**AAS安全扫描常见解决方法**

# AAS-V10配置设置

## 处理header安全问题

### APUSICAS安装目录lib修改

修改 Apusic\aas\lib\install\applications\\_\_admingui\WEB-INF\web.xml

将 <session-config>

 <cookie-config>

 <http-only>true</http-only>

 <secure>false</secure>

 </cookie-config>

</session-config>

改为“true”



取消 <filter>

 <filter-name>XSSFilter</filter-name>

 <filter-class>com.sun.webui.jsf.util.XSSFilter</filter-class>

 </filter>

 <filter>

 <filter-name>CSRFFilter</filter-name>

 <filter-class>com.sun.webui.jsf.util.CSRFFilter</filter-class>

 <init-param>

 <param-name>enabled</param-name>

 <param-value>true</param-value>

 </init-param>

 </filter>

<filter-mapping>

 <filter-name>XSSFilter</filter-name>

 <url-pattern>/\*</url-pattern>

 </filter-mapping>

 <filter-mapping>

 <filter-name>CSRFFilter</filter-name>

 <url-pattern>/\*</url-pattern>

 </filter-mapping>

这两部分的注释



### 管控台页面修改协议

可选择在管控台页面设置，效果与domain.xml添加配置一致

在【sever-config】-【网络配置】-【协议】-【sec-admin-listener】添加以下http请求头







选择合适的ssl密码套件（除了以下过时的）







只选择TLS1.2



### Domain.xml修改协议

可选择直接在domain.xml添加配置，效果与管控台页面修改一致

<protocol name="sec-admin-listener" security-enabled="true">

 <http encoded-slash-enabled="true" default-virtual-server="\_\_asadmin">

 <property name="X-Content-Type-Options" value="nosniff"></property>

 <property name="X-XSS-Protection" value="1;mode=block"></property>

 <property name="Cache-Control" value="no-cache"></property>

 <property name="Cache-Control" value="no-store"></property>

 <property name="Pragma" value="no-cache"></property>

 <property name="Strict-Transport-Security" value="max-age=31"></property>

 <file-cache></file-cache>

 </http>

 <ssl tls-enabled="false" classname="com.sun.enterprise.security.ssl.ApusicSSLImpl" client-auth="want" tls11-enabled="false" cert-nickname="kaas" ssl3-tls-ciphers="+TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256,+TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256,+TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,+TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,+TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256,+TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA,+TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256,+TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA,+TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384,+TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256,+TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,+TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384,+TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA,+TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,+TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256,+TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA,+TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384,+TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384,+TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,+TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256,+TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,+TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384,+TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA,+TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA,+TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,+TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256,+TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA,+TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA,+TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384,+TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,+TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,+TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256"></ssl>

 </protocol>

如下图所示：



## 处理扫描时线程数问题

V10进行安全扫描时，由于网络延时、机器性能等，扫描时发送的大量线程数会无法及时处理，进而造成管控台无法通讯。需要进入管控台，设置【server-config】-【线程池】-【admin-thread-pool】，修改“最大队列数”为4096

设置【default-config】-【线程池】-【admin-thread-pool】，修改“最大线程池”为1024

## Appscan设置

AAS管控台使用https，且包含动态验证码，因而设置【登录管理】-【会话标识】时，取消勾选“JSESSIONID”。

设置【通讯和代理】-【线程数】，设置为5；【超时】设置为60；勾选【不使用代理】

# AAS-V9配置设置

## 开启HTTPS

开启SSL，进入apusic.conf，设置<ATTRIBUTE NAME="SSLEnabled" VALUE="False"/>的value为True。使用HTTPS访问

## 设置验证码任意输入

在webtool.war中修改web.xml的Captcha这个filter，把参数checkDisabled修改为true，设置验证码为任意输入

## 文件vm.options配置

在vm.options添加参数

apusic.admin.multiLogin.enabled=true，允许单用户多次登录

com.apusic.webtool.allowHosts=172.20.140.14，允许访问管控台的IP。

添加一下参数解决header安全问题

apusic.http.header.X-Frame-Options.Enable=true
com.apusic.cookie.noSecurity=false
apusic.http.header.customSize=7
apusic.http.header.name.1=X-Content-Type-Options
apusic.http.header.value.1=nosniff
apusic.http.header.name.2=X-XSS-Protection
apusic.http.header.value.2=1;mode=block
apusic.http.header.name.4=Cache-Control
apusic.http.header.value.4=no-cache
apusic.http.header.name.5=Cache-Control
apusic.http.header.value.5=no-store
apusic.http.header.name.6=Pragma
apusic.http.header.value.6=no-cache
apusic.http.header.name.7=Strict-Transport-Security
apusic.http.header.value.7=max-age=31

## Appscan配置

1. 扫描配置中，“URL和服务器”，勾选“仅扫描此目录中或目录下的链接”。“登录环境”，选择“记录”，使用chromium浏览器，登录后，查看“详细信息”中登录回放方式是否成功，没成功点击“验证”。
2. “通信和代理”，“代理”中勾选“不使用代理”