# 云等保专区

## 用户使用指南

天翼云科技有限公司

# 目录

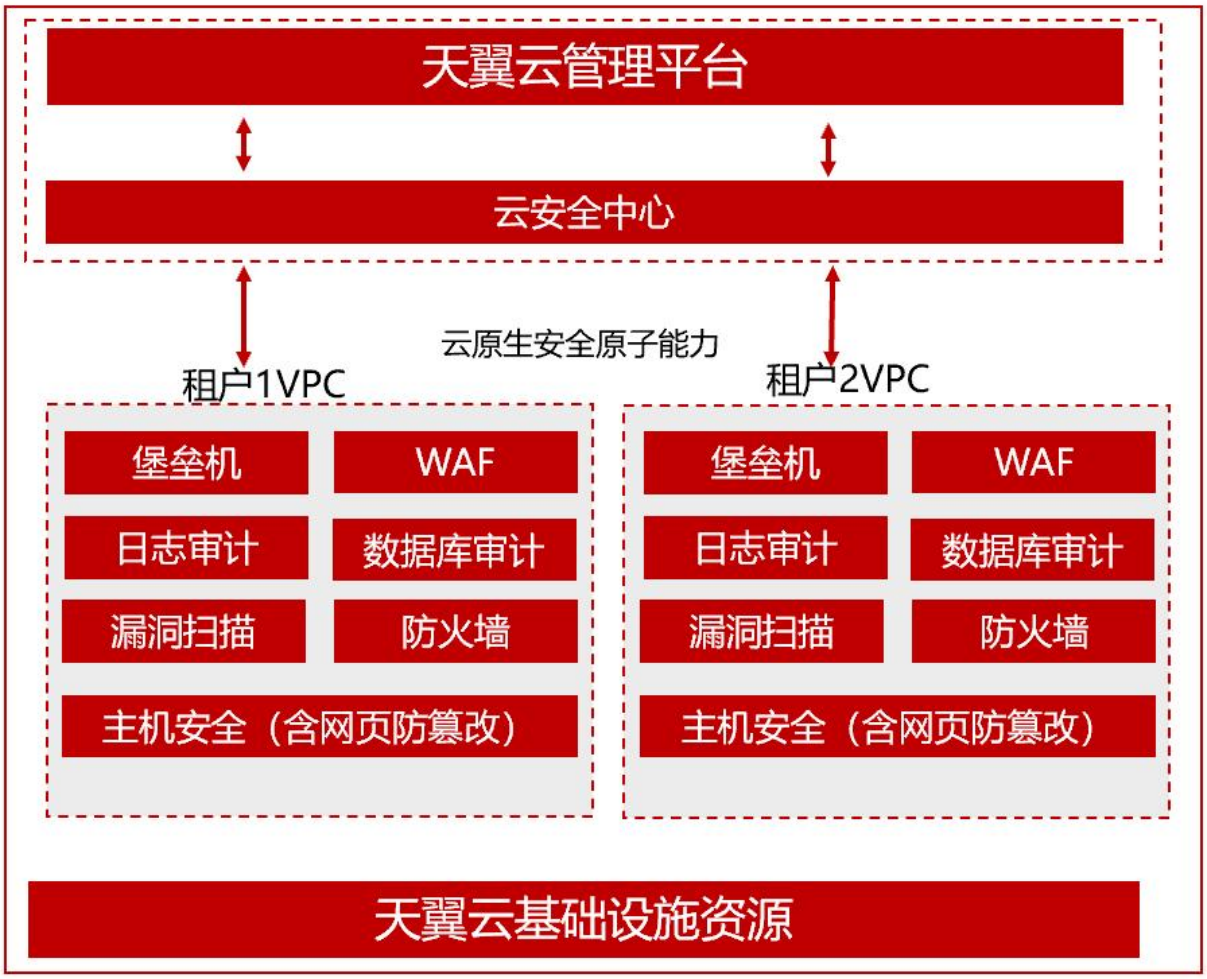
# 1. 产品介绍

## 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，包括云安全中心、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，实现安全原子能力统一管理、统一运营，为用户侧等保合规需求提供便捷下单、自动化部署的能力。

## 1.2. 产品架构



## 1.3. 功能特性

(1)**云安全中心：**云安全中心系统主要包含安全态势、资产中心、风险管理、威胁管理、分析中心、告警管理、编排响应、报表中心、集成配置以及数据源监控等功能。

(2)**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。

(3)**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

(4)**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

(5)**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。

(6)**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。

(7)**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。

(8)**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。

## 1.4. 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。

## 1.5. 应用场景

### 1.5.1. 等保合规场景

**场景特点**

随着《网络安全法》、《信息安全技术网络安全等级保护基本要求》以及各个行业法律法规的发布，用户对于网络安全建设的重视程度日渐提升，等级保护建设逐渐成为了网络安全建设的基线，各行各业的用户都在开始进行等级保护合规建设。

**解决的问题**

云等保专区产品为更好更快捷地帮助用户完成等级保护建设，特地推出等保二级基础版、等保二级高级版、等保三级基础版以及等保三级高级版套餐，用户仅需要根据自己实际合规等级需要，通过勾选对应套餐，就能够轻松通过等保二级、三级测评，满足等保合规要求。

### 1.5.2. 安全加固场景

**场景特点**

用户开通云主机将业务部署完成后，需要对于云上业务进行安全加固防护，会使用到安全产品的能力，例如下一代防护墙的访问控制能力、Web应用防火墙的Web应用攻击防护能力、主机安全的漏洞检测与防护能力等。

**解决的问题**

云等保专区专项推出等保自定义版，能够提供下一代防火墙、Web应用防火墙、日志审计、主机安全、堡垒机、数据库审计以及漏洞扫描等原子能力，用户可根据自己当前云业务网络安全建设的薄弱点以及安全加固防护的需求，进行自主选择需要的安全原子能力进行安全加固建设。

# 1.6. 产品规格

## 1.6.1. 产品套餐说明

| 等保体系 | 等保测评项 | 安全产品名称 | 二级等保基础版 | 二级等保高级版 | 三级等保基础版 | 三级等保高级版 |
|---|---|---|---|---|---|---|
| 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 | 云安全中心 | ✓ | ✓ | ✓ | ✓ |
| | | 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，并在经过充分测试评估后，及时修补漏洞 | 漏洞扫描 | × | × | × | ✓ |
| | | 主机安全 | ✓ | ✓ | ✓ | ✓ |

## 1.6.2. 产品版本规格

| 产品名称 | 版本 | 规格 | 规格说明 |
|---|---|---|---|
| 堡垒机 | v1.0 | 10资产 | 支持10资产管理 |
| | | 20资产 | 支持20资产管理 |
| | | 50资产 | 支持50资产管理 |
| | | 100资产 | 支持100资产管理 |
| | | 200资产 | 支持200资产管理 |
| | | 500资产 | 支持500资产管理 |
| | | 1000资产 | 支持1000资产管理 |
| 数据库审计 | v1.0 | 标准版 | 支持4数据库实例 |
| | | 高级版 | 支持8数据库实例 |
| | | 企业版 | 支持16数据库实例 |
| | v2.0 | 标准版 | 支持4数据库实例 |
| | | 高级版 | 支持8数据库实例 |
| | | 企业版 | 支持16数据库实例 |
| 漏洞扫描 | v1.0 | 10资产 | 支持10个IP地址 |
| | | 20资产 | 支持20个IP地址 |
| | | 50资产 | 支持50个IP地址 |

| 产品名称 | 版本 | 规格 | 规格说明 |
| --- | --- | --- | --- |
| | | 100资产 | 支持100个IP地址 |
| | | 200资产 | 支持200个IP地址 |
| 日志审计 | v1.0 | 10资产 | 支持10个日志源 |
| | | 20资产 | 支持20个日志源 |
| | | 50资产 | 支持50个日志源 |
| | | 100资产 | 支持100个日志源 |
| | | 200资产 | 支持200个日志源 |
| | | 500资产 | 支持500个日志源 |
| 下一代防火墙 | v1.0 | 标准版 | 支持1Gbps |
| | | 高级版 | 支持2Gbps |
| | | 企业版 | 支持4Gbps |
| 云安全中心 | v2.0 | 标准版 | 包含日志分析量为每月50G |
| | | 态势大屏 | 包括安全成果态势、威胁攻击态势大屏 |
| | | 日志分析量 | 默认需购买500G日志分析量，额外购买步长为50G |
| 主机安全 | v1.0 | 标准版 | 支持1个主机 |
| | | 网页防篡改版 | 支持1个主机，提供主机网页防篡改功能 |
| | v2.0 | 旗舰版 | 按照需防护的主机个数购买，提供安全概览、资产管理、入侵检测、漏洞扫描、基线管理功能。 |
| | | 网页防篡改版 | 按照需防护的主机个数购买，提供网页防篡改能力，解决页面篡改、挂马、暗链等网页风险问题。 |
| Web应用防火墙 | v1.0 | 标准版 | 防护10个站点，支持带宽防护200Mb |
| | | 域名扩展包 | 每个扩展包支持10个域名防护 |
| | | 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；<br>单个Web应用防火墙最大支持1000Mb流量，最大可支持16个扩展包。 |
| | v2.0 | 标准版 | 适合中小型网站标准防护 |
| | | 企业版 | 适合大中型网站防护 |
| | | 域名扩展包 | 一个域名扩展包含有：10 个域名防护（含 1 个一级域名） |
| | | 业务扩展包 | 一个业务扩展包包含：1000 QPS |
| | | 规则扩展包 | 一个规则扩展包包含：50 条防护规则（仅支持 IP 黑白名单规则） |

### 1.6.3. 等保服务规格

| 服务项 | 基础包 | 标准包 | 高级包 |
| --- | --- | --- | --- |

| 服务项 | 基础包 | 标准包 | 高级包 |
| --- | --- | --- | --- |
| 1个业务系统服务范围内支持的资产数 | 总资产数2以内 | 总资产数10以内 | 总资产数20以内 |
| 等保定级咨询<br>等保备案咨询<br>差距分析咨询 | 咨询 | 咨询 | 咨询 |
| 调研客户系统技术状况，管理规范情况 | 咨询及评估 | 咨询及评估 | 咨询及评估 |
| 根据合规要求及差距评估，结合客户业务实际需求，提出合规方案 | × | × | 咨询及评估 |
| 提供安全设备上线以及相关系统配置咨询 | × | 咨询 | 咨询 |
| 根据设计方案及合规要求完成安全策略配置咨询 | × | 咨询 | 咨询 |
| 根据差距评估，对客户操作系统进行安全配置加固及安全漏洞补丁加固提供咨询。 | × | × | 咨询 |
| 根据合规要求及差距评估，指导客户网络设备进行安全配置，但不包括设计版本升级 | × | × | 咨询 |
| 数据库安全加固由软件系统提供商负责 | × | × | 咨询 |
| 软件安全加固由软件系统提供商负责 | × | × | 咨询 |

## 1.7. 术语解释

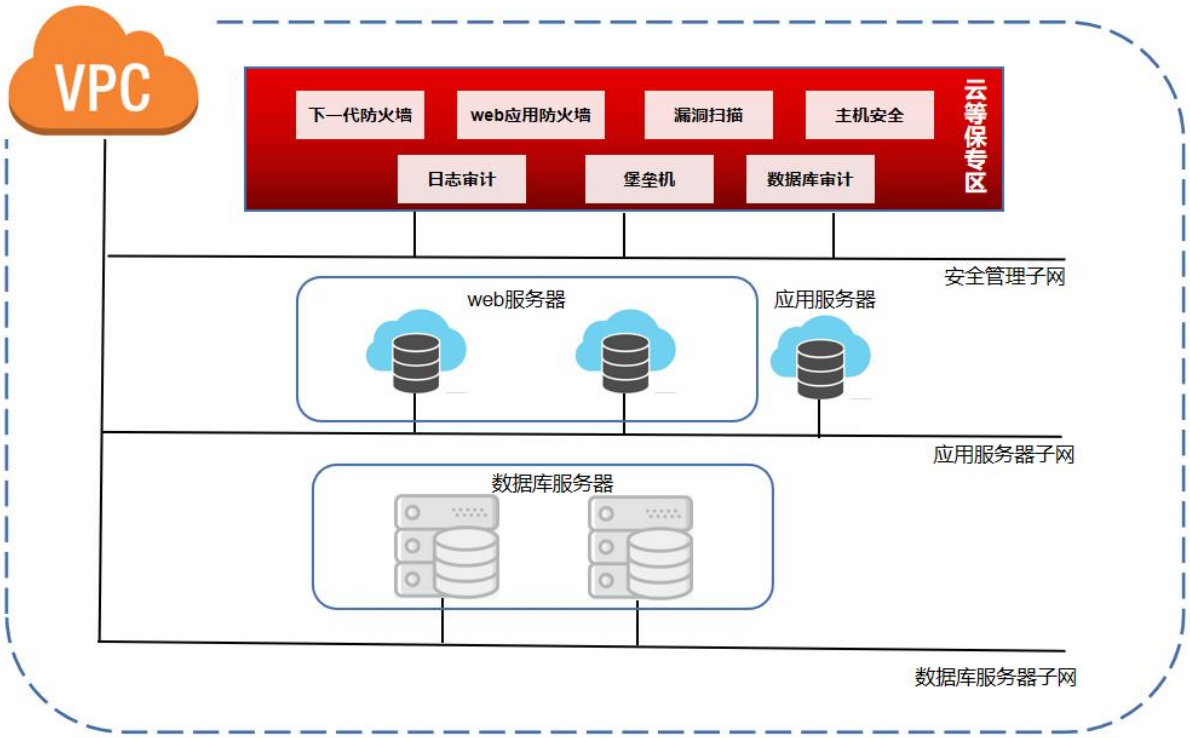
| 术语 | 说明 |
| --- | --- |
| cURL | cURL是一个利用URL语法在命令行下工作的文件传输工具，可用于检测系统是否可以访问目标站点。 |
| Dig | Dig是一个在类Unix命令行模式下查询DNS信息（包括NS记录、A记录、MX记录等）的工具。 |
| 基线核查 | 基线核查是指对主机操作系统、数据库、软件和容器的配置进行安全检测，并提供检测结果说明和加固建议。<br>基线核查可以帮您进行系统安全加固，降低入侵风险并满足安全合规要求。 |
| 漏洞扫描 | 漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利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，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 |

| 术语 | 说明 |
| --- | --- |
| | 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，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。<br>在实体计算机中能够完成的工作在虚拟机中都能够实现。<br>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。 |
| DES | DES（Data Encryption Standard，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。<br>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（Lightweight Directory Access Protocol，是轻量目录访问协议）是互联网上目录服务的通用访问协议。<br>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服务单元的最大尺寸，说明发送方能够接受的有效荷载大小。 |
| SSL | SSL（Secure Sockets Layer，安全套接字协议）及TLS（Transport Layer Security，继任者传输层安全）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，也可以将其称为一种网页后门。<br>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（Simple Network Management Protocol，简单网络管理协议）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（Structured Query Language，结构化查询语言）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。<br>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。 |

## 1.8. 部署拓扑图

在VPC中建立一个安全管理子网，将云等保专区的各个安全原子能力部署在安全管理子网中，便于统一管理。




## 1.9 支持的区域

云等保专区已支持的产品区域如下所示：

| 区域 | 一类节点 | 二类节点 |
| --- | --- | --- |
| 华东地区 | 上海7/华东1/南昌5/上海36/杭州2/杭州7/芜湖4/南京3/南京4/南京5/九江 | 芜湖/南昌/上海4/杭州/苏州 |
| 华南地区 | 华南2/郴州2/长沙42/福州25/佛山3/南宁23/武汉41/海口2/福州4/厦门3/广州6/南宁2/武汉3/武汉4/长沙3 | 福州1/深圳/广州4/南宁/武汉2/长沙2/海口 |
| 西北地区 | 乌鲁木齐27/乌鲁木齐7/兰州2/庆阳2/中卫5/西宁2/西安3/西安5//西安7 | 兰州/西宁/西安2/乌鲁木齐 |
| 西南地区 | 西南1/拉萨3/西南2-贵州/昆明2/成都4/重庆2/贵州3 | 重庆/贵州1/成都3/昆明 |
| 北方地区 | 北京5/晋中/郑州5/华北2/青岛20/太原4/呼和浩特3/石家庄20/辽阳1/内蒙6 | 郑州/华北/内蒙3/青岛/太原 |

# 2. 计费说明

## 2.1. 计费方式

### 2.1.1. 计费模式

云等保专区产品采用包周期计费模式，起售周期为3个月。

支持续订，续订周期为1个月起。

### 2.1.2. 计费项

- 云等保专区根据产品类型、产品版本、产品数量、产品规格进行收费。

  说明：
  “二类节点”区域还需要单独购买不同原子能力配置的云主机，并合计原子能力一起计费，统一下单。

- 云等保专区提供等保固定套餐，用户可以根据自身诉求选择不同版本套餐；也可以根据实际情况，选择自定义版，自行搭配进行选择。

| 套餐 | 说明 |
| --- | --- |
| 固定套餐 | 提供等保二级基础版、等保二级高级版、等保三级基础版以及等保三级高级版固定套餐。<br>说明：<br>选择套餐后，支持更改原子能力数量、对应产品规格，不支持更改购买的原子能力类型。 |
| 自定义套餐 | 若用户需要购买单个原子能力，可以选择等保自定义版，根据实际需要进行原子能力类型以及规格进行勾选。 |

### 2.1.3. 产品价格

**云等保专区原子能力**

| 产品名称 | 版本 | 规格 | 规格说明 | 标准价格（元/月） | 标准价格（元/年） | 优惠活动 |
| --- | --- | --- | --- | --- | --- | --- |
| 堡垒机 | v1.0 | 10资产 | 支持10资产管理 | 1066 | 12791 | - |
| | | 20资产 | 支持20资产管理 | 1523 | 18273 | - |

| 产品名称 | 版本 | 规格 | 规格说明 | 标准价格（元/月） | 标准价格（元/年） | 优惠活动 |
|---|---|---|---|---|---|---|
| | | 50资产 | 支持50资产管理 | 3006 | 36069 | - |
| | | 100资产 | 支持100资产管理 | 4294 | 51527 | - |
| | | 200资产 | 支持200资产管理 | 6134 | 73610 | - |
| | | 500资产 | 支持500资产管理 | 11599 | 139191 | - |
| | | 1000资产 | 支持1000资产管理 | 16570 | 198844 | - |
| 数据库审计 | v1.0 | 标准版 | 支持4数据库实例 | 3333 | 40000 | - |
| | | 高级版 | 支持8数据库实例 | 6250 | 75000 | - |
| | | 企业版 | 支持16数据库实例 | 11667 | 140000 | - |
| | v2.0 | 标准版 | 支持4数据库实例 | 3333 | 40000 | - |
| | | 高级版 | 支持8数据库实例 | 6250 | 75000 | - |
| | | 企业版 | 支持16数据库实例 | 11667 | 140000 | - |
| 漏洞扫描 | v1.0 | 10资产 | 支持10个IP地址 | 937 | 11248 | - |
| | | 20资产 | 支持20个IP地址 | 1339 | 16068 | - |
| | | 50资产 | 支持50个IP地址 | 3493 | 41915 | - |
| | | 100资产 | 支持100个IP地址 | 4990 | 59878 | - |
| | | 200资产 | 支持200个IP地址 | 10530 | 126358 | - |
| 日志审计 | v1.0 | 10资产 | 支持10个日志源 | 1107 | 13289 | - |
| | | 20资产 | 支持20个日志源 | 1582 | 18984 | - |
| | | 50资产 | 支持50个日志源 | 3219 | 38633 | - |
| | | 100资产 | 支持100个日志源 | 4599 | 55190 | - |
| | | 200资产 | 支持200个日志源 | 9606 | 115267 | - |
| | | 500资产 | 支持500个日志源 | 13722 | 164667 | - |
| 下一代防火墙 | v1.0 | 标准版 | 支持1Gbps | 1879 | 22546 | - |
| | | 高级版 | 支持2Gbps | 3406 | 40872 | - |
| | | 企业版 | 支持4Gbps | 5673 | 68079 | - |
| 云安全中心 | v2.0 | 标准版 | 包含日志分析量为每月50G | 1600 | 19200 | 针对一次性付费客户，享受一年及以上8.5折优惠。 |
| | | 态势大屏 | 包括安全成果态势、威胁攻击态势大屏 | 4500 | 54000 | |

| 产品名称 | 版本 | 规格 | 规格说明 | 标准价格（元/月） | 标准价格（元/年） | 优惠活动 |
|---|---|---|---|---|---|---|
| | | 日志分析量 | 默认需购买500G日志分析量，额外购买步长为50G | 225 / 500GB | 2700 / 500GB | |
| 主机安全 | v1.0 | 标准版 | 按照需防护的主机个数购买，提供安全概览、资产管理、入侵检测、漏洞扫描、基线管理功能。 | 167 | 2000 | - |
| | | 网页防篡改版 | 按照需防护的主机个数购买，提供网页防篡改能力，解决页面篡改、挂马、暗链等网页风险问题。 | 695 | 8340 | - |
| | v2.0 | 旗舰版 | 按照需防护的主机个数购买，提供安全概览、资产管理、入侵检测、漏洞扫描、基线管理功能。 | 180 | 2160 | 包年订购折扣：针对一次性包年付费服务，包年优惠价格为1年85折、2年7折、3年5折。 |
| | | 网页防篡改版 | 按照需防护的主机个数购买，提供网页防篡改能力，解决页面篡改、挂马、暗链等网页风险问题。 | 980 | 11760 | |
| Web应用防火墙 | v1.0 | 标准版 | 防护10个站点，支持带宽防护200Mb | 2837 | 34049 | - |
| | | 域名扩展包 | 每个扩展包支持10个域名防护 | 500 | 5998 | - |
| | | 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；<br>单个Web应用防火墙最大支持1000Mb流量，最大可支持16个扩展包。 | 500 | 5998 | - |
| | v2.0 | 标准版 | 适合中小型网站标准防护 | 3880 | 46560 | **包年订购折扣：**<br>针对一次性包年付费服务，包年优惠价格为1年85折、2年7折、3年5折。<br><br>**优惠折扣：**<br>Web应用防火墙v2.0订购享受8折优惠。<br><br>说明：<br>包年订购折扣与优惠折扣不能同享，取低者计算。 |
| | | 标准版-域名扩展包 | 一个域名扩展包含有：10 个域名防护（含 1 个一级域名） | 600 | 7200 | |
| | | 标准版-业务扩展包 | 一个业务扩展包包含：1000 QPS | 1000 | 12000 | |
| | | 标准版-规则扩展包 | 一个规则扩展包包含：50 条防护规则（仅支持 IP 黑白名单规则） | 70 | 840 | |
| | | 企业版 | 适合大中型网站防护 | 9800 | 117600 | |
| | | 企业版-域名扩展包 | 一个域名扩展包含有：10 个域名防护（含 1 个一级域名） | 1000 | 12000 | |
| | | 企业版-业务扩展包 | 一个业务扩展包包含：1000 QPS | 2000 | 24000 | |
| | | 企业版-规则扩展包 | 一个规则扩展包包含：50 条防护规则（仅支持 IP 黑白名单规则） | 70 | 840 | |

### 等保服务包

| 服务规格 | 价格（元/次/业务系统） |
| --- | --- |
| 等保服务基础包 | 1000 |
| 等保服务标准包 | 5000 |
| 等保服务高级包 | 50000 |

## 2.2. 续订

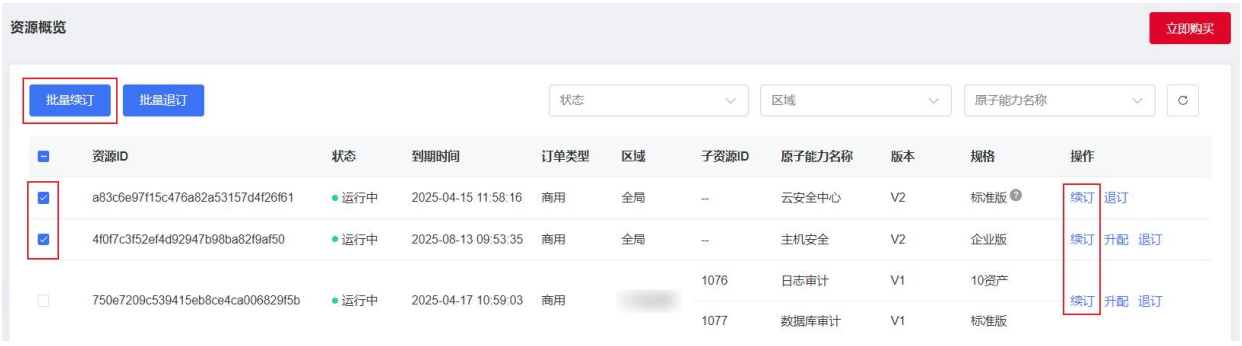
### 续订说明

- 订单到期后，若没有续订，将不能继续使用订单中的服务，建议您提前进行续订。
- 续订“二类节点”区域的资源时，需要同时对原子能力配置的云主机进行续费，云主机合计原子能力一起计费，统一下单。

### 续订步骤

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在页面左侧导航栏单击“产品服务列表”图标，选择“安全 > 云等保专区”。
4. 在“资源概览”中找到需要续订的资源。
5. 点击操作列的“续订”。

   或勾选多个需要续订的资源，单击列表上方的“批量续订”进行批量操作。




6. 在续订页面中，选择“购买时长”。

说明：

- 续订周期为1个月起，最长可续订3年。
- 在“二类节点”区域购买的v1.0版本资源，续订时需要同时对原子能力配置的云主机进行续费，云主机合计原子能力一起计费，统一下单。


7. 勾选“我已阅读，理解并接受《云等保专区服务协议》”后，单击“立即购买”后即可进行续订。

## 2.3. 退订

### 退订说明

购买云等保专区后，您可以随时退订，成功退订后将进行退款。

注意：
云等保专区支持七天无理由退订，七天无理由退订仅限于新购资源的情形，若新购资源在7天内进行了续订或变更（包含但不限于规格升级、扩容、操作系统变更、按需计费转包周期），退订时按非七天无理由退订处理，需要收取相应的使用费用和退订手续费，且不退还代金券及优惠券，更多详情请阅读天翼云“退订规则说明”。

### 退订云等保专区

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。

3. 在页面左侧导航栏单击“产品服务列表”图标，选择“安全 > 云等保专区”。

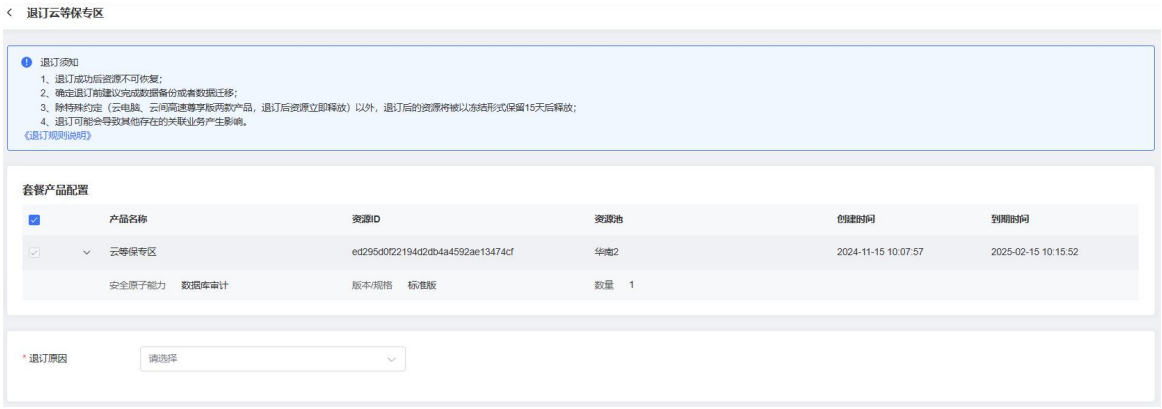
4. 在“资源概览”中找到需要退订的资源。

5. 点击操作列的“退订”。

   或勾选多个需要退订的资源，单击列表上方的“批量退订”进行批量操作。

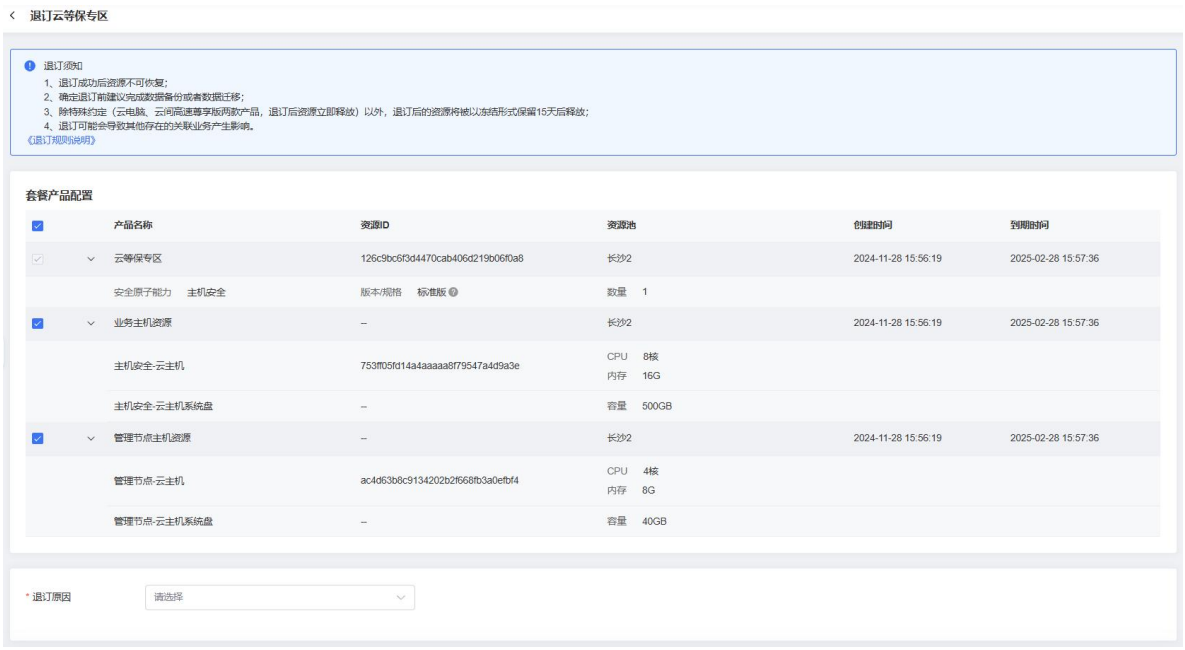

6. 在退订页面，确认需要退订的资源，并选择退订原因。

   - 退订“一类节点”区域的资源：




   - 退订“二类节点”区域的资源：

> 说明：
> 在“二类节点”区域购买的资源，退订时可选择同时退订相应的云主机。




7. 单击“退订”，在弹出的提示框中，单击“确定”后即可进行退订。

## 2.4. 升级与扩容

### 约束限制

各产品升配限制如下：

| 产品 | 升配说明 |
| --- | --- |
| 云安全中心 | 云安全中心不支持在云等保专区控制台升配，若需要升配，请参见云安全中心用户使用指南。 |
| 主机安全 | 主机安全v1.0当前不支持升配，可在同一VPC下购买新的配额。 |
| Web应用防火墙 | ● 若购买时未购买扩展包资源，则升配时不能对扩展包的数量进行升配。<br>● 若一个订单包含了多个WAF实例，则只能同时对该订单中的WAF实例进行升配，且只能升配到相同的配额。 |
| 云下一代防火墙 | 仅支持升配版本，不支持对数量进行调整。 |
| 堡垒机 | 仅支持升配规格，不支持对数量进行调整。 |
| 漏洞扫描 | 仅支持升配规格，不支持对数量进行调整。 |
| 日志审计 | 日志审计暂不支持升配。 |
| 数据库审计 | 仅支持升配版本，不支持对数量进行调整。 |

### 操作步骤

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在页面左侧导航栏单击“产品服务列表”图标，选择“安全 > 云等保专区”。
4. 在“资源概览”中找到需要升配的资源，点击操作列的“升配”。


5. 在升配页面中，选择套餐产品购买的规格/版本。
6. 确认配置信息无误后，阅读《云等保专区服务协议》并勾选“我已阅读，理解并接受《云等保专区服务协议》”，点击“确认”进行升配。

# 3. 快速入门

## 3.1. 购买云等保专区

### 购买方式

云等保为套餐产品组合下单模式，用户可根据需要选购所需组合套餐。

根据所选购买区域，购买步骤略有不同。

### 注意事项

- 本产品一经订购，不支持降级，请谨慎选择产品套餐和规格。
- 本产品需要绑定弹性IP进行管理，成功开通后请勿解绑该弹性IP。
- 同一账号只能开通一个云安全中心实例。

### 购买步骤（一类节点区域）

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在页面左侧导航栏单击“产品服务列表”图标，选择“安全 > 云等保专区”。
4. 单击“立即购买”，进入云等保专区产品购买页面。
5. 配置基础信息。选择购买的区域、虚拟私有云、子网、可用区和CPU分类。

注意：

- 购买时需要单独创建一个安全子网（至少保留9个以上可用IP地址）用于部署云等保专区，不能与业务主机所在子网相同，否则可能会存在无法交付的问题。
- 若需要开启IPv6，请确保所选子网已开启IPv6功能。


6. 选择主套餐规格。


7. 选择套餐产品购买的规格/版本、数量，以及是否购买资源扩展包及资源扩展包数量。


8. 选择购买时长。

   云等保专区仅支持“包年包月”计费模式，最低购买时长为3个月。

9. 确认配置信息无误后，阅读《云等保专区服务协议》并勾选“我已阅读，理解并接受《云等保专区服务协议》”，点击“立即购买”下单。

**购买步骤（二类节点区域）**

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在页面左侧导航栏单击“产品服务列表”图标，选择“安全 > 云等保专区”。
4. 单击“立即购买”，进入云等保专区产品购买页面。
5. 配置基础信息。选择购买的区域、虚拟私有云、子网、弹性IP、可用区和CPU分类。

注意：

- 购买时需要单独创建一个安全子网（至少保留9个以上可用IP地址）用于部署云等保专区，不能与业务主机所在子网相同，否则可能会存在无法交付的问题。
- 若需要开启IPv6，请确保所选子网已开启IPv6功能。
- 仅“二类节点”区域需要在此处配置弹性IP。成功开通后请勿解绑该弹性IP，若误解绑了，请重新绑定原有EIP。

6. 选择主套餐规格。


7. 选择套餐产品购买的规格/版本、数量，以及是否购买资源扩展包及资源扩展包数量。

说明：

- “二类节点”区域还需要单独购买不同原子能力配置的云主机，并合计原子能力一起计费，统一下单。
- 云主机数量和系统盘大小为系统默认选择，不支持修改；部分原子能力还需要数据盘，数据盘支持修改，但不能低于系统限制的最小值，具体限制请在购买时以购买页面的信息为准。


8. 查看云等保专区管理节点的云主机规格及价格。

说明：

- “二类节点”区域还需要单独购买云等保专区管理节点的云主机资源，并合计原子能力一起计费，统一下单。
- 云等保专区管理节点的云主机资源为系统默认选择，不支持修改。
- 该管理节点将为该账户下同一VPC中所有云等保服务提供访问服务，在服务退订完之前，请勿删除，否则将无法访问该服务。当VPC下所有服务均退订后，请尽快删除该管理节点，避免持续收费。


9. 选择购买时长。

   云等保专区仅支持“包年包月”计费模式，最低购买时长为3个月。

10. 确认配置信息无误后，阅读《云等保专区服务协议》并勾选“我已阅读，理解并接受《云等保专区服务协议》”，单击“立即购买”下单。

## 3.2. 购买等保服务包

### 购买方式

云等保服务包为一次性付费服务，用户可根据需要选购所需规格。

### 服务说明

- 本产品提供等保定级和差距评估服务、等保安全加固方案服务。
- 本产品不提供等保测评服务，等保测试服务需用户从测评机构处购买。

### 注意事项

云等保服务包不支持续订、退订。

### 操作步骤

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在页面左侧导航栏单击“产品服务列表”图标，选择“安全 > 云等保专区”。

4. 单击“立即购买”，进入云等保专区产品购买页面。

5. 在等保自定义版中勾选“等保服务包”。


6. 选择等保服务规格和业务系统数量。


7. 填写联系方式。订单生成后，天翼云安全专家会与您取得联系。


8. 确认配置信息无误后，阅读《云等保专区服务协议》并勾选“我已阅读，理解并接受《云等保专区服务协议》”，点击“立即购买”下单。

# 4. 用户指南

## 4.1. 上线配置概览

云等保专区整合了多个原子能力，部分原子能力需要进行安装配置后，才能正常使用。

| 原子能力 | 安装内容及步骤 |
| --- | --- |
| 主机安全v1.0 | Agent下载安装 |
| | 资产管理配置 |
| | 安全策略编辑 |
| | 日志查看 |
| Web应用防火墙v1.0 | 绑定弹性IP |
| | 全局配置 |
| | 添加站点 |
| | 配置策略 |
| | 验证URL |
| 下一代防火墙v1.0 | 绑定弹性IP |
| | 配置子网路由 |
| | 设置安全策略 |
| | 安全日志查看 |
| 堡垒机v1.0 | 绑定弹性IP |
| | 创建部门 |
| | 创建用户 |
| | 创建主机 |
| | 创建运维规则 |
| | 审计规则设置 |
| | 数据归档设置 |
| 漏洞扫描v1.0 | 资产管理 |
| | 扫描策略设置 |
| | 创建扫描任务 |
| | 扫描报告查看 |
| 日志审计v1.0 | 设置日志上传 |
| | 添加资产 |
| | 查询自查信息 |

| 原子能力 | 安装内容及步骤 |
| --- | --- |
| | 创建解决方案包 |
| | 订阅告警 |
| | 查看审计结果 |
| 数据库审计v1.0 | 安装Agent |
| | 添加资产 |
| | 配置规则 |
| | 订阅报表和告警 |

## 4.2. 资源概览

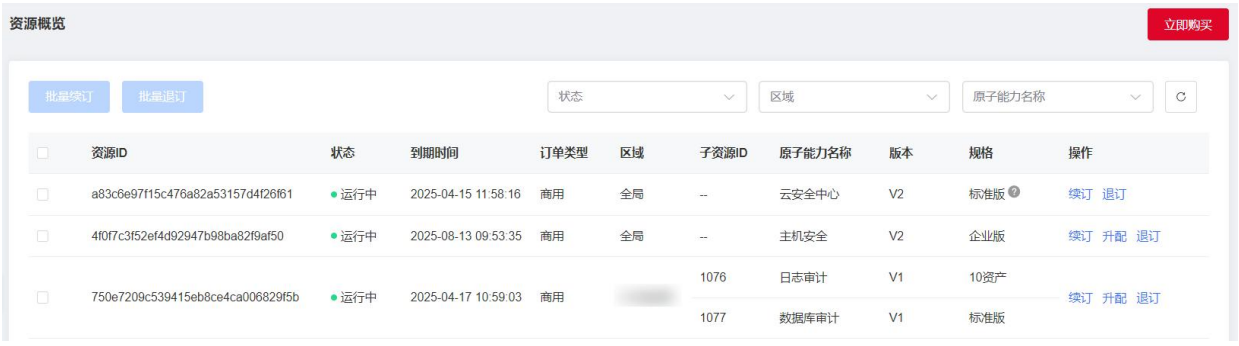
通过云等保专区的资源概览页面，可以查看当前账号下已经形成的订单状态、订单详情，对订单执行续订、退订操作。

### 前提条件

已购买云等保专区。

### 查看资源概览

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云等保专区”，进入云等保专区资源概览页面。




4. 在资源概览页面，查看如下信息。

| 功能 | 描述 |
| --- | --- |
| 资源ID | 主资源的资源ID。 |

| 功能 | 描述 |
| --- | --- |
| 状态 | 主资源的状态，包括开通中、运行中、已退订、部署失败、已过期。 |
| 到期时间 | 资源的到期时间。 |
| 订单类型 | 在控制台上购买的订单，类型为“商用”。 |
| 区域 | 资源所在区域。 |
| 子资源ID | 若一个订单关联了多个原子能力，则每个原子能力通过子资源ID进行标识。 |
| 原子能力名称 | 订单包含的原子能力的名称。 |
| 版本 | 订单包含的原子能力的版本。 |
| 规格 | 订单包含的原子能力的规格。 |

**资源管理**

用户可以根据自身建设需求对资源订单进行管理，包括续订、退订。

## 4.3. 实例资源管理

### 4.3.1. 获取VNC地址

在“一类节点”区域购买的v1.0资源，若用户需要连接原子能力资源配置的云主机，可通过“获取VNC”，获取VNC地址进行远程连接。

**约束限制**

仅“一类节点”区域购买的v1.0资源支持在云等保专区控制台获取VNC地址。

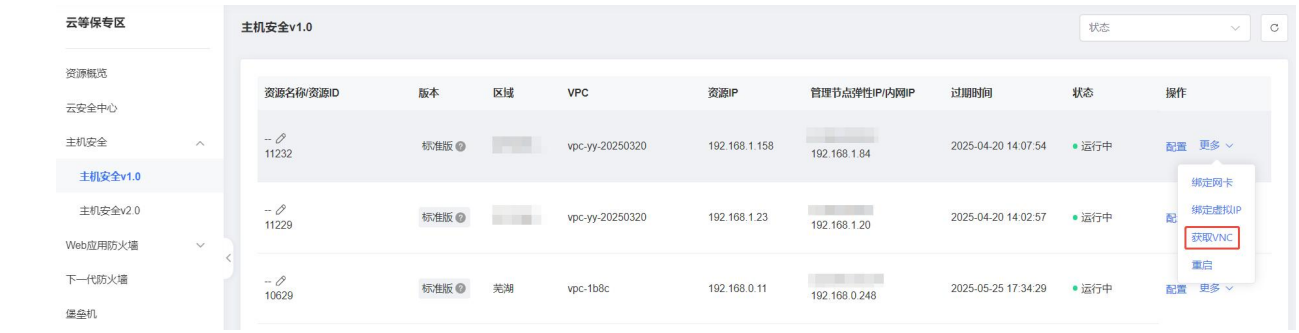
**前提条件**

已购买对应原子能力资源，且资源状态为“运行中”。

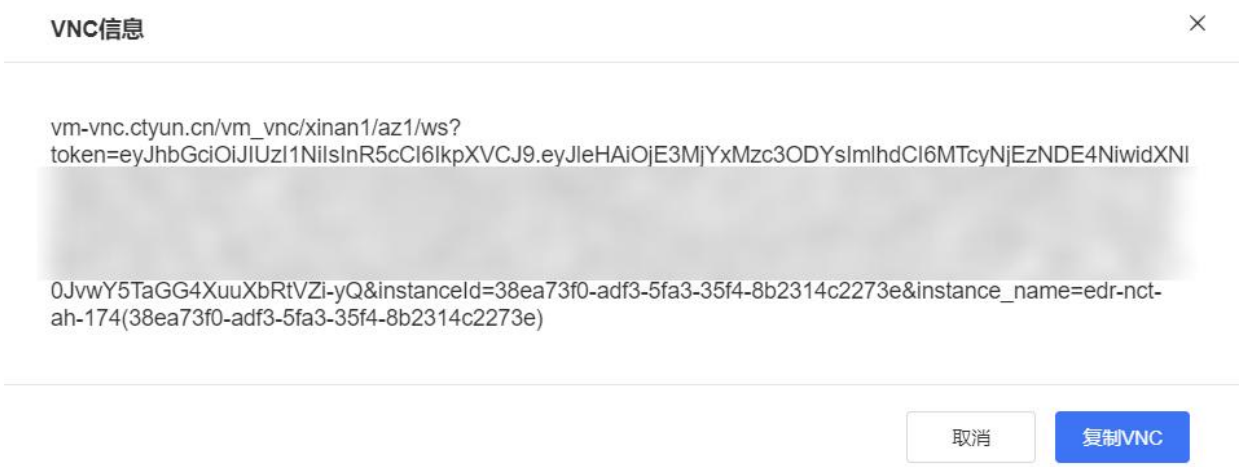
**获取VNC地址**

以下以“主机安全v1.0”为例，介绍如何获取云主机的VNC地址。

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“主机安全 > 主机安全v1.0”，进入云等保专区的主机安全v1.0资源页面。
3. 在目标资源的操作列，单击“更多 > 获取VNC”。




4. 在弹出的“VNC信息”窗口中，单击“复制VNC”。




### 远程连接

1. 在本地计算机上安装VNC客户端软件或通过在线的VNC连接工具（例如https://novnc.com/noVNC/vnc.html）。
2. 打开VNC软件，在连接界面中输入获取的VNC地址。
3. 点击连接按钮后，VNC客户端会尝试与远程计算机建立连接。

## 4.3.2. 重启资源

### 约束限制

仅购买的v1.0版本资源支持在云等保专区控制台执行重启操作。

### 注意事项

重启会导致服务中断，且重启过程中无法执行其他操作，请在业务空闲时进行重启。

### 前提条件

已购买对应原子能力资源，且资源状态为“运行中”。

### 操作步骤

以下以“Web应用防火墙v1.0”为例，介绍如何重启各原子能力资源。

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“Web应用防火墙 > Web应用防火墙v1.0”，进入云等保专区的Web应用防火墙v1.0资源页面。
3. 在目标资源的操作列，单击“更多 > 重启”。


4. 在弹出的提示框中，单击“确定”，资源状态变更为“重启中”，待状态变更为“运行中”时，表示重启完成。

## 4.4. 云安全中心

云安全中心是专为云环境设计的综合性SaaS化安全管理平台，它具备实时监测、防御和分析安全威胁的能力，通过提供一体化的安全运营解决方案，助力用户实现云安全的全面管理和控制，降低用户的安全风险。

在云等保专区控制台购买云安全中心资源后，即可进入云安全中心控制台，接入安全产品日志，云安全中心能通过接入的日志内容进行威胁建模，完成各类安全告警的生成，辅助您进行安全处置，实现安全运营。

### 前提条件

已购买云安全中心资源，且资源状态为“运行中”。

### 进入云安全中心控制台

方式一：

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在产品服务列表页，选择“安全 > 云等保专区”，进入云等保专区控制台。
4. 在左侧导航栏，选择“云安全中心”，跳转到云安全中心控制台。

方式二：

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在产品服务列表页，选择“安全 > 云安全中心”，进入云安全中心控制台。

**使用云安全中心**

请参见《云等保专区-云安全中心 v2.0 用户指南》。

## 4.5. 主机安全

### 4.5.1. 主机安全v1.0

主机安全v1.0（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。

**功能介绍**

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

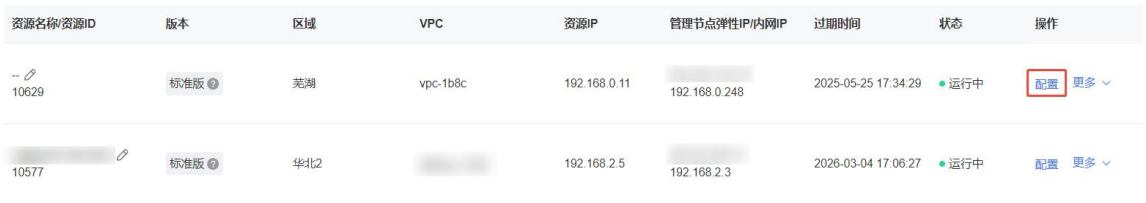
EDR 通过流量画像的流量全景图，展示内网所有流量和主机间通信关系，梳理通 信逻辑，以全局视角对策略进行规划，便于用户第一时间发现威胁，一键清除威 胁。

(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。

**进入控制台**

1. 登录云等保专区控制台。
2. 在左侧导航选择“主机安全 > 主机安全v1.0”，进入主机安全v1.0资源列表页面。




3. 单击目标资源操作列的“配置”，跳转到主机安全v1.0控制台。

**使用主机安全v1.0**

了解更多主机安全v1.0相关操作内容，请下载阅读《云等保专区-主机安全 v1.0 用户指南》。

#### 4.5.2. 主机安全v2.0

主机安全v2.0版本由服务器安全卫士（原生版）提供服务。

**进入控制台**

方式一：

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在产品服务列表页，选择“安全 > 云等保专区”，进入云等保专区控制台。
4. 在左侧导航栏，选择“主机安全 > 主机安全v2.0”，跳转到服务器安全卫士（原生版）控制台。

方式二：

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在产品服务列表页，选择“安全 > 服务器安全卫士（原生版）”，进入服务器安全卫士（原生版）控制台。

**使用主机安全v2.0**

请参见《云等保专区-主机安全 v2.0 用户指南》。

## 4.6. Web 应用防火墙

### 4.6.1. Web应用防火墙v1.0

#### 4.6.1.1. 操作指导

Web应用防火墙v1.0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。

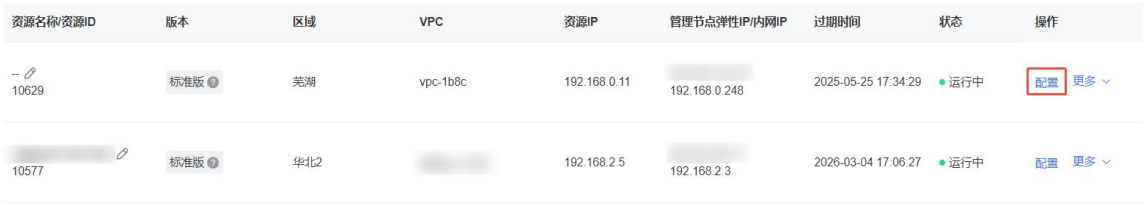
**功能介绍**

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。<br>● 跨站脚本攻击：XSS。<br>● 通用攻击：HTTP请求走私、HTTP响应分割、Session-Fixation等。<br>● 恶意软件：代码上传、Webshell后门、其他木马等。<br>● 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。<br>● 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。<br>● 爬虫攻击：恶意网络爬虫，百度、Google、Yahoo等搜索引擎爬虫。<br>● 第三方组件漏洞：Web容器漏洞、开源CMS漏洞、Web服务器插件漏洞。<br>● 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。<br>● 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。<br>● 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。<br>● 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。<br>● 服务器隐藏：可删除服务器响应头信息。<br>● 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。<br>● 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。<br>● 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。<br>● 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）。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。<br>可选择SSL/TLS协议版本。<br>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。<br>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。<br>记录服务器响应头信息、响应内容。<br>分析访问量最大的URL、IP地址、文件类型等。 |

### 进入控制台

1. 登录云等保专区控制台。
2. 在左侧导航选择“Web应用防火墙 > Web应用防火墙v1.0”，进入Web应用防火墙v1.0资源列表页面。




3. 单击目标资源操作列的“配置”，跳转到Web应用防火墙v1.0控制台。

### 使用Web应用防火墙v1.0

了解更多Web应用防火墙v1.0相关操作内容，请下载阅读《云等保专区-Web应用防火墙v1.0 用户指南》。

## 4.6.1.2. 绑定网卡

开通Web应用防火墙原子能力时，对应原子能力配置的云主机默认只有一张网卡，该网卡为管理口网卡。为了承载业务流量，需要为Web应用防火墙对应的云主机添加新的弹性网卡作为业务流量通道。具体绑定的网卡数量根据实际业务网络规划而定。

### 前提条件

已购买Web应用防火墙资源，且资源状态为“运行中”。

### 操作步骤

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“Web应用防火墙”，进入云等保专区的Web应用防火墙资源页面。
3. 在目标资源的操作列，单击“更多 > 绑定网卡”。

4. 绑定网卡。

根据资源所在区域，绑定网卡的步骤略有不同。

**一类节点区域：**

a. 在弹出的“绑定弹性网卡”窗口中，上方展示当前资源已有网卡，在下方列表中选择需要绑定的网卡。

若没有可绑定的网卡，单击“创建弹性网卡”，创建一个新的网卡。


b. 选择网卡后，单击“确定”，完成绑定。

**二类节点区域：**

单击“绑定网卡”后，会进入对应云主机详情页面。在该页面为云主机绑定网卡。

5. 重启云主机。

当绑定网卡后，需要重启云主机资源使绑定的网卡生效。

> 注意：
> 重启会导致服务中断，且重启过程中无法执行其他操作，请在业务空闲时进行重启。

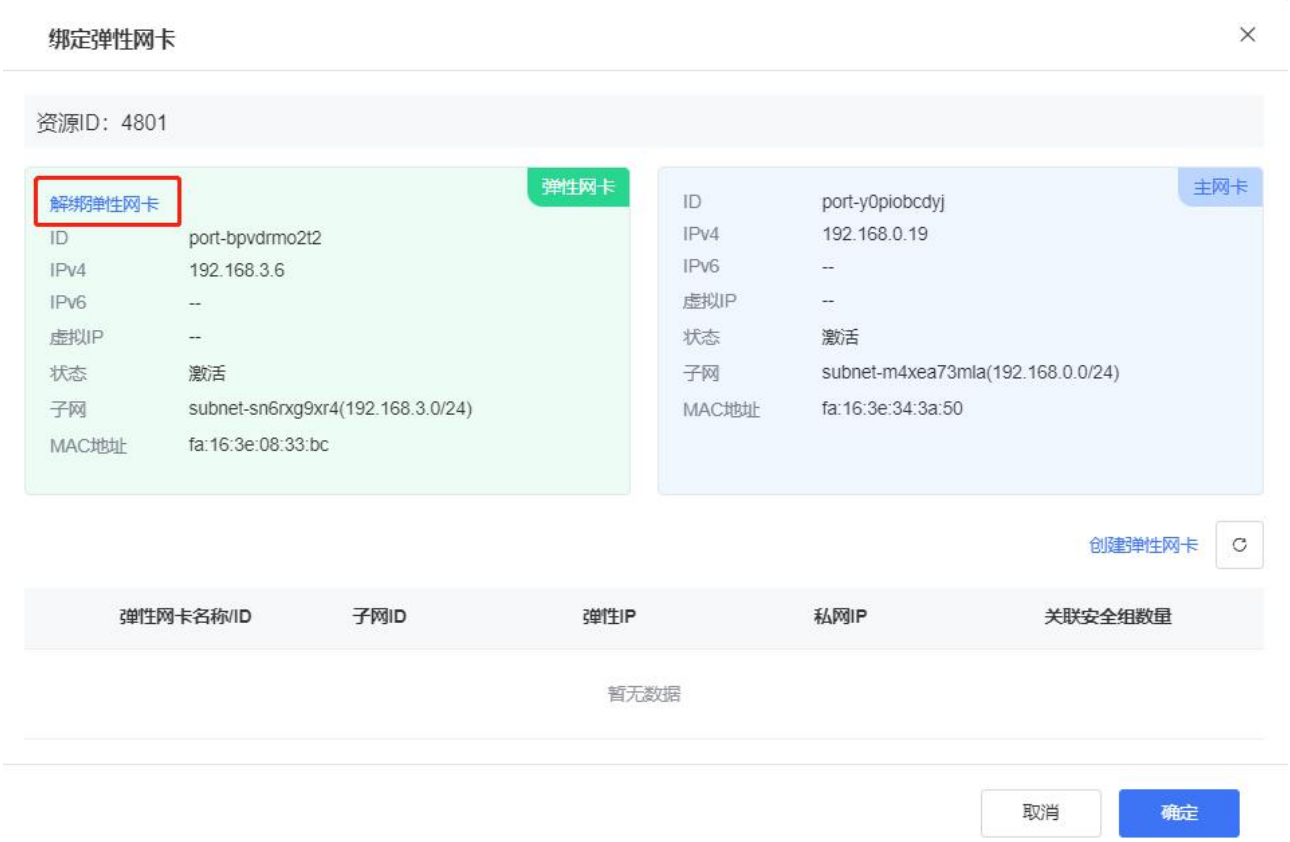
a. 在目标资源的操作列，单击“更多 > 重启”，重启云主机。


b. 在弹出的提示框中，单击“确定”，资源状态变更为“重启中”，待状态变更为“运行中”时，表示重启完成。

> 说明：
> 若重启失败，可再次单击“更多 > 重启”重试。

**相关操作**

若需要解绑网卡，在绑定弹性网卡窗口中，在上方已绑定的网卡模块，单击“解绑弹性网卡”。




### 4.6.1.3. 绑定虚拟IP

## 前提条件

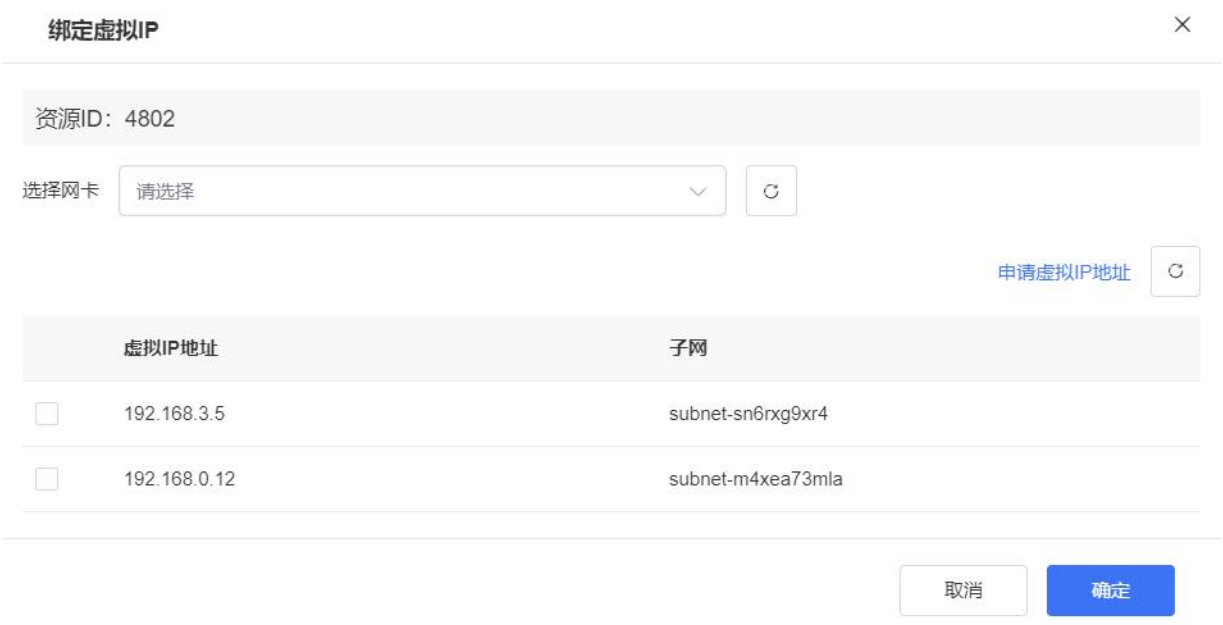
已为Web应用防火墙资源绑定网卡。

## 操作步骤

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“Web应用防火墙”，进入云等保专区的Web应用防火墙资源页面。
3. 在目标资源的操作列，单击“更多 > 绑定虚拟IP”，为网卡绑定虚拟IP。


4. 在弹出的“绑定虚拟IP”窗口中，通过“选择网卡”下拉框中选择一个网卡，在下方列表中选择一个虚拟IP地址。

   若没有可选的虚拟IP地址，单击“申请虚拟IP地址”，创建一个新的虚拟IP地址。




5. 选择完成后，单击“确定”，完成绑定。

### 4.6.1.4. 绑定弹性IP

将用户业务弹性公网IP绑定在Web应用防火墙业务网卡上，从而将用户业务流量接入Web应用防火墙。

**操作步骤**

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“Web应用防火墙”，进入云等保专区的Web应用防火墙资源页面。
3. 在目标资源的操作列，单击“绑定弹性IP”，为资源绑定弹性IP。


4. 在弹出的“绑定弹性IP”窗口中，通过“弹性网卡”下拉框中选择一个网卡，在下方列表中选择一个弹性公网IP地址。

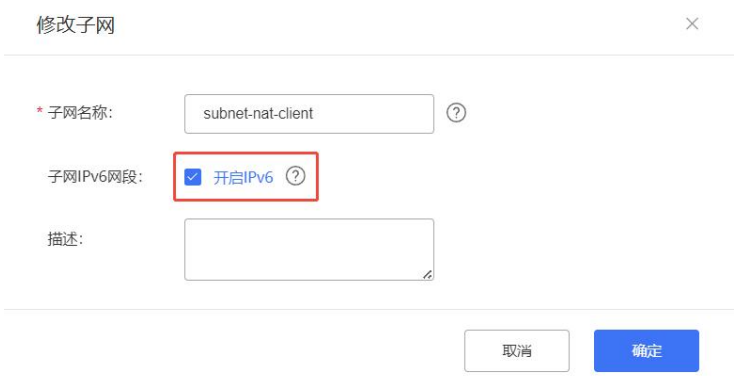
   若没有可绑定的弹性IP，单击“配置弹性IP”，进入创建弹性IP页面，创建一个新的弹性IP地址。


5. 选择完成后，单击“确定”，完成绑定。

#### 4.6.1.5. 开启/切换IPv6防护

**子网开启IPv6**

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“网络 > 虚拟私有云”。
4. 选择对应的虚拟私有云，选择对应子网，点击子网后的“修改”进入修改子网页面，勾选“开启IPv6”，单击“确定”。




**Web应用防火墙设备开通**

在设备成功开通后，默认一张网卡设定为管理网卡，以供单点登录设备时使用；需新增一张网卡专门用于业务操作。

**Web应用防火墙开通**

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云等保专区”。
4. 在资源概览页面右上角，单击“立即购买”。
5. 在购买页面配置基础信息（包括区域、虚拟私有云、子网、可用区和CPU分类），套餐选择自定义中的Web应用防火墙、并进行产品规格配置。
6. 选择购买时长后，勾选“我已阅读，理解并接受《云等保专区服务协议》”，点击“立即购买”。完成购买后等待资源开通成功。

**新增业务网卡**

1. 创建弹性网卡

在天翼云控制中心服务列表页，选择“网络 > 虚拟私有云”；在网络控制台左侧导航栏，选择“弹性网卡”，单击弹性网卡页面右上角的“创建弹性网卡”，配置弹性网卡的区域、名称、VPC、子网、安全组等信息，点击“确定”。

2. 绑定网卡

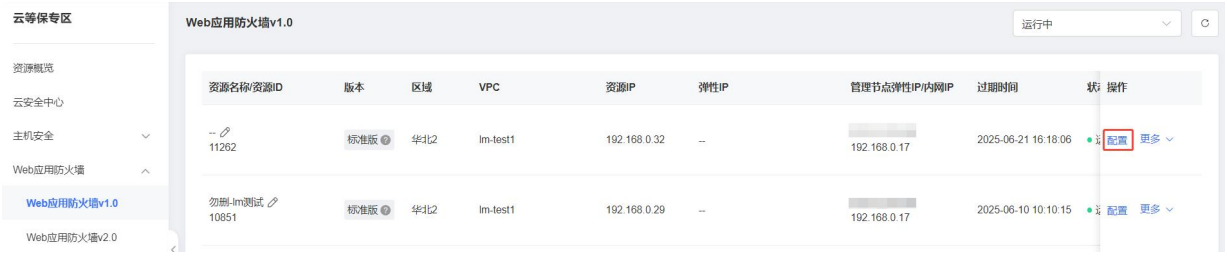
在云等保专区左侧导航栏，选择“Web应用防火墙”，在开通的设备右侧操作列点击“更多 > 绑定网卡”，选中上一步创建的弹性网卡，点击“确定”。

3. 重启Web应用防火墙系统

在云等保专区左侧导航栏，选择“Web应用防火墙”，在开通的设备右侧操作列点击“更多 > 重启”。

## 登录Web应用防火墙界面

在云等保专区左侧导航栏，选择“Web应用防火墙”，在目标资源右侧操作列单击“配置”，进入Web应用防火墙系统。




## 网络配置

### 路由配置

配置管理接口明细路由，单点登录使用。

1. 登录Web应用防火墙界面。

2. 在菜单栏选择“系统管理 > 网络配置 > 路由配置”。

3. 在“静态路由”模块单击“添加”，添加到适配器的明细路由，单击“确定”。

说明：适配器地址获取：“云等保专区 > 目标资源 > 管理节点弹性IP/内网IP”显示的内网IP地址。

### 接口配置

1. 登录Web应用防火墙界面。

2. 在菜单栏选择“系统管理 > 网络配置 > 工作组管理”。
3. 在“工作组”模块单击“添加”，配置工作组的名称，选择接口，单击“确定”。
4. 在接口所在行，单击操作列的“编辑”图标，编辑接口，按照新增网卡的IP信息配置IPv4和IPv6地址及网关信息。

**IPv6业务接入**

1. 登录Web应用防火墙界面。
2. 在菜单栏选择“安全管理 > 站点防护”。
3. 新建站点组：在左侧站点组导航树单击“+”按钮，默认选择“快速模式”，设置“站点组名称”，单击“完成”。
4. 新建站点：选中创建的站点组，在页面右侧单击“新建站点”，配置站点信息后，单击“完成”。
5. 新建虚拟站点：选中创建的站点组，在页面右侧单击“新建虚拟站点”，配置虚拟站点信息后，单击“保存”。

**IPv4接入业务变更为IPv6接入**

1. 登录Web应用防火墙界面。
2. 在菜单栏选择“安全管理 > 站点防护”。
3. 编辑站点：选中需要修改的站点组，选择需要编辑的站点，单击编辑图标，代理IP地址改为IPv6地址，单击“确定”。
4. 编辑虚拟站点：选中需要修改的站点组，选择需要编辑的虚拟站点，单击编辑图标，服务器IP改为IPv6地址，单击“确定”。

### 4.6.2. Web应用防火墙v2.0

Web应用防火墙v2.0版本由Web应用防火墙（原生版）提供服务。

**进入控制台**

方式一：

1. 登录天翼云控制中心。

2. 在控制中心页面顶部选择区域。

3. 在产品服务列表页，选择“安全 > 云等保专区”，进入云等保专区控制台。

4. 在左侧导航栏，选择“Web应用防火墙 > Web应用防火墙v2.0”，跳转到Web应用防火墙（原生版）控制台。

方式二：

1. 登录天翼云控制中心。

2. 在控制中心页面顶部选择区域。

3. 在产品服务列表页，选择“安全 > Web应用防火墙（原生版）”，进入Web应用防火墙（原生版）控制台。

**使用Web应用防火墙v2.0**

请参见《云等保专区-Web应用防火墙 v2.0 用户指南》。

## 4.7. 下一代防火墙

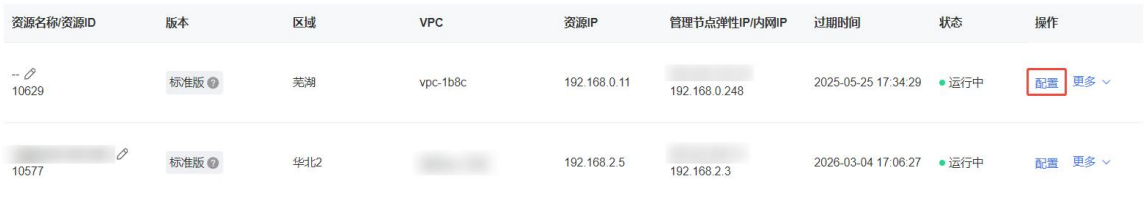
### 4.7.1. 操作指导

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。

**进入控制台**

1. 登录云等保专区控制台。

2. 在左侧导航选择“下一代防火墙”，进入下一代防火墙资源列表页面。




3. 单击目标资源操作列的“配置”，跳转到下一代防火墙控制台。

**使用下一代防火墙**

了解更多下一代防火墙相关操作内容，请下载阅读《云等保专区-下一代防火墙 v1.0 用户指南》。

### 4.7.2. 绑定网卡

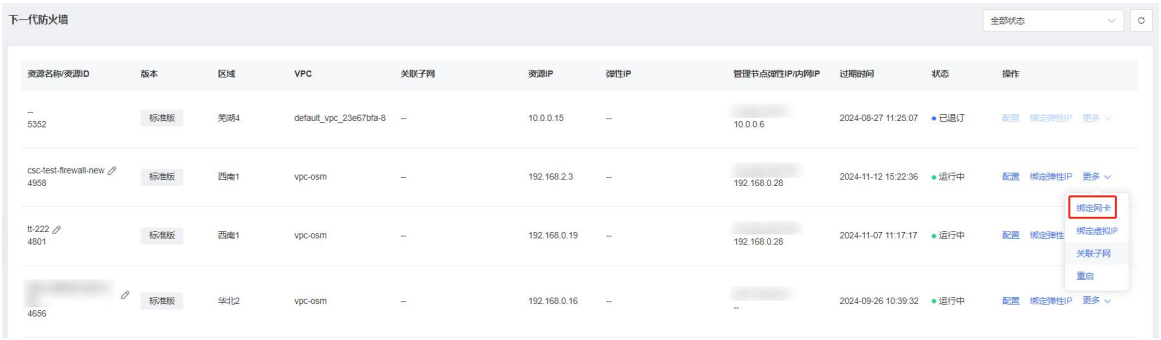
开通下一代防火墙原子能力时，对应原子能力配置的云主机默认只有一张网卡，该网卡为管理口网卡。为了承载业务流量，需要为下一代防火墙对应的云主机添加新的弹性网卡作为业务流量通道。具体绑定的网卡数量根据实际业务网络规划而定。

**前提条件**

已购买下一代防火墙资源，且资源状态为“运行中”。

**操作步骤**

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“下一代防火墙”，进入云等保专区的下一代防火墙资源页面。
3. 在目标资源的操作列，单击“更多 > 绑定网卡”。




4. 绑定网卡。

   根据资源所在区域，绑定网卡的步骤略有不同。

   **一类节点区域：**

   a. 在弹出的“绑定弹性网卡”窗口中，上方展示当前资源已有网卡，在下方列表中选择需要绑定的网卡。

      若没有可绑定的网卡，单击“创建弹性网卡”，创建一个新的网卡。


b. 选择网卡后，单击“确定”，完成绑定。

**二类节点区域：**

单击“绑定网卡”后，会进入对应云主机详情页面。在该页面为云主机绑定网卡。

5. 重启云主机。

当绑定网卡后，需要重启云主机资源使绑定的网卡生效。

> 注意：
> 重启会导致服务中断，且重启过程中无法执行其他操作，请在业务空闲时进行重启。

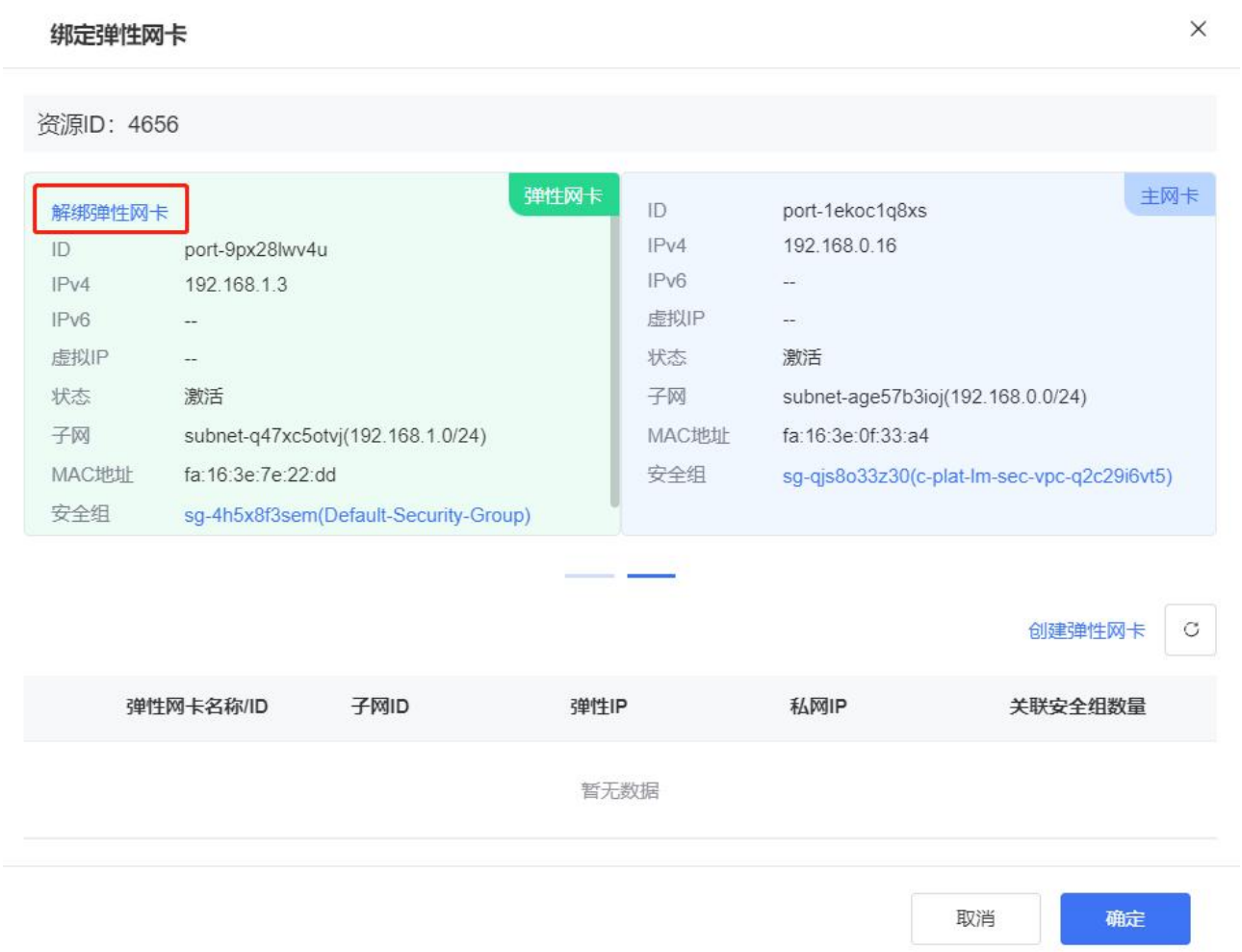
a. 在目标资源的操作列，单击“更多 > 重启”，重启云主机。


b. 在弹出的提示框中，单击“确定”，资源状态变更为“重启中”，待状态变更为“运行中”时，表示重启完成。

> 说明：
> 若重启失败，可再次单击“更多 > 重启”重试。

### 相关操作

若需要解绑网卡，在绑定弹性网卡窗口中，在上方已绑定的网卡模块，单击“解绑弹性网卡”。




## 4.7.3. 绑定虚拟IP

### 前提条件

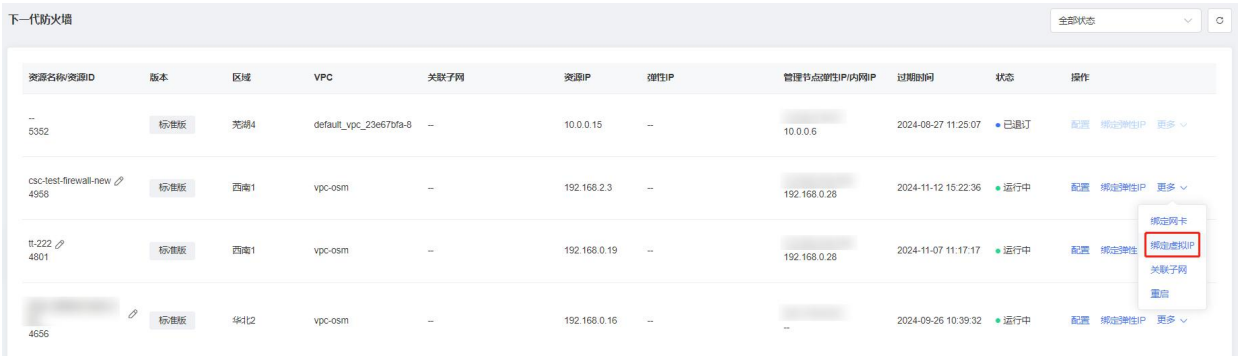
已为下一代防火墙资源绑定网卡。

### 操作步骤

1. 登录云等保专区控制台。

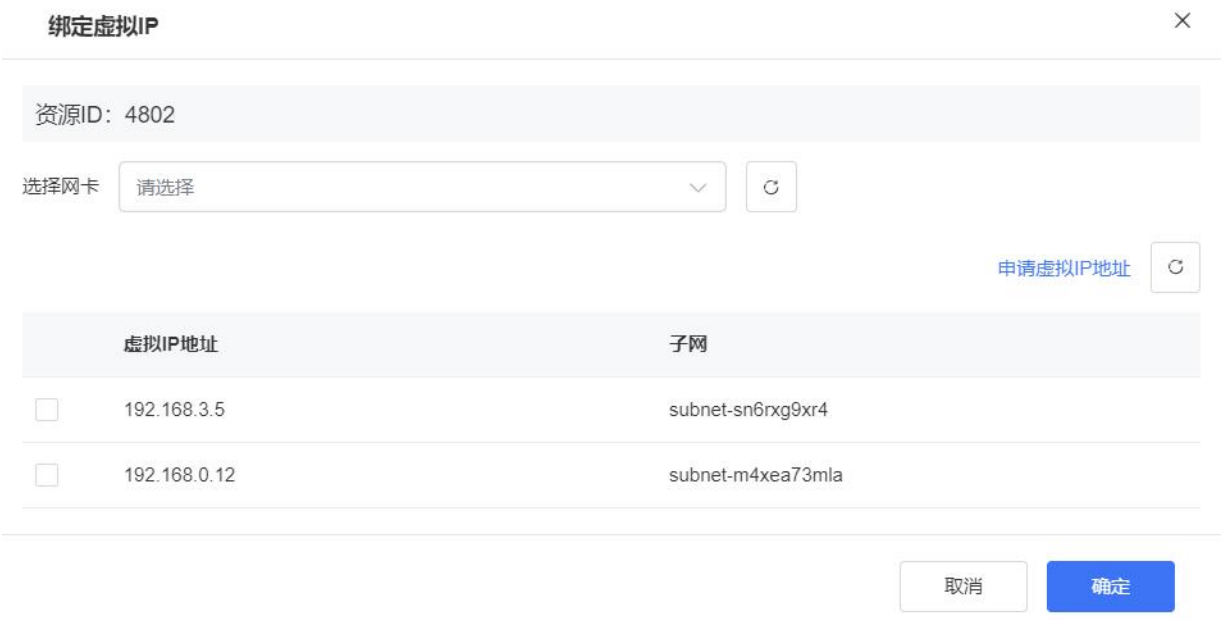
2. 在左侧导航栏，选择“下一代防火墙”，进入云等保专区的下一代防火墙资源页面。

3. 在目标资源的操作列，单击“更多 > 绑定虚拟IP”，为网卡绑定虚拟IP。




4. 在弹出的“绑定虚拟IP”窗口中，通过“选择网卡”下拉框中选择一个网卡，在下方列表中选择一个虚拟IP地址。

   若没有可选的虚拟IP地址，单击“申请虚拟IP地址”，创建一个新的虚拟IP地址。




5. 选择完成后，单击“确定”，完成绑定。

### 4.7.4. 绑定弹性IP

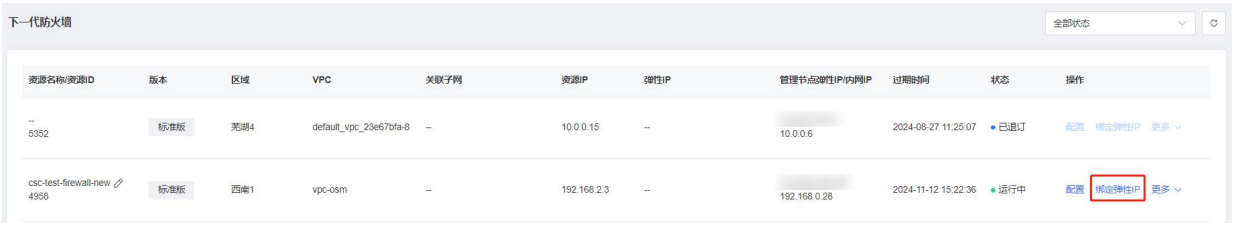
将用户业务弹性公网IP绑定在下一代防火墙业务网卡上，从而将用户业务流量接入下一代防火墙。

**操作步骤**

1. 登录云等保专区控制台。

2. 在左侧导航栏，选择“下一代防火墙”，进入云等保专区的下一代防火墙资源页面。

3. 在目标资源的操作列，单击“绑定弹性IP”，为资源绑定弹性IP。




4. 在弹出的“绑定弹性IP”窗口中，通过“弹性网卡”下拉框中选择一个网卡，在下方列表中选择一个弹性公网IP地址。

   若没有可绑定的弹性IP，单击“配置弹性IP”，进入创建弹性IP页面，创建一个新的弹性IP地址。


5. 选择完成后，单击“确定”，完成绑定。

### 4.7.5. 添加路由子网规则

**约束限制**

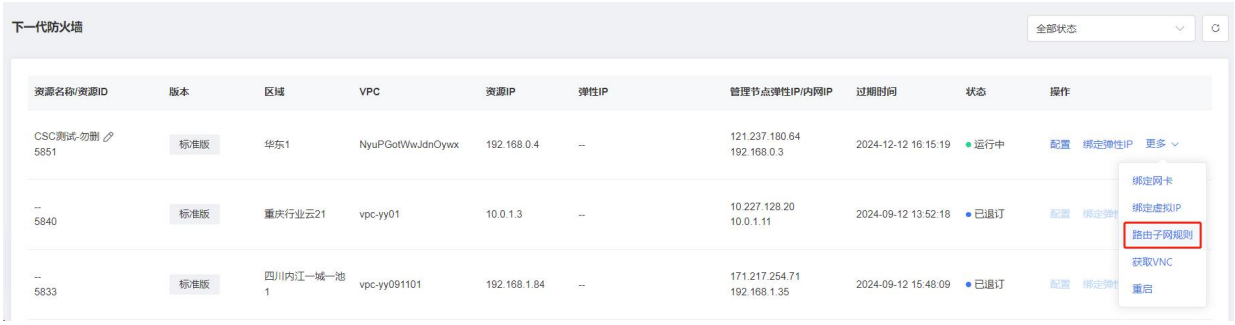
仅“一类节点”区域购买的下一代防火墙资源支持在云等保专区控制台添加子网路由规则。

**前提条件**

已购买下一代防火墙资源，且资源状态为“运行中”。

**操作步骤**

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“下一代防火墙”，进入云等保专区的下一代防火墙资源页面。
3. 在目标资源的操作列，单击“更多 > 路由子网规则”。




4. 在弹出的“添加子网路由规则”窗口中，为弹性网卡选择路由表。

   选择路由表后，单击“查看路由表详情”，可进入路由表详情页面，查看路由表关联的规则和子网信息。


5. 配置完成后，单击“确定”。

## 4.8. 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。

## 功能介绍

| 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。<br>提供短信认证、AD、LDAP、RADIUS认证接口。<br>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。<br>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。<br>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。<br>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。 |
| | 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。<br>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。<br>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。 |

| 功能 | | 描述 |
| --- | --- | --- |
| | 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。<br>允许第三方平台调用API接口，实现用户、资产、权限自动同步。 |

**使用堡垒机**

了解更多堡垒机相关操作内容，请下载阅读《云等保专区-堡垒机 v1.0 用户指南》。

**开启IPv6防护**

堡垒机不支持IPv4和IPv6的切换。若需要开启IPv6防护，请确保在购买堡垒机资源时，所选子网已开启IPv6，否则需要重新购买。

- 购买堡垒机时，选择的子网已启用IPv6，则自动开启IPv6防护。
- 购买堡垒机时，选择的子网未启用IPv6，则需重新下单堡垒机，确保其所选子网已开启IPv6。

## 4.9. 漏洞扫描

### 4.9.1. 操作指导

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 |
| --- | --- |

| 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。<br>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。<br>支持新增、导入、导出、删除、编辑资产。<br>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。<br>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。<br>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。<br>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。<br>支持新增、编辑、另存为、删除、查看策略。<br>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。 |

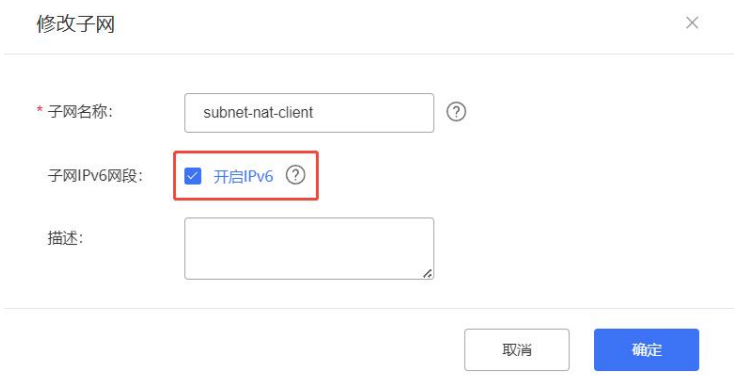
| 功能 | | 描述 |
| --- | --- | --- |
| | | 支持对应用程序、操作系统、网络设备、虚拟化设备、数据库五类资产的安全配置进行核查。<br>支持查看基线模板详情。 |
| | 扫描参数 | 支持设置主机扫描、网站扫描高级参数模板。<br>可根据需要设置与恢复默认扫描参数配置。 |
| | 字典模板 | 主机扫描和弱口令发现任务中引用的各协议弱口令字典。可自定义弱口令字典。 |
| | 报告模板 | 根据不同任务类型，设置离线报告导出的内容。<br>支持设置主机扫描报告、网站扫描报告、数据库扫描报告、基线核查报告、事件内容报告。<br>支持系统默认模板及自定义报告内容模板。 |
| | 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。<br>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。<br>支持新增角色、编辑角色、删除角色。<br>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。<br>支持在线升级和离线升级。<br>支持系统SSH服务开启、系统重启、系统关闭、网卡重启操作。<br>支持设置系统时间。<br>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。<br>支持网卡设置、路由配置、DNS配置、网关配置。<br>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。<br>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《云等保专区-漏洞扫描 v1.0 用户指南》。

### 4.9.2. 开启/切换IPv6防护

#### 子网开启IPv6

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“网络 > 虚拟私有云”。
4. 选择对应的虚拟私有云，选择对应子网，点击子网后的“修改”进入修改子网页面，勾选“开启IPv6”，单击“确定”。




#### 漏洞扫描系统开通

在设备成功开通后，默认一张网卡设定为管理网卡，以供单点登录设备时使用；需新增一张网卡专门用于业务操作。

#### 漏洞扫描系统开通

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云等保专区”。
4. 在资源概览页面右上角，单击“立即购买”。
5. 在购买页面配置基础信息（包括区域、虚拟私有云、子网、可用区和CPU分类），套餐选择自定义中的漏洞扫描、并进行产品规格配置。

6. 选择购买时长后，勾选“我已阅读，理解并接受《云等保专区服务协议》”，点击“立即购买”。完成购买后等待资源开通成功。

### 新增业务网卡

1. 创建弹性网卡

   在天翼云控制中心服务列表页，选择“网络 > 虚拟私有云”；在网络控制台左侧导航栏，选择“弹性网卡”，单击弹性网卡页面右上角的“创建弹性网卡”，配置弹性网卡的区域、名称、VPC、子网、安全组等信息，点击“确定”。

2. 绑定网卡

   在云等保专区左侧导航栏，选择“漏洞扫描”，在开通的设备右侧操作列点击“更多 > 绑定网卡”，选中上一步创建的弹性网卡，点击“确定”。

3. 重启漏洞扫描系统

   在云等保专区左侧导航栏，选择“漏洞扫描”，在开通的设备右侧操作列点击“更多 > 重启”。

## 登录漏洞扫描系统

在云等保专区左侧导航栏，选择“漏洞扫描”，在目标资源右侧操作列单击“配置”，进入漏洞扫描系统。


## 网络配置

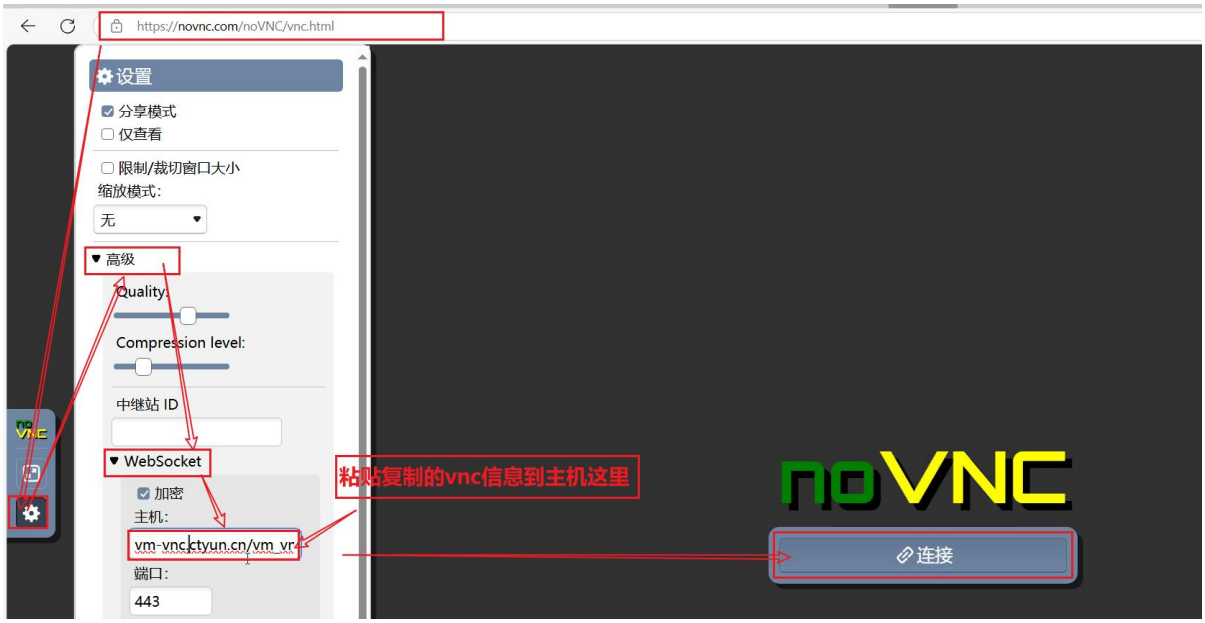
### 路由配置

配置管理接口明细路由，单点登录使用。

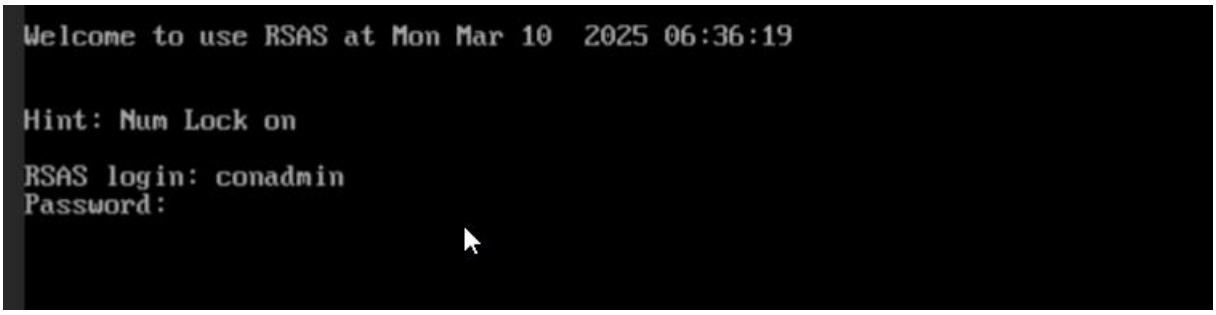
说明：适配器地址获取：“云等保专区 > 目标资源 > 管理节点弹性IP/内网IP”显示的内网IP地址。

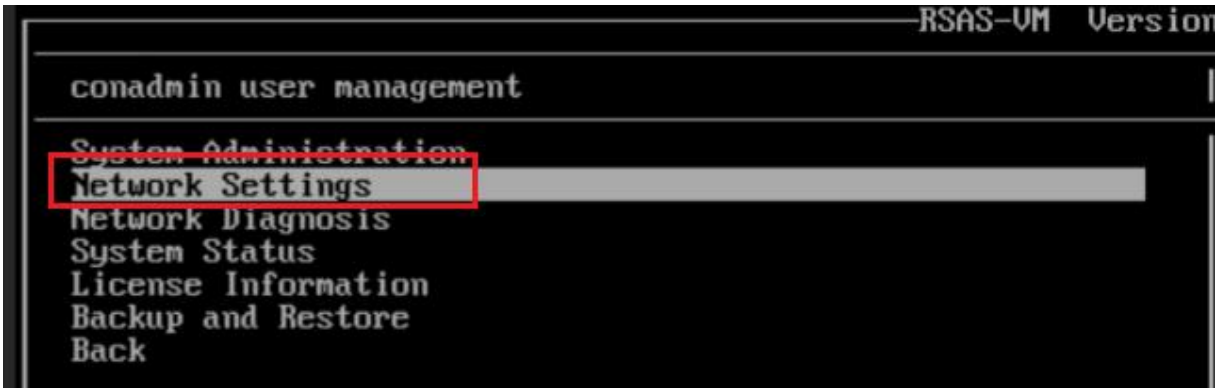
执行以下步骤添加管理口路由：

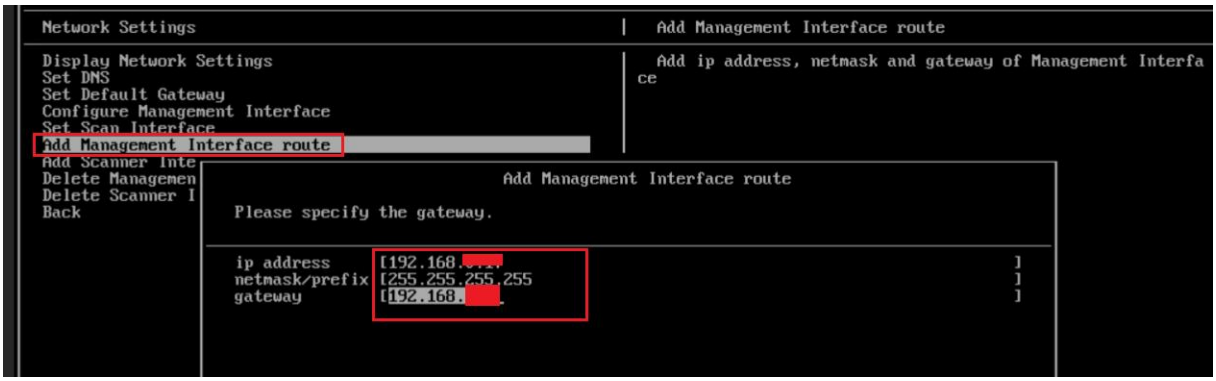
在云等保专区左侧导航栏，选择“漏洞扫描”，在开通的设备右侧操作列点击“更多 > 获取VNC”，单击“复制VNC”，在浏览器访问https://novnc.com/noVNC/vnc.html，配置如下图。




账号密码conadmin/conadmin






**接口配置**

1. 登录漏洞扫描系统。
2. 在菜单栏选择“系统管理 > 配置 > 网络”。
3. 选择接口eth1，单击操作列的“编辑”，地址获取方式改为自动获取或手动配置IP地址、掩码、网关等信息。
4. 单击“确定”，然后重启设备。

## 4.10. 日志审计

### 4.10.1. 操作指导

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。<br>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。<br>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 |

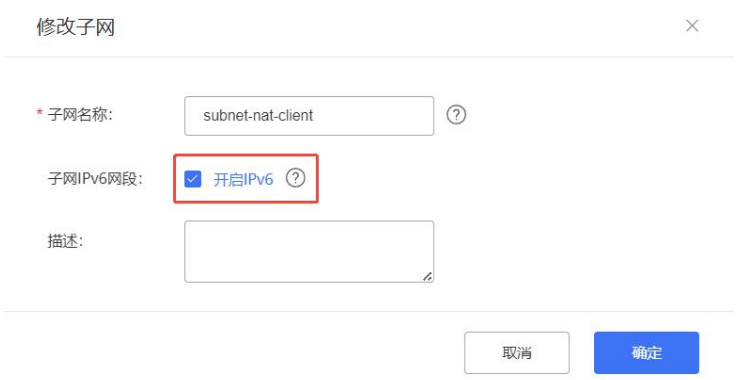
| 功能 | 描述 |
| --- | --- |
| | 检测，可轻松实现各资产间的关联分析。 |
| 脆弱性管理 | 能够收集和管理来自各种Web漏洞扫描工具、主机漏洞扫描工具、网络漏洞扫描工具产生的扫描结果，并实时和用户资产收到的攻击危险进行风险三维关联分析。 |
| 数据挖掘和数据预测 | 支持对历史日志数据进行数据挖掘分析，发现日志和事件间的潜在关联关系，并对挖掘结果进行可视化展示。系统自带多种数据统计预测算法，可以根据历史数据的规律对未来的数据发生情况进行有效预测。 |
| 可视化展示 | 实现对信息资产的实时监控、信息资产与客户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。<br>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。<br>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《云等保专区-日志审计 v1.0 用户指南》。

### 4.10.2. 开启/切换IPv6防护

#### 子网开启IPv6

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“网络 > 虚拟私有云”。
4. 选择对应的虚拟私有云，选择对应子网，点击子网后的“修改”进入修改子网页面，勾选“开启IPv6”，单击“确定”。



## 日志审计开通

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全 > 云等保专区”。
4. 在资源概览页面右上角，单击“立即购买”。
5. 在购买页面配置基础信息（包括区域、虚拟私有云、子网、可用区和CPU分类），套餐选择自定义中的日志审计、并进行产品规格配置。
6. 选择购买时长后，勾选“我已阅读，理解并接受《云等保专区服务协议》”，点击“立即购买”。完成购买后等待资源开通成功。

## 登录日志审计系统

在云等保专区左侧导航栏，选择“日志审计”，在目标资源右侧操作列单击“配置”，进入日志审计系统。

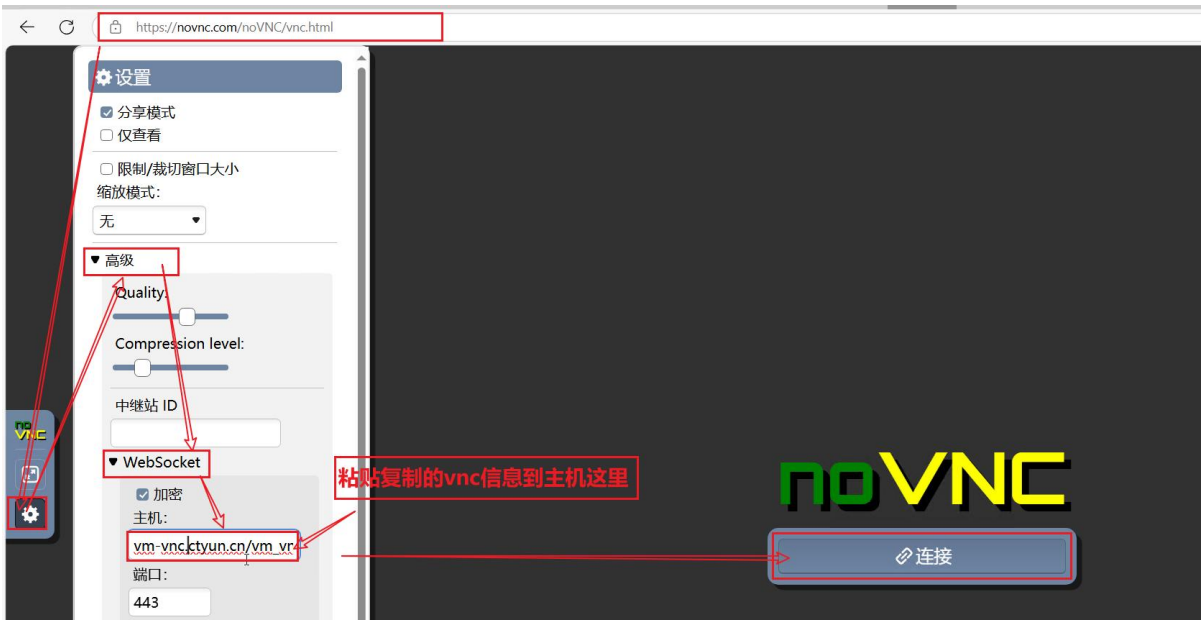

## 网络配置

### 关闭DHCP功能

1. 登录日志审计界面。
2. 右上角设置  图标 > 系统配置 > 网络配置 > 关闭DHCP功能。

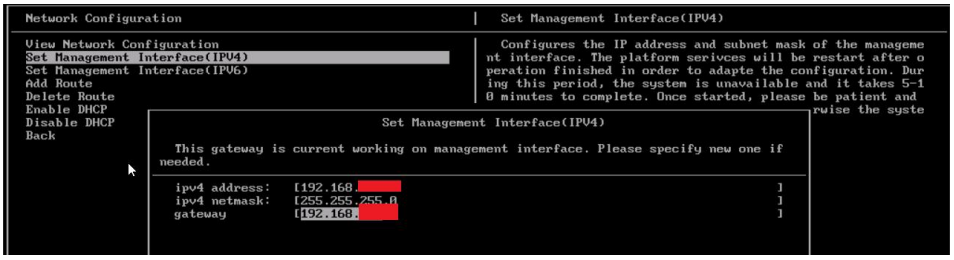
### 串口配置接口地址

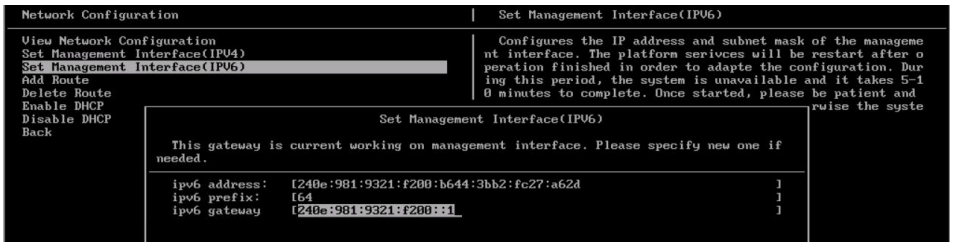
1. 在云等保专区左侧导航栏，选择“漏洞扫描”。
2. 在开通的设备右侧操作列点击“更多 > 绑定网卡”，记录IPv4和IPv6地址信息。
3. 在开通的设备右侧操作列点击“更多 > 获取VNC”，单击“复制VNC”，在浏览器访问https://novnc.com/noVNC/vnc.html，配置如下图。




4. 账号密码conadmin/conadmin@123456，选择English。

5. 键盘上下键移动选项，选择Network ConFiguration > 分别配置管理接口IPv4和IPv6地址（IPv6地址Web配置，登录日志审计界面 > 右上角设置  图标 > 系统配置 > 网络配置 > 编辑接口配置 > 配置IPv6信息 > 然后重启设备。




**IPv4和IPv6转换**

1. 登录日志审计界面。

2. 在右上角设置  图标 > 系统配置 > 网络配置 > 编辑接口配置。

   - 配置IPv6地址信息为IPv6接入。

- 取消IPv6信息为IPv4接入。

说明：

日志审计在IPv6环境使用，完成以上配置后请提交工单联系运维人员进后台手动改配置使日志入库。

## 4.11. 数据库审计

### 4.11.1. 数据库审计v1.0

数据库审计v1.0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。

**功能介绍**

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 |

| 数据库分类 | 数据库系统 | 版本 |
| --- | --- | --- |
| | 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 |
| | 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 PostgreSQL | 10、14 |
| 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 |

| 数据库分类 | 数据库系统 | 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 |
| | 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 |

| 数据库分类 | 数据库系统 | 版本 |
| --- | --- | --- |
| | 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

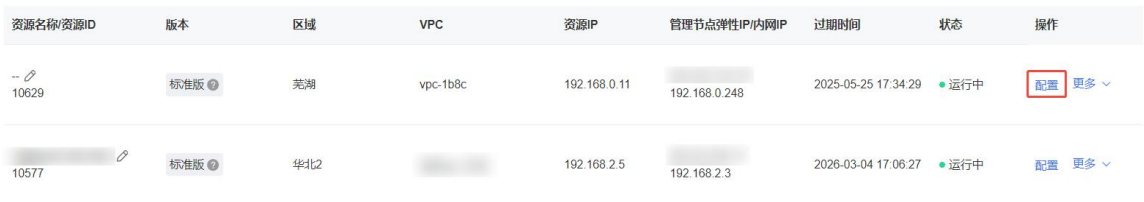
1. 根据 5W1H（What、Where、When、Who、Why、How）分析模型进行规则设置， 提供丰富的规则条件配置方法。
2. 内置 900 多条安全相关的审计分析规则。
3. 根据采集到的数据进行数据分析和产生行为模型。
4. 审计结果查询。

### (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。

### 进入控制台

1. 登录云等保专区控制台。
2. 在左侧导航选择“数据库审计 > 数据库审计v1.0”，进入数据库审计v1.0资源列表页面。



3. 单击目标资源操作列的“配置”，跳转到数据库审计v1.0控制台。

**使用数据库审计v1.0**

了解更多数据库审计相关操作内容，请下载阅读《云等保专区-数据库审计 v1.0 用户指南》。

**开启IPv6防护**

数据库审计不支持IPv4和IPv6的切换。若需要开启IPv6防护，请确保在购买数据库审计资源时，所选子网已开启IPv6，否则需要重新购买。

- 购买数据库审计时，选择的子网已启用IPv6，则自动开启IPv6防护。
- 购买数据库审计时，选择的子网未启用IPv6，则需重新下单数据库审计，确保其所选子网已开启IPv6。

### 4.11.2. 数据库审计v2.0

数据库审计v2.0版本由“天翼云 数据库审计”提供服务。

**进入控制台**

方式一：

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在产品服务列表页，选择“安全 > 云等保专区”，进入云等保专区控制台。
4. 在左侧导航栏，选择“数据库审计 > 数据库审计v2.0”，跳转到数据库审计控制台。

方式二：

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在产品服务列表页，选择“安全 > 数据库审计”，进入数据库审计控制台。

**使用数据库审计v2.0**

请参见《云等保专区-数据库审计 v2.0 用户指南》。

# 5. 最佳实践

## 5.1. 最佳实践汇总

| 原子能力名称 | 版本 | 最佳实践文档 |
| --- | --- | --- |
| 主机安全 | v1.0 | 请参见本文“5.2 主机勒索病毒有效防护”。 |
| | v2.0 | 提供如下最佳实践，请参见《云等保专区-主机安全 v2.0 用户指南》。<br>● 主机安全防护最佳实践<br>● 云上勒索病毒防护实践<br>● 弱口令安全最佳实践<br>● 漏洞扫描最佳实践<br>● 等级保护测评合规最佳实践<br>● 二类节点资产纳管最佳实践 |
| Web应用防火墙 | v1.0 | 请参见本文“5.3 Web应用防火墙高可用部署方案”。 |
| | v2.0 | 提供如下最佳实践，请参见《云等保专区-Web应用防火墙 v2.0 用户指南》。<br>● WAF接入配置最佳实践<br>● 防护配置最佳实践<br>● Web基础防护规则引擎配置最佳实践<br>● CC攻击防护最佳实践 |
| 下一代防火墙 | v1.0 | 请参见本文“5.4 下一代防火墙高可用部署方案”。 |
| 数据库审计 | v2.0 | 提供如下最佳实践，请参见《云等保专区-数据库审计 v2.0 用户指南》。<br>● 审计云上自建数据库<br>● 审计云数据库 |

## 5.2. 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。

1. 在导航栏选择“高级威胁 > 勒索防御”，进入勒索防御页面。
2. 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。

3. 进入系统防护页面，选择“勒索防御”，开启“勒索诱饵防护引擎 ”。


4. 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。


## 5.3. Web应用防火墙高可用部署方案

### 5.3.1. 部署方案

**切换实现逻辑**

WAF设备间的高可用以平台能力虚拟IP来实现，平台虚拟IP绑定多网卡时会自动轮询，将流量自动转发至对应网卡，若虚拟IP所绑定的其中一张网卡down掉，则会自动转发至存活网卡。

**网络要求**

- WAF拉起时使用的子网需避免与客户业务网络处于同一子网，建议新起一段管理子网专用于WAF管理，作为单点跳转使用；新建网卡所在子网需与客户业务子网互通。
- 装好WAF镜像后，单台需要新增1张网卡，作为业务反代网卡，结合初始拉起镜像时自带的主网卡作为M口管理，单台设备共计需要2张网卡。
- 在虚拟云网络中至少申请1个虚IP作为两设备间的两两网卡绑定的虚拟切换地址。

### 5.3.2. 前提条件

- 已完成主备WAF的部署，收集WAF防护云服务器的一些信息；服务器站点以及端口和对应的主机的地址。
- 部署前检查控制台环境。
  1. 确保用户服务器站点没过WAF设备前，是能正常访问的。
  2. 确保WAF与客户业务是否处于同一VPC （与客户业务处在不同VPC得做对等连接）。
  3. WAF设备和服务器安全组是否做了限制。

注意：
安全组配置：请确保防火墙VRRP所绑定网卡处于同一安全组，且将VRRP报文通报端口置于放通状态。

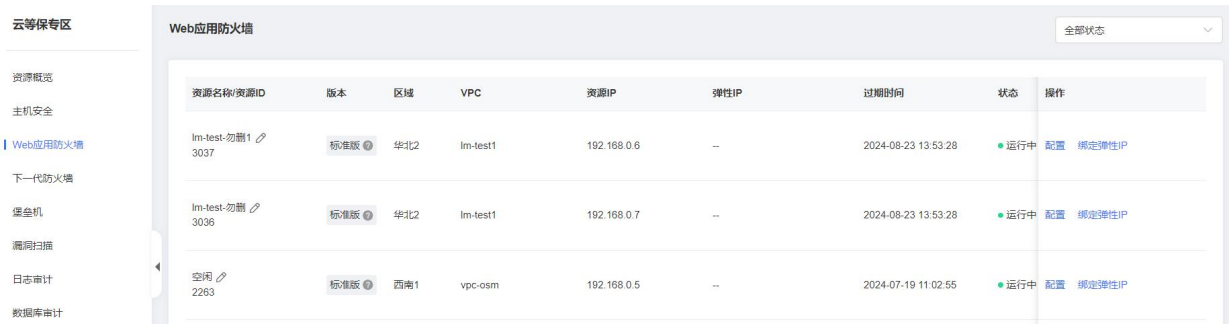
### 5.3.3. 网络规划

示例IP规划如下：

| 网卡 | 子网 | WAF1 IP | WAF2 IP | 虚拟IP |
|---|---|---|---|---|
| eth0 | 192.168.0.0/24 | 192.168.0.6 | 192.168.0.7 | - |
| eth1 | 192.168.2.0/24 | 192.168.2.9 | 192.168.2.10 | 192.168.2.8 |

### 5.3.4. 天翼云控制台配置

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“Web应用防火墙”，查看Web应用防火墙所在VPC。

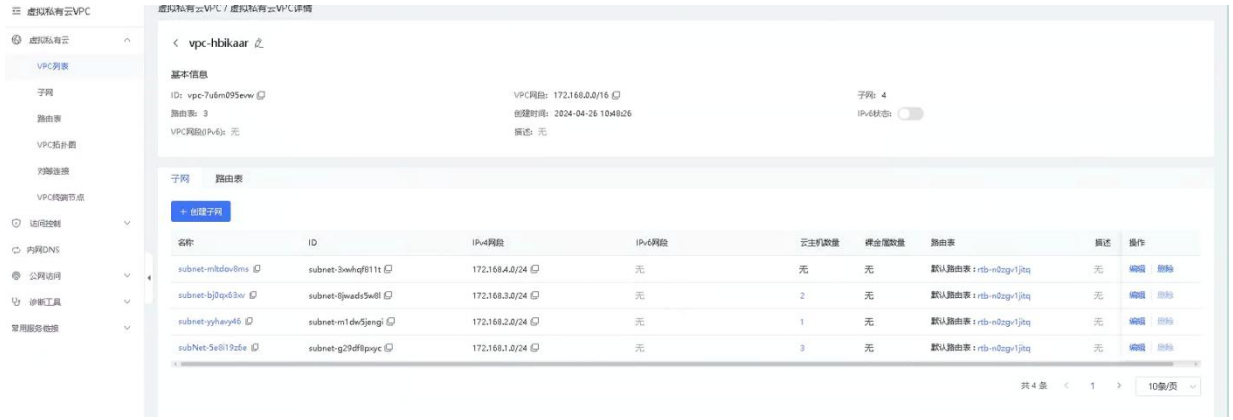



3. 在WAF同VPC内新建子网（基于网络规划进行新建，已有子网分配则无需创建）。

说明：

单台需要新增1张网卡，作为业务反代网卡。

结合初始拉起镜像时自带的主网卡作为M口管理，单台设备共计需要2张网卡。




4. 为防火墙设备绑定网卡。

说明：

WAF云主机绑定网卡时所选子网先后顺序需保持一致。

若绑定网卡时遇到问题，可联系天翼云工作人员。

5. 申请虚拟IP地址并绑定至防火墙设备的网卡。

说明：

请按照以下步骤申请并绑定虚拟IP：

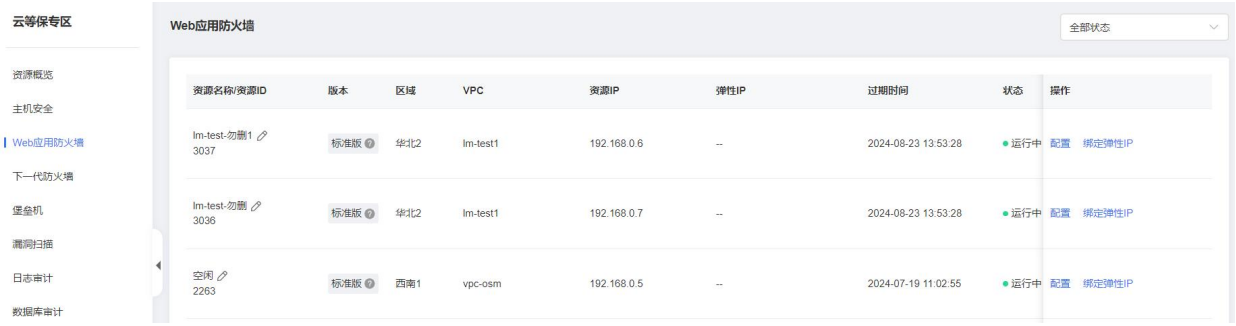
1. 共需根据防火墙子网所在网段购买1个虚拟IP，基于步骤3所创建的子网进行申请虚拟地址。
2. 将申请的虚拟地址绑定至新建的弹性网卡。
3. 将新建的网卡两两绑定至虚拟IP。
4. 绑定完成后，需重启两台添加了网卡的WAF云主机，让设备重新识别网卡。

若绑定虚拟IP时遇到问题，可联系天翼云工作人员协助处理。

### 5.3.5. WAF界面配置

## 登录Web应用防火墙

1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“Web应用防火墙”，单击操作列的“配置”，即可单点登录至Web应用防火墙。

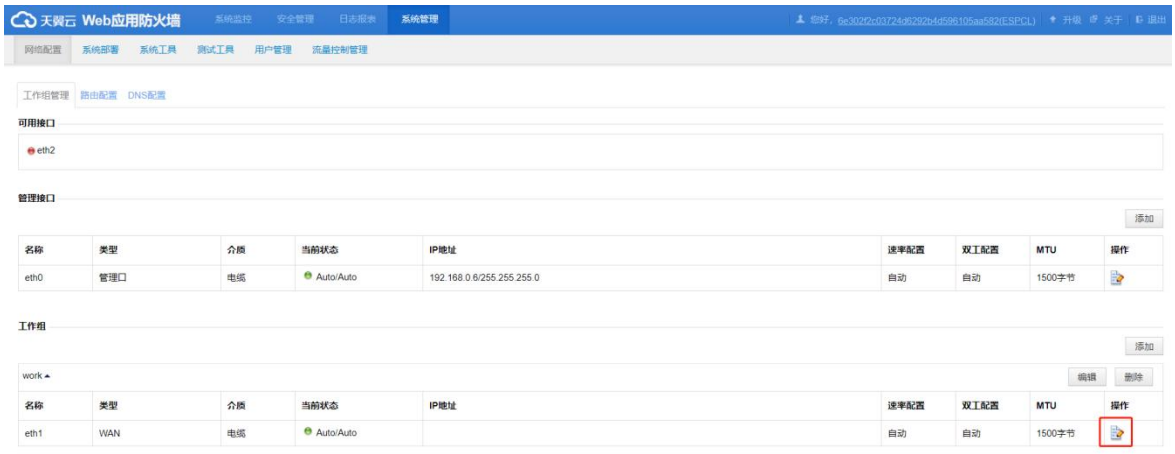



## 配置WAF网卡接口

1. 创建eth1

   点击Web应用防火墙Web界面“系统管理-网络配置-工作组-添加”。


2. 点击“系统管理-网络配置-工作组-eth1编辑”。



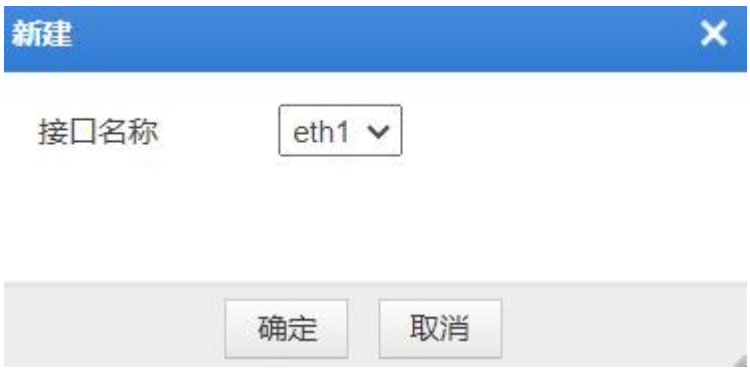
3. 地址设置

将IP地址及掩码按照申请的网卡地址正确填写到IP地址所在位置。并设置工作口网关。

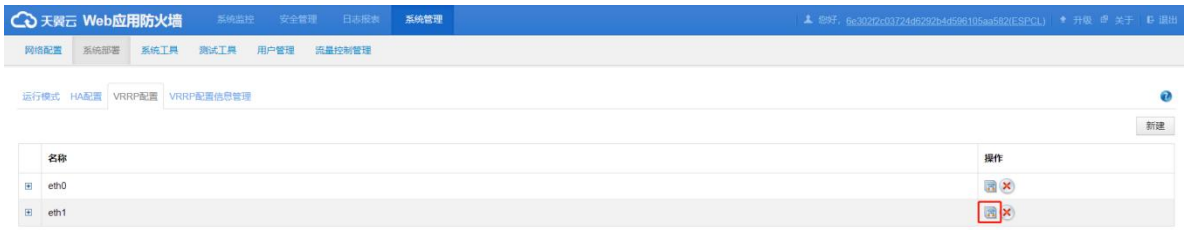

4. 配置WAF VRRP。

a. 点击“系统管理-系统部署-VRRP配置-新建”进入VRRP配置。


勾选eth1网卡。

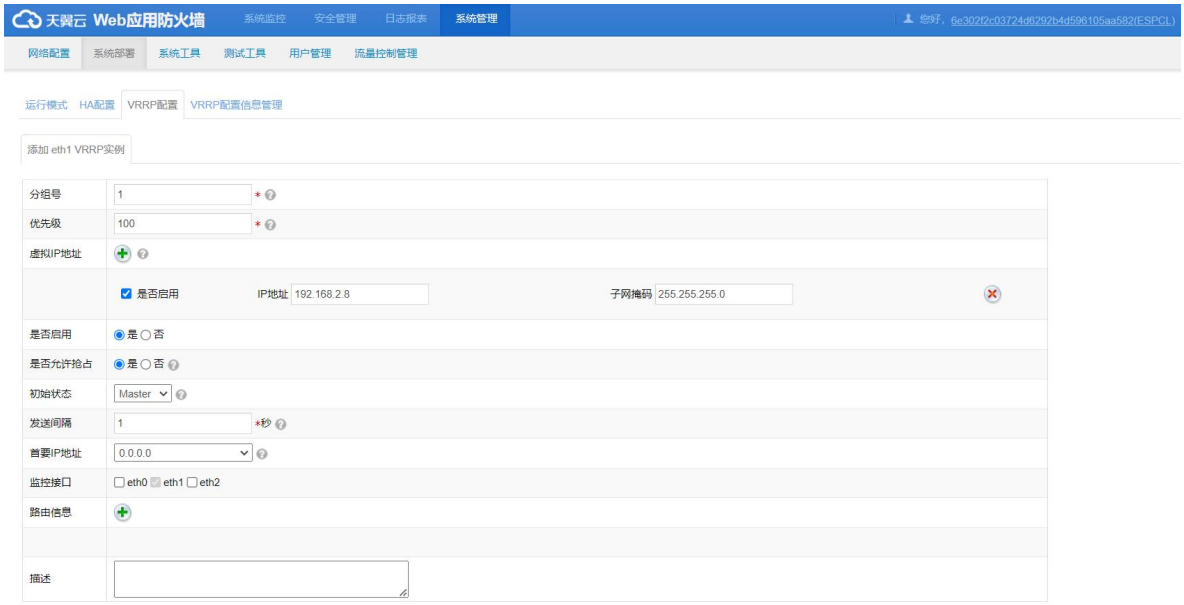


b. 新建完成后点击右边“操作-VRRP实例管理”。

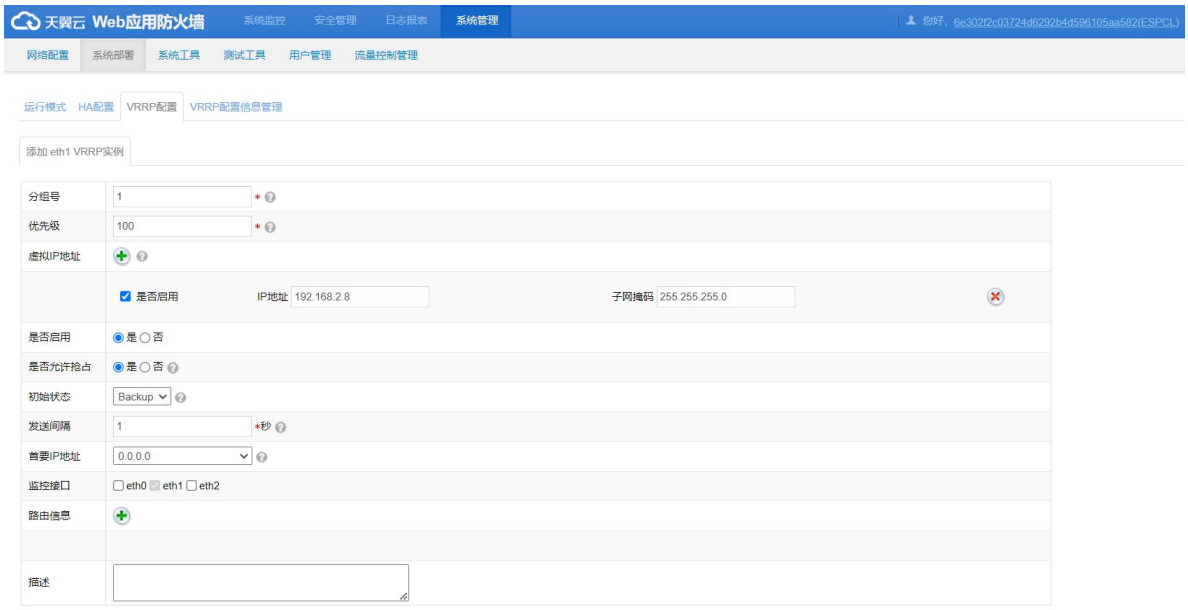



单击“添加”。


自定义填写分组号以及优先级后（数字越高，优先级越高），在虚拟IP地址位置点击“+”号，默认勾选启用，然后申请的虚拟IP地址填入地址栏，点击保存。




备机同此配置，将初始状态改为Backup状态后确认保存配置。




c. 在VRRP配置页面，查看状态。

主：


备：


注意：

由于目前WAF策略同步还处于适配阶段，故两台WAF的策略需手动同步，或在“安全管理 > 站点防护”中配置的安全策略保持一致，且在进行反代策略配置时，接入接口选择eth1口，代理IP地址选择虚拟IP。

## 5.4. 下一代防火墙高可用部署方案

### 5.4.1. 部署方案

- 防火墙拉起时使用的子网需避免与客户业务网络处于同一子网，建议新起一段管理子网专用于防火墙管理，作为单点跳转使用；trust域所在子网需与客户业务子网互通。
- 装好NF镜像后，单台需要新增至少3张网卡，一张trust、一张untrust、一张dmz的VRRP心跳口专用网卡，结合初始拉起镜像时自带的主网卡作为M口管理，单台设备共计需要4张网卡（单臂部署则需要三张）。
- 在虚拟云网络中至少申请三个虚IP作为两设备间的两两网卡绑定的虚拟切换地址。

### 5.4.2. 前提条件

- 已完成主备NF的部署，收集NF防护云服务器的一些信息；服务器站点以及端口和对应的主机的地址。
- 部署前检查控制台环境。
  1. 确保用户服务器站点没过NF设备前，是能正常访问的。
  2. 确保防火墙与客户业务是否处于同一VPC （与客户业务处在不同VPC得做对等连接）。
  3. NF设备和服务器安全组是否做了限制。

注意：
安全组配置：请确保防火墙VRRP所绑定网卡处于同一安全组，且将VRRP报文通报端口置于放通状态。

### 5.4.3. 网络规划

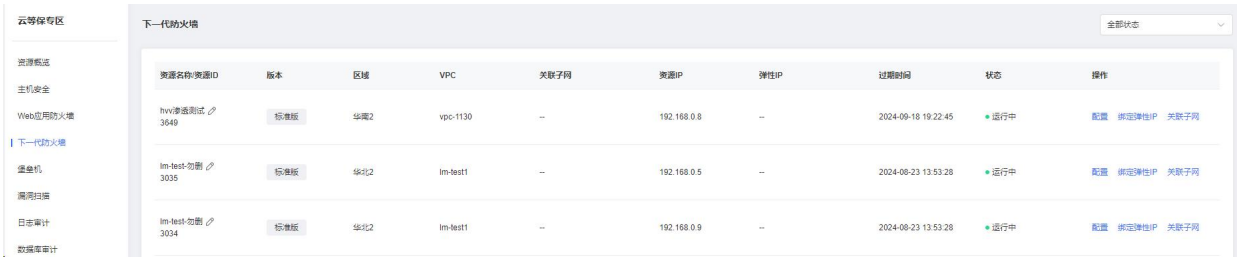
子网及示例IP规划如下：

| 网卡 | 子网 | NF1 IP | NF2 IP | 虚拟IP |
|---|---|---|---|---|
| Manager | 192.168.0.0/24 | 192.168.0.5 | 192.168.0.9 | - |
| Turst | 192.168.2.0/24 | 192.168.2.5 | 192.168.2.6 | 192.168.2.7 |
| Untrust | 192.168.3.0/24 | 192.168.3.3 | 192.168.3.4 | 192.168.3.5 |
| DMZVRRP | 192.168.4.0/24 | 192.168.4.5 | 192.168.4.6 | 192.168.4.7 |

### 5.4.4. 天翼云控制台配置

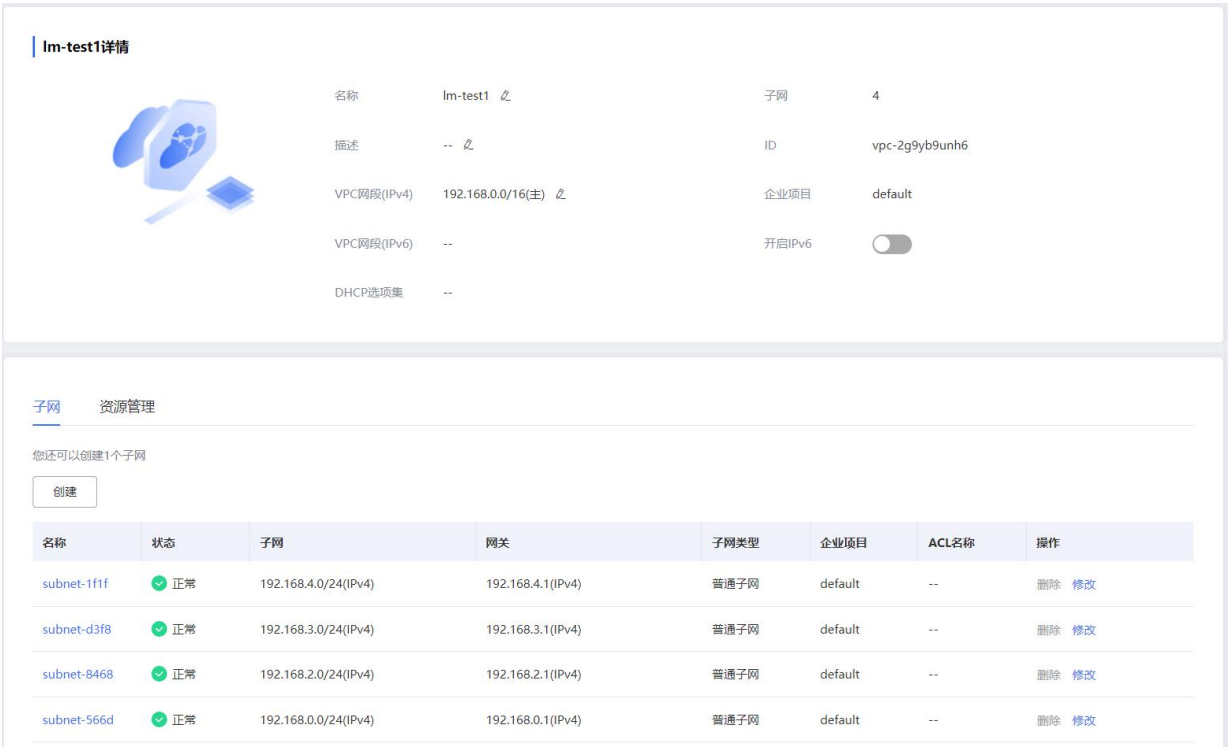
1. 登录云等保专区控制台。

2. 在左侧导航栏，选择“下一代防火墙”，查看下一代防火墙所在VPC。




3. 在防火墙同VPC内新建子网。

> 说明：
> 单台防火墙需要新增至少3张网卡，一张trust、一张untrust、一张dmz的VRRP心跳口专用网卡。
> 结合初始创建防火墙时自带的主网卡作为M口管理，单台设备共计需要4张网卡。




4. 为防火墙设备绑定网卡。

说明：

WAF云主机绑定网卡时所选子网先后顺序需保持一致。

若绑定网卡时遇到问题，可联系天翼云工作人员。

5. 申请虚拟IP地址并绑定至防火墙设备的网卡。

说明：

请按照以下步骤申请并绑定虚拟IP：

1. 共需根据防火墙子网所在网段购买三个虚拟IP，基于步骤3所创建的三个子网进行申请虚拟地址。
2. 将申请的虚拟地址绑定至新建的弹性网卡。
3. 将新建的网卡两两绑定至虚拟IP。
4. 绑定完成后，需重启两台添加了网卡的WAF云主机，让设备重新识别网卡。

若绑定虚拟IP时遇到问题，可联系天翼云工作人员协助处理。

### 5.4.5. NF界面配置

#### 登录下一代防火墙

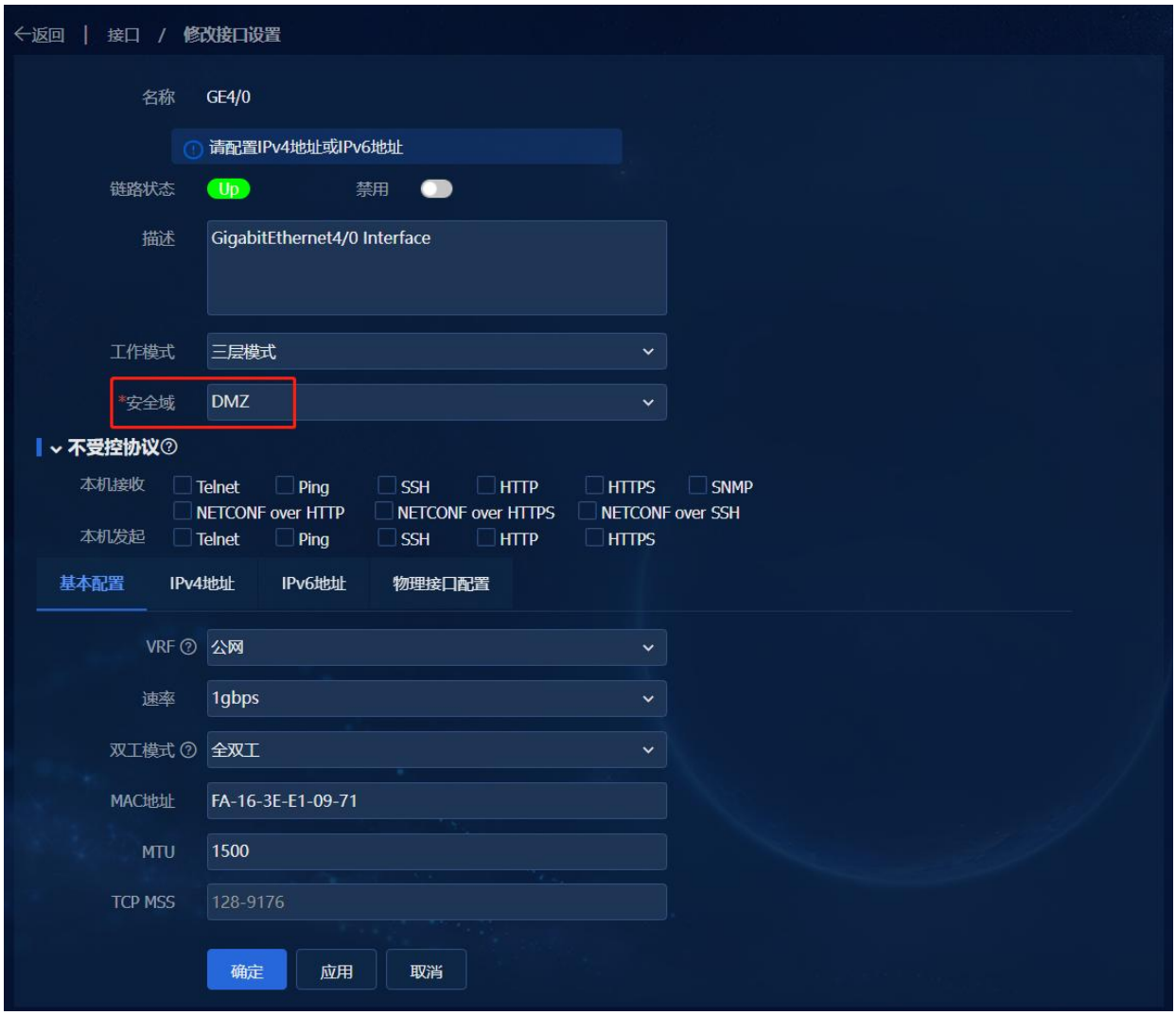
1. 登录云等保专区控制台。
2. 在左侧导航栏，选择“下一代防火墙”，单击操作列的“配置”，即可单点登录至下一代防火墙。


#### 配置NF网卡接口

创建trust,untrust,dmz。如下步骤以GE4/0口为例，其他接口配置步骤类似。

1. 点击防火墙Web界面“网络-接口-接口-GE4/0的编辑按钮”。


2. 点击安全域进行域规划（示例中GE4/0口为DMZ域即VRRP心跳口）。

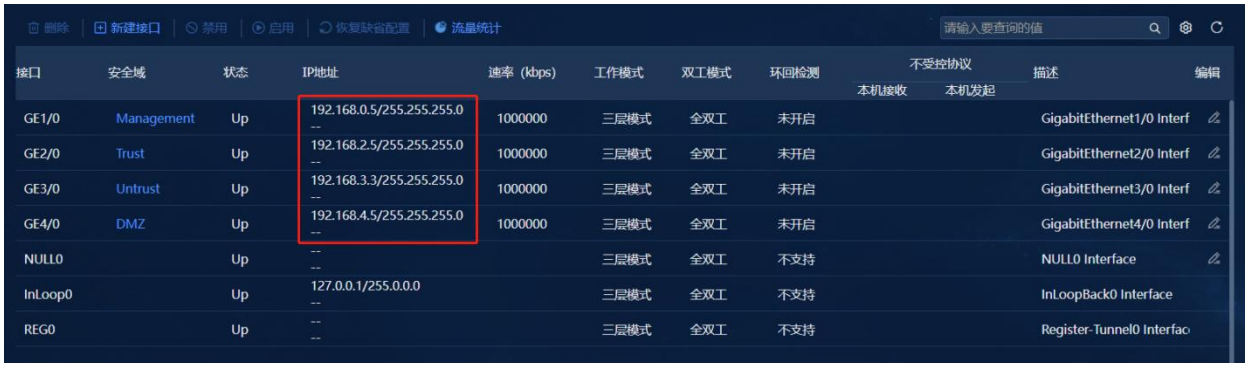



3. 地址设置。

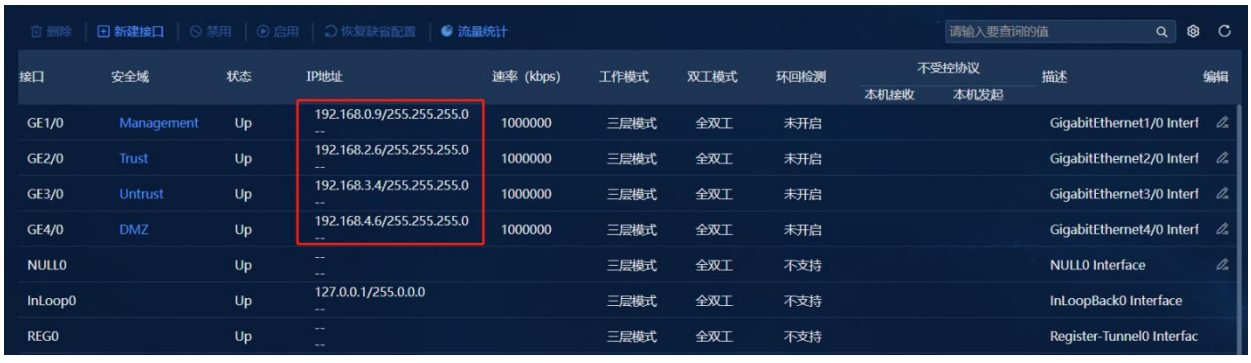
点击编辑页中的“IPV4地址-DHCP”使接口自动获取IP地址。


4. 重复以上操作将两台防火墙四个接口均获取到地址。

NF1：




NF2：



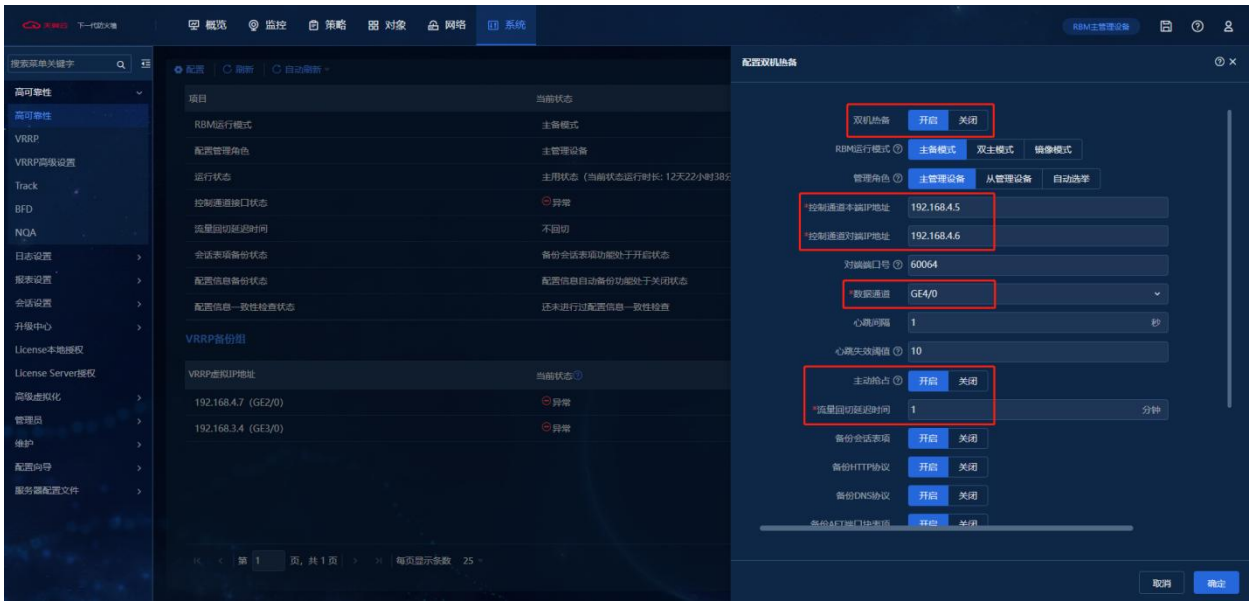

5. 点击右上角保存接口配置。


## 配置NF高可用

1. 点击“系统-高可靠性”，单击“配置”。


2. 在页面右侧弹出的配置双击热备页面，开启设备高可靠性。填入本端IP及对端IP，以GE4/0为通信通道开启1分钟抢占。

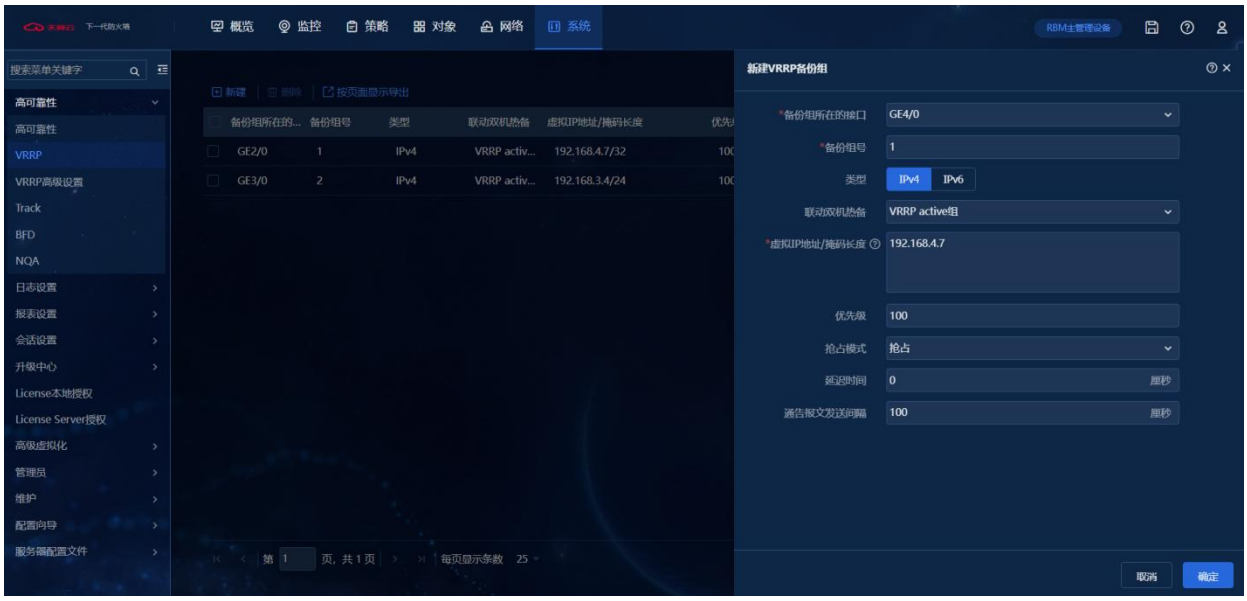
   备机同此配置，将本端与对端地址正确填写后确认保存配置。



3. 开启防火墙VRRP设置。点击防火墙“系统 > 高可靠性 > VRRP”，单击“新建”。

4. 在页面右侧弹出的VRRP配置页面，配置VRRP备份组参数。

| 参数 | 说明 |
| --- | --- |
| 备份组所在的接口 | 选择GE4/0为备份组所在接口。 |
| 备份组号 | 自定义。 |
| 双击热备状态 | 主机选择active组，备机选择standby。 |
| 虚拟IP | 填写在云平台申请的虚拟IP地址/32位掩码。 |
| 优先级 | 自定义。 |
| 抢占模式 | 主备均可开启抢占。 |

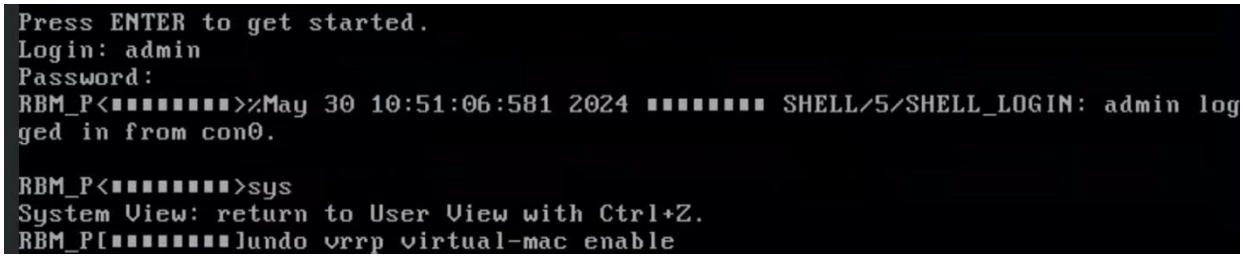



5. 由于云平台的单播特性，需进入防火墙VNC界面将VRRP报文限制为真实MAC通报。

   a. 联系天翼云工作人员获取VNC远程连接，进入VNC界面。

   b. 键入账号密码登录防火墙后，输入 sys 进入系统视图。

   c. 然后输入 undo vrrp virtual-mac enable，限制其虚拟MAC通报（主备均需限制）。




6. 以上配置完成后，单击“系统 > 高可靠性”，查看高可用状态。

# 6. 常见问题

## 6.1. 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) 等保的发展历程是什么?


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。

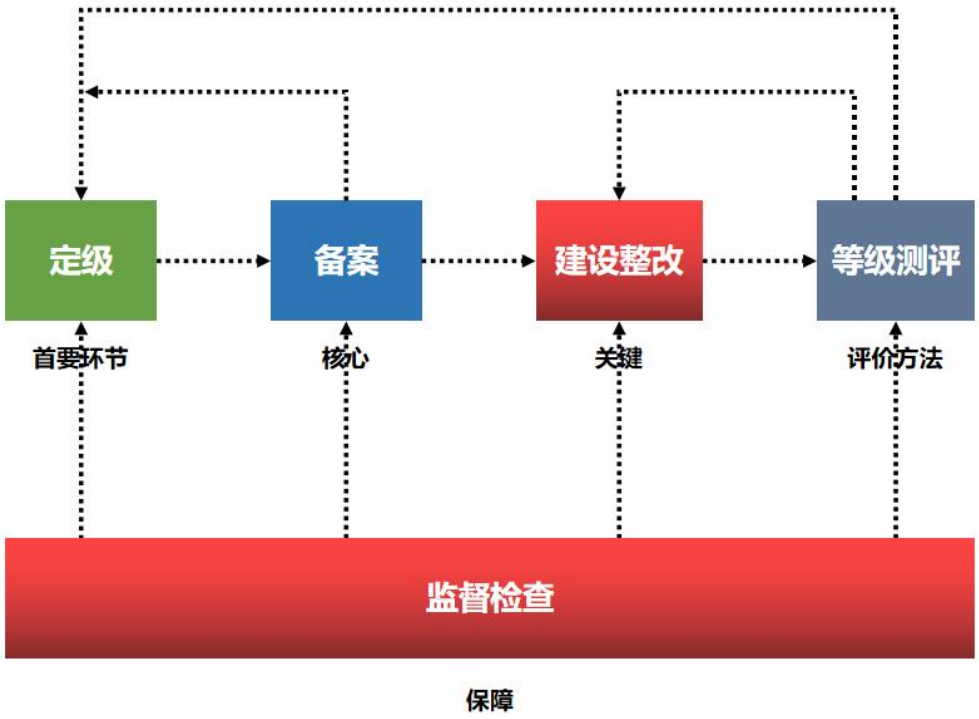
从行业要求层面来说，等保已成为许多行业的必需品。很多行业主管单位明确要求从业机构的信息系统要开展等保工作，比如金融、电力、广电、医疗、教育等行业。

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建设流程是什么？**




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。

## 6.2. 计费类

### (1) 云等保专区产品各安全原子能力的规格以及计费价格是什么？

| 产品名称 | 版本 | 规格 | 规格说明 | 标准价格（元/月） | 标准价格（元/年） | 优惠活动 |
|---|---|---|---|---|---|---|
| 堡垒机 | v1.0 | 10资产 | 支持10资产管理 | 1066 | 12791 | - |
| | | 20资产 | 支持20资产管理 | 1523 | 18273 | - |
| | | 50资产 | 支持50资产管理 | 3006 | 36069 | - |
| | | 100资产 | 支持100资产管理 | 4294 | 51527 | - |
| | | 200资产 | 支持200资产管理 | 6134 | 73610 | - |
| | | 500资产 | 支持500资产管理 | 11599 | 139191 | - |
| | | 1000资产 | 支持1000资产管理 | 16570 | 198844 | - |
| 数据库审计 | v1.0 | 标准版 | 支持4数据库实例 | 3333 | 40000 | - |
| | | 高级版 | 支持8数据库实例 | 6250 | 75000 | - |
| | | 企业版 | 支持16数据库实例 | 11667 | 140000 | - |
| | v2.0 | 标准版 | 支持4数据库实例 | 3333 | 40000 | - |
| | | 高级版 | 支持8数据库实例 | 6250 | 75000 | - |
| | | 企业版 | 支持16数据库实例 | 11667 | 140000 | - |
| 漏洞扫描 | v1.0 | 10资产 | 支持10个IP地址 | 937 | 11248 | - |
| | | 20资产 | 支持20个IP地址 | 1339 | 16068 | - |
| | | 50资产 | 支持50个IP地址 | 3493 | 41915 | - |
| | | 100资产 | 支持100个IP地址 | 4990 | 59878 | - |
| | | 200资产 | 支持200个IP地址 | 10530 | 126358 | - |
| 日志审计 | v1.0 | 10资产 | 支持10个日志源 | 1107 | 13289 | - |
| | | 20资产 | 支持20个日志源 | 1582 | 18984 | - |
| | | 50资产 | 支持50个日志源 | 3219 | 38633 | - |
| | | 100资产 | 支持100个日志源 | 4599 | 55190 | - |
| | | 200资产 | 支持200个日志源 | 9606 | 115267 | - |
| | | 500资产 | 支持500个日志源 | 13722 | 164667 | - |
| 下一代防 | v1.0 | 标准版 | 支持1Gbps | 1879 | 22546 | - |

| 产品名称 | 版本 | 规格 | 规格说明 | 标准价格（元/月） | 标准价格（元/年） | 优惠活动 |
| --- | --- | --- | --- | --- | --- | --- |
| 火墙 | | 高级版 | 支持2Gbps | 3406 | 40872 | - |
| | | 企业版 | 支持4Gbps | 5673 | 68079 | - |
| 云安全中心 | v2.0 | 标准版 | 包含日志分析量为每月50G | 1600 | 19200 | 针对一次性付费客户，享受一年及以上8.5折优惠。 |
| | | 态势大屏 | 包括安全成果态势、威胁攻击态势大屏 | 4500 | 54000 | |
| | | 日志分析量 | 默认需购买500G日志分析量，额外购买步长为50G | 225 / 500GB | 2700 / 500GB | |
| 主机安全 | v1.0 | 标准版 | 按照需防护的主机个数购买，提供安全概览、资产管理、入侵检测、漏洞扫描、基线管理功能。 | 167 | 2000 | - |
| | | 网页防篡改版 | 按照需防护的主机个数购买，提供网页防篡改能力，解决页面篡改、挂马、暗链等网页风险问题。 | 695 | 8340 | - |
| | v2.0 | 旗舰版 | 按照需防护的主机个数购买，提供安全概览、资产管理、入侵检测、漏洞扫描、基线管理功能。 | 180 | 2160 | 包年订购折扣：针对一次性包年付费服务，包年优惠价格为1年85折、2年7折、3年5折。 |
| | | 网页防篡改版 | 按照需防护的主机个数购买，提供网页防篡改能力，解决页面篡改、挂马、暗链等网页风险问题。 | 980 | 11760 | |
| Web应用防火墙 | v1.0 | 标准版 | 防护10个站点，支持带宽防护200Mb | 2837 | 34049 | - |
| | | 域名扩展包 | 每个扩展包支持10个域名防护 | 500 | 5998 | - |
| | | 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；<br>单个Web应用防火墙最大支持1000Mb流量，最大可支持16个扩展包。 | 500 | 5998 | - |
| | v2.0 | 标准版 | 适合中小型网站标准防护 | 3880 | 46560 | **包年订购折扣：**<br>针对一次性包年付费服务，包年优惠价格为1年85折、2年7折、3年5折。<br><br>**优惠折扣：**<br>Web应用防火墙v2.0订购享受8折优惠。 |
| | | 标准版-域名扩展包 | 一个域名扩展包含有：10 个域名防护（含 1 个一级域名） | 600 | 7200 | |
| | | 标准版-业务扩展包 | 一个业务扩展包包含：1000 QPS | 1000 | 12000 | |
| | | 标准版-规则扩展包 | 一个规则扩展包包含：50 条防护规则（仅支持 IP 黑白名单规则） | 70 | 840 | |
| | | 企业版 | 适合大中型网站防护 | 9800 | 117600 | |

| 产品名称 | 版本 | 规格 | 规格说明 | 标准价格（元/月） | 标准价格（元/年） | 优惠活动 |
| --- | --- | --- | --- | --- | --- | --- |
| | | 企业版-域名扩展包 | 一个域名扩展包含有：10 个域名防护（含 1 个一级域名） | 1000 | 12000 | 说明：<br>包年订购折扣与优惠折扣不能同享，取低者计算。 |
| | | 企业版-业务扩展包 | 一个业务扩展包包含：1000 QPS | 2000 | 24000 | |
| | | 企业版-规则扩展包 | 一个规则扩展包包含：50 条防护规则（仅支持 IP 黑白名单规则） | 70 | 840 | |

## 6.3. 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，特地推出等保二级基础版、等保二级高级版、等保三级基础版以及等保三级高级版，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？**

除了主机安全的“网页防篡改”不能单独购买，其他均支持单独购买。

**(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，试用周期为多长时间？**

云等保专区支持试用，如需申请试用，请联系客户经理下单。

**(6) 主机安全如何确定购买个数？**

主机安全的购买个数依据需要防护的ECS数量确定，需要防护多少个ECS就购买多少个主机安全。

**(7) 云等保专区产品是否支持跨资源池防护使用？**

不支持，云等保专区会在每个资源池进行加载，为保证用户业务数据安全，暂时不支持用户跨资源池使用，用户可在就近资源池进行云等保专区产品的购买。

**(8) 云等保专区产品是否支持跨VPC防护？**

支持，但是需要通过对等连通打通两个VPC之间的网络连接。

**(9) Web应用防火墙购买数量是否具有限制？**

不限制购买数量，但是一个订单只能购买一个Web应用防火墙（扩展包最多20个），要购买多个，需下多个订单。

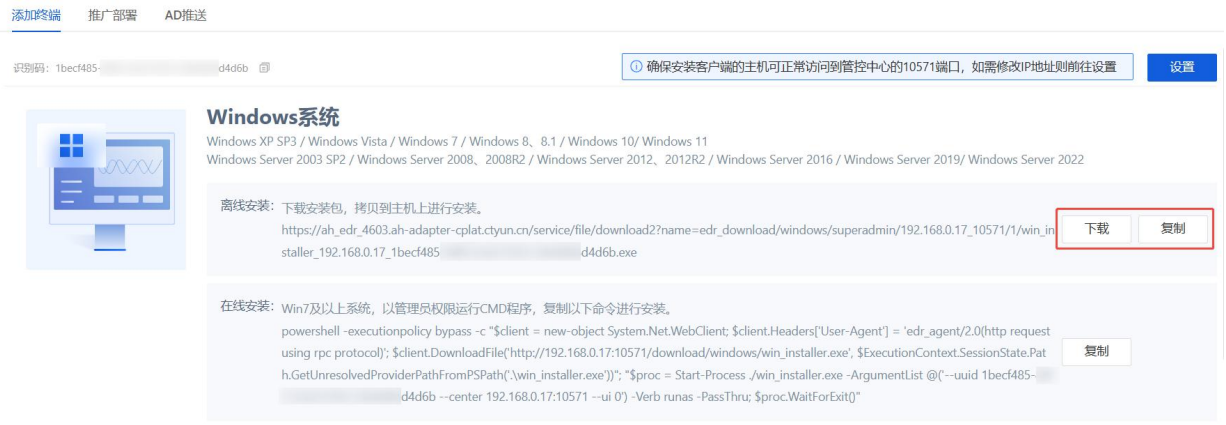
## 6.4. 产品配置类

### 6.4.1. 主机安全

#### 6.4.1.1. 主机安全v1.0

**(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在左侧导航栏选择“ 系统管理+添加资产 ”进入添加资产页面，用户可在Windows系统区域进行Windows系统资产的离线安装及在线安装Agent。




在左侧导航栏选择“ 系统管理 +添加资产 ”，进入添加资产页面，用户可在Linux系统区域进行Linux系统资产的离线安装及在线安装Agent。


2. 资产风险排查。用户可以对资产进行病毒查杀、木马查杀、漏洞管理等操作，在导航栏选择“资产管理>资产概况 ”进入资产概况页面，选择需要查看的主机资产，点击资产名称。


3. 进入资产指纹页面，即可查看该主机资产的详细信息，并可进行远程重 启主机、关闭主机及修改远程端口操作。


4. 编辑安全策略，EDR 支持以模板形式配置主机策略，包括基础信息、系统防护、网络防护、渗透追踪、网页防篡改、Web 应用防护、信任名单、桌面管控。

5. 查看日志，用户可以查看相关的防护、操作、运维类日志。

展开查询条件：


日志列表：


## (2) 主机安全的agent可以部署在哪些操作系统的机器上？

支持部署在如下操作系统：

- 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

**(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。

#### 6.4.1.2. 主机安全v2.0

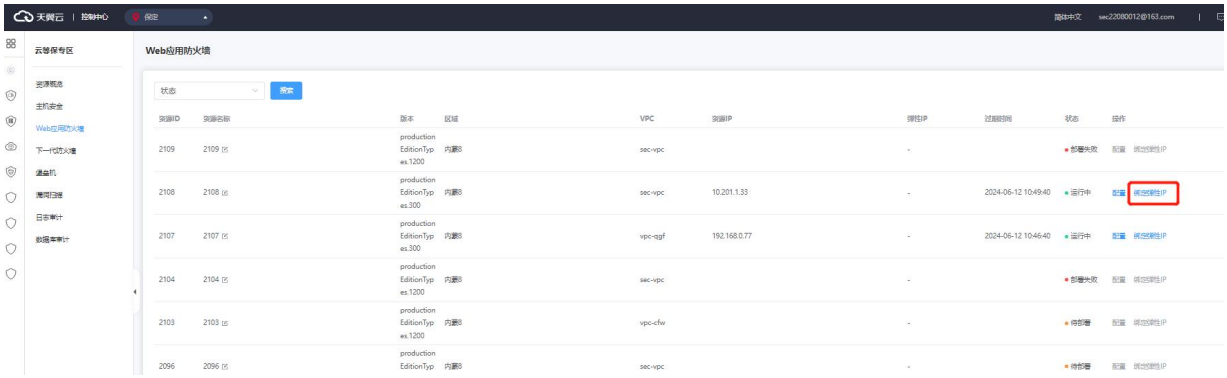
主机安全v2.0常见问题请参见《云等保专区-主机安全 v2.0 用户指南》。

### 6.4.2. Web应用防火墙

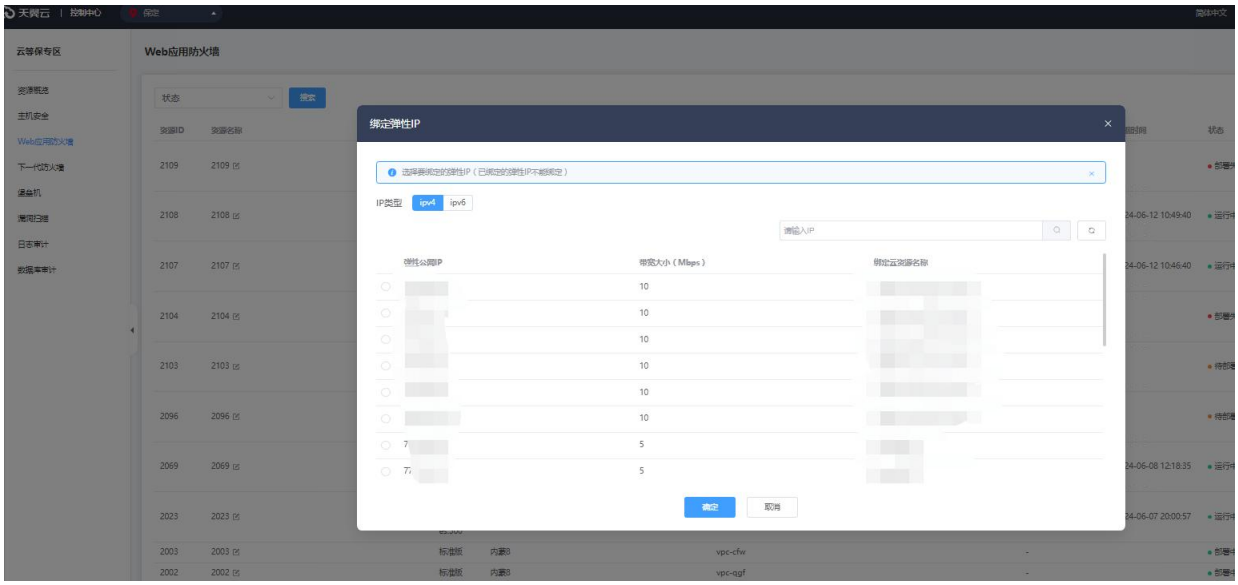
#### 6.4.2.1. Web应用防火墙v1.0

**(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，在左侧导航树选择“Web应用防火墙”，进入Web应用防火墙原子能力，进行绑定弹性IP操作。



根据弹出的弹性IP地址列表，选择将要绑定弹性IP。




2. 选择Web应用防火墙部署模式，更多信息请参考《云等保专区-Web应用防火墙 用户使用指南》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”。


3. 添加保护站点，详细操作可查看《云等保专区-Web应用防火墙 用户使用指南》-配置保护站点操作细则。

4. 配置防护策略，详细操作可查看《云等保专区-Web应用防火墙 用户使用指南》-规则组和自定义规则。
5. 完成基础配置后，可通过以下步骤验证是否配置成功。
   a. 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。
   b. 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。
   c. 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，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。

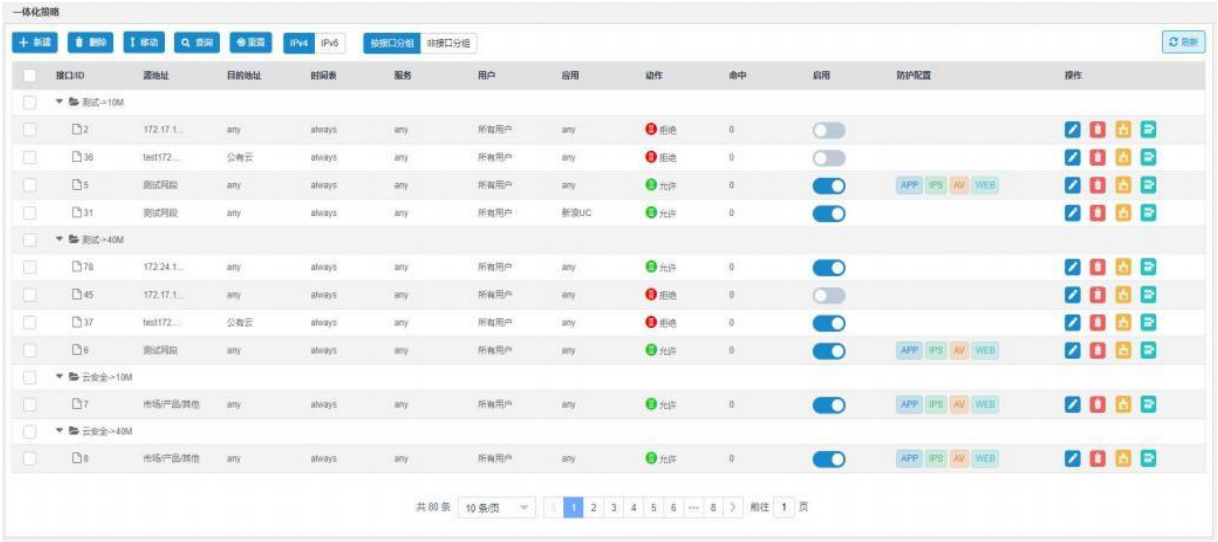
### 6.4.2.2. Web应用防火墙v2.0

Web应用防火墙v2.0常见问题请参见《云等保专区-Web应用防火墙 v2.0 用户指南》。

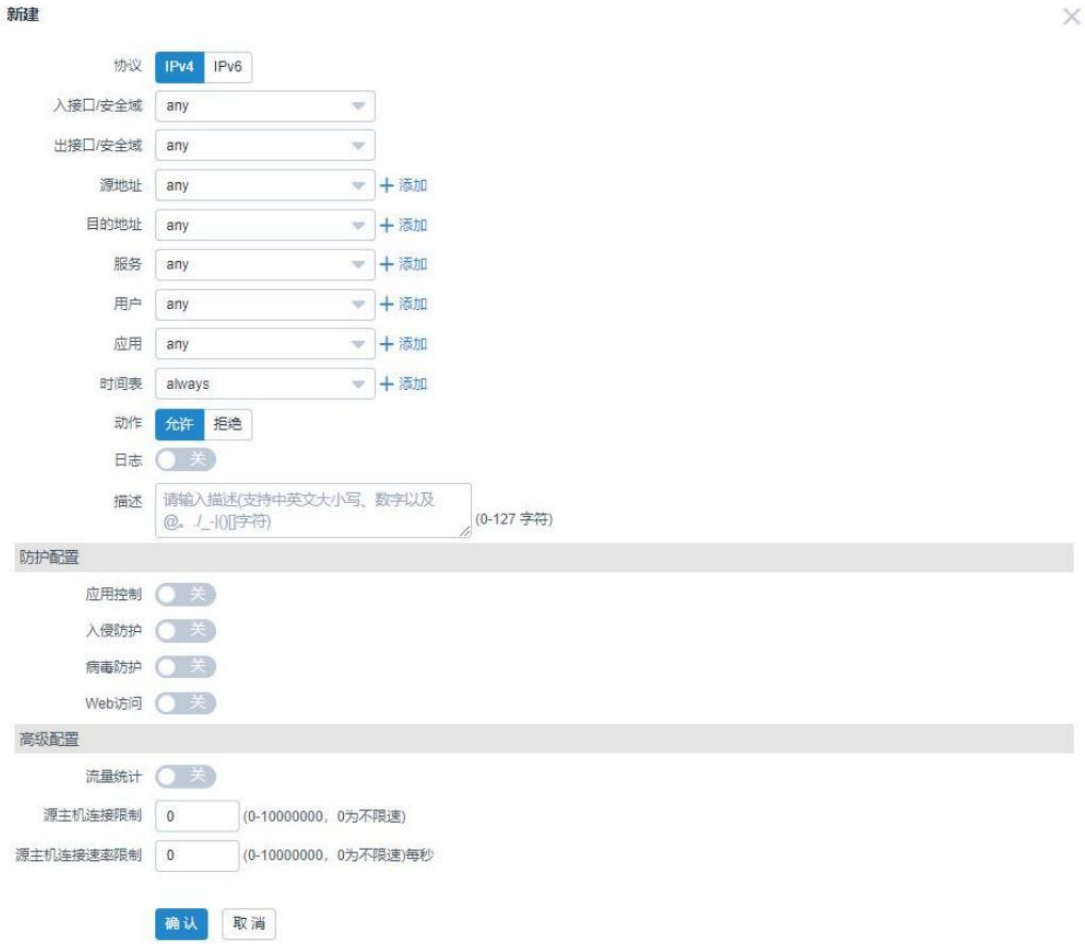
### 6.4.3. 下一代防火墙

**(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。

**(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？**

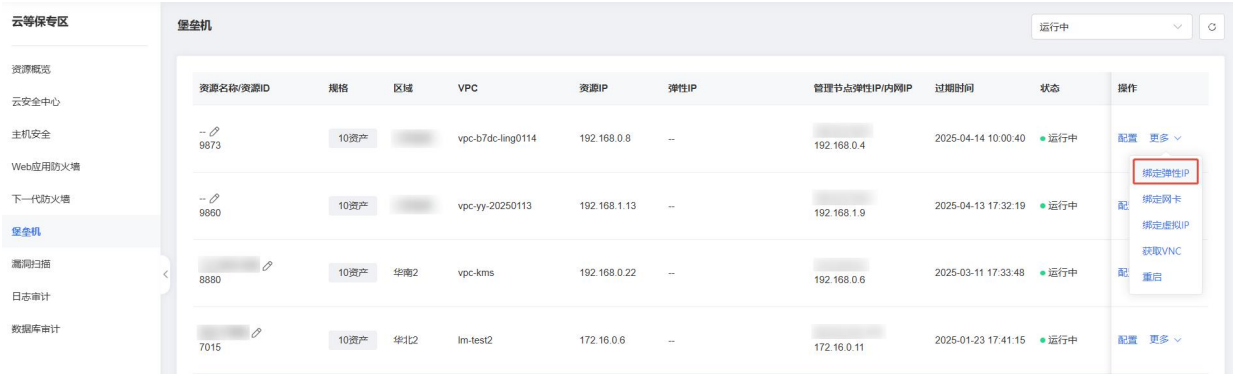
IPS自定义规则最多可配置32条，每条自定义规则最多可包含8个协议字段，每个协议字段最多可包含8个协议匹配条件。

### 6.4.4. 堡垒机

**(1) 堡垒机如何进行接入配置？**

**绑定弹性IP**

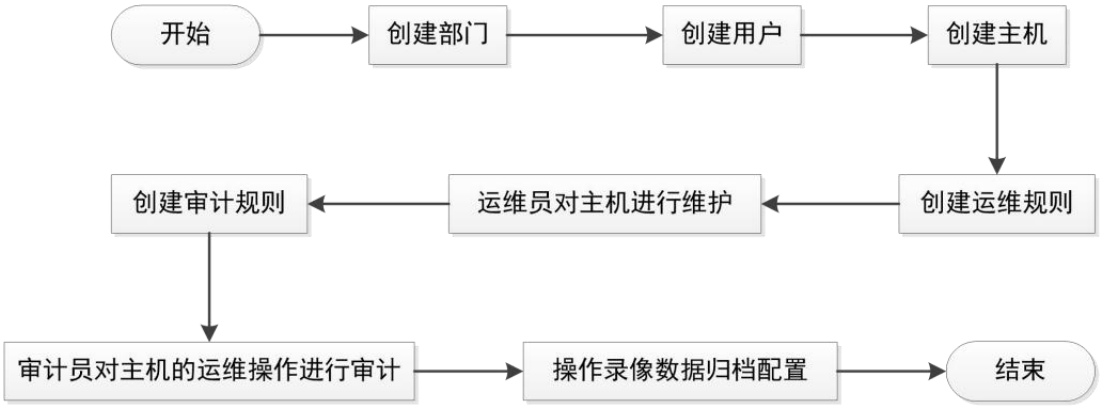
1. 用户登录到云等保专区后，进入“堡垒机”原子能力，进行绑定弹性IP操作，点击“绑定弹性IP”。



2. 根据弹出的弹性IP地址，选择需要绑定的具体IP地址。

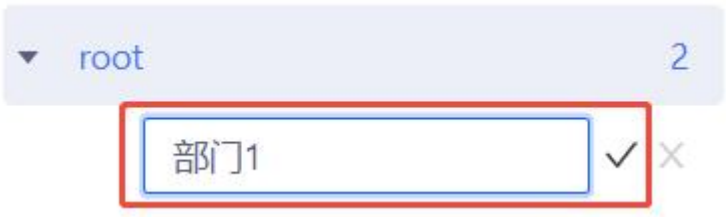

**堡垒机接入配置**

按照下图流程进行操作：



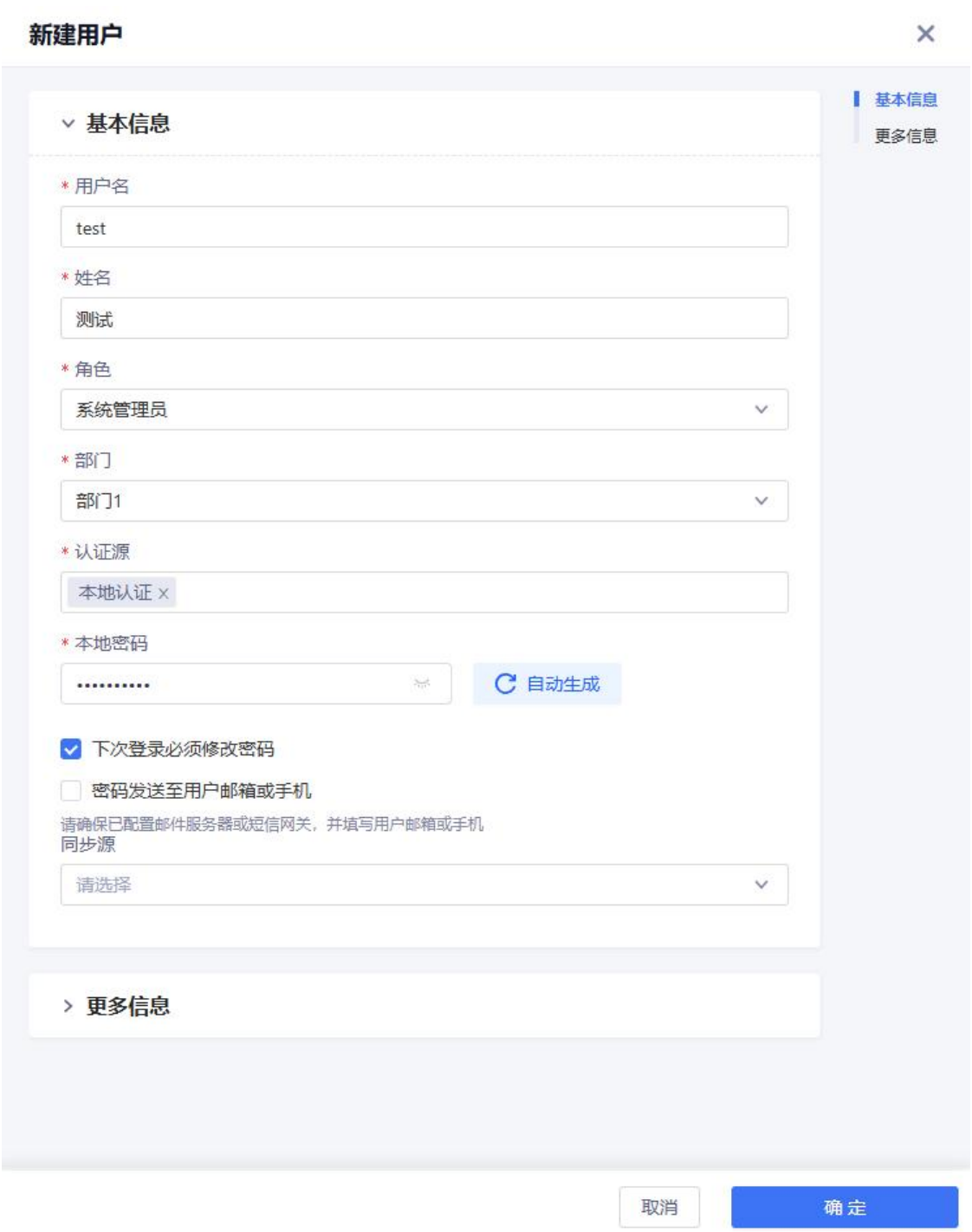

1. 首先创建部门：超级管理员或部门管理员创建部门，在系统菜单栏选择“用户 > 用户管理”，单击root部门右侧数字，选择“新建子部门”。


输入部门名称，点击“√”完成创建。




2. 创建系统用户，例如系统管理员等，在菜单栏选择“ 用户 > 用户管理 ”，进入用户管理页面，点击“新建”。

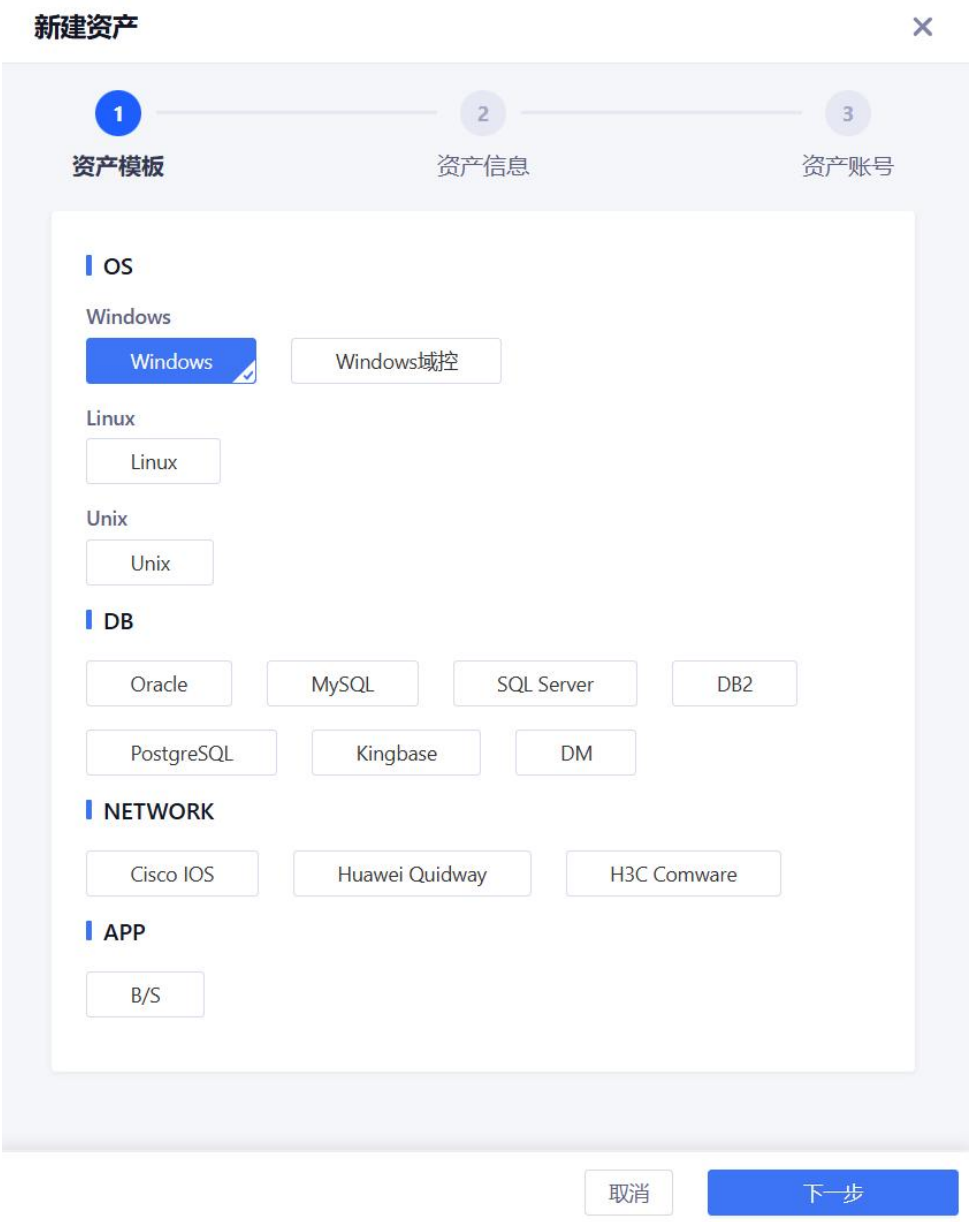

进入新建用户页面，编辑相关信息，点击“确定”。




3. 添加资产：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 > 资产管理 ”，进入资产管理页面。点击“新建”。

进入新建资产页面，选择资产模板、配置资产信息、配置资产账号，点击“确定”完成资产新建。

选择资产模板：




配置资产信息：


新建资产
资产模板
2
资产信息
3
资产账号
基本信息
更多信息
基本信息
资产类型
普通资产
域控
域成员
* 资产名称
test1
* IP/域名
1.1.1.1
所属网络
default
所在节点
根节点
更多信息
备注
请输入
0 / 200
取消
上一步
下一步

配置资产账号：


新建资产
资产模板
资产信息
3
资产账号
资产账号
添加
账号名
密码
操作
administrator
- 未托管 -
编辑
删除

4. 创建授权规则：授权系统管理员可以登录主机进行运维，系统菜单栏选择“ 授权 > 授权规则 ”，进入规则页面。点击“新建”。


进入新建规则页面，配置规则名称、有效期等信息，设置用户与资产的对应关系，点击“确定”，完成规则的创建。

5. 用户对主机进行维护：用户通过系统登录主机并对主机进行维护，详细操作可阅读《云等保专区-堡垒机 用户使用指南》-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：

- 自带免费的手机APP 动态口令认证。
- 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？**

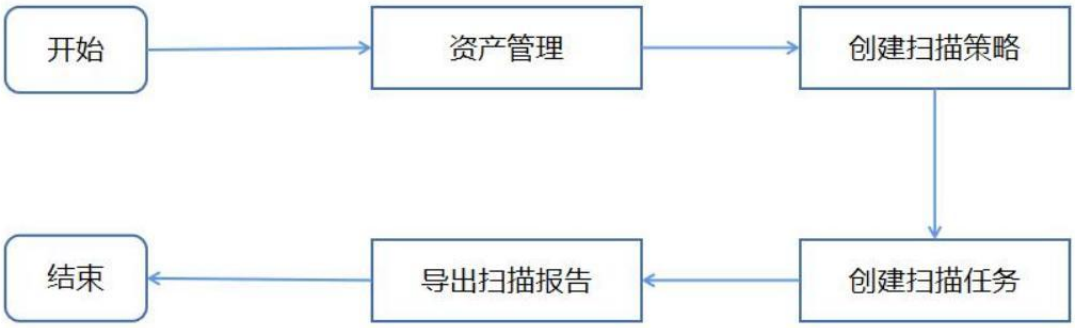
支持，直接利用C/S运维方式，H5运维即可。

**(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。

### 6.4.5. 漏洞扫描

**(1) 漏扫扫描如何进行接入配置？**

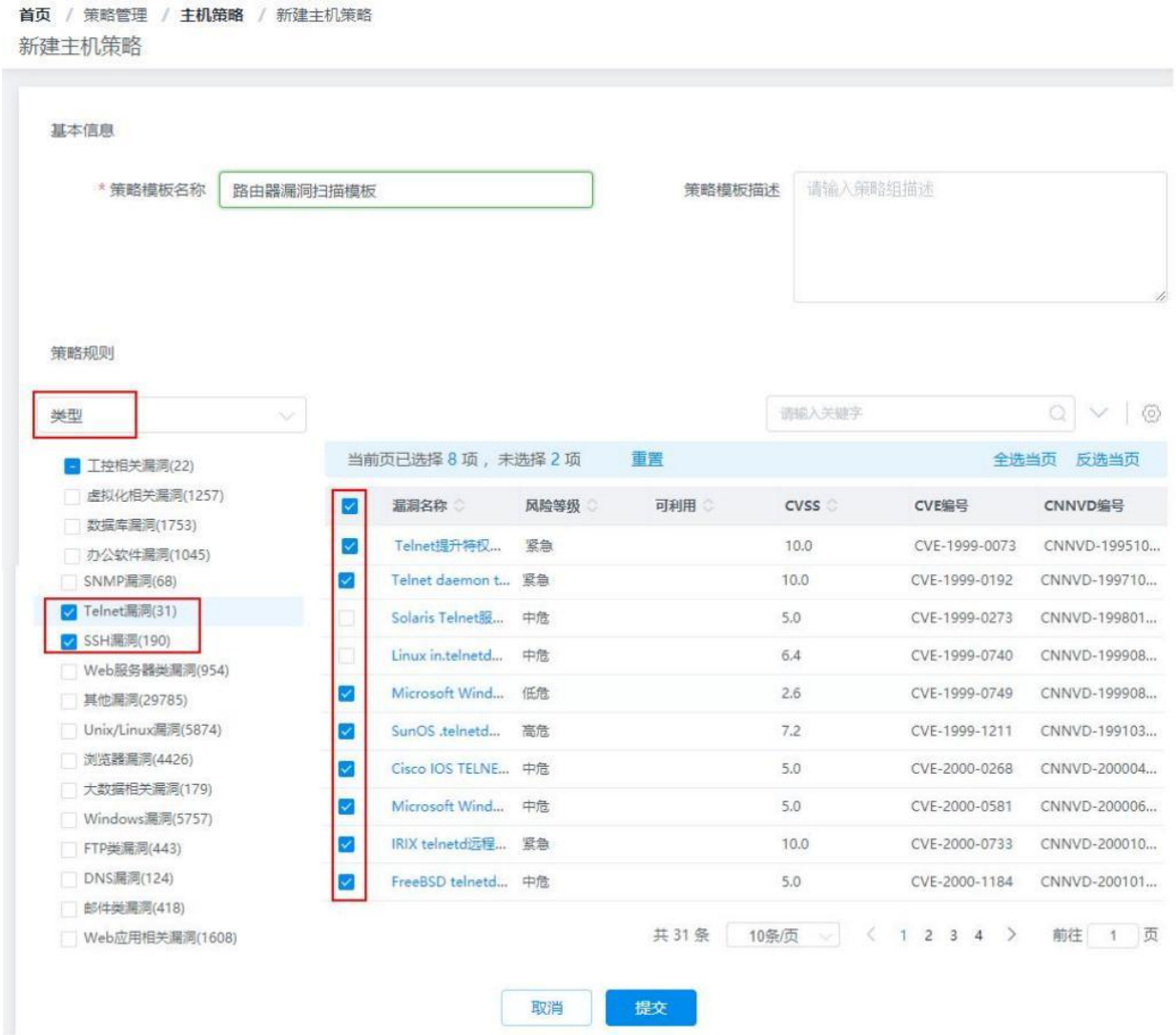



1. 用户登录后先进行资产管理设置，添加资产，便于后续对资产进行扫描，在菜单栏选择“资产管理>资产列表 ”，选择主机资产页签，点击<新增>。


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。


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) 漏扫扫描支持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）漏扫扫描支持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）。

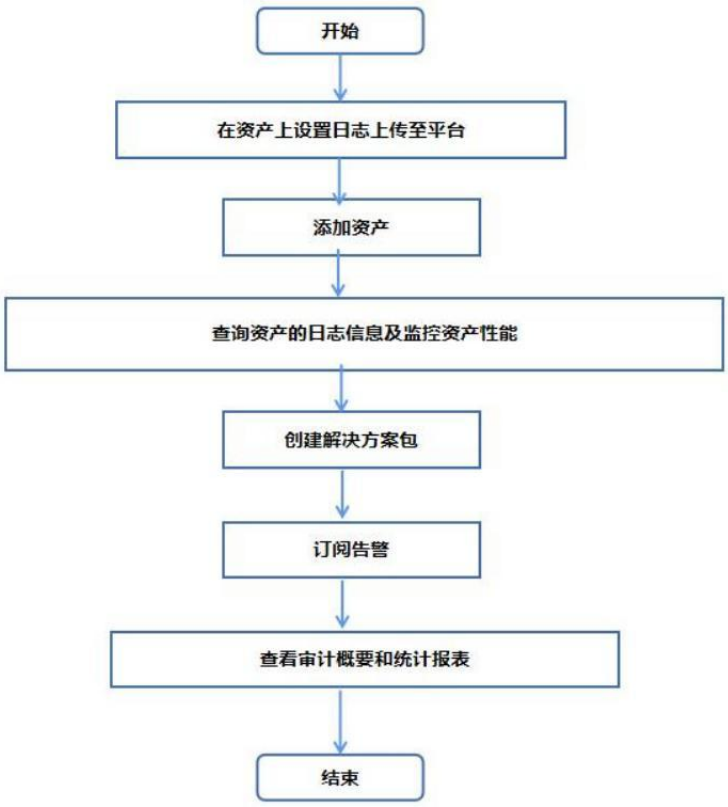
### (8) 漏洞扫描 SysLog 告警通知发送哪些数据？

- 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。
- 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。

- 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。
- 弱点信息数据，包括所属任务 ID、漏洞名称、漏洞详情等。

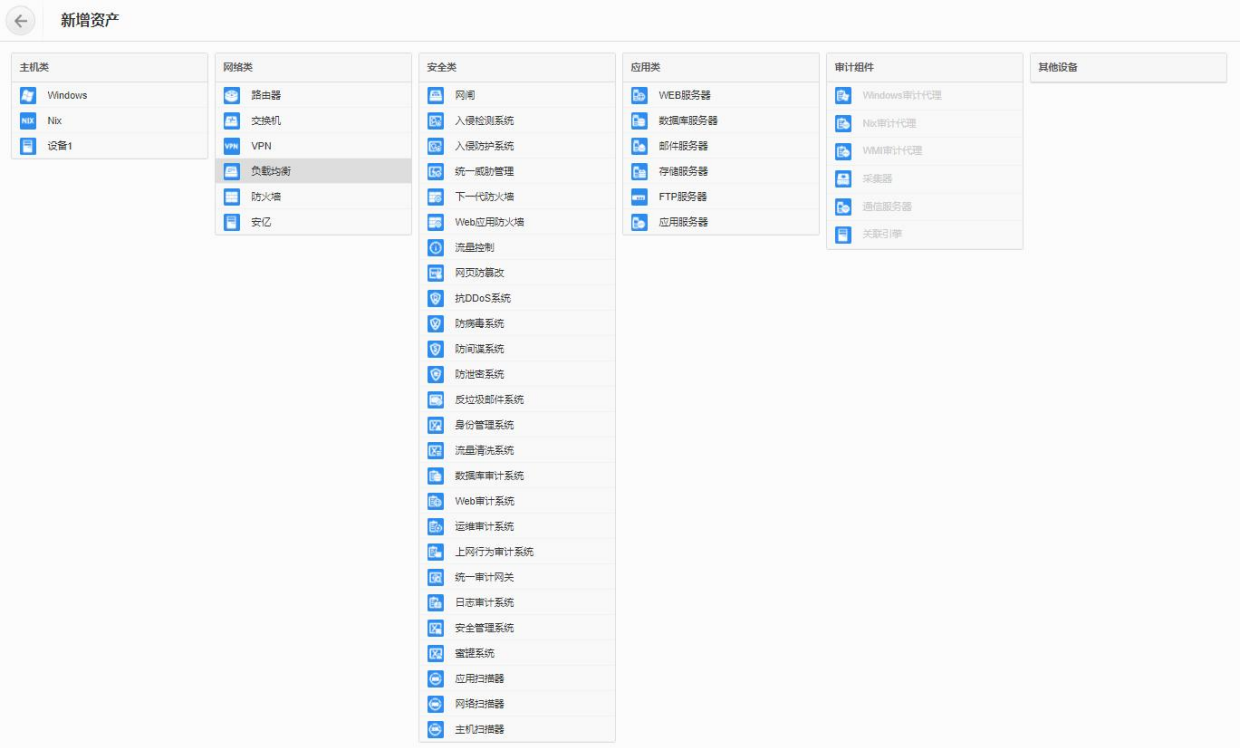
### 6.4.6. 日志审计

**(1) 日志审计设备如何进行接入配置？**

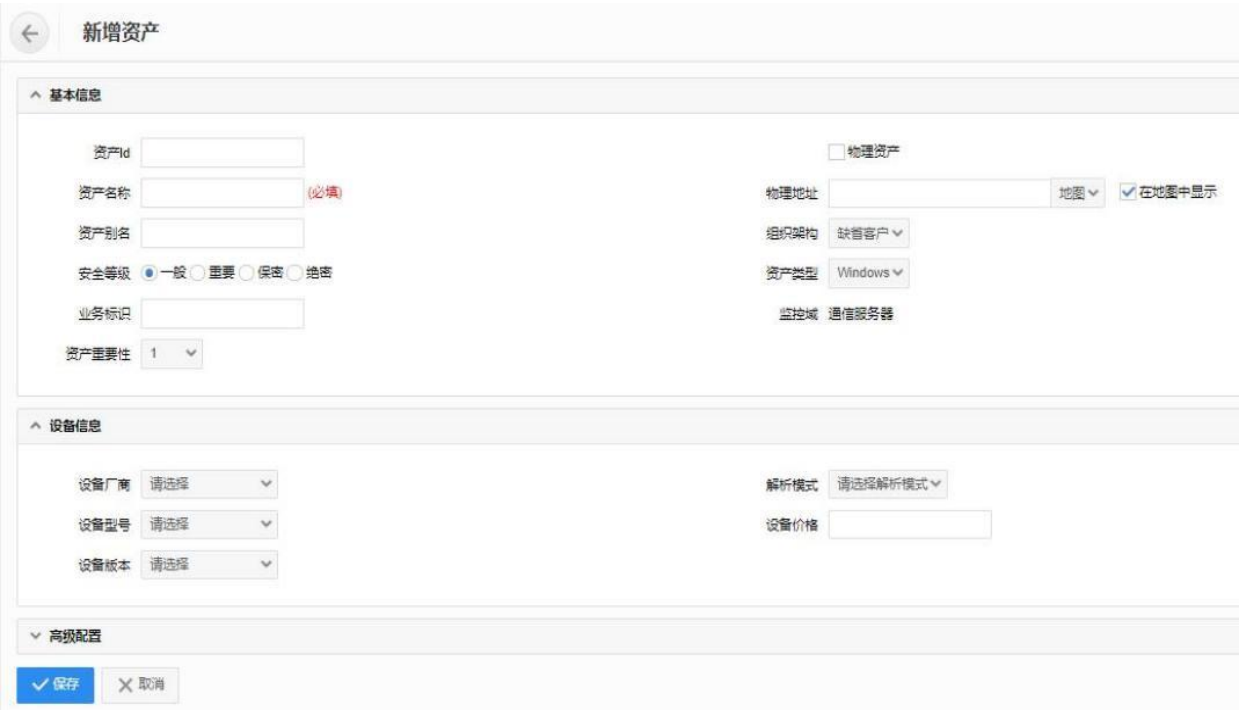



1. 首先在进行审计前，用户需要在资产上设置 Syslog 等协议将日志发送 至平台
2. 平台可自动发现通过 Syslog 等协议向平台发送日志的资产向平台发 送日志的资产，发现这些资产后，需要添加这些资产，在上边栏选择“资产管 理 ”，在左侧菜单栏选择“资产>全部资产 ”进入资产页面，点击<新增>。


进入新增资产页面，选择资产类型（如 Windows）。

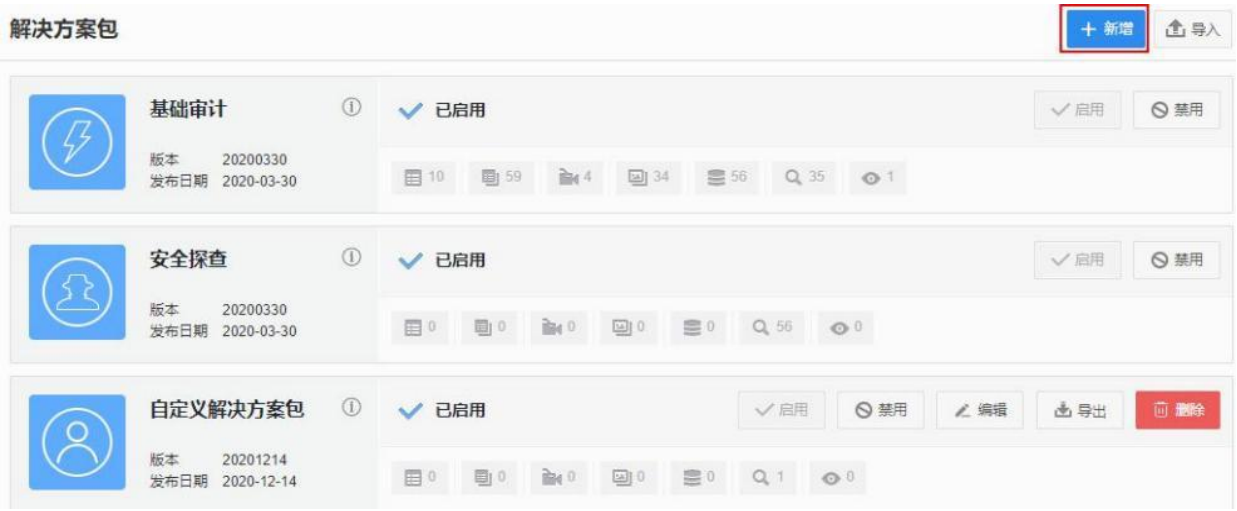



编辑相关信息，点击<保存>。




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。

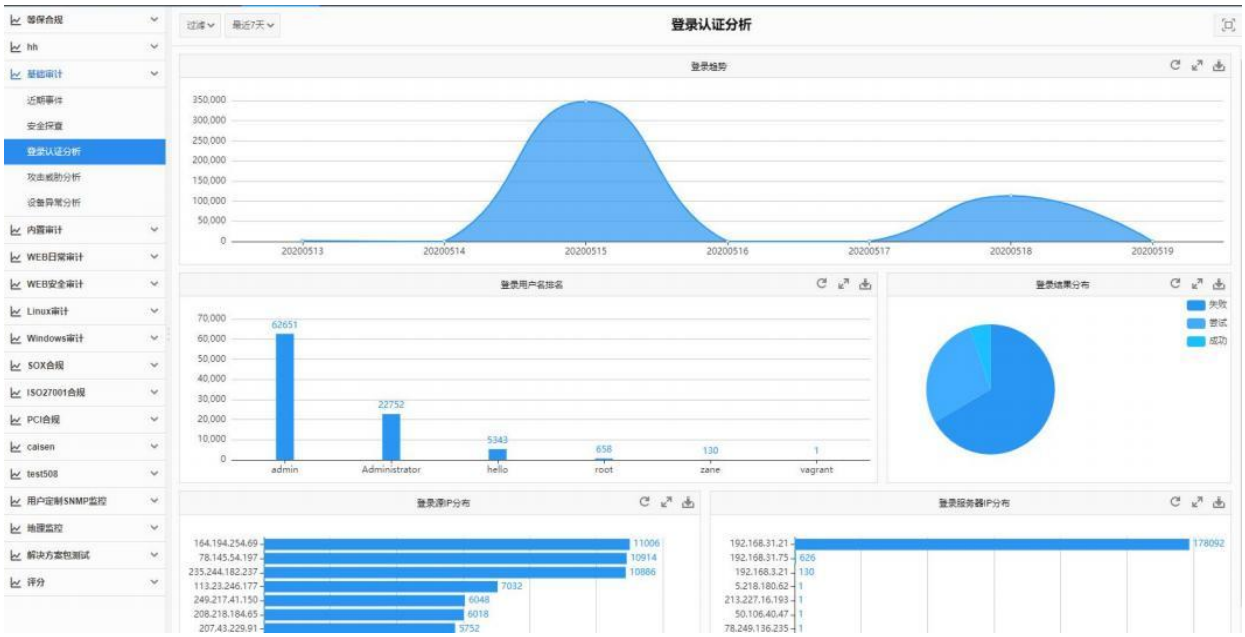



点击<新增>，编辑相关信息，点击<保存>。

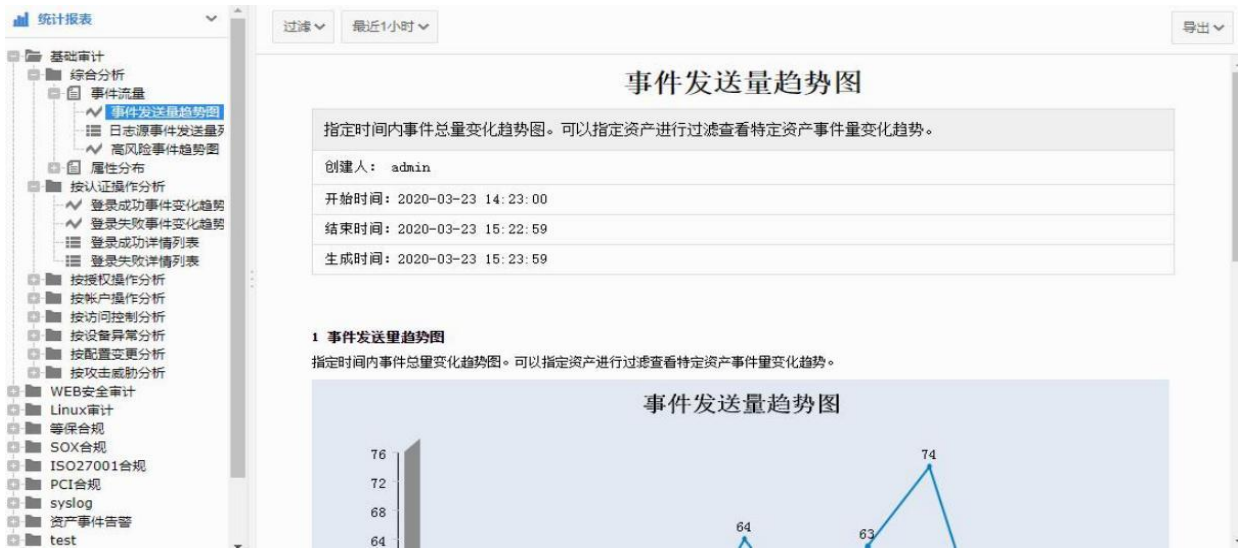

5. 用户还可订阅自己关注的告警事件，可第一时间了解资产的威胁态势，在上边栏选择“事件管理”，在左侧菜单栏选择“告警>告警订阅 ”进入告警订阅页面，选择未订阅页签。

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？**

日志审计对外开放的端口包括：

- tcp443 web 访问的端口
- tcp22 ssh 连接的端口
- udp514 syslog 接收日志端口
- tcp21 ftp 服务开放的端口
- 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。

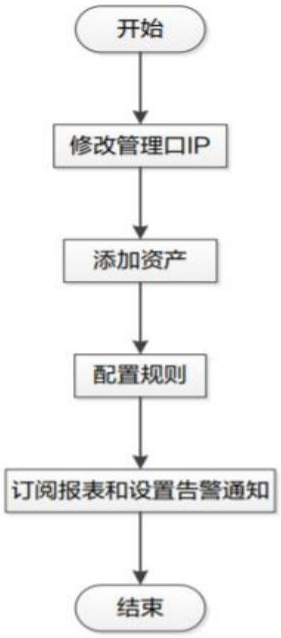
**(6) 日志审计配置自动备份的周期是如何定义的？**

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。

### 6.4.7. 数据库审计

#### 6.4.7.1. 数据库审计v1.0

**(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。

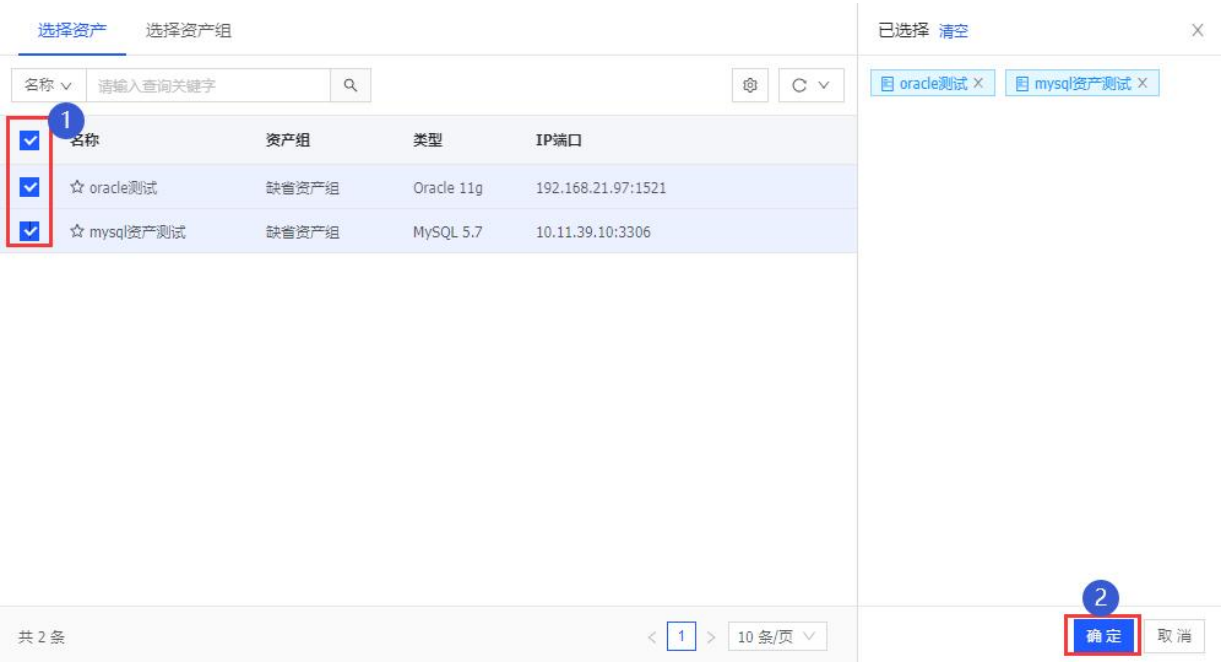

3. 然后配置数据库的安全规则和过滤规则，在菜单栏选择“规则配置>安全规则 ”进入安全规则页面，选择规则管理页签，点击<推荐>，切换至<全部>。


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>。

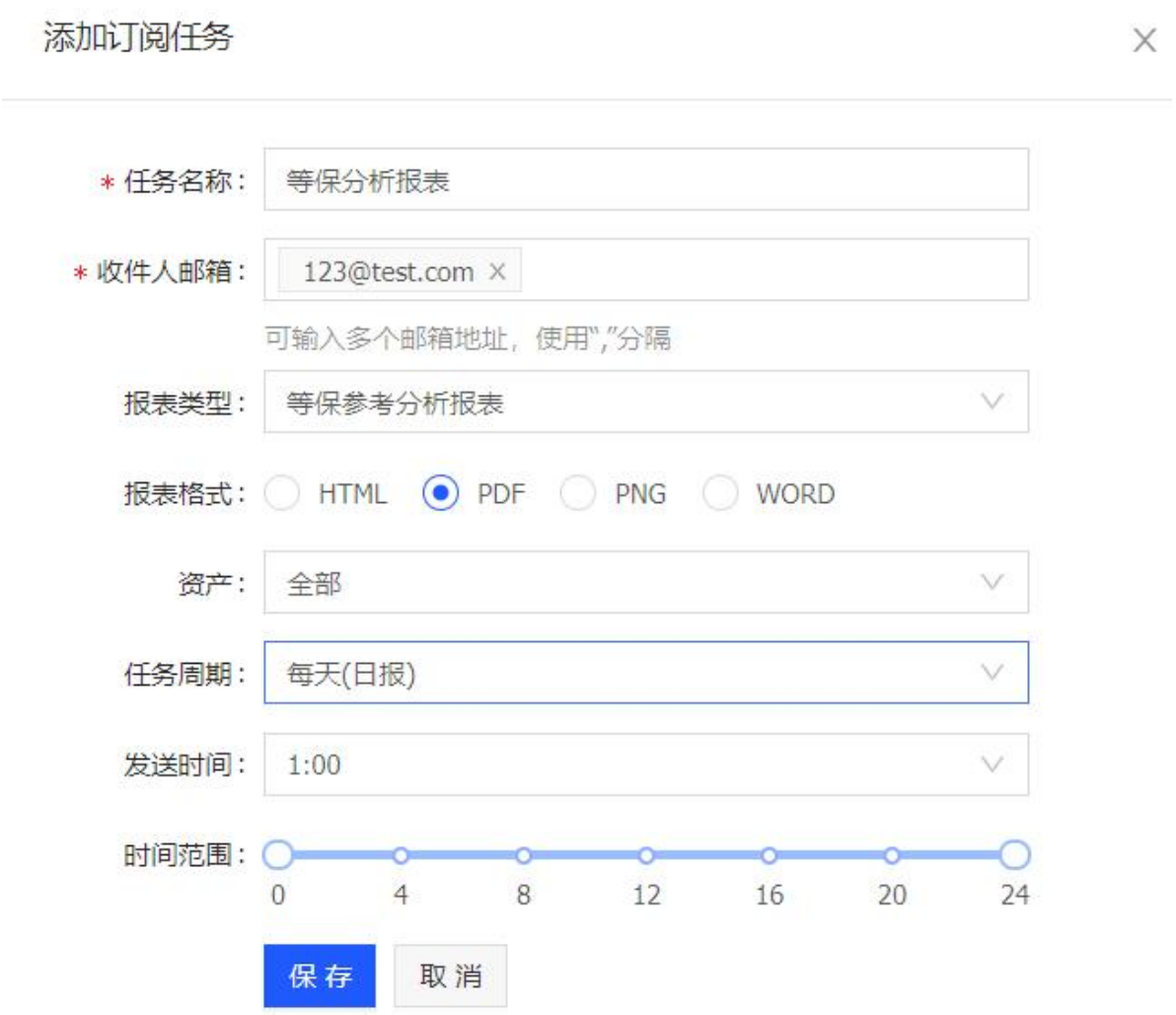

接着启用规则，在菜单栏选择“规则配置>安全规则”进入安全规则页面，选择规则管理页签，在规则列表中勾选目标规则，点击<启用选中项>。


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远程登录审计指的是，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或本地审计：

- 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会显示为远程登录的设备的IP，对所有支持的数据库协议都可用。

- 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。

#### 6.4.7.2. 数据库审计v2.0

数据库审计v2.0常见问题请参见《云等保专区-数据库审计 v2.0 用户指南》。

# 7. 附录

《云等保专区-云安全中心 v2.0 用户指南》

《云等保专区-主机安全 v2.0 用户指南》

《云等保专区-主机安全 v1.0 用户指南》

《云等保专区-Web应用防火墙 v2.0 用户指南》

《云等保专区-Web应用防火墙 v1.0 用户指南》

《云等保专区-下一代防火墙 v1.0 用户指南》

《云等保专区-堡垒机 v1.0 用户指南》

《云等保专区-漏洞扫描 v1.0 用户指南》

《云等保专区-日志审计 v1.0 用户指南》

《云等保专区-数据库审计 v2.0 用户指南》

《云等保专区-数据库审计 v1.0 用户指南》

《云等保专区-安全体检 用户指南》