

**【一站式等保服务平台 V1.0】**  
用户平台操作手册

## 目录

一、产品介绍.....	3
1. 产品简介.....	3
2. 产品架构.....	3
3. 产品用途.....	4
二、操作指南.....	5
1. Web 应用防火墙.....	5
1.1. 域名配置.....	5
1.2. 域名设置.....	6
1.3. 刷新预热.....	11
1.4. 证书管理.....	12
1.5. 负载均衡.....	13
2. 主机防护.....	13
2.1. Agent 安装.....	14
2.2. 主机体检.....	15
2.3. 漏洞风险.....	16
2.4. 入侵威胁.....	22
2.5. 合规基线.....	27
3. 漏洞扫描.....	28
3.1. 扫描目标.....	28
3.2. 扫描任务.....	29
3.3. 扫描报告.....	29
4. 堡垒机.....	30
4.1. 资产管理.....	30
4.2. 授权凭证.....	31
4.3. 会话管理.....	32
4.4. 运维审计.....	33
5. 安全审计.....	33
5.1. 数据库管理.....	34
5.2. 主机管理.....	35
5.3. 应用管理.....	36
5.4. 审计日志.....	37
5.5. 订阅报告.....	37
5.6. Agent 管理.....	38
6. 数据备份.....	38
7. 平台管理.....	38
7.1. 子账号管理.....	38
7.2. 操作日志.....	39
7.3. 安全策略.....	40

# 一. 产品介绍

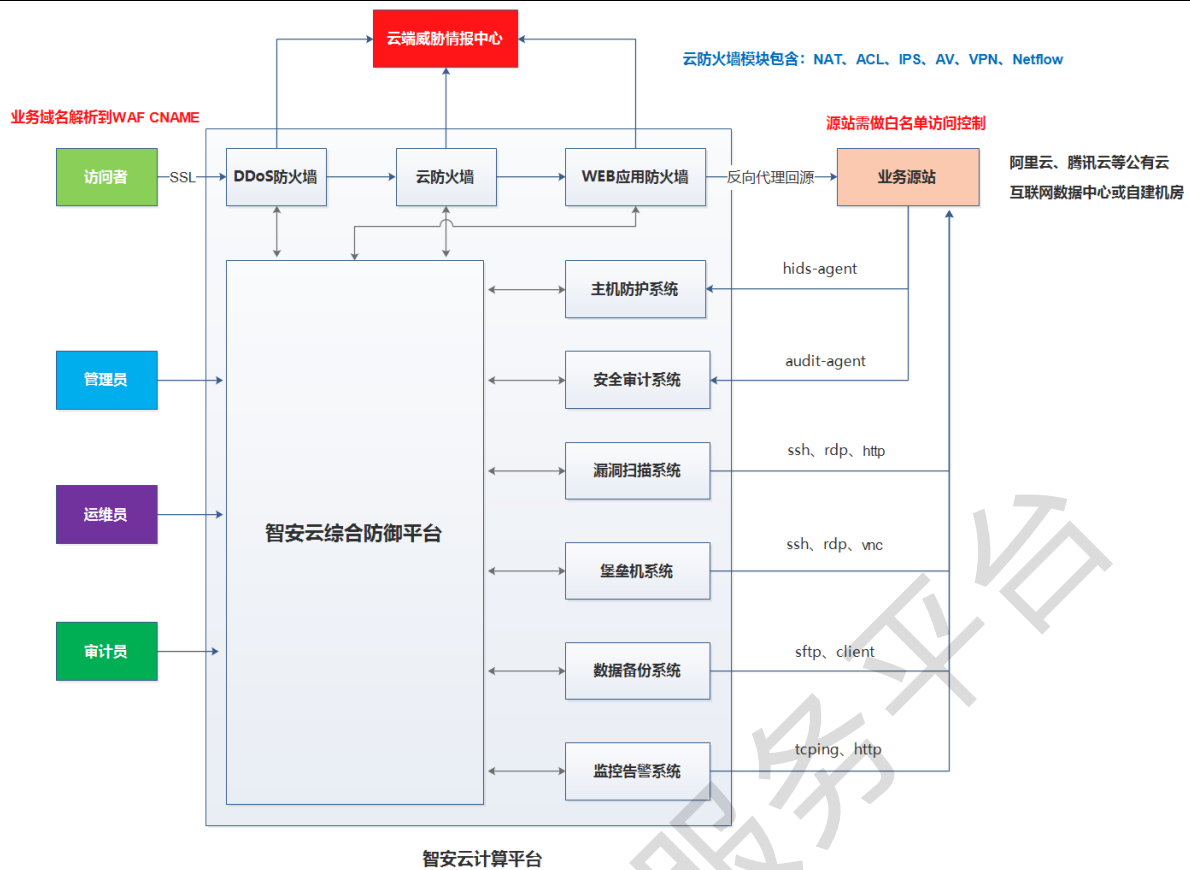
## 1. 产品简介

一站式等保服务平台（后文简称“等保云”）为用户提供一站式的等保服务，平台采用分布式部署的云虚拟安全资源池和至少为 1 台的下一代防火墙（带 DDOS 能力），基于“一个中心三重防护”的合规理念进行设计，为云上业务提供云安全服务。通过控制转发、管理审计、虚拟机等相关设计思路，由下一代防火墙实现通信网络和安全区域边界的防护，由安全虚拟资源池实现运维审计、日志审计、漏洞扫描等功能，最后将系统管理、审计管理、安全管理集中整合到一块，同时结合云化平台里面的云主机管理、容器管理，形成了一个以企业业务上云并完成等保安全建设的一个多态化的安全管理中心，为企业省时省力，满足等保 2.0 合规的主要能力要求。

## 2. 产品架构

将云计算积累的 SDN 能力赋予本平台，将安全产品虚拟化，从而将安全能力软件定义话、资源池化，从而形成等保云平台。

整体架构如下图所示：



### 3. 产品用途

等保云助力企业用户快速实现等保合规落地，建设标准完全符合等保2.0 相关规范。等保云核心解决中小企业源站在云端的等保建设和整改服务。云上安全建设的几大要素均可在等保云上实现。企业用户的云端源数据通过特定的加密传输方式经过等保云实现加密，审计，记录等功能以满足等保测评的所有要素。

等保测评需要第三方机构进行测评，而等保云属于建设方，能够帮住企业用户搭建等保环境，然后邀请测评机构进行测评。

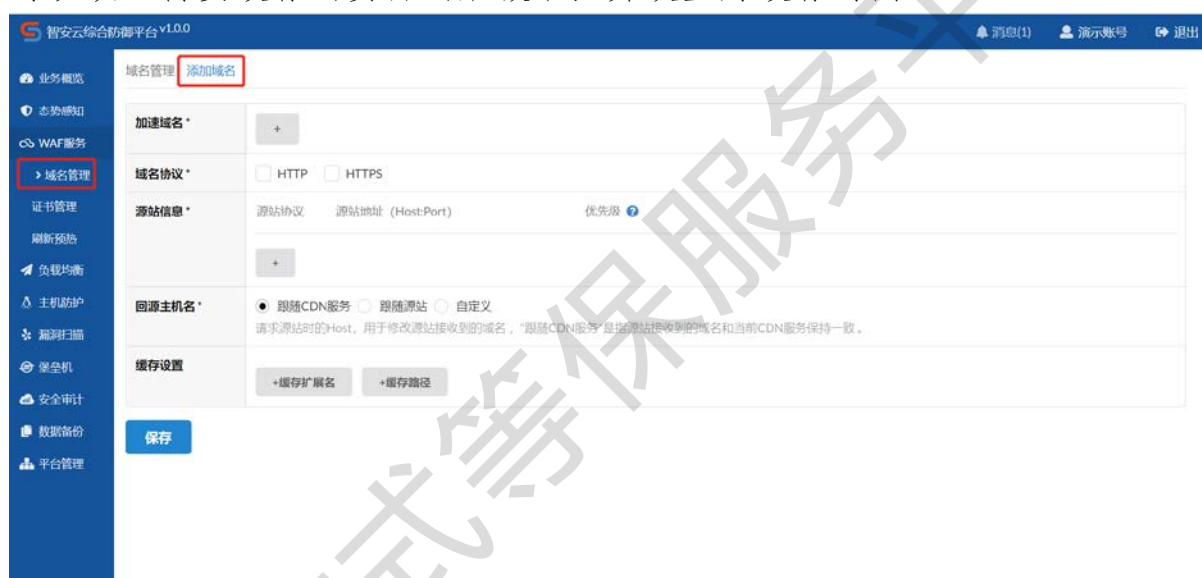
## 二. 操作指南

### 1. Web 应用防火墙

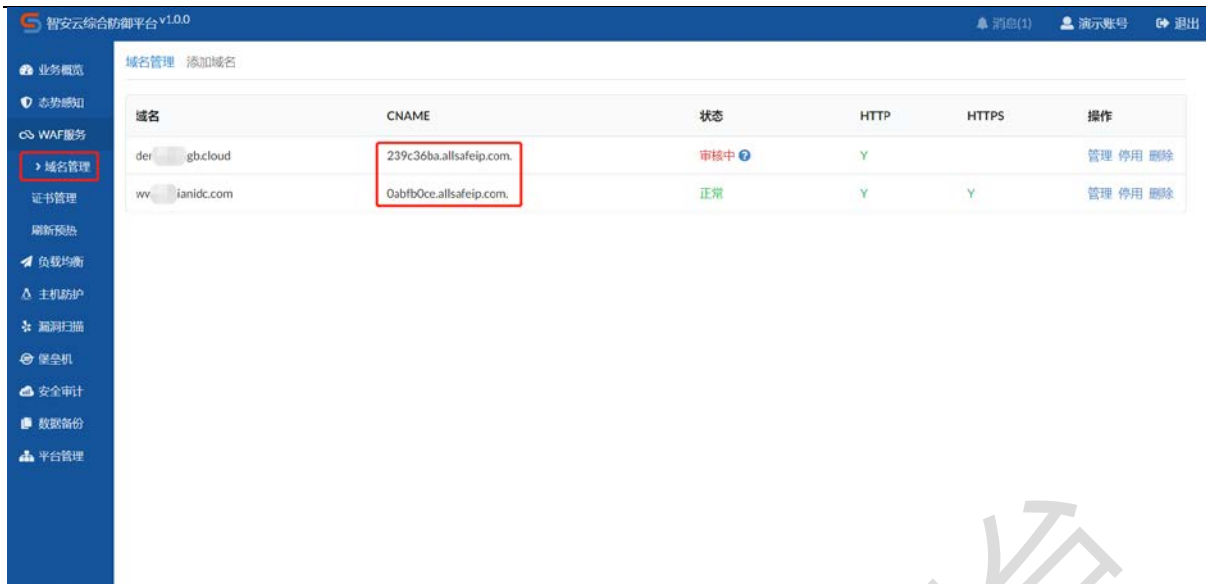
Web 应用防火墙包含了静态资源缓存、TCP/HTTP 代理、安全防护、日志、统计、监控等功能，用户在正确配置域名后可使用相关功能。

#### 1.1. 域名配置

添加域名：填入需要接入的域名-勾选域名协议(有证书勾选 HTTPS，无证书勾选 HTTP)-添加源 IP-选中跟随 CDN 服务-缓存设置-保存。缓存设置可以填入需要缓存的资源的后缀名，并设置好缓存时间。



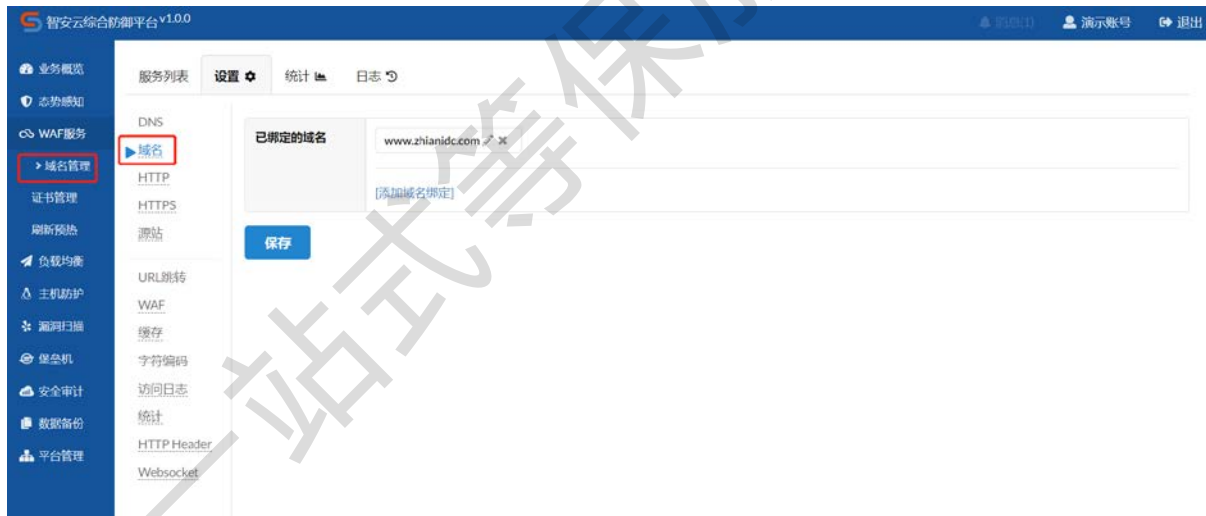
修改域名的 CNAME 记录：在添加域名后，系统会生成一条专属 cname，需要到对应的 DNS 服务商添加该 cname 记录。以阿里云为例：进入阿里云域名解析界面，操作步骤为：添加记录-选择记录类型” CNAME” -填写主机记录” www” -线路选择” 默认” -记录值填入平台分配的 CNAME 地址-确认。



## 1.2. 域名设置

### 1.2.1. 域名设置

点击设置-域名，可以添加域名绑定，支持批量添加域名。



### 1.2.2. HTTP 设置

点击设置-HTTP，可以选择是否启用HTTP、HTTP是否需要跳转到HTTPS。



### 1.2.3. HTTPS 设置

点击设置-HTTPS，可以选择的是否启用 HTTPS，如需要，则点击 HTTPS 进行证书和私钥的上传。



### 1.2.4. 源站设置

点击设置-源站，可配置源站信息（包括源站协议、源站地址以及权重设置），支持配置多个源站。



### 1.2.5. URL 跳转设置

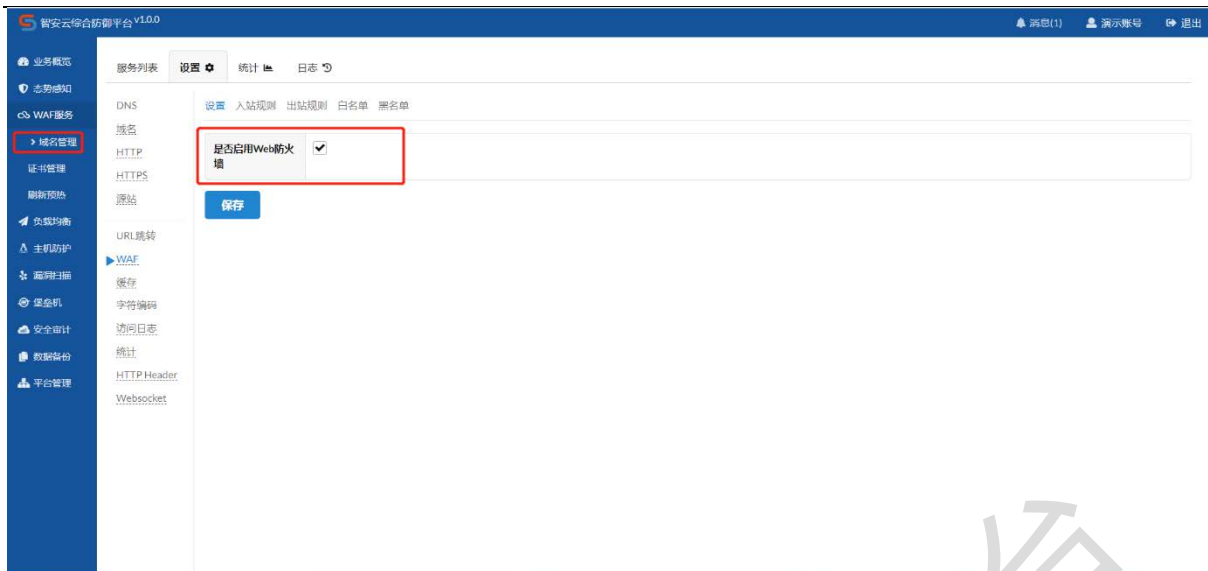
点击设置-URL 跳转，设置跳转后，可实现 HTTP 与 HTTPS 访问的自动跳转。



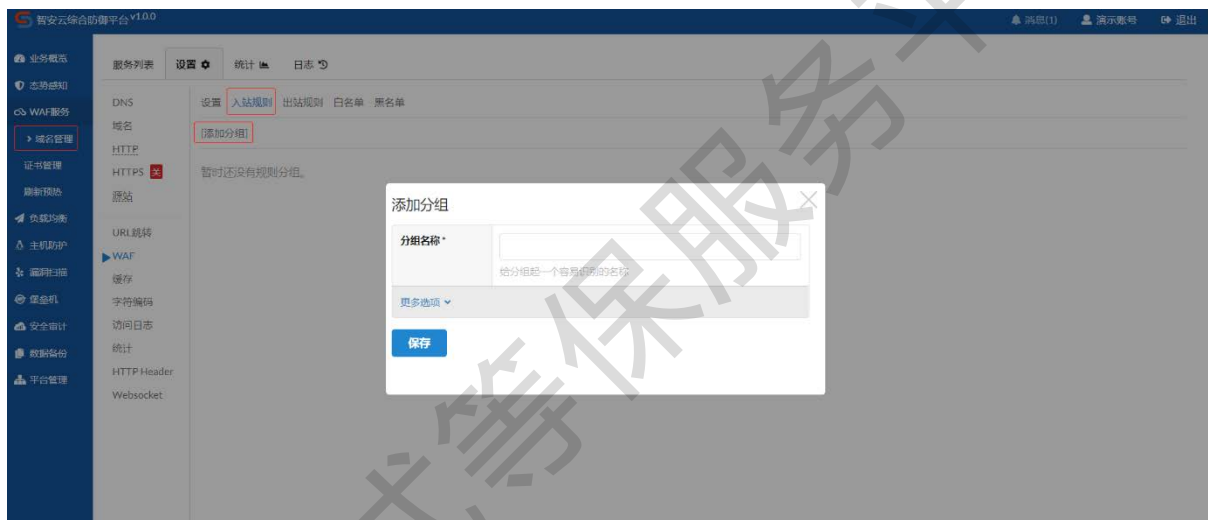
### 1.2.6. WAF 规则设置

开启防火墙功能：点击设置-WAF，然后勾选开启 web 应用防火墙，点击保存。

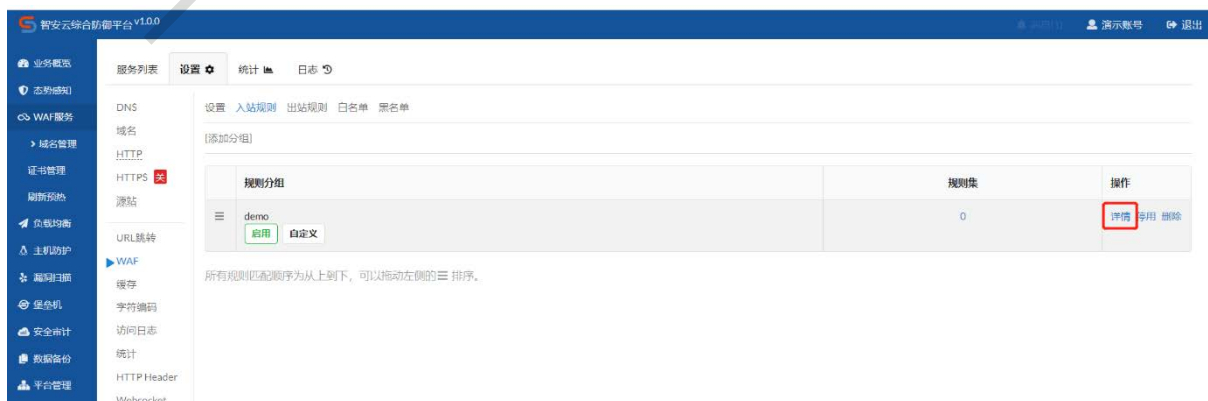


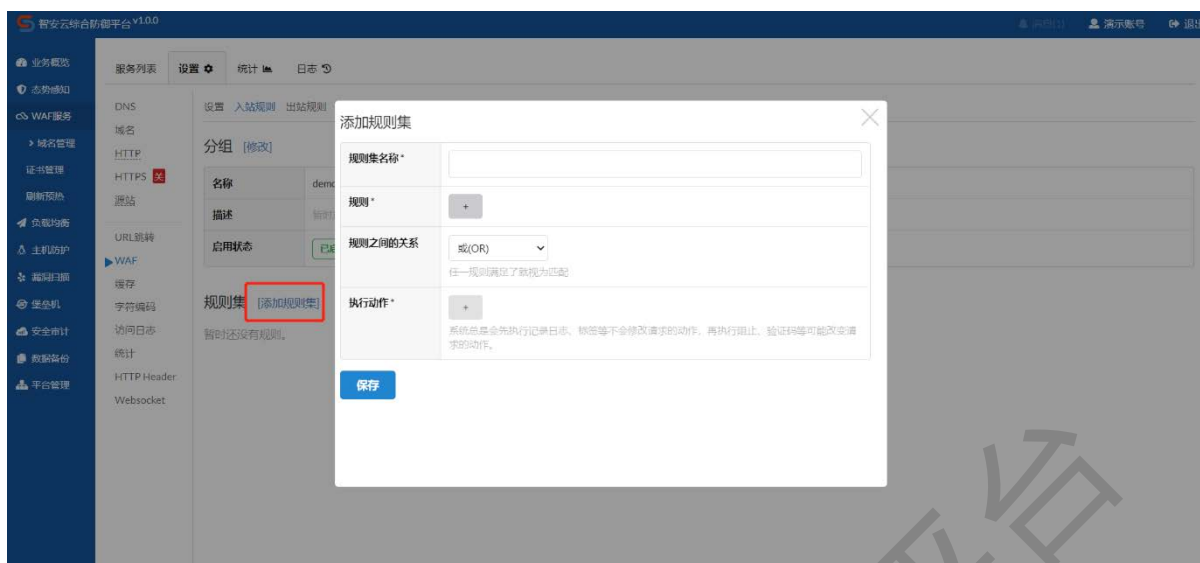


添加入站规则分组：点击入站规则，并创建分组。



添加入站规则：通过点击规则分组的详情按钮，进入规则新增页面，按需添加入站规则。



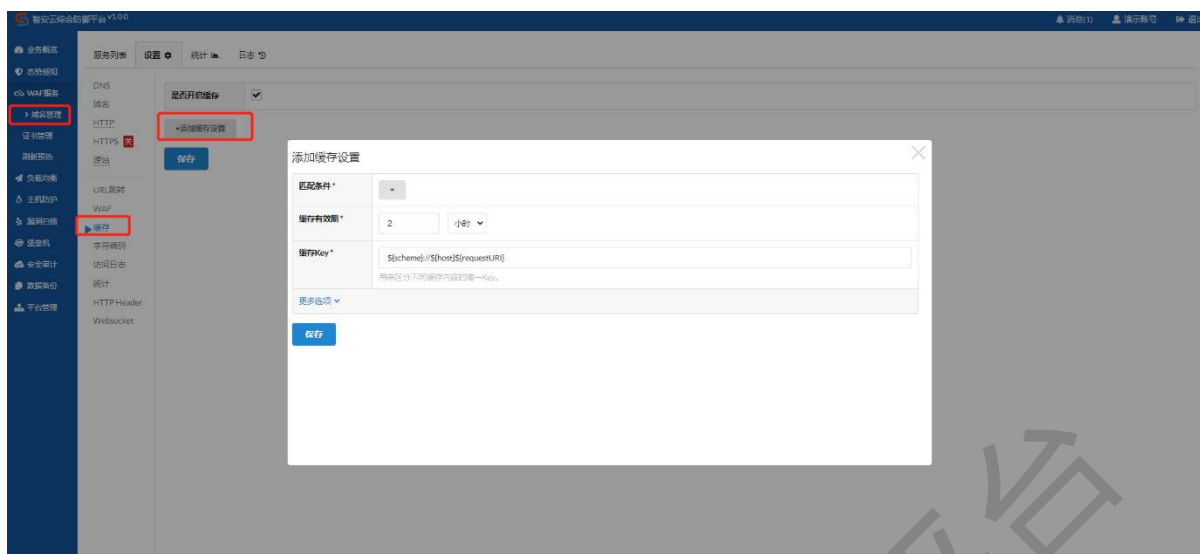


### 1.2.7. 缓存设置

**开启缓存：**可以根据业务需要开启和关闭缓存，点击设置-缓存-进入缓存设置界面

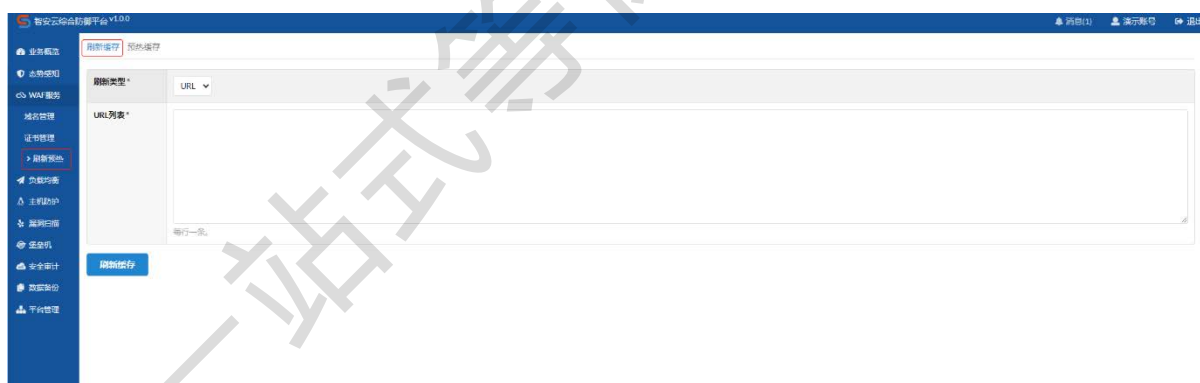


**添加缓存设置：**可自主设置缓存策略，包含匹配条件、缓存有效期、缓存 key，可缓存的最大文件的大小，状态码、需要跳过的 Cache-Control 值等等，设置完成后点击保存即可。

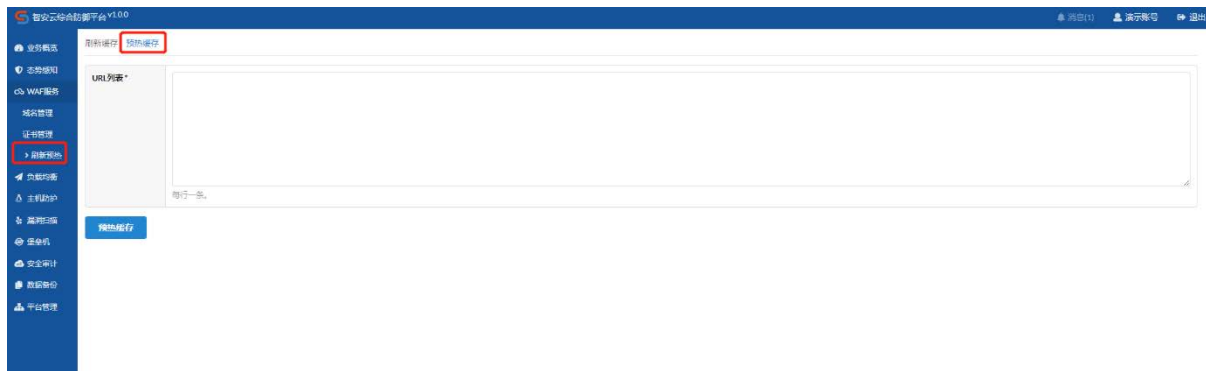


### 1.3. 刷新预热

刷新缓存：选择刷新类型，输入需要刷新的 URL（每行一条 URL），点击刷新缓存即可，缓存刷新生效后，节点内容将被更新。

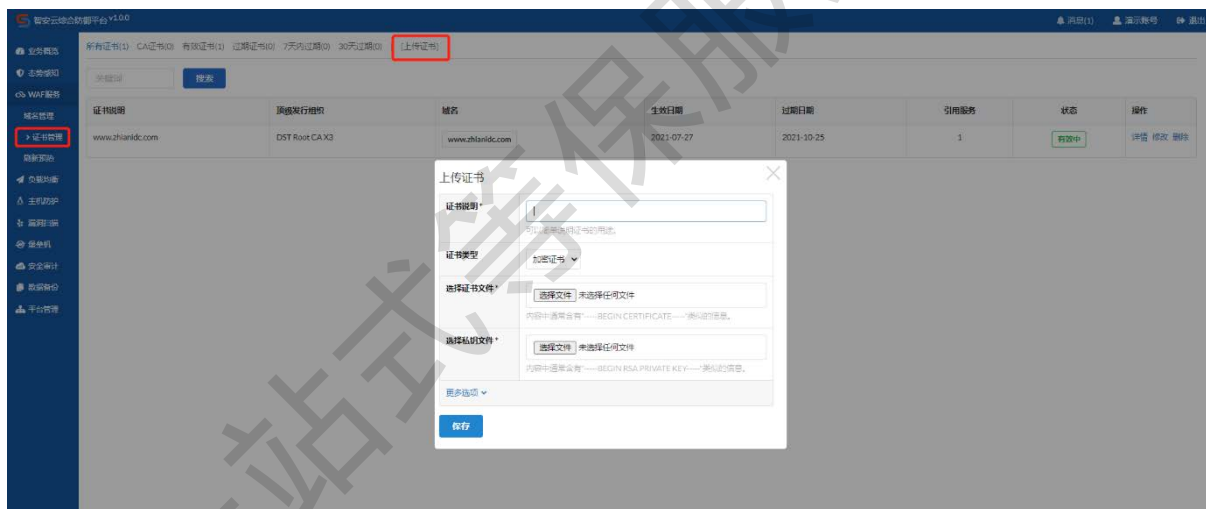


缓存预热：点击“预热缓存”，进入缓存预热设置界面，输入需要缓存的 URL，点击预热缓存保存设置，设置完成后该 URL 的内容将会被主动缓存到 WAF 节点上。

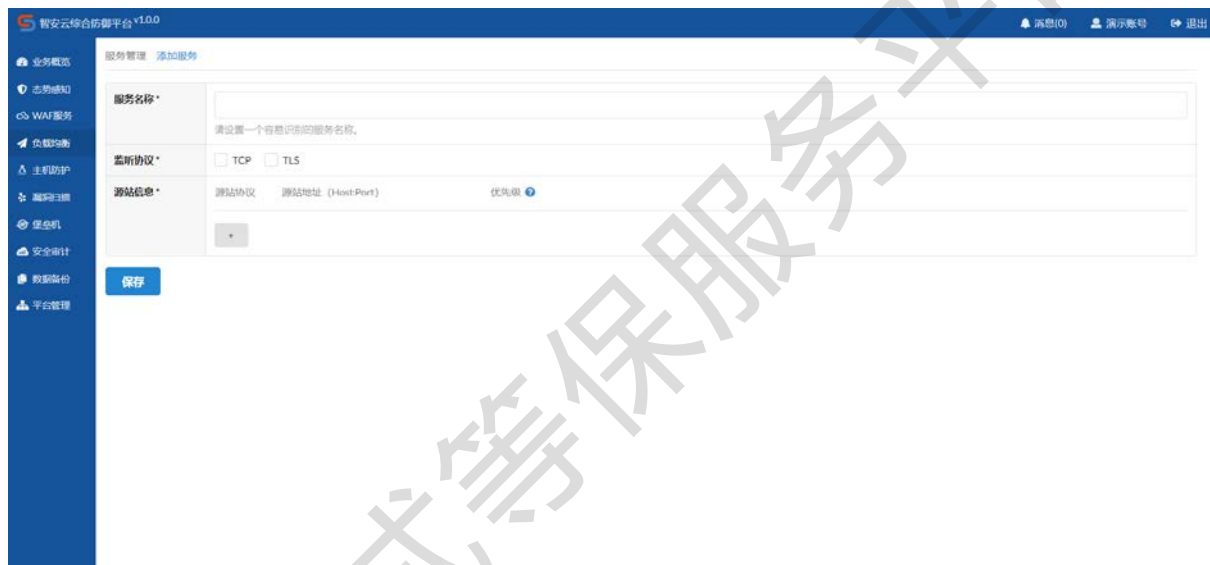
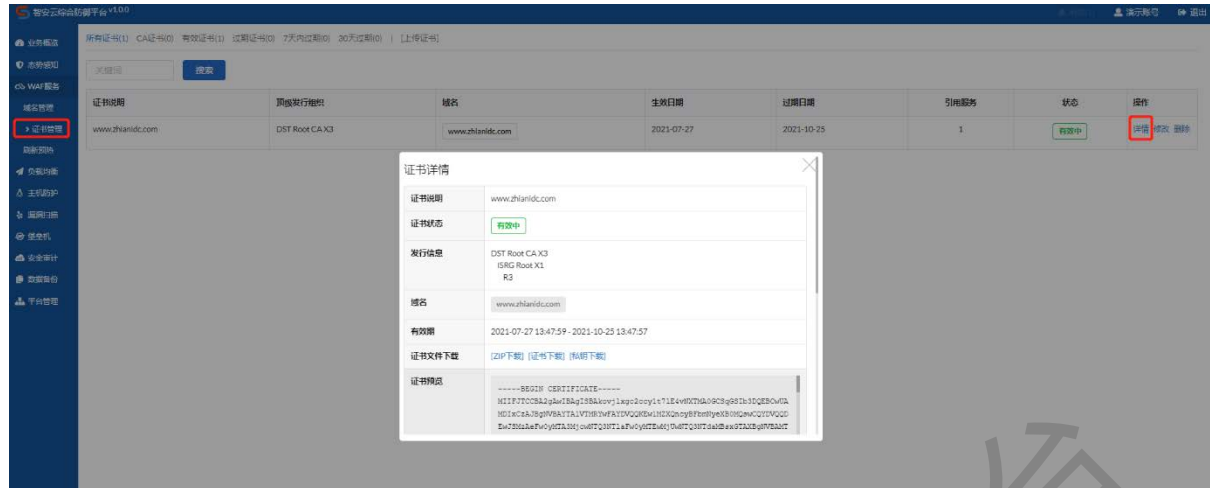


## 1.4. 证书管理

上传证书：用户从【WAF 服务】进入“证书管理”界面，点击右上方“上传证书”



证书详情：用户从【WAF 服务】进入“证书管理”界面，可查看所有证书，可查看证书详情，修改和删除证书。



## 1.5. 负载均衡

添加服务：用户从【负载均衡】进入“添加服务”界面，点击左上方“添加服务”

管理员在后台管理界面，【WAF 服务】-【服务列表】里查看服务所在集群，在【WAF 服务】-【集群列表】选择对应集群中任意【IP+端口】给用户即可。

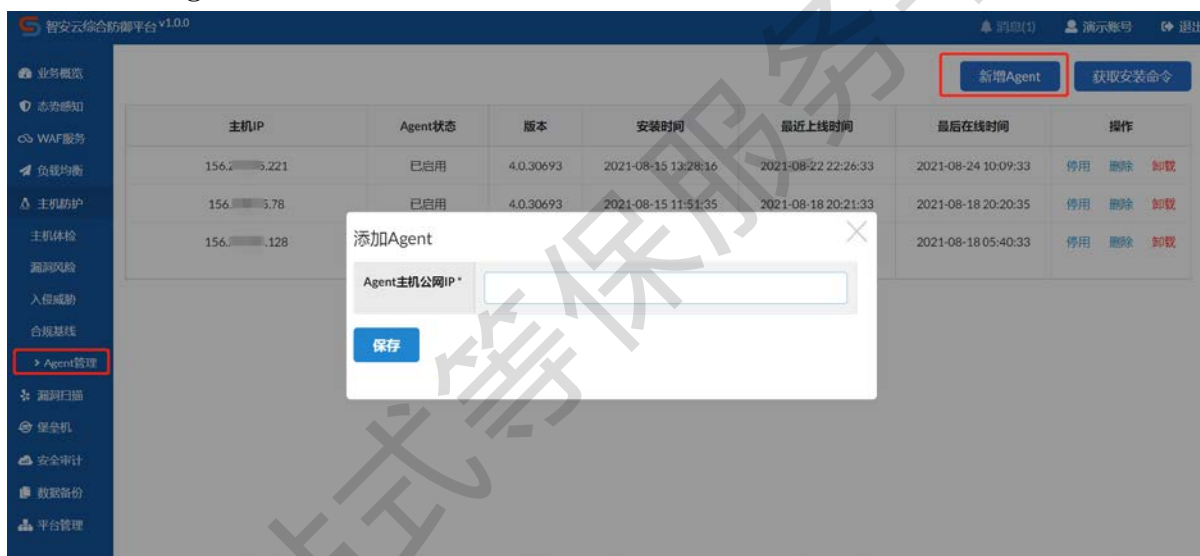
## 2. 主机防护

主机防护模块包含了安全体检、漏洞风险、入侵威胁、合规基线等多个功能模块，各个模块进行联动，模块间数据联通，形成闭环系统，为用户提供强有力的采集、检测、监测、防御、捕获能力，对主机进行全方位的安全防护。

## 2.1. Agent 安装

在使用主机防护功能之前，需要在对应主机上下载并安装 Agent。安装完毕后即可使用主机防护所有功能。

填写主机 IP：用户从【主机防护】进入“Agent 管理”界面，点击右上方“新增 Agent”按钮后，填写目标主机的公网 IP 地址。

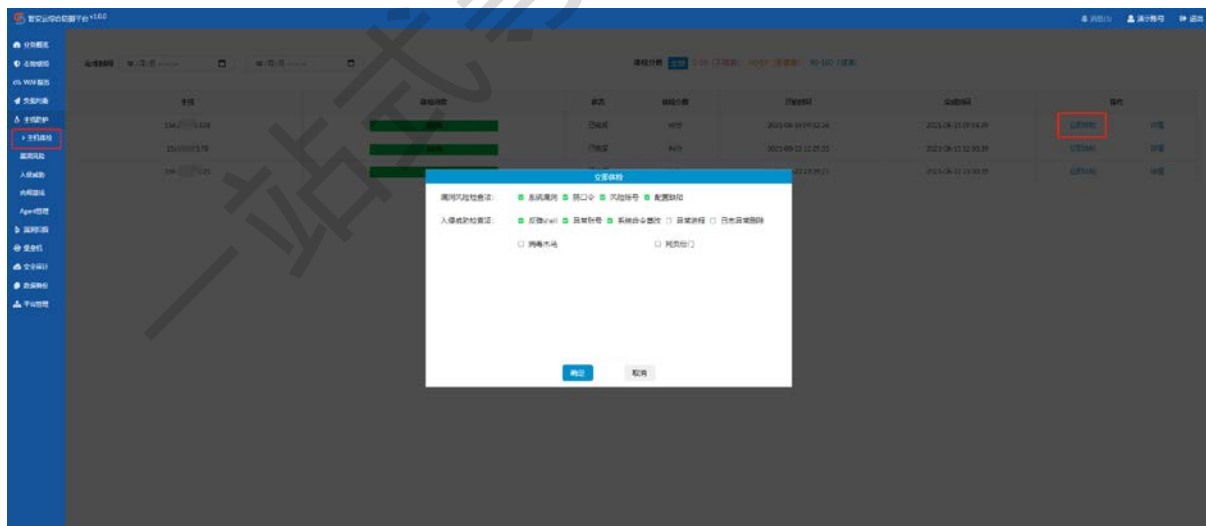


下载并安装 Agent：用户从【主机防护】进入“Agent 管理”界面，点击右上方“获取安装命令”按钮，复制对应操作系统的安装命令并在目标主机运行。

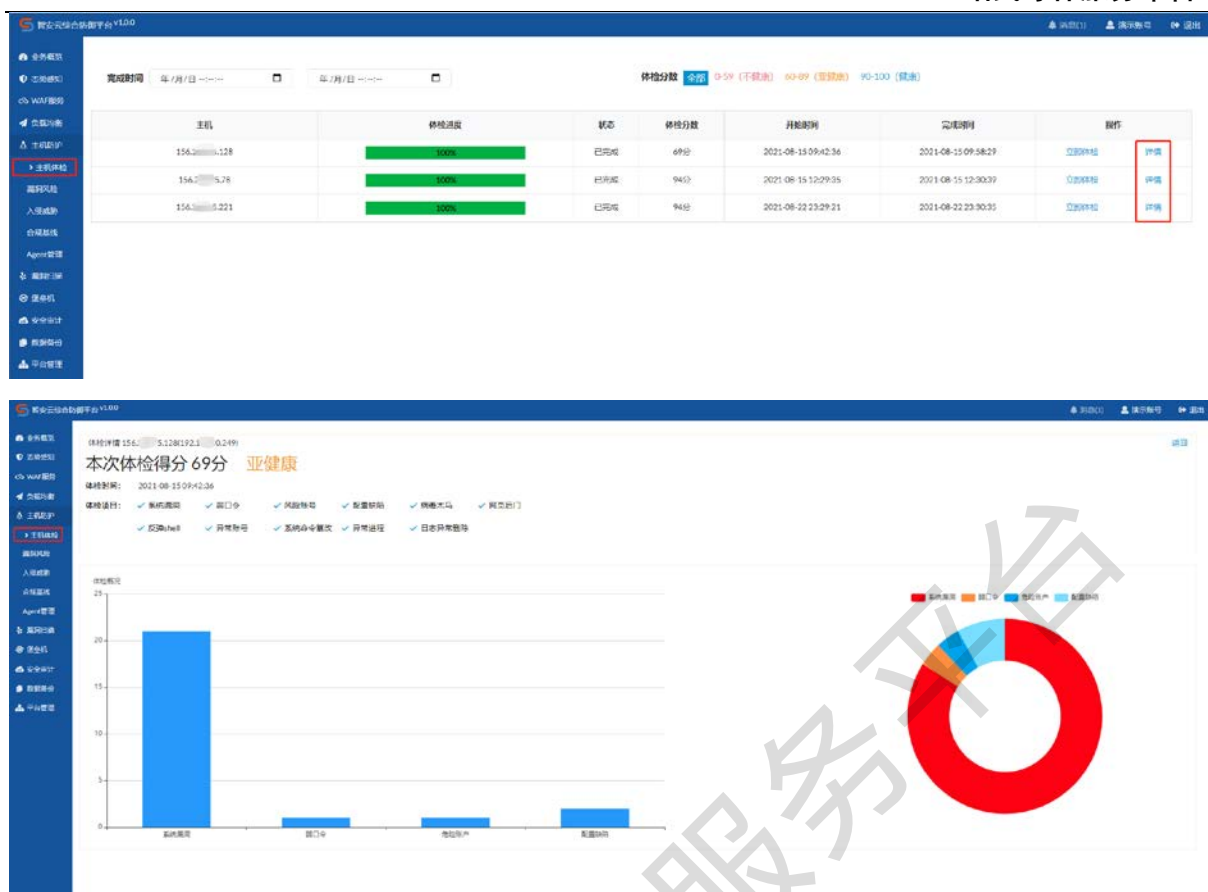


## 2.2. 主机体检

主机体检：用户从【主机防护】进入“主机体检”界面，在主机体检中用户可主动发起主机深度检测，检测的项目包括：系统漏洞、弱口令、高危账号、配置缺陷、病毒木马、网页后门、反弹 shell、异常账号、日志删除、异常进程、系统命令校验等。主机体检检测出的问题系统自动进行问题归类到漏洞风险及入侵威胁模块中。



体检详情：点击体检列表的详情按钮，可以查看体检报告信息。

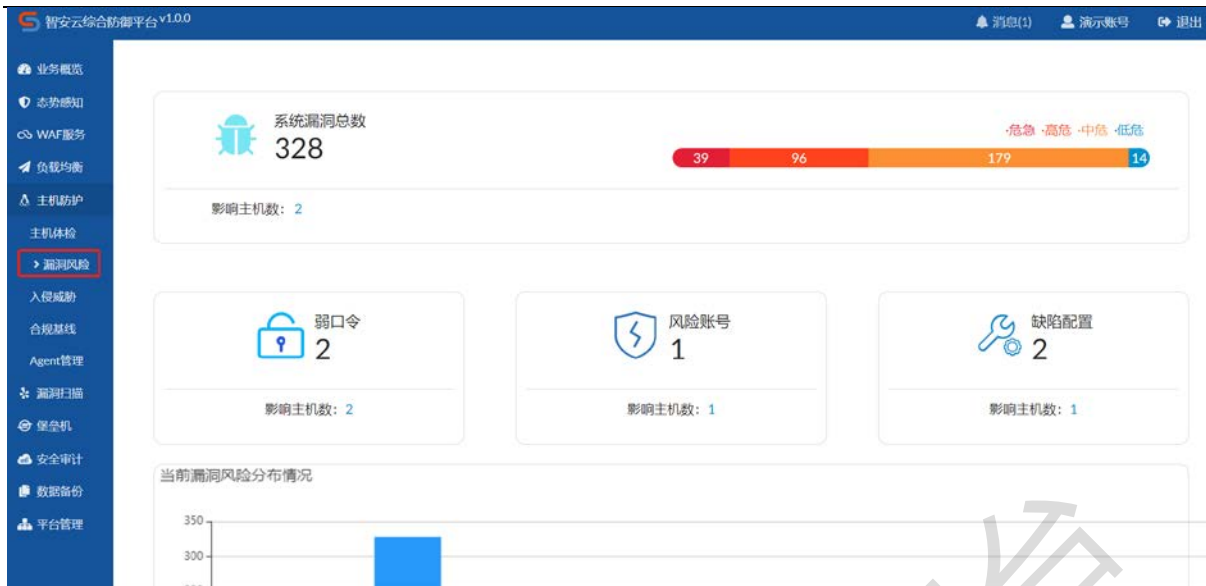


## 2.3. 漏洞风险

漏洞风险包含两个部分，一是主机自身的安全漏洞如系统漏洞（Windows 漏洞及 Linux 系统漏洞）；二是人为原因造成的风险因素如弱口令（操作系统弱口令、数据库弱口令等）、风险账号（高权限账号、空密码账号、用户名和密码相同的账号）、配置缺陷（操作系统配置缺陷、Web 容器配置缺陷、数据库配置缺陷等）。

漏洞风险管理模块会显示当前主机上的漏洞风险情况，同时提供修复方案供用户进行参考；该模块执行时会从云端下载漏洞策略库在本地执行检测，对于存在漏洞风险的主机，会上报应用程序的名称、版本号、路径、发现时间，这个过程不会提取任何涉及用户隐私的数据。对于检测出的各类漏洞风险进行风险等级评估。



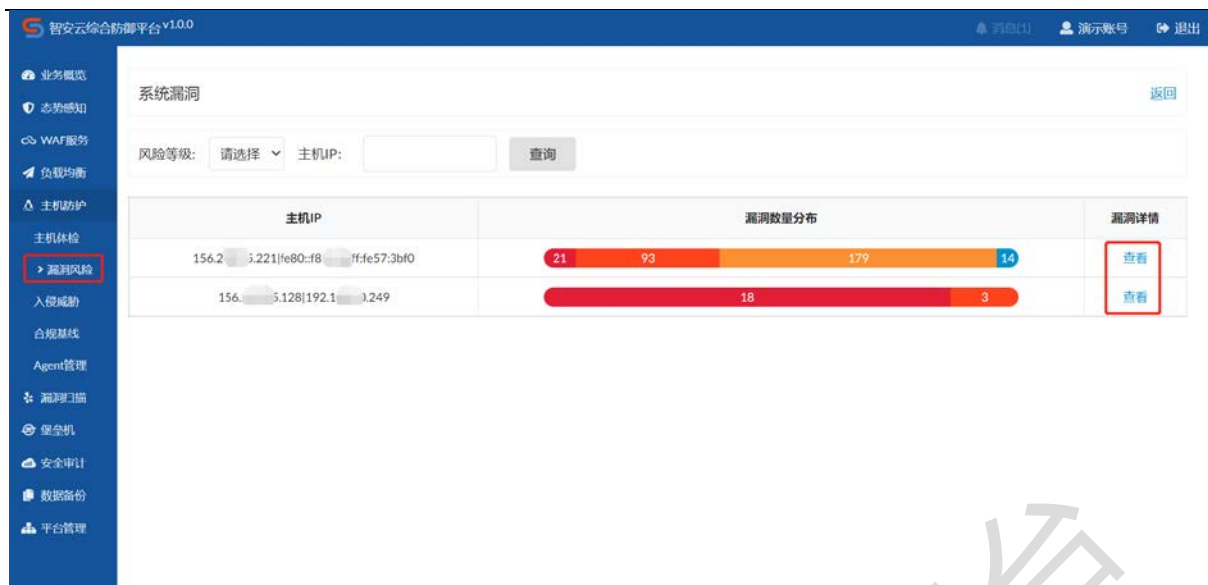


### 2.3.1. 系统漏洞

Windows 漏洞通过订阅微软漏洞更新，当发现主机存在漏洞时推送微软官方补丁信息，支持漏洞忽略；

Linux 漏洞通过检测主机上的软件版本信息，与 CVE 官方漏洞库进行匹配，检测出存在漏洞软件并推送漏洞信息，支持漏洞忽略；





主机信息

操作系统: centos linux7.9.2009\_64bit 上次扫描时间: 2021-08-24 10:27:33 系统漏洞数: 367

待处理(367) 已处理(0)

风险等级	漏洞名称	风险特征	发现时间	来源	状态	操作
中危	CVE-2015-2716	未知影响	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略
低危	CVE-2015-8035	未知影响	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略
中危	CVE-2015-9289	需重启系统	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略
高危	CVE-2016-10745	未知影响	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略
高危	CVE-2016-5131	未知影响	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略
高危	CVE-2017-12652	未知影响	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略
中危	CVE-2017-15412	未知影响	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略
低危	CVE-2017-17807	需重启系统	2021-08-16 20:32:20	本地扫描	待处理	详情 忽略

### 2.3.2. 弱口令

通过系统内置的弱口令库可发现识别操作系统弱口令、数据库弱口令、应用弱口令，支持弱口令忽略；弱口令有可能导致密码轻易被黑客或入侵者识别破译，进而成为入侵主机的快速通道，对弱口令进行检测识别并重新设置更复杂的密码，有利于保障主机安全。



智安云综合防御平台 v1.0.0

消息(1) 演示账号 退出

业务概览 态势感知 WAF服务 负载均衡 主机防护 主机体检 漏洞风险 入侵威胁 合规基线 Agent管理 漏洞扫描 堡垒机 安全审计 数据备份 平台管理

弱口令

主机IP: 查询

主机IP	弱口令数量	详情
156.2 3.221 fe80:f816:3 57:3b10	1	查看
156.2 128 192.1 249	1	查看

智安云综合防御平台 v1.0.0

消息(1) 演示账号 退出

业务概览 态势感知 WAF服务 负载均衡 主机防护 主机体检 漏洞风险 入侵威胁 合规基线 Agent管理 漏洞扫描 堡垒机 安全审计 数据备份 平台管理

主机信息

操作系统: centos linux7.9.2009\_64bit 上次扫描时间: 2021-08-24 10:30:33 弱口令数: 1

待处理(1) 已处理(0)

风险等级	风险说明	类型	发现时间	来源	操作
高危	操作系统: CentOS, 账号: zxl, 密码: 123456	操作系统弱口令	2021-08-22 23:29:36	本地扫描	详情 忽略

### 2.3.3. 风险账号

通过账户防护引擎可识别发现高权限账号、空密码账号、用户名和密码

相同的账号；提权帐号的产生，很可能是系统被入侵后黑客或者入侵者对系统帐号进行了修改，及时对提权账号进行检测识别并删除提权账号有利于保障主机安全；



风险账号

返回

主机IP:  查询

主机IP	风险账号数量	详情
156.240.95.128 192.168.10.249	1	<a href="#">查看</a>

主机信息

返回

操作系统: Microsoft Windows 2012 R2 (64 bit)  
(Build 9,600)

上次扫描时间: 2021-08-18 05:40:33

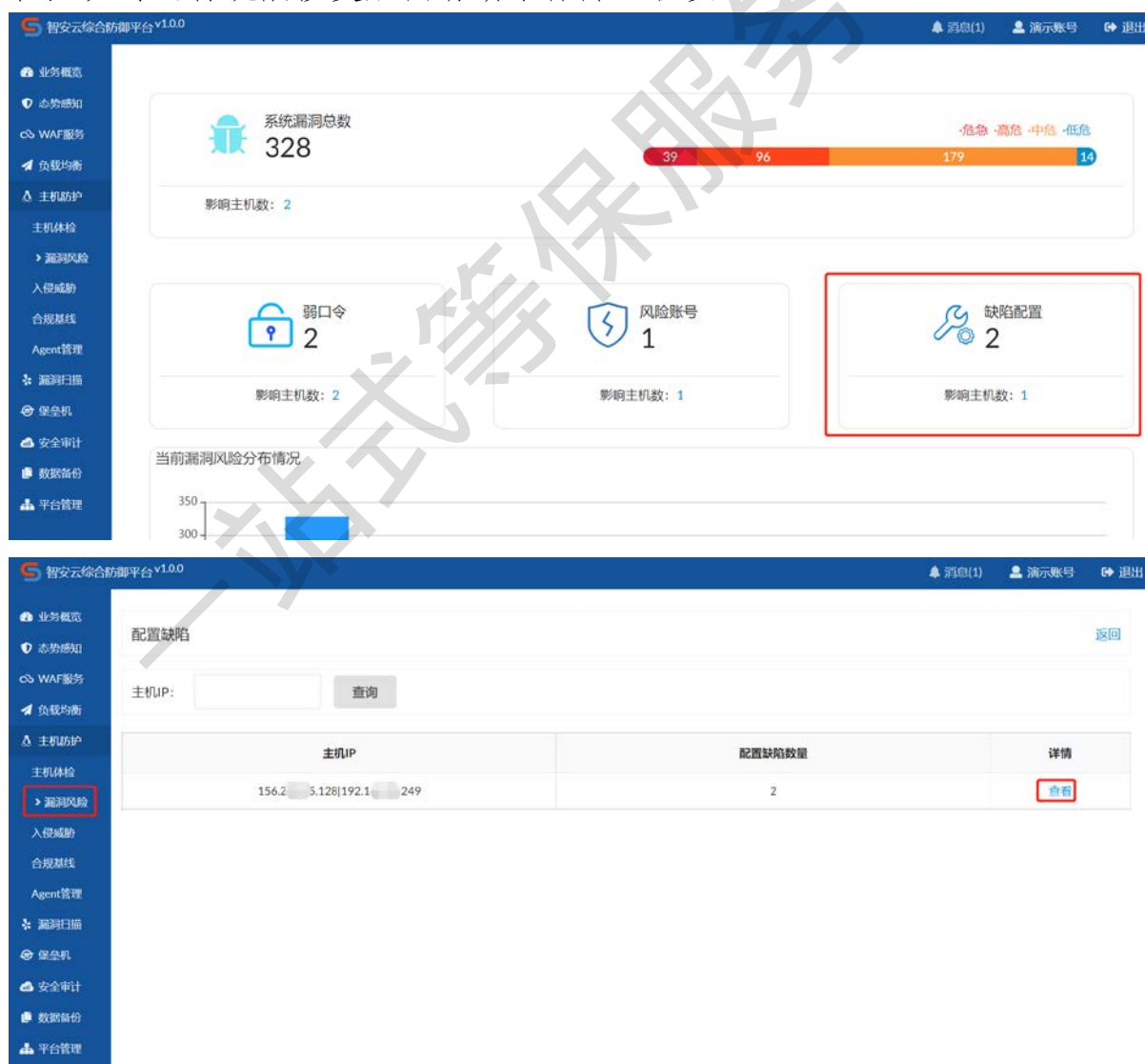
风险账号: 1

待处理(1) 已处理(1)

风险等级	风险说明	类型	发现时间	来源	操作
高危	系统帐号: 123\$,账号风险: 非内置系统管理员帐户	操作系统配置缺陷	2021-08-15 09:45:30	本地扫描	<a href="#">详情</a> <a href="#">忽略</a>

### 2.3.4. 缺陷配置

系统用户强大的操作系统、Web 容器、数据库、及其他应用的配置缺陷检测检测能力,支持 Windows2003、Windows2008、Windows2012、Windows2016 等各种 Windows 系统配置缺陷检测,支持 Memcached、CentOS、Ubuntu、Debian、OpenSUSE、RedHat 等 Linux 操作系统配置缺陷检测;支持 IIS、Apache、Nginx、Tomcat、Weblogic、Tengine、JBoss 等各类 Web 容器配置缺陷检测;支持 Redis、Mongodb、Memcached、ElasticSearch、PostgreSQL、Oracle 等数据库配置缺陷检测;支持 FTP、SNMP、Samba 等应用的配置缺陷检测。各种配置缺陷的存在容易被黑客利用造成严重的损害,及时进行缺陷修复加固有助于保障主机安全。



智安云综合防御平台 v1.0.0

消息(1) 演示账号 退出

业务概览 态势感知 WAF服务 负载均衡 主机防护 主机体检 漏洞风险 合规基线 Agent管理 漏洞扫描 堡垒机 安全审计 数据备份 平台管理

### 主机信息

返回

操作系统: Microsoft Windows 2012 R2 (64 bit) (Build 9,600) 上次扫描时间: 2021-08-18 05:40:33 缺陷配置: 2

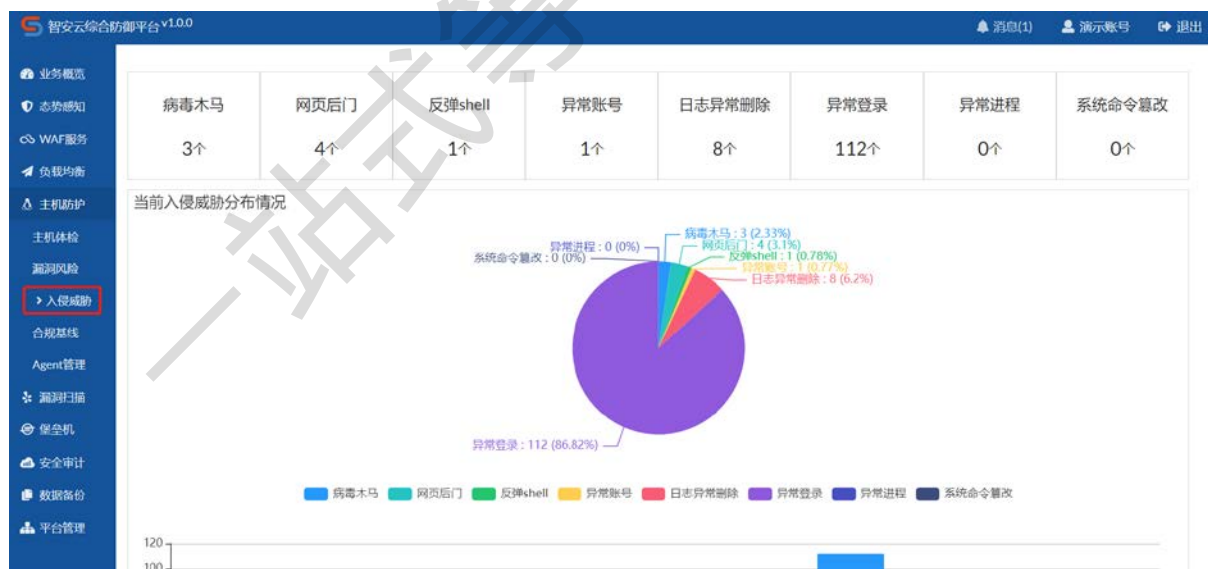
待处理(2) 已处理(1)

风险等级	风险说明	类型	当前版本	安装路径	发现时间	来源	操作
低危	ADMIN\$存在写权限	操作系统配置缺陷	6.3.9.600.17.415	C:\Windows	2021-08-15 09:45:30	本地扫描	详情 忽略
中危	数据库:MySQL, 危险目录:C:\Program Files\MySQL\MySQL Server 5.5\, 危险权限-ALL APPLICATION PACKAGES(可执行, 读), CREATOR OWNER(特别权限)	操作系统配置缺陷	5.5.60	C:\Program Files\MySQL\MySQL Server 5.5	2021-08-15 09:45:30	本地扫描	详情 忽略

## 2.4. 入侵威胁

入侵威胁用以展示及处理各类入侵事件及具有高度威胁的事件, 支持识别并处置的入侵威胁事件包括: 病毒木马、网页后门、反弹 shell、异常账号、日志删除、异常登录、异常进程、系统命令篡改等。

主机防护模块对接国内外主流查杀引擎, 可检测出恶意进程及软件, 并提供隔离、信任等功能。



### 2.4.1. 病毒木马

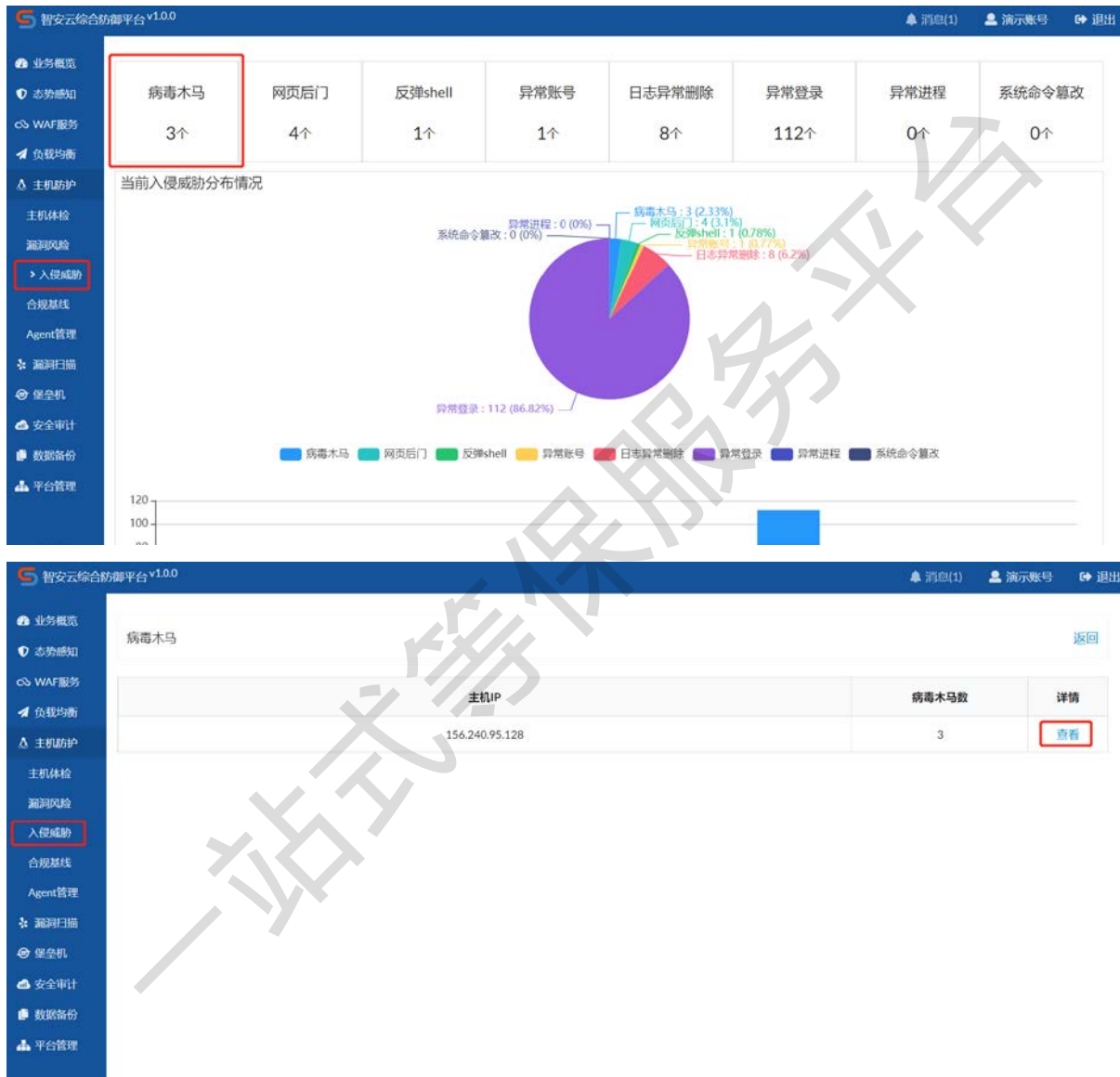
病毒木马程序通常会窃取用户数据或者对外攻击, 消耗大量系统资源导致业务不能正常提供服务。Agent 会采集可疑病毒木马程序的哈希指纹到



云端，通过云查杀模块对哈希进行检测识别。

若确认文件是恶意的，可以对单个文件进行隔离，隔离成功后，原始恶意文件将被加密隔离，后期可以在隔离区进行恢复。

如果文件非恶意的，可以选择信任操作，加入信任后，系统将不再对该文件进行检测，后期可以在信任区对信任文件进行管理。



主机信息

操作系统: Microsoft Windows 2012 R2 (64 bit)  
(Build 9,600)

上次扫描时间: 2021-08-18 05:40:33

病毒木马数: 3

待处理(3) 隔离区(0) 信任区(0) 删除区(0)

病毒木马类型	hash值	路径	发现时间	来源	状态	操作
Trojan(PSW)/Win64.Mimikatz	157A22689629EC876337F5F9409918D5	C:\Users\Administrator\Desktop\nc\mimikatz.sys	2021-08-15 02:31:29	实时防护	未处理	详情 信任 隔离
Trojan(PSW)/Win32.Mimikatz	C09B6FAB1A9B1F04642E195A661FF4BE	C:\Users\Administrator\Desktop\nc\mimilib.dll	2021-08-15 02:31:29	实时防护	未处理	详情 信任 隔离
Trojan/Generis.ASMalwS.2516	A3CB3B02A683275F7E0A0F8A9A5C9E07	C:\Users\Administrator\Desktop\nc\mimikatz.exe	2021-08-15 02:32:29	实时防护	未处理	详情 信任 隔离

### 2.4.2. 网页后门

网站后门木马又叫 webshell，一般是黑客通过漏洞入侵网站后放置的 ASP、PHP、JSP 等动态脚本。黑客可以通过后门木马持续控制服务器，进行文件上传下载、执行命令等各种破坏行为，对网站安全危害极大。

主机防护模块可以实时准确的查杀各类木马恶意文件，同时提供恶意文件检测 and 一键隔离等功能，第一时间清除木马后门文件，确保用户服务器的安全。

主机信息

操作系统: Microsoft Windows 2012 R2 (64 bit)  
(Build 9,600)

上次扫描时间: 2021-08-18 05:40:33

网页后门数: 4

待处理(4) 隔离区(0) 信任区(0) 删除区(0)

网页后门类型	hash值	路径	发现时间	来源	状态	操作
(base64_decode)变量函数	B2232693303F8D5E04E458207E51C080	C:\phpstudy_pro\WWW\web1.php	2021-08-15 00:17:29	实时防护	未处理	详情 信任 隔离
JSP文件木马	D69652E2956F22FA11254B06377BAAF	C:\phpstudy_pro\WWW\web1.jsp	2021-08-15 00:17:29	实时防护	未处理	详情 信任 隔离
PHP一句话木马	E459CDDDEA021874BAF517C559E0D1E	C:\phpstudy_pro\WWW\web1.php	2021-08-15 00:17:29	实时防护	未处理	详情 信任 隔离
(base64_decode)变量函数	AC19C32CDD2D6C1E1A910BC0F248CAAB	C:\phpstudy_pro\WWW\web1shell.php	2021-08-16 14:15:30	实时防护	未处理	详情 信任 隔离

### 2.4.3. 反弹 shell

主机防护模块支持反弹 shell 检测识别及事件关闭，通过对反弹



shell 事件进行检测识别可入侵攻击；

主机信息

操作系统: Microsoft Windows 2012 R2 (64 bit) (Build 9,600) 上次扫描时间: 2021-08-18 05:40:33 反弹shell数: 1

待处理(1) 已处理(0)

进程路径	进程运行参数	是否为外部链接	反弹地址	发现时间	来源	状态	操作
C:\Windows\Help\coder.exe	coder	1	45.124.64.78:34001	2021-08-14 00:44:28	安全监控	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>

#### 2.4.4. 异常账号

主机防护模块支持影子账号、篡改系统账号的检测识别及事件关闭，影子账号支持禁用处理；影子账号是隐藏的账户，有管理员权限的账户，影子帐号的产生，很可能是系统被入侵后黑客或者入侵者对系统帐号进行了修改。对影子账号进行禁用处理有助于保障主机安全。

#### 2.4.5. 日志异常删除

主机防护模块支持日志删除的检测识别及事件关闭，黑客入侵后可能对相关日志信息进行删除，检测识别日志删除事件并产生告警能够帮助安全人员及时跟进做确认。

主机信息

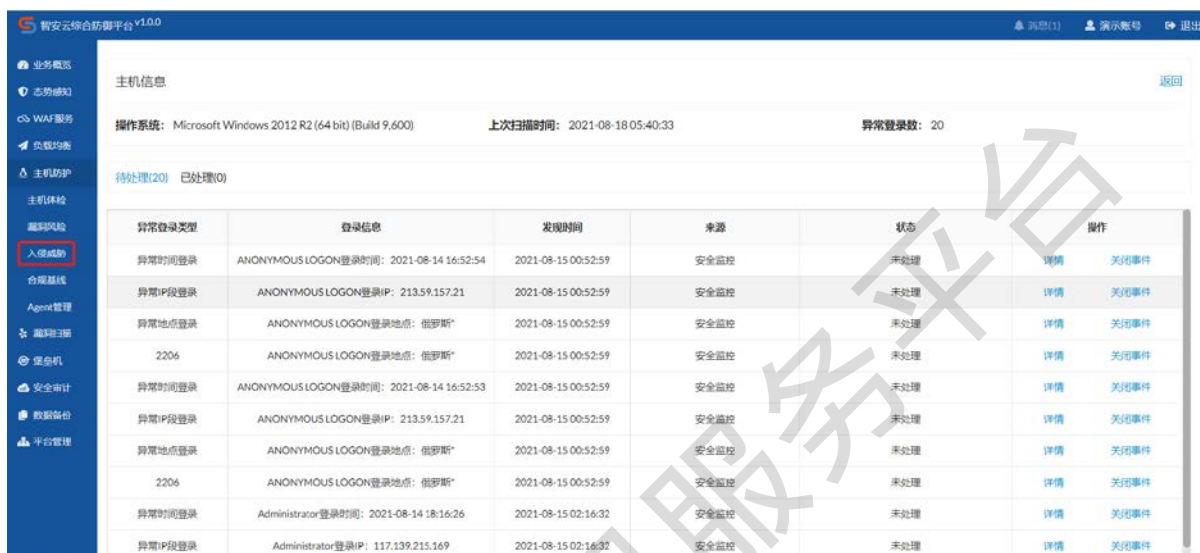
操作系统: Microsoft Windows 2012 R2 (64 bit) (Build 9,600) 上次扫描时间: 2021-08-18 05:40:33 日志异常删除数: 8

待处理(8) 已处理(0)

类型	日志路径	操作用户	发现时间	来源	状态	操作
日志异常删除	C:\Windows\system32\Winevt\Logs\System.evtx_@WINDOWS\Administrator_@System	WINDOWS\Administrator	2021-08-13 17:13:30	本地扫描	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>
日志异常删除	C:\Windows\system32\Winevt\Logs\System.evtx_@WINDOWS\Administrator_@System	WINDOWS\Administrator	2021-08-13 17:13:30	本地扫描	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>
日志异常删除	C:\Windows\system32\Winevt\Logs\System.evtx_@WIN-MIF3TN1VU26_@System	WIN-MIF3TN1VU26	2021-08-13 17:13:30	本地扫描	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>
日志异常删除	C:\Windows\system32\Winevt\Logs\System.evtx_@WIN-MIF3TN1VU26_@System	WIN-MIF3TN1VU26	2021-08-13 17:13:30	本地扫描	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>
日志异常删除	C:\Windows\system32\Winevt\Logs\System.evtx_@WIN-MIF3TN1VU26_@System	WIN-MIF3TN1VU26	2021-08-13 17:13:30	本地扫描	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>
日志异常删除	C:\Windows\system32\Winevt\Logs\Security.evtx_@Administrator_@Security	Administrator	2021-08-13 17:13:30	本地扫描	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>
日志异常删除	C:\Windows\system32\Winevt\Logs\System.evtx_@WINDOWS\Administrator_@System	WINDOWS\Administrator	2021-08-14 17:35:29	本地扫描	未处理	<a href="#">详情</a> <a href="#">关闭事件</a>

### 2.4.6. 异常登录

主机防护模块支持异常地点登陆、异常 IP 段登录、异常时间登录、异常计算机名登录、暴力破解登录 5 种异常登录类型检测及事件关闭。异常登录意味着主机相关密码已经被窃取或破解，检测识别异常登录事件可及时发现主机风险，及时进行补救。



异常登录类型	登录信息	发现时间	来源	状态	操作
异常时间登录	ANONYMOUS LOGON 登录时间: 2021-08-14 16:52:54	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
异常IP段登录	ANONYMOUS LOGON 登录IP: 213.59.157.21	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
异常地点登录	ANONYMOUS LOGON 登录地点: 俄罗斯*	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
2206	ANONYMOUS LOGON 登录地点: 俄罗斯*	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
异常时间登录	ANONYMOUS LOGON 登录时间: 2021-08-14 16:52:53	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
异常IP段登录	ANONYMOUS LOGON 登录IP: 213.59.157.21	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
异常地点登录	ANONYMOUS LOGON 登录地点: 俄罗斯*	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
2206	ANONYMOUS LOGON 登录地点: 俄罗斯*	2021-08-15 00:52:59	安全监控	未处理	详情 关闭事件
异常时间登录	Administrator 登录时间: 2021-08-14 18:16:26	2021-08-15 02:16:32	安全监控	未处理	详情 关闭事件
异常IP段登录	Administrator 登录IP: 117.139.215.169	2021-08-15 02:16:32	安全监控	未处理	详情 关闭事件

### 2.4.7. 异常进程

主机防护模块支持子进程权限高于父进程、隐藏进程、隐藏端口进程 3 种异常进程的检测识别及事件关闭。隐藏端口进程在系统中查看未能发现，但实际却在系统中被监听的端口，极大可能是系统遭遇入侵后被植入的恶意木马程序开启的服务；隐藏进程 在系统中查看未能发现，但实际却在系统中运行的进程，极大可能是系统遭遇入侵后被植入的恶意木马程序。及时检测识别异常进程并关闭异常进程有助于保障 主机安全。

### 2.4.8. 系统命令篡改

主机防护模块支持系统命令校验的检测识别及事件关闭；系统命令如果被恶意修改，可能会导致用户在使用系统命令时，实际使用的是被修改后的恶意程序，导致信息泄露或被入侵。及时检测识别系统命令校验事件，通过重新安装系统命令对应的包，对系统命令进行修复有助于保障主机安全。

## 2.5. 合规基线

在等级保护检查、测评、整改工作过程中，对定级业务系统进行对应级别的安全风险检查是技术方面的必要工作，通过使用主机防护模块的合规基线功能进行基线检查即可轻松完成。

主机防护模块对国家等级保护规范进行了详细整理，把技术标准落实到每一种应用的配置检查工作上。主机防护模块结合等级保护工作过程，对业务系统资产进行等保定级跟踪，根据资产定级自动进行对应级别的安全配置检查，对合规情况出具等保符合性报告，保证系统建设符合等保要求，促使等保监督检查工作高效执行。

基线检查：用户从【主机防护】进入“合规基线”界面，点击立即检查/重新检查按钮，在弹出的窗口中选择基线模板，点击确定后进行基线检查。

检查详情：点击基线检查列表中的详情按钮，可以查看基线检查报告信息。

智安云综合防御平台 V1.0.0

消息(1) 演示账号 退出

业务概览 态势感知 WAF服务 负载均衡 主机防护 主机体检 漏洞扫描 入侵检测 合规基线 Agent管理 漏扫扫描 堡垒机 安全审计 数据备份 平台管理

检查时间 年/月/日 年/月/日 检查结论 全部 基线异常 基线正常

主机	检查进度	状态	异常项/总检查项	完成时间	操作
156.2.15.221	100%	已完成	12/15	2021-08-16 20:06:34	重新检查 详情
156.2.15.78	100%	已完成	10/12	2021-08-18 17:55:42	重新检查 详情
156.2.15.128	100%	已完成	11/16	2021-08-14 22:44:32	重新检查 详情



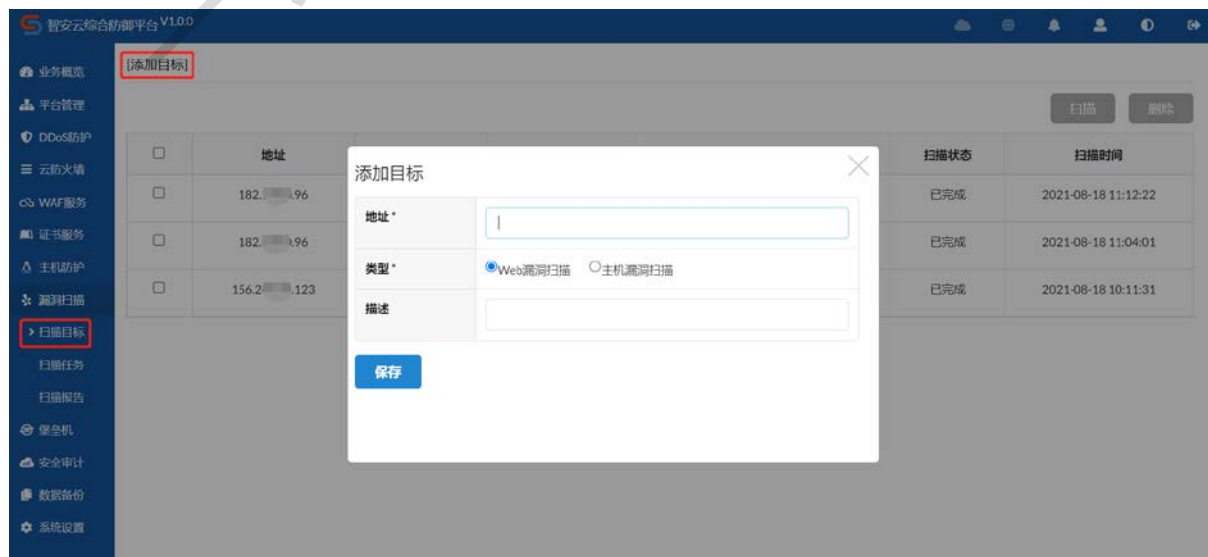
### 3. 漏洞扫描

漏洞扫描模块具备主机漏洞扫描及 Web 应用漏洞扫描两大功能，能为目标资产提供主机服务和 Web 应用服务的深度安全检测，可帮助用户快速、全面地发现资产安全缺陷。提供完备丰富的风险评估报告，分级分析安全漏洞并提出相应加固修补建议方案。

#### 3.1. 扫描目标

添加目标：用户从【漏洞扫描】进入“扫描目标”界面，点击左上角“添加目标”按钮，在弹窗中输入目标 IP 或域名，选择主机漏洞扫描或者 Web 漏洞扫描后点击保存。

开始扫描：选择具体某一目标可执行扫描操作。





### 3.2. 扫描任务

展示所有的扫描任务信息，能直观的查看每一次扫描的状态及漏洞信息。

漏洞详情：点击目标地址，可查看本次扫描的详细漏洞信息。

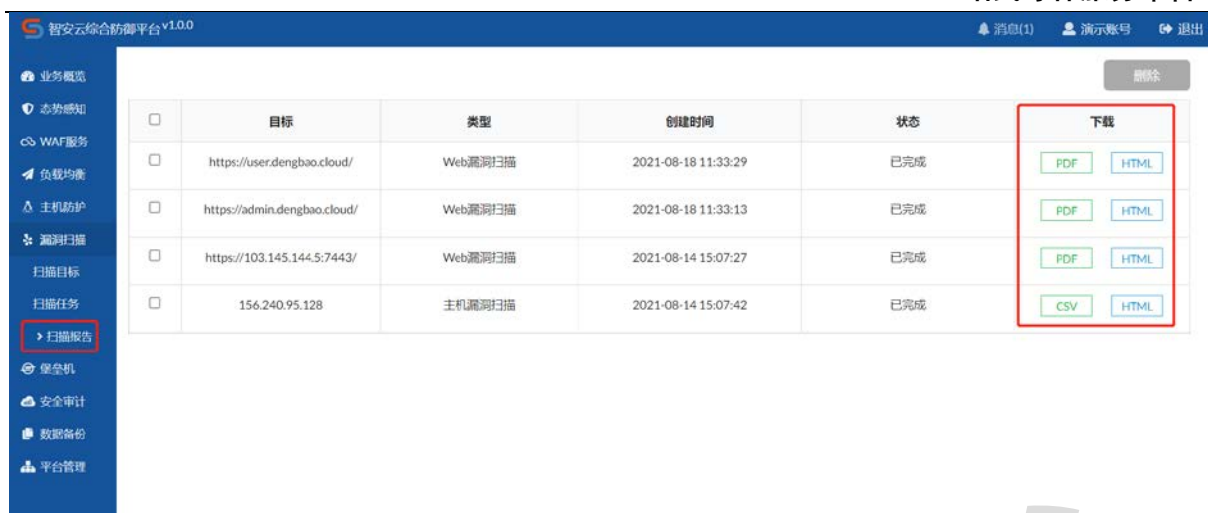
生成报告：针对已扫描完成的任务，可点击生成报告按钮预生成扫描报告。



### 3.3. 扫描报告

展示所有创建的扫描任务报告，可将报告下载到本地。





## 4. 堡垒机

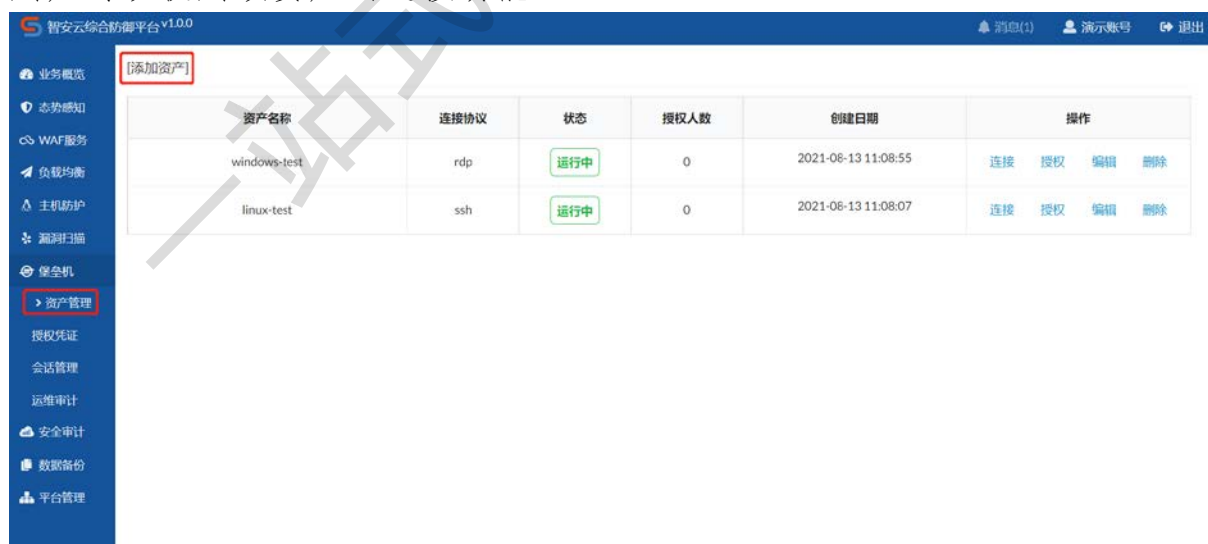
堡垒机模块提供远程运维管理所需要的集中身份认证、集中访问控制、集中操作审计等功能。

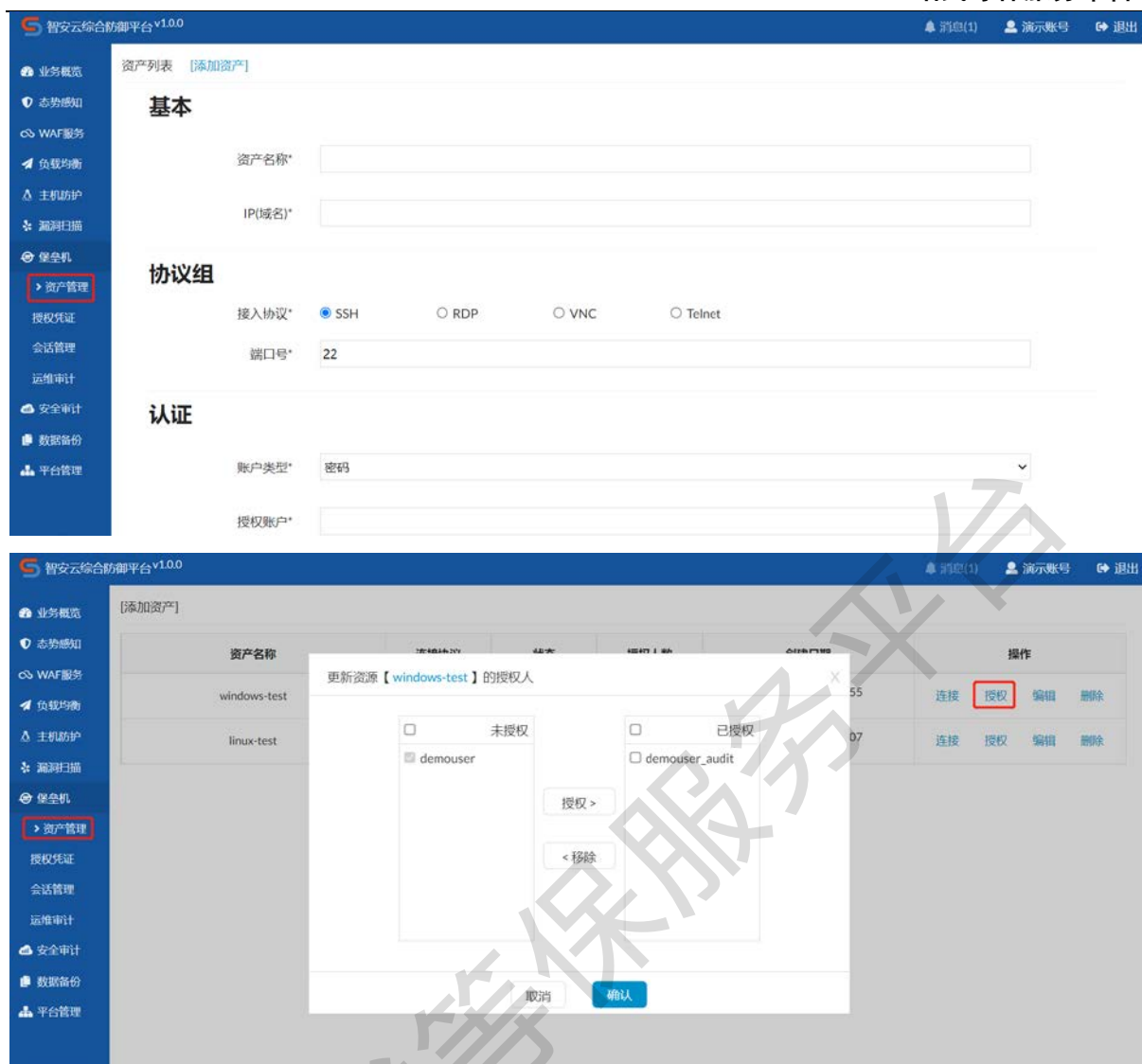
### 4.1. 资产管理

添加资产：添加需要通过堡垒机集中管控的主机资产。

连接资产：点击连接按钮，可以连接到对应服务器，执行运维操作。

授权：点击授权按钮，将当前资产授权给其他用户。成功授权后，其他用户可以使用该资产的连接功能。

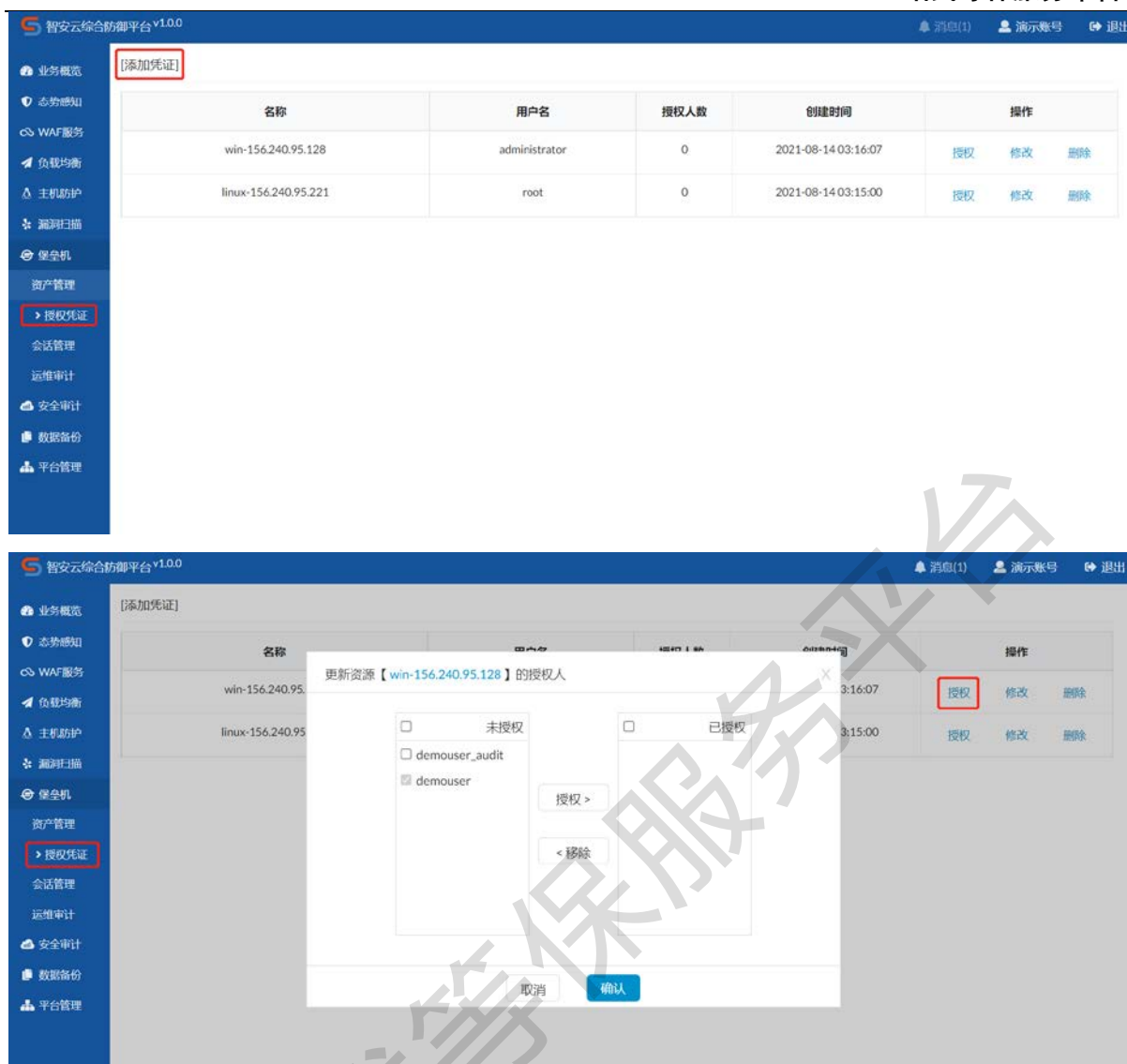




## 4.2. 授权凭证

添加凭证：添加需要集中管控的主机凭证信息。

授权：点击授权按钮，将相关凭证授权给其他用户，成功授权后，其他用户可在添加主机资产时使用该凭证。

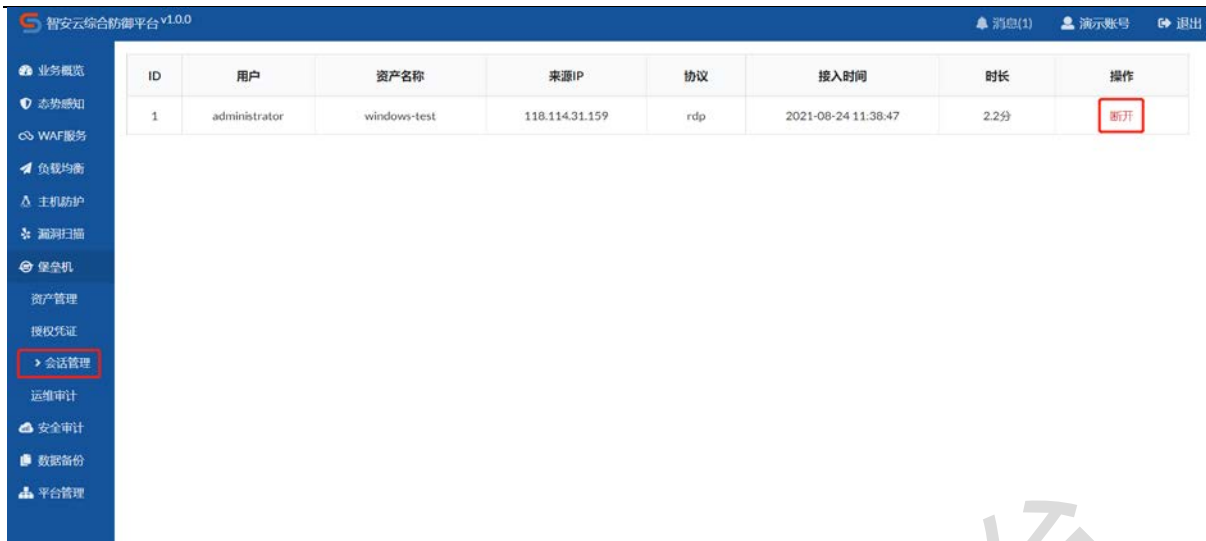


### 4.3. 会话管理

展示当前正在连接中的主机资产。

断开连接：点击断开，可以强制关闭本次会话连接。

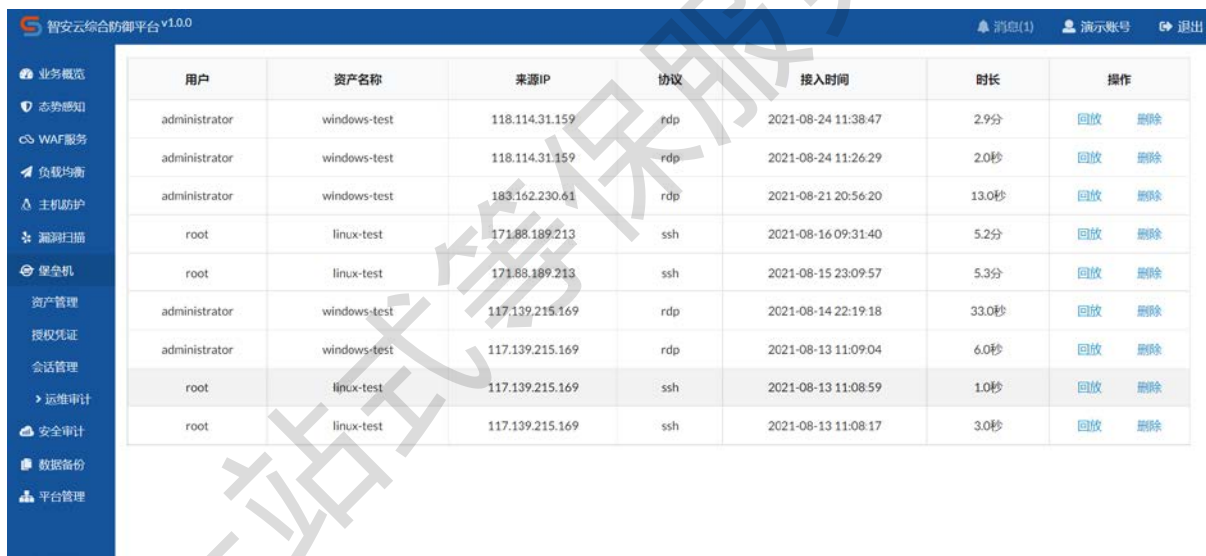




#### 4.4. 运维审计

展示所有已经结束连接的会话信息。

回放：点击回放按钮，可以查看该会话的操作录像。



#### 5. 安全审计

安全审计模块主要包含数据库安全审计、主机安全审计和应用安全审计，满足网络安全等级保护要求。

数据库安全审计：针对数据库的各种操作和行为进行审计。能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规

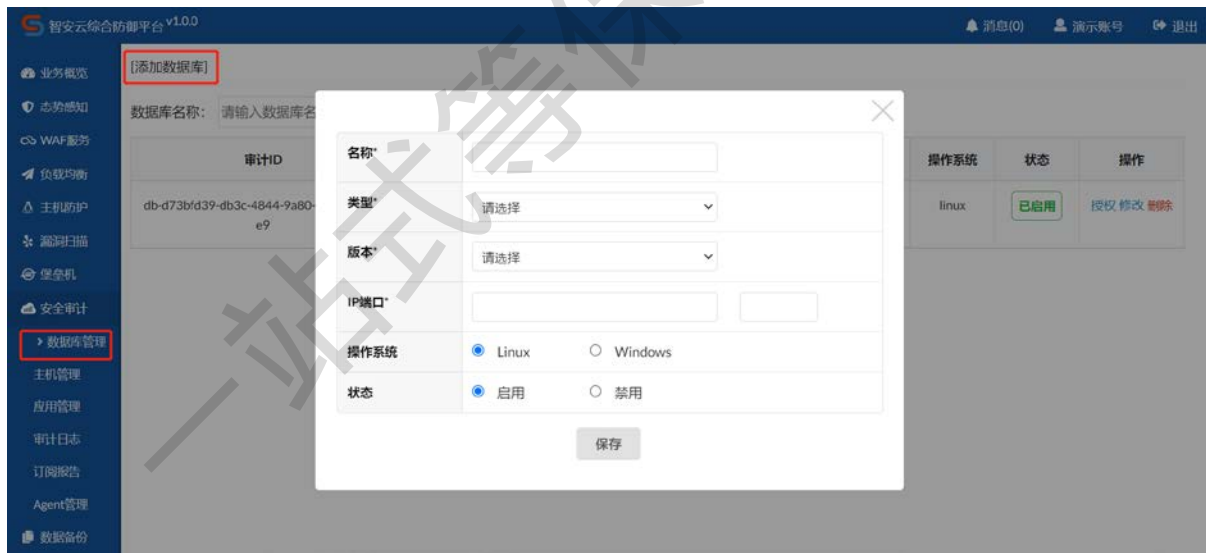
报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

**主机安全审计：**针对主机的各种操作和行为进行审计。根据信息系统的统一安全策略，实现集中审计。审计范围覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；

**应用安全审计：**针对应用系统的各种操作和行为进行审计。根据系统统一安全策略，提供集中审计，提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

## 5.1. 数据库管理

**添加资产：**添加需要被审计的数据库资产，选择对应的数据库类型、版本及操作系统，并填写数据库 IP 和端口信息。



**授权：**点击授权按钮，将数据库资产授权给其他用户，其他用户可以查看该数据库的日志信息

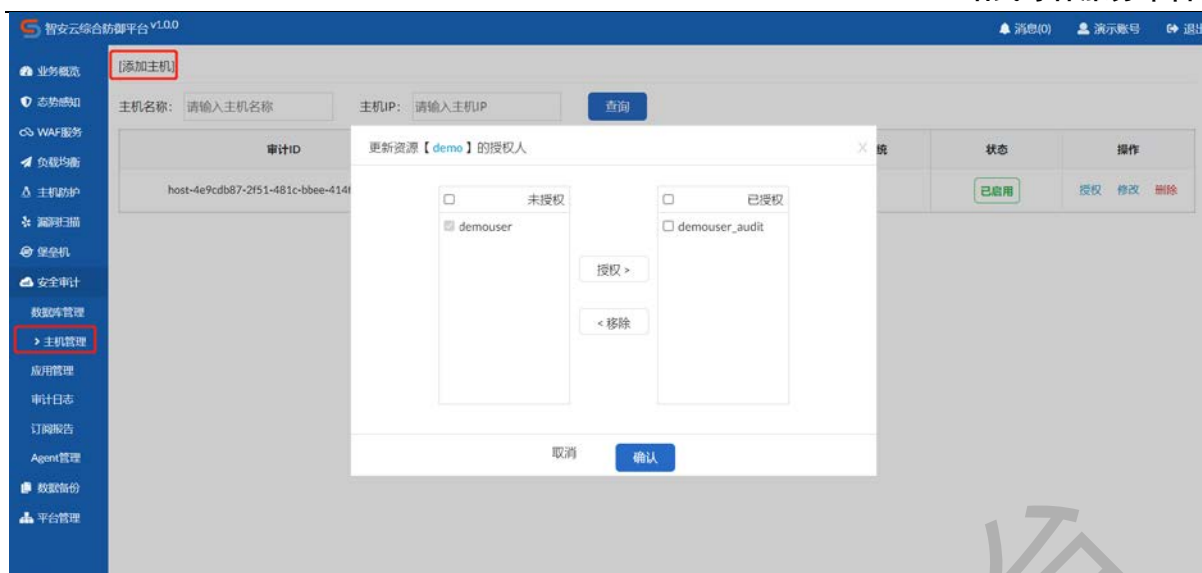


## 5.2. 主机管理

添加资产：添加需要被审计的主机资产，选择操作系统，并填写主机 IP 信息。



授权：点击授权按钮，将主机资产授权给其他用户，其他用户可以查看该主机的日志信息

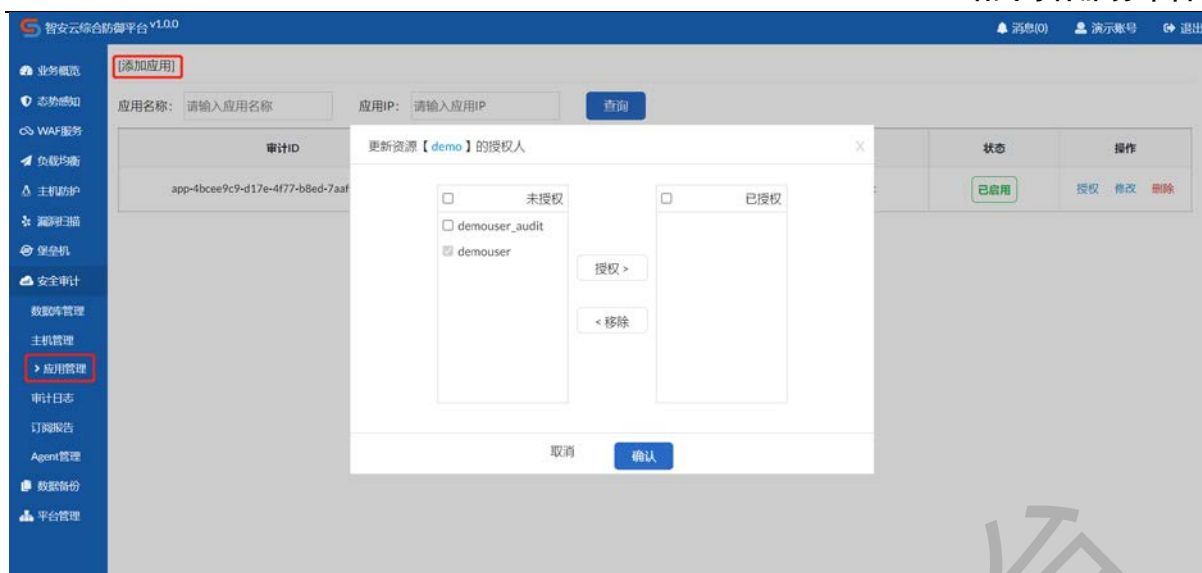


### 5.3. 应用管理

添加资产：添加需要被审计的应用资产，选择应用类型，并填写应用IP信息。



授权：点击授权按钮，将应用资产授权给其他用户，其他用户可以查看该应用的日志信息



## 5.4. 审计日志

展示数据库、主机、应用等资产的日志信息，支持多条件筛选，日志可存储 180 天。

导出：点击导出按钮，可将当前日志数据导出为 Excel 表格。



## 5.5. 订阅报告

添加任务：创建报告订阅任务，系统支持日报、周报、月报三种周期的报告，可填写多个收件人邮箱，可选择具体某一个资产或全部资产的日志信息用于生成报告。



## 5.6. Agent 管理

可在此页面下载审计系统部署文档，按照部署文档操作，完成在资产服务器上的相关审计配置。



## 6. 数据备份

可上传或下载自己的数据、配置等文件。

## 7. 平台管理

### 7.1. 子账号管理

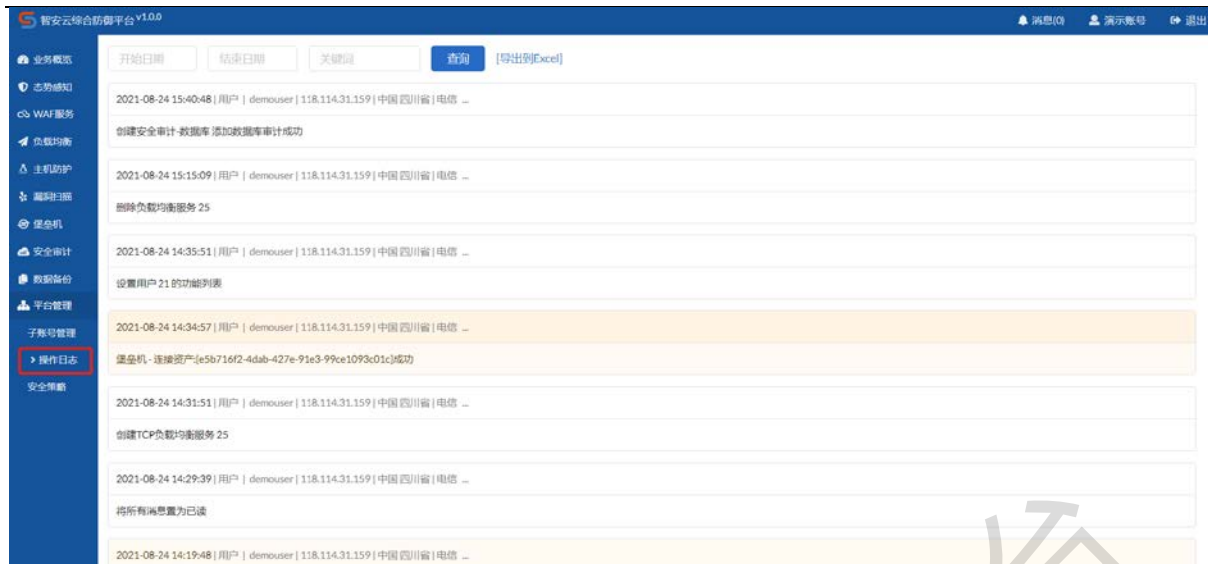
创建子账号：点击创建按钮，在弹窗中填写需要新增的子账号信息。

分配权限：点击详情按钮，在权限模块中可以分配给子账号相应的功能权限



## 7.2. 操作日志

查看用户及其所有子账号的平台操作日志，并支持导出功能。



### 7.3. 安全策略

安全策略：展示系统当前的密码复杂度策略以及登录安全策略。



访问设置：用户可以添加系统访问的 IP 白名单。



