Apusic 金蝶天燕

生成时间：2026-05-19

安装手册

金蝶Apusic应用服务器V10 智能安全版

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 概述

1.1 摘要

本快速入门指南主要介绍金蝶Apusic应用服务器V10智能安全版（简称"AAS-V10 智能安全版"）安装、卸载等基本过程，适用于使用金蝶Apusic应用服务器进行开发的开发人员、生产环境的系统管理员、运维人员等。

1.2 基础介绍

金蝶Apusic应用服务器为复杂应用提供了一个简便、快速的开发和运行平台，对于分布式的企业级应用，提供了易扩展、可伸缩和高安全性等特性。智能安全版在企业版的基础上增加智能安全模块，称为金蝶天燕实时安全防护软件(简称ARSP)，为企业应用提供精准全面的安全检测与防御。精确分析用户输入在应用程序里的行为，根据分析结果区分合法行为和攻击行为，实施高效的防御，在以边界防御为主的防火墙无法应对的企业安全中发挥关键的作用。能够有效防御OWASP常见安全问题，保护应用系统运行安全，增强应用系统的数据安全。在需要更加高级的应用安全防御能力要求的情况可使用该版本。

金蝶天燕实时安全防护软件(简称ARSP)是基于运行时应用程序自我保护思想进行开发，精确分析用户输入在应用程序里的行为，根据分析结果区分合法行为和攻击行为，实时高效的防御，在以边界防御为主的防火墙无法应对的企业安全中发挥关键的作用；金蝶天燕实时安全防护软件不依赖于网络流量分析，因此避免了协议解析、字符解码以及基于签名的威胁鉴别等问题。

1.3 术语

1. Apusic 应用服务器

服务器是应用服务器的物理部署单元。直观的来说，是应用服务器在一台用户机器上的一个物理安装。

2. 金蝶天燕实时安全防护软件

为企业应用提供精准全面的安全检测与防御的安全模块。分为两部分：安全探针和管控中心。安全探针：与应用系统运行在一起，为应用系统提供安全检测、监控与防御，并收集安全数据发回管控中心进行分析统计；管控中心：对安全探针收集到的数据进行查询、分析与统计，指导用户进行安全决策。属于金蝶Apusic应用服务器的一个模块。

1.4 默认管理值

名称	默认值
AAS安装目录	{APUSIC_HOME}
域安装目录	{DOMAIN_HOME}

域名	mydomain
asadmin命令行实用程序	{APUSIC_HOME}/bin
配置文件	{DOMAIN_HOME}/config
日志文件	{DOMAIN_HOME}/logs
ARSP安全探针安装目录	{ARSP_HOME}

1.5 默认模块端口

功能模块	端口
管控端口	6848
HTTP 端口	6888
HTTP SSL端口	6887
IIOP SSL端口	6838
IIOP MUTUALAUTH端口	6839
JMS 端口	6876
IIOP端口	6837
JMX 端口	6886
OSGI SHELL 端口	6866
JAVA DEBUGGER端口	8000

2 系统环境要求

2.1 操作系统

1. Linux：
    - 国产操作系统：银河麒麟系列、中标麒麟系列、普华、中科红旗、深度等
    - RedHat系列
    - CentOS
    - Suse Linux系列
2. Windows：
    - Windows 7系列
    - Windows 8系列
    - Windows 10系列
    - Windows 2003系列
    - Windows 2008系列
    - Windows 2012系列
3. Unix：
    - HP Unix系列
    - IBM AIX系列
    - Solaris系列

2.2 JDK版本

1. Oracle JDK 8+
2. Open JDK 8+
3. IBM JDK 8+

3 产品包清单

产品安装包通常打包为`AAS-[version].tar.gz`、`AAS-[version].zip`、`AAS-[version].bin`、`AAS-[version].exe`等格式。`[version]`表示该产品包版本，默认为`V10`。

其中`.tar.gz`、`.zip`为直接安装方式，适用于非图形化安装等场景，兼容各类操作系统，通常情况下使用这两种格式的产品安装包。

`.bin`、`.exe`为图形化安装方式，适用于图形化安装场景，`.bin`为Linux、Unix操作系统使用，`.exe`为Windows操作系统使用。

下表为常用格式版本的产品安装包说明。

产品包	说明
AAS-[version].zip/AAS-[version].tar.gz	金蝶Apusic应用服务器V10安装包

产品包目录说明：

目录名/文件名	说明
ApusicAS	Apusic应用服务器及其他自带工具文件归档目录
aas	Apusic应用服务器安装目录归档名称
bin	应用服务器批处理文件所在的目录
install	第三方插件所在的目录
javadb	Derby数据库目录
mq	MQ工具目录
samples	应用程序示例目录
tools	引用的第三方工具所在的目录

Apusic应用服务器目录说明：

目录名/文件名	说明
bin	应用服务器启动、停止等脚本所在的目录
domains	应用服务器的域所在的目录，默认域为mydomain
config	应用服务器配置文件所在的目录

lib	应用服务器JAR文件等资源所在的目录
modules	应用服务器模块资源包目录
osgi	osgi目录
templates	模板资源目录
jmods	存放JDK各种模块的目录
docs	产品操作等文件存放的目录
license.xml	产品的授权文件

4 安装与卸载

本章节介绍AAS的安装与卸载方式。

4.1 JAVA环境

安装前，需要先确认java环境。JDK版本建议在1.8.0_201及以上，查看JDK版本命令如下：

```
[root@myRabbitA bin]# java -version
java version "1.8.0_212"
Java(TM) SE Runtime Environment (build 1.8.0_212-b10)
Java HotSpot(TM) 64-Bit Server VM (build 25.212-b10, mixed mode)
```

支持指定 AAS V10 中的 JAVA 运行环境，通过设置 `AS_JAVA` 值得方法指定。

Windows: 修改 `$APUSIC_HOME}\config\asenv.bat` ，增加 `AS_JAVA` 变量。

```
set AS_JAVA=H:javajdk1.8.0_201
```

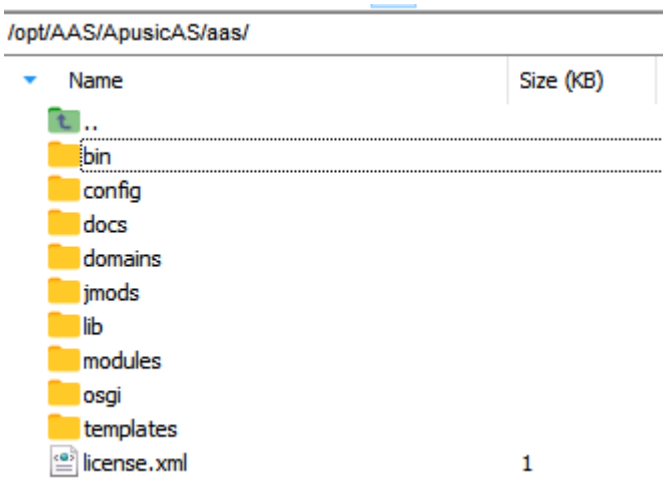
Linux: 修改 `${APUSIC_HOME}/config/asenv.conf` , 增加 `AS_JAVA` 变量。

```
AS_JAVA="/home/java/jdk1.8.0_211"
```

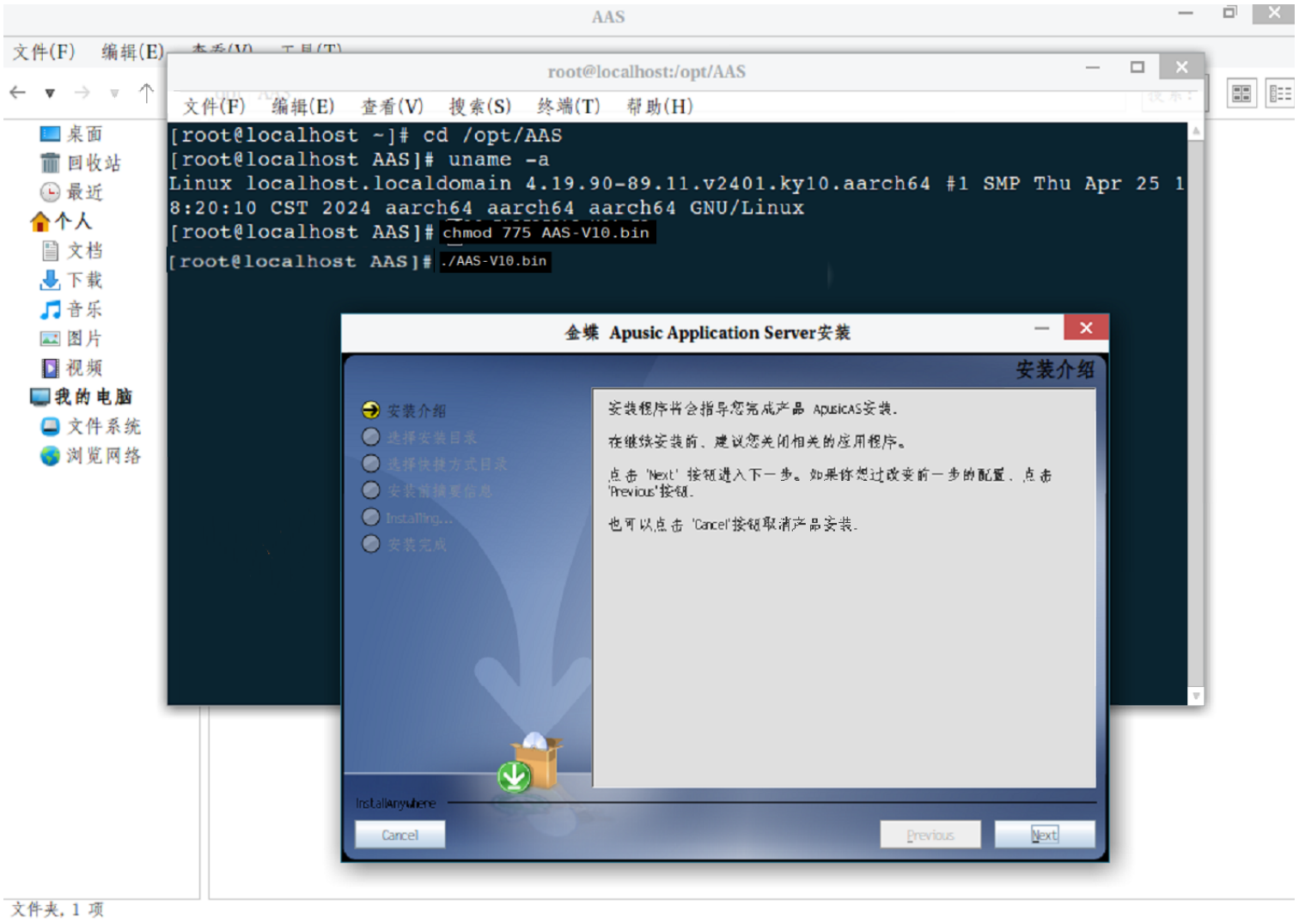
4.2 安装

4.2.1 Linux下安装

如若安装包为 `.zip` 包，放置指定目录，执行命令 `unzip AAS-V10.zip` ，解压安装包完成安装。

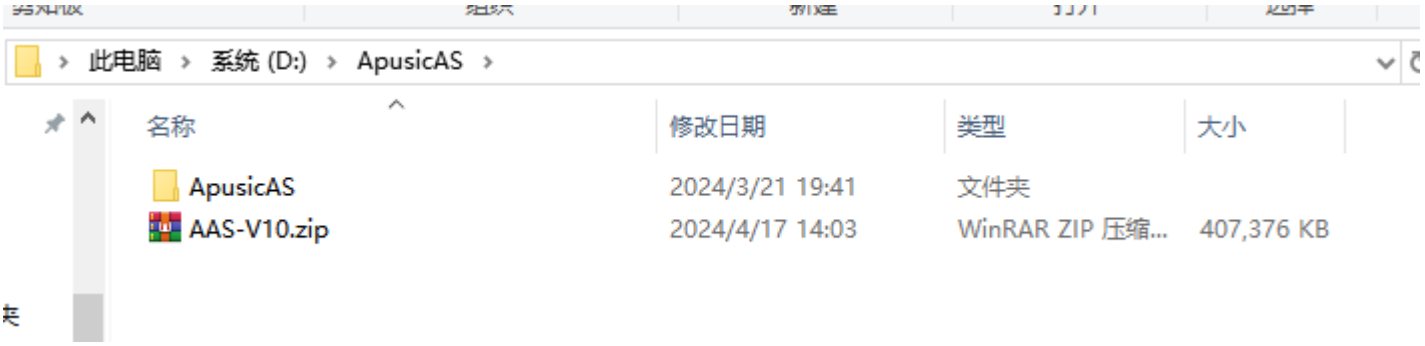


获取图形化安装包，放置指定目录，执行授权命令，`chmod 755 AAS-V10.bin`；再执行`AAS-V10.bin`，按照安装指引完成安装。

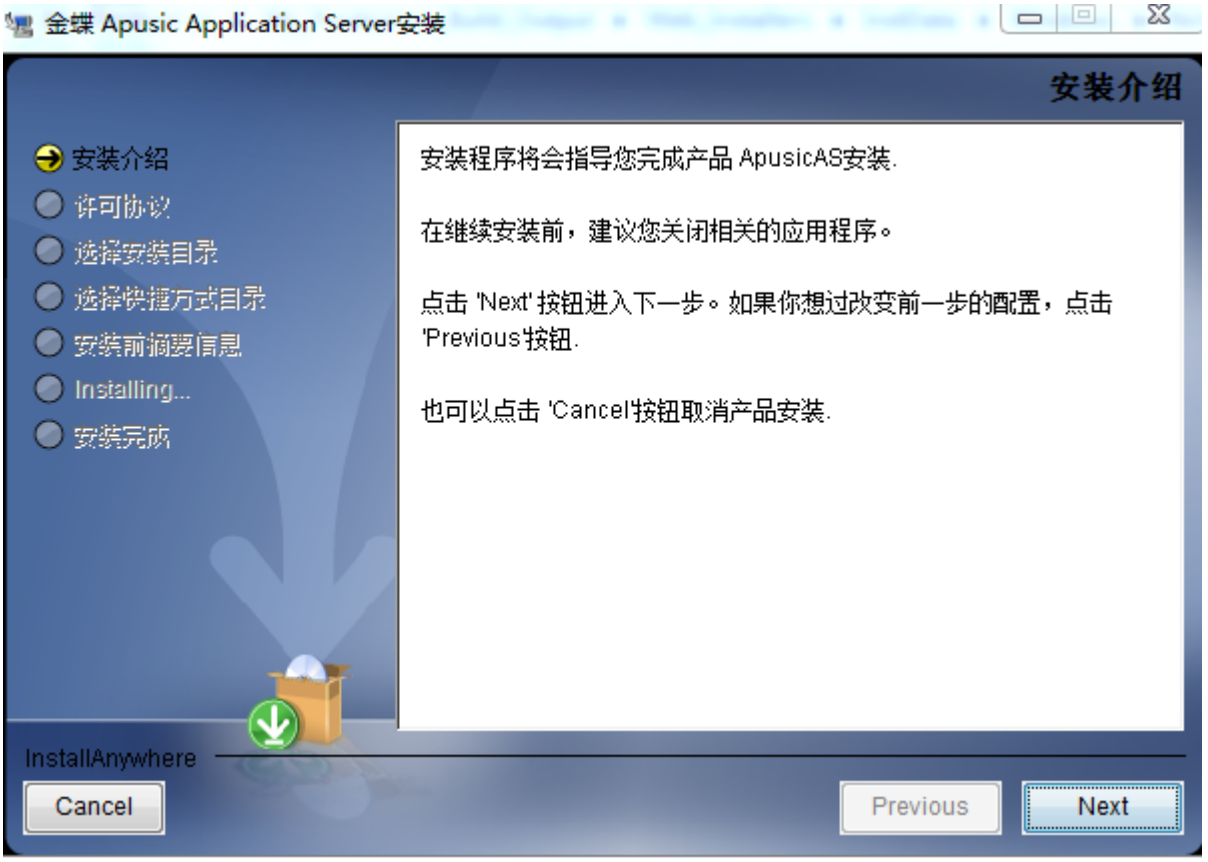


4.2.2 Windows下安装

如若安装包为 `.zip` 包，放置指定目录，直接解压安装包 `AAS-V10.zip` 完成安装。



如若安装包为 `.exe` ，双击执行 `AAS-V10.exe` ，按照安装指引安装程序。



4.3 卸载

4.3.1 Linux下卸载

如若安装方式为直接解压的zip包，可进入安装目录，直接删除安装目录即可卸载。

如若安装方式为图形化安装，可点击双击"卸载AAS"。

注：卸载之前需要停止运行AAS

4.3.2 Windows下卸载

如若安装方式为直接解压的zip包，可进入安装目录，直接删除安装目录即可卸载。

如若安装方式为图形化安装，可点击开始->程序->金蝶Apusic应用服务器->卸载Apusic应用服务器。

5 许可证授权

AAS需要有对应的许可证才能正常使用，通常情况下，金蝶天燕会根据用户购买的产品版本配套对应的许可证。

产品授权方式分为普通授权和集中授权。

5.1 普通授权

普通授权指根据IP、域名等方式生成 `license.xml` 文件，将授权文件放置安装目录下，`${APUSIC_HOME}/license.xml` 。

5.2 集中授权

集中授权指连接授权中心，进行统一授权。需要先搭建金蝶Apusic授权中心，操作方式可参考《金蝶Apusic许可授权中心用户手册》，或联系金蝶天燕技术支持人员。

在系统环境中配置环境变量，或在AAS安装目录 `${APUSIC_HOME}` 下创建 `acls.properties` 文件，添加以下参数：

```
apusic_acls_enable=true
apusic_acls_authUrls=172.24.4.166:6886
apusic_acls_ns=apusic
apusic_acls_tenant=ApusicTest
```

连接参数说明：

参数名	参数值说明

apusic_acls_enable	是否开启授权中心认证，取值为true或false，为true则表示开启授权中心认证。没有该参数或该参数值为false，都表示没有开启授权中心认证；
apusic_acls_authUrls	授权中心的地址，可设置多个授权地址，格式为ip1:port1,ip2:port2，如果一个授权地址链接失败，会轮询其他的地址；如果开启授权中心认证，则为必填参数，其中端口为授权中心的https端口；
apusic_acls_ns	设置该实例所属的命名空间名称，可选参数；默认值为public，具体的命名空间可以在授权中心管理控制台-系统管理-授权管理查看。
apusic_acls_tenant	设置该实例所属的租户名称，可选参数。

AAS启动时将会自动连接到Apusic授权中心。

5.3 获取特征码

如果在使用过程中出现许可证过期或无效等问题，建议优先联系对接的天燕服务人员，重新申请对应许可证。重新申请对应许可证时，需要将产品的特征码(auth code)提供到天燕对接人员。

在`${Apusic_HOME}/bin`，执行`startserv -ac [ethname or ip]`，`[ethname or ip]`取值为ip地址或者网卡名称，类似如下:

```
startserv -ac 172.20.140.17
```

打印特征码信息，类似如下，Auth Code=特征码内容:

```
Auth Code=SZTY942563117
Command auth-code executed successfully.
```

获取特征码后再提供特征码申请授权文件。

如果是节点出现授权问题，可查看日志，日志会打印出对应的特征码(auth code)，拷贝特征码(auth code)提供至天燕对接人员重新申请对应许可证。

6 启动与停止

6.1 启动

6.1.1 Linux下启动

进入安装目录`${APUSIC_HOME}/aas/bin`，执行`asadmin start-domain`。首次启动需要设置默认管理员用户密码。

```
[apusic@test2 bin]# ./asadmin start-domain

This domain requires an administrative password to be set before
the domain can be started. Please specify an administrative password.
Enter an administrative password for user "audit">
Enter an administrative password for user "audit" again>
Password for User audit has change Successfully!

Enter an administrative password for user "admin">
Enter an administrative password for user "admin" again>
Password for User admin has change Successfully!

Enter an administrative password for user "secure">
Enter an administrative password for user "secure" again>
Password for User secure has change Successfully!
Waiting for mydomain to start ....
Successfully started the domain : mydomain
domain  Location: /opt/testz/1213/ApusicAS/aas/domains/mydomain
Log File:
/opt/testz/1213/ApusicAS/aas/domains/mydomain/logs/server.log
Admin Port: 6848
Command start-domain executed successfully.
```

6.1.2 Windows下启动

进入安装目录`${APUSIC_HOME}\aas\bin`，执行`asadmin start-domain`。首次启动需要设置默认管理员用户密码。

```
E:\testz\1213\AAS-V10\ApusicAS\aas\bin>asadmin start-domain

This domain requires an administrative password to be set before
the domain can be started. Please specify an administrative password.
Enter an administrative password for user "audit">
Enter an administrative password for user "audit" again>
Password for User audit has change Successfully!

Enter an administrative password for user "admin">
Enter an administrative password for user "admin" again>
Password for User admin has change Successfully!

Enter an administrative password for user "secure">
Enter an administrative password for user "secure" again>
Password for User secure has change Successfully!
Waiting for mydomain to start .............
Successfully started the domain : mydomain
domain  Location: E:\testz\1213\AAS-V10\ApusicAS\aas\domains\mydomain
Log File: E:\testz\1213\AAS-
V10\ApusicAS\aas\domains\mydomain\logs\server.log
Admin Port: 6848
Command start-domain executed successfully.
```

6.2 停止

6.2.1 Linux下停止

进入安装目录`${APUSIC_HOME}/aas/bin`，执行`asadmin stop-domain`。

```
[apusic@test2 bin]# ./asadmin stop-domain
Waiting for the domain to stop .
Command stop-domain executed successfully.
```

6.2.2 Windows下停止

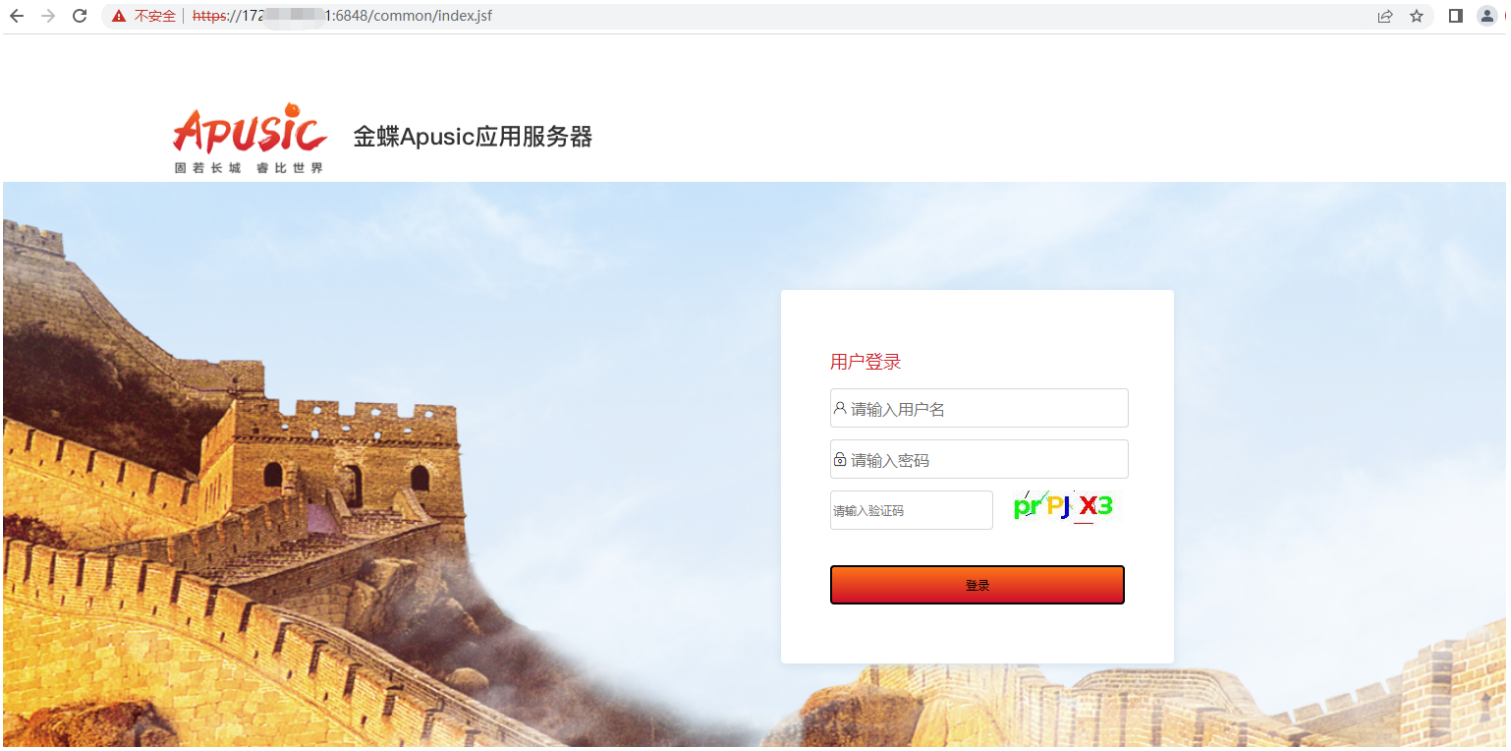
进入安装目录`${APUSIC_HOME}\aas\bin`，执行`asadmin stop-domain`。

```
E:\testz\1213\AAS-V10\ApusicAS\aas\bin>asadmin stop-domain
Waiting for the domain to stop .
Command stop-domain executed successfully.
```

7 基础使用介绍

7.1 应用服务器管控平台访问

安装并启动后，浏览器访问：https://ip:port:6848。



7.2 ARSP管控中心访问

启动应用服务器后，访问http://IP:6888/arsp 或https://IP:6887/arsp。

注意：登录ARSP管控中心不能在同一浏览器访问应用服务器管控平台。

7.3 基础角色

AAS V10管控功能将集群管理控制台、安全管理控制台、通用管理控制台合并。 支持三员分立功能，默认三种角色以及用户：

- 系统管理员(sysadmin): admin。主要负责用户创建及管理、日常系统维护设置，资源以及集群管理等工作。
- 安全保密员（security）: secure。主要负责系统的日常安全保密管理工作。
- 审计员（auditor）: audit。主要负责对系统管理员、安全管理员的操作行为进行审计跟踪分析和监督检查。

默认管理员密码为应用服务器初始化时设置的密码。

ARSP管控中心支持三员分立功能。

- 系统管理员: 默认用户admin，初始化密码为`apusic123456!@#$%^`。负责探针管理、实践管理、用户创建等工作。
- 操作员：主要负责事件管理、探针管理、告警管理、报表管理工作。用户需要系统管理员创建。
- 安全审计员：主要负责日志管理模块。用户需要系统管理员创建。
- 安全保密员：主要负责系统设置模块。用户需要系统管理员创建。

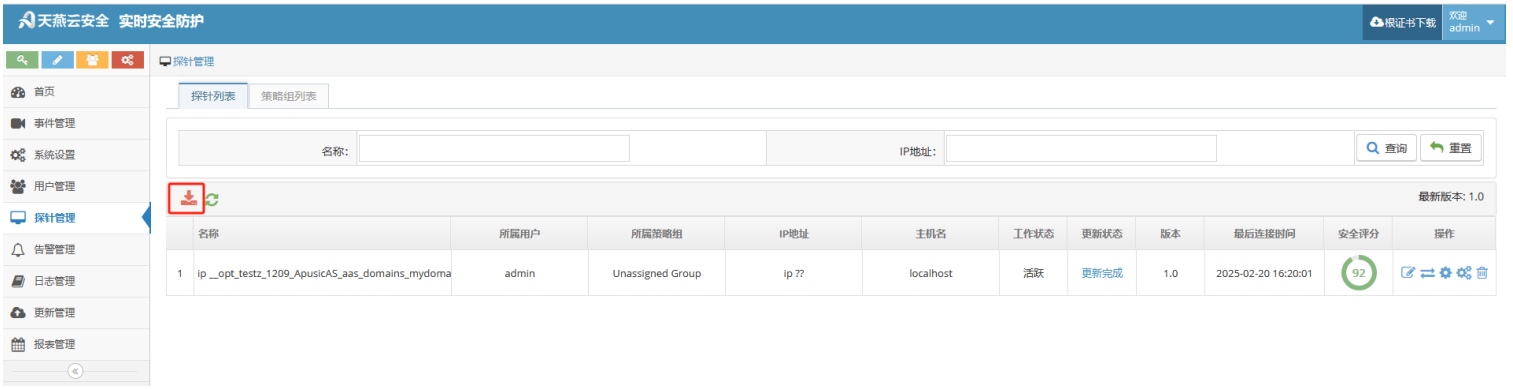
用户首次登录ARSP管控中心需要重置密码。

8 探针管理

8.1 探针下载

安全探针需与应用系统运行在一起，为应用系统提供安全检测、监控与防御，并收集安全数据发回管控中心进行分析统计。

进入ARSP管控中心，在“探针管理”页面，点击下载图标按钮下载安全探针。



8.2 探针安装

将探针文件拷贝至需要监控的服务器上，解压。

注意：安全探针不能安装在部署ARSP管控中心的应用服务器中。

```
[root@AAS-168 1209]# ls
ApusicAS  ARSPV1.0  ARSPV1.0.tar
```

```
[root@AAS-168 1209]# cd ARSPV1.0
[root@AAS-168 ARSPV1.0]# ls
bin  bin-1.0  config  internal  lib  lib-1.0  log  version
[root@AAS-168 ARSPV1.0]#
```

8.3 探针配置与启动

通用的启动方式是在应用系统的启动脚本中加上：`-javaagent:${ARSP_HOME}/lib/secg-agent.jar`，然后再启动应用系统，下面以安全探针运行在各应用服务器为例：

注：`${ARSP_HOME}`为探针的安装路径，需要根据实际路径替换该变量。

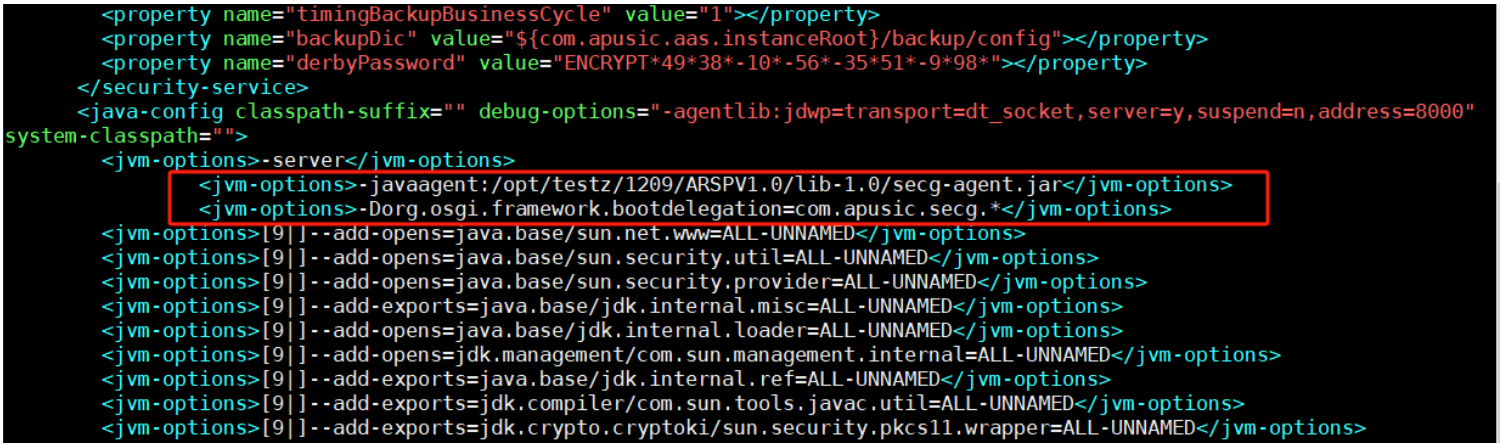
8.3.1 Linux下配置与启动

8.3.1.1 Apusic应用服务器V10企业版

进入`${DOMAIN_HOME}/config`目录下，在`domain.xml`文件的`server-config`中新增

```
<jvm-options>-javaagent:${ARSP_HOME}/lib-1.0/secg-agent.jar</jvm-options>
<jvm-options>-Dorg.osgi.framework.bootdelegation=com.apusic.secg.*</jvm-options>
```

如图：



探针启动：进入`${APUSIC_HOME}/bin`,执行`./startserv`启动Apusic应用服务器过程中会同时启动探针。

启动成功后可以在ARSP的管控中心的探针管理界面看到该探针的信息，并且状态为"活跃"。

8.3.1.2 Apusic应用服务器V10敏捷版

进入`${APUSIC_HOME}/bin`目录，在`apusic.sh`文件中添加

```
-javaagent:${ARSP_HOME}/lib/secg-agent.jar
```

如图：

```
# Bugzilla 37848: When no TTY is available, don't output to console
have_tty=0
if [ -t 0 ]; then
    have_tty=1
fi

# For Cygwin, switch paths to Windows format before running java
if $cygwin; then
  JAVA_HOME=`cygpath --absolute --windows "$JAVA_HOME"`
  JRE_HOME=`cygpath --absolute --windows "$JRE_HOME"`
  APUSIC_HOME=`cygpath --absolute --windows "$APUSIC_HOME"`
  APUSIC_BASE=`cygpath --absolute --windows "$APUSIC_BASE"`
  APUSIC_TMPDIR=`cygpath --absolute --windows "$APUSIC_TMPDIR"`
  CLASSPATH=`cygpath --path --windows "$CLASSPATH"`
  [ -n "$JAVA_ENDORSED_DIRS" ] && JAVA_ENDORSED_DIRS=`cygpath --path --windows "$JAVA_ENDORSED_DIRS"`
fi

if [ -z "$JSSE_OPTS" ] ; then
  JSSE_OPTS="-Djdk.tls.ephemeralDHKeySize=2048"
fi
JAVA_OPTS="-javaagent:/opt/testz/ARSPV1.0/lib/secg-agent.jar $JAVA_OPTS $JSSE_OPTS"

# Register custom URL handlers
# Do this here so custom URL handles (specifically 'war:...') can be used in the security policy
JAVA_OPTS="$JAVA_OPTS -Djava.protocol.handler.pkgs=com.apusic.ams.webresources"

# Set by etcd etc.
MEMORY_JVMOPTS=""
if [ -n "$MEMORY_JVMOPTS" ] ; then
  JAVA_OPTS="$JAVA_OPTS $MEMORY_JVMOPTS"
fi
```

探针启动：进入 `${APUSIC_HOME}/bin`,执行 `./apusic.sh run` 启动Apusic应用服务器过程中会同时启动探针。

启动成功后可以在管控中心的探针管理界面看到该探针的信息，并且状态为“活跃”。

8.3.1.3 Apusic应用服务器V9.0版本

进入 `${DOMAIN_HOME}/bin`,修改 `startapusic` 文件，在 `JVM_OPTS` 处加入

```
-javaagent:${ARSP_HOME}/lib-1.0/secg-agent.jar
```

如图：

```
OTHERS_JVMOPTS="-server -Djava.net.preferIPv4Stack=true -Djava.security.egd=file:/dev/./urandom"
MEMORY_JVMOPTS="-Xms512m -Xmx1024m -XX:MaxPermSize=256m"
GC_JVMOPTS=""
JVM_OPTS="-javaagent:/lgrtest/arsp_110/ARSPv1.0/lib/secg-agent.jar $OTHERS_JVMOPTS $MEMORY_JVMOPTS $GC_JVMOPTS"

#Change the value of "user.dir" property
cd $DOMAIN_HOME

APUSIC_ENDORSED_DIRS="$APUSIC_HOME/lib/endorsed"
ENDORSED_1_6_DIR="$APUSIC_HOME/lib/endorsed_jdk1.6"
eval $($JAVA_RUN -version 2>&1 | awk '/java version/ {print $3}'|sed 's/"//g'|awk '{if (substr($1,1,4)=="1.6.") print "IS_JDK_1_6='true'"}')
if [ $IS_JDK_1_6 ] ; then
    APUSIC_ENDORSED_DIRS=$APUSIC_ENDORSED_DIRS:$ENDORSED_1_6_DIR
fi

echo "Using APUSIC_HOME:     $APUSIC_HOME"
echo "Using DOMAIN_HOME:     $DOMAIN_HOME"
echo "Using JAVA_HOME:       $JAVA_HOME"

STATUS_MODE="OFF"
SUSPEND="n"
```

探针启动：进入 `${DOMAIN_HOME}/bin` ，执行 `./startapusic` ,启动Apusic应用服务器的过程中，会启动ARSP安全探针，安全探针的启动日志在 `${ARSP_HOME}/log/secg.log` 文件里面。

启动成功后可以在管控中心的探针管理界面看到该探针的信息，并且状态为“活跃”。

8.3.2 Windows下配置与启动

8.3.2.1 Apusic应用服务器V10企业版

进入 `${DOMAIN_HOME}\config` 目录下，在 `domain.xml` 文件的 `server-config` 中新增

```
<jvm-options>-javaagent:${ARSP_HOME}\lib-1.0\secg-agent.jar</jvm-options>
<jvm-options>-Dorg.osgi.framework.bootdelegation=com.apusic.secg.*</jvm-options>
```

探针启动：进入 `${APUSIC_HOME}\bin` ,执行 `startserv.bat` 启动Apusic应用服务器过程中会同时启动探针。

启动成功后可以在ARSP的管控中心的探针管理界面看到该探针的信息，并且状态为“活跃”。

8.3.2.2 Apusic应用服务器V10敏捷版

进入 `${APUSIC_HOME}\bin` 目录，在 `apusic.bat` 文件中添加

```
-javaagent:${ARSP_HOME}\lib\secg-agent.jar
```

探针启动：进入 `${APUSIC_HOME}\bin` ,执行 `apusic.bat run` 启动Apusic应用服务器过程中会同时启动探针。

启动成功后可以在管控中心的探针管理界面看到该探针的信息，并且状态为“活跃”。

8.3.2.3 Apusic应用服务器V9.0版本

进入 `${DOMAIN_HOME}\bin` ,修改 `startapusic.cmd` 文件，在 `JVM_OPTS` 处加入

```
-javaagent:${ARSP_HOME}\lib-1.0\secg-agent.jar
```

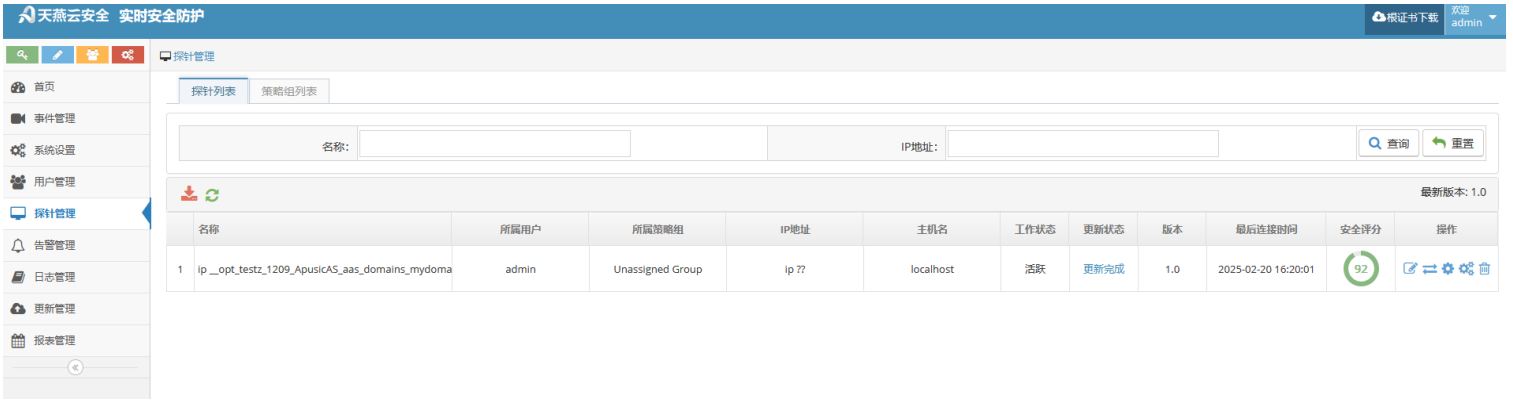
探针启动：进入 `${DOMAIN_HOME}\bin` ，执行 `startapusic.bat` ,启动Apusic应用服务器的过程中，会启动ARSP安全探针，安全探针的启动日志在 `${ARSP_HOME}\log\secg.log` 文件里面。

启动成功后可以在管控中心的探针管理界面看到该探针的信息，并且状态为“活跃”。

8.4 探针参数与规则管理

进入ARSP管控中心，点击“探针管理”，可对探针及策略进行管理。

“探针管理”页面默认显示已检测到安装有探针的服务器信息。可修改探针名称、策略组等信息。

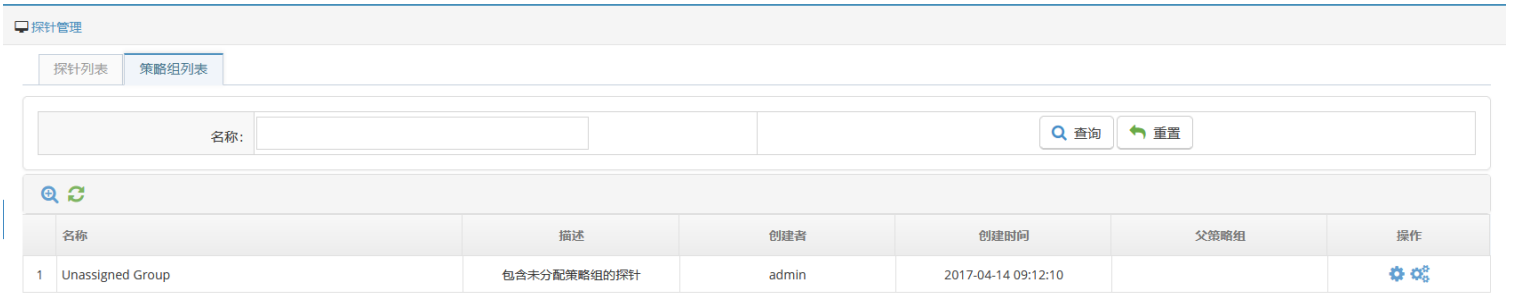


8.5 策略组列表

系统自带一个“Unassigned Group”策略组，刚注册还没有分配的探针就归属于这个组，后续可以根据实际情况给探针重新分配策略组；

探针所在策略组如果被删除了的话，也会将探针归属于“Unassigned Group”策略组。

可以新增、修改或删除策略组信息。



8.5.1 修改策略组规则

界面上选中某个策略组，点击配置按钮可以对策略组的规则，规则参数和特例进行设置。

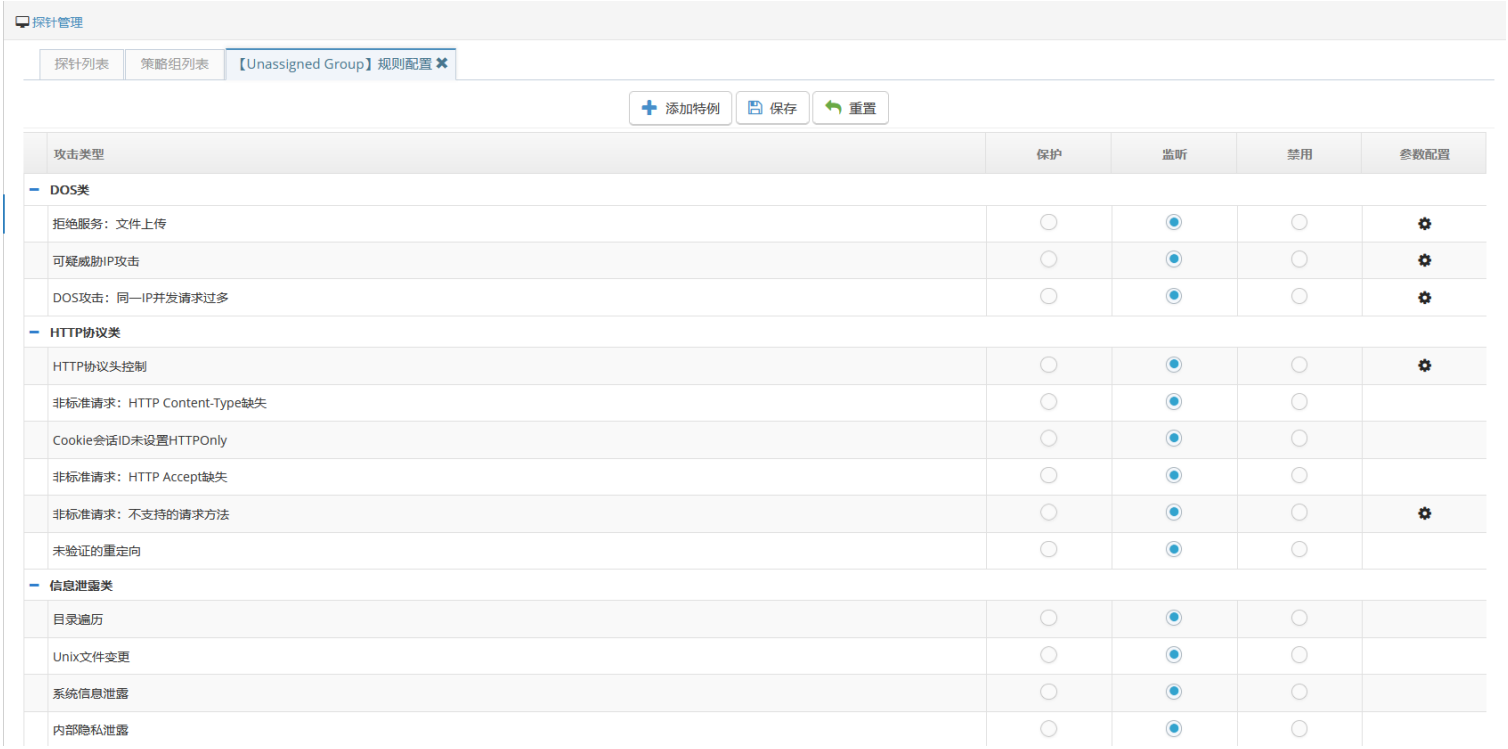
1).配置攻击类型的规则

可以设置每个攻击类型的规则为保护或者监听或者禁用模式，设置完成后点击“保存”按钮进行保存。

注：保护模式：探针检测到应用系统有该类型的攻击时，进行阻止攻击，并且记录该攻击数据返回到管控中心。

监听模式：探针检测到应用系统有该类型的攻击时，不阻止攻击，只记录该攻击数据返回到管控中心。

禁用模式：探针检测到应用系统有该类型的攻击时，不阻止攻击，也不记录。

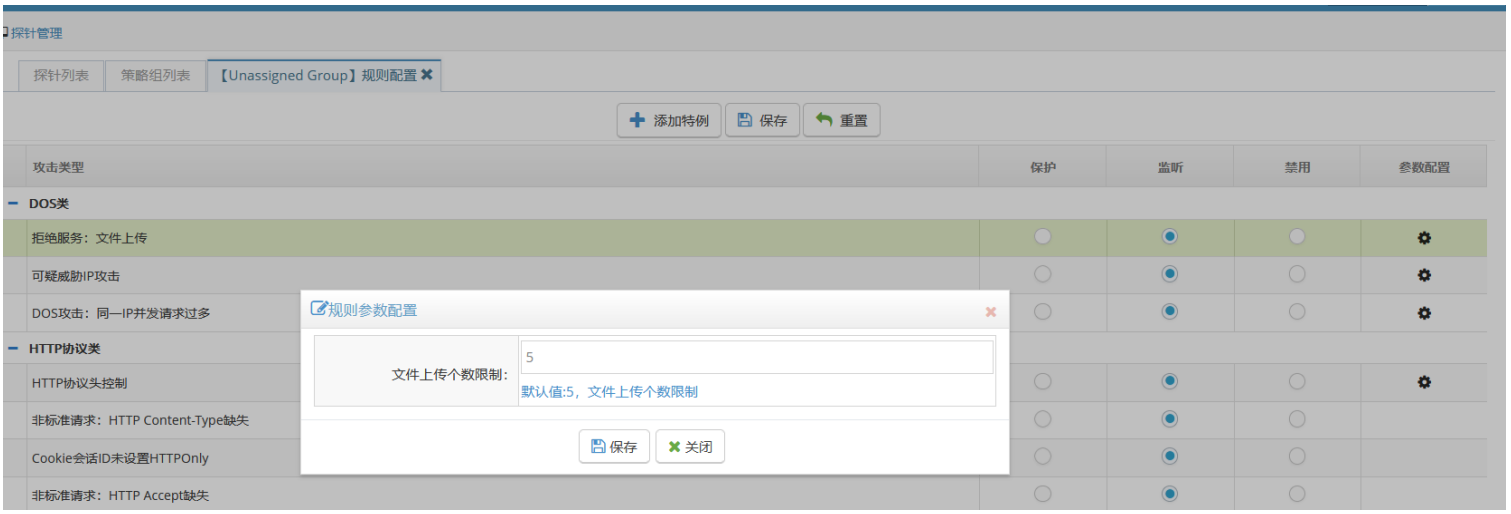


2）规则参数设置

在探针规则配置界面，对应的攻击类型处点击配置参数按钮。

出现参数配置界面，以“拒绝服务：文件上传”为例：

填写文件上传个数限制，点击保存，当同时上传超过5份文件时探针监测到的非法攻击事件。

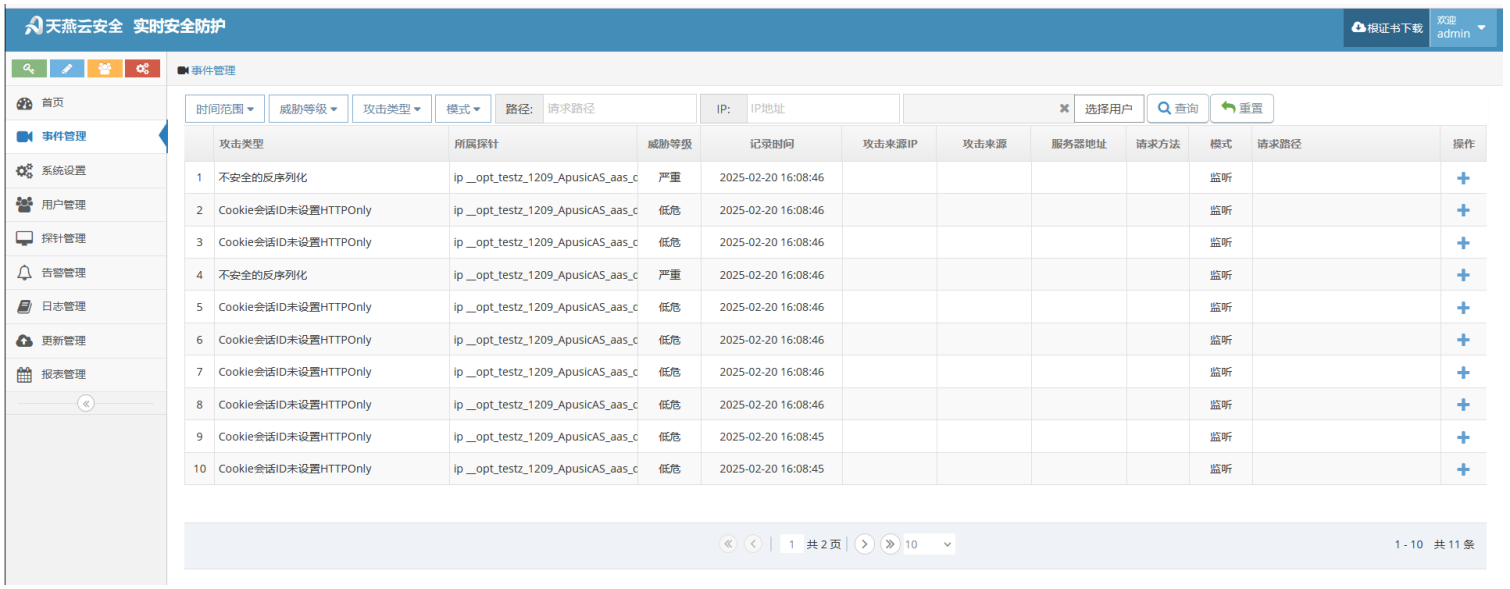

探针管理
探针列表
策略组列表
【Unassigned Group】规则配置
添加特例
保存
重置
攻击类型
保护
监听
禁用
参数配置
DOS类
拒绝服务：文件上传
可疑威胁IP攻击
DOS攻击：同一IP并发请求过多
HTTP协议类
HTTP协议头控制
非标准请求：HTTP Content-Type缺失
Cookie会话ID未设置HTTPOnly
非标准请求：HTTP Accept缺失
规则参数配置
文件上传个数限制：
5
默认值:5，文件上传个数限制
保存
关闭

9 事件管理

事件管理界面记录系统所有用户的探针监测到的非法攻击事件。

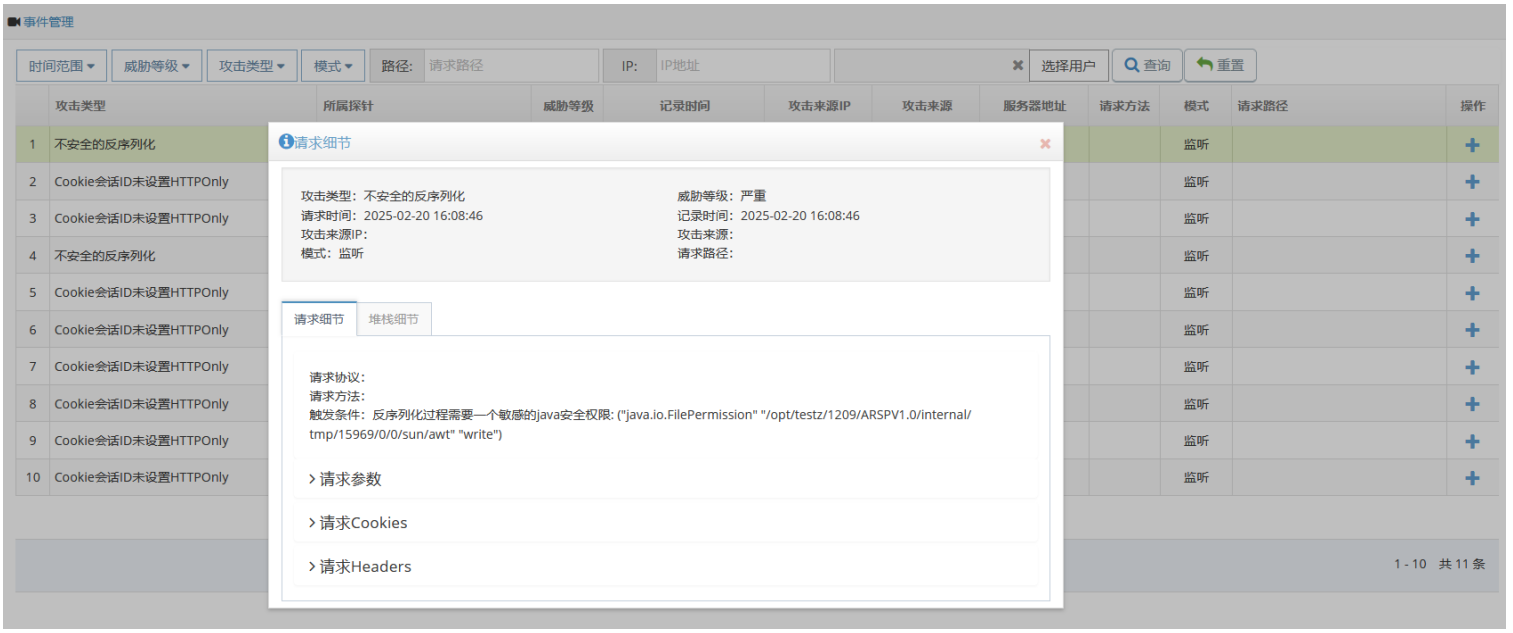
9.1 攻击查询

可以通过如下条件过滤查询：时间范围、威胁等级、攻击类型、模式、路径、IP和用户。



9.2 事件详情

双击某个事件，打开该攻击事件的请求细节页面。



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