Apusic 金蝶天燕

生成时间：2026-05-19


# 等级保护指南

金蝶Apusic应用服务器V9

## 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 |
| --- | --- | --- | --- |
| 2024年2月 | V9E02F01 | AAS V9.0 | 更新三员说明 |

# 2 前言

本文档是金蝶Apusic应用服务器V9的等级保护指南，详细介绍等级保护相关配置使用说明。

## 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应用服务器等级保护指南内容：

- 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

# 3 等级保护

等保的全称是信息安全等级保护，是我国网络安全领域的基本国策、基本制度。等级保护不仅仅是针对信息系统程序安全，还包括物理安全、应用安全、通信安全、边界安全、环境安全、管理安全等方面。

金蝶Apusic应用服务器提供满足等保要求的功能。

# 4 三员分立

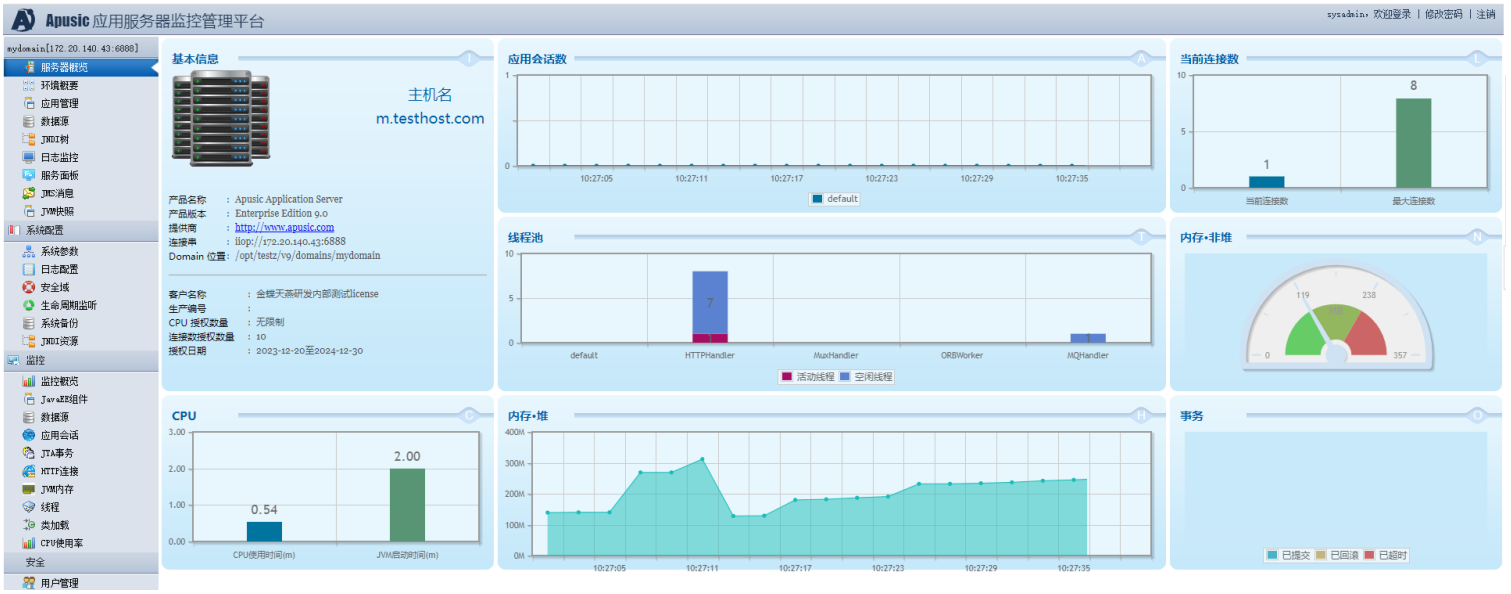
金蝶Apusic应用服务器支持三员分立功能，提供安全保密管理员、安全审计员、系统管理员三个角色。其中安全保密管理员主要管理角色管理、用户管理、密码策略等信息；安全审计员主要管理日志、操作审计信息；系统管理员主要管理应用部署、资源管理、配置管理等功能。

金蝶Apusic应用服务器默认带有管理员用户角色，安全保密管理员（security）默认用户为security；安全审计员（audit）默认用户为auditor；角色为系统管理员（system）默认用户为sysadmin。应用服务器中至少需要保留三员角色，每个角色至少需要有一个可用的用户。默认管理员用户的默认密码为 `1qazXSW@` 。初次登录需要更改密码。

角色为安全保密管理员（security）的用户访问,如使用默认安全保密管理员用户 security登录，进入到系统界面如下:


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

角色为系统管理员（system）的用户访问，如使用默认系统管理员用户sysadmin登录，进入到系统界面如下:



# 5 角色管理

安全管理员登录管控平台，可管理角色信息。

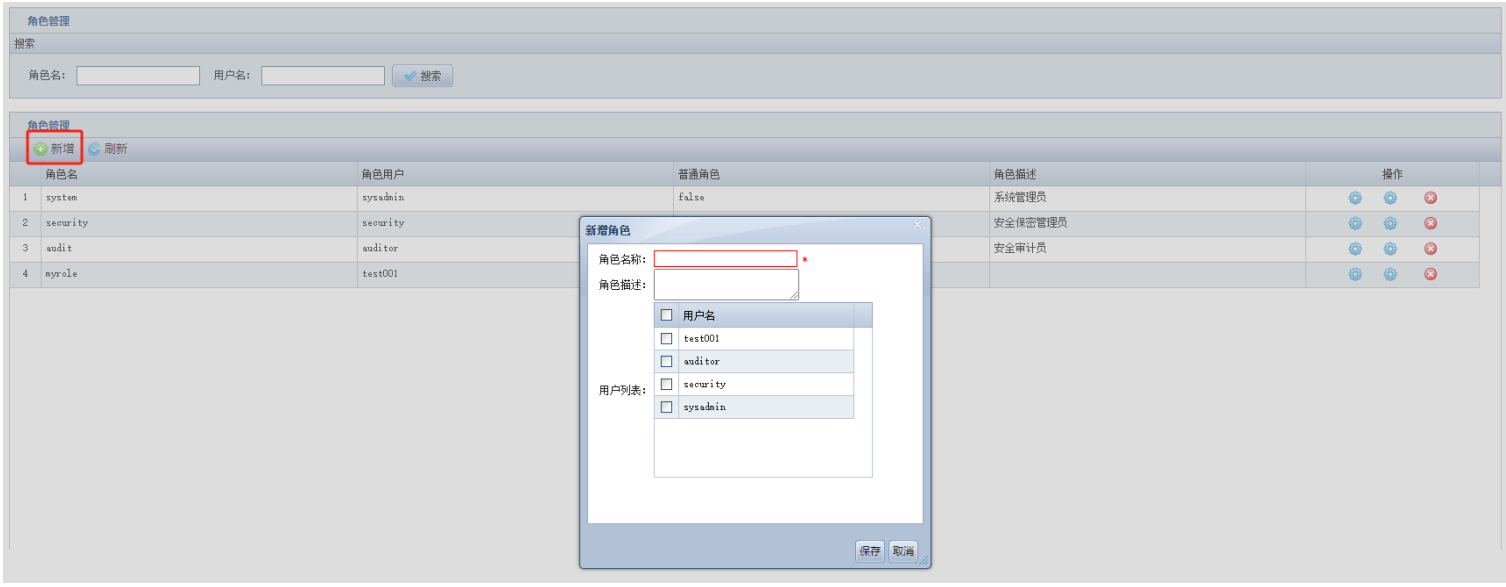
创建并管理角色，金蝶Apusic应用服务器自带角色包括 system,security,audit。

- **角色名**: 角色的名称。
- **角色用户**: 当前角色下的用户，角色 system,security,audit必须有一个以上的用户，且用户只能为一个角色，【用户管理】中设置"系统角色"将实时更新。
- **普通角色**: 当前角色是否为普通角色； 非普通角色非必要，不要删除。


## 5.1 新建角色

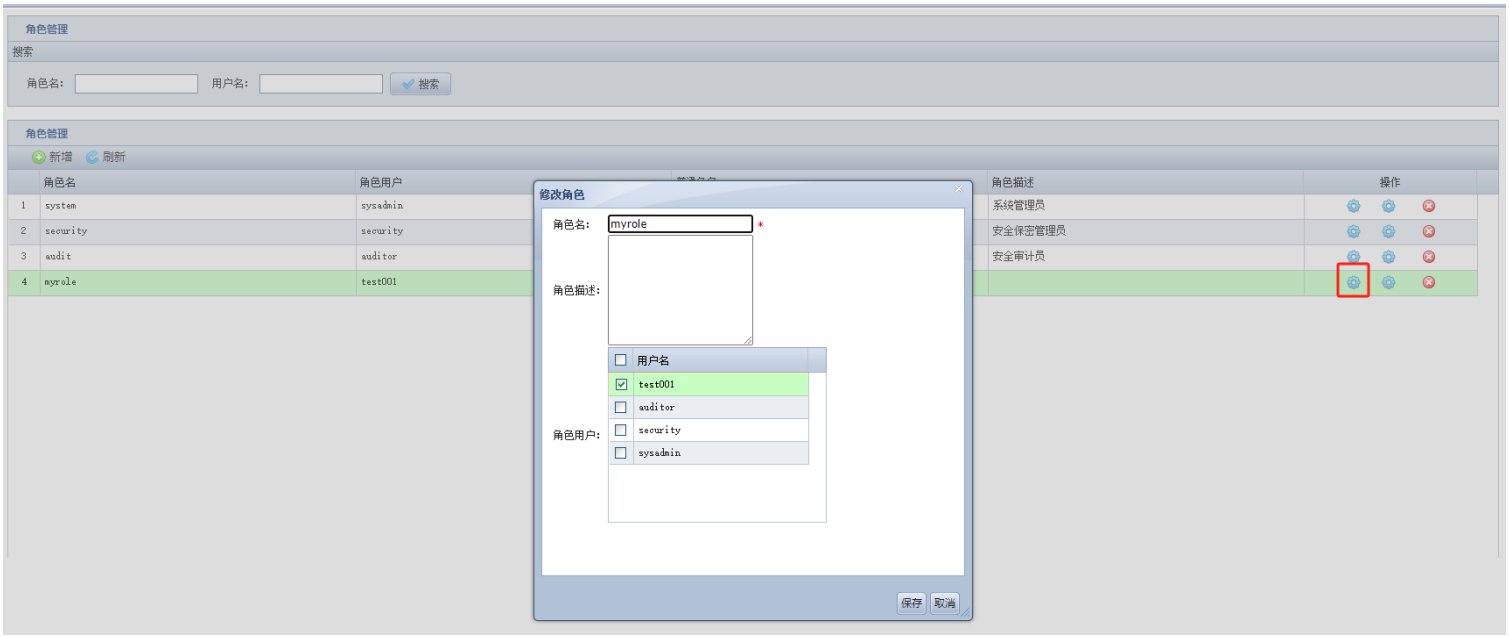
点击"新建"，进入新建系统角色页面。

- **角色名**: 角色的名称，只能包含字母数字,下划线,短横线或点字符，需要唯一。
- **角色描述**: 对角色进行说明。
- **用户列表**: 设置当前角色的用户，可以选择多选。




## 5.2 编辑角色

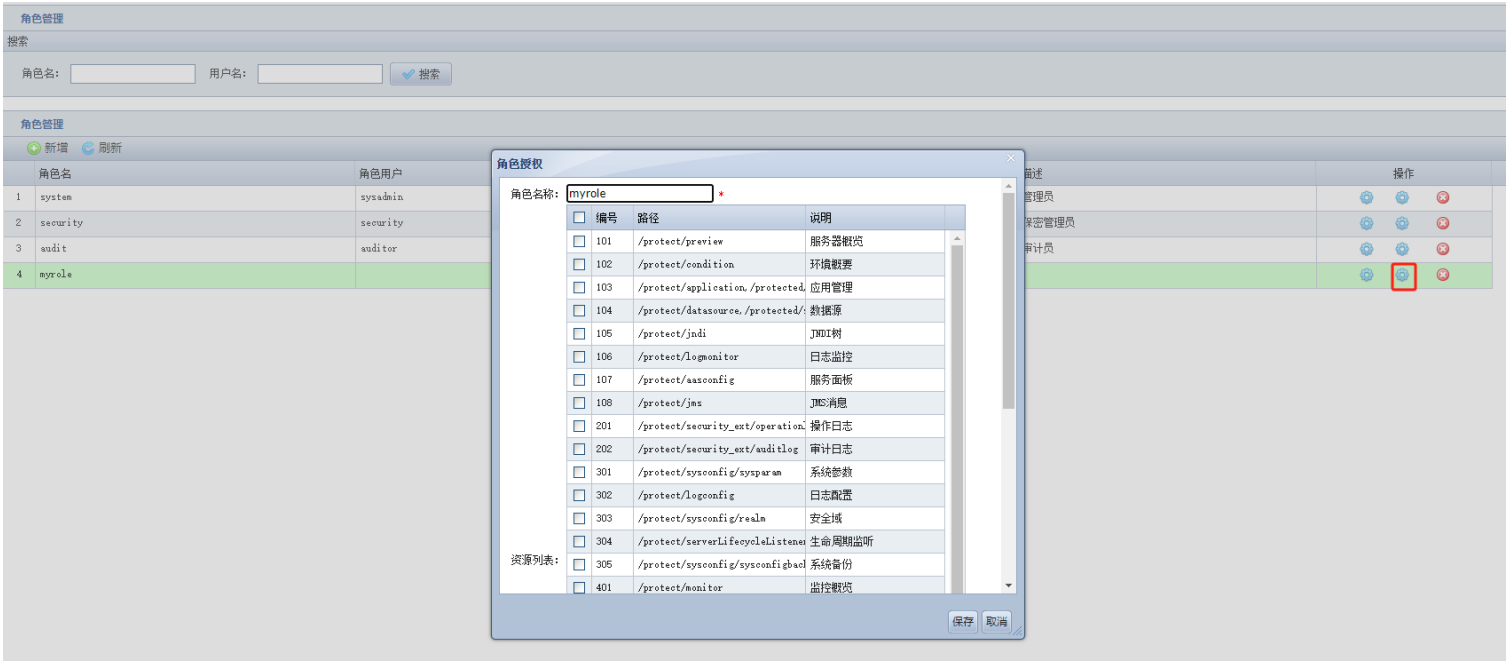
点击角色列表中的“操作”-“编辑角色”，将进入修改角色页面，可对角色信息进行编辑。修改后，用户需要重新登录管控平台才能生效。




## 5.3 角色授权

点击角色列表中的“操作”-“角色授权”，将进入角色授权页面，可为角色添加资源，建议选择“编号”101。修改后，用户需要重新登录管控平台才能生效。

需注意，非必要，不要修改默认角色的资源列表。




## 5.4 删除角色

点击角色列表中的“操作”-“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 system,security,audit，非必要不能删除。

# 6 用户管理

角色为安全保密员（security）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。

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。

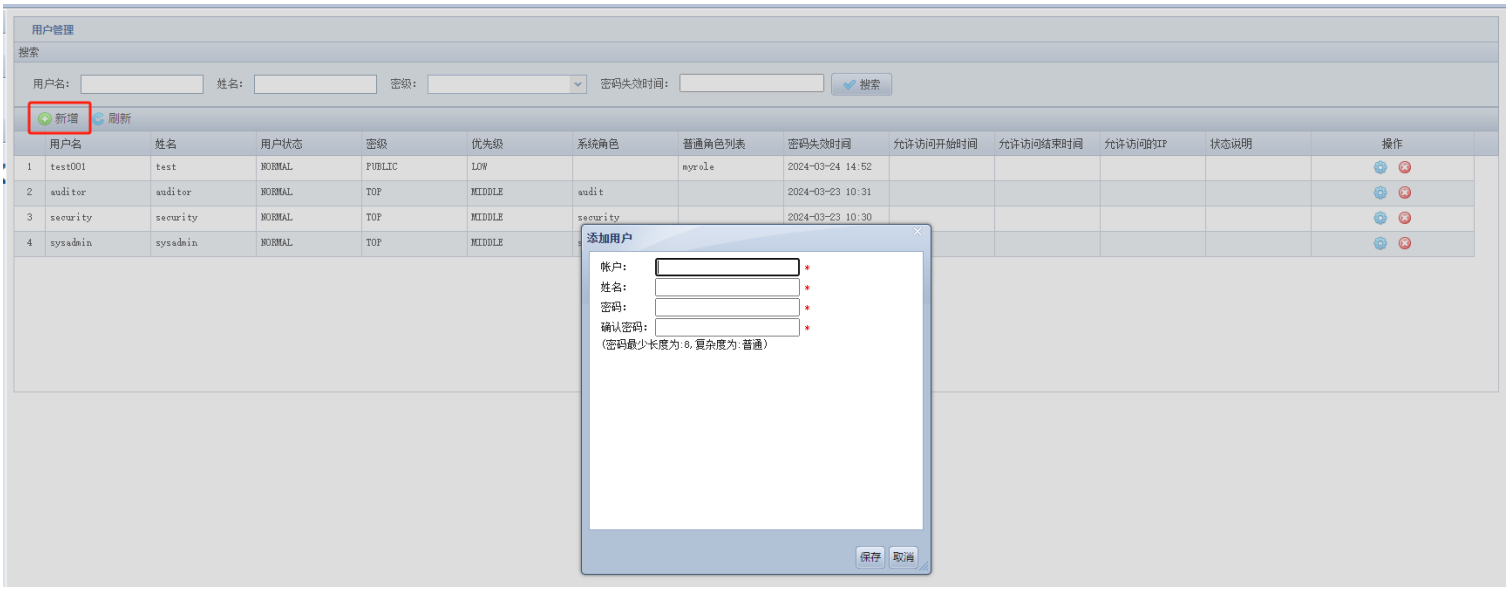
- **用户名**: 应用服务器的用户名称，需要唯一，需要使用用户名登录管控平台。
- **姓名**: 该用户的名字。
- **用户状态**: 显示用户的状态。NORMAL为正常状态；LOCK为锁定，锁定时间默认为15分钟；DISABLED为禁用，此时无法访问。
- **系统角色**: 该用户为系统角色，每个默认系统角色最少需要一个用户。
- **普通角色列表**: 该用户为普通角色。
- **密码失效时间**: 显示密码的失效时间，默认为初始化用户后 30 天，在【系统管理】中修改"密码失效时间"，该处的时间将会同步修改。
- **允许访问开始时间（HH: MM）**: 用户允许访问管控台的开始时间，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。


## 6.1 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。



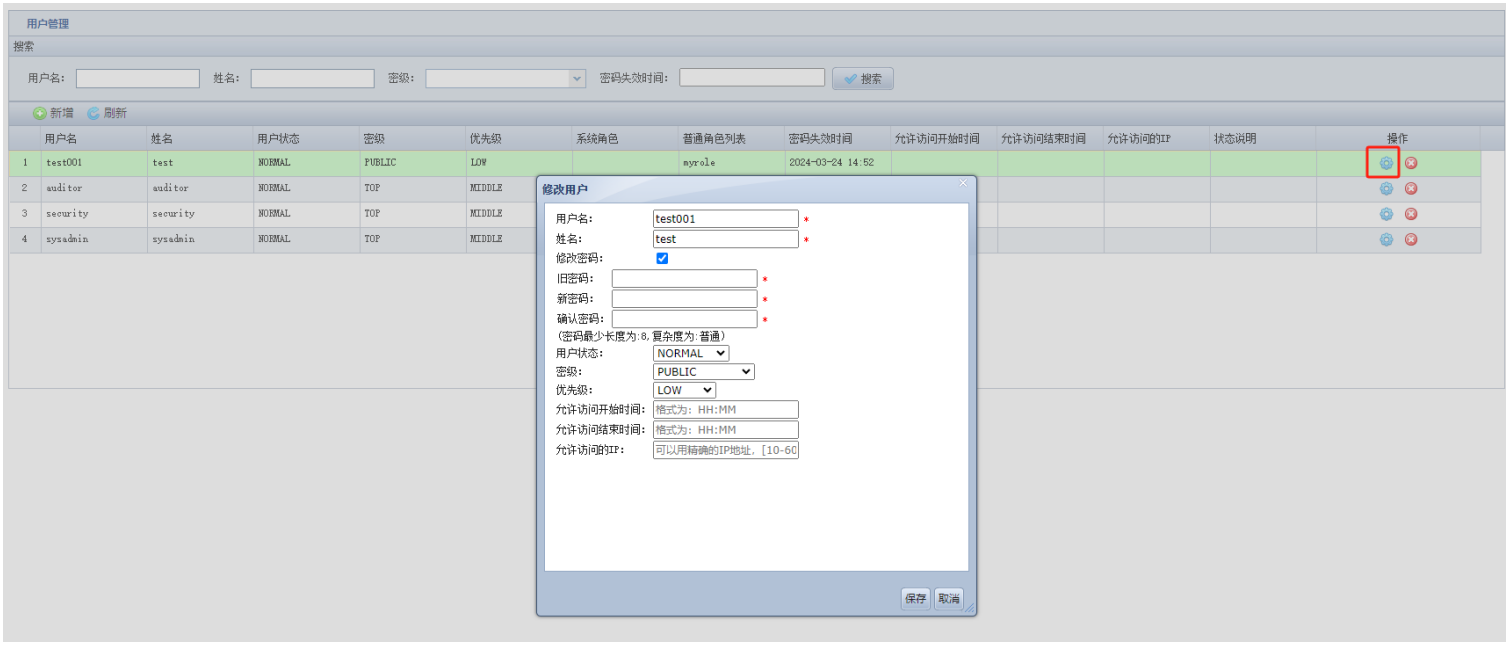

## 6.2 编辑用户信息

点击"用户管理"列表中的"操作"-"编辑用户"，进入对应用户的编辑页面。

- **用户名**: 该用户的名称，不能编辑。
- **姓名**: 该用户的姓名。
- **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。
- **修改密码**: 点击可以修改密码。
- **旧密码**: 修改密码时需要输入用户的旧密码。
- **新密码**: 设置用户的密码，【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。
- **确认新密码**: 需要输入与"新密码"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。*




## 6.3 删除用户信息

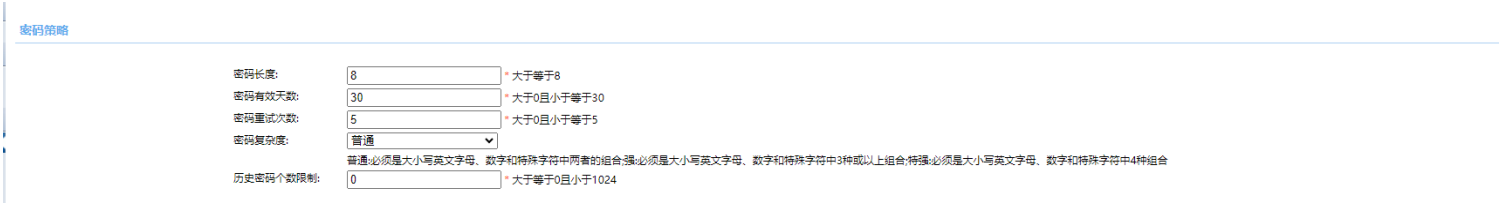
点击"用户管理"列表中的"操作"-"删除"，确认删除后将可删除该用户。需注意:系统必须有 system,security,audit分别对应的用户。

# 7 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。
- **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；。
- **历史密码个数限制**: 修改用户密码时，限制多少次内密码不能重复。

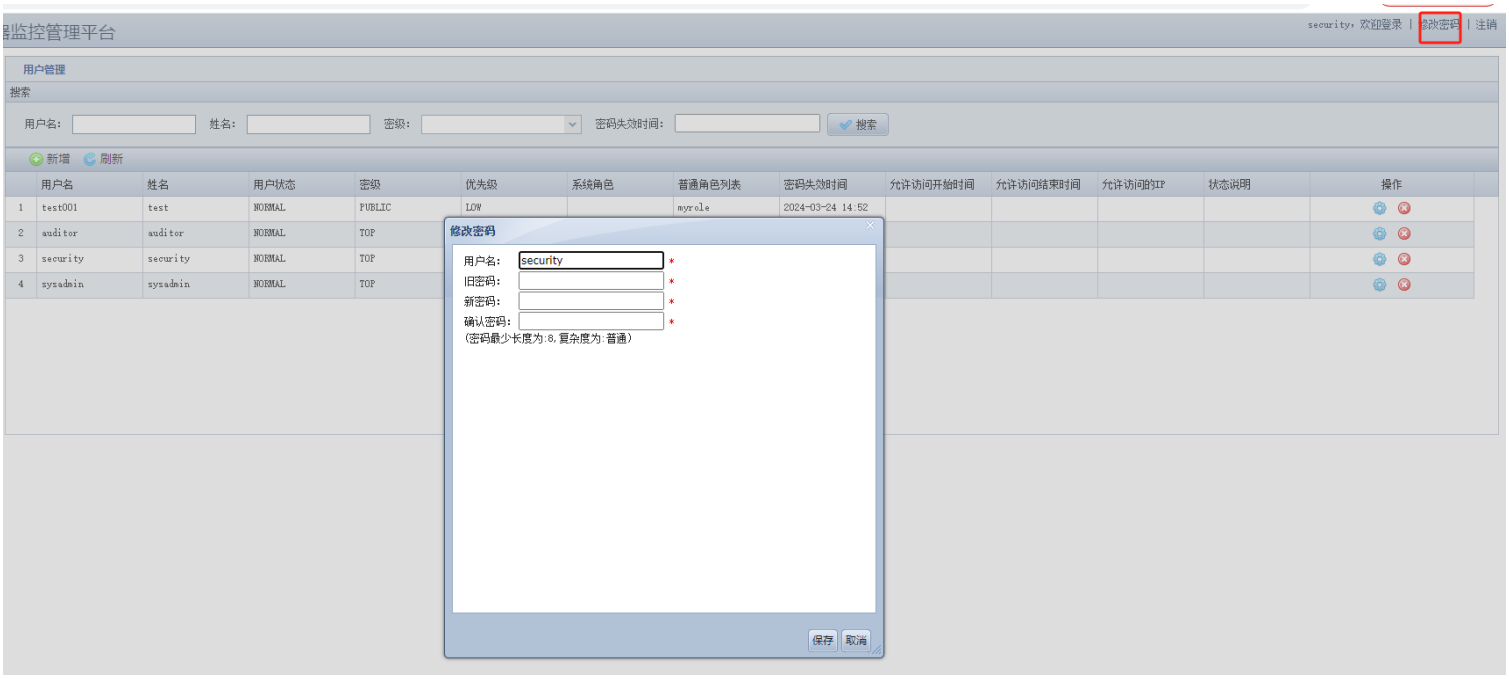


# 8 重置密码

用户重置密码可参考以下方法。

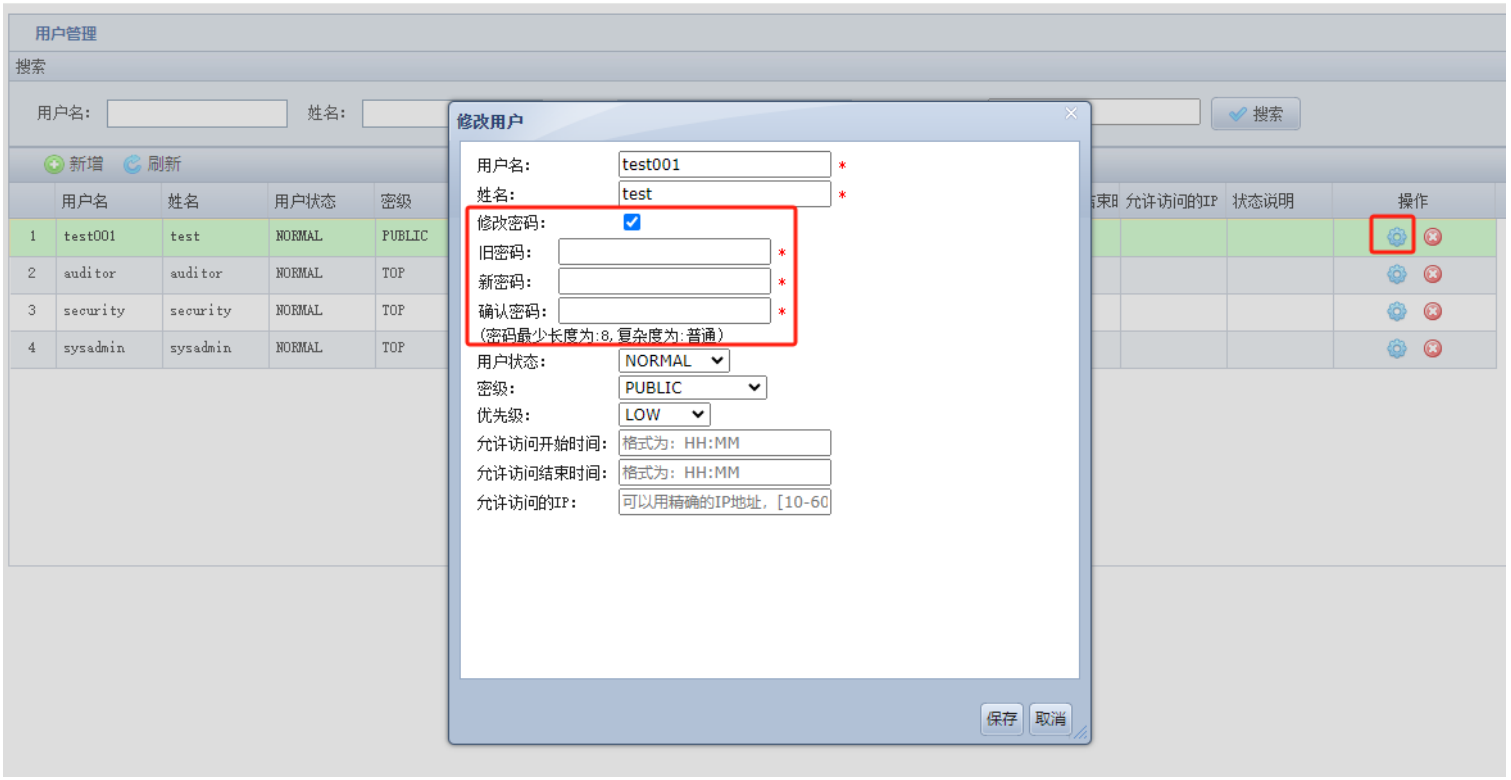
一、当前用户重置密码

当前用户登录管控平台，通过右上角"修改密码，进入【修改密码】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】，点击用户名称中的"操作，进入该用户编辑页面，可以为该用户设置密码。

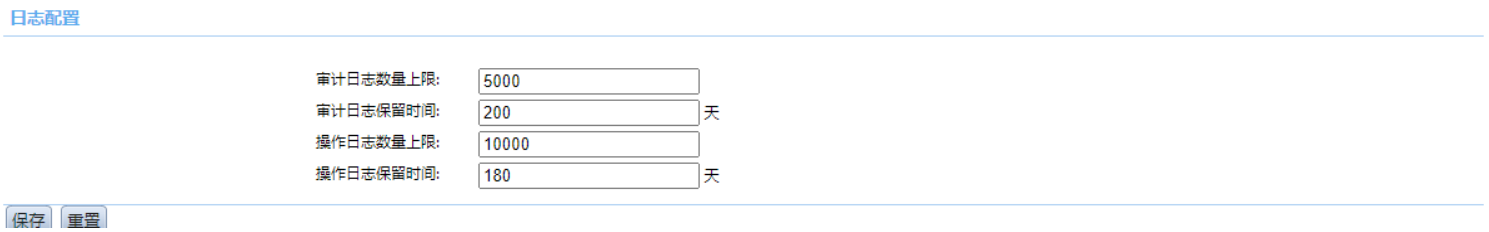

用户管理
搜索
用户名:
姓名:
搜索
新增
刷新
用户名
姓名
用户状态
密级
允许访问的IP
状态说明
操作
1 testOO1 test NORMAL PUBLIC
2 auditor auditor NORMAL TOP
3 security security NORMAL TOP
4 sysadmin sysadmin NORMAL TOP
修改用户
用户名: test001
姓名: test
修改密码:
旧密码:
新密码:
确认密码:
(密码最少长度为:8,复杂度为:普通)
用户状态: NORMAL
密级: PUBLIC
优先级: LOW
允许访问开始时间: 格式为：HH:MM
允许访问结束时间: 格式为：HH:MM
允许访问的IP: 可以用精确的IP地址，[10-60
保存
取消

# 9 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。



# 10 日志审计

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。

## 10.1 操作日志

使用角色为审计管理员（audit）的用户，如默认审计管理员auditor，登录管控，切换到操作日志界面。


## 10.2 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。

在审计日志界面可以做如下操作:

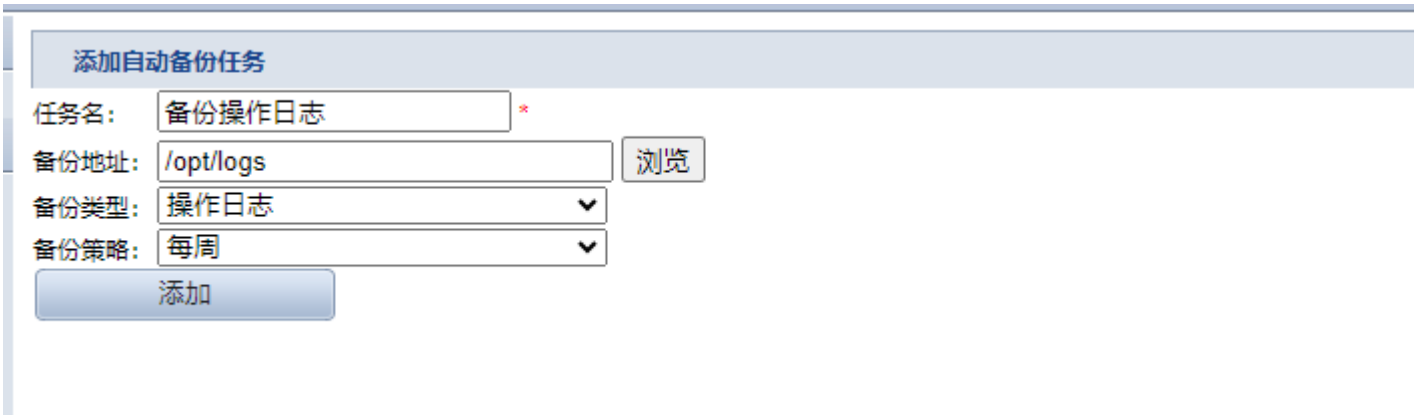
- 可以查看系统所有的审计日志，并且可以根据添加进行过滤查询。
- 点击【备份】按钮可以对审计日志进行备份操作，备份的日志文件存放在 `${APUSIC_HOME}/domain_name/store/audit` 目录下。

## 10.3 自动备份设置

使用角色为审计员的用户登录管控，切换到自动备份设置界面，可以设置自动备份策略。


点击“新增”，进入添加自动备份任务页面，输入：

- **任务名**: 定义该任务名称。
- **备份地址**: 选择该备份文件需要存放到的目录，该目录需要有权限。
- **备份类型**: 选择该任务的类型，操作日志或审计日志。
- **备份策略**: 设置自动备份的周期，每小时、每日、每周、每月、每年。



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