云等保专区使用手册

天翼云科技有限公司

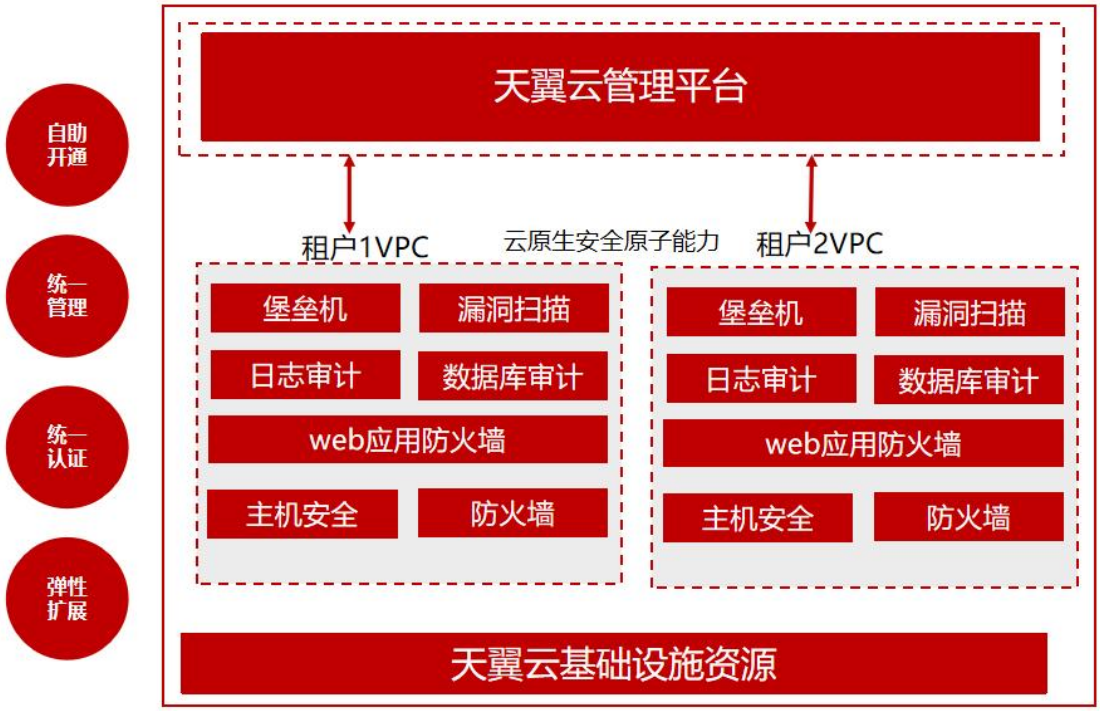
目录

1. 产品介绍

1.1. 产品定义

云等保专区是满足等保合规 2.0 云原生安全合规平台。云等保专区提供安全统一管理、传输安全、计算环境安全等安全合规能力，实现统一管理、统一运营，整体上降低等保建设难度和日常管理运营复杂度。本产品为满足等保合规，提供一揽子安全原子能力，实现安全原子能力统一管理、统一运营包含，为客户侧等保合规需求提供便捷下单，自动化部署的能力，共包含 7 款原子能力：主机安全、Web 应用防火墙、下一代防火墙、堡垒机、漏洞扫描、日志审计、数据库审计。

1.2. 产品架构



1.3. 产品优势

云等保专区利用自研云原生安全运营平台纳管生态层安全原子能力，提供：

1. 安全合规：遵照等保 2.0 要求，结合云平台业务特性设计，满足合规要求。

2. 按需交付：为不同的云使用者提供适合自身业务需求的安全能力。
3. 统一管理：实现云管以及安全管理平台的统一，避免用户使用多重管理界面，降低安全运维管理压力。
4. 一站式等保：提供多种不同厂商丰富的云安全原子能力，满足租户等保合规诉求，一站式等保合规。
5. 满足 XC 要求：云等保专区方案全面适配 XC 环境，兼容主流的芯片和操作系统，实现一云多芯的安全服务能力。

1.4. 功能特性

(1) **主机安全：**为云服务器提供基于客户端的防护，提供主机系统防护与加固、主机网络防护与加固等功能，具备业界领先的勒索专防专杀、网页防篡改、网络隔离与防护、补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力,帮您快速发现网站潜在安全隐患。

(2) **Web 应用防火墙：**精准覆盖各类 Web 应用攻击，为客户识别恶意请求，防御未知威胁，分钟级接入实现防入侵、防扫描、防攻击、防数据泄露、防 CC 等攻击防护，等保必备

(3) **下一代防火墙：**提供云上互联网边界和 VPC 边界的防护，包括：实时入侵检测与防御、全局统一访问控制、全流量分析可是胡、日志审计与溯源分析

(4) **堡垒机：**4A 统一安全管控平台，为企业提供集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体的运维管理服务。

(5) **漏洞扫描：**能够对 Web 应用的资产进行识别分类以及对 Web 应用进行深度弱点探测。通过漏洞产生的原理和渗透测试的方法，快速分析出被测目标所开放的端口服务和对应的协议信息，发现资产暴露面。漏洞库覆盖国内外常见 CMS、中间件、操作系统等严重漏洞，帮助用户全面分析 Web 应用网络环境中存在的安全弱点。

(6) **日志审计：**通过主被动结合的方式，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储（可根据日志规模大小进行分布式存储，支持水平弹性扩展和数据高可靠性存储）、索引、

备份、全文检索、实时搜索、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。

(7) **数据库审计：**通过 Agent 抓包方式旁路部署，提供数据库审计，SQL 注入攻击检测，风险操作识别等功能，保障云上数据库的安全。

1.5. 应用场景

本产品适用于天翼云上的租户，通过勾选各个不同的安全组件对天翼云上租户的业务提供不同的网络安全能力，结合内置的等保二级、三级套餐，能够帮助用户通过等保二级、三级测评，满足等保合规要求。

1.6. 产品规格

产品名称	规格	说明	单位
堡垒机	标准版	支持 20 资产管理	套
	高级版	支持 100 资产管理	套
	企业版	支持 500 资产管理	套
数据库审计	标准版	支持 4 数据库实例	套
	高级版	支持 8 数据库实例	套
	企业版	支持 16 数据库实例	套
漏洞扫描	标准版	支持 20 个并发 IP 地址	套
	高级版	支持 50 个并发 IP 地址	套
	企业版	支持 100 个并发 IP 地址	套
日志审计	标准版	支持 20 个日志源	套
	高级版	支持 100 个日志源	套
	企业版	支持 500 个日志源	套
下一代防火墙	标准版	支持 1Gbps	套
	高级版	支持 2Gbps	套
	企业版	支持 4Gbps	套
主机安全	标准版	支持 1 个主机	套

	网页防篡改版	支持 1 个主机，提供主机网页防篡改功能	套
Web 应用防火墙	标准版	防护 10 个站点	套
	域名扩展包	每个扩展包支持 10 个域名防护；	套
	带宽扩展包	单个防护带宽扩展包，每个扩展包规格 50MB，可叠加，单个 web 应用防火墙最大可支持 20 个扩展包，最大支持扩展流量 1000MB；	套

1.7. 术语解释

术语	说明
cURL	cURL 是一个利用 URL 语法在命令行下工作的文件传输工具，可用于检测系统是否可以访问目标站点。
Dig	Dig 是一个在类 Unix 命令行模式下查询 DNS 信息（包括 NS 记录，A 记录，MX 记录等）的工具。
基线核查	基线核查是指对主机操作系统、数据库、软件和容器的配置进行安全检测，并提供检测结果说明和加固建议。基线核查可以帮您进行系统安全加固，降低入侵风险并满足安全合规要求。
漏洞扫描	漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。
引擎	本文的“引擎”为扫描核心技术，即最终进行漏洞扫描工作的服务。
资产	即扫描器所扫描的主机、数据库、网站等。
DDoS	分布式拒绝服务攻击(Distributed Denial of Service Attack，简称 DDoS)是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施

术语	说明
	攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击，其中的攻击者可以有多个。
EDR	端点检测与响应（Endpoint Detection & Response，EDR）是一种主动的安全方法，可以实时监控端点，并搜索渗透到防御系统中的威胁。EDR 是一种新兴的技术，可以更好地了解端点上发生的事情，提供关于攻击的上下文和详细信息。
认证	是一种信用保证形式。按照国际标准化组织（ISO）和国际电工委员会（IEC）的定义，是指由国家认可的认证机构证明一个组织的产品、服务、管理体系符合相关标准、技术规范（TS）或其强制性要求的合格评定活动。
虚拟机	虚拟机（Virtual Machine）指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。在计算机中创建虚拟机时，需要将实体机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟机都有独立的 CMOS、硬盘和操作系统，可以像使用实体机一样对虚拟机进行操作。
AES	密码学中的高级加密标准（Advanced Encryption Standard，AES），又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES（Data Encryption Standard），已经被多方分析且广为全世界所使用。
Apache	Apache 是一款 Web 服务器软件。它可以运行在几乎所有广泛使用的计算机平台上，由于其跨平台和安全性被广泛使用，是最流行的 Web 服务器端软件之一。
CC 攻击	CC 攻击（Challenge Collapsar Attack，挑战黑洞攻击）是 DDoS 攻击的一种类型，使用代理服务器向受害服务器发送大量假冒合法的请求，造成被攻击服务器资源耗尽，一直到宕机崩溃。
DDoS	分布式拒绝服务攻击（Distributed Denial of Service Attack，简称 DDoS）是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时

术语	说明
	实施攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击，其中的攻击者可以有多个。
DES	DES 全称为 Data Encryption Standard，即数据加密标准，是一种使用密钥加密的块算法，1977 年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），并授权在非密级政府通信中使用，随后该算法在国际上广泛流传开来。
HA	高可靠性（High Availability，简称 HA）能够在通信线路或设备发生故障时提供备用方案，防止由于单个产品故障或链路故障导致网络中断，保证网络服务的连续性。
LACP	LACP（Link Aggregation Control Protocol，链路聚合控制协议）是一种基于 IEEE802.3ad 标准的协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）与对端交互信息。链路聚合往往用在两个重要节点或繁忙节点之间，既能增加互联带宽，又提供了连接的可靠性。
LDAP	LDAP 是轻量目录访问协议（Lightweight Directory Access Protocol）的缩写，是互联网上目录服务的通用访问协议。LDAP 服务可以有效解决众多网络服务的用户账户问题，LDAP 服务器是用于查询和更新 LDAP 目录的服务器，包括用户账号目录。
MTU	最大传输单元（Maximum Transmission Unit，MTU）用来通知对方所能接受数据服务单元的最大尺寸，说明发送方能够接受的有效载荷大小。
SSL	SSL(Secure Sockets Layer，安全套接字协议)及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS 与 SSL 在传输层与应用层之间对网络连接进行加密。
VRRP	虚拟路由冗余协议（Virtual Router Redundancy Protocol，简称 VRRP）是由 IETF 提出的解决局域网中配置静态网关出现单点失效现象的路由协议，它是一种路由容错协议，也可以叫做备份路由协议。

术语	说明
WebShell	Webshell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将 asp 或 php 后门文件与网站服务器 Web 目录下正常的网页文件混在一起，然后就可以使用浏览器来访问 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的。
Kafka	Kafka 是一种高吞吐量的分布式发布订阅消息系统，可以处理消费者规模的网站中所有动作流数据。这些数据通常由于吞吐量要求而通过处理日志和日志聚合来解决。
SNMP	SNMP 是简单网络管理协议（Simple Network Management Protocol）的简称，是标准 IP 网络管理协议，支持目前主流的网络管理系统。
SQL	SQL 是结构化查询语言（Structured Query Language）的简称，是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统；同时也是数据库脚本文件的扩展名。
Syslog	Syslog 是一种行业标准的协议，可用来记录设备的日志。Syslog 日志消息既可以记录在本地文件中，也可以通过网络发送到接收 Syslog 的服务器。服务器可以对多个设备的 Syslog 消息进行统一的存储，或者解析其中的内容做相应的处理。常见的应用场景是网络管理工具、安全管理系统、日志审计系统。

2. 计费说明

2.1. 计费模式

产品采用包周期计费模式，用户按指定的周期方式来使用产品，如用户可按年的周期方式来订购，订购周期为 1 年，续订周期为 1 年。

2.2. 如何购买云等保专区

(1) 登录天翼云官网（https://www.ctyun.cn），点击天翼云云等保专区产品详情页。

(2) 单击【立即开通】，进入到天翼云云等保专区产品购买页面。

(3) 选择购买区域，主套餐规格和资源扩展包购买数量、以及购买时长。

(4) 阅读《天翼云云等保专区服务协议》后，勾选我已阅理解并接受，即可点击“立即开通”下单。

等保体系	等保测评项	安全产品名称	等保二级套餐	等保三级套餐
安全通信网络	应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段	下一代防火墙	√	√
安全区域边界	应具有提供访问控制、边界防护、入侵防范等安全机制	Web 应用防火墙	√	√
安全计算环境	应启用安全审计功能，数据进行安全审计	日志审计	√	√
		数据库审计		√
	应对用户进行身份鉴别、访问控制、运维审计	堡垒机	√	√
	应能发现已知	漏洞扫描		√

	漏洞，并在经过充分测试评估后，及时修补漏洞	主机安全	√	√

2.3. 续订

该产品支持续订，续订周期 1 年起。

2.4. 退订

该产品自新购 5 天内，支持每年 10 次 5 天无理由退订，超过 5 天的退订需要收取手续费。

2.5. 升级与扩容

当前不支持升级与扩容。

3. 用户指南

3.1. 资源管理

登录天翼云控制中心，点击云等保专区即可进入云等保专区产品的控制中心，在控制中心能够进行资源总览，通过资源总览能够看到当前已经形成的订单情况，每个订单可以点击展开，展示该订单关联的所有已经购买的安全组件，点击各个安全组件会弹出安全组件建设详情，包括订单状态生效中、即将过期、已过期、资源已释放，同时用户可以根据针对订单以及自身建设需求对于安全组件进行资源管理，包括续订、退订等操作。

3.2. 主机安全

主机安全（简称“EDR”或“EDR”）是一款集成了丰富的系统防护与加固、网络防护与加固等功能的主机安全产品。EDR 通过自主研发的文件诱饵引擎，有着业界领先的勒索专防专杀能力；能通过内核级东西向流量隔离技术，实现网络隔离与防护；并拥有补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。

EDR 具有以下功能模块：

(1) 防御已知和未知类型勒索病毒

EDR 不仅可以阻止已知勒索病毒的执行，而且面对传统杀毒软件束手无策的未知类型勒索病毒时，EDR 采用诱饵引擎，在未知类型勒索病毒试图加密时发现并阻断加密行为，有效守护主机安全。

(2) 防御高级威胁全流程攻击

EDR 根据 ATT&CK 理论，对攻防对抗的各个阶段进行防护，包括单机扩展、隧道搭建、内网探测、远控持久化、痕迹清除。不仅可以做到威胁攻击审计，而且还可以防止黑客进行渗透攻击，实现攻防对抗 360 度防御。

(3) 管控全局终端安全态势

服务器、PC 和虚拟机等终端安装了客户端软件后，上传资产指纹、病毒木马、高危漏洞、违规外联、安全配置等威胁信息到管理控制中心。用户在管理控制中心可以看到所有安装了客户端软件的主机及安全态势，并进行统一任务下发，策略配置。

(4) 全方位的主机防护体系

EDR 不仅包含传统杀毒软件的病毒查杀、漏洞管理、性能监控功能，在系统防护方面还可做到主动防御、系统登录防护、系统进程防护、文件监控，还支持网络防护、Web 应用防护、勒索挖矿防御、外设管理等多个功能点。

(5) 流量可视化，安全可见

EDR 通过流量画像的流量全景图，展示内网所有流量和主机间通信关系，梳理通信逻辑，以全局视角对策略进行规划，便于用户第一时间发现威胁，一键清除威胁。

(6) 简单配置，离线升级，补丁管理

EDR 支持用户自主进行安全配置，能够明确、有效的进行主机防护。主程序、病毒库、漏洞库、补丁库、Web 后门库、违规外联黑名单库全部支持离线导入升级包、一键自动升级，可在专网使用。

了解更多主机安全相关操作内容，请下载阅读《主机安全使用手册-云等保专区.docx》

3.3. Web 应用防火墙

web 应用防火墙具备专业的 Web 应用安全防护能力，可拦截针对网站的各类攻击行为，帮助用户应对网站运营中的安全风险，为 Web 应用提供全方位的防护，构建覆盖全生命周期的 Web 应用安全防护解决方案，功能主要如下：

功能	描述
防护对象	多链路数据防护，网段数量不限。 以域名和 IP 方式进行防护。 IPv4/IPv6 双协议栈。
攻击防护	注入类攻击：SQL 注入、代码注入、命令注入、LDAP 注入、文件注入、SSI 注入等。 跨站脚本攻击：XSS。 通用攻击：HTTP 请求走私、HTTP 响应分割、Session-Fixation 等。 恶意软件：代码上传、Webshell 后门、其他木马等。 信息泄露：目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露、敏感文件信息泄漏、其他信息泄漏。 扫描工具：阻断 Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan、N-Stealth、Acunetix Web Vulnerability Scanner 等多种扫描器的扫描行为。 爬虫攻击：恶意网络爬虫，百度、Google、Yahoo 等搜索引擎爬虫。 第三方组件漏洞：Web 容器漏洞、开源 CMS 漏洞、Web 服务器插件

功能	描述
	漏洞。 HTTP 协议规范性：协议违规、报头缺失、HTTP 方法限制、畸形请求、文件限制、头部长度限制。 其他：CC 攻击、防敏感词发布、敏感信息隐藏、防盗链、Cookie 防篡改/防劫持。
高级防护	智能语义分析：内置 SQL 注入、XSS 语义分析安全规则。 机器学习：内置机器学习安全引擎，对用户 Web 业务系统建立安全的访问模型，学习内容包括 URL、参数、参数类型、参数长度、匹配频率等。 地图区域访问控制：在地图上指定某一地理区域进行访问控制，阻断此区域 IP 的访问。 服务器隐藏：可删除服务器响应头信息。 自定义规则：对 HTTP 请求中 URI、HOST、参数、参数名、请求头、Cookie、版本号、方法和请求体及 HTTP 响应的响应体等条件自定义正则，支持多种组合条件。 智能攻击者锁定：智能识别攻击者，对发起攻击的 IP 地址自动锁定禁止访问被攻击的网站。 威胁情报：云端威胁情报联动，主动发现僵尸 IP、代理 IP、扫描 IP、黑产 IP、C&C 等恶意 IP 发起的访问行为，实时统计威胁情报攻击类型占比和攻击频率。 云端高防联动：一键开启防护，L3-L7 DDoS 安全防护，最高可提供 1TB 抗 DDoS 服务。
应用交付	HTML、TXT、JPG、DOC 等静态文件缓存，响应内容 gzip 算法压缩，识别压缩的响应内容。
高可靠性	链路聚合提升网络带宽、增加容错性和链路负载均衡。 VLAN 子接口，业务口可承载多个 VLAN 通道。 主-主模式、主-备模式。 硬件 BYPASS（即物理直通）。

功能	描述
	软件 BYPASS（即过载 BYPASS）。
SSL 防护	支持第三方认证机构颁发的证书链，实现 HTTPS 应用系统的防御。 可选择 SSL/TLS 协议版本。 部署在 SSL 网关后可解析到真实的访问者 IP，对真实的 IP 进行防护和阻断。 内置 SSL 加速卡提高设备 HTTPS 处理性能。
审计	记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容、cookie 等所有请求头内容。 记录服务器响应头信息、响应内容。 分析访问量最大的 URL、IP 地址、文件类型等。

了解更多 web 应用防火墙相关操作内容，请下载阅读《Web 应用防火墙使用手册-云等保专区.docx》

3.4. 下一代防火墙

下一代防火墙能够提供应用层防火墙、入侵防护、防病毒、反 APT、DOS 防护、内容过滤、URL 过滤、智能带宽管理、上网行为管控与审计等多重安全特性；同时，它全面适配云环境，支持主流的公有云、私有云及虚拟化平台；全特性支持 RESTful API，具备高效的协同联动能力，能够提供立体化防护能力。

了解更多下一代防火墙相关操作内容，请下载阅读《下一代防火墙使用手册-云等保专区.docx》

3.5. 堡垒机

堡垒机具备统一安全管理与审计能力，提供集身份认证（Authentication）、帐户管理（Account）、控制权限（Authorization）、日志审计（Audit）功能于一体。支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议

的安全监控与历史查询，具备全方位运维风险控制能力，可满足各类法律法规（如等级保护、赛班斯法案 SOX、PCI、企业内控管理、分级保护、ISO/IEC 27001 等）对运维审计的要求。

功能	描述
认证&授权	
双因子认证	内置手机 APP 认证（谷歌动态口令验证）、OTP 动态令牌、USBkey 双因素认证引擎。 提供短信认证、AD、LDAP、RADIUS 认证接口。 支持多种认证方式组合。
权限管理	系统预置多种用户角色：超级管理员、部门管理员、运维管理员、审计管理员、运维员、审计员、系统管理员和密码管理员。每种用户角色的权限均不同，且可自定义用户角色。
集中授权	梳理用户与主机之间关系，提供一对一、一对多、多对一、多对多的灵活授权模式。
单点登录	托管主机的帐户和密码，运维人员直接点击<登录>即可成功自动登录到目标主机中进行运维操作，无需输入主机的帐户和密码。
自动学习	运维人员通过堡垒机成功登录目标主机后即可自动录入主机信息，减轻管理员配置主机信息、用户与主机关系的工作量。
运维&审计	
运维协议支持	支持管理 Linux/Unix 服务器、Windows 服务器、网络设备（如思科/H3C/华为等）、文件服务器、Web 系统、数据库服务器、虚拟服务器、远程管理服务器等。 兼容 Xshell、XFTP、SecureCRT、MSTSC、VNC Viewer、PuTTY、WinSCP、FlashFXP、SecureFX 等多种客户端工具。
统一审计	对所有操作进行详细记录，提供综合查询；审计日志可在线或离线播放，自动备份归档。 审计内容包括图形、字符、文件、应用、SQL 语句等会话及应用会话。

功能	描述
浏览器客户端运维	基于 H5 技术实现浏览器客户端运维，无需安装本地工具，直接通过浏览器打开运维界面。 支持通过 SSH、Telnet、Rlogin、RDP、VNC 协议的 Web 客户端运维。
文件传输审计	记录所有操作会话，包括在线监控、实时阻断、日志回放、起止时间、来源用户、来源 IP、目标设备、协议/应用类型、命令记录、操作内容。 完整备份传输文件，为上传恶意文件、拖库、窃取数据等危险行为提供查询依据。
自动运维	实现自动化的运维任务并将执行结果通知相关人员。
资产管理	支持主机、主机组、混合云、帐号、帐号组、应用等多种资产类型。
命令控制	集中命令控制基于不同主机、不同用户设置不同的命令控制策略，包括命令阻断、命令黑名单、命令白名单、命令审核四种动作。
工单流程	运维人员向管理员申请需要访问的设备，选择条件包括设备 IP、设备帐户、运维有效期、备注事由等，运维工单以邮件方式通知管理员。
其他	
系统自审	对系统自身变化信息进行审计，形成系统分析报表。
冗余架构	结合端口聚合技术、RAID 技术和 HA 技术，实现三重冗余备份的高可用架构。
API 接口	提供用户、资产、授权的增删改查等 API 接口。 允许第三方平台调用 API 接口，实现用户、资产、权限自动同步。

了解更多堡垒机相关操作内容，请下载阅读《堡垒机使用手册-云等保专区.docx》

3.6. 漏洞扫描

漏洞扫描系统功能主要包含网站漏洞扫描、数据库漏洞扫描、基线核查、主机漏洞扫描、安全事件扫描五大扫描功能，以及统计报告控制体系、用户权限管理体系等辅助功能。

功能	描述
首页	
资产总量分布	统计资产总数及不同类型资产数目及占比。 统计主机风险资产、网站风险资产占比（风险等级非信息类资产）。
弱点总量分布	统计当前发现的所有弱点数及根据不同弱点类型统计弱点数目。
资产风险分布	从不同风险等级维度统计风险资产数量。
风险主机 TOP5	根据风险主机弱点数，列出风险数最多的 5 个主机资产。
风险网站 TOP5	根据风险网站的弱点数，列出风险数最多的 5 个网站资产。
主机资风险/服务分布	统计主机资产出现次数最多的 10 个弱点、漏洞风险、服务类型、端口。
网站资产风险/服务分布	统计网站资产出现次数最多的 10 个弱点、漏洞风险、服务类型。
弱点发现趋势	按时间展示弱点的趋势状态，弱点的数据包括所有扫描类型的数据（不包含信息类漏洞）。
资产管理	
资产列表	支持主机资产、网站资产两种类型。 支持新增、导入、导出、删除、编辑资产。 支持按照组织视角展示资产。
授权管理	支持主机授权信息管理。 支数据库授信息管理。
任务管理	
创建任务	支持创建通用任务、专项任务。

功能	描述
	通用任务支持主机扫描、网站扫描、数据库扫描、基线配置核查、事件内容。 专项任务支持弱口令扫描、存活主机探测、大数据漏洞扫描、物联网漏洞扫描、信创漏洞扫描。
任务列表	支持查看已下发的所有扫描任务，可对任务进行集中管理，包括查询任务、新增任务、执行任务等。
模板中心	
漏洞模板	支持主机策略、网站策略、数据库策略管理。 支持新增、编辑、另存为、删除、查看策略。 支持使用自定义策略下发扫描任务。
基线模板	支持工信部、公安部行业基线核查模板。 支持对应用程序、操作系统、网络设备、虚拟化设备、数据库五类资产的安全配置进行核查。 支持查看基线模板详情。
扫描参数	支持设置主机扫描、网站扫描高级参数模板。 可根据需要设置与恢复默认扫描参数配置。
字典模板	主机扫描和弱口令发现任务中引用的各协议弱口令字典。可自定义弱口令字典。
报告模板	根据不同任务类型，设置离线报告导出的内容。 支持设置主机扫描报告、网站扫描报告、数据库扫描报告、基线核查报告、事件内容报告。 支持系统默认模板及自定义报告内容模板。
端口列表	系统默认提供的端口列表模板。
报告管理	
报告管理	支持对已扫描完成的任务导出离线报告。 支持对已导出报告进行下载。
系统管理	
用户管理	支持角色管理及用户管理。

功能	描述
	支持新增角色、编辑角色、删除角色。 支持新增用户，并指定用户角色。
系统设置	提供系统服务、升级、数据备份等管理功能。 支持在线升级和离线升级。 支持系统 SSH 服务开启、系统重启、系统关闭、网卡重启操作。 支持设置系统时间。 支持根据需要备份系统数据。
配置管理	提供网络配置、安全配置、告警配置、版权配置功能。 支持网卡设置、路由配置、DNS 配置、网关配置。 支持密码安全复杂度、登录安全设置、超时设置、磁盘告警设置、多因子认证设置。 支持验证码登录、认证证书登录、用户名密码登录。
引擎管理	支持对系统各个引擎状态进行查看与监控。
常用工具	支持 Ping、Traceroute、Dig、Telnet、SSH、CURL、Nmap 命令工具。
许可管理	支持查看许可授权内容及更新许可。

了解更多漏洞扫描相关操作内容，请下载阅读《漏洞扫描使用手册-云等保专区.docx》

3.7. 日志审计

日志审计具备信息资产的综合性管理能力，通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件。为管理人员提供全局的视角，确保客户业务的不间断运营安全。通过采集网络资产设备上报的日志，实时监视网络各类操作行为及攻击信息。根据设置的规则，智能判断出各种风险行为，对风险行为进行报警。

功能	描述
全面日志采集	全面支持 Syslog、SNMP、OPSec、XML、FTP 及本地文件

功能	描述
	等协议，可以覆盖主流硬件设备、主机及应用，保障日志信息的全面收集。实现信息资产（网络设备、安全设备、主机、应用及数据库）的日志获取，并通过预置的解析规则实现日志的解析、过滤及聚合。同时可将收集的日志通过转发功能转发到其它网管平台。
大规模安全存储	内置 TB 级别存储设备，可以选配各种 RAID 级别进行数据冗余和安全保障。系统拥有多项自主知识产权的存储加密机制和查询机制，十分适合等保、密保等行业的应用要求。
智能关联分析	实现全维度、跨设备、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，可轻松实现各资产间的关联分析。
脆弱性管理	能够收集和管理来自各种 Web 漏洞扫描工具、主机漏洞扫描工具、网络漏洞扫描工具产生的扫描结果，并实时和用户资产收到的攻击危险进行风险三维关联分析。
数据挖掘和数据预测	支持对历史日志数据进行数据挖掘分析，发现日志和事件间的潜在关联关系，并对挖掘结果进行可视化展示。系统自带多种数据统计预测算法，可以根据历史数据的规律对未来的数据发生情况进行有效预测。
可视化展示	实现对信息资产的实时监控、信息资产与客户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。通过各种事件的归化处理，实现高性能的海量事件存储和检索优化功能，提供高速的事件检索能力。事后的合规性统计分析处理，可对数据进行二次挖掘分析。
分布式部署和管理	平台支持分布式部署，可以在中心平台管理规则、配置策略自动分发、远程自动升级等，极大地降低了分布式部署的难度，提高了可管理性。
灵活的可扩展性	提供多种定制接口，实现强大的二次开发能力以及与第

功能	描述
	三方平台对接和扩展的能力。

了解更多日志审计相关操作内容，请下载阅读《日志审计使用手册-云等保专区.docx》

3.8. 数据库审计

数据库审计是专业的数据库应用安全防护产品，帮助用户应对网站运营中的安全风险，为数据库应用提供全方位的防护，提供覆盖数据库使用全生命周期的安全防护解决方案。

产品功能分成原始信息收集、审计信息标准化、审计信息筛选、预警与报表四大模块。

(1) 原始信息收集

1. 通过旁路镜像的模式部署
2. 不改变用户现有网络结构
3. 不占用数据库服务器资源
4. 不影响数据库性能
5. 支持分布式部署
6. 实现配置与报表的集中管理
7. 并发流量采集与处理、多点存储、多级管理
8. 自动定期发现功能，及时发现未知数据库

(2) 审计信息标准化

支持国内外主流数据库，包括传统的数据库系统、大数据系统和 Web 系统等，具体支持的系统和版本如下表所示。

数据库分类	数据库系统	版本
关系型	Oracle	8i、9i、10g、11g、12c、18c、19c、21c
	MySQL	4.0、4.1、5.0、5.1、5.5、5.6、5.7、8.0
	SQL Server	2000、2005、2008、2012、2014、2016、2017、2019
	Sybase ASE	11.9、12.5

数据库分类	数据库系统	版本
	DB2	v80、v81、v82、v95、v97、v10.5、v11.1、v11.5
	Informix	IDS9
	Oscar	5.5、5.7
	达梦（DM）	DM7、DM8
	Cache	2010、2016
	PostgreSQL	9、10、11、12、13、14
	Teradata	所有版本
	人大金仓（Kingbase）	V6、V7、V8
	GBase	8.5a、8.8s
	MariaDB	5.1、5.2、5.3、5.5、10.0、10.1、10.2、10.3
	Hana	1.0、2.0
	GaussDB	100、200、300
	LibrA	6
	K-DB	11
	Sybase IQ	15.4
	TiDB	4.X、5.X
	Vertica	7、8、9、10、11
	OceanBase	2.X
	PolarDB	MySQL、PostgreSQL、兼容 Oracle 语法
	PolarDB-X	1.0/MySQL5、1.0/MySQL8、2.0/MySQL5.7
	AnalyticDB	MySQL、PostgreSQL
	TBase	V2
	HighGo	6.0
	TDSQL-C MySQL	5.7、8.0
	TDSQL-C	10、14

数据库分类	数据库系统	版本
	PostgreSQL	
非关系型	MongoDB	2.x、3.x、4.x、5.x
	HBase（protobuf）	所有版本
	HBase（thrift）	Thrift1、thrift2
	Hive	1.X、2.X、3.X
	Redis	所有版本
	Elasticsearch	所有版本
	Cassandra	3.X
	HDFS	所有版本
	Impala	3.X
	Graphbase	6
	Greenplum	5、6
	Spark SQL（thrift）	1.x、2.x
	Spark SQL（RESTful）	1.x、2.x
	SSDB	所有版本
	ArangoDB	3.4.9
	Neo4j	4.2.0
	OrientDB	3.1.6
大数据	HBase（protobuf）	所有版本
	HBase（thrift）	thrift1、thrift2
	Hive	1.X、2.X、3.X
	Cassandra	3.X
	HDFS	所有版本
	Impala	3.X

数据库分类	数据库系统	版本
	Graphbase	5、6
	Spark SQL（thrift）	1.x、2.x
	Spark SQL（RESTful）	1.x、2.x
	SSDB	所有版本
	MAX COMPUTE	所有版本
图形	Graphbase	6
	ArangoDB	3.4.9
	Neo4j	4.2.0
	OrientDB	3.1.6
全文检索	Elasticsearch	所有版本
文档	MongoDB	2.x、3.x、4.x、5.x
	ArangoDB	3.4.9
键值	Redis	所有版本
其他	HTTP	所有版本
	Telnet	所有版本
	FTP	所有版本
RDS	MySQL	5.5、5.6、5.7、8.0
	SQL Server	2008 R2 云盘版、2012 Web、2012 企业版 单机、2012 企业版、2012 标准版、2014 企业版、2014 标准版、2016 Web、2016 企业版、2016 标准版、2017 Web、2017 企业集群版、2017 标准版、2019 Web、2019 企业集群版、2019 标准版
	PostgreSQL	10、11、12、13、14

将不同数据库协议按照标准化的格式进行展示，方便管理人员阅读和分析。

(3) 审计信息筛选

1. 根据 5W1H（What、Where、When、Who、Why、How）分析模型进行规则设置，提供丰富的规则条件配置方法。
2. 内置 900 多条安全相关的审计分析规则。
3. 根据采集到的数据进行数据分析和产生行为模型。
4. 审计结果查询。

(4) 预警与报表

1. 提供 Syslog、短信、邮件、SNMP、钉钉、企业微信等告警通知方式，可第一时间通知管理人员。
2. 可与综合日志审计分析平台等进行日志的整合。
3. 内置 23 种高价值、符合法律法规的分析报表，可从数据库账号增删、密码修改、权限变更、高危操作、违规告警、账号复用、数据库性能分析等维度进行分析。
4. 提供自定义报表功能，可根据客户的业务需要，选择不同的维度和指标对审计数据进行统计和分析。

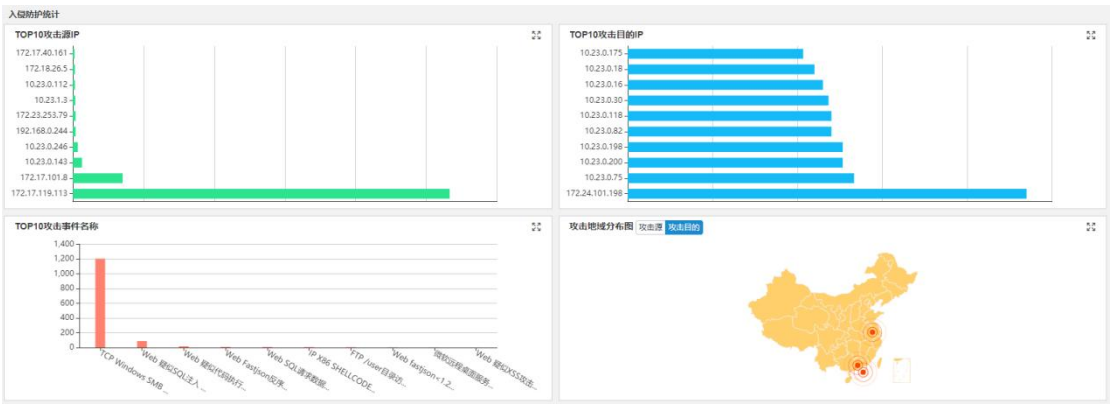
了解更多数据库审计相关操作内容，请下载阅读《数据库审计使用手册-云等保专区.docx》

4. 最佳实践

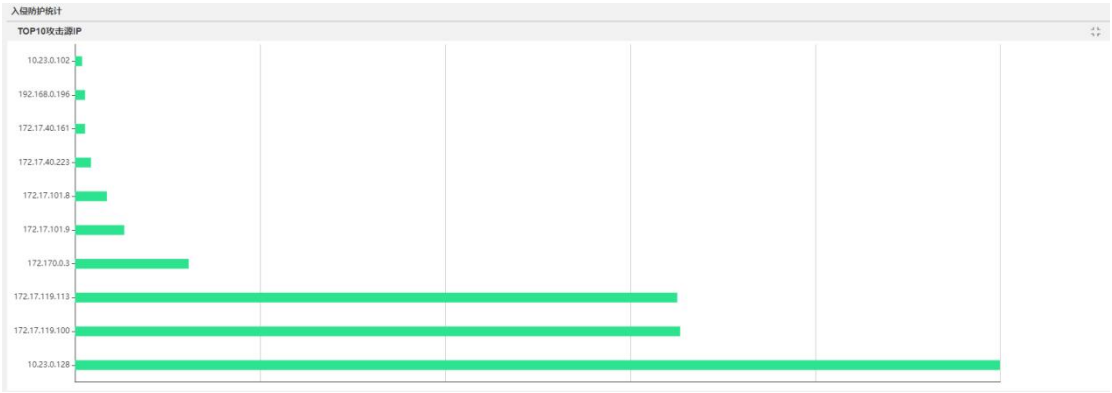
4.1. 快速掌握网络安全态势

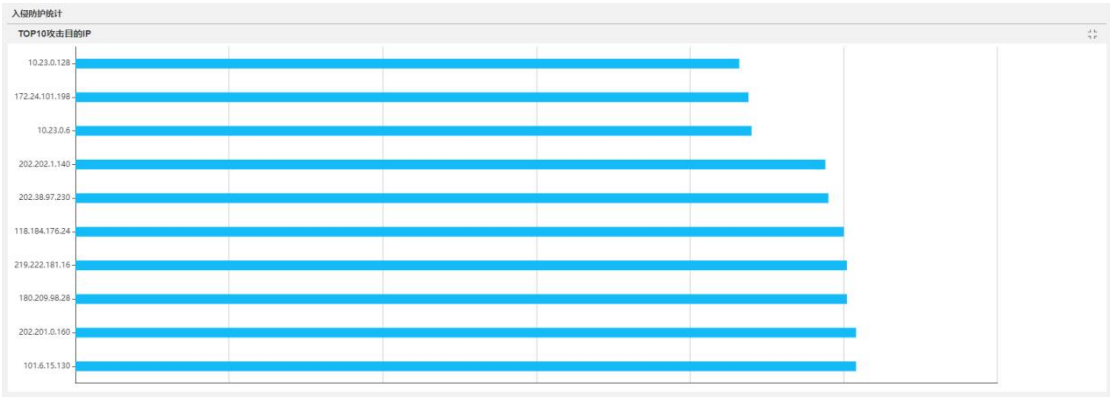
4.1.1. 入侵防护统计

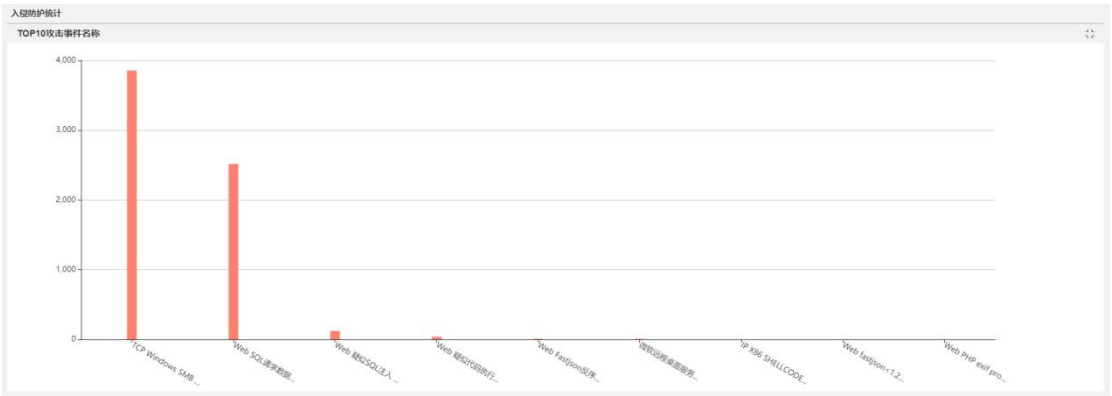
在系统菜单选择 “监控>安全分析>入侵防护统计”查看入侵防护统计。在入侵防护统计中统计排行前十的攻击源 IP、目的 IP、攻击事件名称，以及对攻击源和目的 IP 的所在地显示。



点击统计右上角的图标，能够放大显示选择的统计类型。

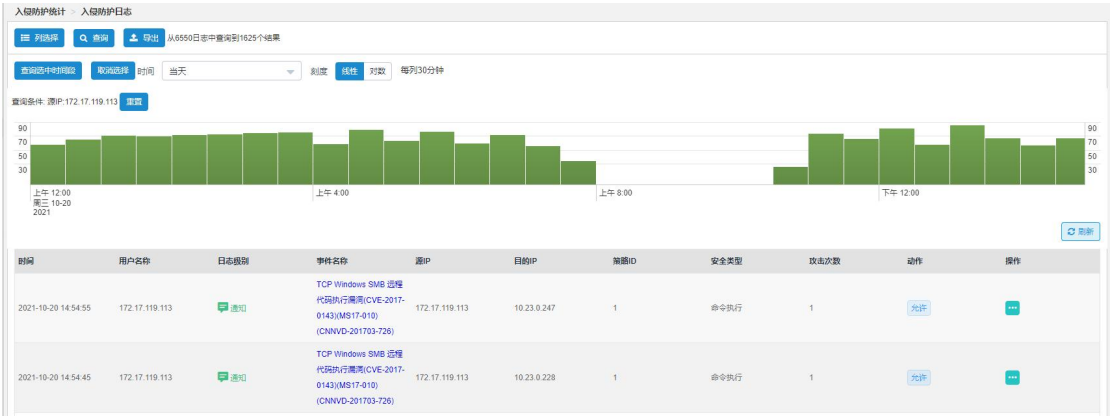






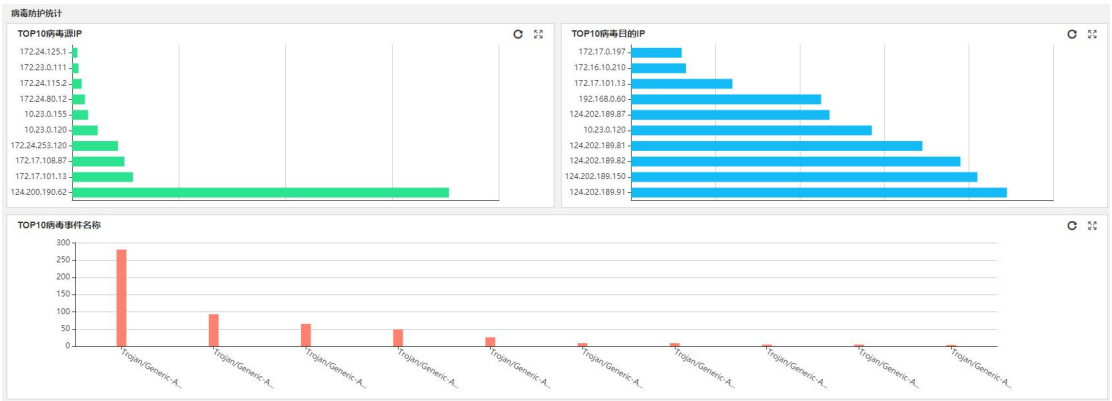
点击统计右上角的图标，能够返回整体显示统计页面。

点击统计显示的单个统计对象能够链接到入侵防护统计日志界面，并过滤出当前用户相关的日志详细内容。



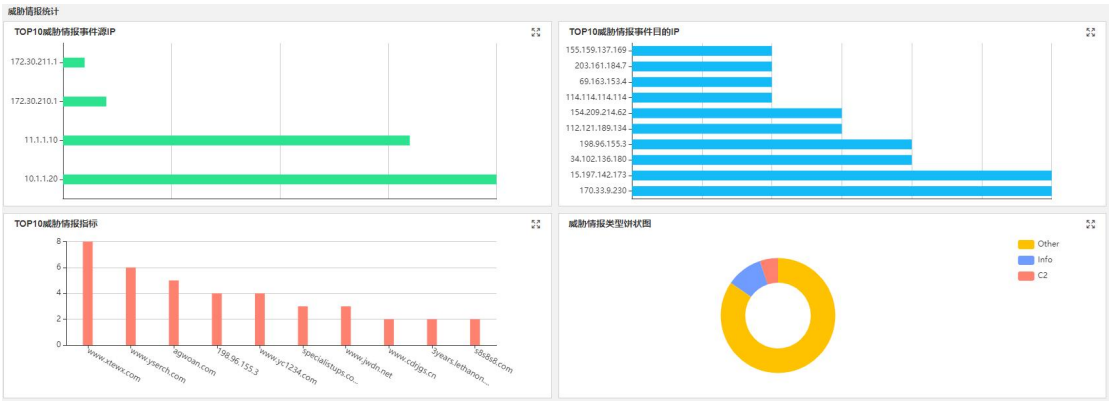
4.1.2. 病毒防护统计

在系统菜单栏点击“监控>安全分析>病毒防护统计”，进入病毒防护统计页面。分别列出了 TOP10 病毒源 IP、TOP10 病毒目的 IP、TOP10 病毒事件名称信息。

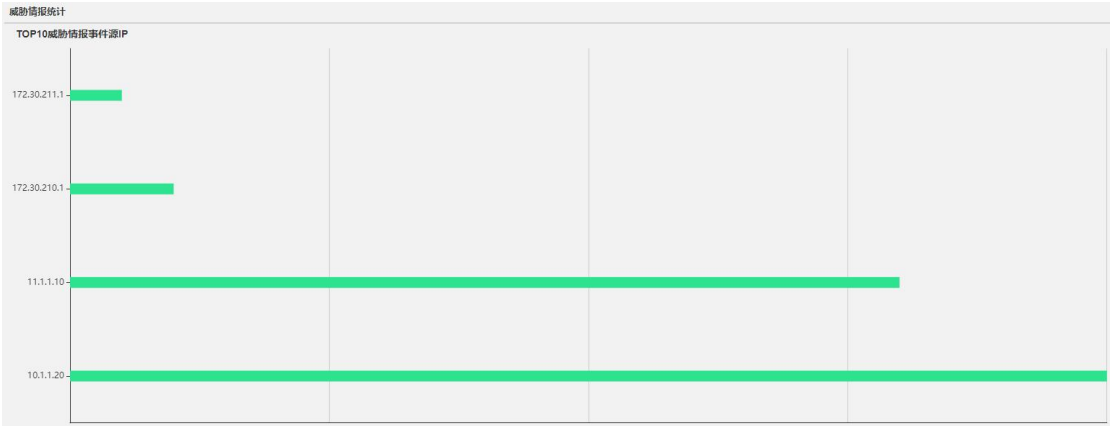


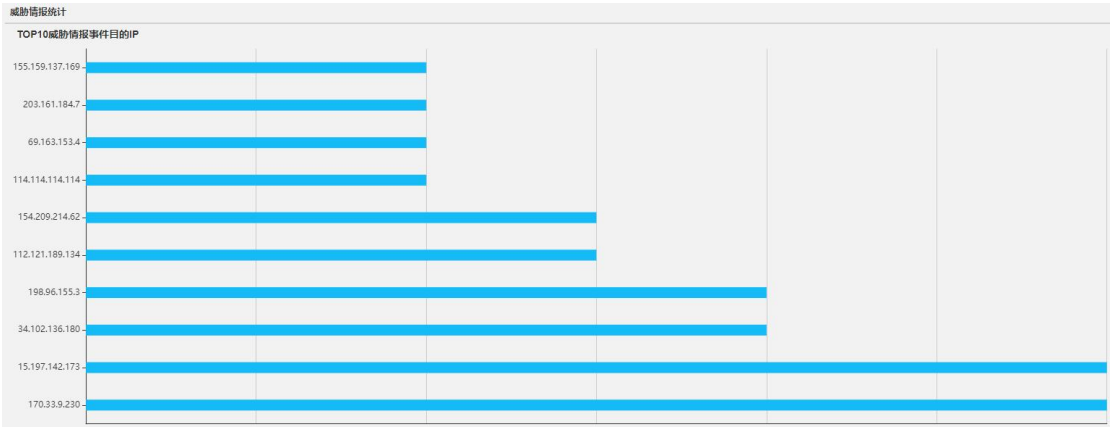
4.1.3. 威胁情报统计

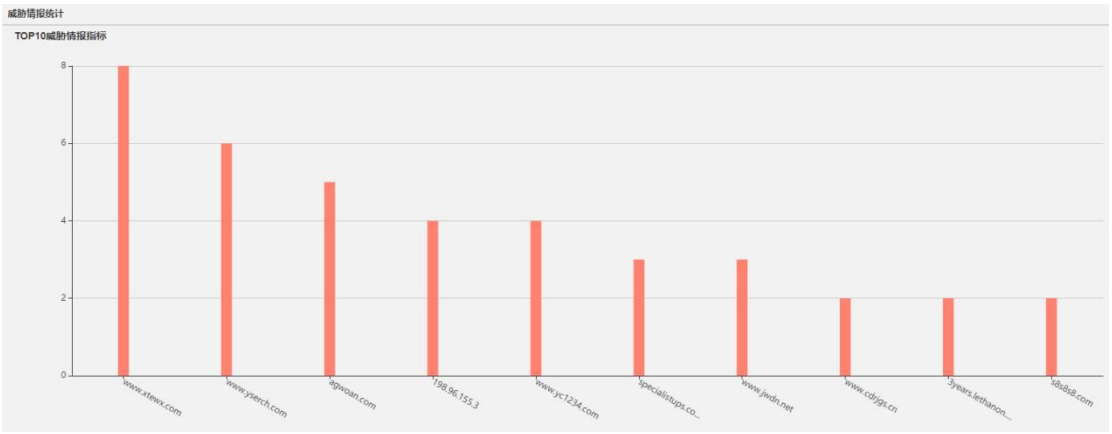
在系统菜单选择“监控>安全分析>威胁情报统计”查看威胁情报统计。在威胁情报统计中统计排行前十的威胁情报源 IP、目的 IP、威胁情报指标，以及对威胁情报类型的比例显示。

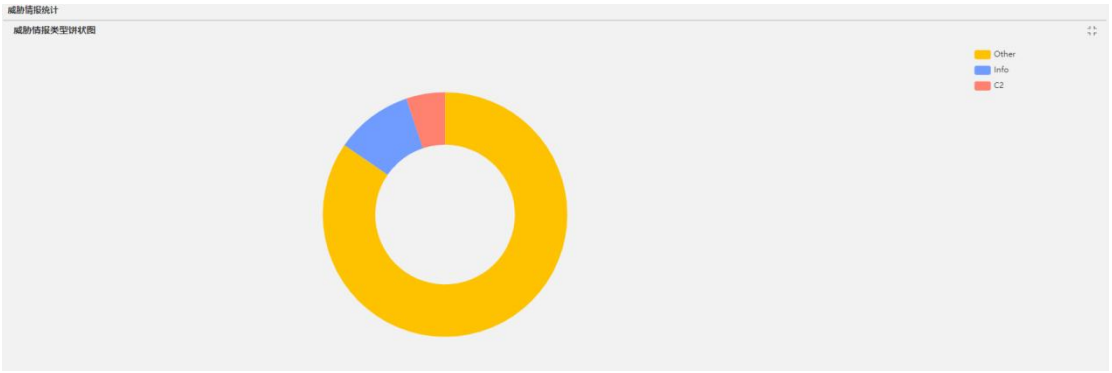


点击统计右上角的图标，能够放大显示选择的统计类型。



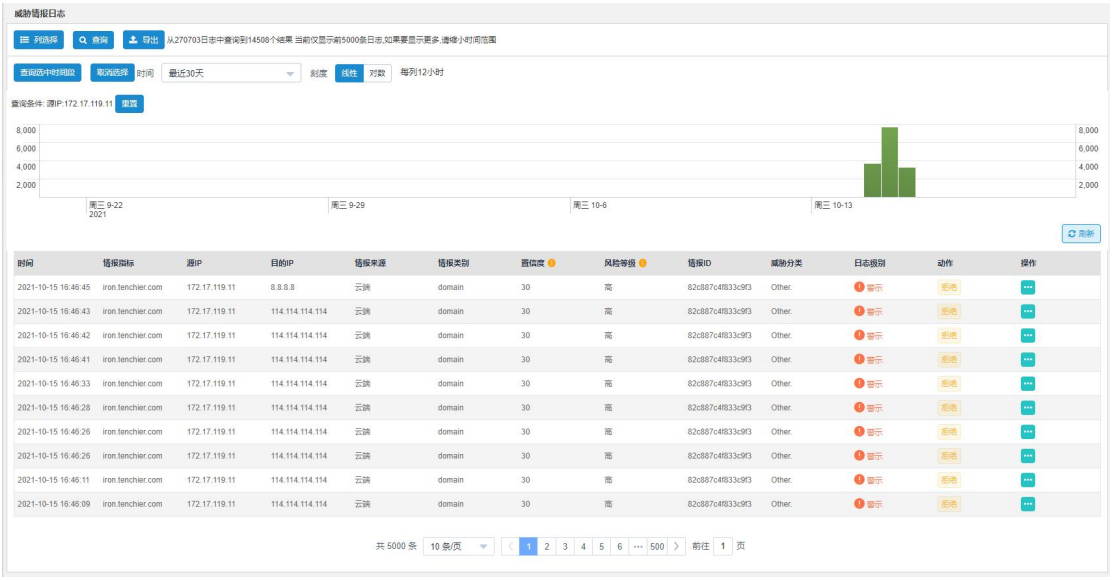






点击统计右上角的图标，能够返回整体显示统计页面。

点击统计显示的单个统计值能够连接到威胁情报统计日志界面，并过滤出当前统计相关的日志详细内容。



4.2. 主机勒索病毒有效防护

勒索病毒因其具备快速横向传播、变种迅速、对文件加密等特点因此导致用

户难以对其进行有效防护，天翼云云等保专区主机安全提供内核级多维度防御引擎，及时发现并阻断勒索病毒，准确高效地实时保护用户关键数据，在导航栏选择“高级威胁➤勒索防御”进入勒索防御页面，选择需要设置的引擎类型，点击引擎右侧区域的<去设置>。

勒索诱饵防护引擎，针对勒索病毒遍历文件实施加密的特点，在终端关键目录下放置诱饵文件，当有勒索病毒尝试加密诱饵文件时及时中止进程，阻止勒索病毒的进一步加密和扩散。

勒索行为防护引擎，通过分析常见的勒索软件样本，总结了样本具有的共性特征形成了引擎行为库，系统 API 级别分析，有效抵御未知勒索病毒。

文件保险柜，添加访问控制策略，对重要文件进行访问权限控制，仅允许配置的例外进程操作，避免被勒索病毒破坏。

进入系统防护页面，选择“勒索防御”，开启“勒索诱饵防护引擎”。

点击“文件保险柜”按钮，弹出文件保险柜对话框，点击<添加一行>，输入保护项、例外程序后点击<保存>，再点击<确定>，即可添加文件保险柜，针对重要文件进行保护。

5. 常见问题

5.1. 计费类

产品名称	产品规格	标准价格（元/年）
云等保专区-堡垒机	标准版	18273
	高级版	51527
	企业版	139191
云等保专区-数据库审计	标准版	24133
	高级版	76977
	企业版	326439
云等保解专区-漏洞扫描	标准版	16068
	高级版	59878
	企业版	126358
云等保专区-日志审计	标准版	18984
	高级版	55190
	企业版	164667
云等保专区-下一代防火	标准版	22546

墙	高级版	40872
	企业版	68079
云等保专区-主机安全	标准版	2000
	网页防篡改版	8340
云等保专区-Web 应用防火墙	标准版	34049
	域名扩展包	5998
	带宽扩展包	5998

5.2. 购买类

(1) 如何知道应当购买那些安全原子能力？

当前天翼云根据多年安全经验以及最佳实践帮助用户更简单的通过等保，特地推出等保二级、等保三级套餐，您可根据当前在天翼云上业务的定级等级情况自主选择等保二级、三级套餐。

(2) 如何选择单个安全原子能力规格？

当前安全组件规格分为基础版、高级版和企业版，每个规格有其对应参数，您可根据自身业务的流量、ECS 的数量等综合评估，自助选择相应安全组件的规格。

(3) 是否支持单独购买安全原子能力？

支持，但是主机安全的网页防篡改不能单独购买。

(4) Web 应用防火墙的带宽扩展包是否有购买上限？

当前 Web 应用防火墙最大支持购买扩展 20 个扩展包。

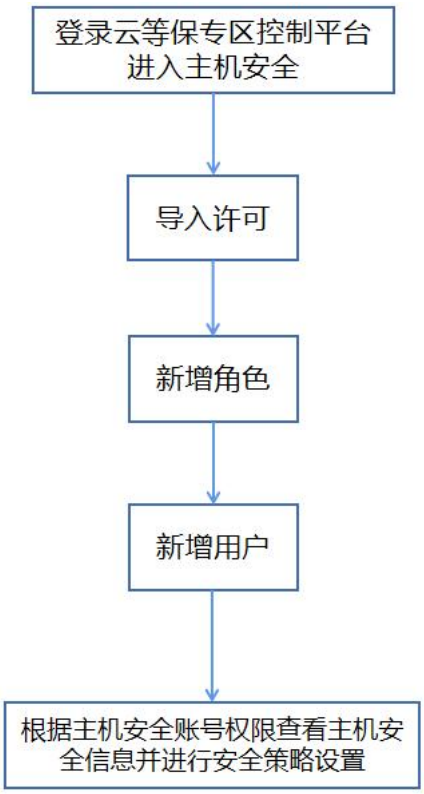
(5) 产品是否可以试用，使用周期为多长时间？

当前产品不支持试用。

5.3. 产品配置类

5.3.1. 主机安全

(1) 如何在服务器上开启主机安全防护？



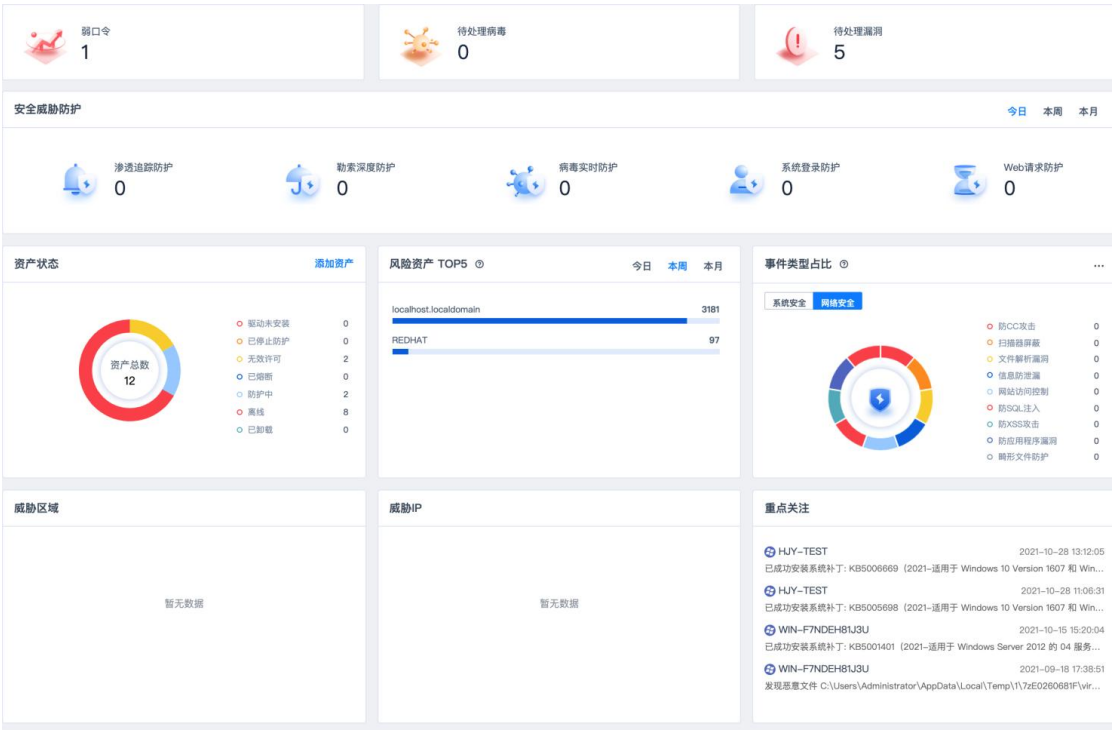
① 用户登录云等保专区控制平台，进入到主机安全原子能力。

② 然后进行主机安全许可导入工作，用户需获得许可授权后使用 EDR 系统。

③ 完成许可导入后尽进行新增角色创建，EDR 支持自定义用户角色及自定义角色权限功能，可对不同角色赋予不同权限，详情可参照用户手册中的角色管理。

④ 进行用户新增设置，根据不同的权限要求新增角色权限后，用户可根据实际业务需求，自定义创建租户并为租户选择对应角色，详情可参照用户手册中新增租户操作。

⑤ 用户根据创建的租户角色登录，查看主机安全信息并进行主机安全策略设置。



(2) 主机安全的 agent 可以部署在哪些操作系统的机器上？

Windows server 2008、Windows server 2012、Windows server 2016、win 7、win 8、win 10、Centos 5.0 +、Redhat 5.0 + 、 Suse11 +、 Ubuntu 14 +，兆芯+中标麒麟 V7.0、V10/统信 UOSV20，龙芯+中标麒麟 V7.0、V10/统信 UOSV20，鲲鹏+中标麒麟 V7.0、V10/统信 UOSV20，飞腾+银河麒麟 V4.0、V10，海光+中标麒麟 V7.0、V10/统信 UOSV20 等操作系统

(3) 主机安全 EDR 支持导出多少条防护日志？

EDR 支持最多支持导出 10 万条防护日志，当前总数超过 10 万条的则导出最新的 10 万条。

操作日志和运维日志也是支持最多导出 10 万条。

(4) 主机安全 EDR 是否支持病毒查杀后进行自动处理？

支持，在主机安全配置中选择“资产管理-病毒查杀”，点击<查杀设置>，可设置处理方式为自动处理。

(5) agent 服务器性能占比？

正常情况下内存大约 100M,CPU 不超过 1%。

(6) 主机安全的漏洞补丁是如何更新的？

补丁检测规则会自动从云等保专区的主机安全原子能力推送给 Agent，云等保专区主机安全原子保持更新；Agent 在检测到相应补丁后，需自行联网下载修复。

(7) 主机安全网页防篡改版能否保护网站数据库，如何保护？

网页防篡改系统的 Web 防攻击模块中的 SQL 防注入功能，通过设定正则表达式的规则，可以有效的防止黑客通过注入 SQL 语句的方式从网站关联的数据库中获取、修改数据信息或攻击数据库，如拦截 mdb 文件上传下载、一般 SQL 注入猜测、SQL 写操作关键字、SQL 存储过程关键字及系统 shell 关键字。

(8) 主机安全网页防篡改系统后，占用的系统资源大概是多少？会不会影响网速？

主机安全网页防篡改版安装后，占用的系统资源<3%，基本不占用服务器资源。

(9) 网站被黑后，网页防篡改能否及时恢复？

主机安全网页防篡改版是采用最先进的第三代内核驱动技术实现的，可以确保最高权限的用户也无法对网页文件进行非法篡改。同时具备同步模块，确认网页文件能及时的从同步端同步到 WEB 服务器上。

5.3.2. Web 应用防火墙

(1) Web 应用防火墙如何进行接入配置？

① 用户登录到云等保专区后，进入 web 应用防火墙原子能力，选择 web 应用防火墙部署模式，更多信息请参考全局配置。

在菜单栏中选择“配置➤全局配置”进入全局配置页面，编辑相关信息，点击<保存>。

② 添加保护站点，详细操作可查看用户手册中-配置保护站点操作细则。

③ 配置防护策略，详细操作可查看用户手册中规则组和自定义规则。

④ 完成基础配置后，可通过以下步骤验证是否配置成功：

⑤ 使用客户端浏览器访问被保护对象，如基础配置保护站点中添加的保护

站点为 http://192.168.26.120:8080，则在浏览器中输入该 URL 检查是否能够访问正常。

⑥ 在浏览器中输入以下 URL 模拟 SQL 注入攻击：http://192.168.26.120:8080/index.asp?id=1%20and%201=1。

⑦ 在菜单栏选择“日志➤应用防护日志”，查看系统是否记录到 SQL 注入攻击事件。

⑧ 如存在，点击事件名称检查告警详细信息中记录的主机名和客户端 IP 地址与测试中使用的保护站点和客户端 IP 地址是否一致。如一致，说明已经完成 web 应用防火墙那个接入配置。

(2) Web 应用防火墙的防护准确性如何？

天翼云 Web 应用防火墙采用智能语义分析、机器学习、云端威胁情报联动、行为分析、云端高防等五大引擎联动的方式进行攻击防护，防护准确率高、误报率低。

(3) 天翼云语义分析相比传统规则库方式的优势是什么？

传统规则库采用正则规则库的形式对攻击特征进行匹配，存在检出率低、误报率高、性能消耗过多、规则库维护成本高、无法防御未知攻击等劣势，而天翼云语义分析结合词法分析、语法分析、语义分析三个处理逻辑进行攻击检测，能在不占用过多系统性能的同时，相比传统方式提高检出率、降低误报率。

(4) Web 应用防火墙是否支持 IPv6？

支持，本身天翼云 web 应用防火墙中的保护站点可填写 IPv6， 也可转发 IPv6 流量，同时 web 应用防火墙自身管理口地址可填写 IPv6。

(5) Web 应用防火墙是否支持长连接？

支持， 保护站点中可以设置开启长连接。

(6) Client 请求包的源端口，经过 Web 应用防火墙，是否被改变？

会被改变。 Web 应用防火墙的透明代理及反向代理属于 7 层代理机制，当 Client 的源端口请求包送达后， Web 应用防火墙从后端链路接口转发给 Server，此时 Server 收到的请求包源端口是 Web 应用防火墙的源端口。

(7) Web 应用防火墙是否支持日志外发？

支持。外发日志只支持应用防护日志和系统日志，其他日志暂不支持。

(8) Web 应用防火墙能否防暴力破解？

可以， 可在行为分析页面中对 CC 规则进行配置来实现。

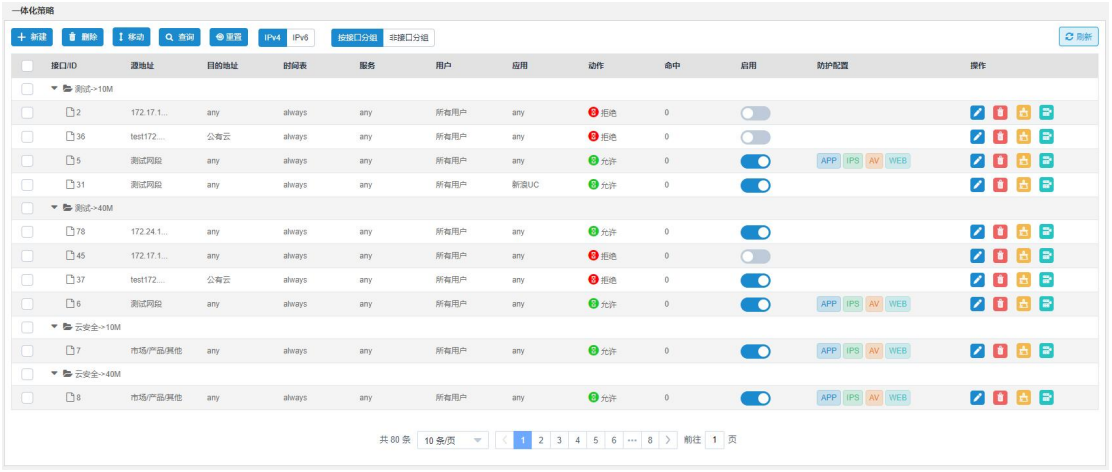
(9) Web 应用防火墙的保护站点 SSL 证书有变更，Web 应用防火墙需要变更吗？

需要更新，如果不更新， WAF 将无法解析 SSL 加密流量。

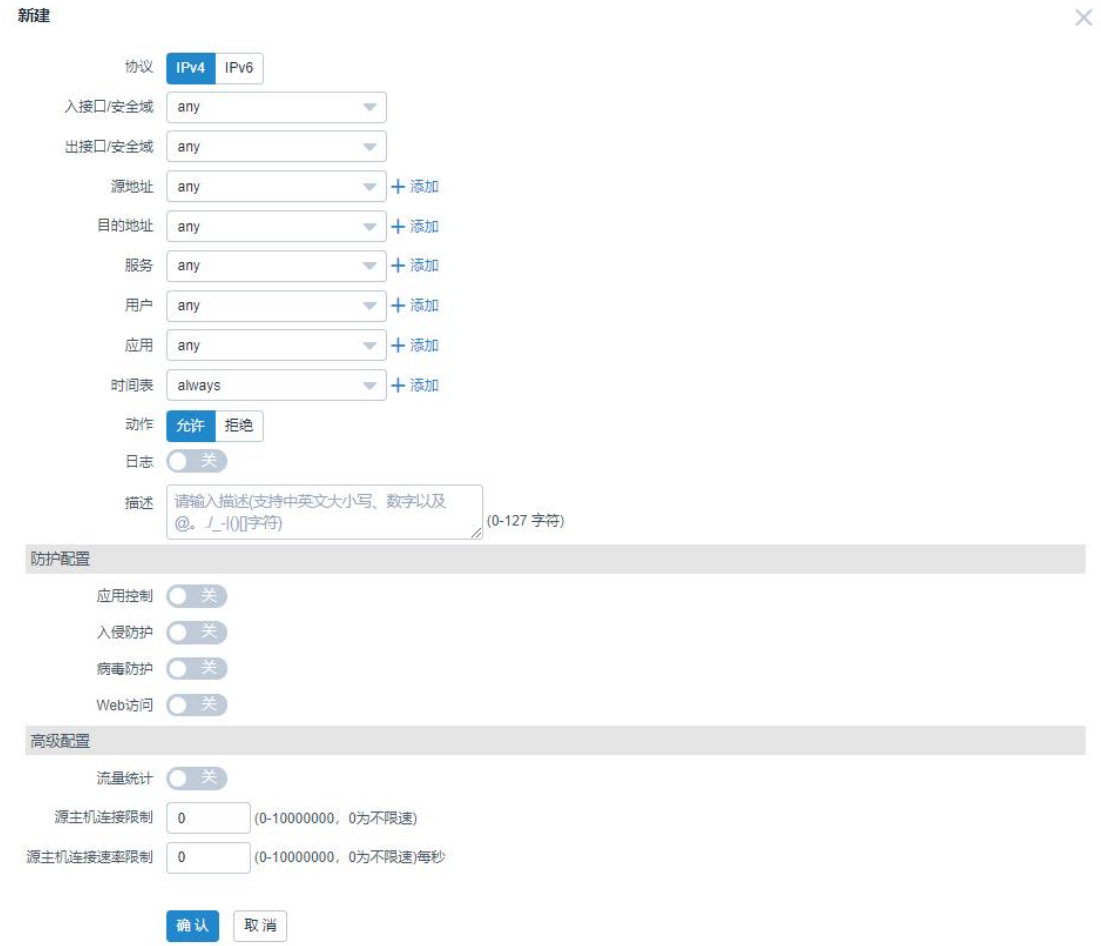
5.3.3. 下一代防火墙

(1) 下一代防火墙如何进行接入策略设置？

① 用户登录到云等保专区后，进入下代防火墙原子能力，的在系统菜单中点击“策略>防火墙策略>一体化策略”，进入一体化策略配置页面。



② 点击<新建>创建新的一体化策略



(2) 防火墙精确访问控制规则的匹配顺序是什么，一条精确访问控制规则内多个条件的关系是什么？

多条精确访问控制规则之间是或的关系，匹配顺序为从上往下顺序匹配，如果匹配中某一条精确访问控制规则，将不再匹配后续的规则。

一条精确访问控制规则可以包含 10 个匹配条件，多个匹配条件之间是与的关系，流量必须满足该条规则的所有条件，才能命中该条规则。

(3) 防火墙的关键字过滤功能区分大小写字母吗？

关键字过滤不区分大小写字母，无论配置为大写或小写均可正常检测和过滤。

(4) 防火墙的策略分析功能有什么作用？

当前网络环境的复杂性，网络服务与网络终端的多样性，相应的防火墙设备就需要更多、更复杂的控制策略。这些控制策略经过一段时间的积累，往往会造成老策略不敢删，新策略不断增加，单个防火墙会积累成千上万的策略，极大降低设备性能和用户体验。

从策略分析的角度，一键分析当前的冲突、冗余、隐藏、合并、过期和空策略，一定程度上解决防火墙管理的难题，使每一条策略都直观可视，让下一代防火墙更易于使用、便于维护管理。

(5) 每 IP 限速和通道带宽限制的处理关系是什么？

流量先被每 IP 限速处理，然后再被流控通道处理。每 IP 限速的周期是一秒，流控通道是实时的。被 IP 限速通过的流量可能会继续被流控通道丢弃。

(6) 防火墙防病毒能力支持处理哪些压缩格式的文件？

目前支持对.zip、.gz、.bz2 等压缩文件进行扫描。

(7) 防火墙 P2P 智能识别三种级别宽松度有什么区别？

P2P 智能识别，是针对 UDP 流量进行固定特征+并发连接识别方式。“严格”和“适中”都是先进行并发连接识别，再进行固定特征识别，“严格”要求并发连接阈值高。“宽松”是固定特征识别方式，有误报的可能。

(8) 防火墙告警日志记录最大规格是多少？

记录到 1 万条日志时，会删除最初的 1000 条。

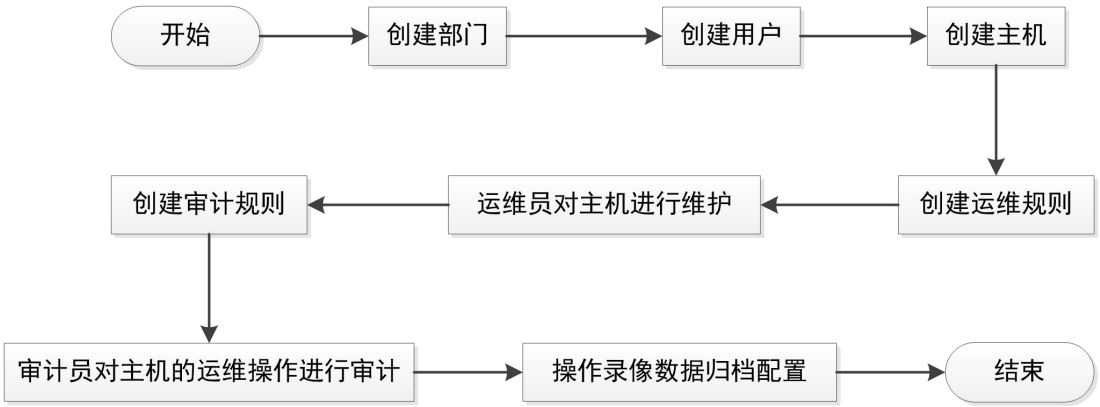
(9) 防火墙支持 IPS 自定义规则的最大规格是多少？

IPS 自定义规则最多可配置 32 条，每条自定义规则最多可包含 8 个协议字段，每个协议字段最多可包含 8 个协议匹配条件。

5.3.4. 堡垒机

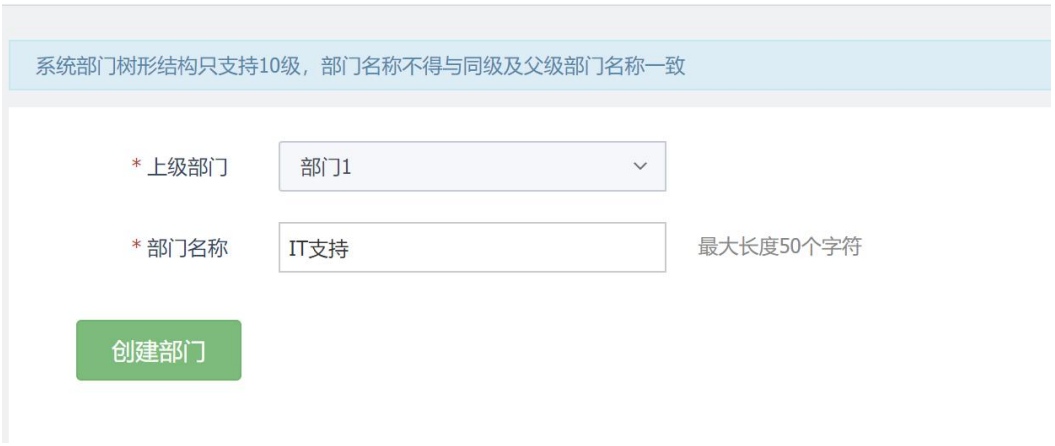
(1) 堡垒机的如何进行接入配置？

① 用户登录到云等保专区后，进入堡垒机原子能力



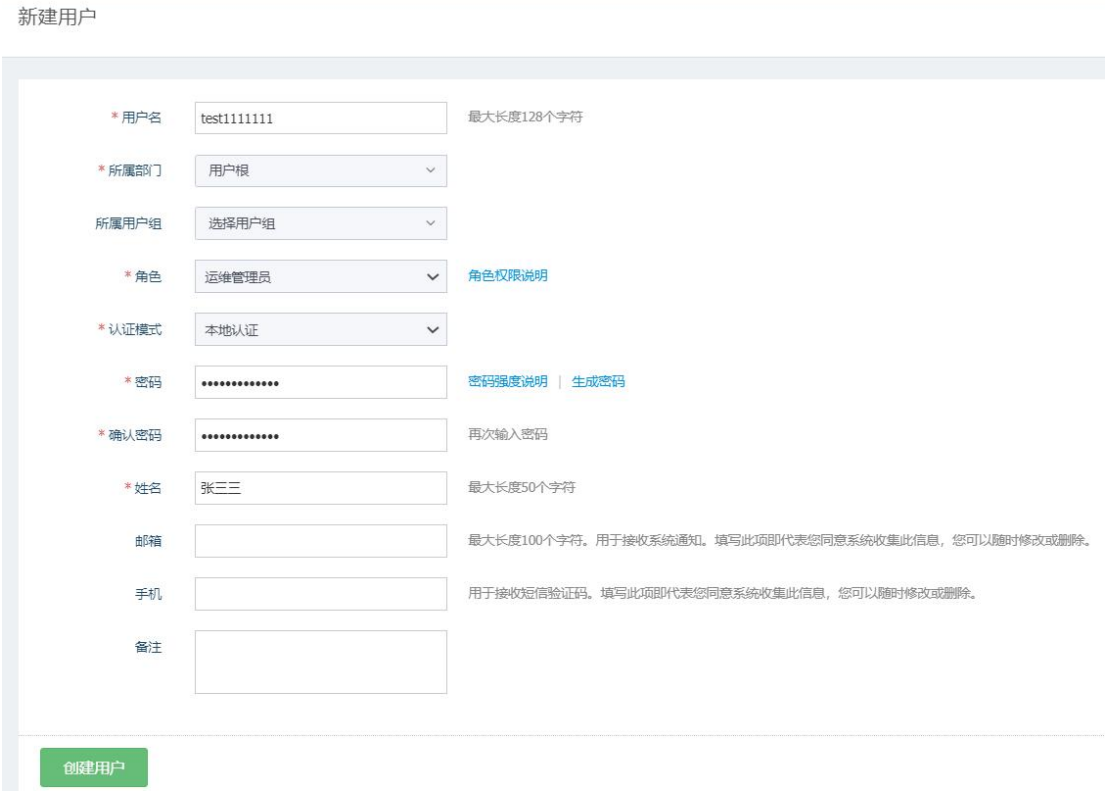
② 首先创建部门：超级管理员或部门管理员创建部门，在系统菜单栏选择“部门”，进入部门页面，点击<新建部门>。

选择部门所属的上级部门并输入部门名称，点击<创建部门>完成创建。



③ 创建系统用户，例如运维员等，在菜单栏选择“用户➤用户管理”，进入用户管理页面，点击<新建用户>。

进入新建用户页面，编辑相关信息，点击<创建用户>。



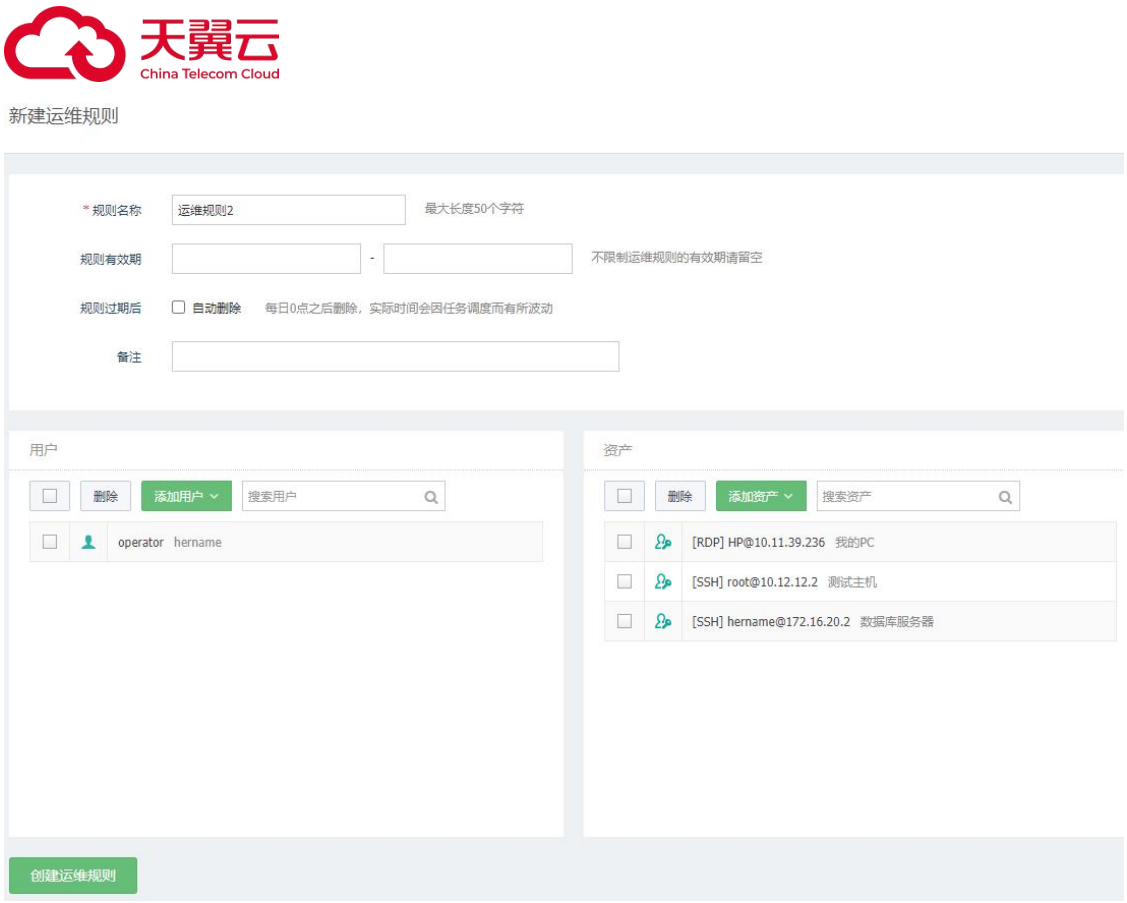
④ 创建主机：将主机添加至系统后，系统才能对主机的运维进行审计，在系统菜单栏选择“资产➤主机管理”，进入主机管理页面。点击页面右上角的<新建主机>。

进入新建主机页面，编辑相关信息，点击<创建主机>完成新建主机。

新建主机

⑤ 创建运维规则：授权运维员可以登录主机进行运维，系统菜单栏选择“授权➤运维规则”，进入运维规则页面。点击右上角的<新建运维规则>。

进入新建运维规则页面，填写运维规则名称、有效期等信息，设置用户与资产的对应关系（将资产的运维权限赋予给用户），点击<创建运维规则>，完成运维规则的创建。



⑥ 运维员对主机进行维护：运维员通过系统登录主机并对主机进行维护，详细操作可阅读用户手册-主机运维配置

(2) 堡垒机的部署对网络有什么样的要求？
堡垒机要求与被运维终端网络可达。

(3) 堡垒机支持双因素身份认证吗？
支持双因素认证，如：

1) 自带免费的手机 APP 动态口令认证。

2) 可与短信网关平台对接，实现短信口令认证。

(4) 堡垒机能对数据库程序进行审计吗？
支持对主流数据库（如 Oracle、MySQL、Sql Server、DB2）的运维审计。

(5) 堡垒机能对文件传输进行审计吗？
文件传输方式很多（如 SFTP、FTP、RDP、RZ、SZ）,堡垒机可以备份这些协议传输过的文件，便于事后定位追踪，同时堡垒机还能对重要的服务器控制文件传输，防止数据失泄密。

(6) 可以使用 macOS 或 Linux 系统电脑访问堡垒机再访问服务器吗？

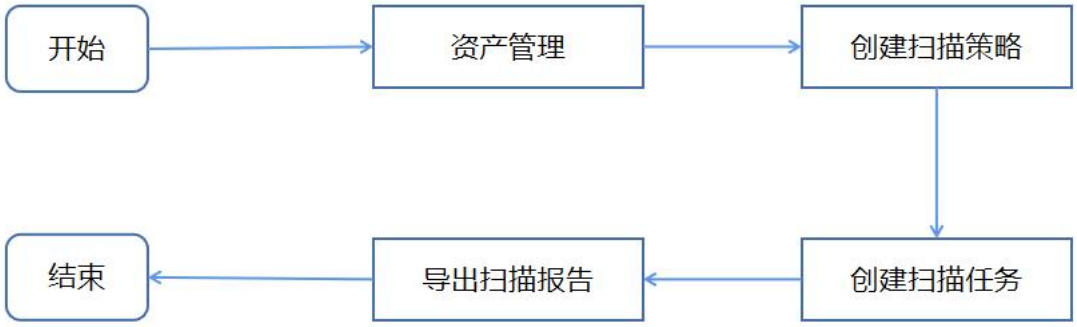
支持，直接利用 C/S 运维方式，H5 运维即可。

(7) 堡垒机是否支持 API 接口供其它平台调用？

堡垒机提供开放的 API 接口，允许第三方平台调用堡垒机的用户数据、主机数据、授权数据、审计数据。

5.3.5. 漏洞扫描

(1) 漏扫支持扫描如何进行接入配置？

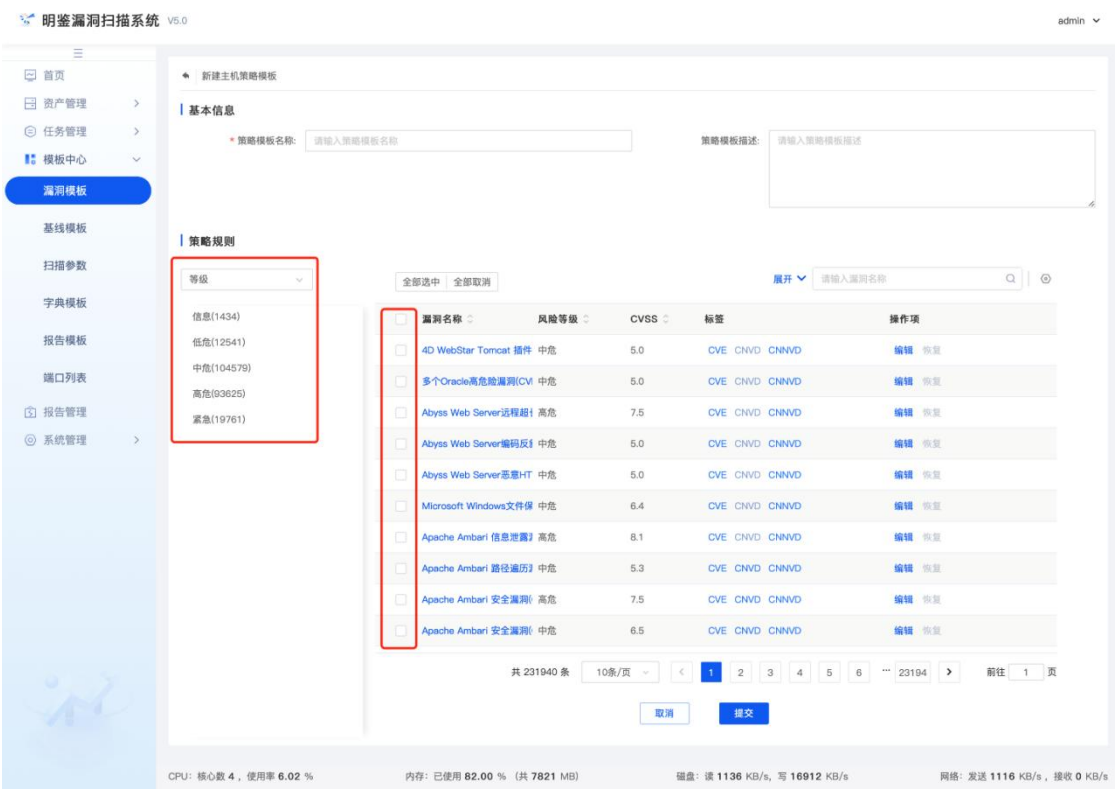


① 用户登录后先进行资产管理设置，添加资产，便于后续对资产进行扫描，在菜单栏选择“资产管理➤资产列表”，选择主机资产页签，点击<新增>。

在弹出的新建主机资产对话框中编辑相关信息，点击<提交>。

② 接着创建扫描策略，制定扫描策略模板，使扫描任务更具针对性，在菜单栏选择“模板中心➤漏洞模板”，选择主机策略页签，点击<新增>。

进入新建主机策略模板页面，编辑策略模板名称，选择策略规则（策略规则从等级、目标、类型三个维度进行分类），勾选对应的策略，点击<提交>。



③ 然后创建扫描任务，开启扫描任务后对于主机漏洞进行扫描，在菜单栏选择“任务管理➤任务列表”，进入任务列表页面，点击<新增>，页面跳转至创建任务页面，具体操作请参见创建任务。

。

④ 最后扫描结束后，导出扫描报告，针对扫描结果分析资产安全风险，菜单栏选择“报告管理”，进入报告管理页面，点击<新增>。

进入新建报告页面，编辑相关信息，点击<输出报告>。

(2) 漏扫支持扫描的操作系统类型有哪些？

漏扫的工作原理主要是通过探测存活主机，然后针对存活主机识别开放端口和服务版本来进行漏洞发现的，理论上市面上常见的操作系统都支持漏洞扫描，包括主流 windows 操作系统、Linux 操作系统、类 Unix 操作系统和国产操作系统。

(3) 漏扫支持扫描的数据库类型有哪些？

漏扫默认的主机扫描模块针对常见的关系型数据库和非关系型数据库都支持扫描，具体包含如下：

ORACLE、MySQL、MariaDB 、SQL Server、Sybase、PostgreSQL、DB2、Redis、Informix、MongoDB、Memcached、Elasticsearch、达梦、人大金仓等。

以上数据库漏洞扫描能力默认采用非授权扫描方式即可支持，对于选配的数据库扫描模块则采用授权方式进行扫描，支持的数据库类型和版本包含：

数据库类型	支持的版本号
ORACLE	9, 10, 11, 12, 13, ……19
MySQL	5.0.*-8.0.21

SQL Server	SQL Server2000, 2005, 2008, 2012,2014 ,2016
Sybase	V15.7,V16
PostgreSQL	全版本覆盖
DB2	V8, V9, V10, z/os
Informix	V12,V14
达梦	DM7,DM8
人大金仓	V7,V8

(4) 漏洞扫描支持扫描的弱口令协议有哪些？

漏洞扫描支持扫描的弱口令协议多达 22 种，包含：FTP、Telnet、pop3、SMB、SSH、RDP、ORACLE、SMTP、Imap、MSSQL、DB2、Rlogin、MySQL、RTSP、Weblogic、Tomcat、MongoDB、Sybase、SIP、Onvif、SNMP、Redis，默认将提供对应协议的弱口令字典，用户也可以自定义口令字典。

(5) 漏洞扫描是否支持 IPv6？

自身支持 IPv4 和 IPv6 两种网络协议的部署，也支持对 IPv4 和 IPv6 协议的目标进行扫描，包括域名类型。

(6) 漏扫扫描时是否会影响业务？

主机扫描：通过发送数据包来探测目标是否存活、开放的端口、运行的服务和版本信息等，理论上不会出现任何的影响，但是不排除由于防火墙的设置导致的服务宕机、由于目标服务对发送的报文处理导致的宕机等，一般情况下基本不会产生，实际漏扫引擎已经做了很多规避策略，但不能保证 100%无影响，市面上的漏扫原理基本一样。

网站扫描：原理是模拟用户的正常 HTTP 请求和模拟黑客的无害攻击，一般来说是不会影响被扫描对象的业务正常运行，但是如果对方服务器的并发连接数本身就较低，那么可能会导致服务中断，需要重启中间件，漏扫引擎具备动态流控的功能，该影响的概率极低基本不会发生。

基线配置核查：原理与数据库扫描类似，主要是查询相关配置，可能会产生临时文件和删除临时文件操作，但不会影响业务。

(7) 授权扫描和非授权扫描有什么区别？

漏扫的扫描方式包括授权扫描和非授权扫描两种，也有称登录扫描和非登录扫描，实际是一个含义。

授权扫描：在对目标进行漏洞扫描的过程中，要输入帐号、密码等信息，属于“登录授权”进行的扫描。因为通过输入帐号信息登录后进行的扫描，因此扫描获得的信息更多，漏洞也将发现的更多，且误报率更低。（适用于主机扫描、数据库扫描、网站扫描、基线核查四大扫描模块）

非授权扫描：不需要目标的账户密码等授权信息即直接扫描，通过远程探测目标的信息来判断漏洞，可能会产生误报和漏洞（适用于主机扫描、网站扫描量大扫描模块）。

(8) 漏洞扫描 SysLog 告警通知发送哪些数据？

① 资源消耗数据，包括 CPU 信息、内存信息、磁盘读写信息、网络读写速度信息。

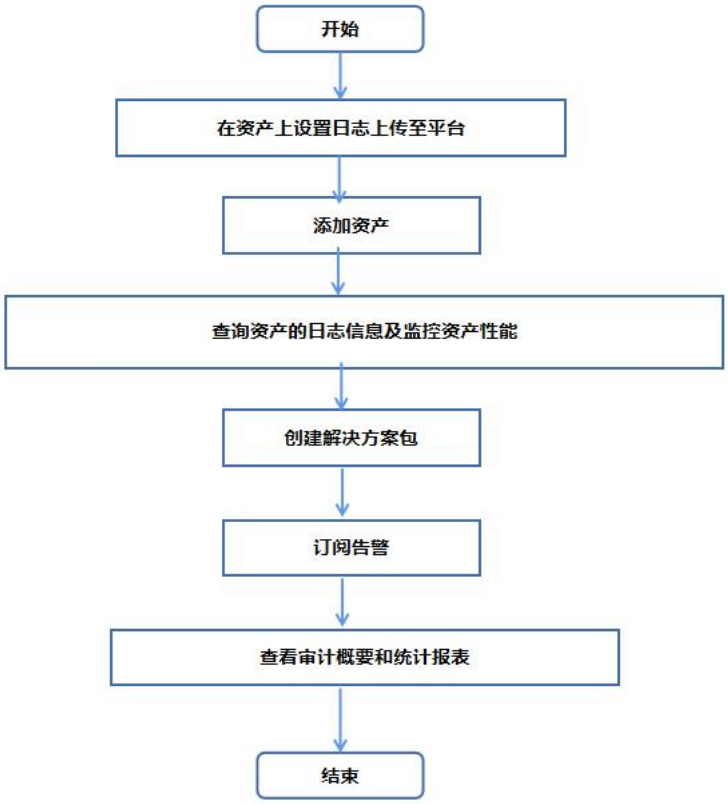
② 任务扫描数据，包括任务名称、任务类型、任务状态、任务进度、任务开始结束时间、任务漏洞数。

③ 审计日志数据，包括操作用户、操作时间、事件名称、详细信息、状态、操作类型。

④ 弱点信息数据，包括所属任务 ID、漏洞名称、漏洞详情等。

5.3.6. 日志审计

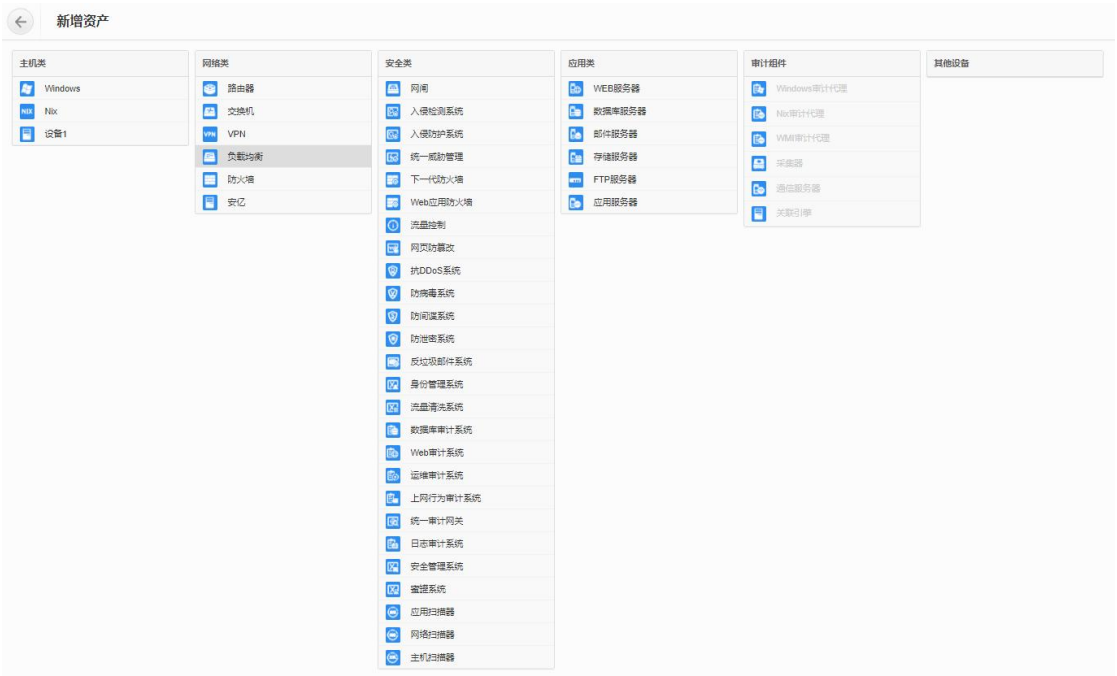
(1) 日志审计设备如何进行接入配置？



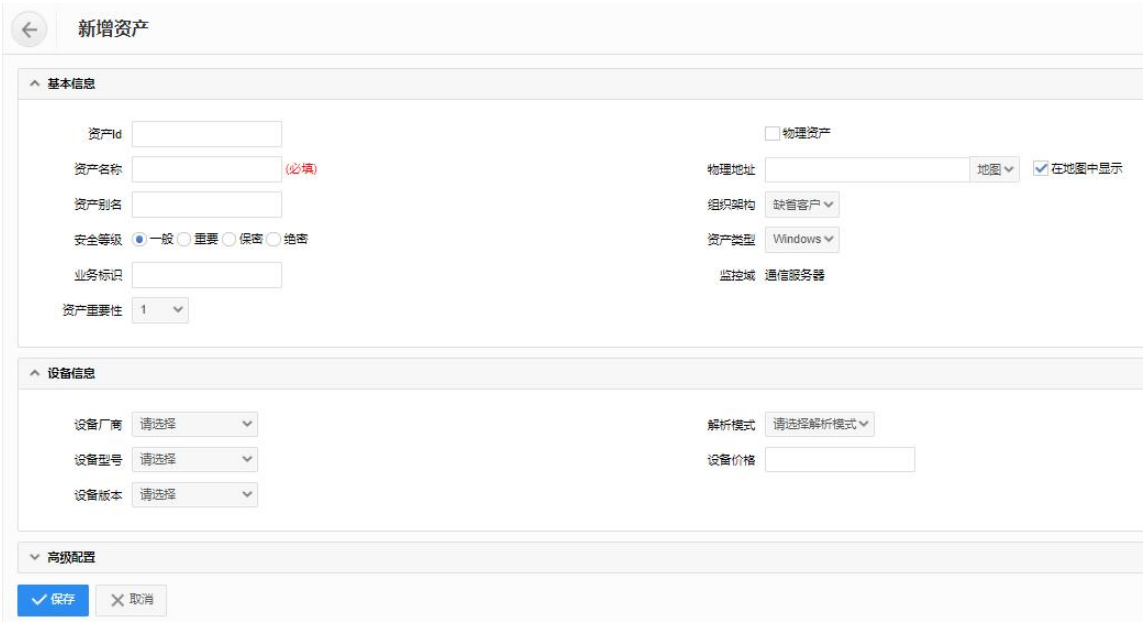
① 首先在进行审计前，用户需要在资产上设置 Syslog 等协议将日志发送至平台

② 平台可自动发现通过 Syslog 等协议向平台发送日志的资产向平台发送日志的资产，发现这些资产后，需要添加这些资产，在上边栏选择“资产管理”，在左侧菜单栏选择“资产➤全部资产”进入资产页面，点击<新增>。

进入新增资产页面，选择资产类型（如 Windows）。

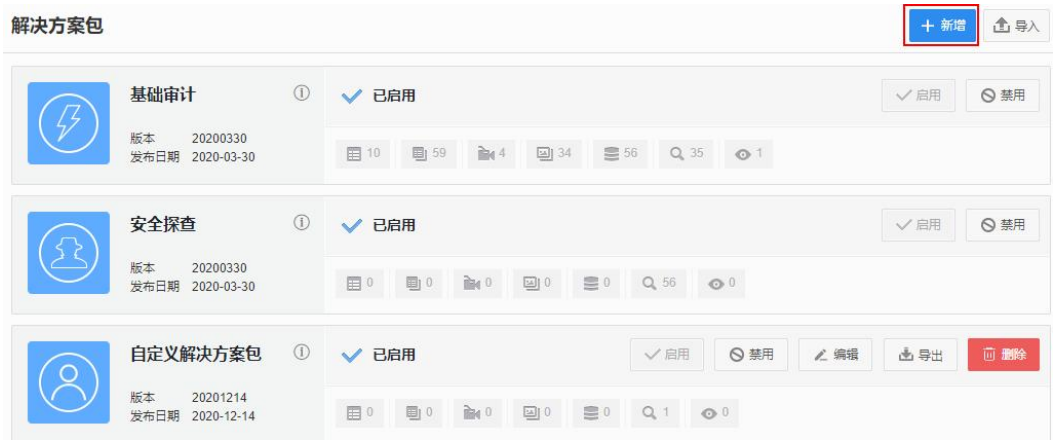


编辑相关信息，点击<保存>。



③ 在事件管理模块中可查询资产的日志信息，在性能监控模块中监控资产的性能状态，在上边栏选择“事件管理”，在左侧菜单栏选择“事件➤自定义查询”进入自定义查询页面。设置查询条件，点击<查询>即可查询事件，点击<清空>可清空查询条件。

④ 创建解决方案包为可选操作，平台已经内置了 2 个解决方案包。用户可根据需要创建解决方案包，解决方案包是一系列安全事件模板的集合，平台根据这些模板分析资产的风险趋势，对于威胁事件给予告警，在上边栏选择“规则库”，在左侧菜单栏选择“解决方案包”进入解决方案包页面。



点击<新增>，编辑相关信息，点击<保存>。

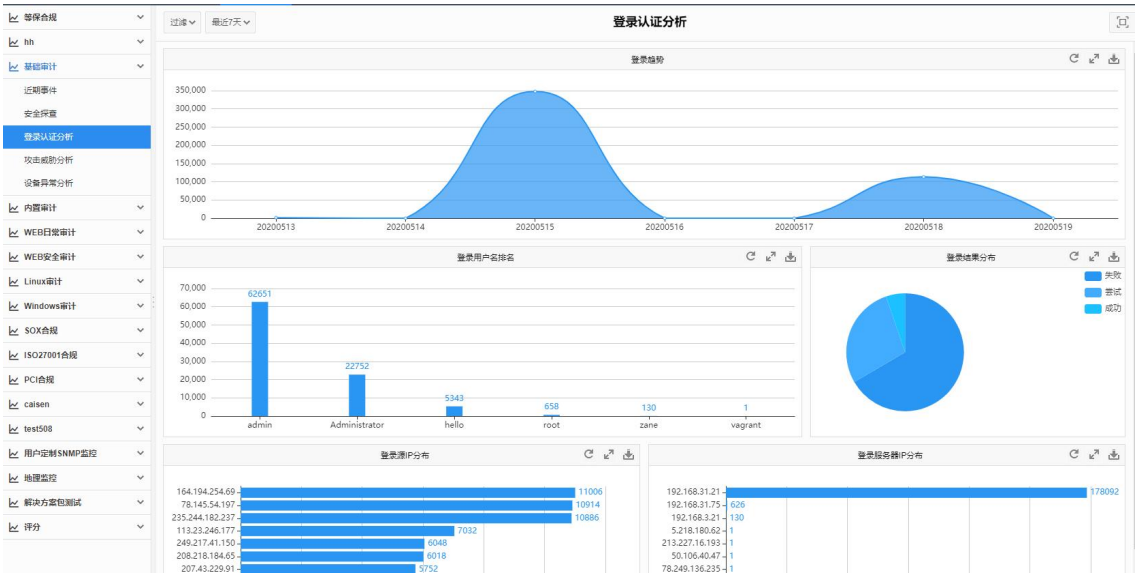
。

⑤ 用户还可订阅自己关注的告警事件，可第一时间了解资产的威胁态势，

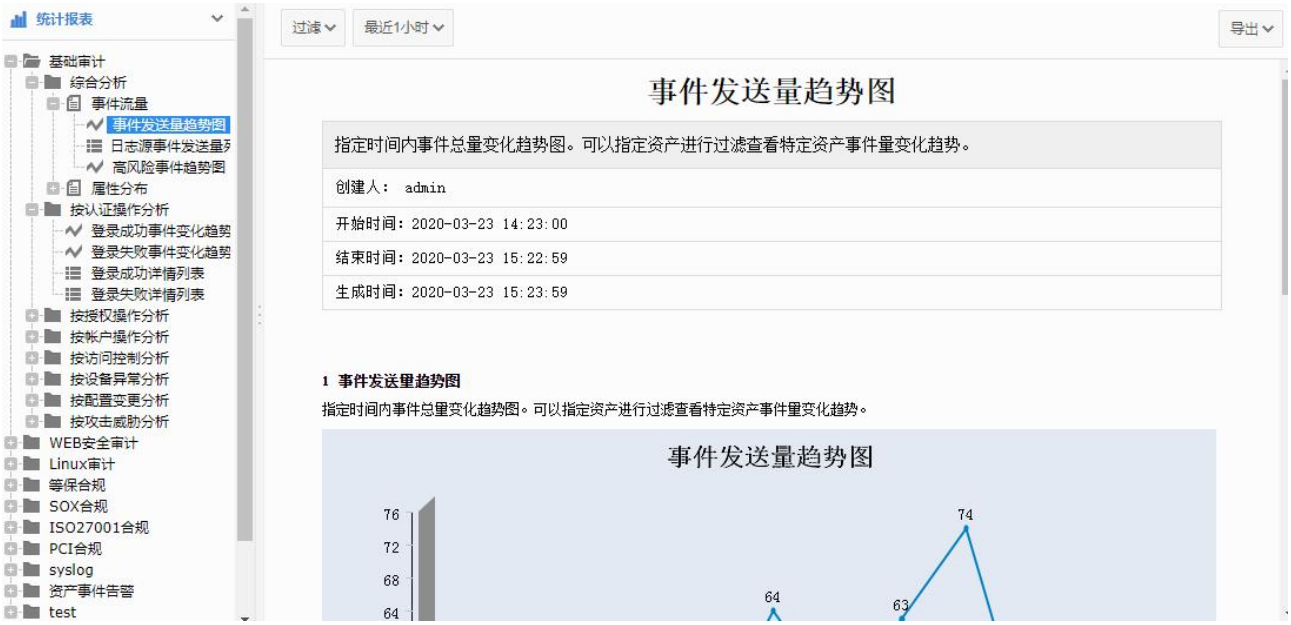
在上边栏选择“事件管理”，在左侧菜单栏选择“告警➤告警订阅”进入告警订阅页面，选择未订阅页签。在左侧解决方案包导航栏中选择事件（如“防火墙阻断”），选择邮件订阅、短信订阅、FTP 订阅和 TCP 订阅的用户，点击<保存>。

。

⑥ 平台会根据解决方案包对日志事件进行审计并对威胁趋势做出统计，用户可查看审计概要和统计报表，在上边栏选择“审计概要”进入审计概要页面，在左侧解决方案包导航栏中选择具体项目，即可查看该项目的审计概要信息。



在上边栏选择“统计报表”，在左侧菜单栏选择“统计报表”，选择报表项，可查看该报表项的信息。



点击<过滤>，在弹出的对话框中设置过滤条件，点击<过滤>即可查看符合过滤条件的统计信息。

点击时间下拉框，选择时间段可查看对应时间段内的事件统计信息。

点击页面右上角的<导出>，在弹出的菜单栏中选择<导出 Word>、<导出 PDF>即可将统计报表导出为 Word、PDF 文件保存至本地。

(2) 日志审计设备对外开放的端口有哪些？

① 日志审计对外开放的端口包括：

② tcp443 web 访问的端口

③ tcp22 ssh 连接的端口

④ udp514 syslog 接收日志端口

⑤ tcp21 ftp 服务开放的端口

⑥ udp161 snmp 服务开放的端口

(3) 日志审计能否不通过远程备份直接将数据文件下载到本地存储和恢复？

可以，可以在数据分区处手动下载备份文件在本地存储，恢复时上传文件恢复。

(4) 日志审计中弱点库的作用具体是什么？

弱点库是弱点知识库的集合，系统可以通过检查资产是否匹配弱点库中的信息来发现资产弱点。

(5) 日志数据存储是否加密，以及加密算法具体是什么？

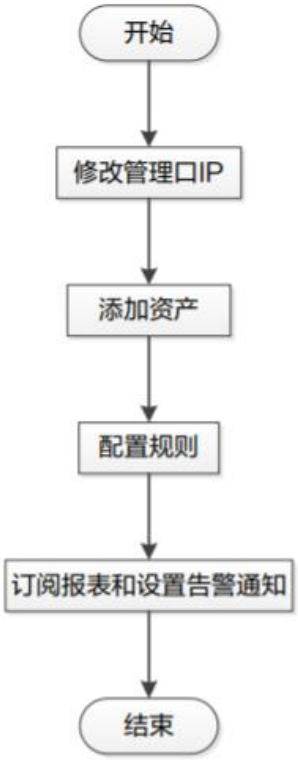
数据存储支持加密，但需要手动开启。在系统日志收发-加密配置处启用加密模式，加密算法可选择 AES 加密及 SM4 加密。

(6) 日志审计配置自动备份的周期是如何定义的？

每 7 天进行一次自动备份，系统设定是以服务重启后开始计算周期。

5.3.7. 数据库审计

(1) 数据库审计如何进行接入配置？



① 首先进入到数据库审计原子能力后先修改管理口 IP，在菜单栏选择“系统管理➤系统配置”进入系统配置页面，选择网络页签，点击操作列中的<编辑>。

在弹出的编辑网口对话框中修改网口的 IPv4 地址、子网掩码、IPv6 等配置信息，点击<保存>。

如果该网口是管理口，除修改网口的 IPv4 地址、子网掩码、IPv6 配置信息，还可设置 IPv4 网关。

在网口管理区域的操作列中点击是否启用开关，可启用或禁用选中的网口（管理口无法被禁用）。

② 然后添加系统需要审计的数据库，在菜单栏选择“资产➤资产管理”进入资产管理页面，选择资产管理页签，点击<添加>。

在弹出的添加资产页面编辑相关信息。

如需配置其他更多信息，可点击<更多配置>，选择单向审计或双向审计，设置加密协议审计。

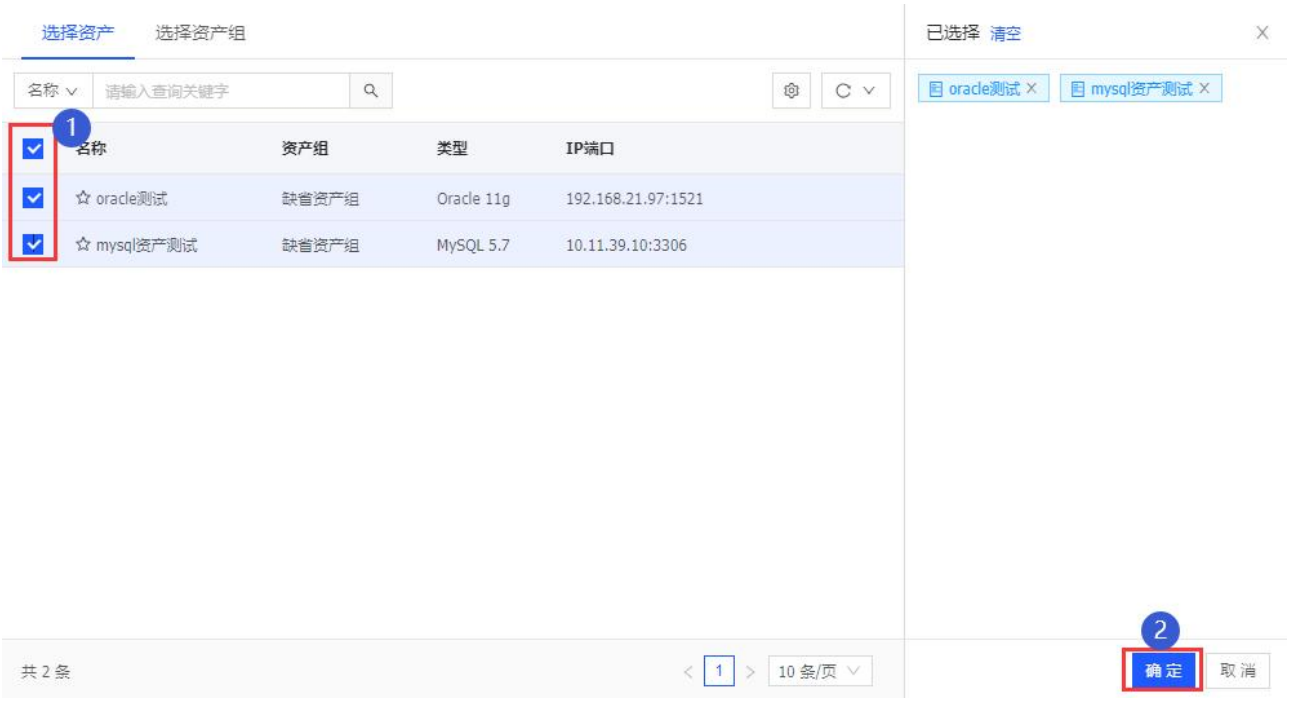
③ 然后配置数据库的安全规则和过滤规则，在菜单栏选择“规则配置➤安全规则”进入安全规则页面，选择规则管理页签，点击<推荐>，切换至<全部>。

用户也可以管理自定义的规则，新增自定义安全规则的操作方法如下：在菜单栏选择“规则配置➤安全规则”进入安全规则页面，选择规则管理页签，点击<新增>。

在新增规则对话框中编辑相关信息，点击<保存>。

接着启用规则，在菜单栏选择“规则配置➤安全规则”进入安全规则页面，选择规则管理页签，在规则列表中勾选目标规则，点击<启用选中项>。

在弹出对话框中勾选资产，点击<确定>，则可将已启用的规则直接应用到选择的资产上。



④ 最后便于用户及时了解数据库的运行状态及安全告警信息，可查看报表订阅和告警通知，在菜单栏选择“报表中心➤报表预览”进入报表预览页面，点击页面右上角的<订阅.>。

进入添加订阅任务页面，编辑相关信息，点击<保存>。

系统支持多种消息通知模式，可及时将当前资产告警情况以及系统本身的状态信息提供给管理员，目前支持邮件、短信、企业微信、钉钉、SNMP、Syslog 六种通知方式，详情阅读用户手册进行设置。

(2) 数据库审计是否支持备份行为的过滤，具体是怎样实现的？

可以通过设计规则来实现，如源 IP 是主数据库，目的 IP 是备数据库，这类命令全部过滤，不审计。

(3) 数据库审计 Agent 在服务器上生成的日志包含哪些内容？

数据库审计 agent 在服务器上生成的日志只是 agent 的运行日志，且日志的容

量有上限,50M*7=350M,存 7 天，循环覆盖,单日最大是 50M。

(4) 数据库审计是否支持报表导出 ofd 格式？

不支持。

(5) 在数据库所在服务器上，用数据库工具对数据库进行操作能审计到吗？

对应本地审计功能，通过安装 agent 的方式是可以的。

(6) 用户的数据库有区分主库和备库，这种情况占用几个授权？

数据库审计对授权占用是按照“业务 IP+端口”这个组合来确定的，每一个这样的组合会占用一个授权，可以结合实际主库和备库对外“业务 IP+端口”的数量来确定需要的授权数。

(7) 数据库审计是否支持对于某个数据库的日志单独设置保存时长，或者单独设置日志外送？

不支持单独设置某个库的日志存留时间，但是可以对某个库单独设置日志外送任务，在外送任务建立之后，会实时转发每一条日志，但是对于设置日志外送任务之前的日志，则无法单独外送。

(8) 加密的数据库，没有密钥，是否有审计数据？

无密钥，就没有审计记录。

(9) SSH 远程登陆审计与本地审计是否支持？

SSH 远程登陆审计指的是，在远程通过 SSH 登录数据库本地的情况下，可以审计到远程的设备的 IP，并不会因为此次行为的本质是数据库本地操作而止步数据库 IP 作为源 IP。SSH 远程登录，源头 IP 被审计到之后，下一步会流转到本地回环审计 OR 本地审计：

① 本地回环审计，会产生网络流量，会有审计日志，审计日志中的源 IP 会显示为远程登陆的设备的 IP，对所有支持的数据库协议都可用；

② 本地审计，无网络流量，这种情况要看数审目前支持的本地审计的矩阵，矩阵之内的，可以审计到，并且有审计日志，在矩阵之外的，审计不到，没有审计日志。

5.4. 云等保基础类

(1) 什么是等保

以《中华人民共和国网络安全法》为法律依据，以 2019 年 5 月发布的《GB/T22239-2019 信息安全技术 网络安全等级保护基本要求》为指导标准的网络安全等级保护办法，业内简称“ 等保 2.0 ”。

(2) 等保的发展历程

在 1994 年，国务院令第 147 号文件第九条“计算机信息系统实行安全等级保护”首次提出了等级保护的概念，期间经历 13 年，在 2007 年公通字[2007]43 号文中明确了信息安全等级保护的五个动作，为开展等级保护工作提供了规范保障，在 2008 年时，《信息系统安全等级保护基本要求 GB/T22239-2008》正式面世，即为等保 1.0 相应指导标准，在 2019 年，等保 2.0 核心标准 GB-T22239-2019《信息安全技术 网络安全等级保护基本要求》正式发布，标准着正式进入等保 2.0 时代。

(3) 为什么要做等保

从法律要求层面来说，网络安全等级保护是国家信息安全保障基本制度、基本策略、基本方法。《中华人民共和国网络安全法》明确规定信息系统运营、使用单位应当按照网络安全等级保护制度的要求，履行安全保护义务，如果拒不履行，将会受到相应处罚。

从行业要求层面来说，等保已成为许多行业的必需品。很多行业主管单位明确要求从业机构的信息系统要开展等保工作，比如金融、电力、广电、医疗、教育等行业。

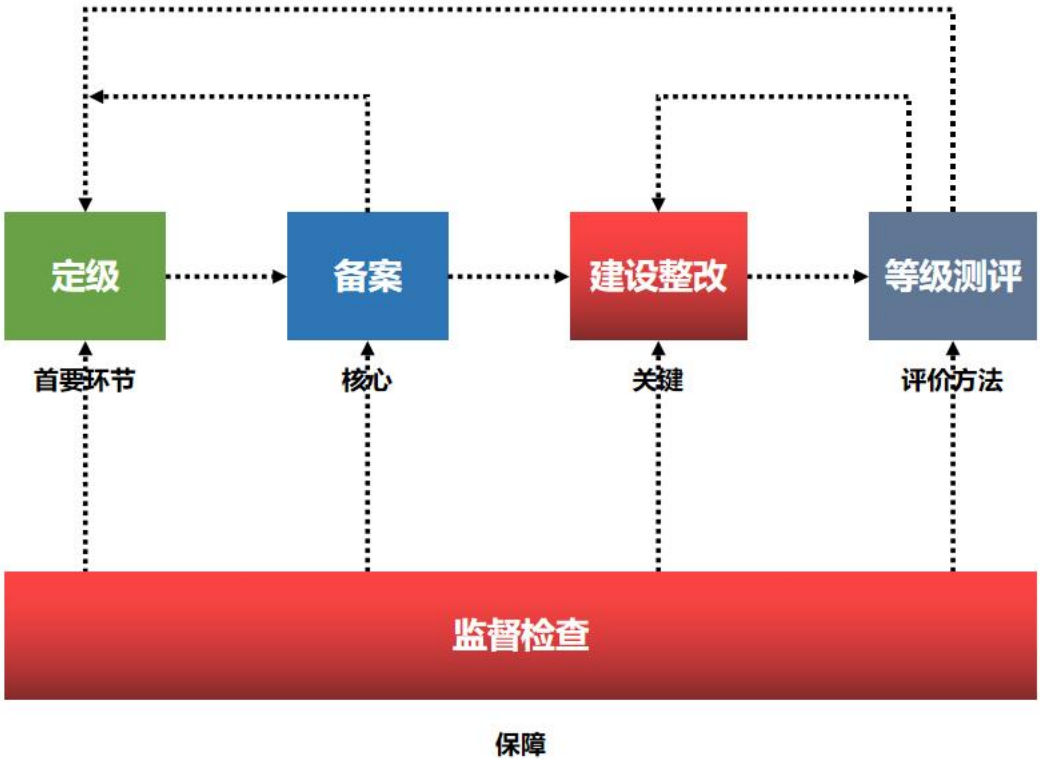
从安全要求层面来说，信息系统运营、使用单位通过开展等保工作可以发现系统内部的安全隐患与不足之处，可通过安全整改提升系统的安全防护能力，降低被

攻击的风险。

(4) 云租户为什么需要单独做等保

根据 “ 谁运营谁负责，谁使用谁负责，谁主管谁负责 ” 的原则，系统的责任主体还是属于网络运营者自己，所以云租户还是得承担相应的网络安全责任。由于天翼云平台本身就已经通过等保，所以在做等保的过程中，云租户无需再关注物理环境和网络环境，只需关本身业务系统合规即可。

(5) 等保 2.0 建设流程



整个等保 2.0 的建设流程分为五个步骤，分别是：

1. 定级：确定定级对象，初步确定安全保护等级，专家评审，主管部门审核、公安机关备案审查

2. 备案：持定级报告和备案表到当地公安机关网安部门进行备案，获取备案证明

3. 建设整改：参照网络安全等级保护相关标准及规范要求，对信息系统进行整改加固。

4. 等级测评：委托具备测评资质的测评机构对信息系统进行等级测评，形成正式的测评报告。

5. 监督检查：向当地公安机关网安部门提交测评报告，配合完成对信息安全

等级保护实施情况的检查。

6. 文档下载

《主机安全使用手册-云等保专区.docx》

《Web 应用防火墙使用手册-云等保专区.docx》

《下一代防火墙使用手册-云等保专区.docx》

《堡垒机使用手册-云等保专区.docx》

《漏洞扫描使用手册-云等保专区.docx》

《日志审计使用手册-云等保专区.docx》

《数据库审计使用手册-云等保专区.docx》

7. 服务协议

《云等保专区服务协议》