员的权限配置等内容。

2.1 面向对象

本手册主要面向对象为使用金蝶Apusic应用服务器进行应用开发的开发人员，生成环境的系统管理员，应用发布人员，技术运维人员等。具备以下技能可能会更好理解和使用金蝶Apusic应用服务器管理员使用手册内容：

- 熟悉Linux常用命令
- 基本的系统管理任务
- 安装和管理软件
- 基本信息安全管理知识

2.2 术语

APUSIC_HOME：金蝶Apusic应用服务器安装目录

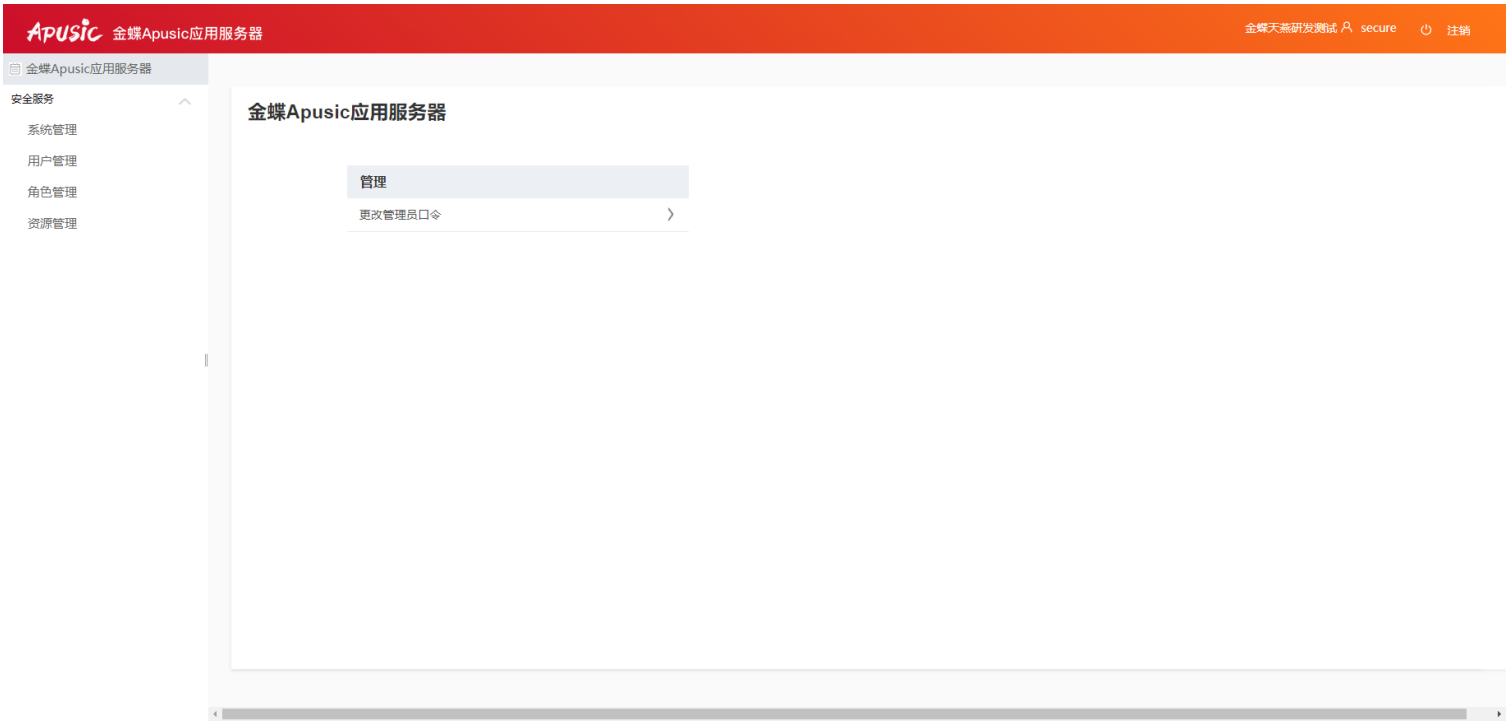
DOMAIN_HOME：金蝶Apusic应用服务器域目录

3 三元分立

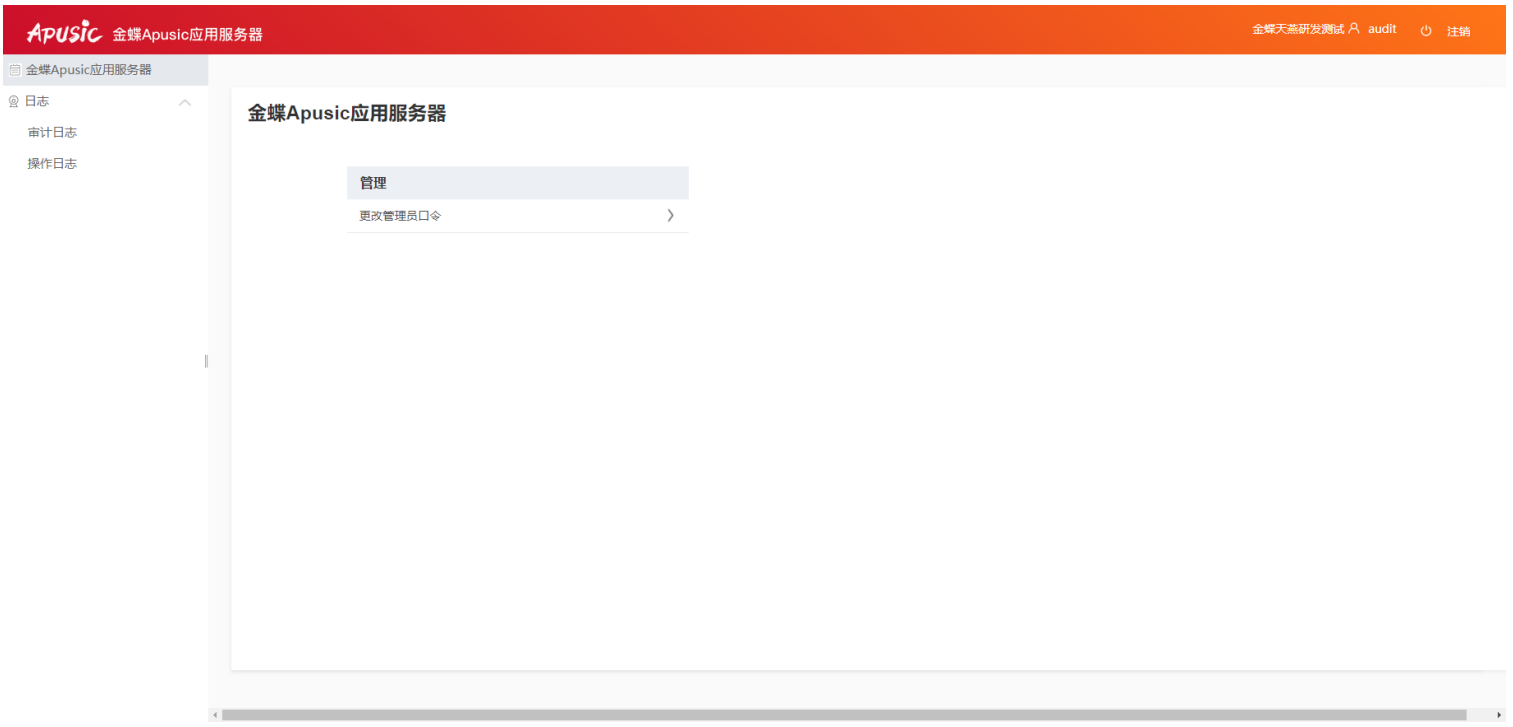
金蝶Apusic应用服务器支持三元分立功能，提供安全保密员、安全审计员、系统管理员三个角色。其中安全保密员主要管理角色管理、用户管理、密码策略等信息；安全审计员主要管理日志、操作审计信息；系统管理员主要管理应用部署、资源管理、配置管理等功能。

金蝶Apusic应用服务器初始化时需要设置默认管理员的密码。

角色为安全保密员（security）的用户访问,如使用默认安全保密员用户 secure 登录，进入到系统配置界面下:



角色为安全审计员（auditor）的用户访问，如使用默认安全审计员用户audit登录，进入到系统配置界面下:



角色为系统管理员（sysadmin）的用户访问，如使用默认系统管理员用户admin登录，进入到系统配置界面下:

4 安全管理员操作

安全保密员主要管理角色管理、用户管理、密码策略等信息。

4.1 角色管理

安全管理员登录管控平台，可管理角色信息。

创建并管理角色，金蝶Apusic应用服务器自带角色包括 sysadmin,security,auditor，不能编辑或删除。自带开发者角色 publish_role，允许编辑或删除。

- **角色名**: 角色的名称。
- **角色所属用户**: 当前角色所属的角色，【用户管理】中设置"系统角色"将实时更新。
- **角色资源**: 角色拥有的资源。

角色管理

创建并管理角色，无法修改删除保留的privilege 角色包括sysadmin,security,auditor。

角色 (5)

添加 删除 刷新

选择	角色名	角色所属用户	角色资源	PRIVILEGE
☐	security	secure	common_index,security_all	TRUE
☐	auditor	audit	common_index,auditor_logs	TRUE
☐	publish_role	testrole	common_index,sysadmin_domain,sysadmin_management_app_server,sysadmin_cluster,sysadmin_stand_alone,sysadmin_node,sysadmin_applications,sysadmin_life_cycles,sysadmin_monitor,sysadmin_transaction,sysadmin_resource,sysadmin_configuration	FALSE
☐	sysadmin	admin	common_index,sysadmin_domain,sysadmin_management_app_server,sysadmin_cluster,sysadmin_stand_alone,sysadmin_node,sysadmin_applications,sysadmin_life_cycles,sysadmin_monitor,sysadmin_transaction,sysadmin_resource,sysadmin_configuration	TRUE
☐	testrole		common_index,sysadmin_domain,sysadmin_applications	FALSE

4.1.1 新建角色

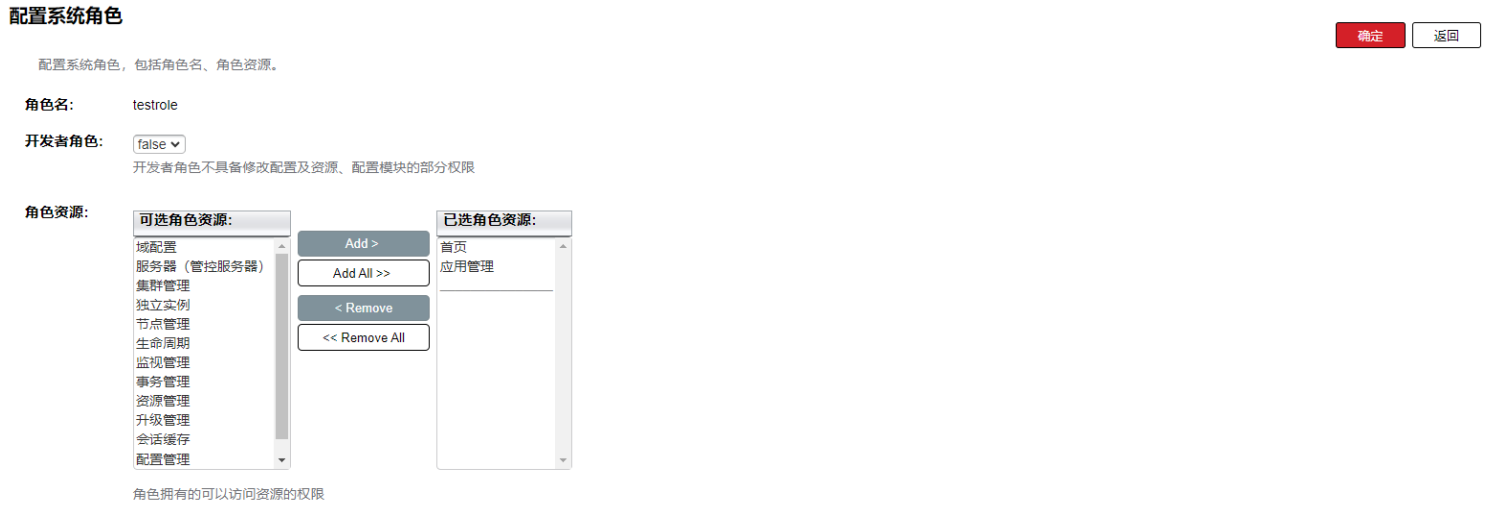
点击"新建"，进入新建系统角色页面。

- **角色名**: 角色的名称，名称最多可以包含 255 个字符, 并且只能包含字母数字,下划线,短横线或点字符，需要唯一。
- **开发者角色**: 开发者角色不具备修改配置及资源、配置模块的部分权限，默认选择为 false。
- **角色资源**: 设置当前角色的资源，shift 键可以连续多选，Ctrl 键可以选择多选。建议需要选择"首页"。

用户 test1 所属的角色为 testrole，因而其登录管控平台只显示有 testrole 的资源。

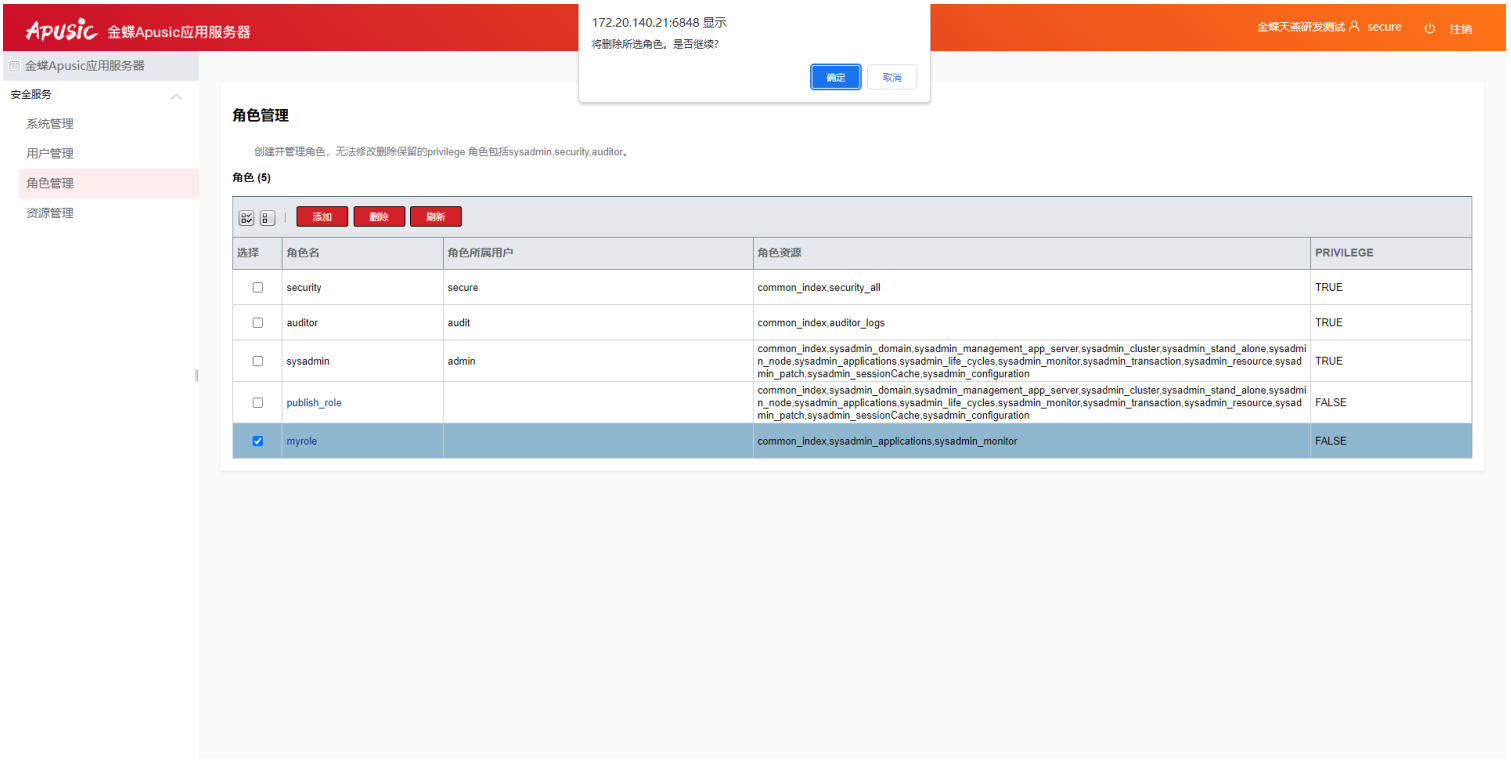
4.1.2 编辑角色

点击角色名称，将进入编辑角色页面，可对角色资源进行编辑。修改后，用户需要重新登录管控平台才能生效。



4.1.3 删除角色

选择需要删除的角色，点击“删除”，确认删除后将会删除该角色信息。需注意，AAS 自带角色包括 sysadmin,security,auditor，不能编辑或删除。自带开发者角色 publish_role，允许编辑或删除。



4.2 用户管理

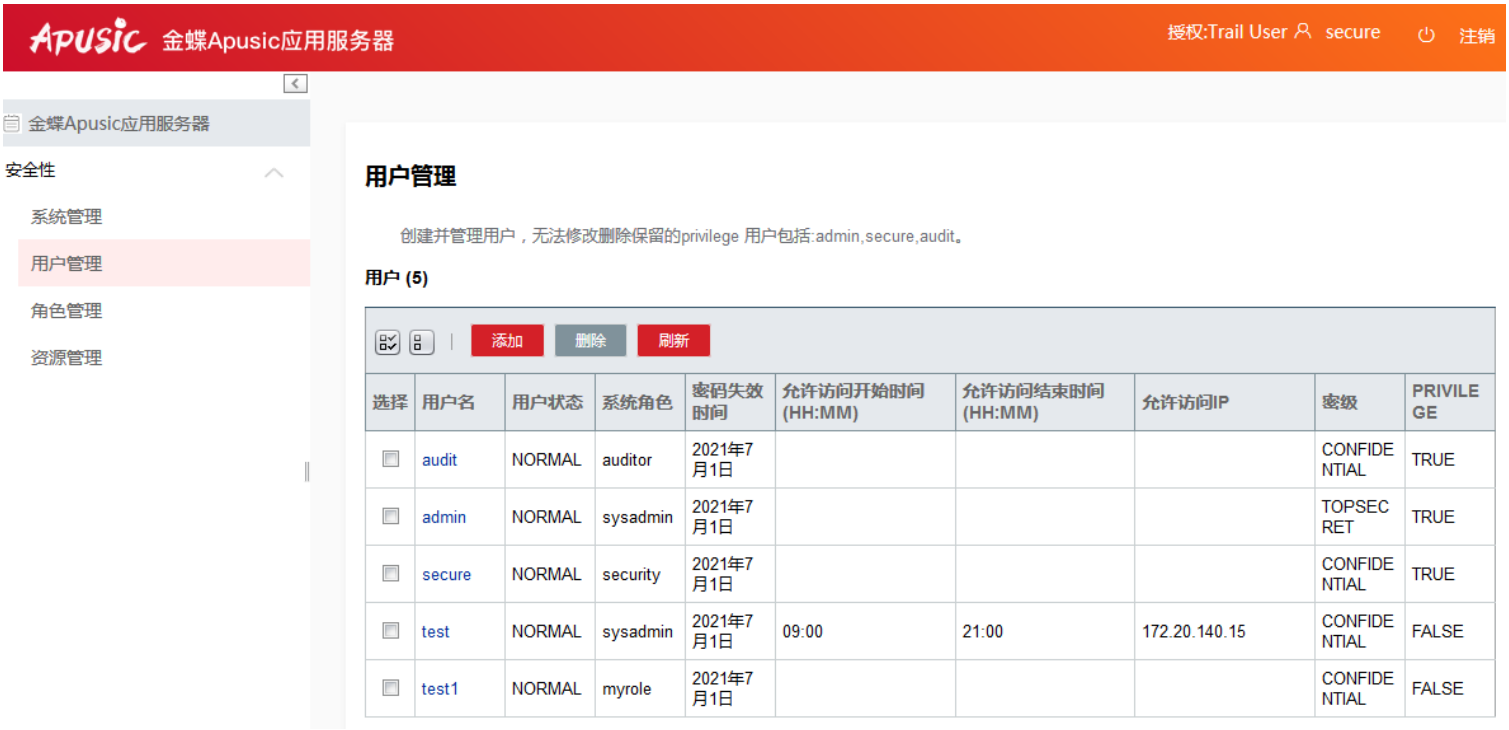
角色为安全保密员（secure）的用户登录管控平台，可以对用户进行新增、修改删除等管理操作，还可以对用户进行安全属性的设置，如对用户进行锁定、禁用、IP 访问限制以及访问时间段限制等操作。

用户信息存储在 `${DOMAIN_HOME}/mydomain/config/admin-keyfile` 中。

使用角色为安全保密管理员的用户登录管控，切换到用户管理界面。

在用户管理界面可以对用户进行添加、编辑和删除操作。

- **用户名**: 应用服务器的用户名称，需要唯一。
- **用户状态**: 显示用户的状态。
- **系统角色**: 显示用户的角色。
- **密码失效时间**: 显示密码的失效时间，默认为初始化用户后 30 天，在【系统管理】中修改"密码失效时间"，该处的时间将会同步修改。
- **允许访问开始时间（HH: MM）**: 用户允许访问管控台的开始时间，格式为 HH: MM。
- **允许访问结束时间（HH: MM）**: 用户允许访问管控台的结束时间，格式为 HH: MM。
- **允许访问 IP**: 用户允许访问的 IP，即为浏览器所在的 IP。
- **密级**: 用户所属的密级。
- PRIVILEGE: 是否为初始化用户，为 TRUE 时，该用户不能直接删除。



4.2.1 新建用户

可点击"添加"，进入新建用户页面。

- **用户名**: 应用服务器的用户名称，名称最多可以包含 255 个字符, 并且只能包含字母数字,下划线,短横线或点字符，需要唯一。
- **角色名**: 选择用户的角色，不同角色有不同的权限。分别有 security、sysadmin、auditor、publish_role（表示新建、编辑等操作受限制的用户）。
- **新口令**: 设置用户的口令，【系统管理】中，"密码复杂度"设置完为"普通"时，密码必须包含字母、数字和特殊符号中的至少两种组合;"复杂"时，密码必须包含字母、数字和特殊符号。
- **确认新口令**: 需要输入与"新口令"一致。

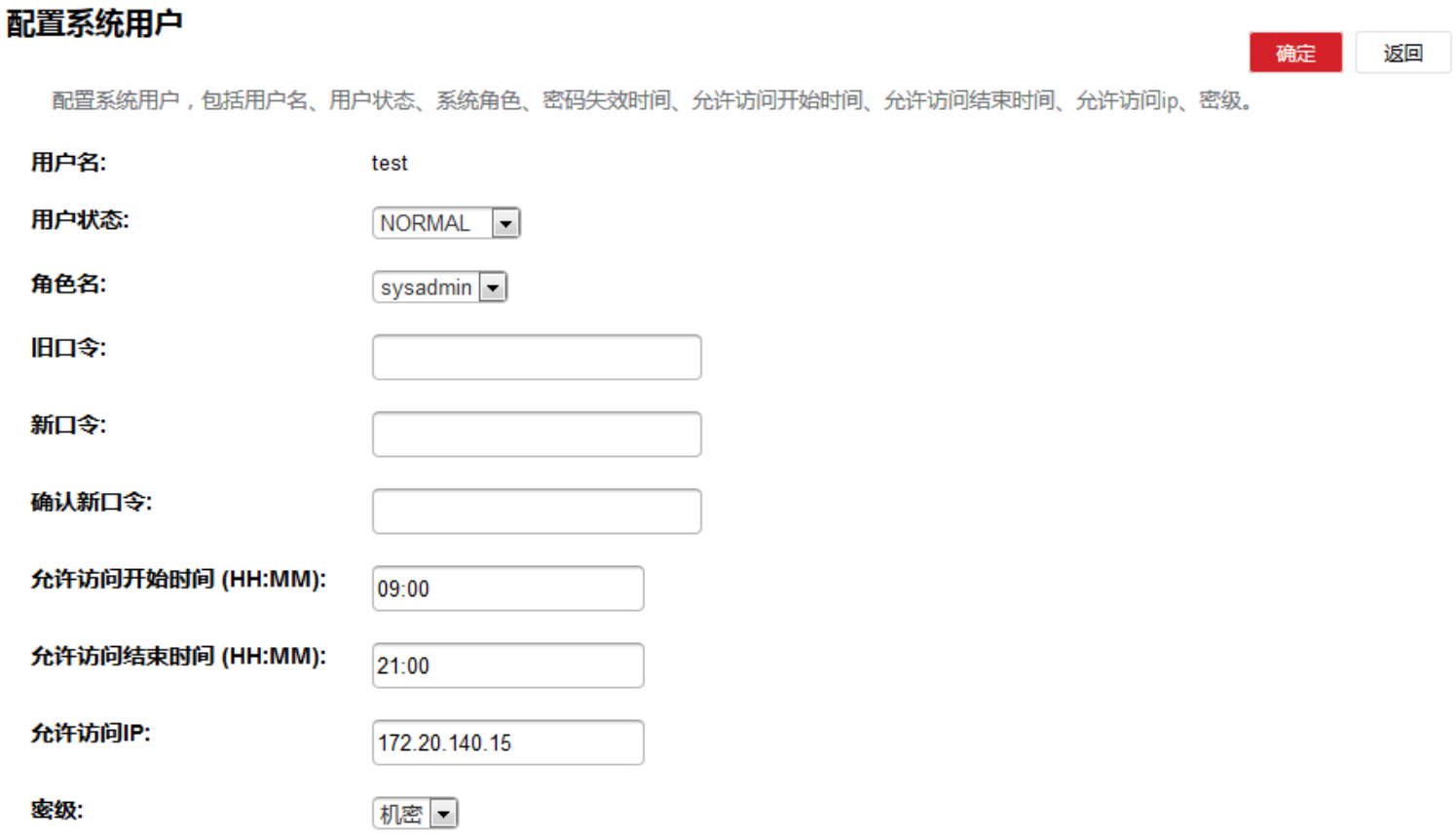
4.2.2 编辑用户信息

点击"用户管理"列表中的"用户名"，进入对应用户的编辑页面。

- **用户名**: 该用户的名称，不能编辑。
- **用户状态**: 设置用户的状态，NORMAL 表示正常；LOCKED 表示锁定，默认为锁定 15 分钟；DISABLED 表示禁用。
- **系统角色**: 设置用户的角色。
- **旧口令**: 修改密码时需要输入用户的旧口令。
- **新口令**: 设置用户的口令，【系统管理】中，"密码复杂度"设置完为"普通"时，密码必须包含字母、数字和特殊符号中的至少两种组合;"复杂"时，密码必须包含字母、数字和特殊符号。修改密码 5 次内不能重复。
- **确认新口令**: 需要输入与"新口令"一致。
- **允许访问开始时间（HH: MM）**: 用户允许访问管控台的开始时间，格式为 HH: MM。
- **允许访问结束时间（HH: MM）**: 用户允许访问管控台的结束时间，格式为 HH: MM。

- **允许访问 IP**: 对用户访问管控的 IP 进允许限制,即为浏览器所在的 IP 可以用精确的 IP 地址，[10-60]及*格式，多个 IP 使用英文逗号分隔。
- **密级**: 用户所属的密级，该用户只能访问同一等级或低等级的应用或资源。当前有秘密、机密、绝密三个等级，权限等级：秘密<机密<绝密。

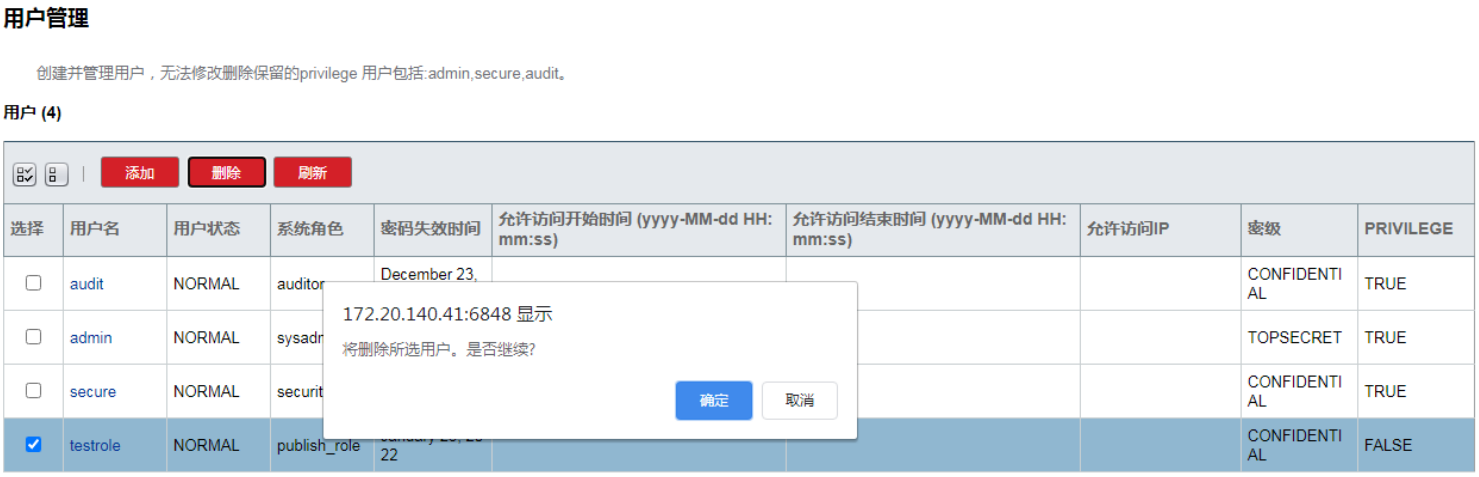
> ***注意**: 编辑用户信息后，会同步刷新用户的 session 状态，处于登录中的会话将会失效，退出登录。*



4.2.3 删除用户信息

选择用户，点击"删除"将可删除该用户。需注意:

1. "PRIVILEGE"为 TRUE 的用户不能直接删除；若需要删除，需要删除数据库 ${DOMAIN_HOME}/mydomain/database/userDataBase，修改 ${DOMAIN_HOME}/mydomain/config/admin-keyfile 中对应的用户名为其他用户名，重启 AAS。
2. 系统必须有初始化的对应角色的用户。



4.3 密码策略

安全管理员登录管控平台，可配置密码策略。

密码策略配置项主要总体配置用户的密码的长度复杂度等，具体属性如下:

- **密码长度**: 规定所有用户包括管理员的密码长度要求，必须大于等于设定值；默认为 8 个字符。
- **密码有效天数**: 规定密码从修改日开始的有效天数，超过有效天数则需要重新修改；默认为 30 天。
- **账号有效小时数**: 规定账号的有效小时数，自首次登录开始计时，超过设置的有效小时数后账号将会被禁用；默认为 720 小时。角色为 security 的用户不受影响。
- **密码重试次数**: 用户登陆时允许重试密码的次数，超过此次数则锁定用户；默认为 5 次。
- **密码复杂度**: 普通，必须是大小写英文字母、数字和特殊字符中两者的组合；复杂，必须是大小写英文字母、数字和特殊字符中两者以上的组合；。
- **用户锁定时间**: 用户登录失败后锁定的期限，锁定时间超过该值后会自动解锁。默认为 15 分钟。

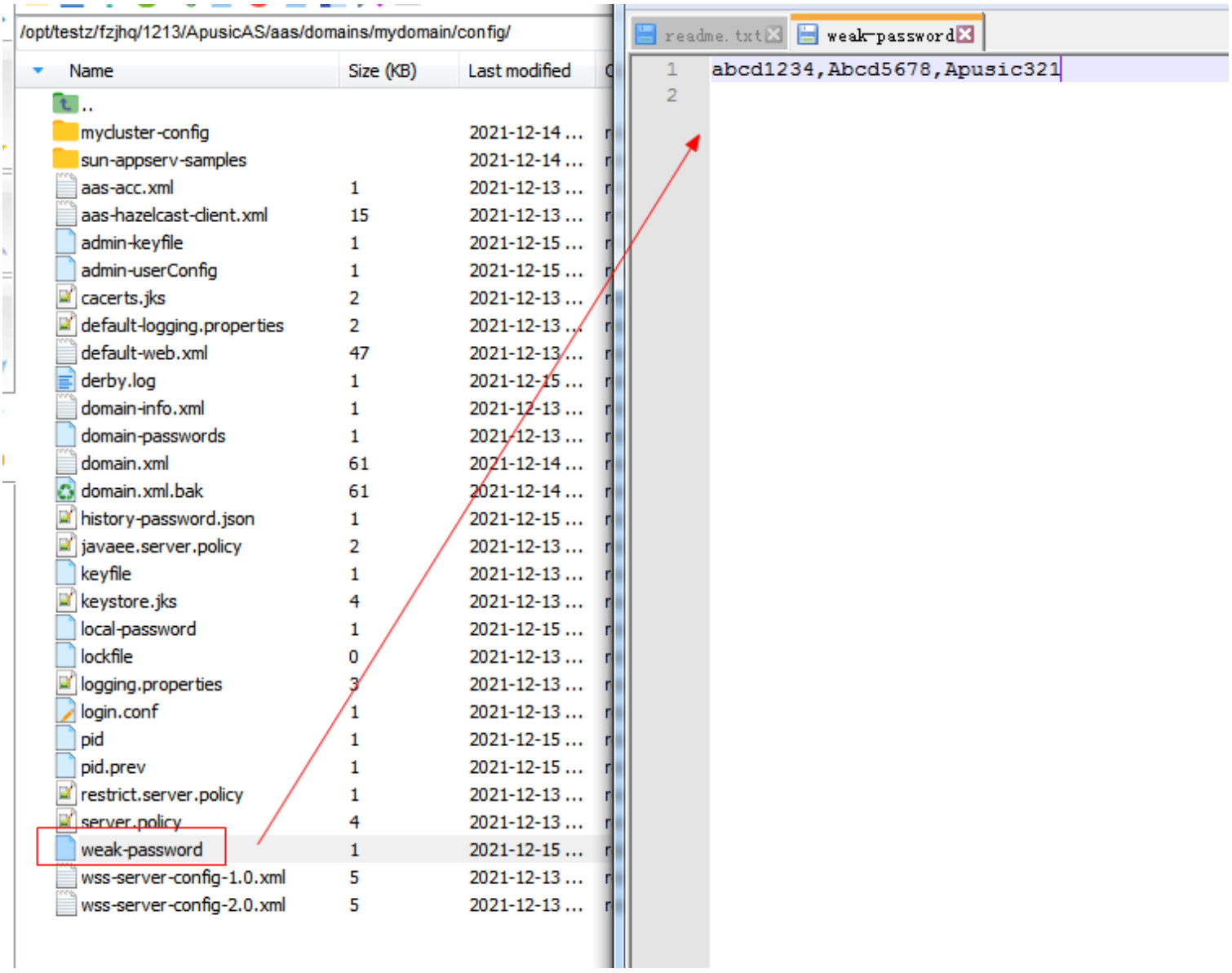
> ***注意**: 用户修改密码时，限制五次内密码不能重复。*

对应 domain.xml

```
<security-service>
    <property name="pwdLength" value="8"></property>
    <property name="pwdValidateDay" value="30"></property>
    <property name="maxLoginAttempts" value="5"></property>
    <property name="pwdComplex" value="common"></property>
```

```
    <property name="pwdRestoreMinute" value="15"></property>
    <property name="validHour" value="720"></property>
</security-service>
```

- **弱密码设置**: 在${DOMAIN_HOME}/config/下创建文件 weak-password，在文件中设置的口令即为弱口令，用户设置口令时校验不允许设置。多个口令用英文,隔开，如设置 abcd1234、Abcd123、Apusic321 为弱口令，用户设置密码为 abcd1234、Abcd123、Apusic321 时校验不允许设置。



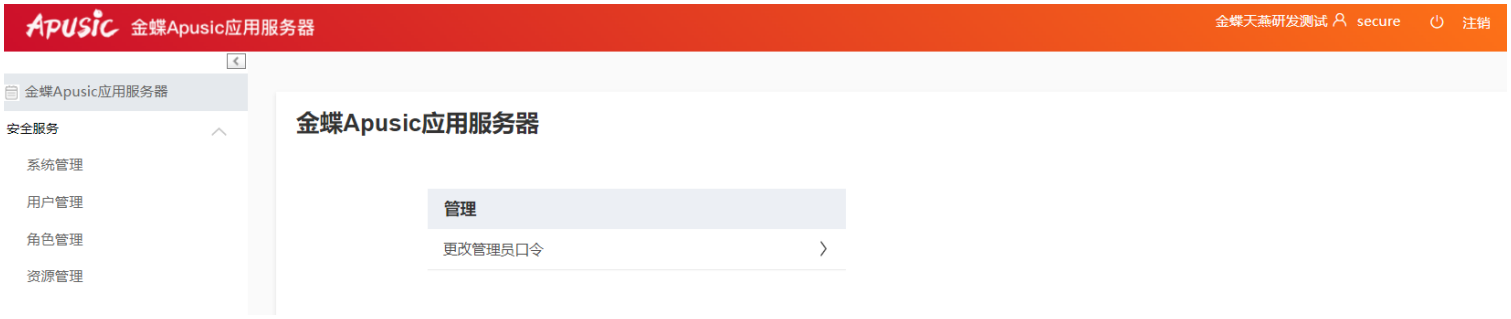
用户密码设置为 abcd1234 时显示提示:

4.4 重置密码

用户重置密码可参考以下方法。

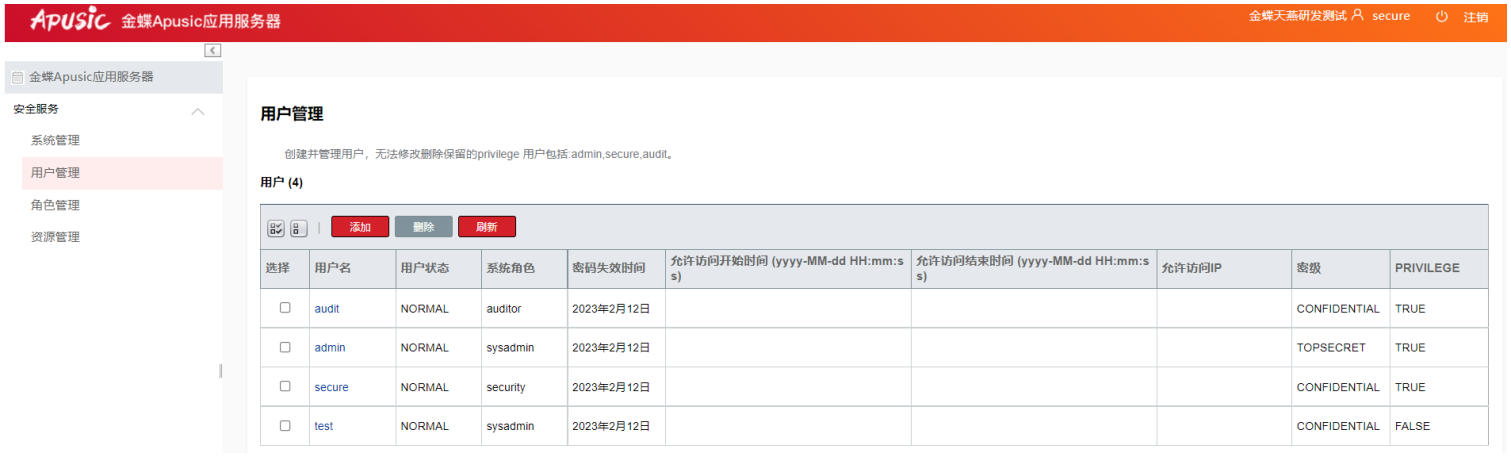
一、当前用户重置密码

当前用户登录管控平台，通过首页进入【管理员口令】页面，可自行修改密码



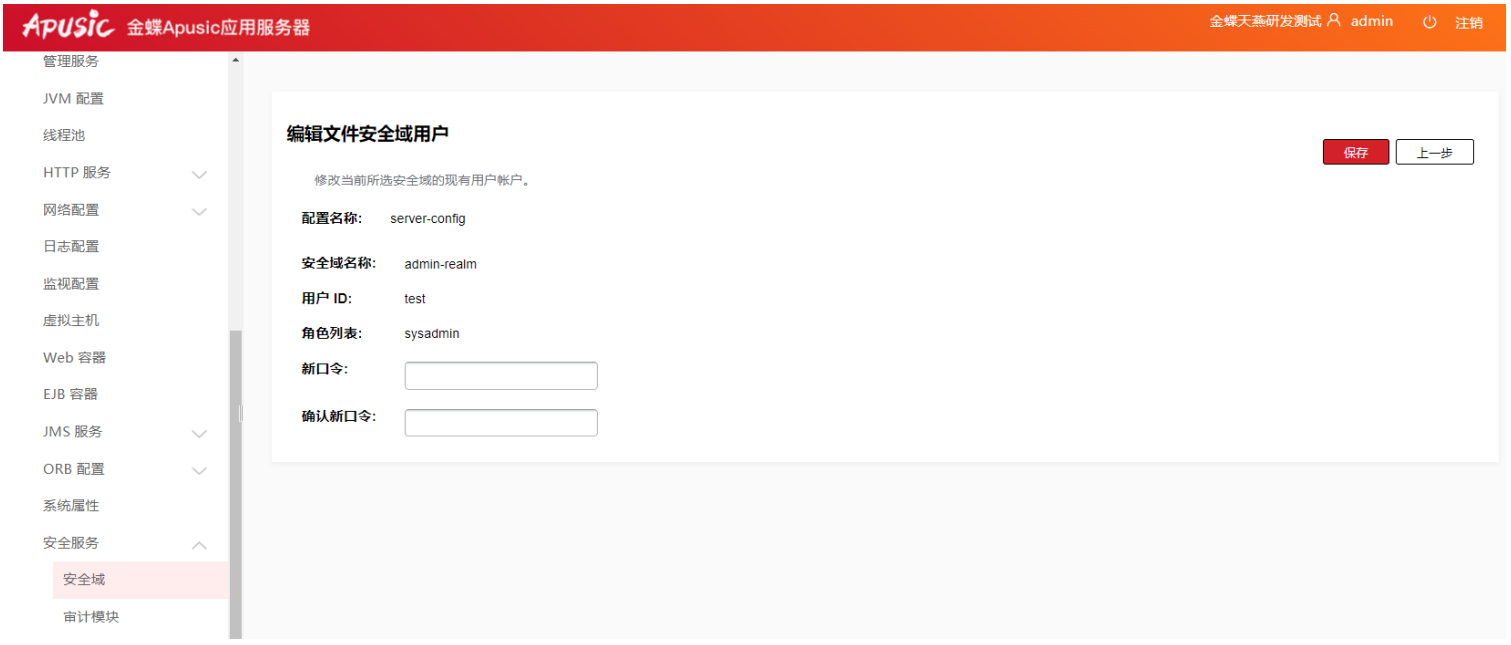
二、通过安全管理员重置用户密码

安全管理员登录管控平台，进入【用户管理】，点击用户名称，进入该用户编辑页面，可以为该用户设置密码



三、通过系统管理员重置用户密码

系统管理员登录管控平台，进入【配置管理】-【server-config】-【安全服务】-【安全域】-【admin-realm】-【管理用户】，点击用户名，进入编辑页面可修改用户密码



四、忘记密码时重置用户密码

方法 1: 如果某个非安全管理的用户，如 admin 密码忘记了，通过安全管理员登录管控平台，为该用户重置密码。

方法 2: 如果某个管理员包括安全管理员和系统管理员密码忘记了，但是其他用户密码知道，就可以拷贝安装路径下 mydomain/config/admin-keyfile 中的其他用户的密码，替换需要修改密码的 用户的密码。需要重启系统才生效。

方法 3: 如果某个管理员包括安全管理员密码忘记了，系统管理员的密码还记得，使用系统管理员 如admin 登陆管理，进入【配置管理】-【server-config】-【安全服务】-【安全域】-【admin-realm】-【管理用户】页面，点击用户名称编辑用户，可以修改用户密码。

方法 4: 修改 mydomain/config/admin-keyfile 文件里面对应的用户的密码，使用如下密码替换 `"{SSHA256}iU4Ef2uGWYh3V+BQjpW5f8BTbgGWzKp7pfrNU020Nu2l9YLEwCWOpA=="`，重置为空密码，重启系统，需要重新设置密码。

4.5 修改初始用户名

一般情况下系统自带初始化三员用户名，分别为 admin/secure/audit，默认情况下不建议修改。如果需要修改的话分两种情况解决。

第一种: AAS 尚未初始化。此时可进入${DOMAIN_HOME}/mydomain/config/admin-keyfile 将对应的用户名修改为需要设置的用户名，保存，启动 AAS。

第二种: AAS 已经初始化。需要删除数据库${DOMAIN_HOME}/mydomain/database/userDataBase；修改${DOMAIN_HOME}/mydomain/config/admin-keyfile 中对应的用户名为需要设置的用户名，保存。启动 AAS，此时需重新输入用户密码。

4.6 审计日志配置

安全管理员可管理审计日志和操作日志配置。

审计和操作配置项主要分别配置审计日志和操作日志的数量和保留时间等信息,具体配置属性如下:

- **审计日志数量上限**: 审计日志存储数据库里的数量限制，超过此限制则从最早的记录开始覆盖。
- **审计日志保留时间**: 审计日志记录保存时间，单位是天。
- **操作日志数量上限**: 操作日志存储数据库里的数量限制，超过此限制则从最早的记录开始覆盖。
- **操作日志保留时间**: 操作日志记录保存时间，单位是天。
- **定时备份周期**: 审计和操作日志设置的定期备份周期，默认保存目录为${DOMAIN_HOME}/audit/timing,单位为月/次。
- **定时备份保留时间**: 定时备份的审计和操作日志保留的时间，单位为天。-1 表示永久保留。

```
<security-service>
<property name="maxAuditLogNum" value="10000"></property>
<property name="maxAuditLogPreservedDay" value="180"></property>
```

```
<property name="maxOperateLogNum" value="10000"></property>
<property name="maxOperateLogPreservedDay" value="180"></property>
<property name="timingBackupCycle" value="1"></property>
<property name="timingBackupSaveDay" value="-1"></property>
</security-service>
```

日志配置:

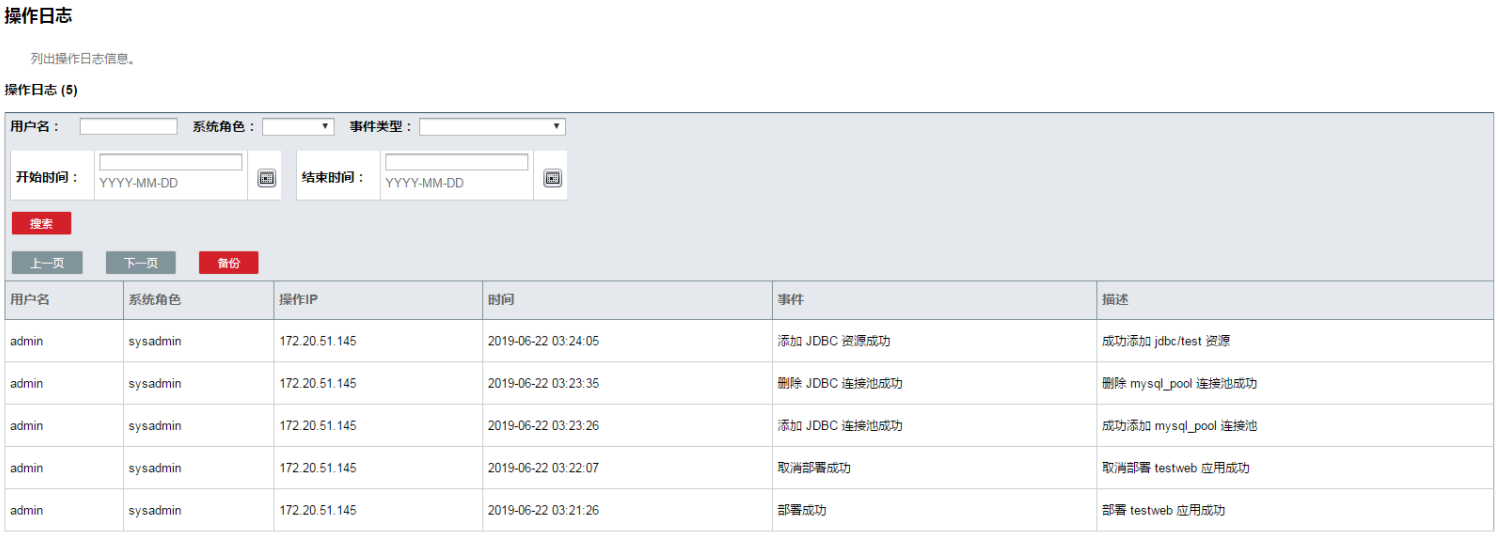
审计日志数量上限:	10000	
审计日志保留时间：	180	天
操作日志数量上限:	10000	
操作日志保留时间：	180	天
定时备份周期：	1	月/次
定时备份保留时间：	-1	天
	若为-1表示永久保留	

5 审计管理员操作

对系统重要的操作，敏感数据等操作或者一些非法操作等系统会生成相应的日志，审计员可以对这些日志进行审计。

5.1 操作日志

使用角色为审计管理员（auditor）的用户登录管控，切换到操作日志界面。



用户名	系统角色	操作IP	时间	事件	描述
admin	sysadmin	172.20.51.145	2019-06-22 03:24:05	添加 JDBC 资源成功	成功添加 jdbc/test 资源
admin	sysadmin	172.20.51.145	2019-06-22 03:23:35	删除 JDBC 连接池成功	删除 mysql_pool 连接池成功
admin	sysadmin	172.20.51.145	2019-06-22 03:23:26	添加 JDBC 连接池成功	成功添加 mysql_pool 连接池
admin	sysadmin	172.20.51.145	2019-06-22 03:22:07	取消部署成功	取消部署 testweb 应用成功
admin	sysadmin	172.20.51.145	2019-06-22 03:21:26	部署成功	部署 testweb 应用成功

在操作日志界面可以做如下操作:

- 可以查看系统所有的操作日志，并且可以根据添加进行过滤查询。
- 点击【备份】按钮可以对操作日志进行备份操作，备份的日志文件存放在 ${APUSIC_HOME}/domain_name/audit 目录下。

5.2 审计日志

使用角色为审计员的用户登录管控，切换到审计日志界面。

审计日志

列出审计日志信息。

审计日志 (15)

用户名： 系统角色： 事件类型：

开始时间： YYYY-MM-DD 结束时间： YYYY-MM-DD

搜索

上一页 下一页 备份

用户名	系统角色	操作IP	时间	事件	描述
admin	sysadmin	172.20.51.145	2019-06-22 03:20:29	登录成功	
audit	auditor	172.20.51.145	2019-06-22 03:19:47	登录成功	
audit	auditor	172.20.51.145	2019-06-22 03:14:53	登录成功	
secure	security	172.20.51.145	2019-06-22 03:14:40	注销	
secure	security	172.20.51.145	2019-06-22 03:14:20	登录成功	
admin	sysadmin	172.20.51.145	2019-06-22 03:14:04	注销	
secure	security	172.20.51.145	2019-06-22 03:00:23	登录成功	
admin	sysadmin	172.20.51.145	2019-06-22 03:00:06	注销	
admin	sysadmin	172.20.51.145	2019-06-22 02:59:46	登录成功	
admin	sysadmin	172.20.51.145	2019-06-22 02:55:42	登录成功	

在审计日志界面可以做如下操作:

- 可以查看系统所有的审计日志，并且可以根据添加进行过滤查询。
- 点击【备份】按钮可以对审计日志进行备份操作，备份的日志文件存放在 ${APUSIC_HOME}/domain_name/audit 目录下。

6 系统管理员操作

系统管理员主要管理应用部署、资源管理、配置管理等功能。

6.1 应用管理

使用系统管理员登录系统，对应用程序相关属性进行设置。

应用程序界面用于管理当前域实例以及所有独立实例和集群实例的应用程序，应用程序可以是企业应用程序, Web 应用程序或各种类型的模块。通过单击重新加载链接重新启动应用程序或模块,此操作仅适用于启用了应用程序或模块的目标。

"应用程序"页面显示 Apusic 应用服务器上部署的应用程序列表。您可以查看和管理已部署的应用程序，还可以部署更多应用程序。

对于每个应用程序，提供以下信息。

- **名称**: 应用程序名称。
- **部署顺序**: 应用程序的部署顺序。具有较低编号的应用程序首先在服务器启动时加载。在部署顺序为 110 的应用程序之前加载部署顺序为 102 的应用程序。如果在部署应用程序时未指定部署顺序，则会分配默认部署顺序 100。如果两个应用程序具有相同的部署顺序，则首先加载首先部署的应用程序。如果应用程序具有依赖关系并且必须按特定顺序加载，则指定部署顺序非常有用。
- **状态**: 应用程序在目标实例中的是否启用状态。
- **引擎**: 应用程序使用的容器类型。容器类型可以是以下任何一种:
    - web
    - webservices

    - ejb
    - connector
    - appclient
    - weld（Java EE 平台应用程序的上下文和依赖注入的容器）
    - eba
    - osgi
- **操作**: 指向部署后可在组件上执行的操作的链接: 为所有组件重新部署和重新加载，为 Web 应用程序和应用程序客户端启动，以及为应用程序客户端下载客户端存根。

"应用程序"表还包含以下选项。

- **部署**: 用于部署应用程序的按钮。
- **取消部署**: 按钮取消部署一个或多个选定的应用程序，会取消该应用程序在所有目标实例上的部署。
- **启用**: 如果仅 server 存在默认服务器实例，则启用一个或多个所选应用程序的按钮。
- **禁用**: 如果仅 server 存在默认服务器实例，则禁用一个或多个所选应用程序的按钮。
- **过滤器**: 按引擎过滤应用程序的下拉列表。

6.1.1 部署应用程序

使用"部署应用程序或模块"页面部署应用程序，应用程序可以采用打包的文件格式, 也可以指定为目录。

分为4个步骤，第一步为【部署应用】。该步骤主要为上传应用程序文件。”下一步“表示进入【部署属性】页面，”返回“表示返回列表页面

配置项	说明	默认值
路径	上传应用文件，可以选择“要上传到服务器的打包文件”或“可以从 Apusic 应用服务器访问的本地打包文件或目录”	要上传到服务器的打包文件
要上传到服务器的打包文件	从本地选择应用程序部署，格式包括war, ear, eba, rar, jar, appClient	
可以从 Apusic 应用服务器访问的本地打包文件或目录	从服务器选择应用程序包或者目录部署。“浏览文件”为上传打包文件，“浏览文件夹”为上传目录文件。 使用文件夹方式部署不能部署到远程实例，如果需要部署，需要在远程节点目录中创建一个与应用程序所在的位置相同的目录，且需要有对应权限。如应用程序所在的位置为/opt/testz/，远程目录也要有/opt/testz/，testz/下的内容需要相同	

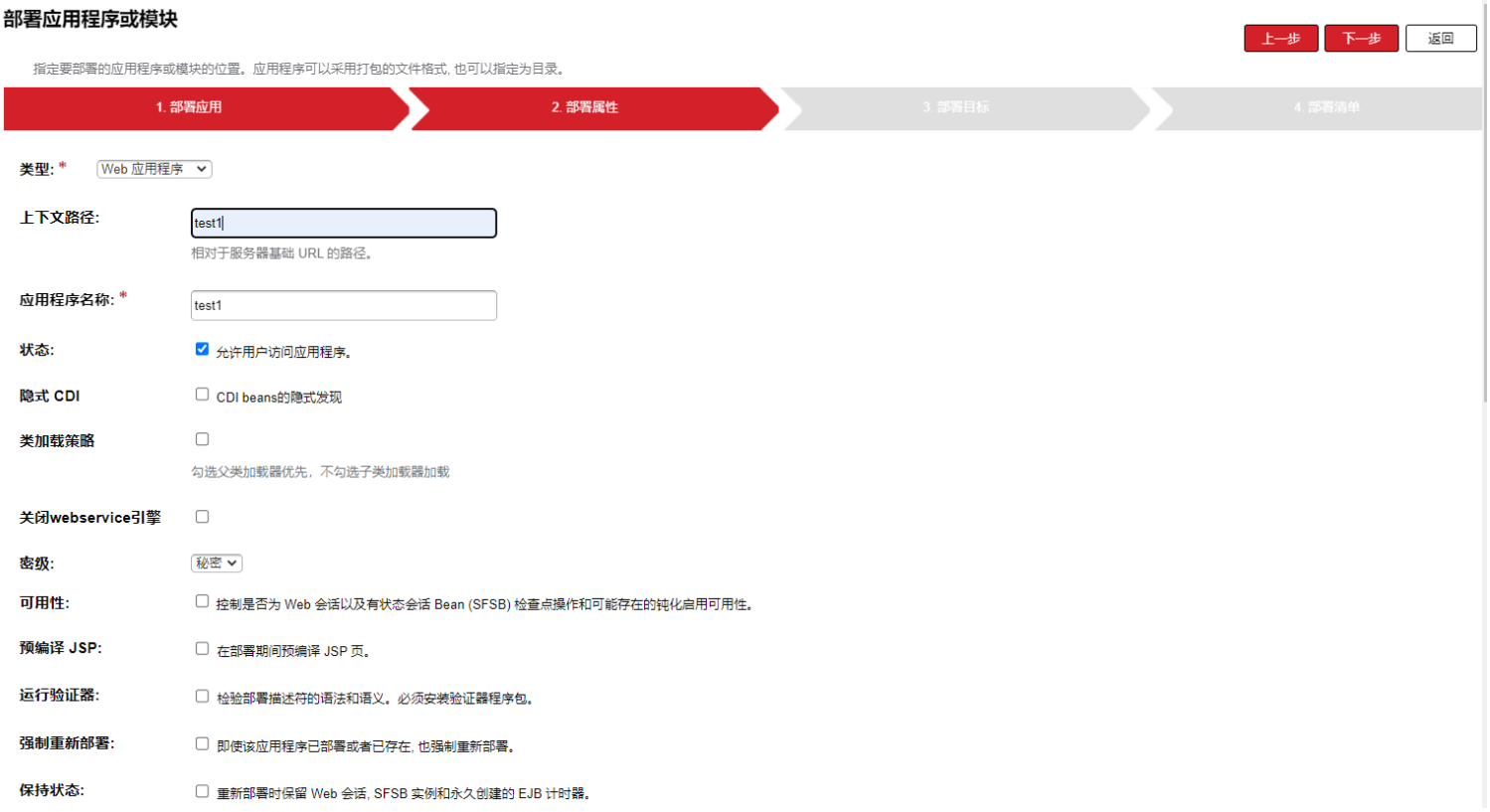
上传	选择完成应用打包文件或者目录之后，需要点击“上传”按钮，上传后可以检测出该应用的类型。如果是ear包，将会检测出该应用程序包含的模块，如ejb/web等	

第二步为【部署属性】。该步骤主要为配置应用程序相关属性。“上一步”表示返回【部署应用】页面，”下一步“表示进入【部署目标】页面，”返回“表示返回列表页面

配置项	说明	默认值
类型	应用程序的类型。可用的选择是: Web 应用程序 企业应用 程序 EBA应用程序 应用程序客户端 连接器模块 EJB Jar 其他	根据上传的应用打包文件显示对应类型
上下文路径	应用程序相对于服务器基础 URL 的路径，通常情况下应用程序的类型为web应用时设置。例如输入/test，访问时为 http://IP:PORT/test。不输入时会自动生成，一般为[应用程序名称]+日期	
应用程序名称	当前部署的应用程序名称，需要唯一	应用文件名称
选择部署模块	当企业应用程序有web/ejb或其他模块时会显示该属性；可根据需要选择部署模块。默认全选	web、ejb都启用
可用性	如果选中复选框，则会为 Web 会话和有状态会话 Bean（SFSB）检查点以及可能的钝化启用高可用性。一般为配置了服务器集群才显示，使用 session 复制时需要勾选	不启用
状态	为真时，允许用户访问应用程序	启用

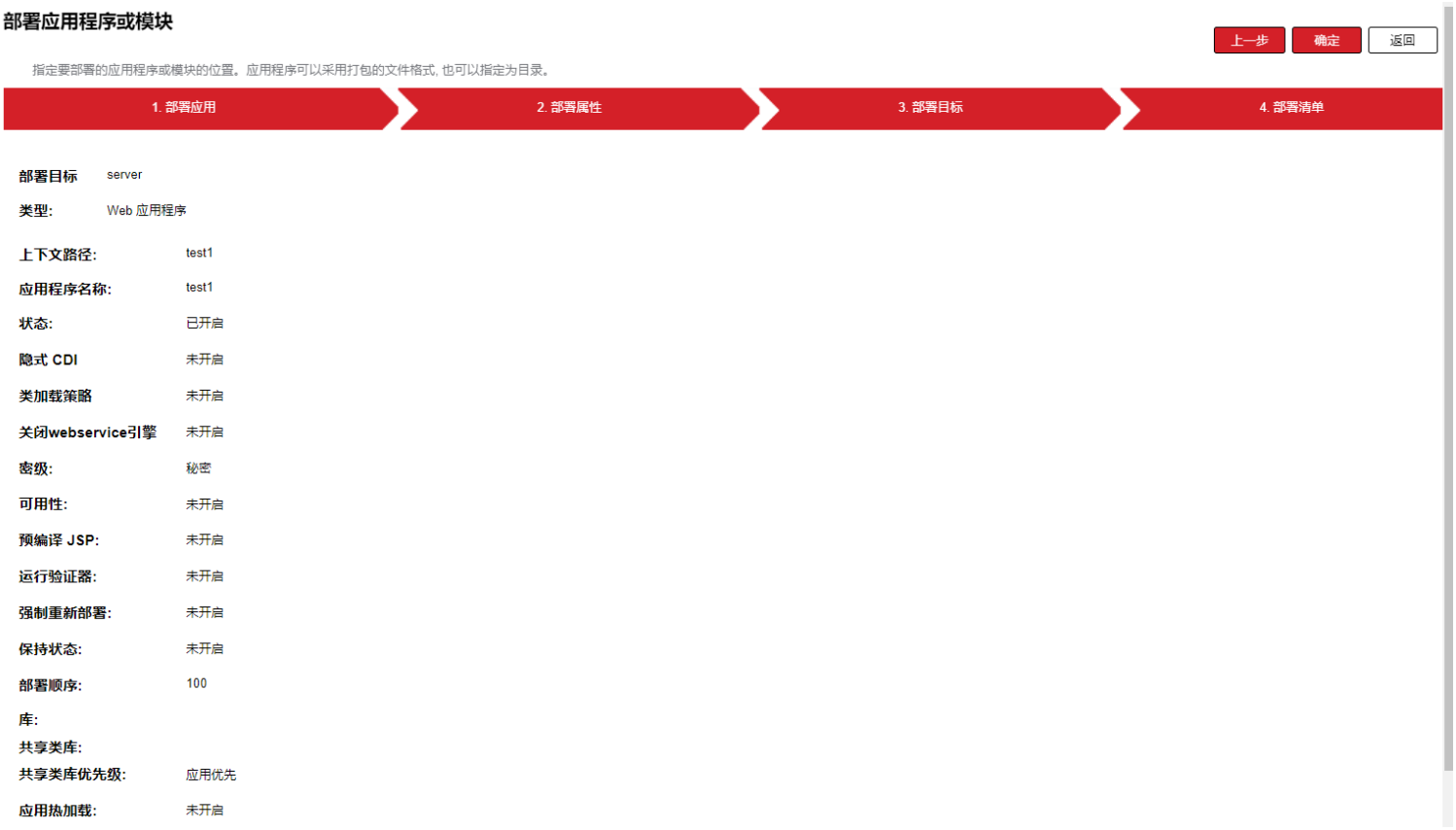
隐式 CDI	Java EE 的上下文和依赖注入（Contexts and Dependency Injection for Java EE，CDI）为真时，CDI beans 的隐式发现。 全局取消"隐式CDI"，在 config-server 下添加	不启用
类加载策略	勾选父类加载器优先，不勾选子类加载器加载。除了java,javax, sun, org.xml.sax, org.w3c.dom, org.apache.taglibs.standard, com.sun.faces, org.apache.commons.logging 开头的包强制遵循双亲类加载机制（需通过额外jvm参数打破此机制）。通常用于应用程序与AAS有类冲突的情况	不启用
密级	为该应用程序设置密级，限制有权限的角色可操作	秘密
OSGI类型	设置组件是否为已打包为 OSGi 绑定，一般在"类型"为"其他"才会显示	不启用
Java Web Start	为该应用程序设置密级，限制有权限的角色可操作	启用
预编译 JSP	为真时，在部署期间预编译 JSP 页，文件解压在${DOMAIN_HOME}/generated/下	不启用
运行验证器	为真时，检验部署描述符的语法和语义。必须安装验证器程序包	不启用
强制重新部署	为真时，即使该应用程序已部署或者已存在, 也强制重新部署	不启用
保存状态	为真时，重新部署时保留 Web 会话, SFSB 实例和永久创建的 EJB 计时器	不启用
库	以逗号分隔的库 JAR 文件列表。按照相对或绝对路径指定库 JAR 文件。指定相对于 instance-root/lib/applibs 的相对路径。这些库按指定顺序提供给应用程序使用	
共享类库	设置该应用引用共享类库。可在【共享类库】配置	不启用
共享类库优先级	设置共享类库加载顺序，可设置项为： 共享类库优先：共享类库 >应用classes文件夹 >应用lib包 Classes目录优先：应用classes文件夹 >共享类库 >应用lib包 应用优先：应用classes文件夹 >应用lib包 >共享类库	应用优先
应用热加载	勾选表示启用应用热加载功能	不启用
应用热加载延迟时间	开启"应用热加载后，检测到应用发生修改后的延迟加载时间	60秒
会话储存	配置会话管理，可在【会话缓存】配置。设置后，该应用程序使用会话管理器	不启用

开启AAS内置组件组件	部署该应用程序时，需要同时开启AAS内置的组件。包括JPA、JSF、CDI、Bean Validation、JSONP、RESTful、Web Service。多选。该功能需要根据应用实际设置	JPA、CDI、Web Service
说明	部署说明	



第三步为【部署目标】。该步骤主要为配置应用程序的部署目标，默认为server。“上一步”表示返回【部署属性】页面，“下一步”表示进入【部署清单】页面，“返回”表示返回列表页面。

第四步为【部署清单】。该步骤主要为展示应用程序的部署清单。“上一步”表示返回【部署目标】页面，“确定”表示将会开始部署该应用程序，部署成功后会返回列表页面，“返回”表示返回列表页面。



6.1.2 访问应用程序

默认监听端口情况下，可在浏览器中访问 `http://IP:6888/[context]` 或 `https://IP:6887/[context]` 。

也可在应用程序列表中的操作栏中点击【访问】按钮，出现应用程序链接页面，该页面中显示通过各目标实例访问应用的访问链接，点击链接可以访问到该应用。

如果是 ear 文件，需要进入编辑页面模块和组件部分进入"访问"，或在浏览器手动输入访问地址。

6.2 其他功能模块

系统管理员其他功能模块请参考《金蝶Apusic应用服务器V10用户手册》。

全国统一服务热线

4008-555-800

金蝶天燕云计算股份有限公司(简称“金蝶天燕云”)成立于2000年，前身为“金蝶中间件公司”，是金蝶集团旗下新一代软件基础云平台服务商，云计算国家标准制定企业，国家信创产业核心软件企业。金蝶天燕是国家863重点研发计划与核高基重大专项承接企业，也是“两网一站四库十二金”国家重点工程的基础平台提供商，产品广泛应用于政府、军工、金融、能源等关键行业，累计服务客户总数超过10万家。

Apusic 金蝶天燕

云计算国家标准制定企业

金蝶集团旗下基础软件企业

信息技术应用创新核心企业

官网：www.apusic.com