天翼云 • 安全专区

用户使用指南

中国电信股份有限公司云计算分公司

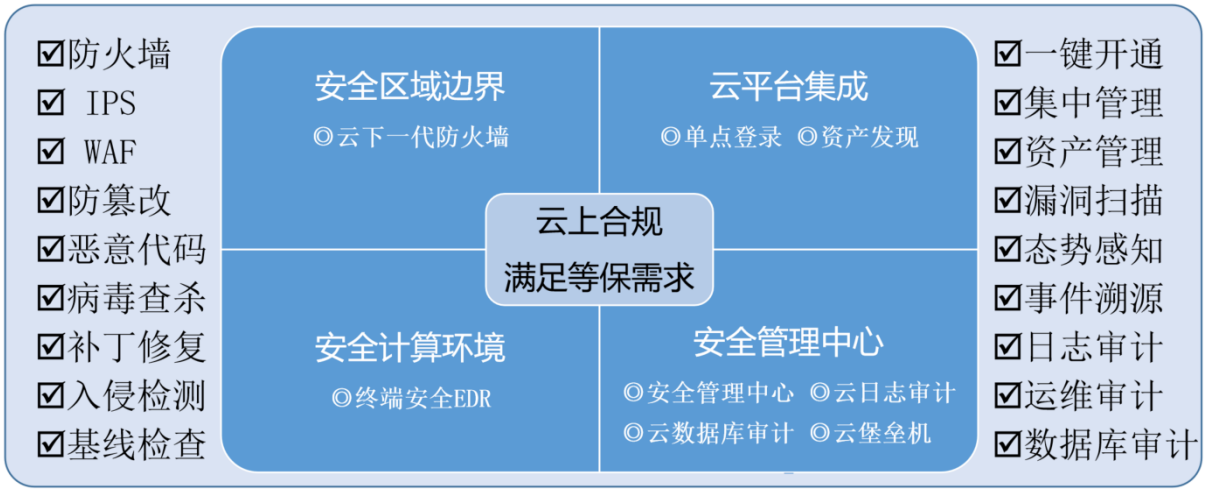
目 录

1. 产品介绍

1.1. 产品定义

安全专区是针对天翼云用户场景打造的安全产品，整合云安全管理中心、云防火墙、终端安全 EDR、云数据库审计、云日志审计、云堡垒机等各类云安全合规组件，具备云安全防护能力，满足等级保护防护需求。

安全专区为用户提供单点登陆、自动授权、即开即用、统一管理、弹性扩容、能力完善的云安全等保一体化合规解决方案。



1.2. 术语解释

等级保护：信息安全等级保护是指对国家重要信息、法人和其他组织及公民专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。《中华人民共和国网络安全法》在 2017 年 6 月 1 日施行，作为网络安全基础性法律，在第 21 条明确规定了“国家实行网络安全等级保护制度，要求网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”。

安全管理中心：针对信息系统的安全策略及安全计算环境、安全区域边界和安全通信网络三部分的安全机制，形成一个统一的安全管理中心，实现统一管理、统一监控、统一审计、综合分析且协同防护。通过智能分析模块，针对监控数据和审计数据进行关联分析，把握被保护系统的安全运维态势，对可能出现的安全事件进行预警，对组织的安全策略制定和配置管理策略的统一调整提供指导意见。对应等级保护安全管理中心技术要求。

云防火墙：云防火墙，是一款可以全面应对应用层威胁的高性能防火墙，集成入侵检测，恶意代码等功能，部署在网络边界提供外网入侵防御功能。对应等级保护安全区域边界技术要求。

终端安全 EDR：终端检测和响应是一种主动式终端安全解决方案，通过记录终端与网络事件（例如用户，文件，进程，注册表，内存和网络事件），并将这些信息本地存储在终端或集中数据库，结合已知的攻击指示器(Indicators of Compromise，IOCs)、行为分析的数据库来连续搜索数据监测任何可能的安全威胁，并对这些安全威胁做出快速响应，还有助于快速调查攻击范围，并提供响应能力。对应等级保护安全计算环境技术要求。

云数据库审计：云数据库审计（简称 DBAudit）能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高资产安全。对应等级保护集中审计技术要求。

云日志审计：云日志审计全面收集安全设备、网络设备、数据库、服务器、应用系统、主机等设备所产生的日志（包括运行、告警、操作、消息、状态等）并进行存储、监控、审计、分析、报警和报告的系统。对应等级保护集中审计技术要求。

云堡垒机：云堡垒机为了保障网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段监控和记录运维人员对网络内的服务器、网络设备、安全设备、数据库等设备的操作行为以便集中报警、及时处理及审计定责。对应等级保护集中审计技术要求。

1.3. 产品功能

1.3.1. 安全管理中心

安全态势总览

作为云用户安全驾驶舱的安全管理中心，具有集中管控云环境整体安全态势的功能。安全管理员通过安全态势总览可监管所有资产受保护状态、安全防御能力部署情况、云环境整体安全评分、实时风险/威胁趋势分析。

资产安全管理

平台识别云用户所有资产，并自动收集资产的安全监测数据，提供每个资产详细的安全数据分析评估能力。云用户通过资产安全管理功能对所有资产的安全配置状态、审计状态、漏洞数据、基线数据、补丁数据、告警数据安全级别进行统一管控；对应具体的资产及应用，平台提供资产安全分析、时间轴分析及资产安全报告功能。

安全风险分析

汇总全网安全专区实时防御产生的风险数据，为云用户提供集中查询分析、统计溯源、全局监测资产风险项目的管理手段。风险分析覆盖全网主机漏洞、应用漏洞、基线检查、系

统补丁、病毒查杀五项详细安全数据，安全管理员可按时间、类别、级别、资产、风险项、修复状态等多维度进行查询及趋势分析。

威胁告警分析

汇总全网安全专区实时防御产生的威胁告警数据，为云用户提供集中查询分析、统计溯源、全局监测网络威胁项目的管理手段。威胁告警数据全面覆盖防火墙/WAF/IPS 等网络告警、终端安全 EDR 系统终端侧告警、日志/数据库审计行为类告警，安全管理员可按时间、类别、级别、资产、威胁告警项、处理状态等多维度进行查询及趋势分析。

安全运维报告

根据用户云环境的安全态势及风险威胁处置数据生成安全运营报告。

安全漏洞扫描

安全管理中心集成主机漏洞及应用漏洞扫描功能，能够帮助用户高效、全方位的检测出服务环境中的各类脆弱风险，并提供专业、有效的安全分析和修补建议。

组件集中管理

安全管理中心集中管理全网安全专区能力组件，已部署的组件规格、部署区域、版本许可信息、运行状态等配置信息统一展现，安全管理员从天翼云控制台即可单点登录所有安全组件进行策略配置及备份策略，无需繁琐的分别登录组件进行管理。

1.3.2. 云防火墙

云防火墙以用户识别、应用识别为基础，为用户提供应用层防火墙、入侵防护、防病毒、反 APT、VPN、智能带宽管理、多出口链路负载均衡、内容过滤、URL 过滤等多重安全功能。

应用访问控制

包括但不限于 4-7 层访问控制、入侵防御、病毒过滤等安全功能。

Web 应用防御

包括防跨站、防 SQL 注入、防篡改、防木马、防黑客攻击等。

网页防篡改

集成网页防篡改功能，Web 服务器安装防篡改客户端后由防火墙进行管理。

威胁情报

能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。

恶意代码检测

支持远程控制木马或者病毒等恶意软件检测，能对检测到的恶意软件行为进行深入的分析，展示外部命令控制服务的交互行为和其他可疑行为。

1.3.3. 云堡垒机

云堡垒机为用户提供运维审计解决方案，运维人员可通过云堡垒机远程访问云主机，实现统一账号管理、双因子、认证管理、权限管理、审计管理，解决系统账号复用、运维权限混乱、运维过程不透明等问题。

支持 RDP、VNC、X11 等图形终端操作的连接情况下进行记录及审计。

记录发生时间、发生地址、服务端 IP 地址、客户端 IP 地址、操作指令、返回信息、操作备注、客户端端口号、服务器端口号、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息。

1.3.4. 云日志审计

云日志审计通过对用户的网络、安全、应用等系统日志进行全面的标准化处理，帮助用户及时发现各种安全威胁、异常行为事件，满足网络安全法对日志数据留存 6 个月以上的要求。

支持从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段。

对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义。

1.3.5. 终端安全 EDR

终端安全管理 EDR 系统，提供集中管理手段对各客户端系统进行安全事件分析、杀毒、基线核查等功能。

入侵检测

包含智防、智控、智响应模块以及服务端防护模块，Webshell 检测、暴力破解检测。

基线检查

支持对指定终端/终端组进行合规性检查，对不合规的检查项提供设置建议。一键式操作，可视化展示终端的基线合规检查结果

病毒查杀

支持快速查杀、全盘查杀、通用病毒清除、多引擎扫描、CPU 资源占用设置、病毒文件自动隔离等功能。

补丁修复

支持开启定期进行指定终端组的漏洞扫描、对指定终端组设置漏洞扫描后进行自动修复并对终端补丁包获取服务器地址进行自定义设置。

1.3.6. 云数据库审计

云数据库审计系统可通过设计其相关业务策略，实现审计符合业务策略的网络行为、跟踪访问重要数据源的网络行为，发现不符合业务策略的不法网络行为。

支持绝大部分数据库类型审计，支持 Oracle、SQL-Server、DB2、MySQL、MariaDB、Informix、postgresql、sysbase、cache、ES、Hive、HBASE、MongoDB、Redis 等数据库。

审计

通过对网络行为进行的记录，可用来分析网络状况和确定网络使用者的相关责任的活动。

策略

根据业务需求，而制定的网络行为分析引擎。产品的核心功能，对网络行为进行采集的分析引擎进行配置，将通过引擎的数据包过滤后，提供给审计功能使用。

告警

包含告警规则设置和告警事件的查看功能告警规则，系统对审计事件之间的关系进行形式化描述。针对符合策略的事件进行关联分析。抽取出对于安全管理人员真正有用的安全信息，提供实时告警，从而协助安全管理人员快速识别安全事故。

事后调查取证

对于所有行为能够进行事后查询、取证、调查分析，出具各种审计报表报告。

安全预警

对入侵和违规行为进行预警和告警，并能够指导管理员进行应急处理；

数据操作实监控

对所有外部或是内部用户访问数据库和主机的各种操作行为实时监控；

1.4. 产品优势

快速合规方案：产品套餐依据等级保护要求针对云上各种应用场景进行合规设计，产品自动交付，一次购买可满足云用户多个系统的等保合规技术要求，快速解决云上合规整改问题。

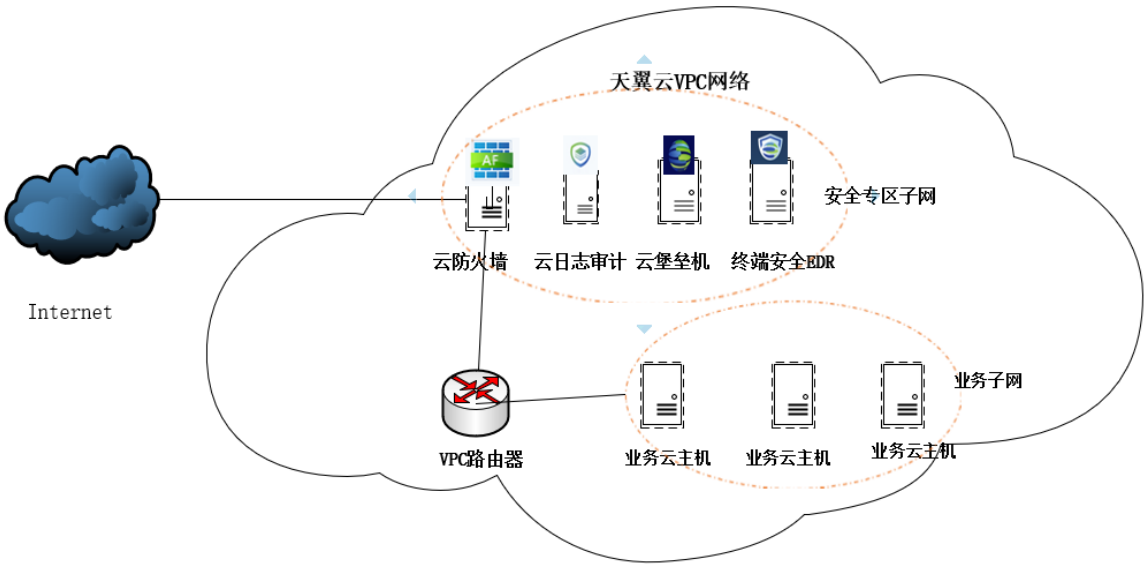
平台紧密集成：自动识别所有云资产，关联安全组件能力自动评估云用户资产安全态势，用户使用云平台账号即可登录安全专区实施所有安全管理工作。

网端管三层防护：提供覆盖网络安全、终端安全、应用安全、数据安全各层面的安全能力，网端管联动分析，为云上应用系统安全运行提供全面保障。

集中管理全管控：集中管理用户云上资产安全，集中管理云上安全设备，集中管理云网边界、虚机系统、业务系统的漏洞、告警、用户行为等安全运行数据，提供全覆盖的安全态势管理能力。

1.5. 应用场景

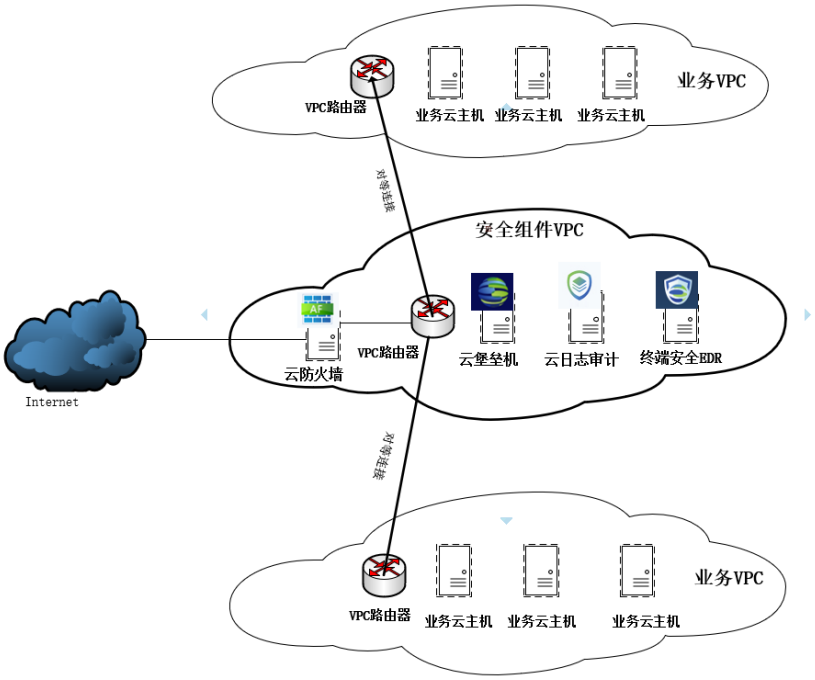
1.5.1 单 VPC 场景



用户在天翼云上一个 VPC 内部署了业务系统，需要进行安全防护。

部署方案：在 VPC 内新建一个子网，把安全专区开通到新开的子网内，弹性 IP 部署在安全专区的云防火墙外联接口，业务服务器外部流量通过安全专区子网进行安全管理。

1.5.2 多 VPC 场景



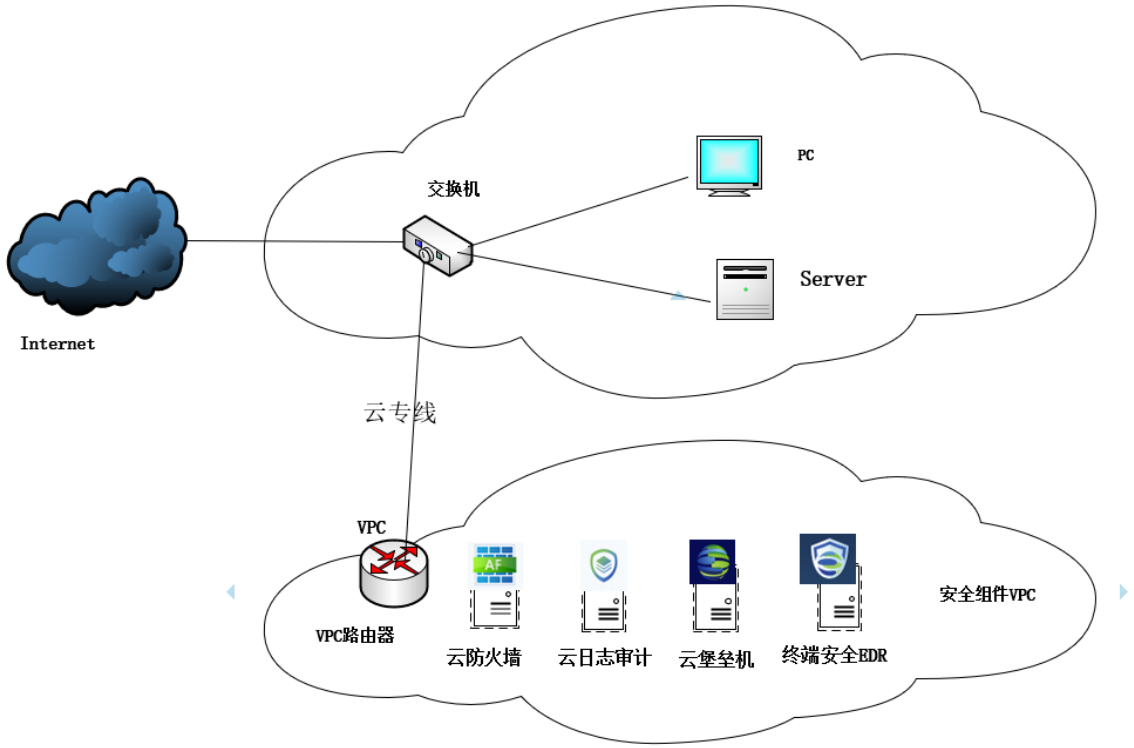
用户在天翼云上同一个数据节点多个 VPC 内部署了业务系统，需要进行安全防护。

部署方案：

1）可按单个 VPC 的方式分别部署多个安全专区。

2）新建一个安全专区 VPC，在安全专区 VPC 内开通安全专区服务，业务 VPC 通过对等连接接入安全专区 VPC，由安全专区统一对所有 VPC 业务进行安全防护。

1.5.3 线下引流场景



用户的业务在本地机房，需要进行安全防护。

部署方案：在天翼云上部署一个安全专区 VPC，在安全专区 VPC 内开通安全专区服务，线下机房通过云专线策略路由接入到安全专区，由安全专区同对线机房内业务进行安全防护。

2. 购买指南

2.1. 规格

安全专区产品按等保级别订制 4 个套型号销售，套餐功能特性及安全组件规格如下：

等保级别	套餐型号	套餐安全功能特性	可选安全组件及规格
二级等保	入门版	云防火墙（含 WAF/防篡改模块）	云防火墙：100M/200M/300M/400M/500M/800M/1G/1.6G
		云日志审计	云日志审计：10/20/50/100/200/300/500 资产
		主机漏扫	安全管理中心基础版：10/20/50/100/200/300/500 资产
		安全管理中心	
	基础版	云防火墙（含 WAF/防篡改模块）	云防火墙：100M/200M/300M/400M/500M/800M/1G/1.6G
		云日志审计	云日志审计：10/20/50/100/200/300/500 资产
		终端安全 EDR（防病毒/补丁/基线/微隔离）	终端安全 EDR：实际资产数
		云堡垒机	云堡垒机：10/20/50/100/200/300/500 资产
		主机漏扫	安全管理中心基础版：10/20/50/100/200/300/500 资产
		安全管理中心	
三级等保	高级版	云防火墙（含 WAF/防篡改模块）	云防火墙：100M/200M/300M/400M/500M/800M/1G/1.6G
		云日志审计	云日志审计：10/20/50/100/200/300/500 资产
		终端安全 EDR（防病毒/补丁/基线/微隔离）	终端安全 EDR：实际资产数
		云堡垒机	云堡垒机：10/20/50/100/200/300/500 资产
		主机漏扫	安全管理中心基础版：10/20/50/100/200/300/500 资产
		安全管理中心	

		云数据库审计	云数据库审计：100M/200M/400M/600M
	旗舰版	云防火墙（含 WAF/防篡改模块）	云防火墙：100M/200M/300M/400M/500M/800M/1G/1.6G
		云日志审计	云日志审计：10/20/50/10/200/300/500 资产
		终端安全 EDR（防病毒/补丁/基线微隔离）	终端安全 EDR：实际资产数
		云堡垒机	云堡垒机：10/20/50/10/200/300/500 资产
		主机漏扫	安全管理中心高级版：10/20/50/100/200/300/500 资产
		应用漏扫	
		安全管理中心	
		云数据库审计	云数据库审计：100M/200M/400M/600M

安全专区根据等保等级要求配置所需的安全能力，不同套餐包含的安全组件参见上表，其中云防火墙及云数据库审计组件按应用吞吐量授权，安全管理中心、云日志审计、云堡垒机、终端安全 EDR 组件按资产数量授权。用户在选定套餐后，根据业务的资产数及需求量选定组件规格。

2.2. 试用

本产品不支持试用。

2.3. 购买

安全专区按套餐购买，用户可根据自身业务规模选购对应的组件规格，具体价格请参照天翼云官网。

安全专区根据用户开通的套餐及规格自动在用户指定开通的 VPC 内新开相应的功能承载虚机。根据等级保护的要求，安全能力组件需要独立的网管网段。**因此强烈建议购买开通之前，用户在 VPC 内新创建一个子网作为安全专区的开通子网段，然后在订购页面选定新子网进行业务开通。安全专区开通后，不能对安全专区的承载虚机进行任何手动操作。**

2.4. 升级

用户可以通过升级操作，增加安全组件的规格。

2.5. 续订

用户可以通过续订，延长产品服务有效时间。

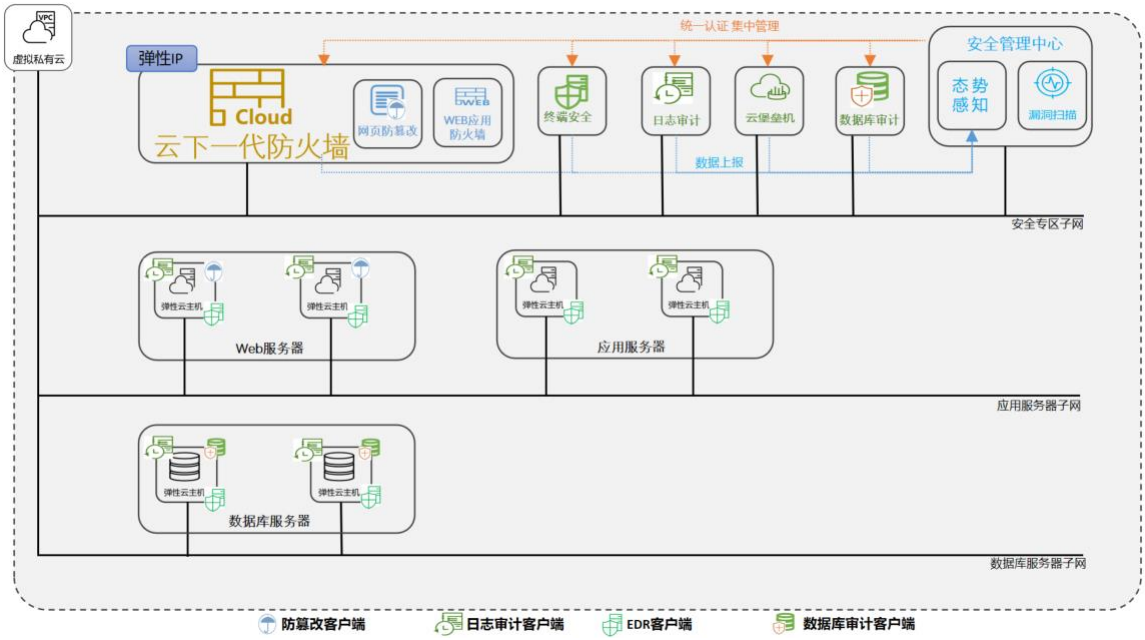
2.6. 退订

本产品不支持退订。

3. 安装配置指南

本章节为安全专区的快速安装指引，根据以下内容完成组件的上线配置，为天翼云安全专区用户安全运维及等保合规助力。

3.1. 专区拓扑图



3.2. 上线配置步骤

安全专区整合了安全管理中心、云防火墙、云日志审计、云数据库审计、云堡垒机、终端安全 EDR 等组件，用户采购开通后，需要进行以下初始安装配置，才能正常使用。

安全组件	安装内容及步骤	备注
云防火墙	VPC 环境调整	请参考 3.5 章节
	网络配置	
	访问策略配置	
	安全策略配置	
	网络割接	
	网络测试	
云堡垒机	运维账号	请参考 3.6 章节
	添加资产	
	管理授权	
	映射端口	

	登录运维	
云日志审计	添加资产	请参考 3.7 章节
	采集器配置	
	客户端安装	
终端安全 EDR	客户端安装	请参考 3.8 章节
	策略配置	
云数据库审计	部署方式	请参考 3.9 章节
	添加审计策略	
	添加保护对象	
	客户端安装	

云防火墙：部署在网络边界提供边界防御能力，上线配置工作包括 VPC 环境调整、网络配置、策略配置、网络割接等几个部分，详细操作指引请参考 3.5 章节。

云堡垒机：负责审计业务系统运维操作，配置包括运维账号管理、添加资产及授权，详细操作指引请参考 3.6 章节。

云日志审计：集中收集并审计所有业务系统及安全产品的系统日志，需添加资产、配置采集器、安装配置客户端，详细操作指引请参考 3.7 章节。

终端安全 EDR：部署在业务系统主机，提供防病毒、补丁管理、入侵侦测响应等端点安全防护能力，需要在业务主机系统安装客户端，详细操作指引请参考 3.8 章节。

云数据库审计：集中收集并审计所有数据库系统操作日志，配置包括客户端安装和数据库信息录入，详细操作指引请参考 3.9 章节。

安全组件配置完成后，安全管理中心可实时从安全组件收集全网资产的风险、威胁安全数据，关联分析评估用户云环境的安全态势。

3.3. 安全专区登录

3.3.1. 管理员登录

登录天翼云的控制中心，点击『安全产品』→『安全专区』，即展示当前账号所拥有的安全专区实例。选择对应的安全专区实例，在『操作』列的『进入通道』，点击进行页面跳转，即可进入安全专区管理界面。

3.3.2. 普通用户登录

安全管理员、审计人员及运维人员，直接访问安全管理中心。登录页面下图所示，输入安全专区账号用户名、密码及验证码后点击确定即可完成登陆。

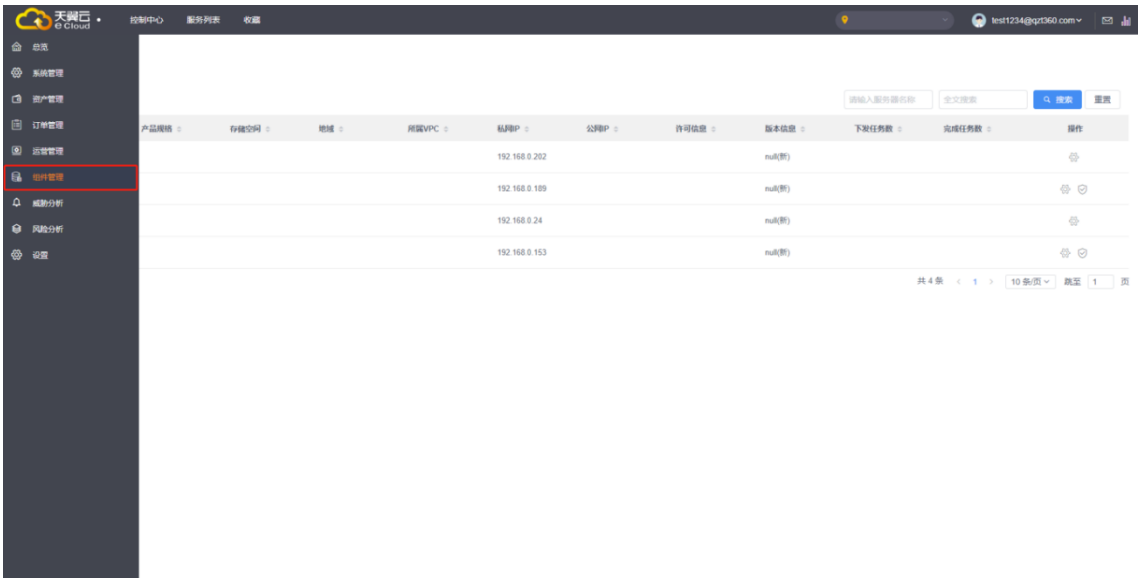
登录成功，进入安全管理中心首页。

首页最左侧是安全管理中心功能菜单，鼠标移至菜单图标上，可打开菜单。用户可以通

过菜单进行安全管理、配置及查询分析。

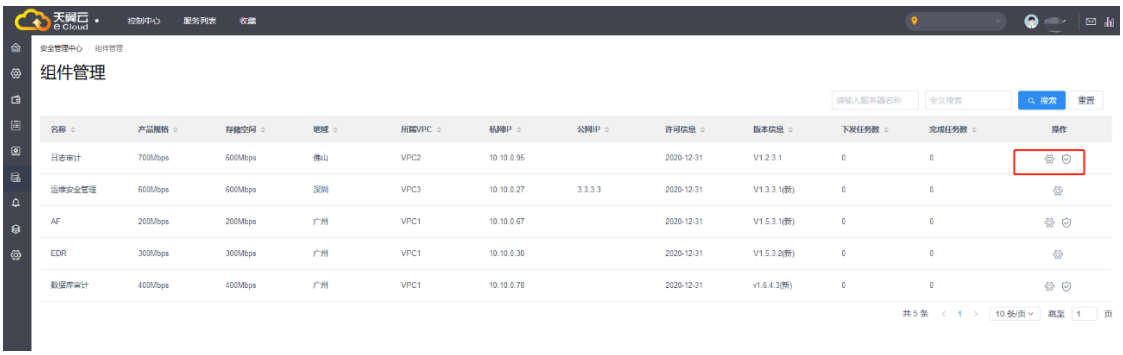
3.3.3. 访问安全组件

打开左侧菜单栏进入『组件管理』



该页面可管理安全专区所有安全组件

组件列表承载主机名称、所在数据中心、所属 VPC、IP 地址、许可及版本等信息。点击『操作』→『进入管理』，进入该组件的配置管理界面。



3.4. 创建用户账号

根据等级保护要求，安全管理包括三个角色：安全管理员、安全审计员、运维人员。

天翼云主账号拥有系统管理员的权限，其余角色需要在安全管理中心平台进行用户权限配置。

3.4.1. 用户管理页面

安全管理员点击左侧导航栏的【系统管理】，进入【用户管理】页面可进行账号管理。

3.4.2. 创建账号

点击【添加用户】，按照页面提示完整填写用户信息，添加新的账号。

打开用户注册信息窗口

[用户名]：填写用户邮箱作为用户名（系统将发送邮件到该邮箱）

[手机号]：填写用户手机号（登录接收验证码）

[角色分配]：

✓ 安全管理员：负责安全策略配置

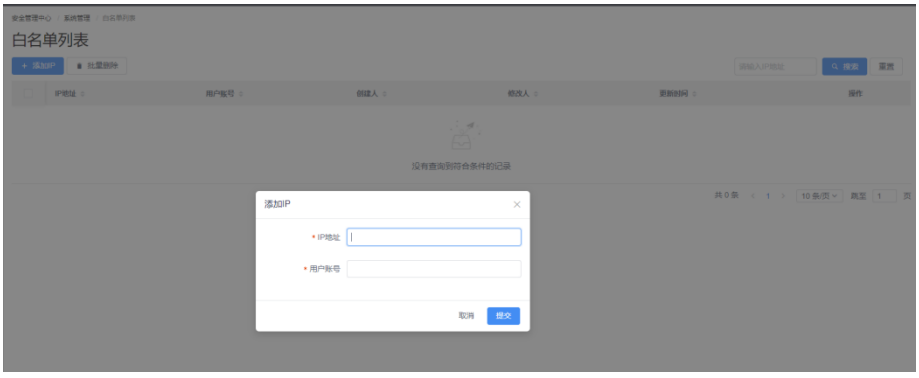
✓ 审计人员：可查看及管理日志

✓ 运维人员：业务系统运维人员只能登录云堡垒机，对业务系统进行操作

3.4.3. 账号访问控制

如需限制账号登录地址，可在【系统管理】→『白名单列表』进行操作。

点击『添加 IP』，设置白名单信息。



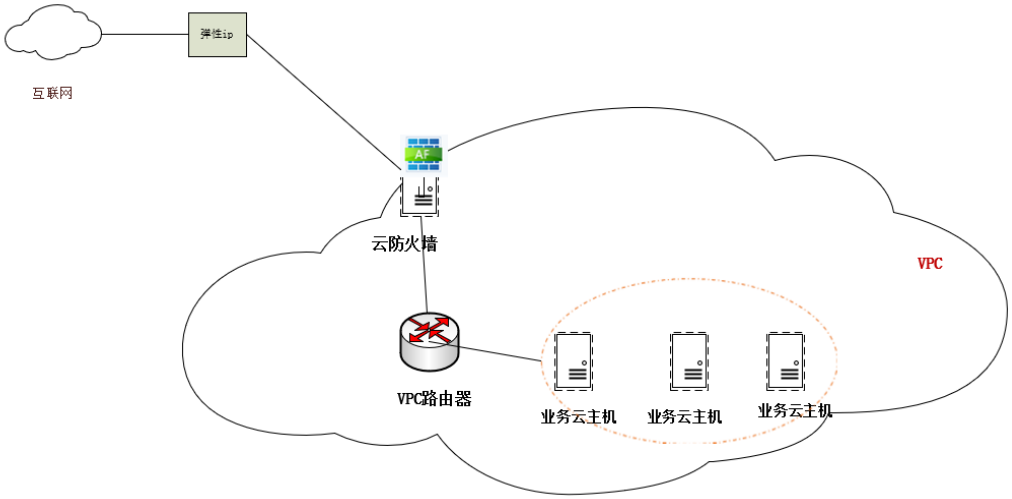
[IP 地址]：可登录访问安全专区的客户 IP 地址，

[用户账号]：为登录安全专区的账号。

3.5. 云防火墙配置

云防火墙作为边界设备，管控 VPC 内外网进出流量及拦截分析风险行为数据，为云上业务提供漏洞攻击防护、web 应用防护、防范僵尸网络、检测内容安全等多重安全功能。

云防火墙在客户云环境内部署，需要作为三层路由的出口网关，链路上串接互联网到 VPC 内网的流量通道。



如拓扑图所示，云防火墙的接入需要接管业务弹性 IP，引导业务流量通过防火墙实现对网络边界防御。

部署方式：把弹性 IP 绑定到防火墙的网卡上（如果弹性 IP 已经绑定部署业务系统虚机，需要先将弹性 IP 解绑），配置防火墙的地址转换策略，映射到云主机的端口上，业务应答数据通过防火墙返回互联网客户端。

客户可根据自身情况进行业务网络与防火墙的调整。购买天翼云安全专区组件前已有互联网业务进行的情况下，防火墙的接入需要对 VPC 的网络调整割接。如属于天翼云新客户，则需要为防火墙另外购买弹性 IP。

部署云防火墙前，请先对 VPC 内的云主机地址、端口、网络情况进行全面分析，记录下原有云主机的弹性 IP 和 VPC 网内网卡地址的绑定关系。解绑弹性 IP 时，会导致互联网中断，请选择在合适时间内进行云防火墙上线。

3.5.1. VPC 环境调整

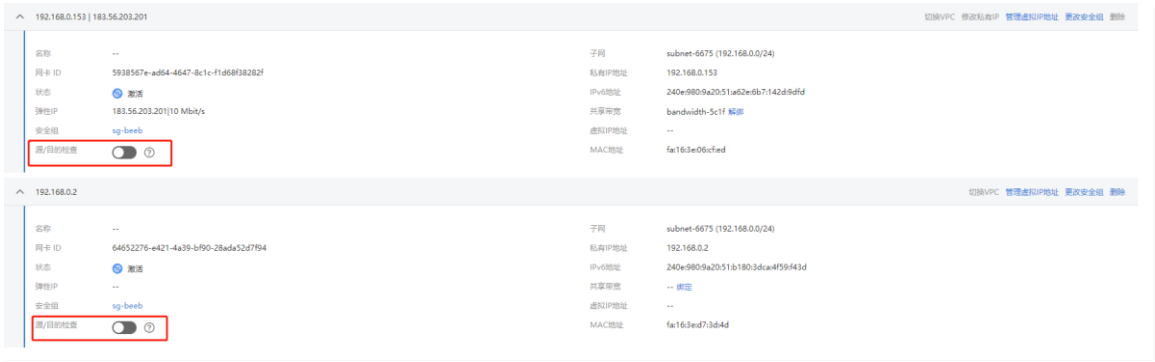
云防火墙需要实现 IP 地址转换功能，所以需要关闭云主机的网络接口 IP 地址检查，同时放通相关网络端口。

关闭云防火墙虚机网络检查

在【天翼云控制中心】页面中的『控制中心』→『计算』→『弹性云主机』，找到承载云防火墙（AQZQ-AF-***）的云主机。

点击该云主机名称，选择网卡，确认该云主机下有两个网卡。

将所有网卡的『源/目的检查』选项设置关闭。



确认网卡的安全组是否放通业务流量端口（必须放通 TCP/443 端口）。

进入『控制中心』→『网络』→『虚拟私有云』，检查安全专区所在 VPC 子网，详情如图所示，记录子网“IPv4 网络”与“网关”。

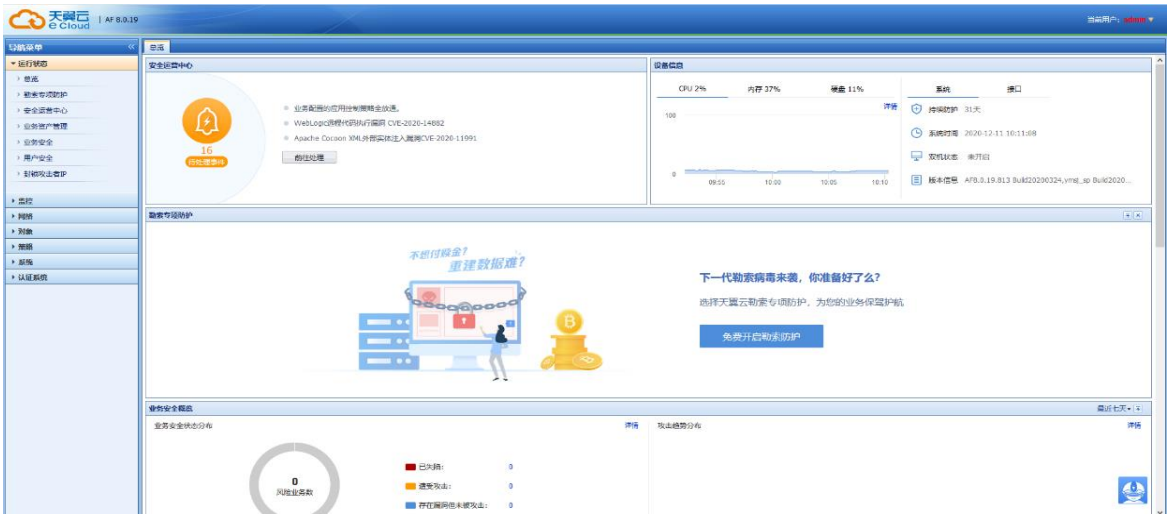
3.5.2. 网络配置

配置防火墙的 IP 地址及路由，确认防火墙的网络连通。

配置网卡

从组件列表登录云防火墙 web 管理界面（参考 3.3.3 章节），在【安全专区】页面中『组件管理』登录云防火墙管理。

云防火墙管理页面如下图所示：

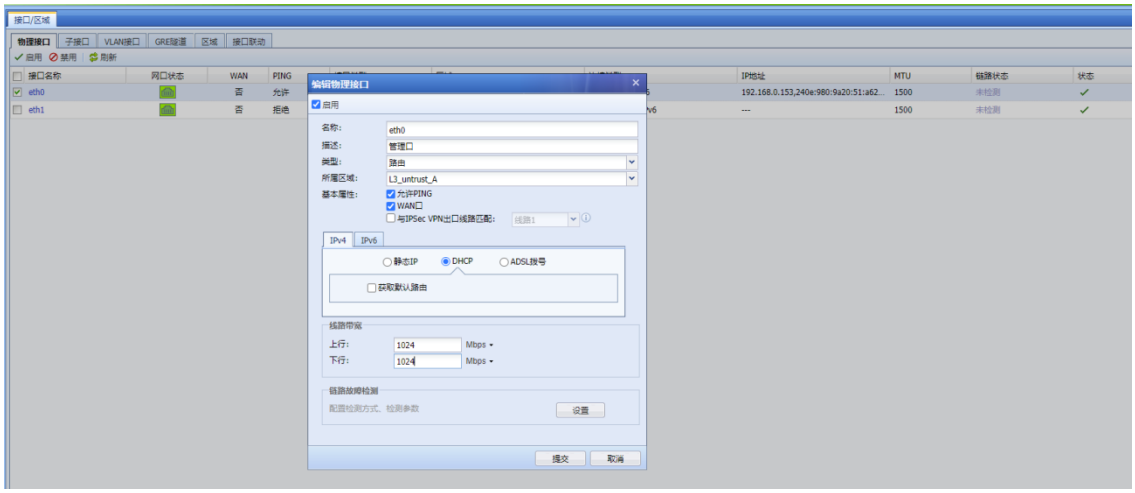


点击 『网络』→『接口/区域』→『物理接口』，列出网卡。

eth0 作为网络边界外网口，需进行以下配置：

点击“eth0”网卡，打开接口配置窗口，并根据弹性 IP 数量进行配置：

1、 单一弹性 IP 场景配置：



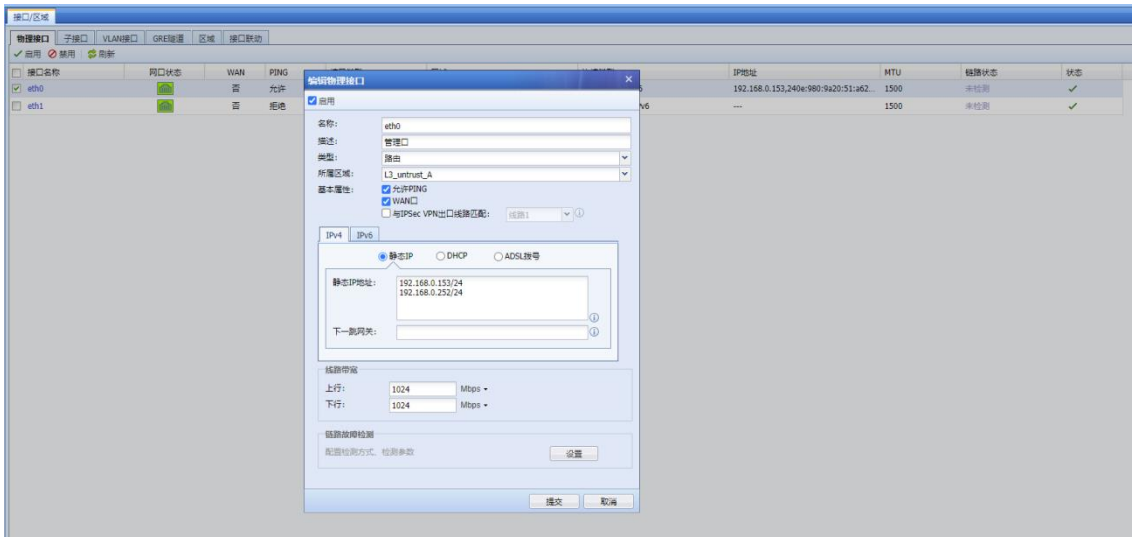
[区域]：选择“L3_untrust_A”，设置网卡所在区域；

[基本属性]：勾选“允许 PING”“WAN 口”；

[线路带宽]：“上行\下行”设置 1024Mbps。

[IPv4]:默认选择“DHCP”，保持默认选择，无需更改。；

2、 多个弹性 IP 场景配置：



[区域]：选择“L3_untrust_A”，设置网卡所在区域；

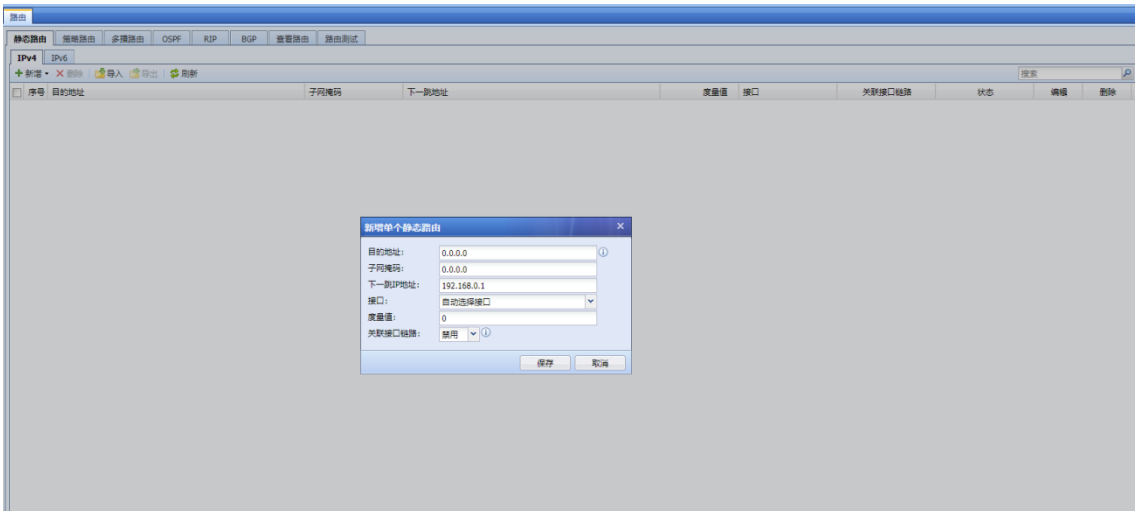
[基本属性]：勾选“允许 PING”“WAN 口”；

[线路带宽]：“上行\下行”设置 1024Mbps。

[IPv4]： 勾选“静态 IP”，在 IP 地址栏填写防火墙的私有 IP 及其绑定的虚拟 IP，虚拟 IP 与弹性 IP 一一对应（虚拟 IP 的申请及绑定通过天翼云控制台操作）；

配置路由

为防火墙设置默认路由，在『网络』→『路由』→『静态路由』→『IPV4』下新增单个静态路由，如下图：



[目的地址]：0.0.0.0

[子网掩码]：0.0.0.0

[下一跳 IP 地址]：设置为 eth0 的网关（参考 3.4.1 已记录的子网网关）；

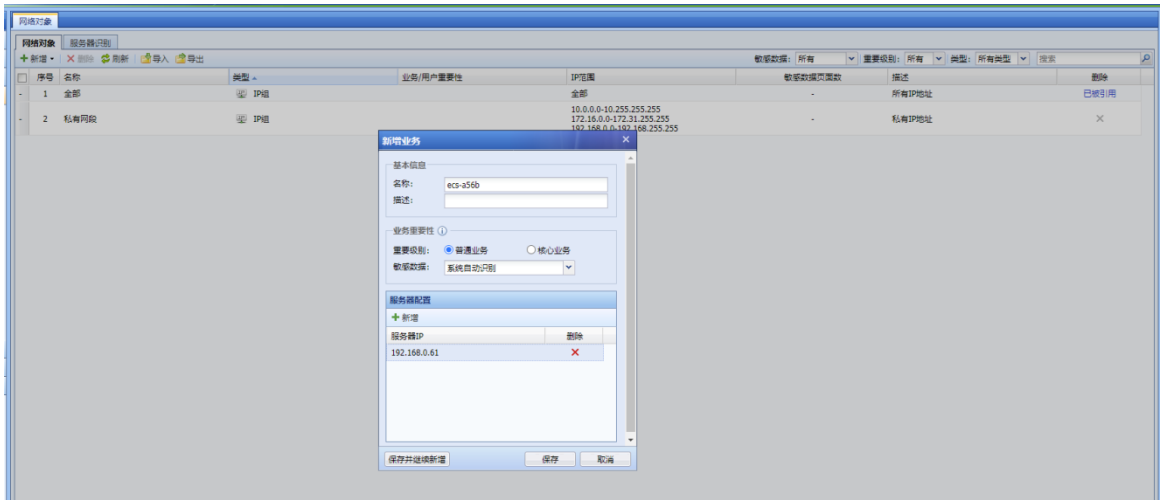
防火墙的网络设置完成，可尝试从其他云主机测试互通。

3.5.3. 访问策略配置

配置防火墙的访问策略，对外映射业务服务器端口，同时放通业务服务器访问互联网。

新建网络对象

根据互联网业务的需要，需为每个业务云主机创建网络对象，从【导航菜单】页面中，点击『对象』→『网络对象』→『新增』→『业务』，进行相关配置。



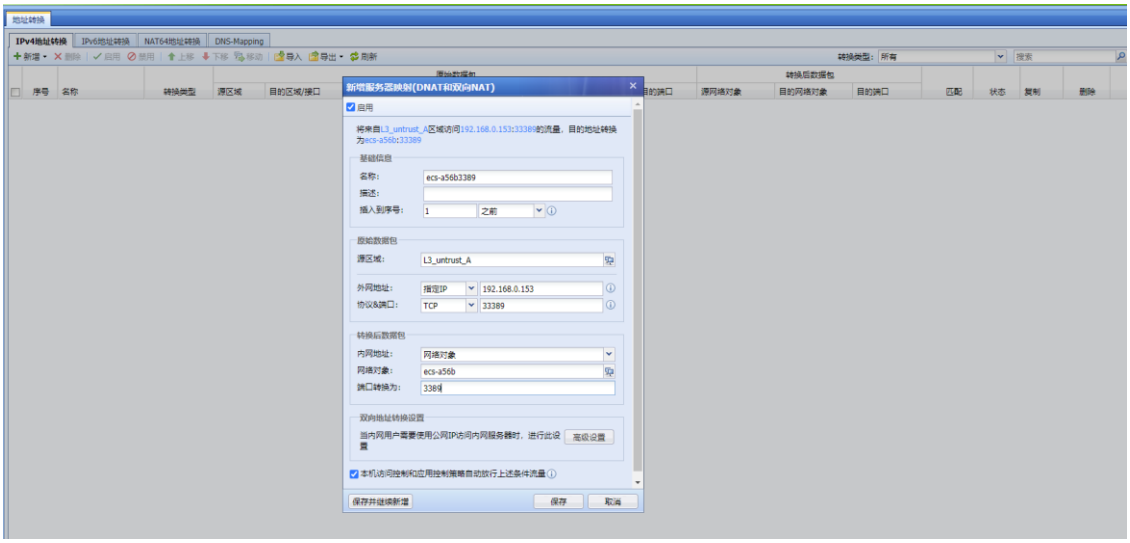
[名称]：按需命名

[服务器 IP]：业务云主机的 IP 地址

服务器映射

根据业务的需要，配置目的 IP 转换策略，允许外网用户通过防火墙访问业务云主机服务。

在『策略』→『地址转换』→『IPV4 地址转换』→『新增』→『服务器映射』：



『原始数据包』

[源区域]：选择“L3_untrust_A”

[外网地址]：eth0 地址（与绑定弹性公网 IP 对应的私有地址）

[协议&端口]：互联网访问的协议及端口

『转换后数据包』

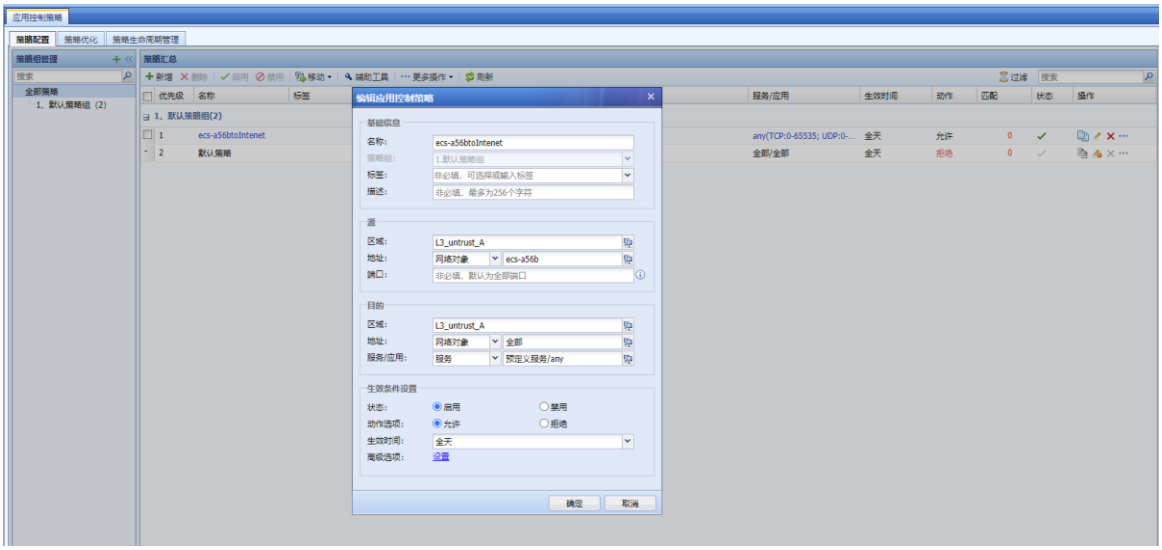
[内网地址]：选择网络对象

[网络对象]：业务云主机对象

[端口转换为]：业务云主机提供的服务端口

应用控制策略

云主机放通互联网访问，首先设置应用控制策略，在『策略』→『访问控制』→『应用控制策略』→『策略汇总』→『新增』:



『源』

[区域]：选择“L3_untrust_A”

[地址]：选择网络对象，勾选需要访问互联网的业务云主机对象

『目的』

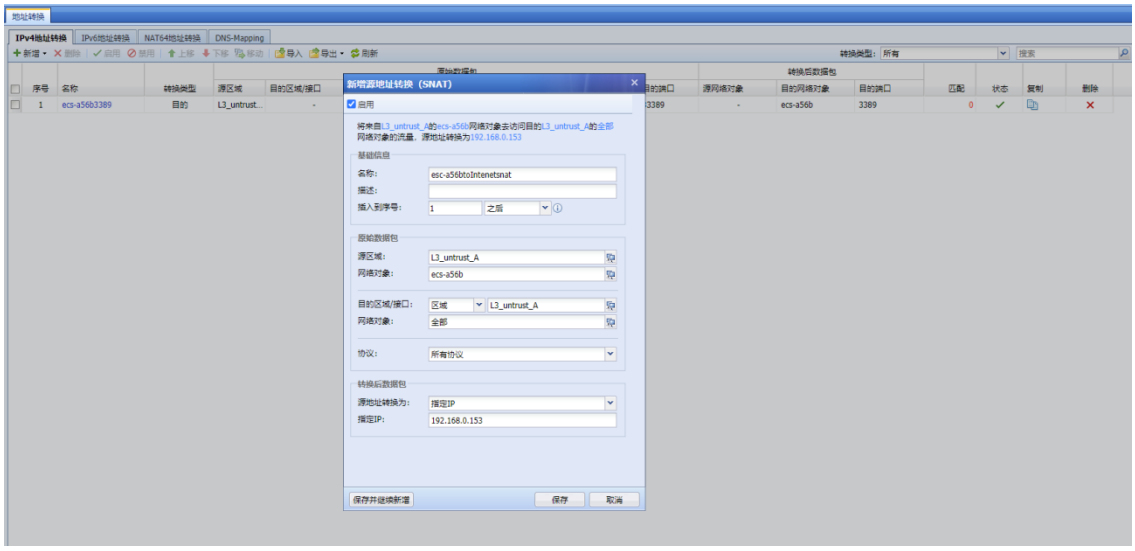
[区域]：选择“L3_untrust_A”

[地址]：勾选网络对象，选择全部

[服务/应用]：勾选服务，需访问的互联网服务端口可选择 any 全端口。

源地址转换

设置应用控制策略后，业务云主机访问互联网需要对防火墙分配弹性 IP 地址，点击『策略』→『地址转换』→『IPV4 地址转换』→『新增』→『源地址转换』，进行相关策略配置。



『原始数据包』

[源区域]：选择“L3_untrust_A”

[网络对象]：勾选区域，填写需要访问互联网的业务云主机对象

[目的区域/接口]：选择“L3_untrust_A”

[网络对象]：全部互联网对象

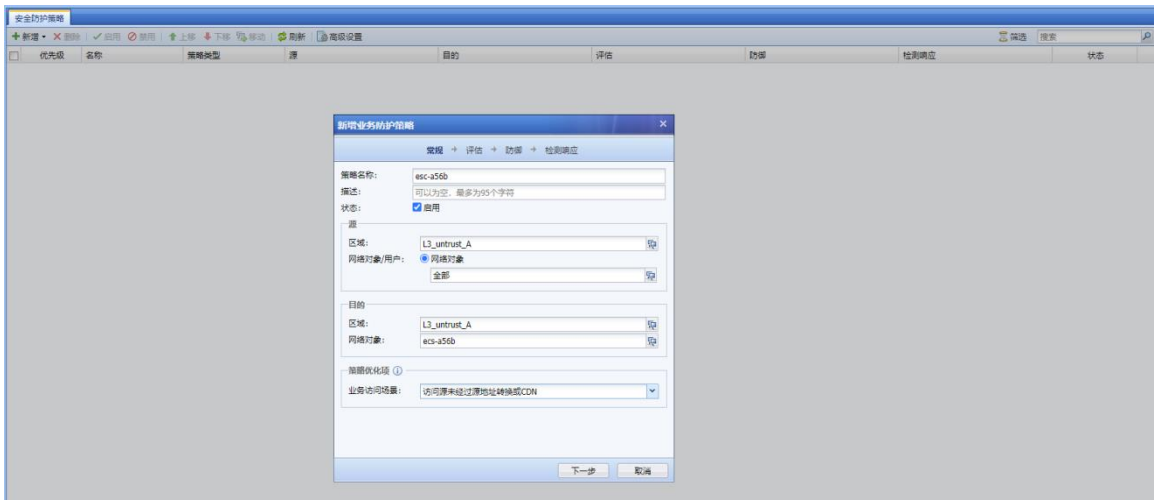
『转换后数据包』

[源地址转换为]：指定 IP

[IP 地址]：eth0 地址（与绑定弹性公网 IP 对应的私有地址）

3.5.4. 安全策略配置

开启云防火墙防护功能，在『策略』→『安全策略』→『安全防护策略』，新增业务防护策略。



『源』

[源区域]：选择“L3_untrust_A”

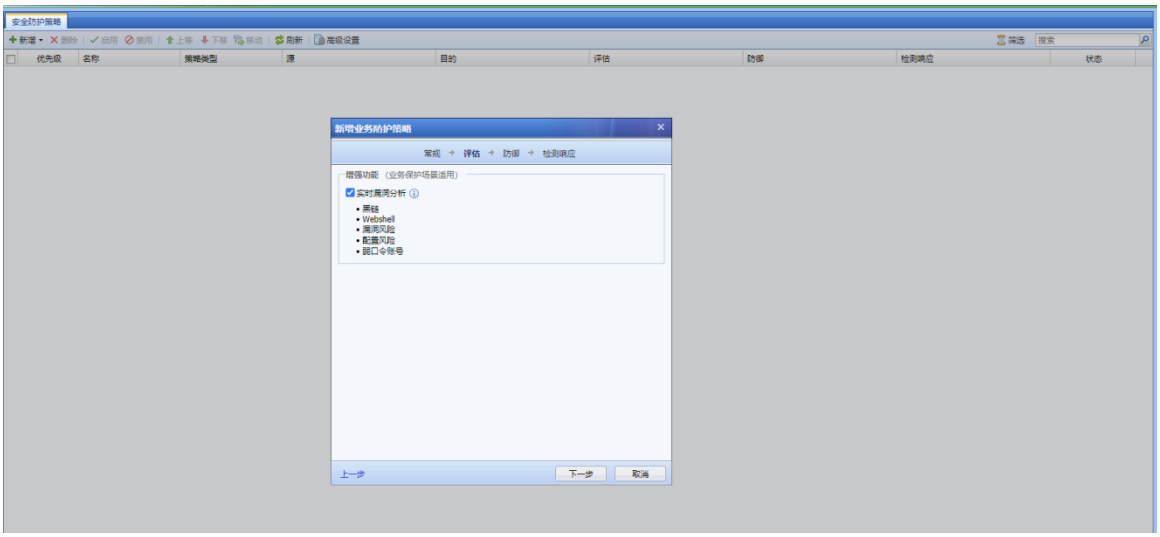
[网络对象]：勾选全部

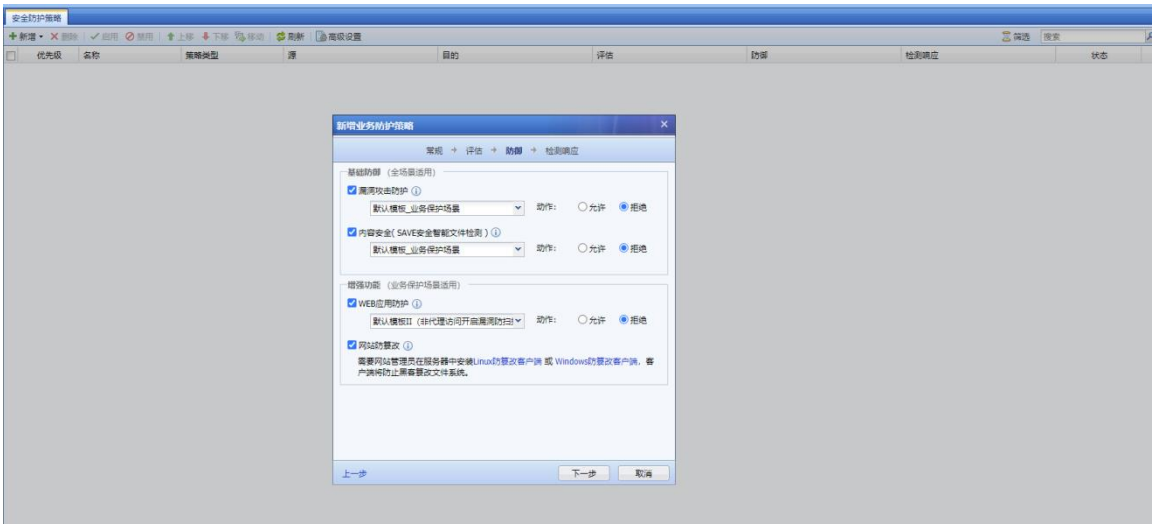
『目的』

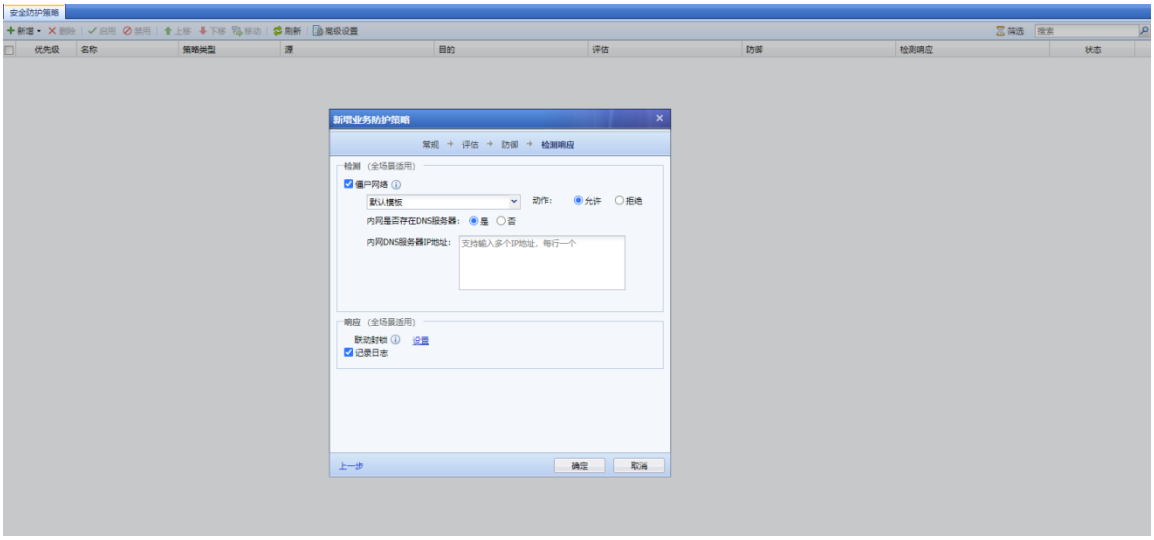
[目的区域/接口]：选择“L3_untrust_A”

[网络对象]：勾选业务云主机对象

按窗口提示点击【下一步】，过程参见以下截图。







安全防护策略请跟据实际业务进行设置调整，详细参考《天翼云安全专区云防火墙用户使用指南》。

3.5.5. 网络割接

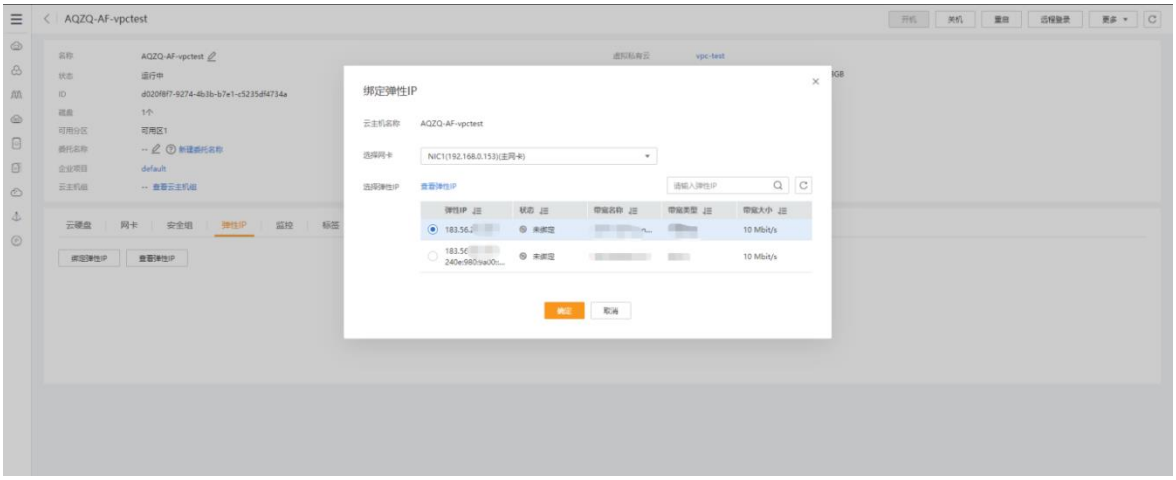
防火墙网络及策略配置完毕后，需要进行网络割接，把防火墙嵌入南北向流量，才能实现安全检测防御。割接工作主要包括弹性 IP 迁移，割接过程网络会中断。

云防火墙通过私有 IP 地址（或虚拟 IP 地址）与业务的弹性公网 IP 绑定，并通过服务器映射（参考 3. 5 .3 章节）接入业务网络链路。

弹性 IP 迁移

如果弹性 IP 已经绑定在业务主机，进入【天翼云控制中心】→『弹性云主机』，点击绑定弹性 IP 的业务云主机，进入『弹性 IP』→『绑定弹性 IP』，把弹性 IP 从业务云主机解绑。

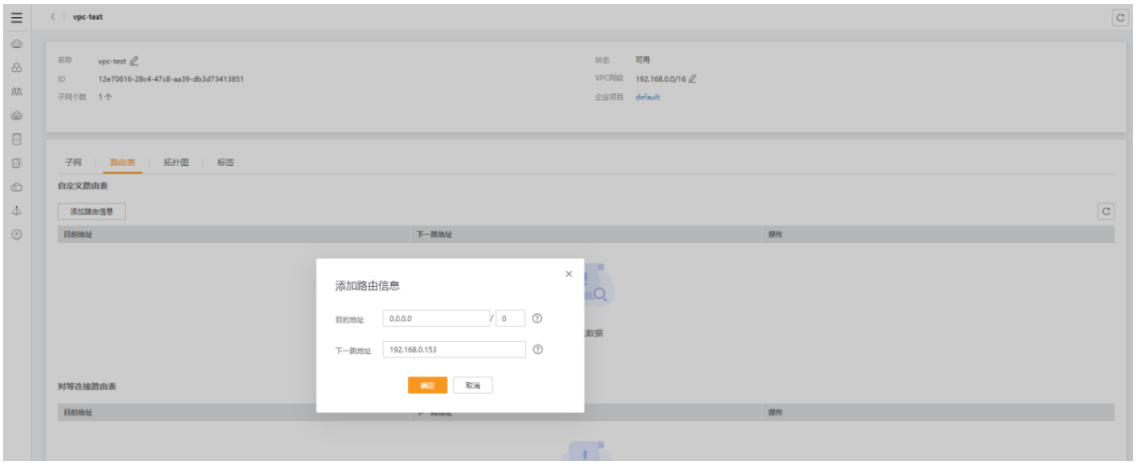
点击云防火墙云主机（AQZQ-AF-***），进入『弹性 IP』→『绑定弹性 IP』，将弹性 IP 重新绑定到防火墙云主机的 NIC1 主网卡上。



如有多个弹性 IP 地址，请通过云防火墙的虚拟 IP 地址绑定，点击（AQZQ-AF-***）的云主机，进入『网卡』→『管理虚拟 IP 地址』→『绑定弹性 IP』，

配置 VPC 路由

进入『控制中心』→『虚拟私有云』→『路由表』→『添加路由信息』。



[目的地址]：0.0.0.0/0

[下一跳地址]：填写云防火墙 eth0 的 IP 地址

3.5.6. 网络测试

从业务服务器 Ping 互联网 IP，测试是否可以 Ping 通，确认防火墙割接完成。

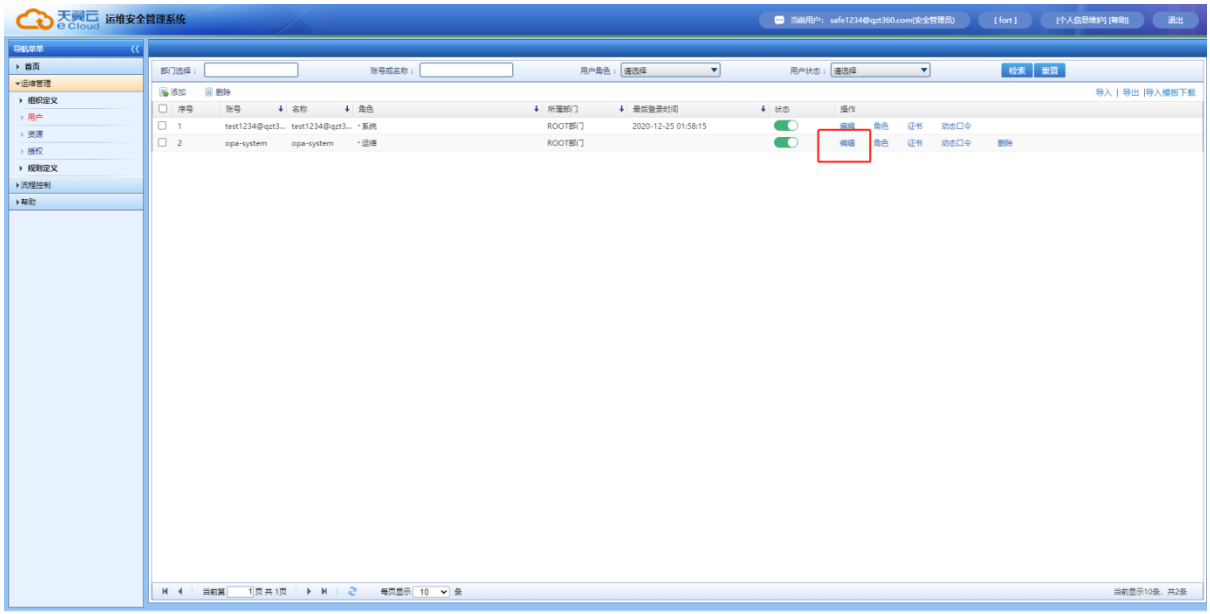
3.6. 云堡垒机

云堡垒机作为运维的集中管理系统，具有集中管理资产权限，全程记录操作数据，实时还原运维场景的功能。

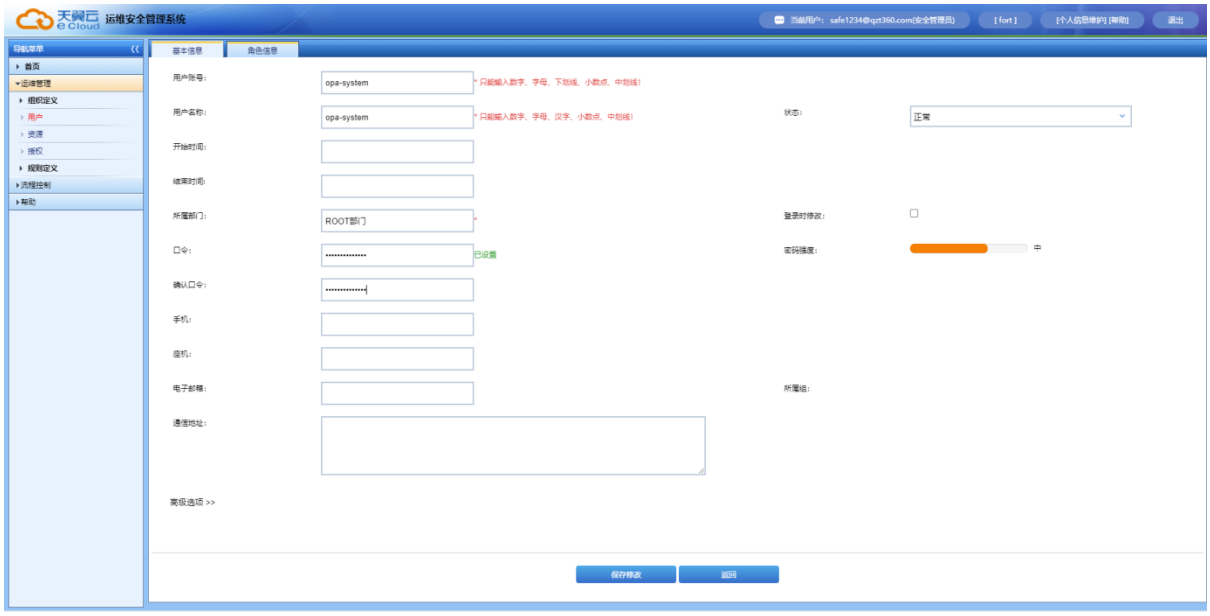
使用“安全管理员”角色用户登录安全管理中心，进入云堡垒机管理页面。

3.6.1. 运维账号

通过安全专区创建“运维人员”账号，运维账号会自动同步到云堡垒机，但需要进行密码修改。点击『运维管理』➔『用户』，进行密码编辑。



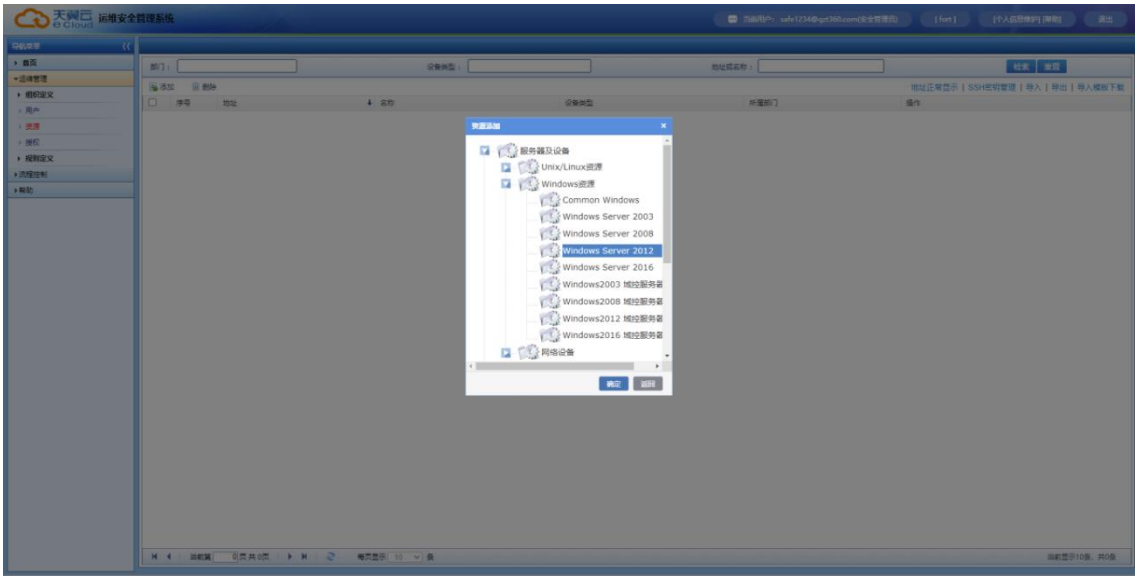
更改“运维人员”账户密码。

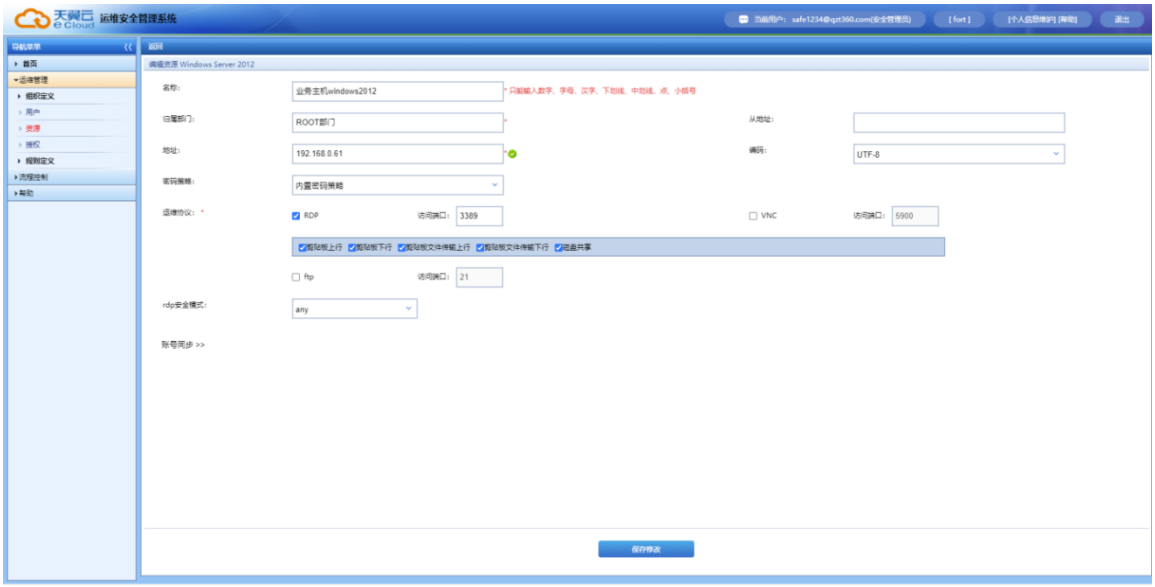


3.6.2. 添加资产

点击『运维管理』→『资源』→『添加』，可以添加不同类型的运维资源。

选择设备资源类别。





[名称]：自定义

[归属部门]：Root 部门

[地址]：业务云主机 IP 地址

[密码策略]：内置密码策略

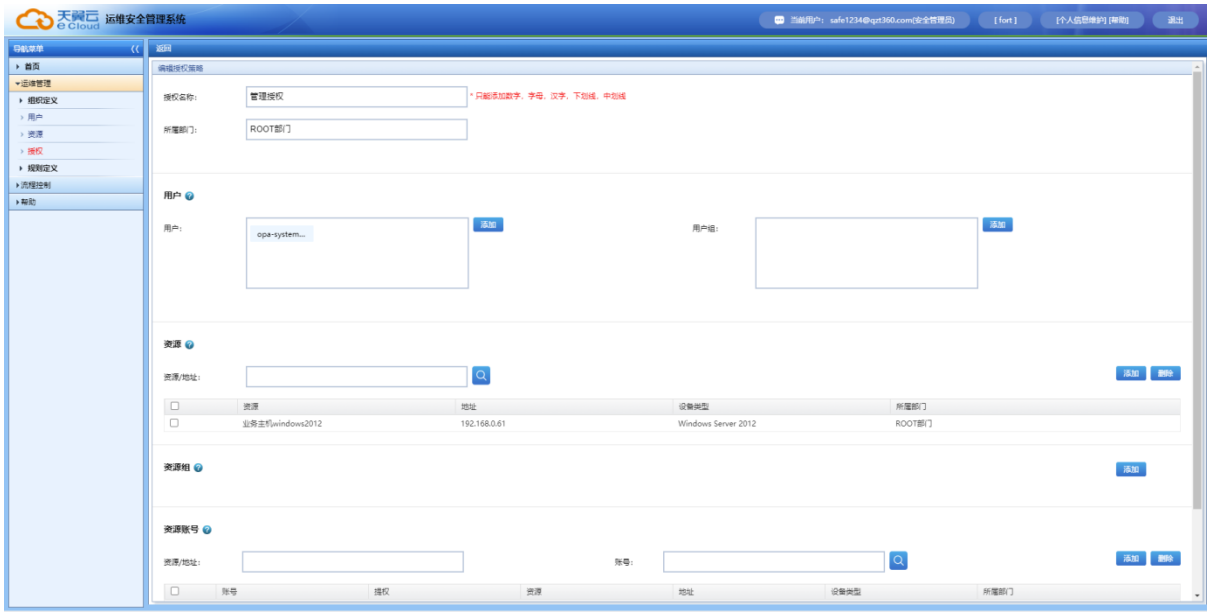
[运维协议]：按实际需求选择，可参考上图

请确保资源的网络及管理端口与云堡垒机网络互通，管理端口如 SSH 的 22 端口及 RDP 的 3389 端口可让云堡垒机访问。

3.6.3. 管理授权

添加授权，点击『运维管理』→『授权』→『新增』，对云堡垒机运维账号、运维资源以

及登录运维资源的系统账号进行授权绑定



【用户】

[用户]：运维人员账号

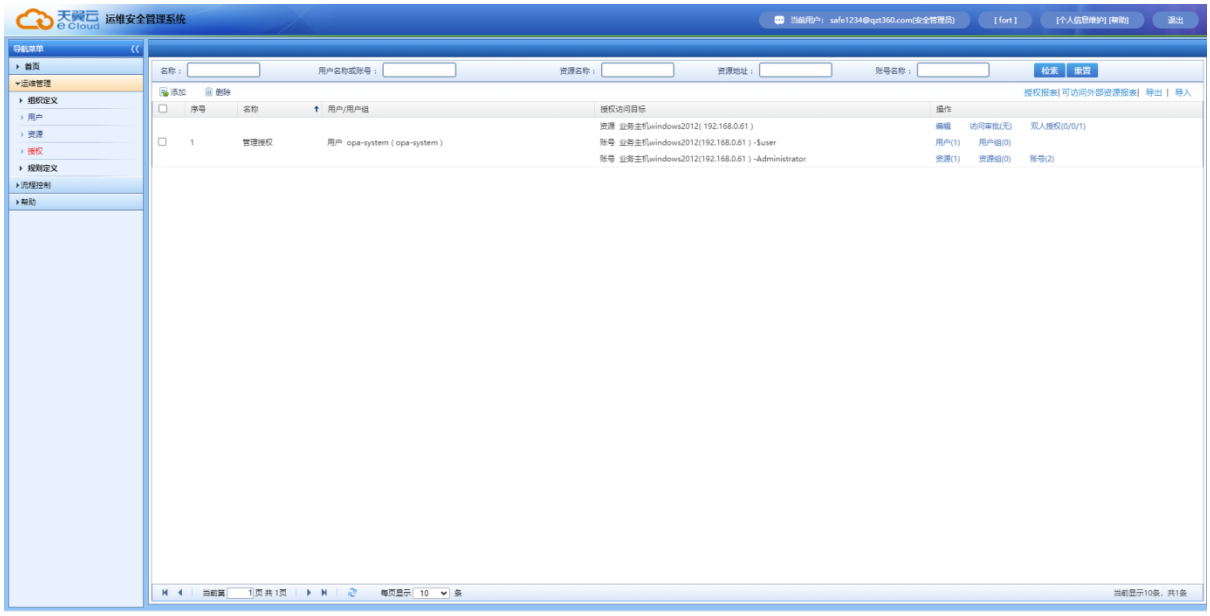
【资源】

[资源/地址]：提供给运维人员的运维资源

【资源账号】

[资源/地址]：运维资源的系统登录账号

授权添加成功后如下图所示：

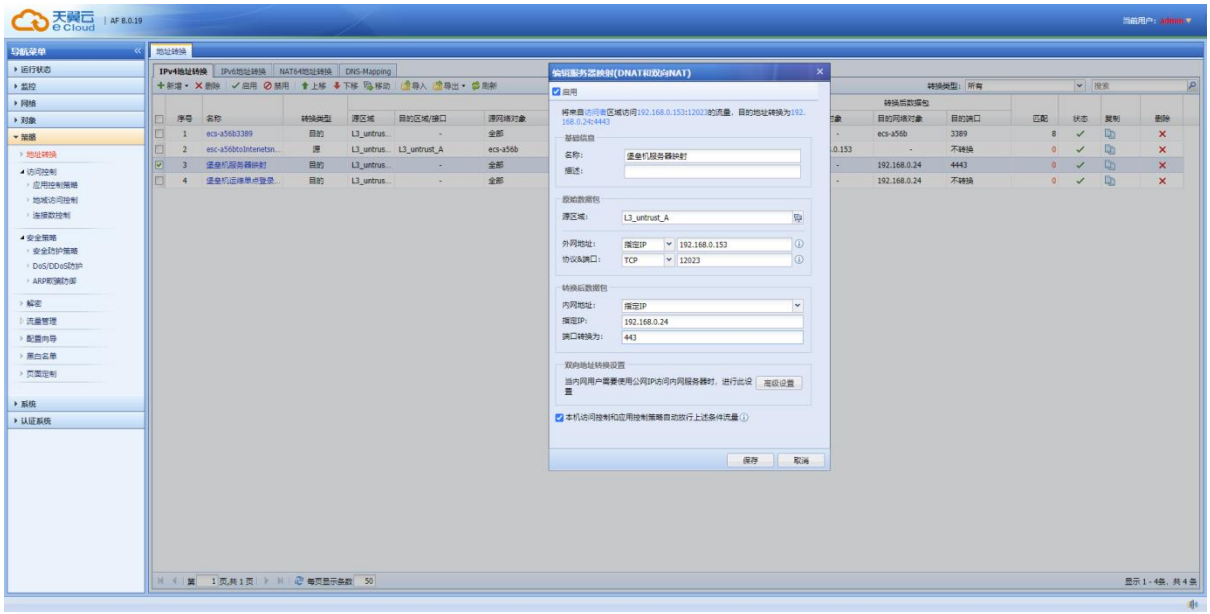


3.6.4. 映射端口

如需要从互联网访问云堡垒机，需在云防火墙设置服务器映射策略，操作请参考 3.5.3。策略配置如下：

使用“系统管理员”的账户登录安全专区，访问云防火墙组件管理。

进入『策略』→『地址转换』→『新增』→『服务器映射』，为云堡垒机添加端口服务映射，需要添加两个云堡垒机的映射策略，包括“堡垒机管理端口服务映射”和“堡垒机运维单点登录映射端口”：



添加“堡垒机管理端口服务映射”：

『原始数据包』

[源区域]：选择“L3_untrust_A”

[外网地址]：eth0 地址（与绑定弹性公网 IP 对应的私有地址）

[协议&端口]：互联网访问的协议及端口

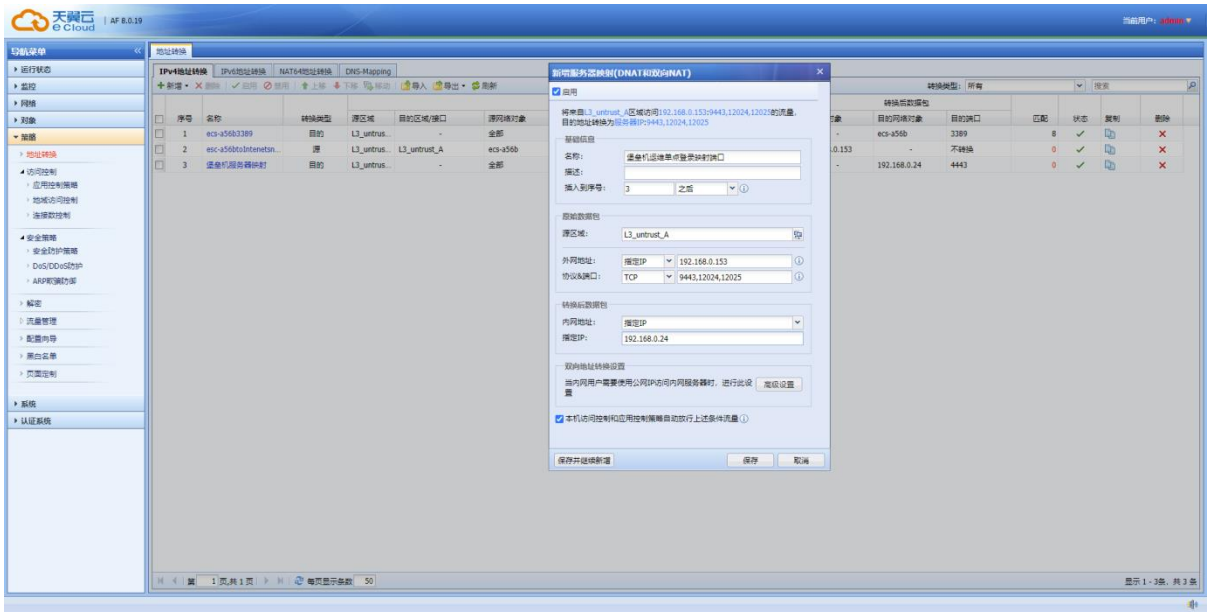
『转换后数据包』

[内网地址]：指定 IP

[指定 IP]：云堡垒机 IP 地址

[端口转换为]：443 端口

添加“堡垒机运维单点登录映射端口”：



『原始数据包』

[源区域]：选择“L3_untrust_A”

[外网地址]：eth0 地址（与绑定弹性公网 IP 对应的私有地址）

[协议&端口]：9443，12024，12025 端口

『转换后数据包』

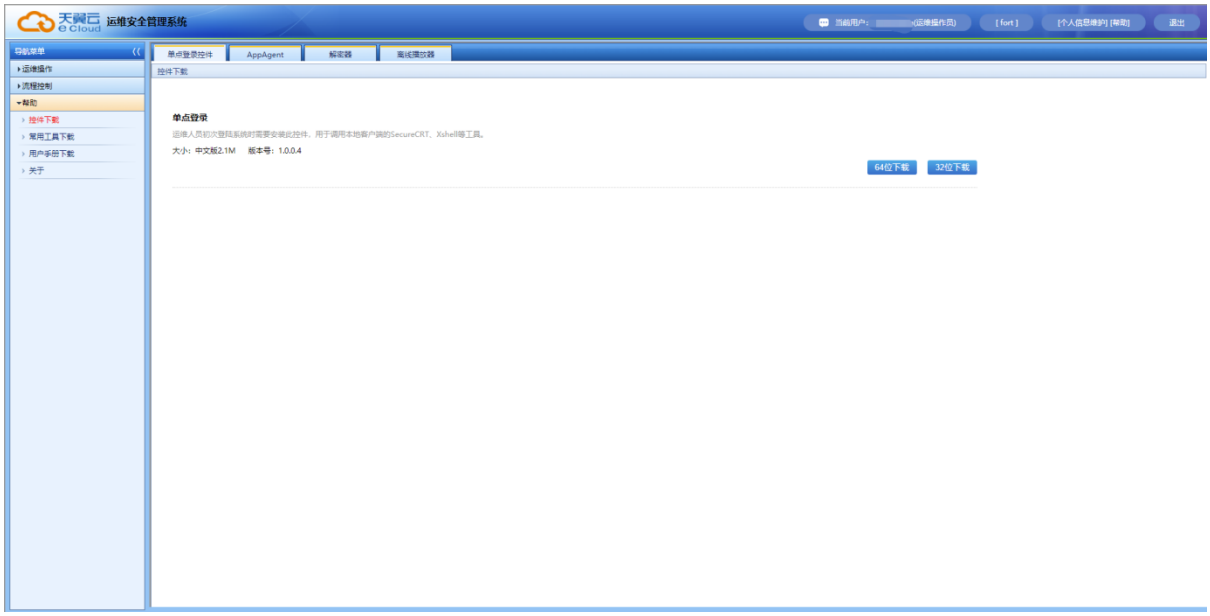
[网络对象]：指定 IP 地址

[指定 IP]：云堡垒机 IP 地址

3.6.5. 登录运维

安装插件

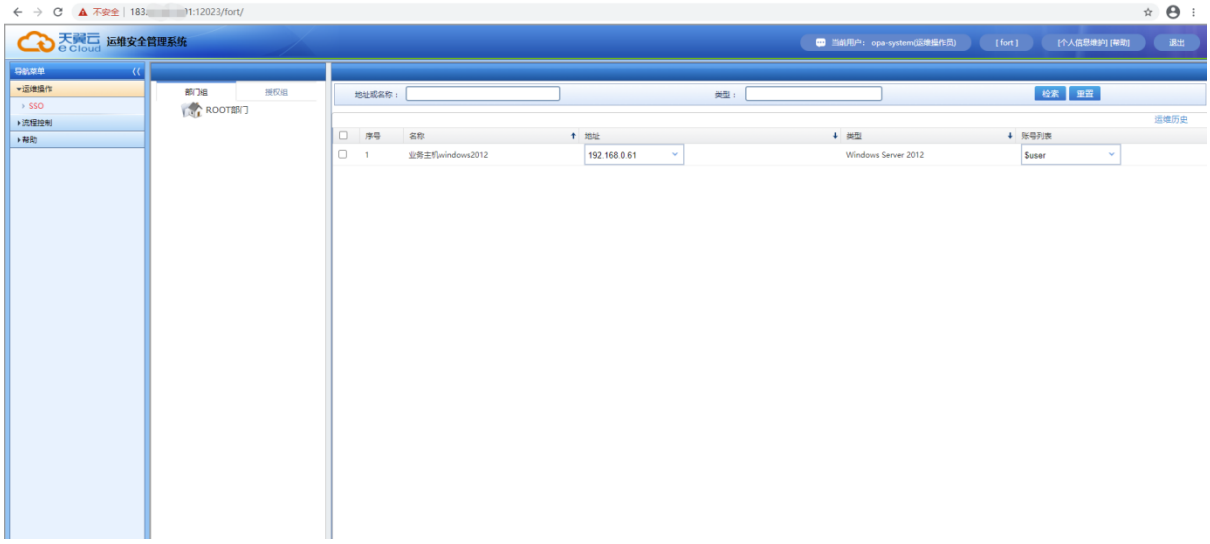
从互联网通过云堡垒机设置的“运维员”账号访问云堡垒机端口（https://云防火墙的弹性公网 IP：“堡垒机管理端口服务映射”中的对外映射端口，详情参考 3.6.4 章节），点击『帮助』→『控件下载』，选择合适的插件下载并进行安装。



根据提示完成安装插件。

测试登录

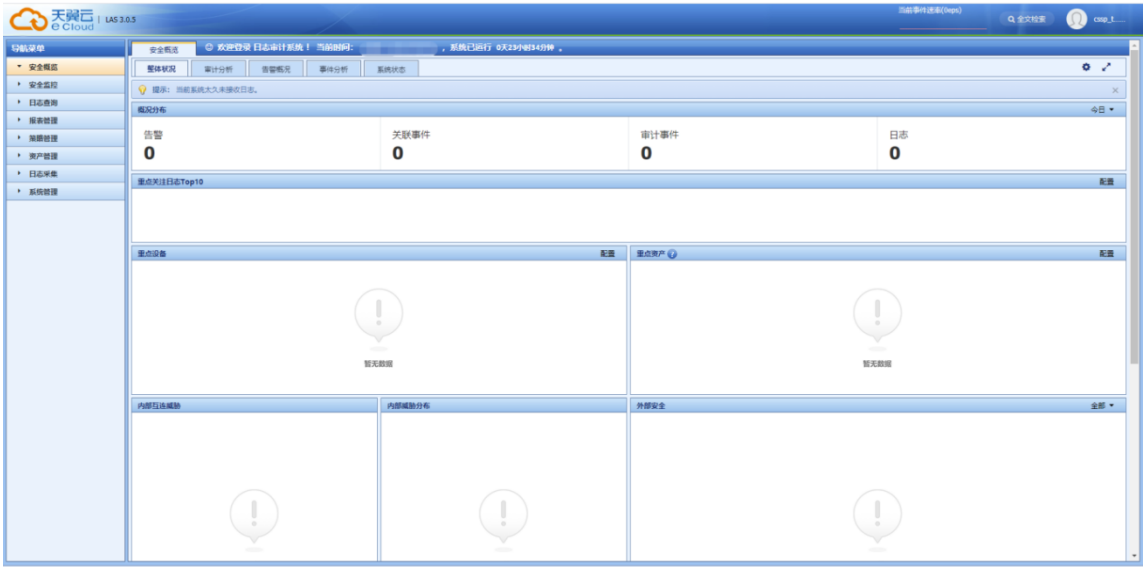
点击『运维操作』→『SSO』，可看到本账号在（详情参考 3.6.3 章节管理授权）授权需要运维的资源，即可选择相应的运维方式进入单点登录。



3.7. 云日志审计

云日志审计支持记录从不同设备或系统中所获得的各类日志、事件，支持高危事件检测并告警，提供可记录、可查询功能，可实现风险合规的目的。

进入云日志审计组件管理界面（登录方式请参考 3.3.3 章节），



3.7.1. 添加资产

新增资产，点击『资产管理』→『资**产管理**』→『新增』，如下图为 Windows 模板进行配置：

[注意]：红*为必填项

[资产名称]：根据实际网络、设备自定义取名

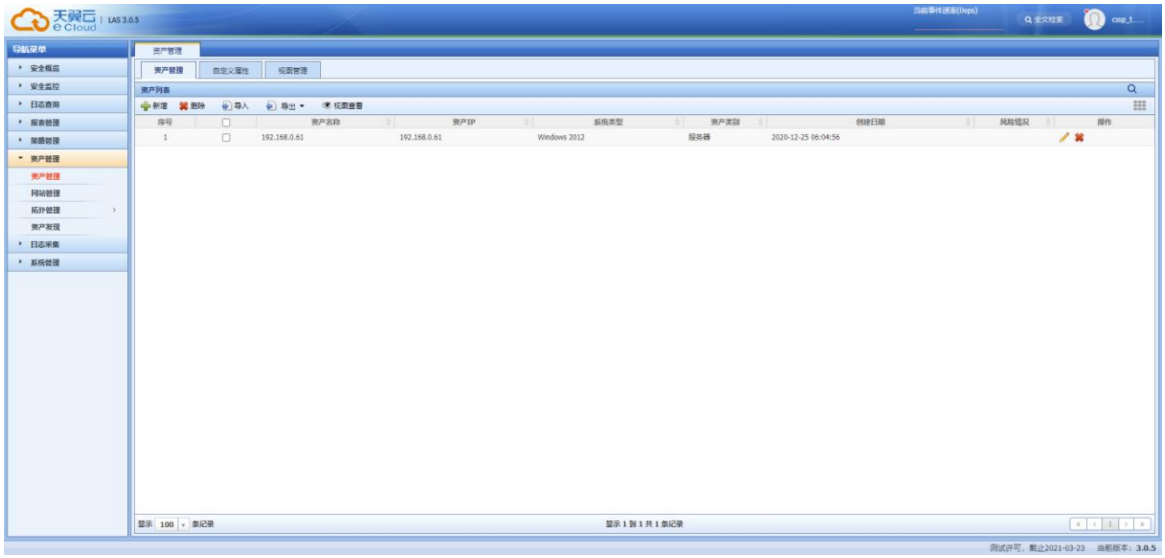
[系统类型]：按业务服务器选择

[IP 地址段]：填写业务服务器的私有 IP 地址

[资产类别]：此处选择服务器

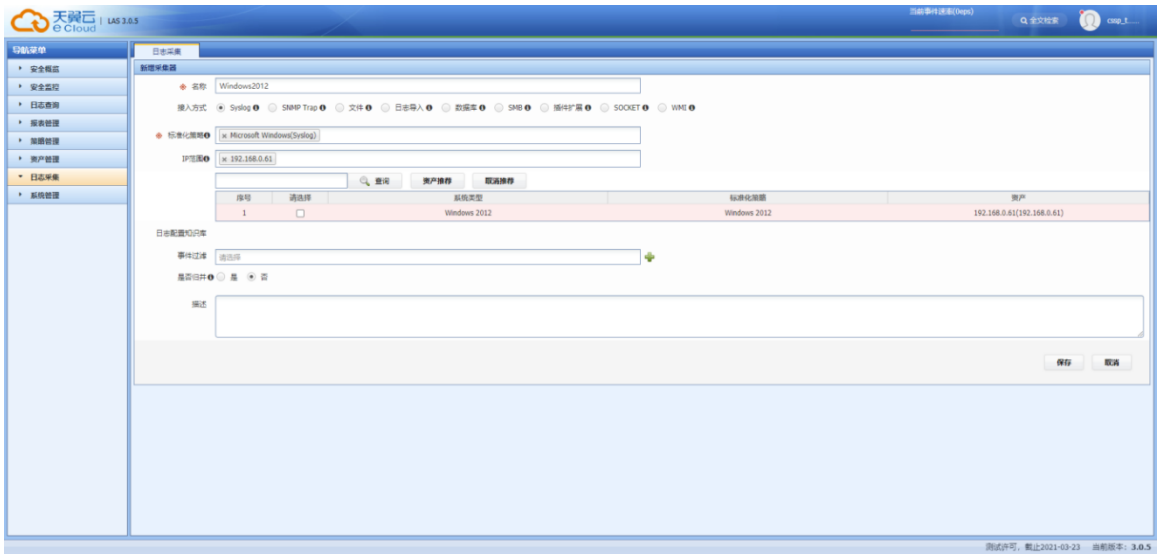
[资产 IP]：此处填写需要增加资产的实际 IP

通过"查询"按钮可以快速的查询当前已添加的资产



3.7.2. 采集器配置

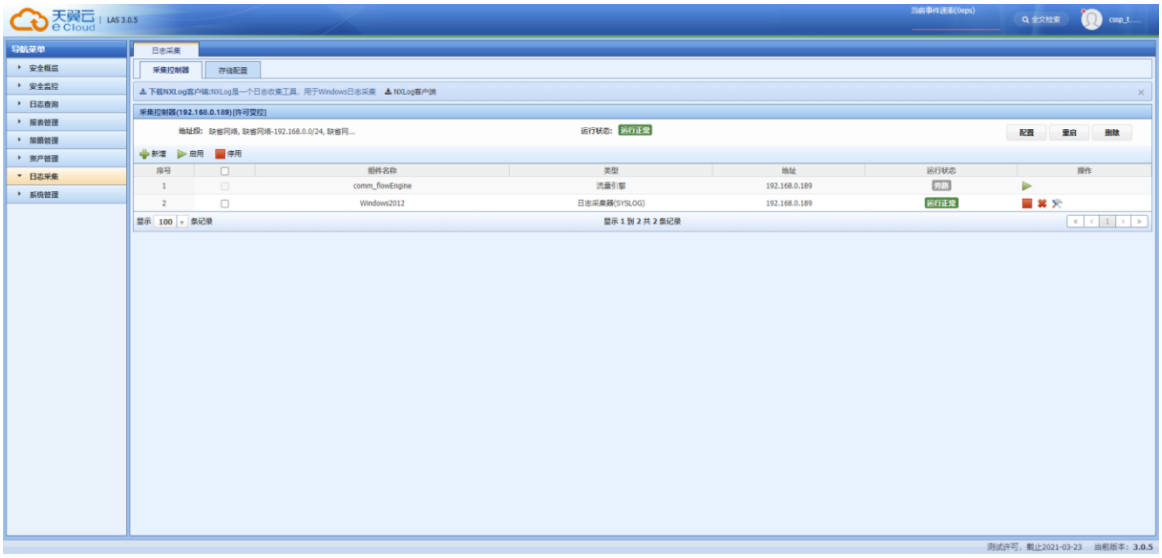
新增采集器：点击『日志采集』→『采集控制器』→『新增』，如下图所展示。



[类型]：选择"事件采集器"；

[标准化策略]：选择系统内置对应的模版，系统将自动关联；

[IP 范围]：填写准确 IP 地址以便系统能够识别。



3.7.3. 客户端安装

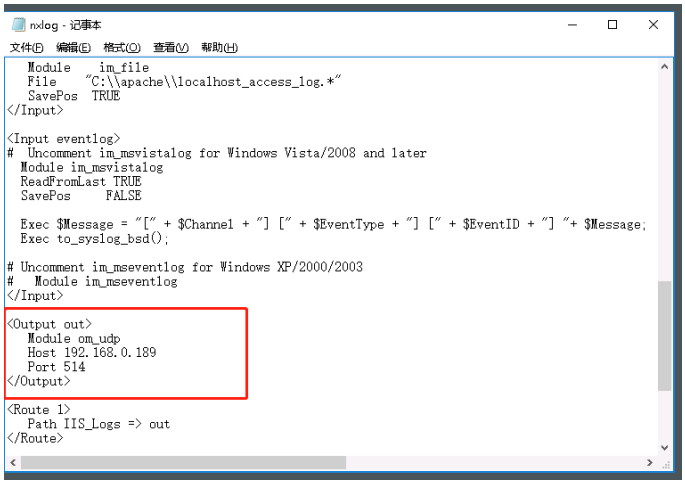
Windows 系统客户端配置

进入『日志采集』→『采集控制器』，点击“NXLog”客户端，进行下载。

压缩包内包括客户端配置程序、配置文件、操作方法。

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
nxlog.conf	1,206	472	CONF 文件	2019/7/1 20:50	A445DA...
nxlog-ce-2.9.1716.msi	3,977,216	3,202,217	Windows Installe...	2019/7/1 16:42	7D1E0E...
nxlog-ce-2.9.1716-1_rhel6.x86_64.rpm	1,558,136	1,548,402	RPM 文件	2019/7/1 20:26	E9CEA5...
nxlog-win2003.conf	2,674	1,100	CONF 文件	2019/7/1 20:50	8D2738...
nxlog-win2008.conf	2,144	877	CONF 文件	2019/7/1 20:49	3EC7546B
NXLog安装与配置说明.docx	5,144,071	5,103,263	Microsoft Word ...	2020/9/3 17:12	EE06F603

相关配置文件需注意，“Host”为云日志审计 IP 地址。



配置文件修改后，重启服务。

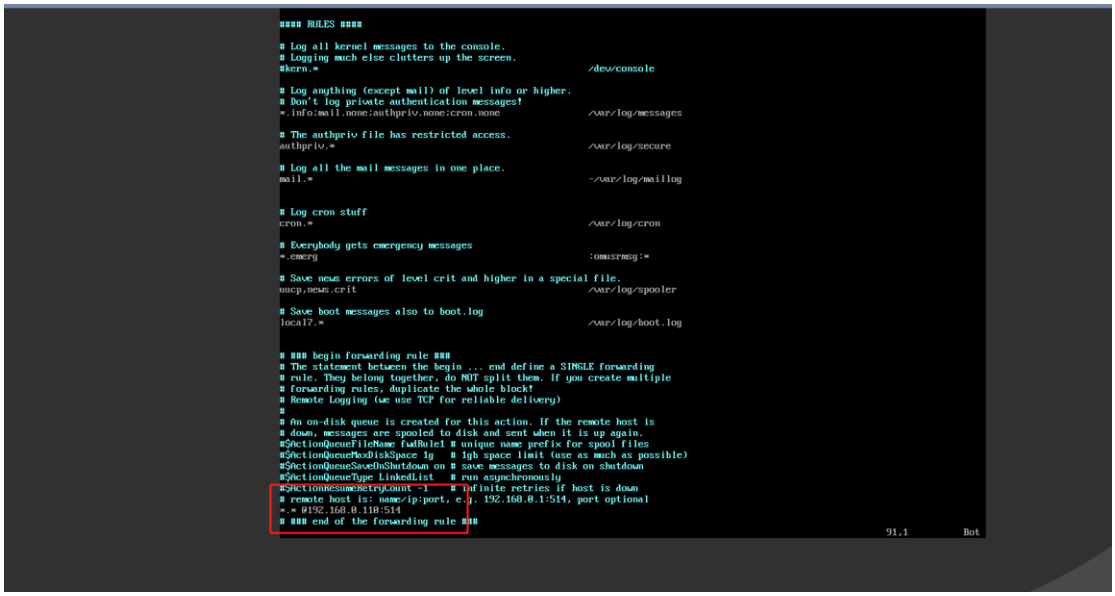
Linux 客户端配置

进入 Linux 系统，进行 rsyslog 进程配置

命令：# vim /etc/rsyslog.conf

修改配置如下：

. @云日志审计 IP 地址（写入发送日志指向的云日志审计地址）



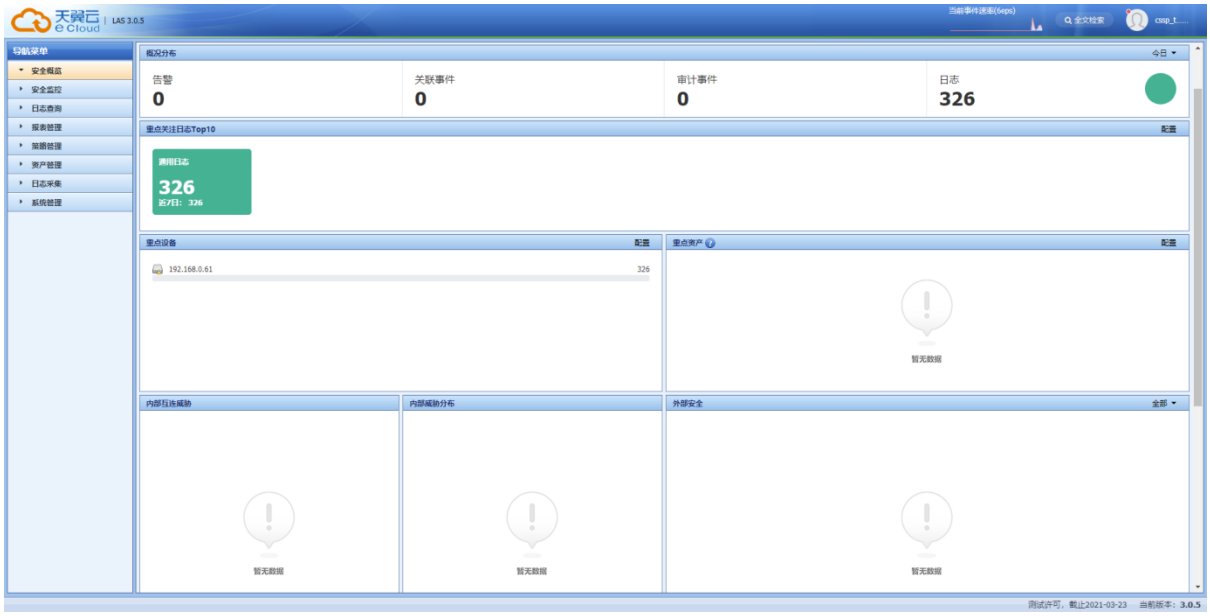
启动 rsyslog 服务

systemctl start/restart rsyslog.service

其他类型资产日志配置

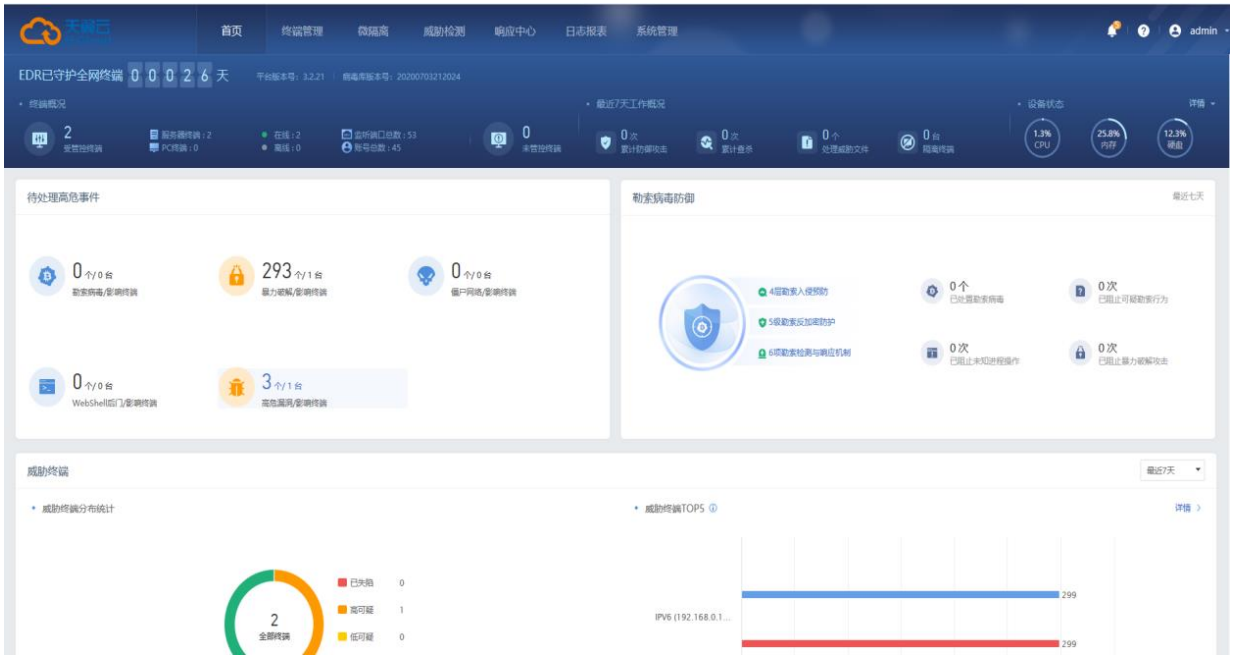
其他类型资产可选择内置 syslog 方式，填写云日志审计组件 IP 地址。

若配置完成，可到【安全概览】下查看资产设备的日志分析。



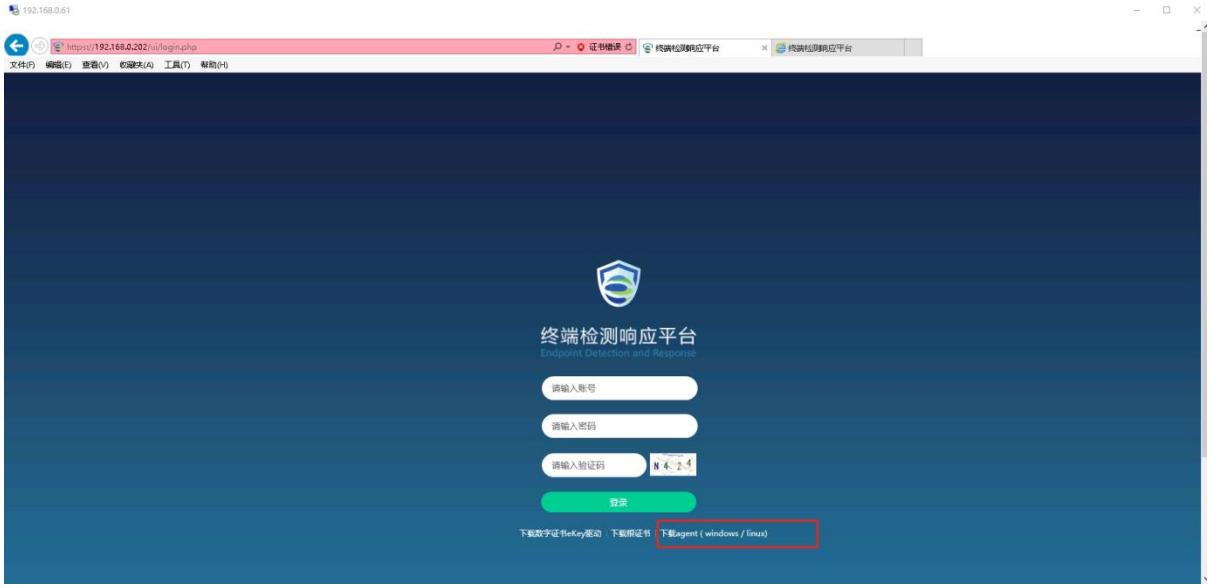
3.8. 终端安全 EDR

进入终端安全 web 管理界面（登录方式请参考 3.3.3 章节）



3.8.1. 客户端安装

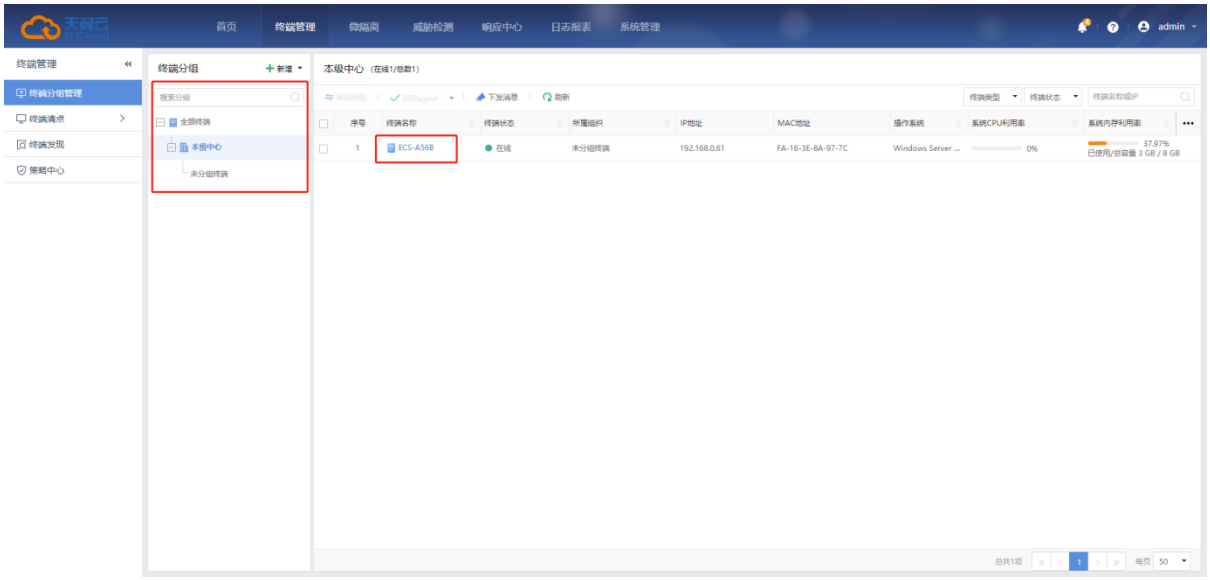
通过远程登录进入业务云主机，使用终端安全 EDR 内网地址，该界面登录如下图，点击客户端下载安装。



根据安装提示，完成客户端安装。

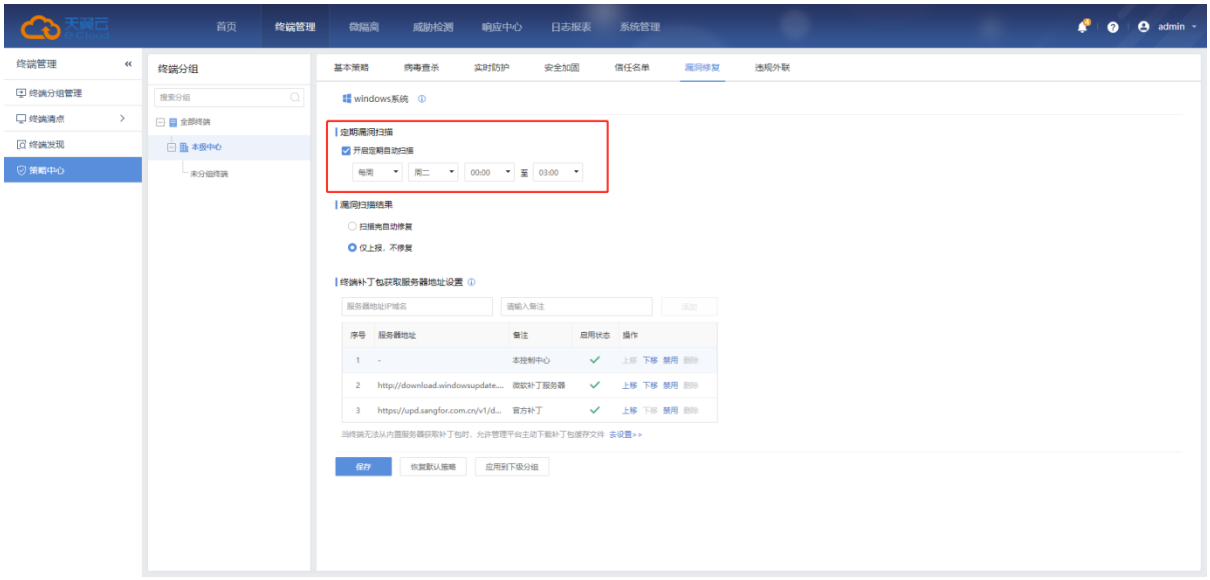
3.8.2. 策略配置

在『终端管理』→『终端分组管理』，进入配置



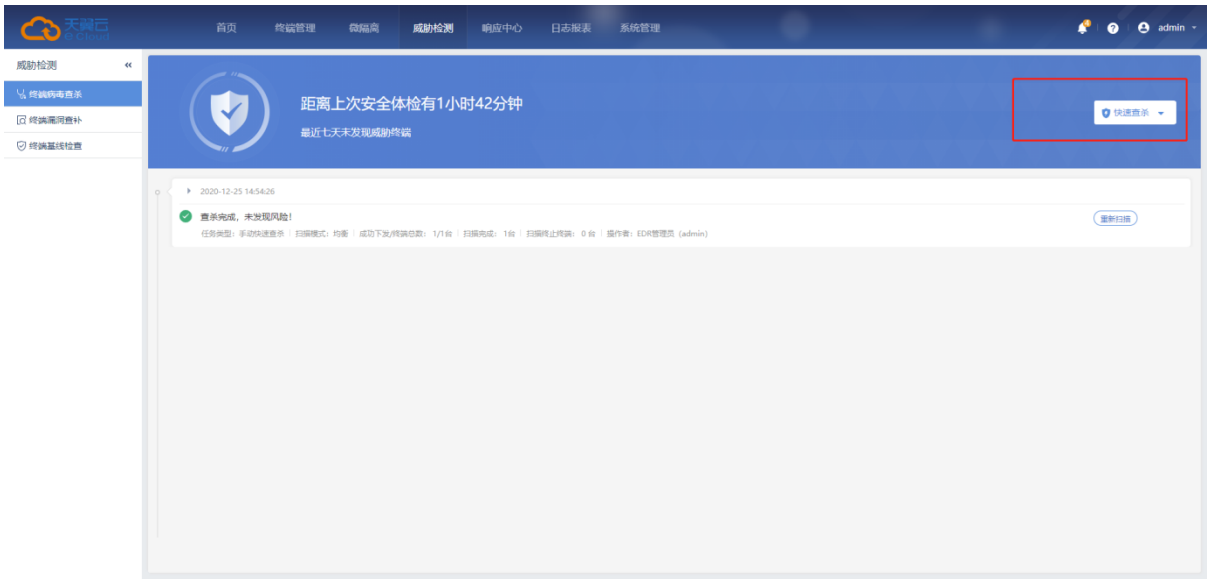
进行策略配置，在『终端管理』→『策略中心』→『病毒查杀』，勾选“开启定期自动扫描”，点击保存。

在『终端管理』→『策略中心』→『病毒查杀』，勾选“定期漏洞扫描”，点击保存。

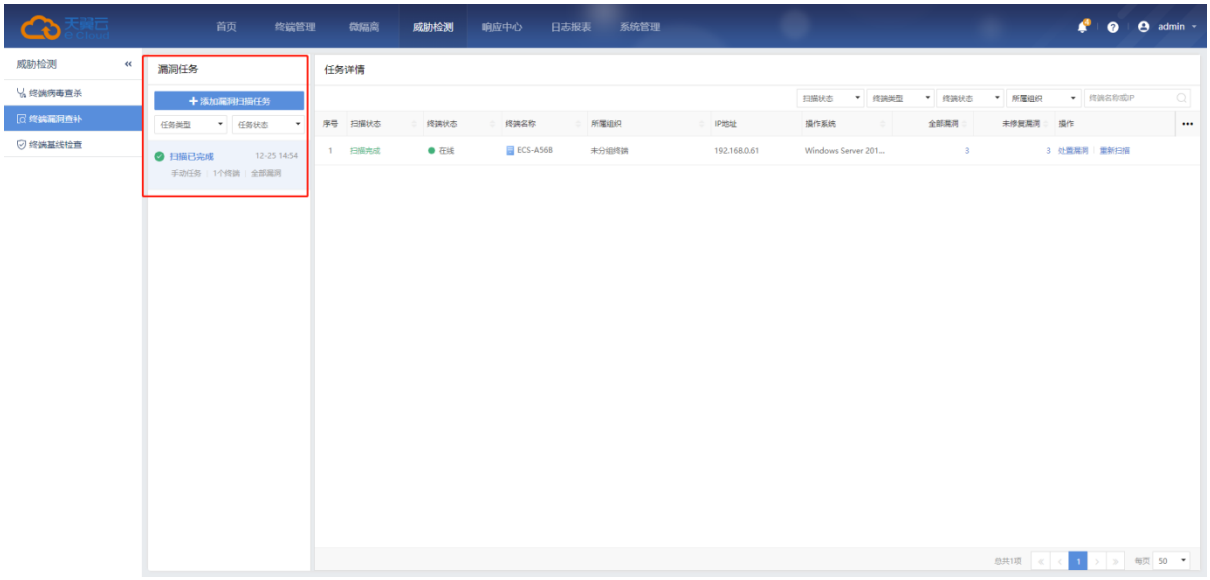


威胁检测配置

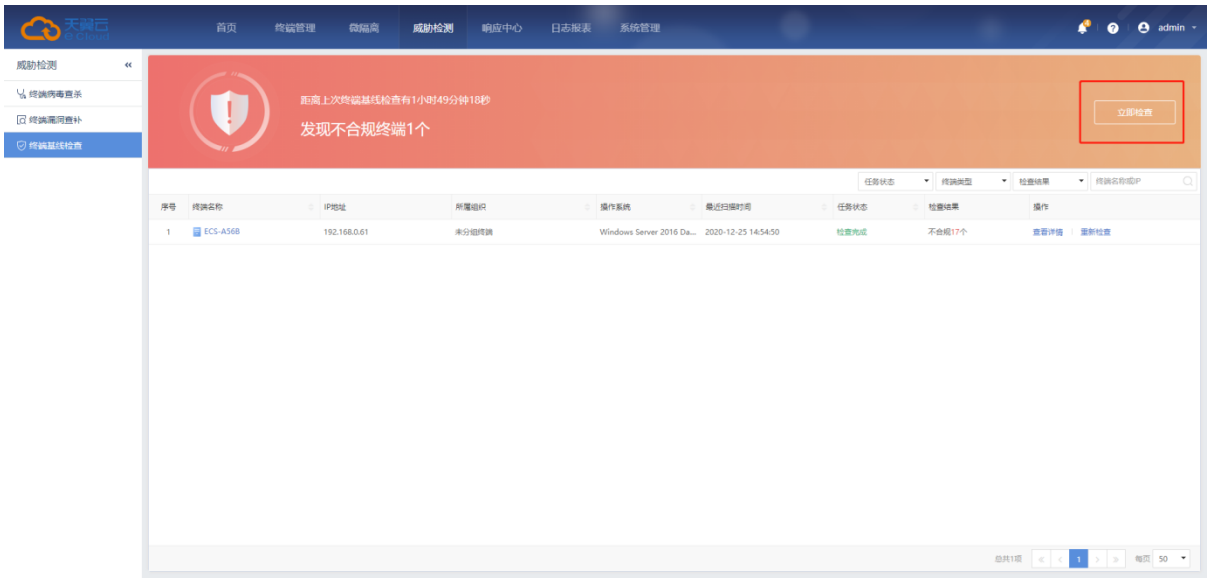
部署安装客户端后，在『威胁检测』→『终端病毒查杀』下，点击“快速查杀”，开启任务完成病毒查杀。



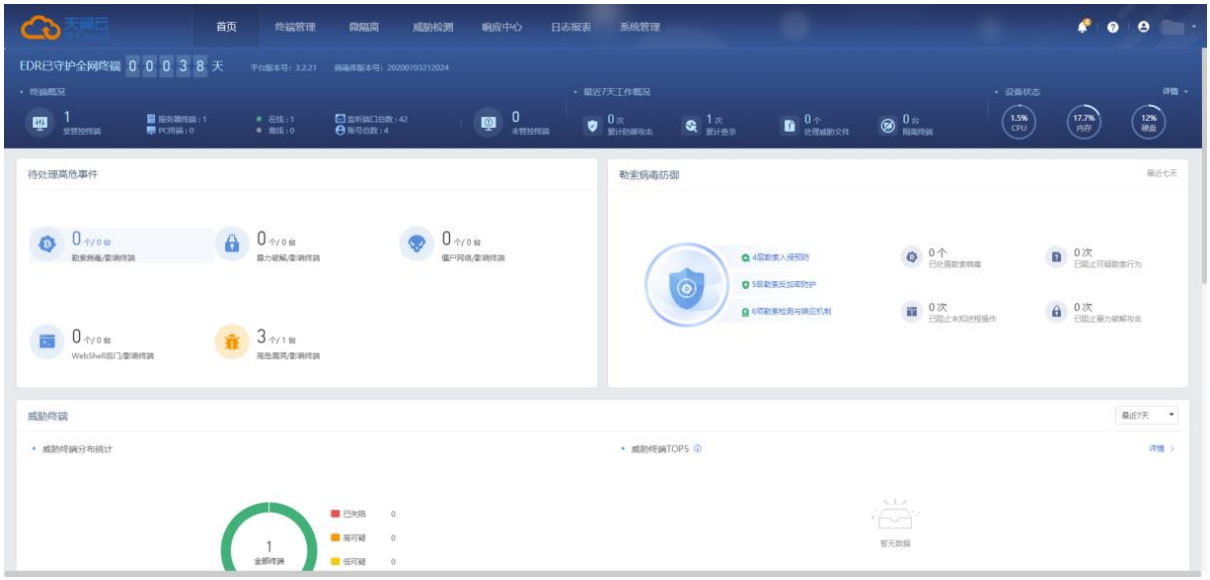
开启扫描任务，在『威胁检测』→『终端病毒查补』，进行终端漏洞查补，完成漏洞扫描。



开启终端基线检查，在『威胁检测』→『终端基线检查』，点击“立即检查”，完成基线检查。



以上完成客户端安装及策略配置，检查完成后安全信息将在安全专区展示



3.9. 云数据库审计

云数据库审计系统作为审计产品，可通过设计其相关业务策略，实现审计符合业务策略的网络行为、跟踪访问重要数据源的网络行为。

3.9.1. 部署方式

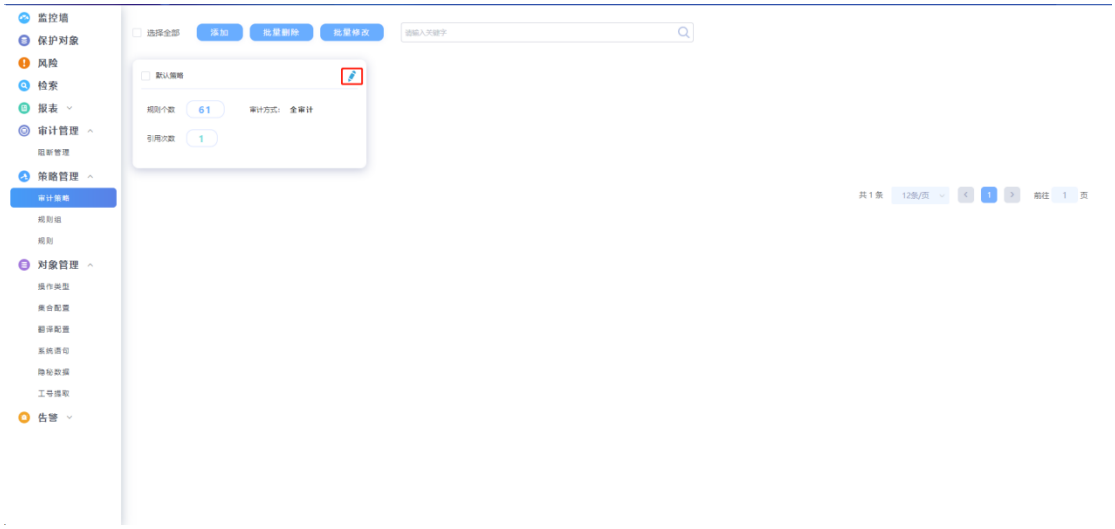
登录云数据库审计系统平台-部署方式（登录方式请参考 3.3.3 章节）

设置 Agent 引流操作，点击【部署方式】，勾选部署方式的“Agent 引流”并保存

3.9.2. 添加审计策略

使用安全管理员用户登录安全管理中心，点击进入云数据库审计。

设置审计策略：点击【策略管理】→『审计策略』→『默认策略』，进行编辑

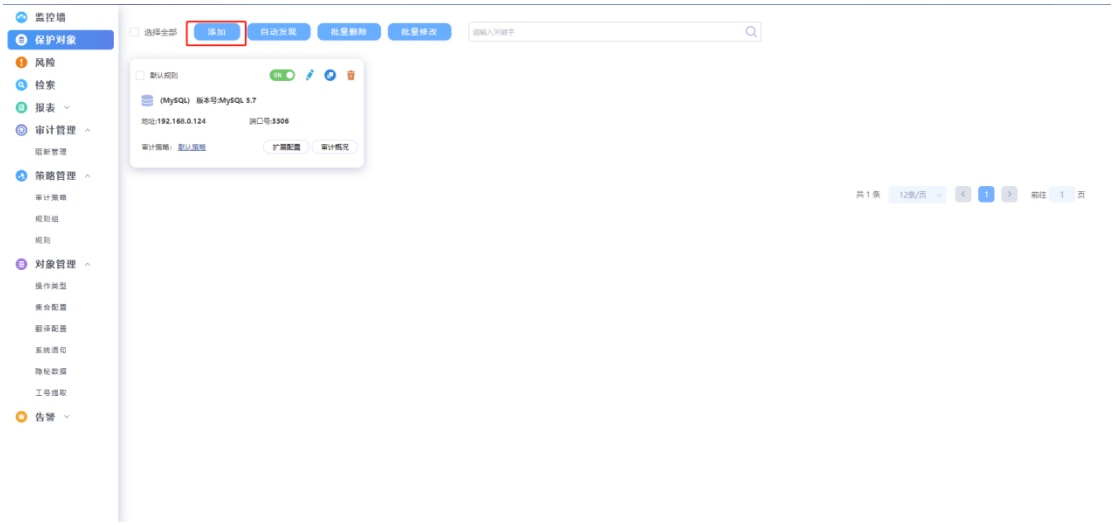


将“未选中的规则”进行全选，左移到“选中的规则”，点击保存即可

3.9.3. 添加保护对象

数据库中的保护对象是指受审计的数据库

点击【保护对象】→『添加』，进行添加保护对象设置



填写受保护对象相关信息

[对象名]：自定义

[状态]：默认开启

[告警]：默认关闭（按需开启）

[数据库类型]：MySQL（选择对应的数据库版本）

[版本号]：MySQL5.7（选择安装的对应版本号）

[Ip 地址]：192.168.0.124（可输入 IP 段形式，用 ‘-’ 隔开）

[端口号]：3306（可输入多端口，用 ‘|’ 隔开）

[数据字符集]：GB2312（选择适当的编码）

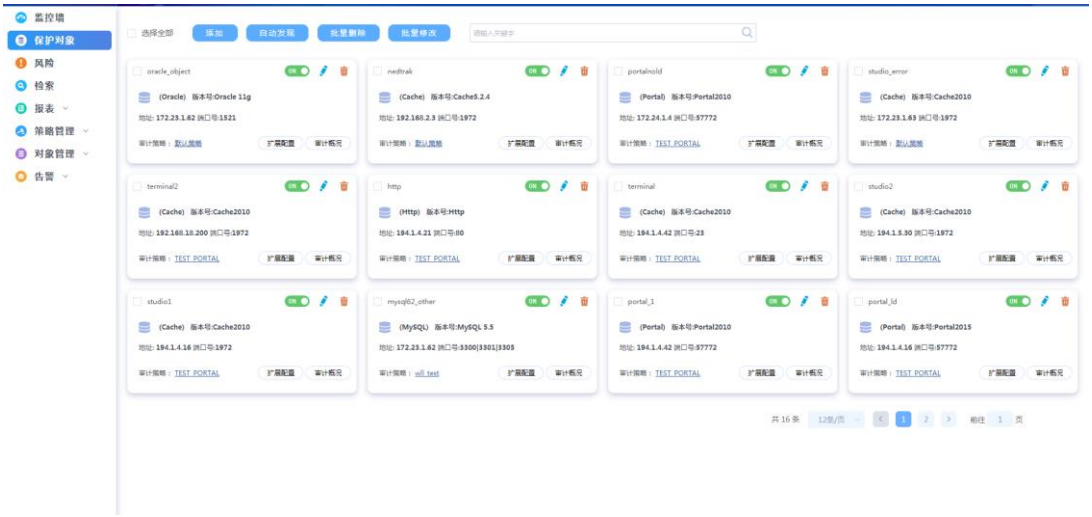
[His 产商]：空（按需配置）

[审计策略]：默认策略（按需配置）

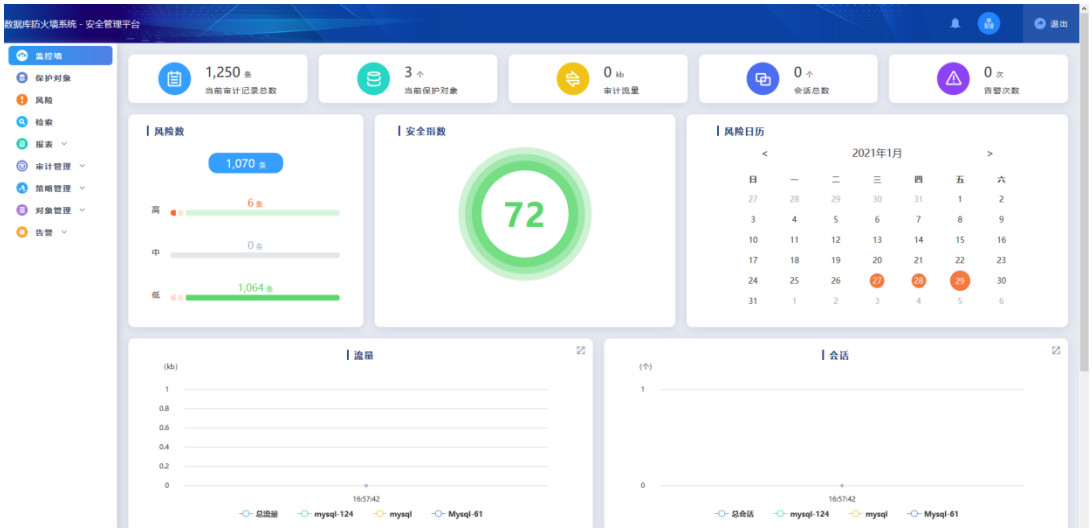
[告警策略]：空（按需配置）

注意：根据自己数据库安装时的配置选择编码，编码选择错误可能会导致乱码问

保存成功后，可对原有配置进行单个编辑，配置扩展配置以及批量修改（状态、策略）。



完成以上客户端安装及策略配置，数据库的访问操作将会发送到云数据库审计上并展示。



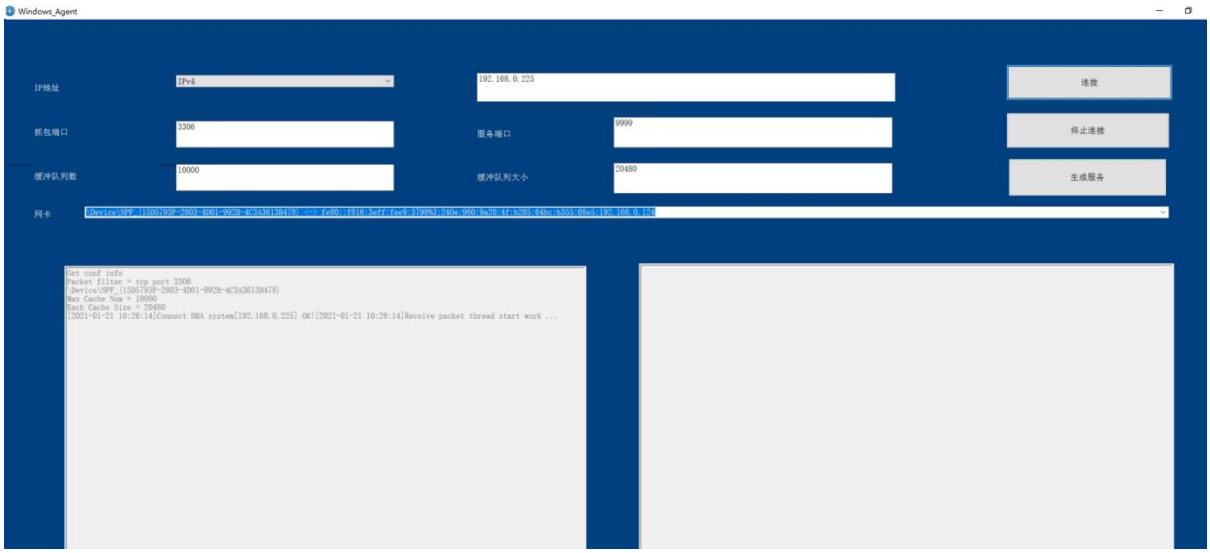
3.9.4. 客户端安装

下载客户端，选择对应的客户端进行下载

下载安装包，根据包中的 Agent 安装手册提示完成安装及连接配置。

名称	修改日期	类型	大小
Window Agent-setup.exe	2020/8/24 15:39	应用程序	3,714 KB
Windows agent _manual.dec.docx	2020/8/24 15:31	Microsoft Word ...	1,135 KB

填写信息，进行客户端与云数据库审计的连接。



在 Windows 上安装 Agent 客户端，默认安装即可；

执行 Agent，选择接收、发送数据包的网卡，并填写相应的信息。

[IP 地址]：云数据库审计管理口地址 192.168.0.225

[抓包端口]：本地数据库端口，如默认 ORACLE 端口 1521，MSSQL 默认 1433，MYSQL 默认 3306，如需添加多个端口，请使用逗号进行分隔。

[服务端口]：默认云数据库审计设备服务端口，默认 9999，请使用默认配置。

缓冲队列个数，缓冲队列大小，使用默认配置即可。

[收发网卡]：请根据实际情况进行选择，程序支持自动发现功能。

注意：Agent 必须要保证始终运行，才能将本地数据库连接信息发送给审计设备，一旦关闭，将不会向审计系统发送本地审计数据。因此请将 Agent 设置为服务.

运行后，如出现如下内容，表示工作，并正常发送数据包

```
Get conf info
Packet filter = tcp port 1433
\Device\NPF_{8B0F5205-513F-4B9D-8F4A-6472E87B7EE0}
\Device\NPF_{8B0F5205-513F-4B9D-8F4A-6472E87B7EE0}
Max Cache Num = 10000
Each Cache Size = 20480
[2019-02-20 11:24:54]Connect AAS[192.168.213.251] OK!
[2019-02-20 11:24:54]Receive packet thread start work ...
```

连接成功后，可到【部署方式】，查看已连接到的客户端

完成以上操作部署后，可在安全专区平台进行日常运营。建议客户根据第五章-常见问题对云主机安全组进行安全加固。

4. 安全专区使用手册

4.1. 安全专区总览

安全专区总览作为系统平台的安全运营展示界面，通过多维度实时展现了资产状态、威胁信息统计、安全组件详情等安全情况，提供实时监控、告警界面等展示方式，帮助用户对资产进行统一的安全管控。

4.1.1. 资产状态

展示服务器安全状态、服务器数量、存在风险的服务器数量和未受保护的服务器数量，统一查看服务器资产安全状态。

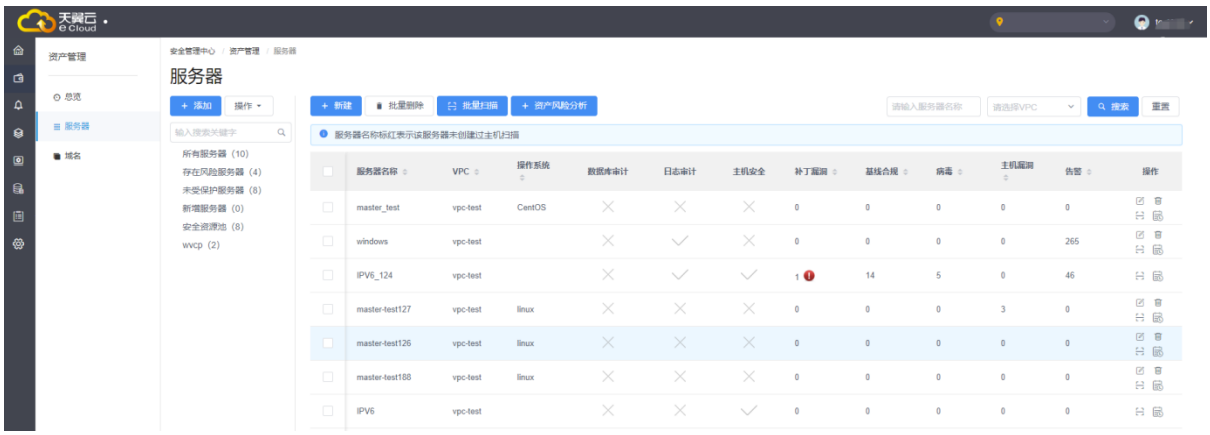
『资产总数』：服务器资产以及资产的风险状态统计数据。

『未防护资产』：未被授权保护的服务器资产。

『存在风险服务器』：存在漏洞、基线风险、告警等安全风险的服务器。

『存在风险网站』：存在漏洞、基线风险等安全风险的网站

点击存在风险的服务器数量、未受保护的服务器数量和存在风险的服务器数量，可跳转到资产管理页面查看具体服务器资产的安全信息，并详细分析资产安全状态。



4.1.2. 防御能力

展示已部署的安全能力及组件信息。

4.1.3. 安全评分

展示云资产整体安全水平，掌握资产的安全分值，发现资产安全风险数量。

4.1.4. 安全态势

威胁信息统计展现待处理告警、待处理漏洞及待处理基线，实时展示威胁统计状态。

待处理告警：展示资产中的告警总数量；点击【去处理】，即进入【告警中心】进行详细风险查询以及处理风险；

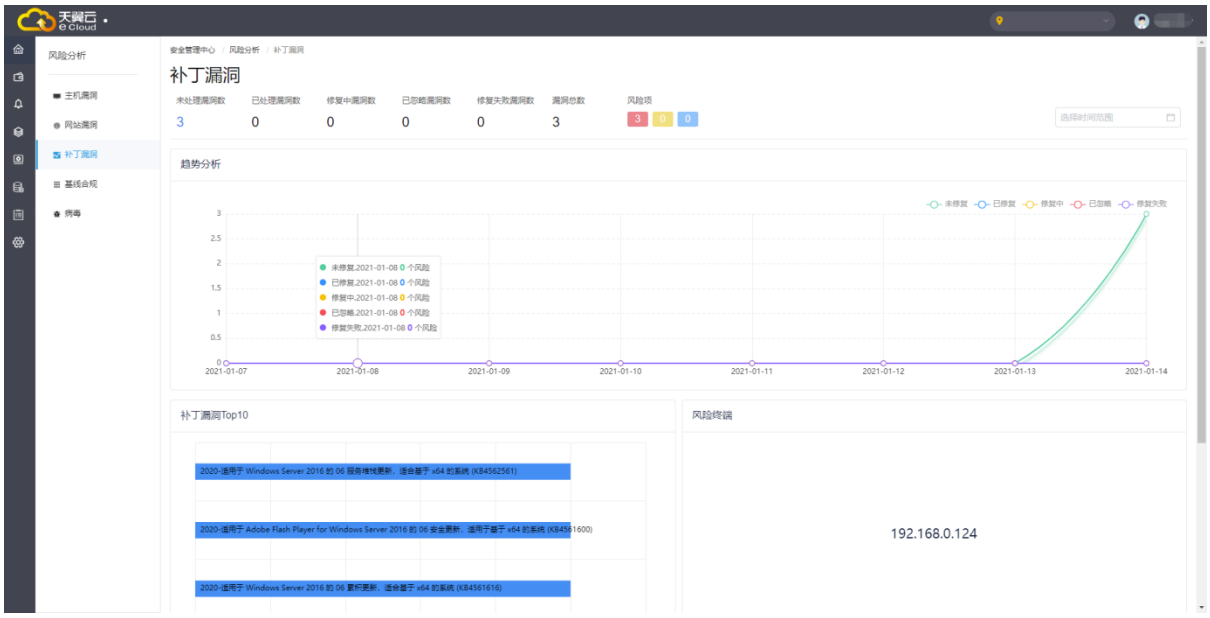
待处理漏洞：资产中存在的漏洞总数；点击【去处理】，即进入【风险分析】的“主机漏洞”，在该页面，可进行主机漏洞的详细查询及进行处理；

待处理基线：资产中存在的基线风险总数量；点击【去处理】，即可进入【风险分析】里的“基线合规”，可进行基线合规、不合规项数据、基线漏洞情况的详细查询及处理；

4.1.5. 风险事件

实时反馈补丁漏洞相关风险，对资产在使用过程中暴露的问题进行实时告警，自动检测产生安全风险评估、分析并给出处理导向。

点击【去处理】，进入相关的组件进行具体事件的分析处置。



安全专区总览查询后，可打开左侧边栏主菜单。

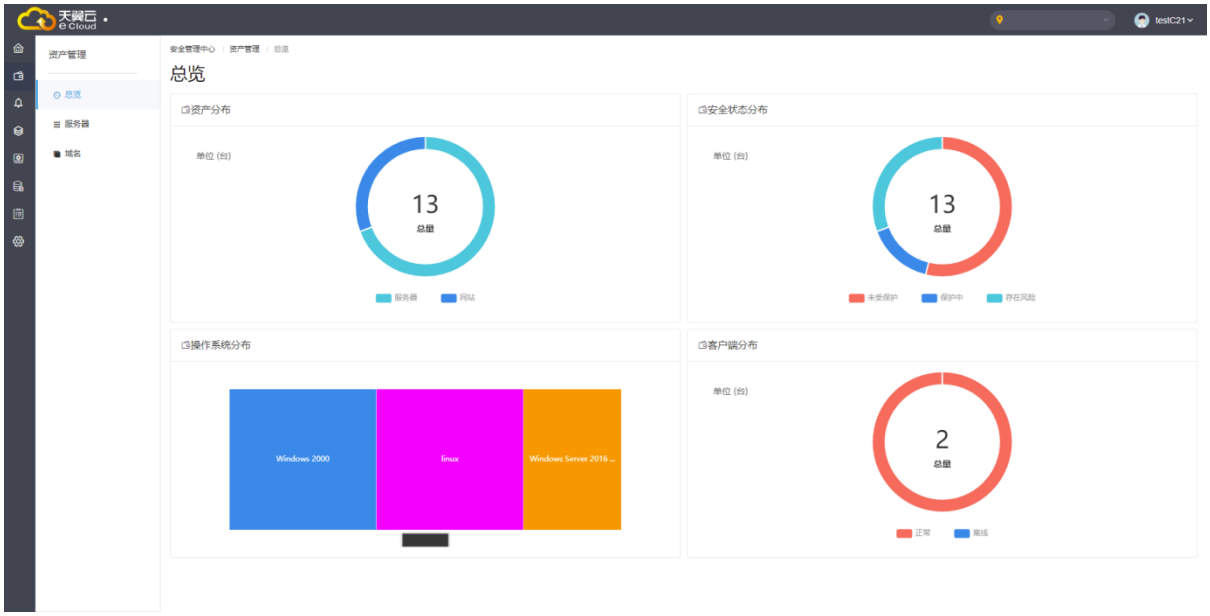
4.2. 资产管理

资产管理从资产的类型、防护状态、风险状态等维度分别展示资产对应安全信息。为便于对资产信息进行管理，资产管理提供了资产分组分类功能，可以通过资产分组查看安全事件；也可以通过资产标签查看具有相同属性的资产以进行数据分析溯源。

资产管理模块还具备对资产进行漏洞扫描功能，对资产的脆弱性进行评估。

4.2.1. 资产总览

资产管理总览页面展现资产信息，展示用户资产分布及安全状态情况。

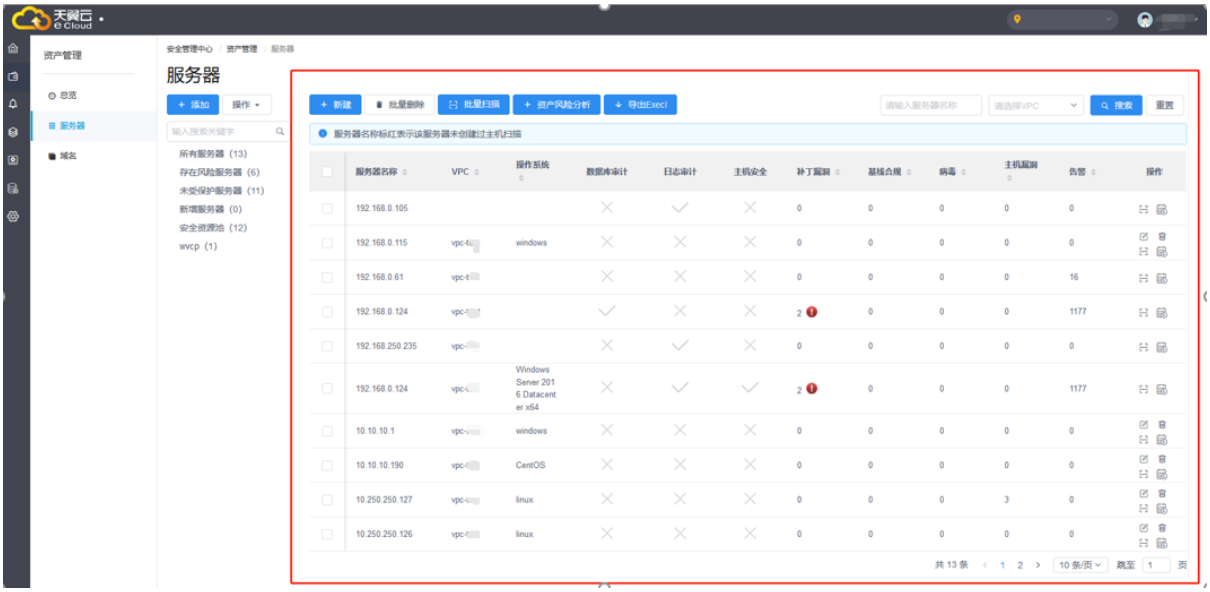


4.2.2. 服务器主机

资产管理功能自动识别租户云资产，并关联安全组件部署配置信息、关联安全组件的风险检查结果、威胁检测结果，实时、全面展示服务器资产整体的安全防护及运行状态。

用户可以对服务主机资产进行分组管理，发起主机漏洞扫描，从资产的维度进行风险分析，系统提供时间轴视图方便事件溯源。

资产列表



资产描述区域

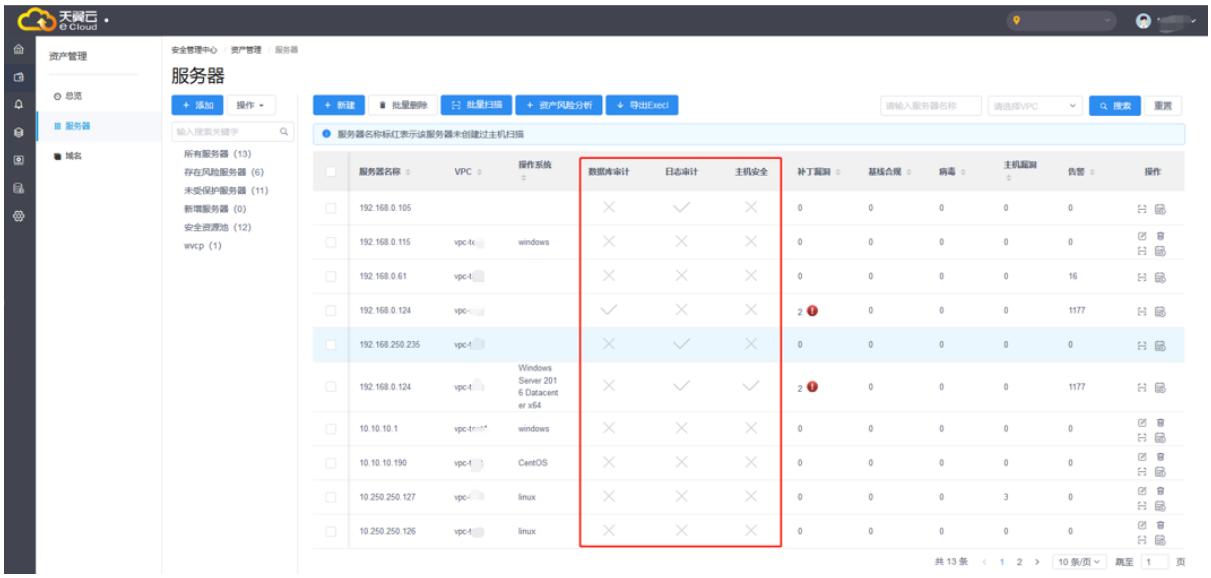
[服务器名称]：服务器资产 IP 地址

[所属 VPC]：可选择

[操作系统]：服务器资产类型

防御部署状态区域

服务器主机安全组件部署情况。



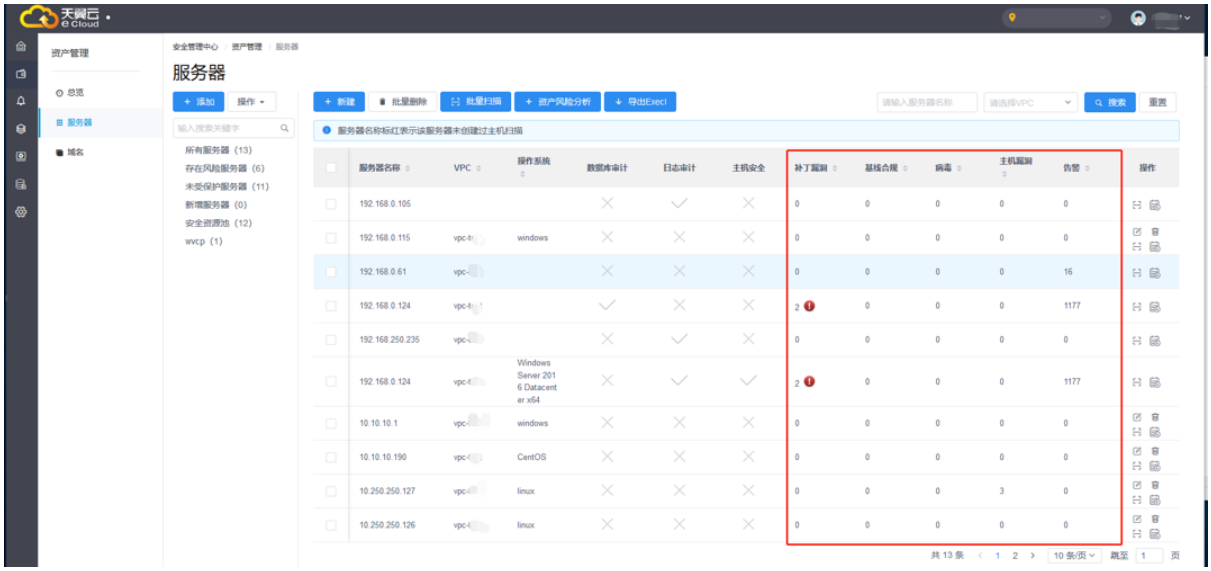
[数据库审计]：是否已配置数据库审计

[日志审计]：是否已配置日志审计

[主机安全]：是否已安装终端安全 EDR 客户端

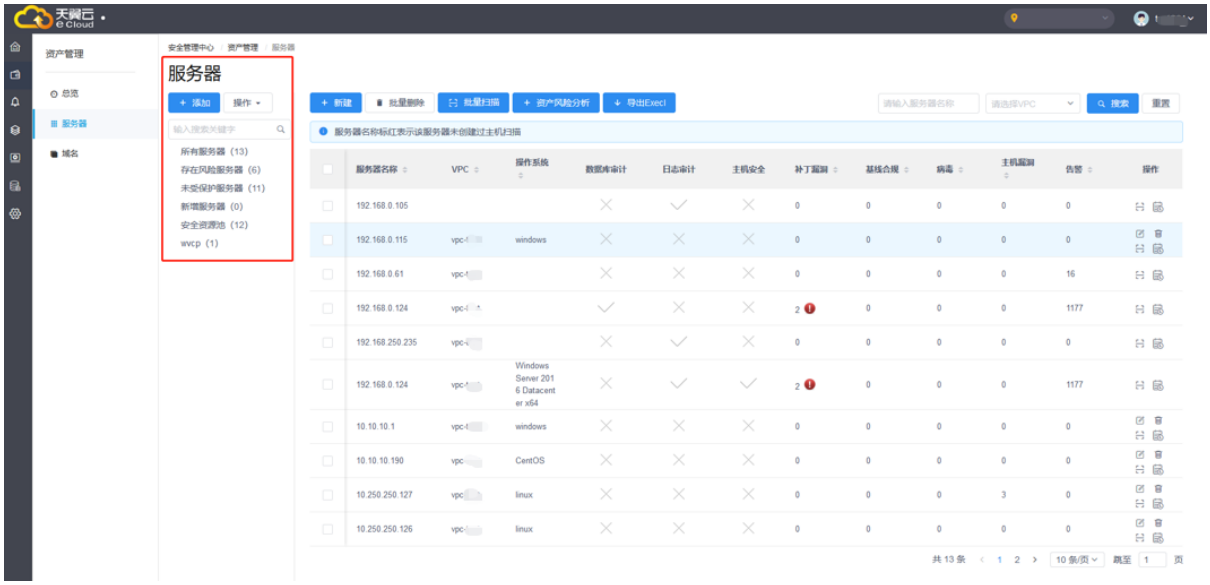
安全数据区域

汇总展示服务器主机威胁、漏洞安全情况。



分组浏览

可选择服务器分组进行筛选资产。

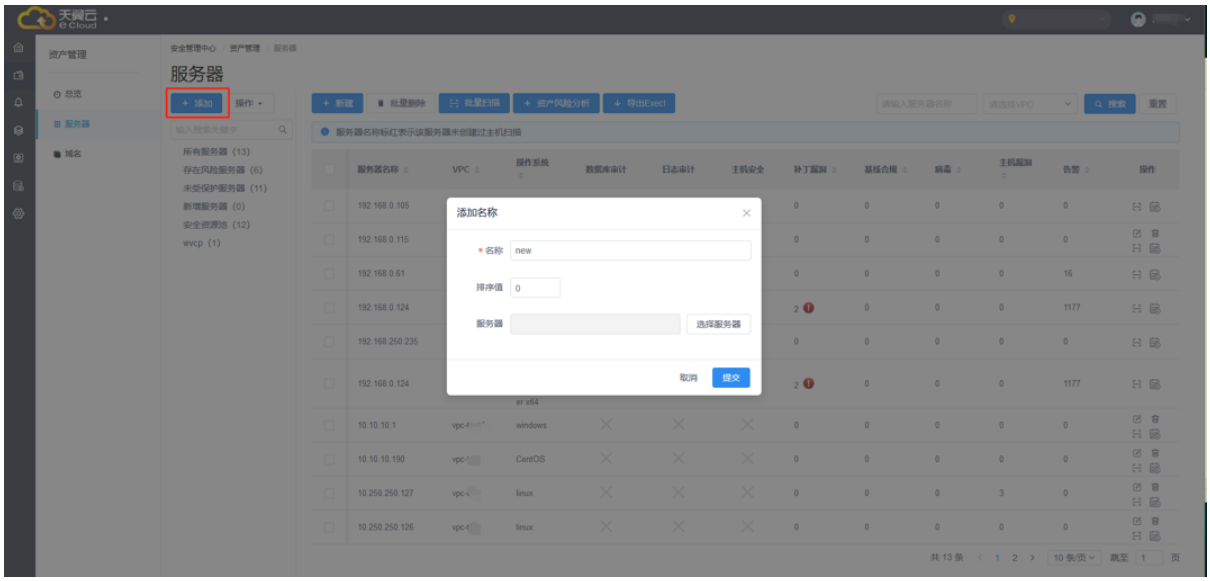


资产管理

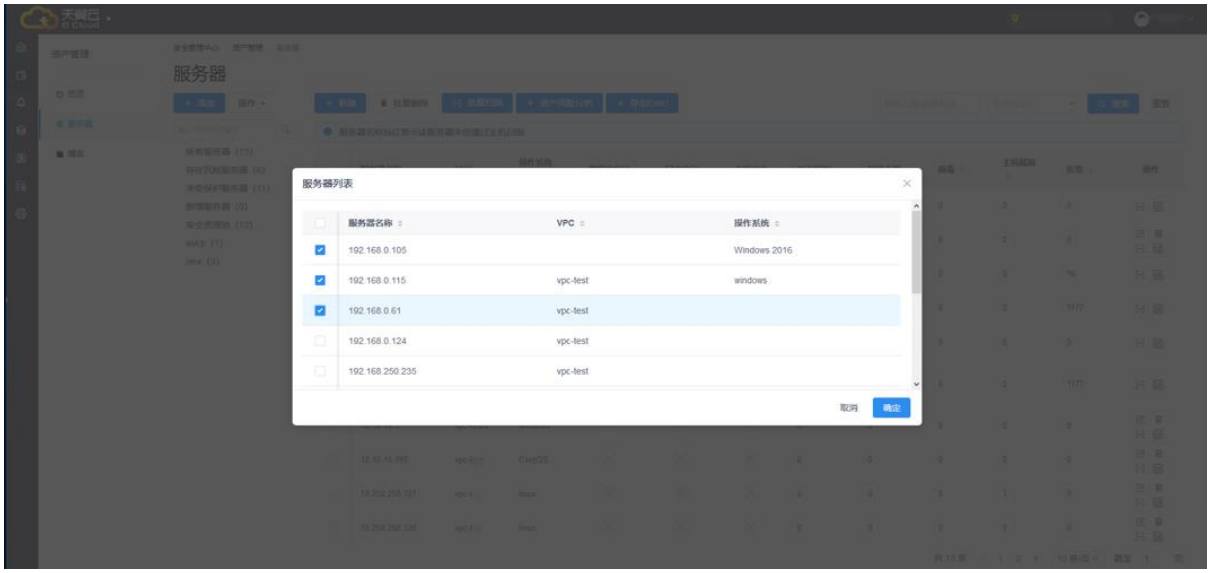
云上资产可通过自动识别添加，线下的资产可通过手动增加自定义资产。

新建服务器组

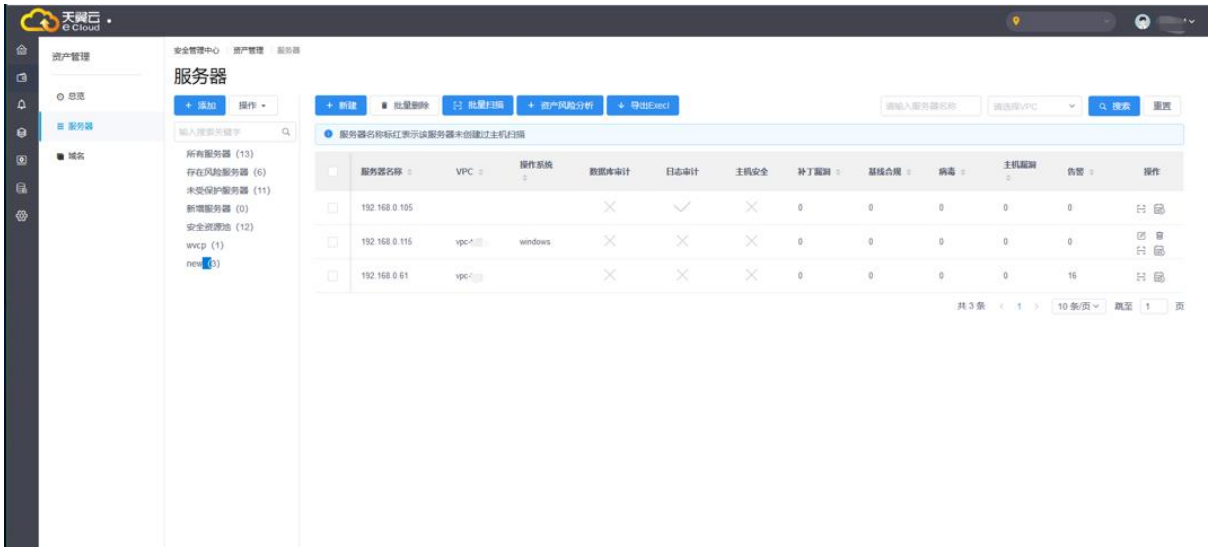
进入『资产管理』➔『添加』，新建服务器组，填写组别名称，设置排序值。



点击『选择服务器』，进入服务器列表，选择要分配到该组的资产服务器，『确定』提交

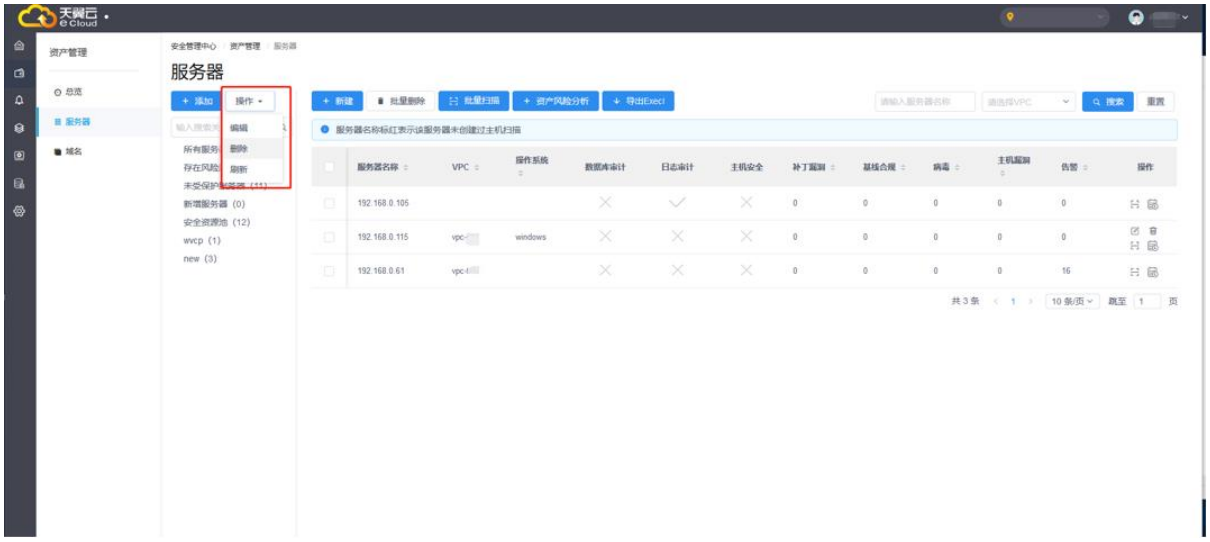


点击确定按钮，则新增成功



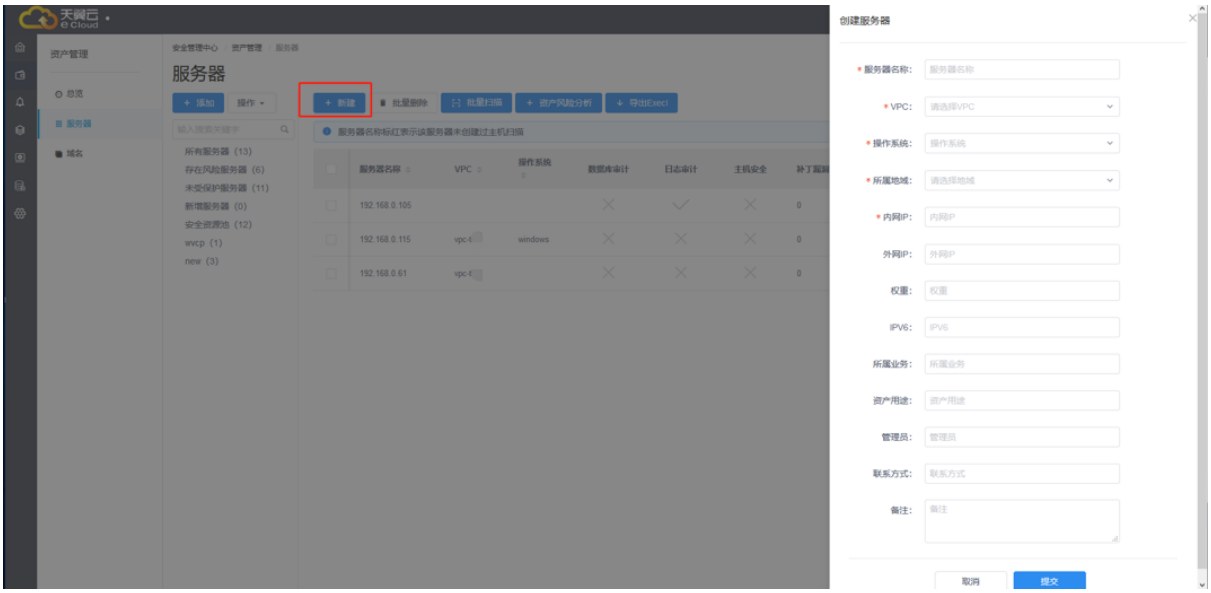
编辑服务器分组

选择所要编辑的服务器组，点击『操作』，可进行『编辑』、『删除』以及『刷新』操作。



自定义服务器

进入『资产管理』→『新建』，打开自定义服务器窗口，填写服务器资料，新建自定义服务器。



[服务器名称]:服务的名称

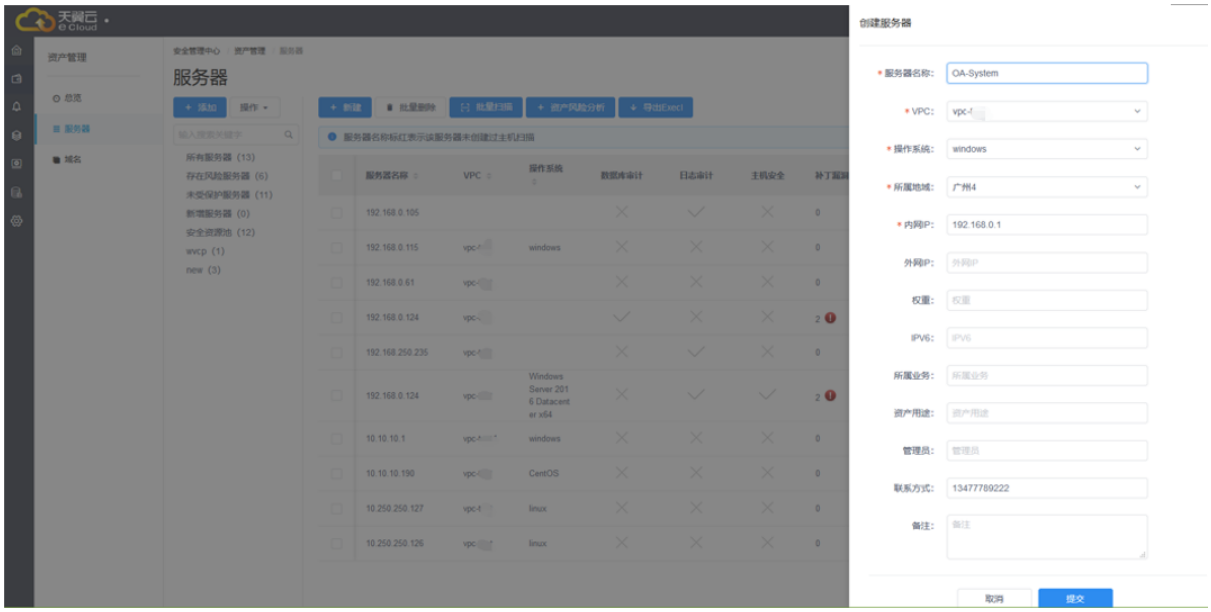
[VPC]：所属 VPC

[操作系统]:选择操作系统类型

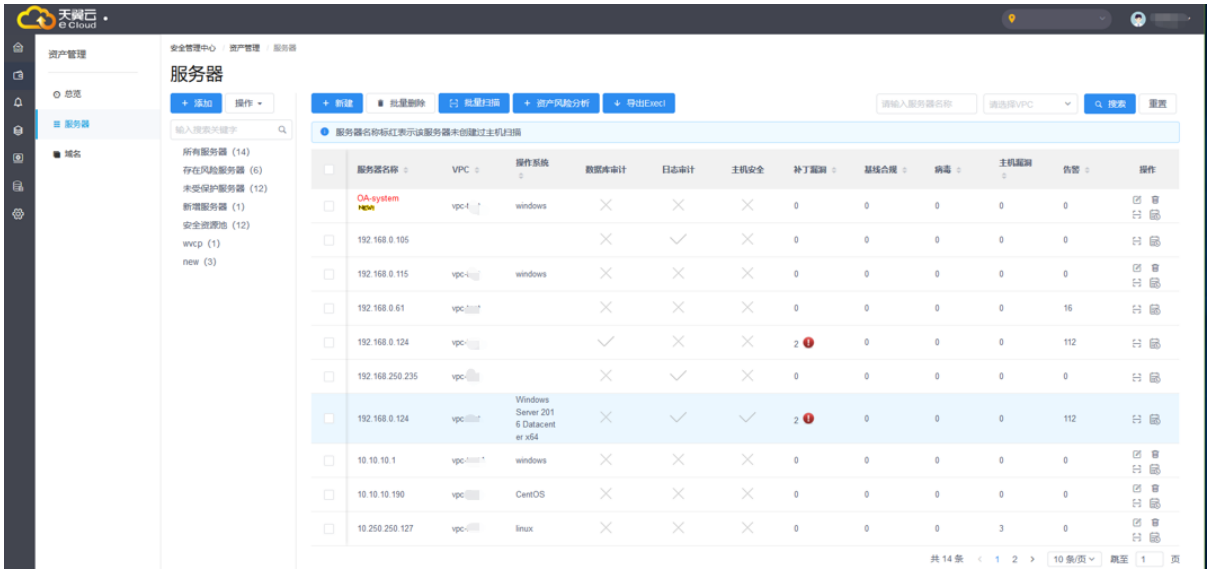
[所属地域]:选择服务所在区域

[内网 IP]：服务器 IP 地址

所示模板如下，进行点击『提交』，即可创建成功。

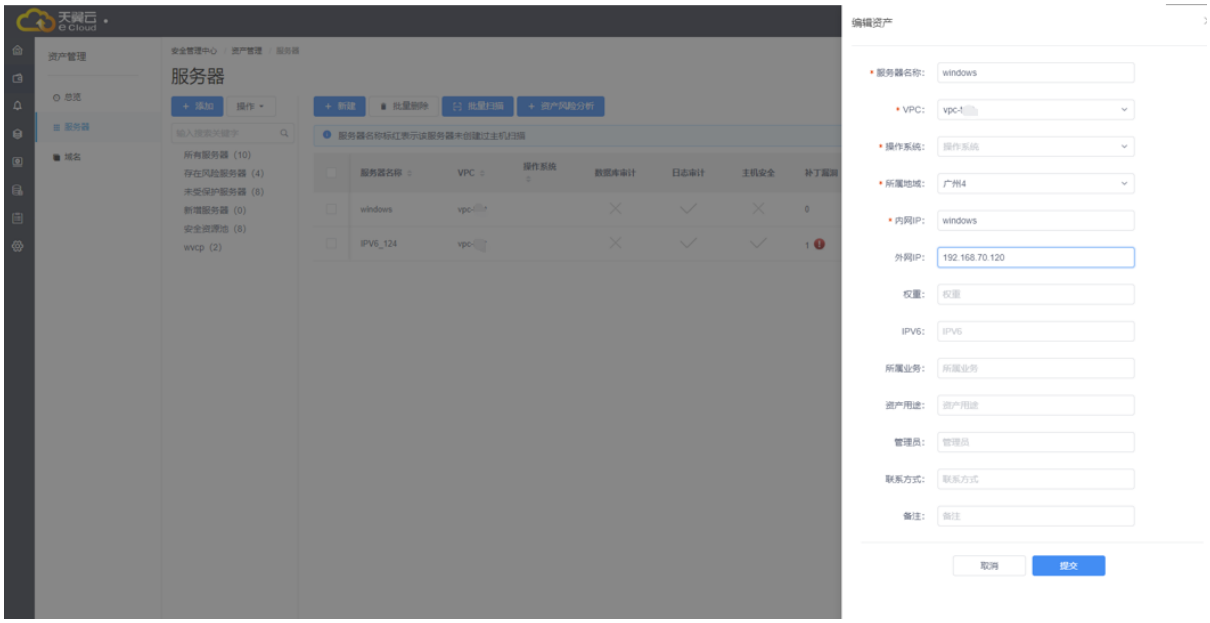


在【新增服务器】列表中可查看到新增的服务器信息（新增的服务器有 new 图标标识，查看或编辑后该图标则消失）



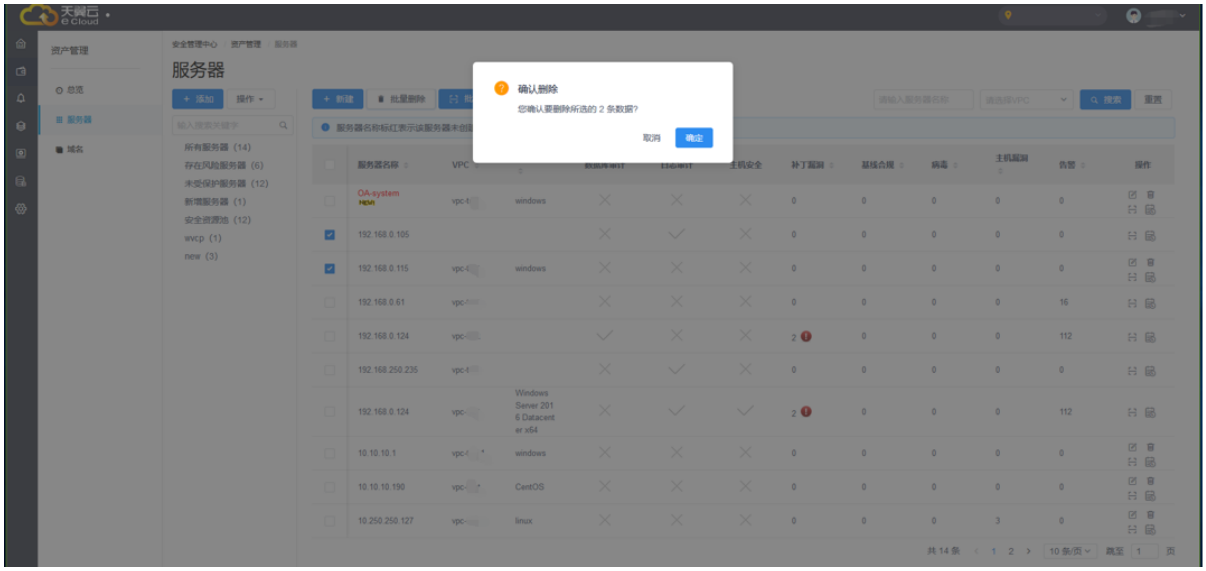
服务器信息编辑

进行单个服务器设置，点击服务器右侧栏『操作』→『编辑』，进行资产的编辑及修改。



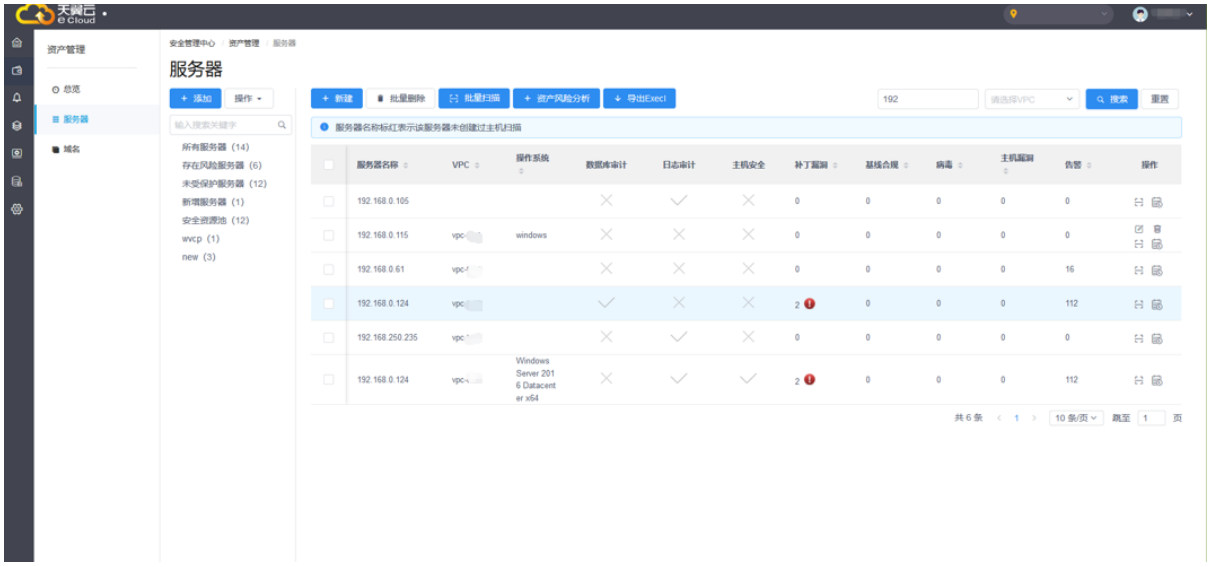
删除自定义服务器

勾选需要删除的服务器记录，点击『批量删除』→『确定』，即删除完成

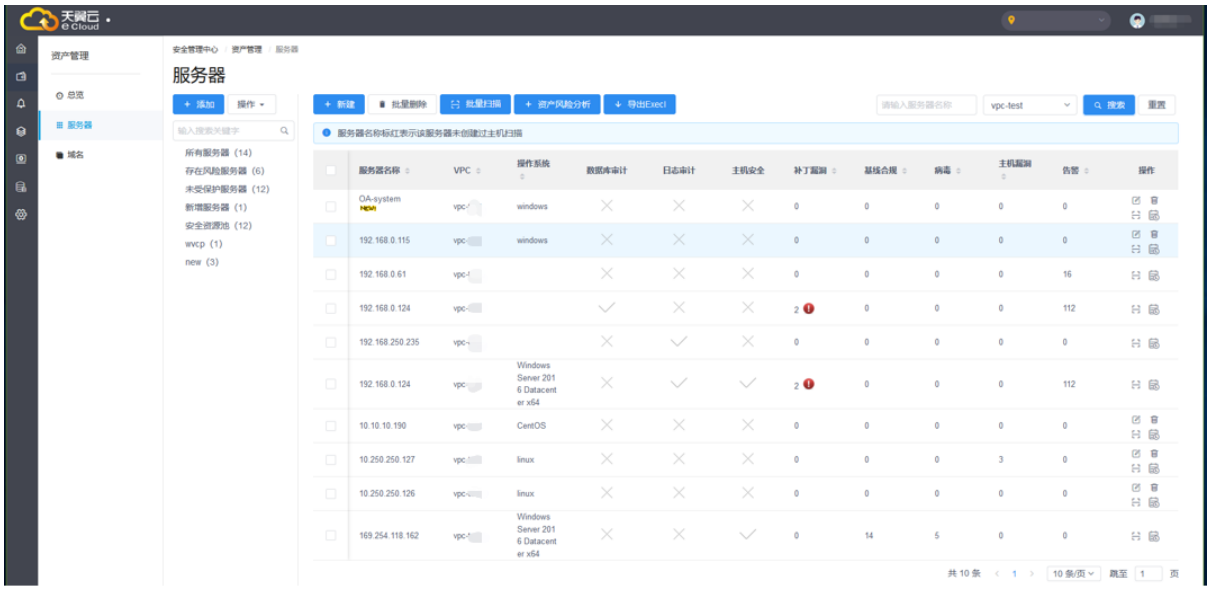


服务器记录查询

搜索功能操作，可进行“服务器名称”关键词、“VPC”名称筛选，选择服务器，名称筛选。

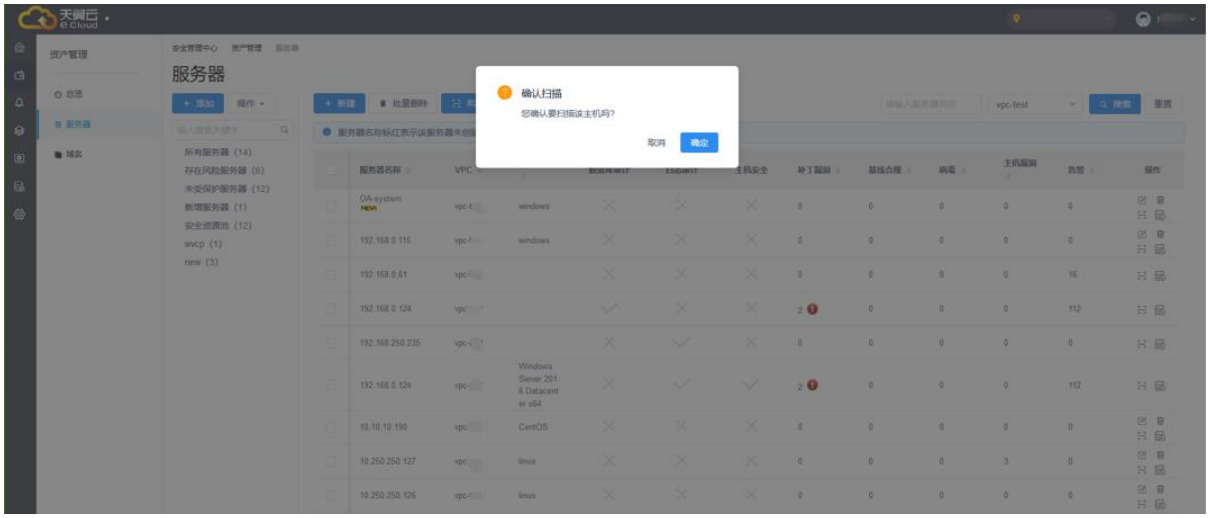


选择 VPC 筛选，输入“vpc”，即可进行查询。

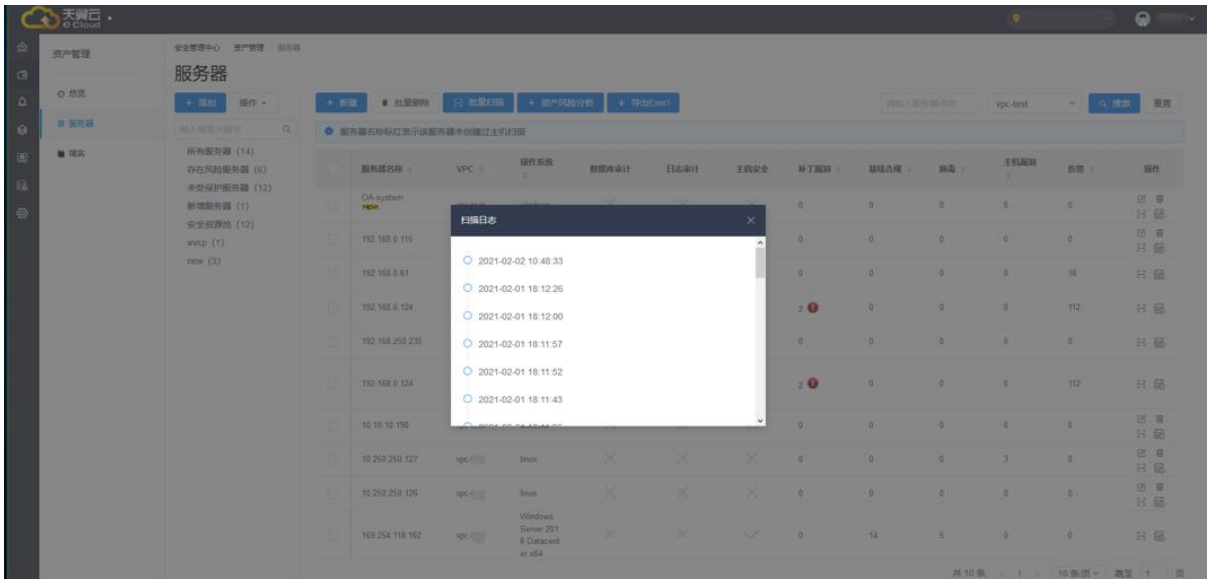


主机漏洞扫描

进行单个服务器配置扫描，可选择『操作』→『扫描』，点击『确定』即可进行扫描。



点击操作下的『扫描日志』，可查看扫描出来的日志，查看扫描的时间记录。

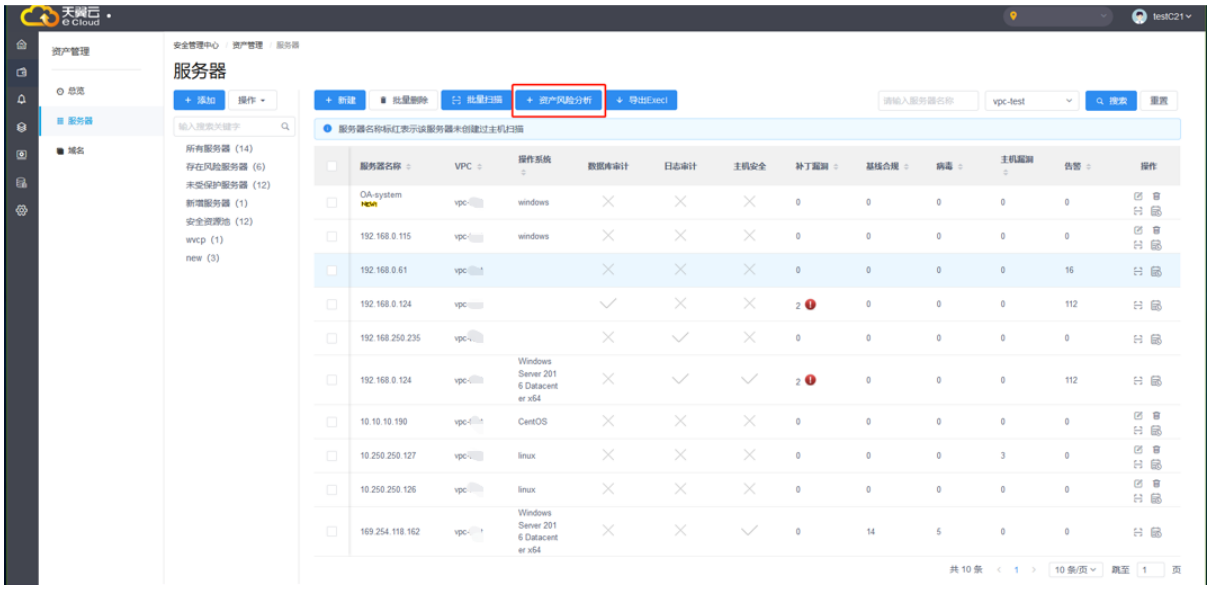


也可以选定多个服务器记录，点击『批量扫描』进行批量的主机漏扫。

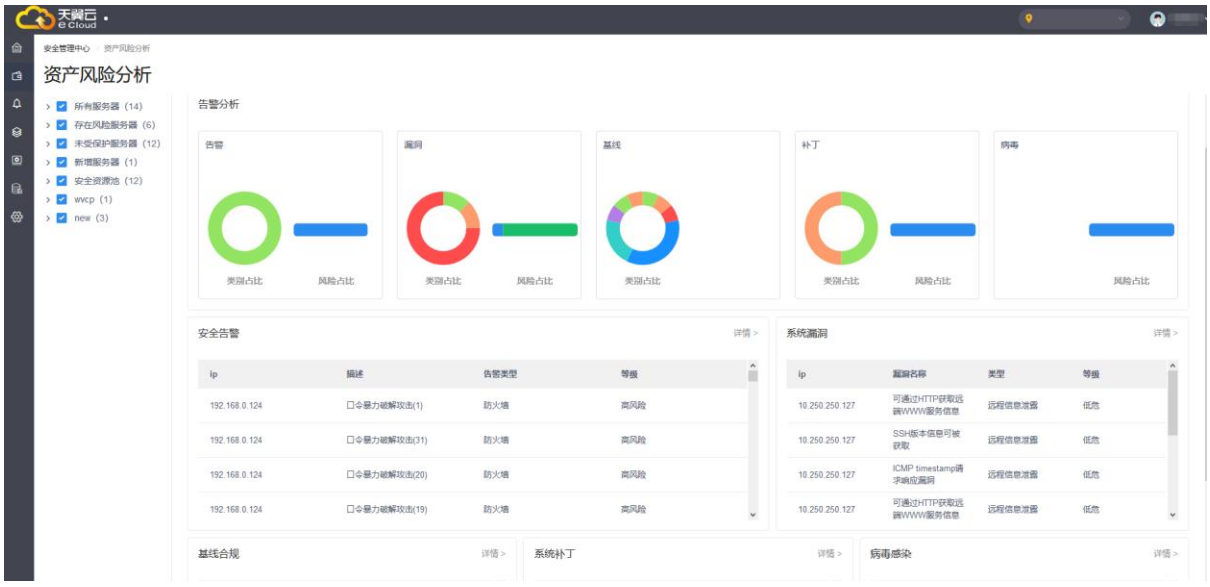
资产风险分析

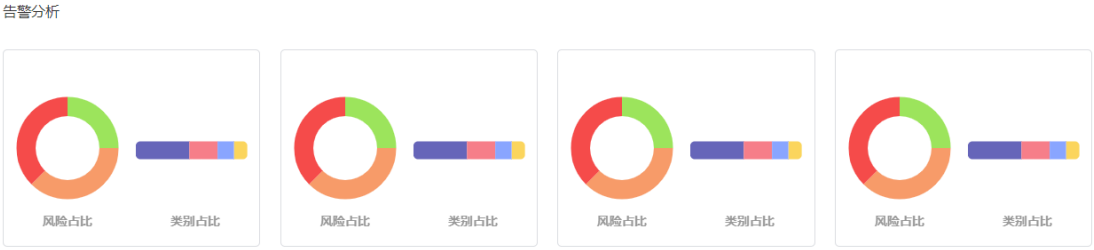
资产风险分析页面把所筛选的资产相关的未处理的告警、漏洞、基线、补丁、病毒五类安全数据整合在一个页面展示，方便安全管理员分析。

进入『资产管理』→『服务器』，点击『资产风险分析』，可查询分析指定服务器的各类安全漏洞、威胁、报警。



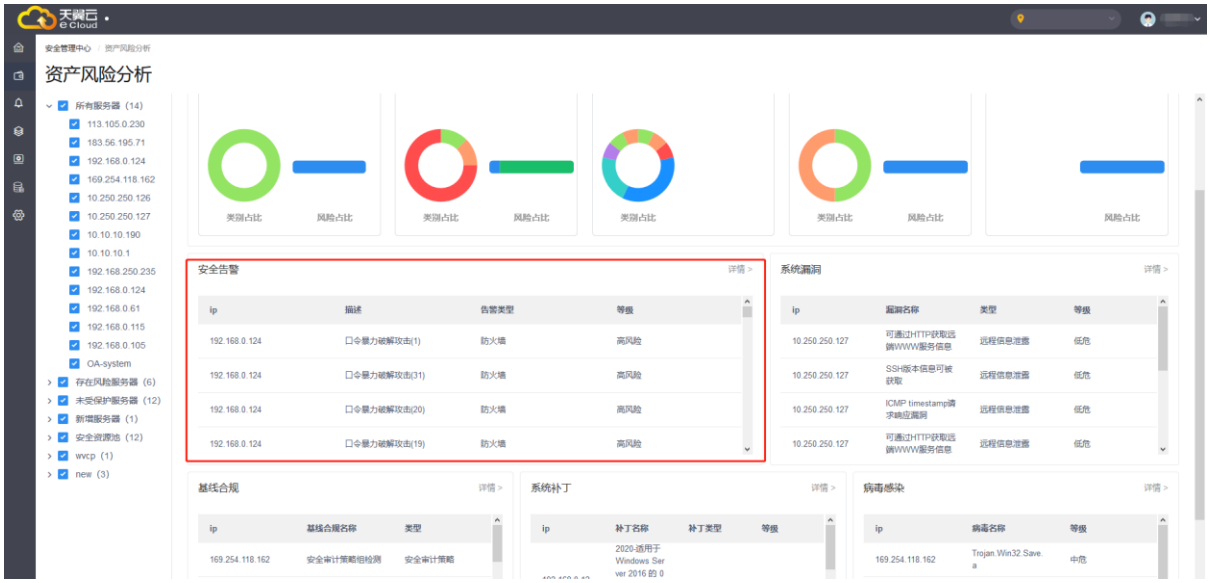
在左侧分组选定需要分析的指定服务器分组及服务器，进行资产信息筛选。页面右边栏实时同步更新所选择资产的展示，其中根据告警分析、安全告警、系统漏洞、基线合规、系统补丁及病毒感染等几大模块。



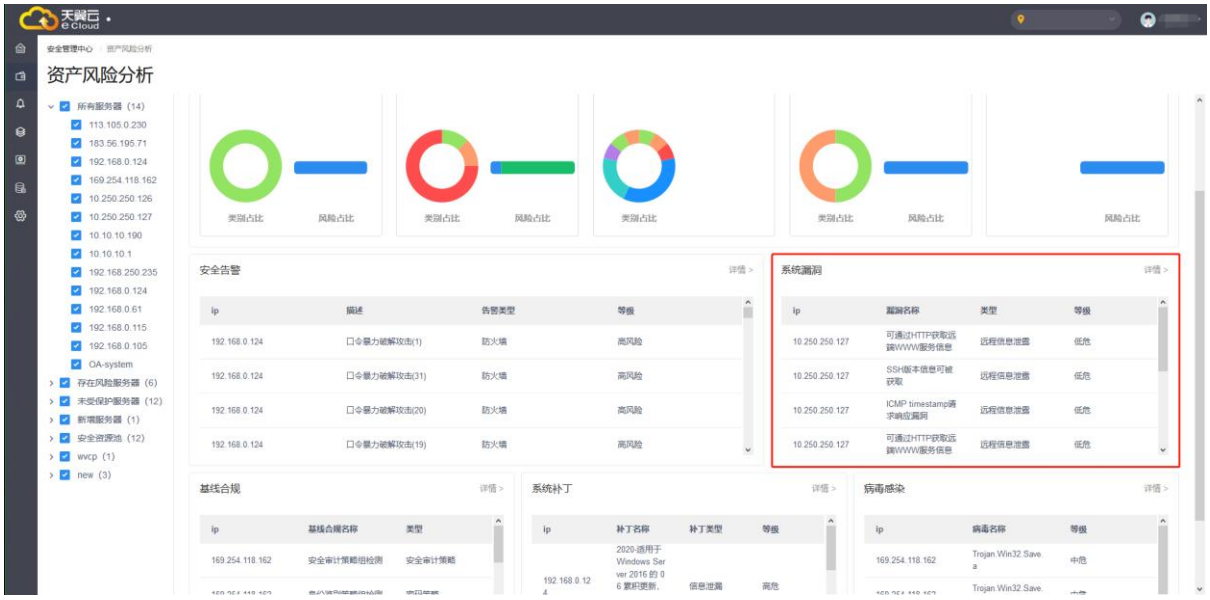


安全告警模块，实时更新服务器所出现问题，展示服务器 IP 地址、出现告警的问题、出现问题的服务设施以及告警的风险等级。

点击右上角『详情』，即进入【告警中心】，可查询更详细的告警信息。

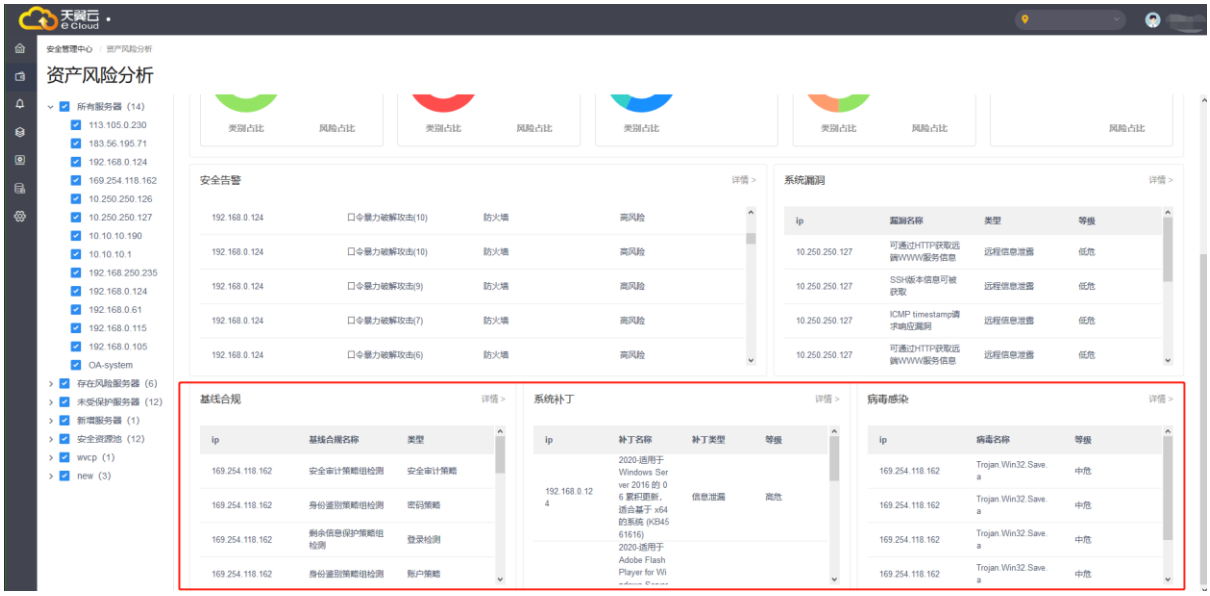


系统漏洞展示具体 IP 地址所发生的具体漏洞信息，分类漏洞等级情况。点击『详情』，即进入【威胁分析】→『待办告警』进行详细处理。



基线合规、系统补丁及病毒感染等模块都展示了系统风险状态、漏洞所属类型、漏洞所属风险等级。

、



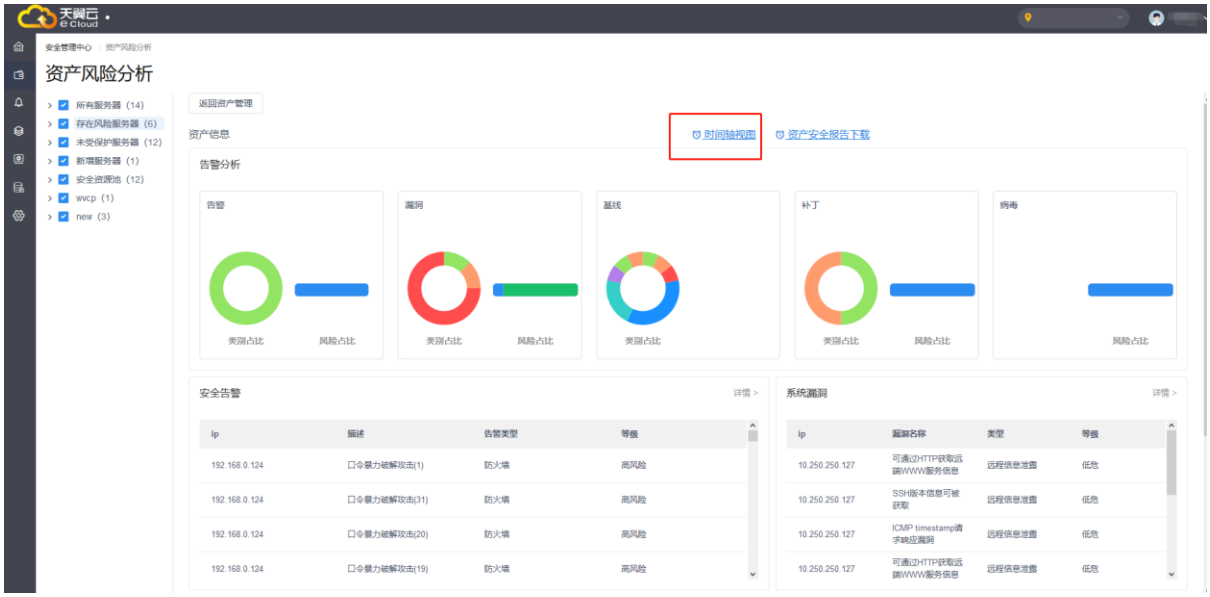
击【基线合规】→『详情』，即页面跳转进入【风险分析】→『基线合规』进行分析、处理。

点击【系统补丁】→『详情』，即页面跳转进入【风险分析】→『补丁漏洞』进行分析、处理。

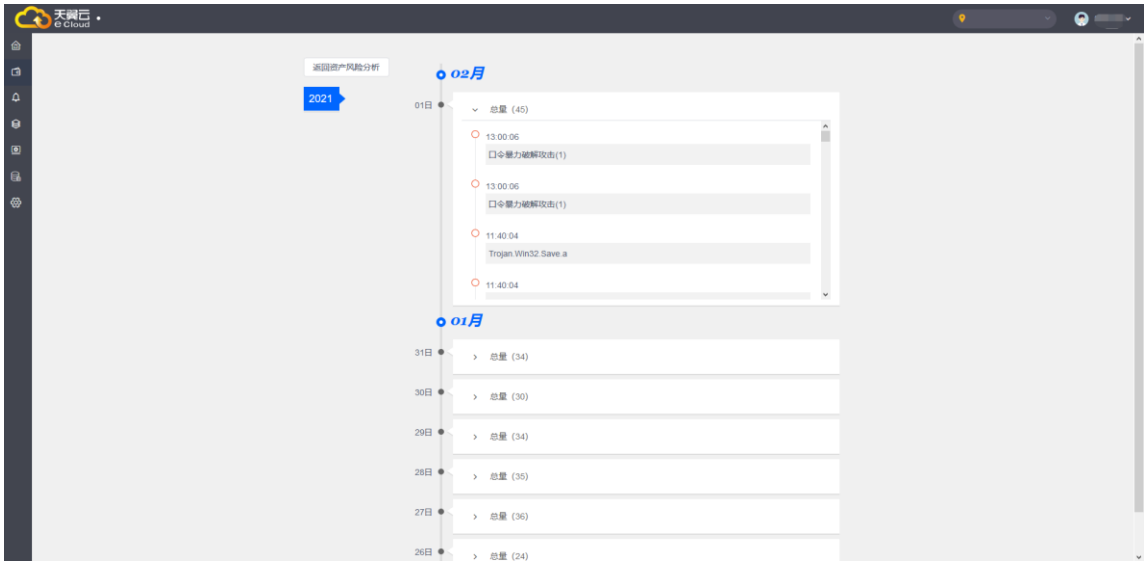
点击【系统补丁】→『详情』，即页面跳转进入【风险分析】→『主机漏洞』进行分析、处理。

安全事件溯源

在左侧选择需要分析的服务器或服务组，然后点击『时间轴视图』，可以进入时间轴视图进行事件溯源。

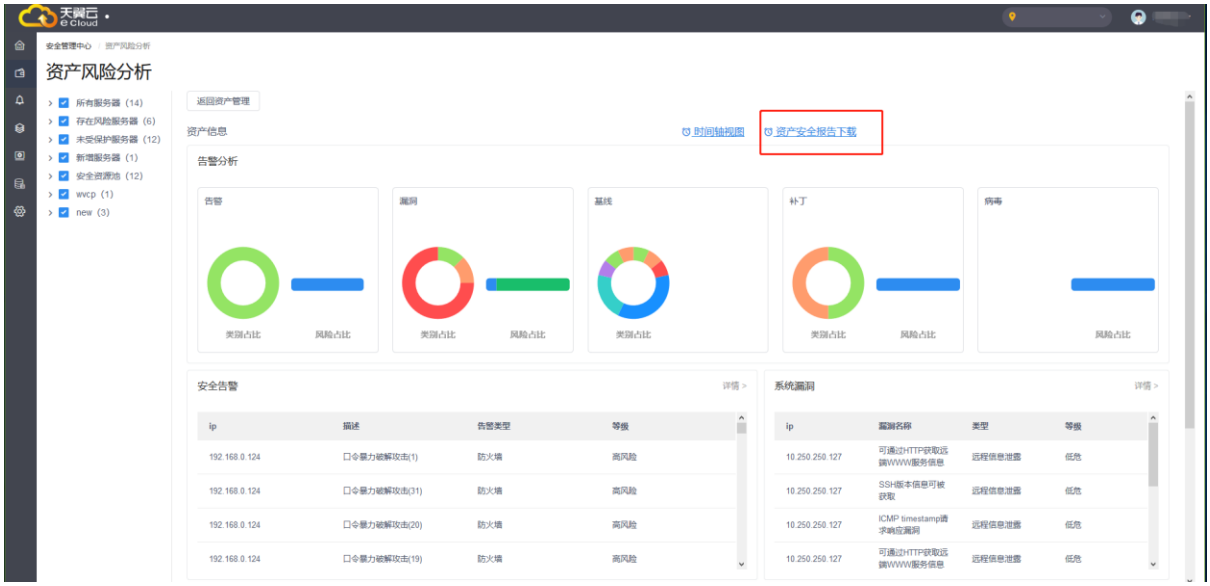


跳转到时间轴页面，时间轴视图按发生时间倒叙统计展示资产相关的安全事件，协助管理员从时间角度分析事件发生来龙去脉。



资产安全报告

在资产分析页面，点击『资产报告下载』，可下载所选定资产的安全分析报告。

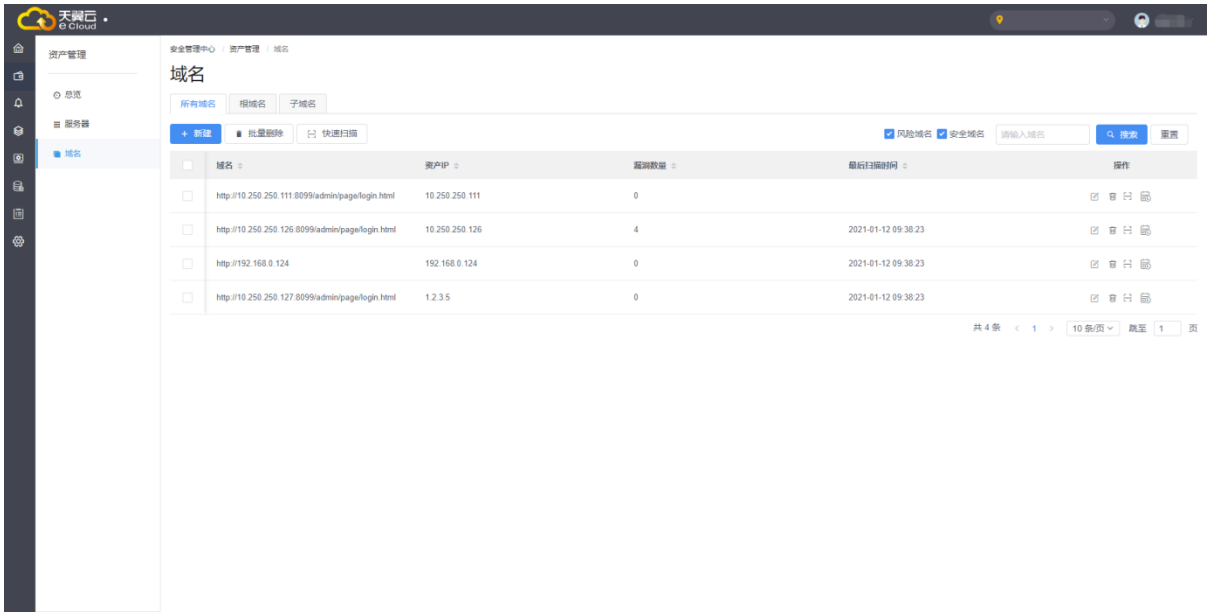


4.2.3. 应用域名

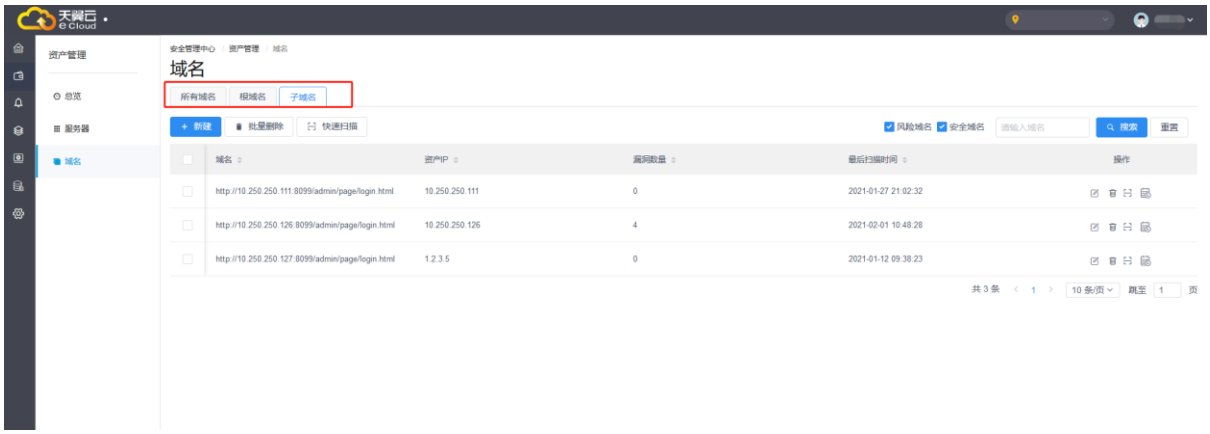
安全专区高级版支持进行网站漏洞扫描，分析网站安全问题。包括网站根域名、子域名漏洞扫描及其资产的风险状态和告警数量统计信息。

应用列表

进入【资产管理】→『域名』，通过域名对 WEB 资产进行安全状态管理。



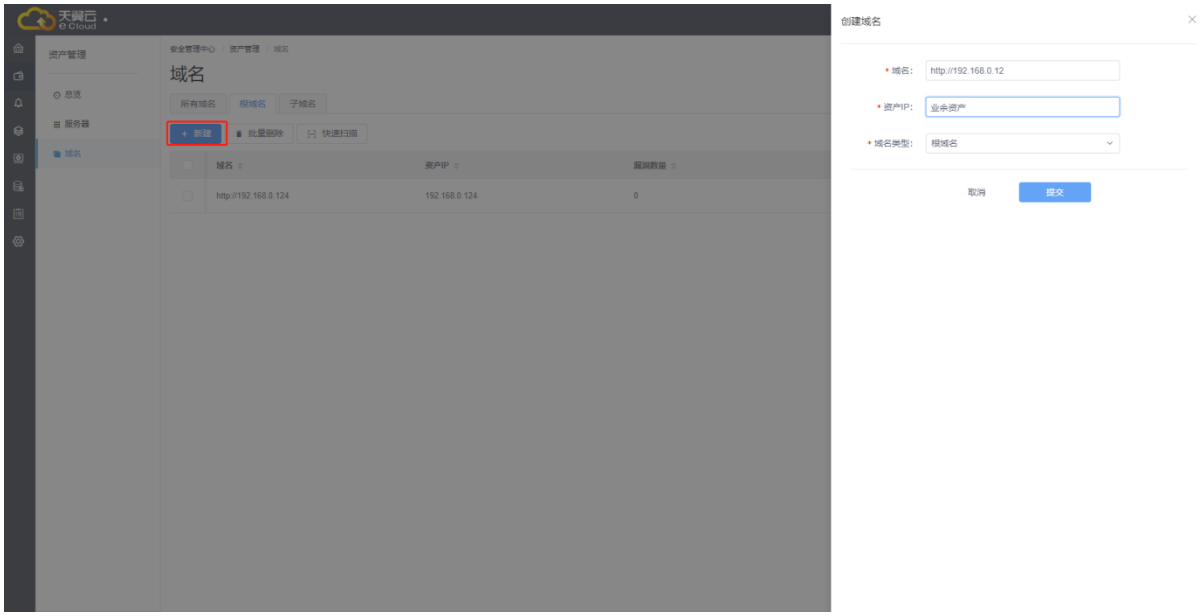
可选择点击『根域名』和『子域名』进行分组查询和管理。



应用管理

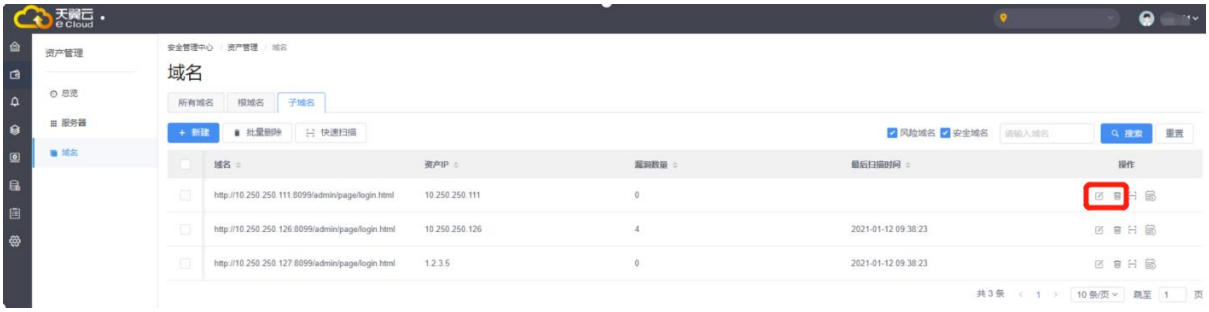
新建应用域名

点击左上角『新建』，进行应用域名创建，填写域名、资产 IP 地址及选择域名类型。提交确定即可。



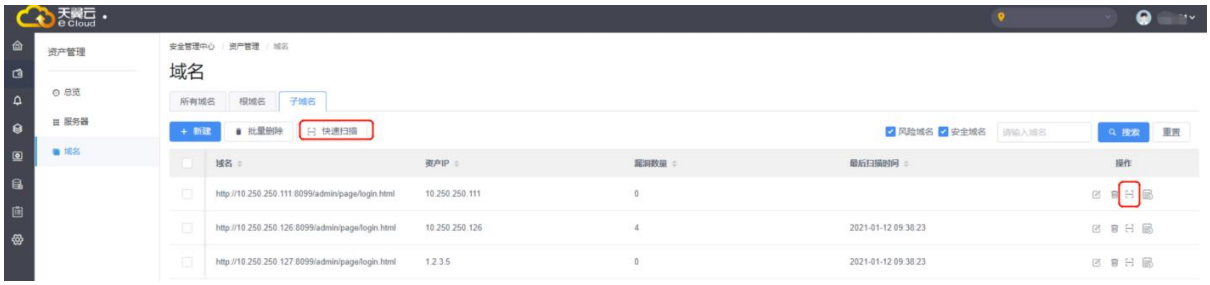
编辑应用域名

在域名操作栏，点击编辑及删除按钮，可对应用域名进行编辑或删除。



WEB 漏洞扫描

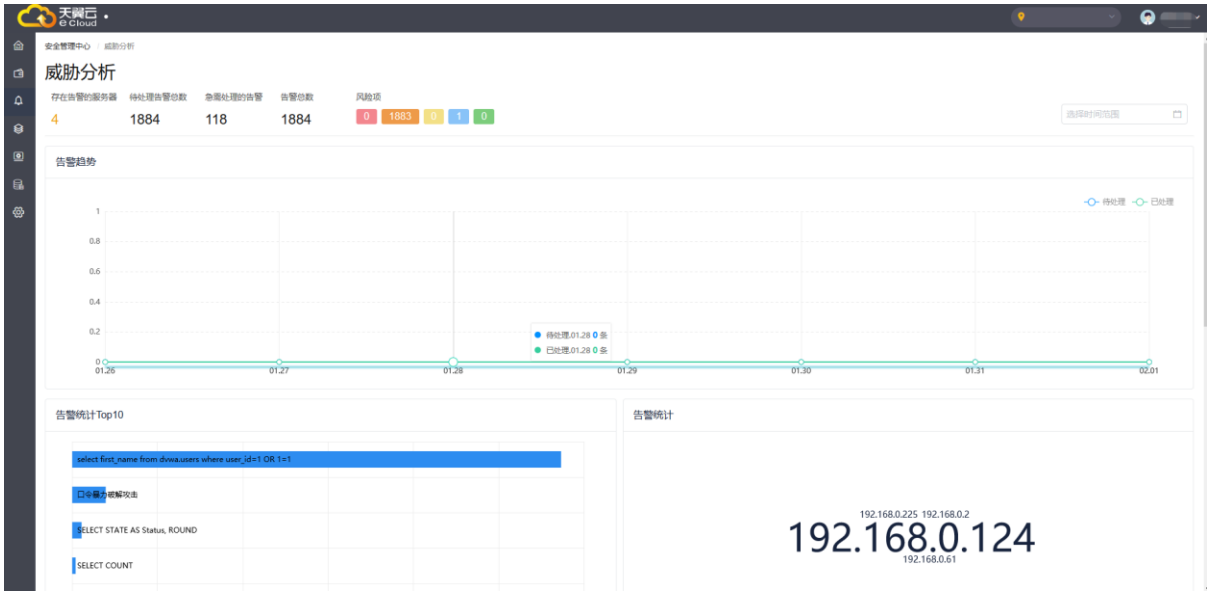
在域名操作栏，点击『扫描』按钮，可对应用域名进行 WEB 漏洞扫描。选定多个域名，点击『快速扫描』按钮可进行批量扫描。



扫描任务完毕后，系统会自动更新域名漏洞数据及扫描时间。点击任务的日志信息，可查看相关任务详情，例如具体终端 IP 地址、任务发生时间等。

4.3. 威胁分析

安全管理中心集中所有安全组件的告警数据，提供汇总集中的威胁关联分析手段。通过数据统计、告警趋势图、Top10 榜单、告警云、告警清单列表等分析工具，安全管理员可以快捷查询、统计、分析资产整体威胁情况。

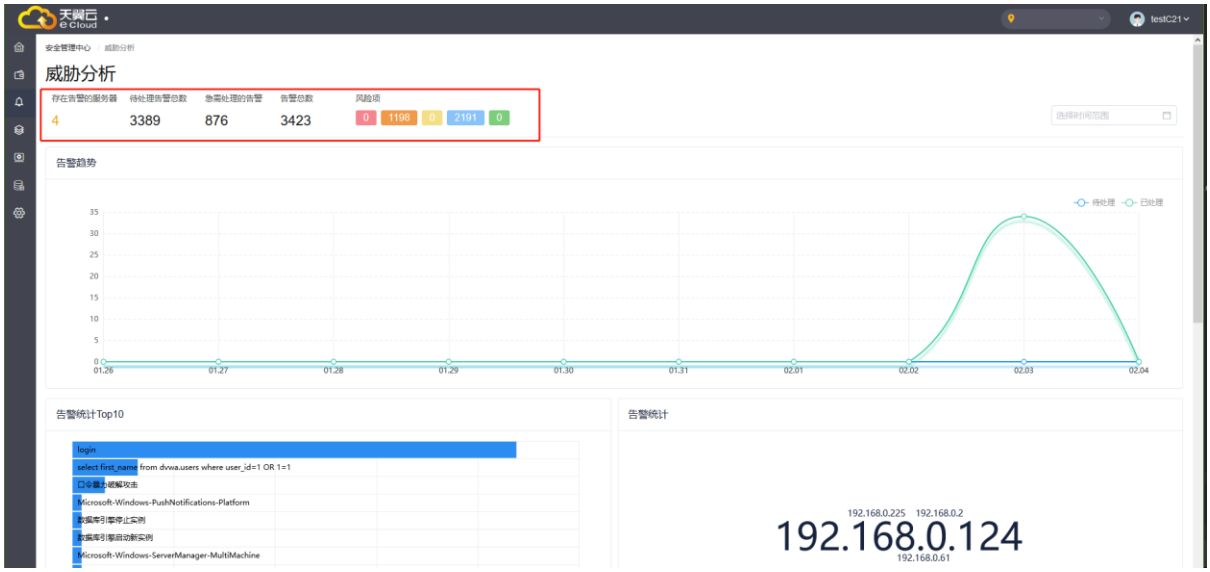


4.3.1. 告警数据统计

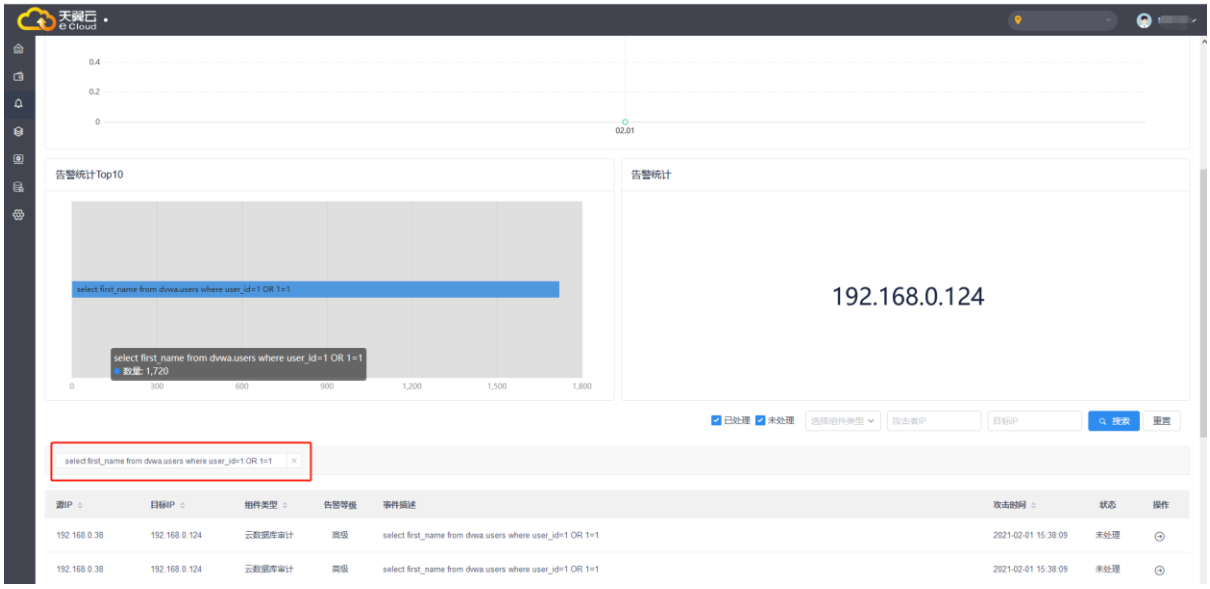
威胁分析页面顶部的数据统计栏展示了所有安全组件产生的告警数量及风险级别。

风险项级别分为严重（红）、高（橙）、中（黄）、低（蓝）、提示（绿）5 级。

统计项目包括存在告警的服务器数量、待处理告警数、急需处理告警数、所有告警总数，急需处理报警包括严重与高级别报警。

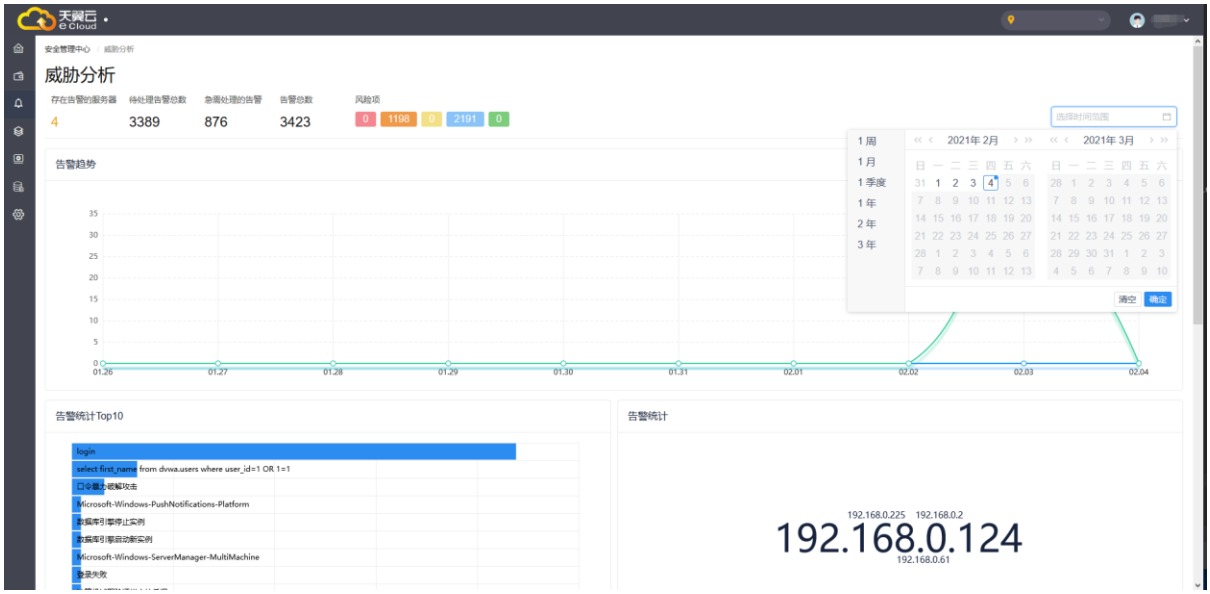


点击统计项目数字及风险项级别，可以把统计项目与风险级别加为筛选条件，页面下方的趋势图、告警云、TOP10、告警列表会即时根据筛选结果更新。如需取消筛选条件，在告警列表头上方删除条件。



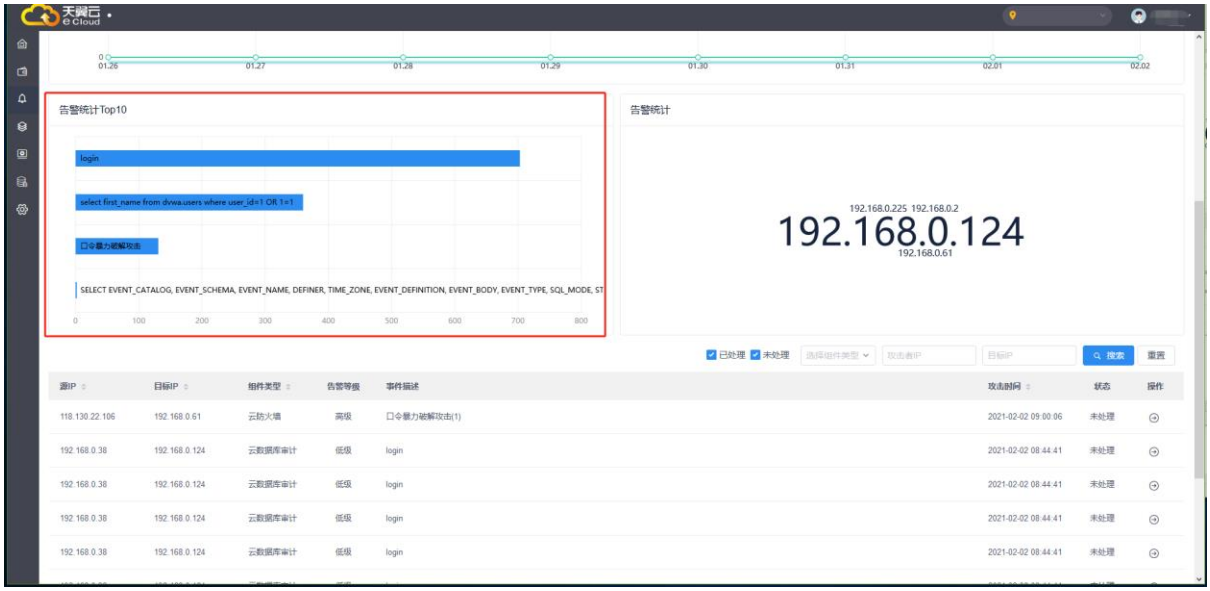
4.3.2. 告警趋势图

告警趋势图根据时间及告警数量的关系直观展示告警趋势，图形根据筛选数据结果实时更新。点击时间控件选择或输入统计起始时间。

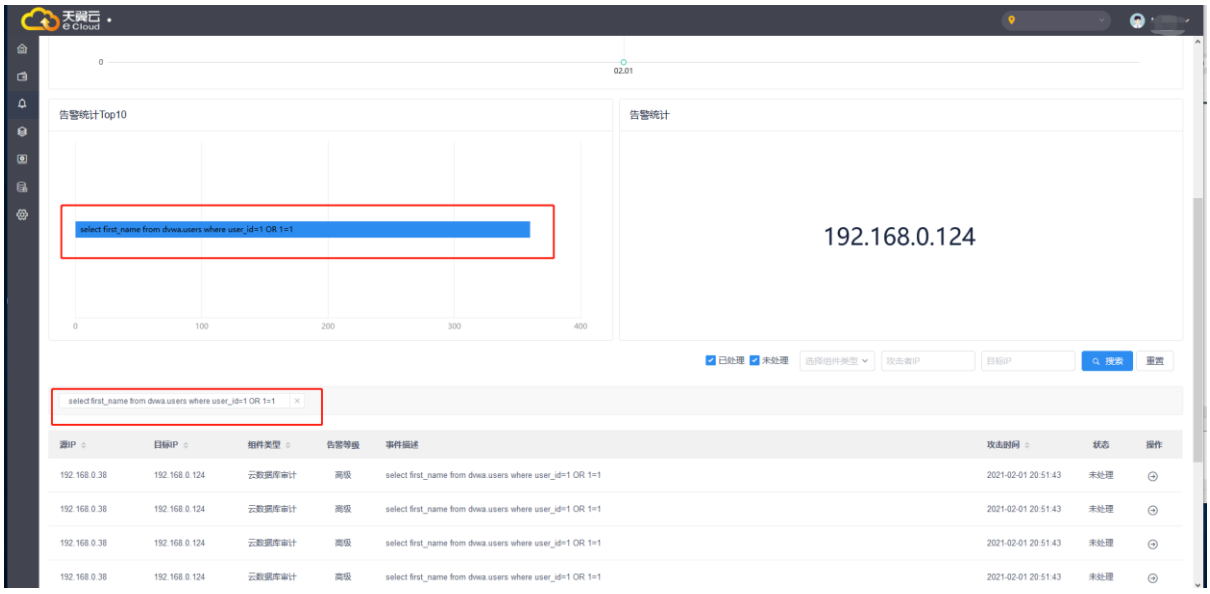


4.3.3. Top10 榜单

主机漏洞 Top10 榜单展示统计数量最高的事件排行榜，排行榜根据筛选数据实时更新。点击事件图示，可以把该事件加入筛选条件进一步分析。

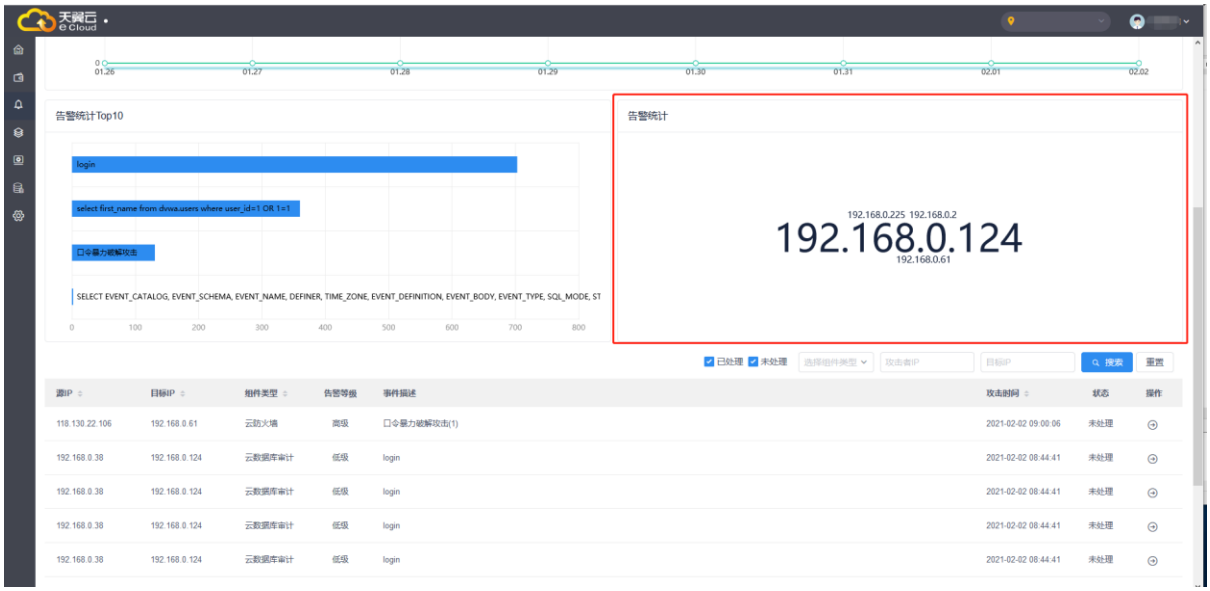


点击具体的告警，自动把告警名称加入筛选条件

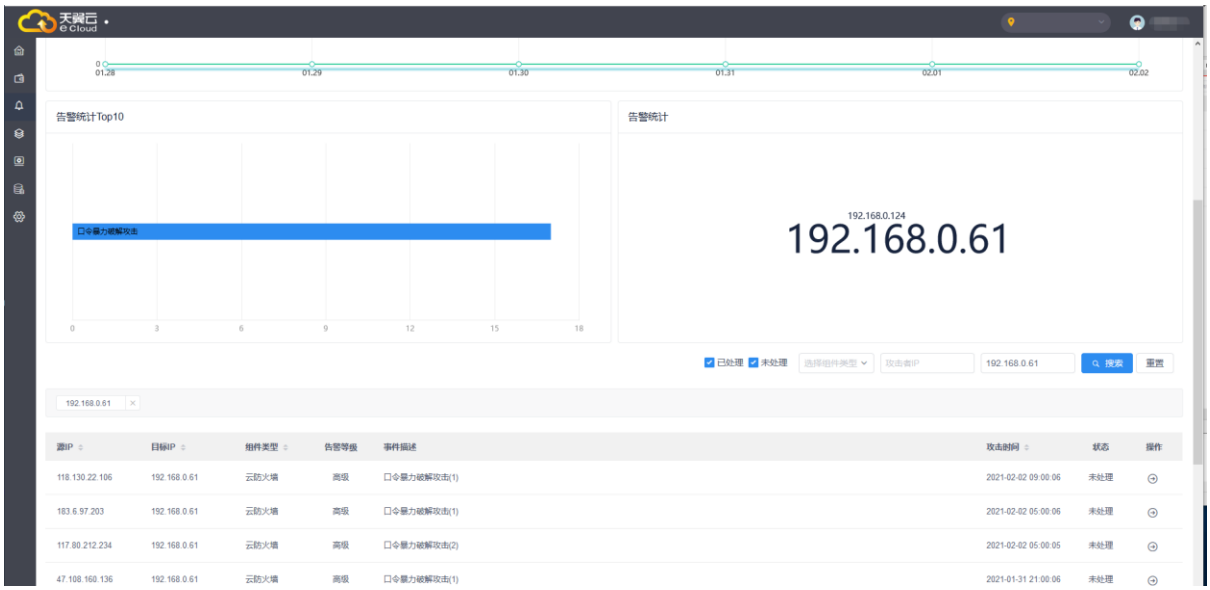


4.3.4. 告警云

告警云展示所有威胁目标 IP，并统计威胁目标 IP 关联告警数量。告警数量越多，IP 图形越大，凸显威胁情况越严重。

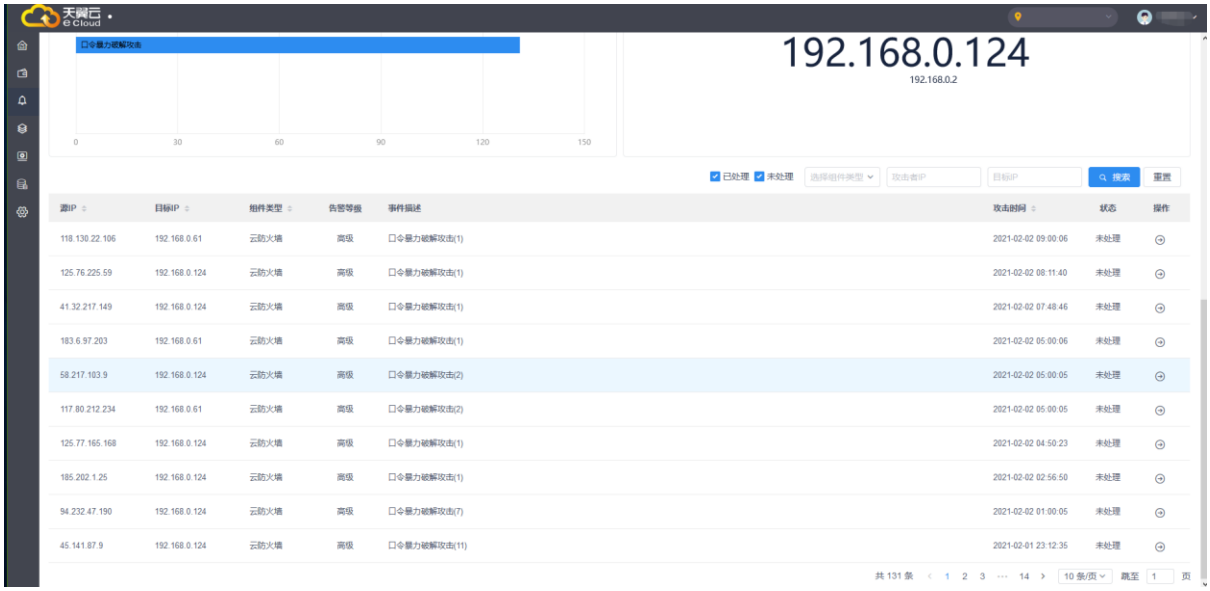


点击 IP 图形，自动把 IP 地址加如筛选条件

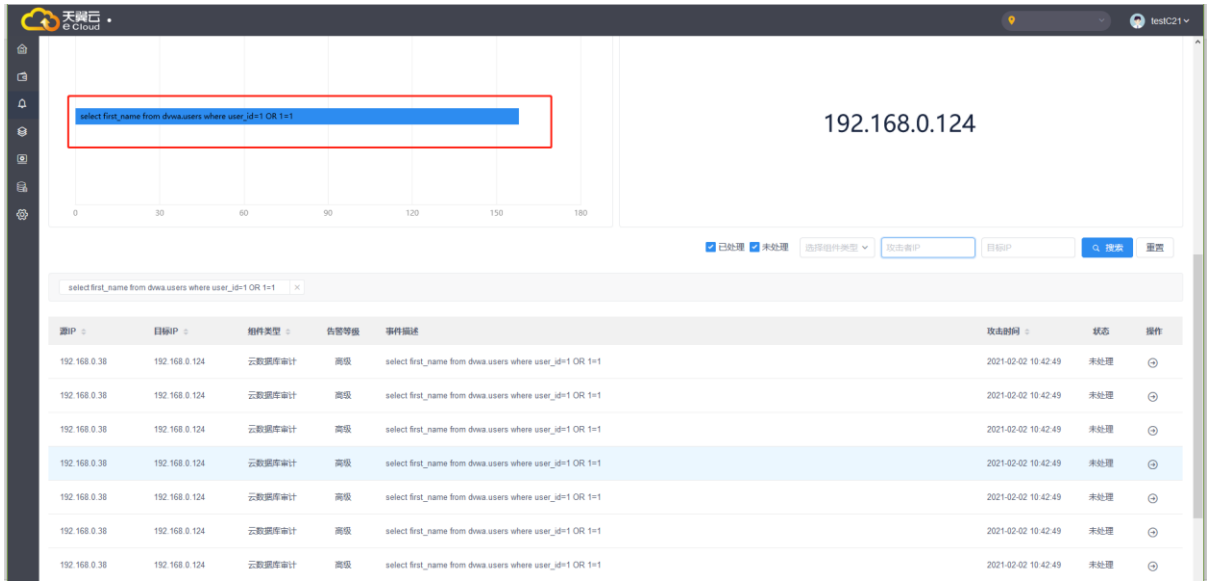


4.3.5. 告警列表

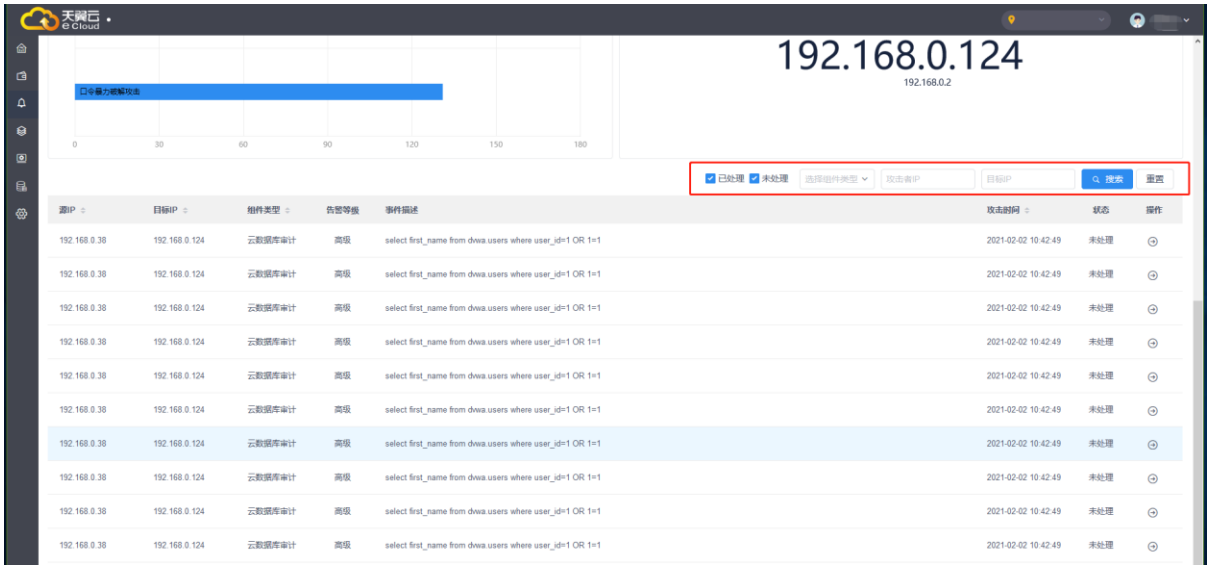
展示源 IP 地址、目的 IP 地址、来源的组件类型、告警等级以及告警产生时间等。



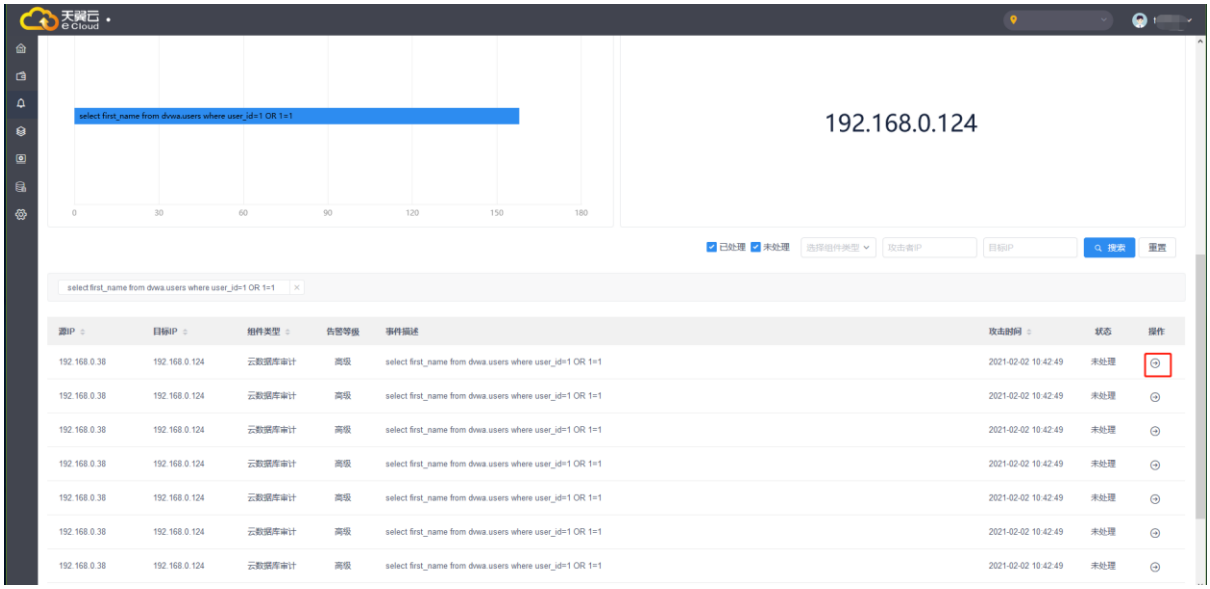
根据条件查询，选择高威胁统计，可出现如下：被攻击目标 IP 地址、产生日志组件类型、告警等级、告警事件描述、被攻击具体时间、处理状态等设置；



可根据已处理或者未处理方式，选择组件类型，填写“攻击者 IP”和“目标 IP”进行数据筛选



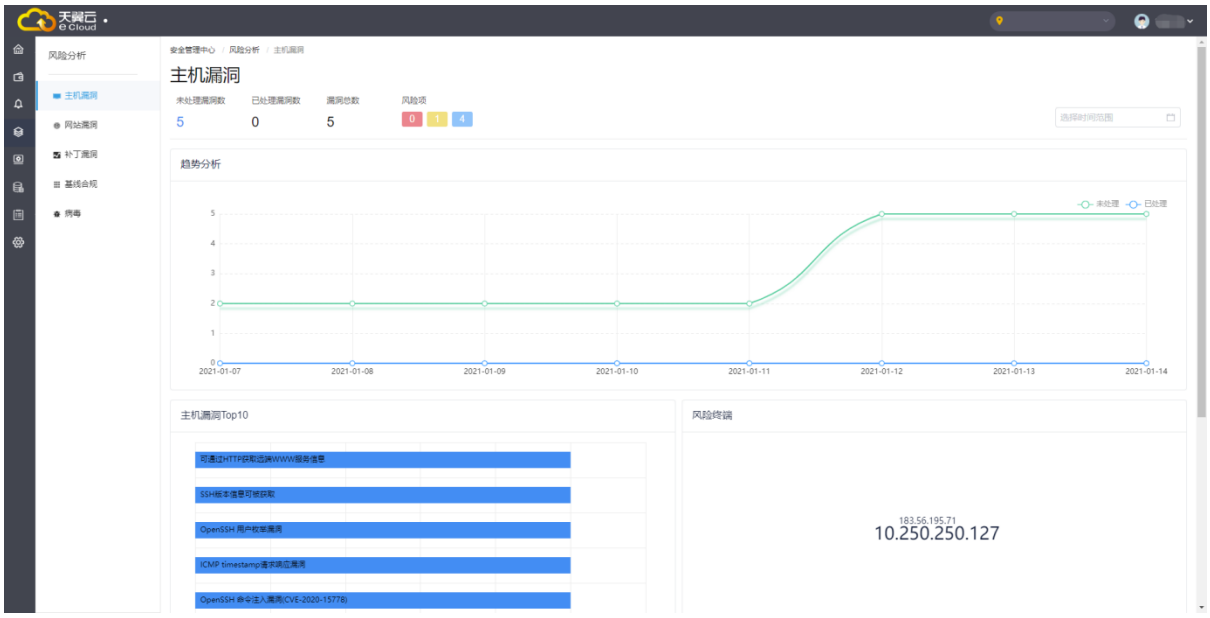
告警处理操作：查看未处理状态，点击『去处理』。



即可跳转到相应组件管理页面进行处理。

4.4. 风险分析

风险分析展示了漏洞分析数据、风险趋势等界面，通过多维度对资产进行系统分析及分组展示，其中包括主机漏洞、网站漏洞、补丁漏洞、基线合规及病毒查杀。实时展示主机漏洞 Top10 数据，具体定位风险终端地址，详细展示漏洞信息。



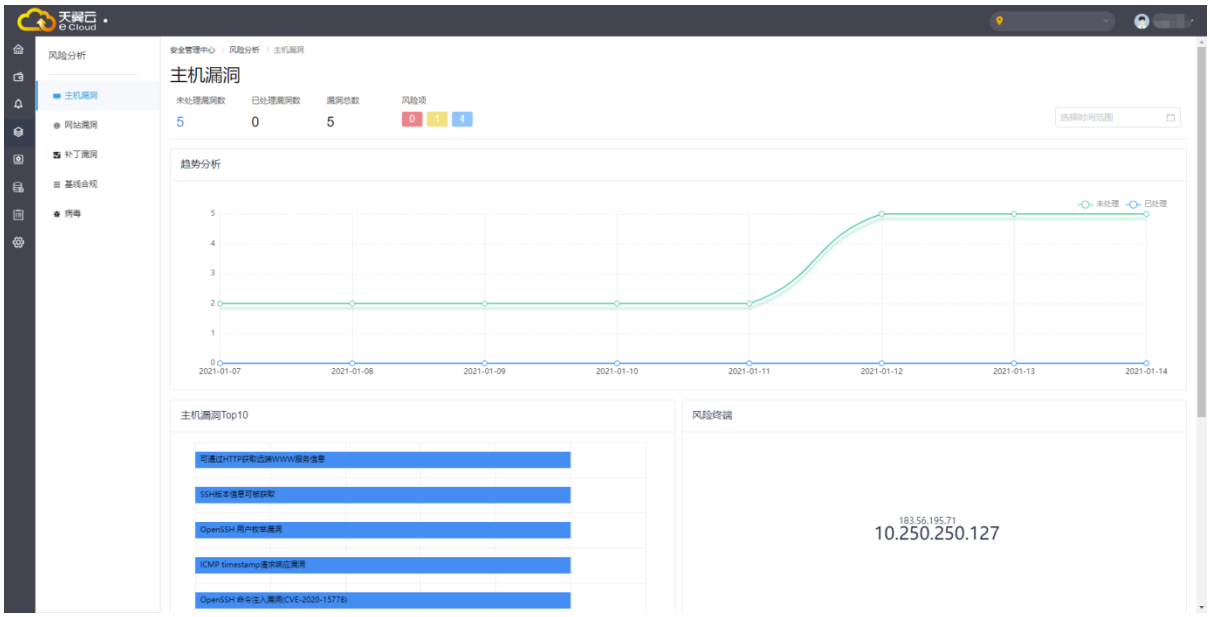
4.4.1 主机漏洞

主机漏洞扫描主要包含对应用服务、网络设备、安全设备等相关主机设备的漏扫扫描以及对应主机安全的相关服务和操作系统的漏洞进行扫描。

漏洞数据来源：『资产管理』→『服务器』中，点击『扫描』，将漏洞数据同步到【主机

漏洞】模块

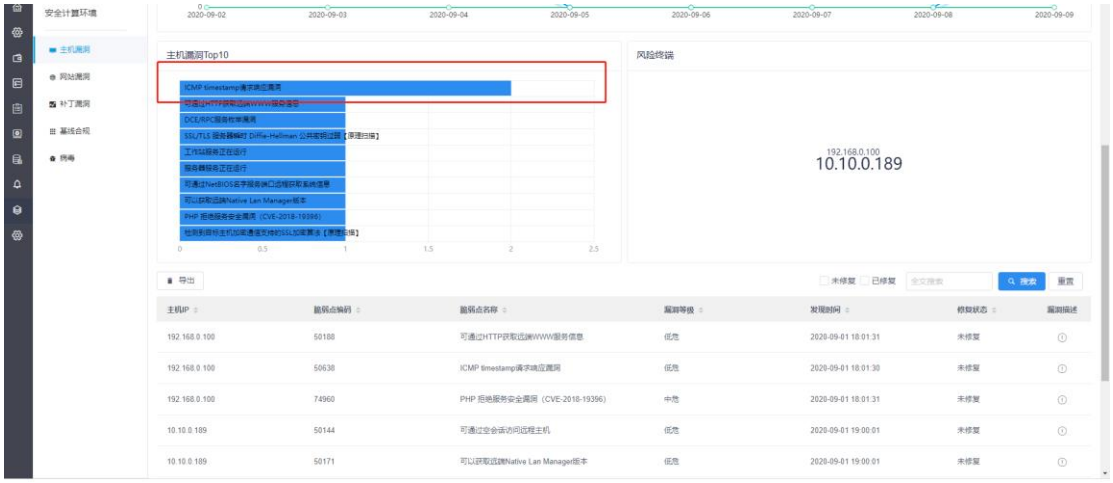
趋势分析图默认展示当前一周的数据，通过右上角可筛选不同的时间段查看趋势图



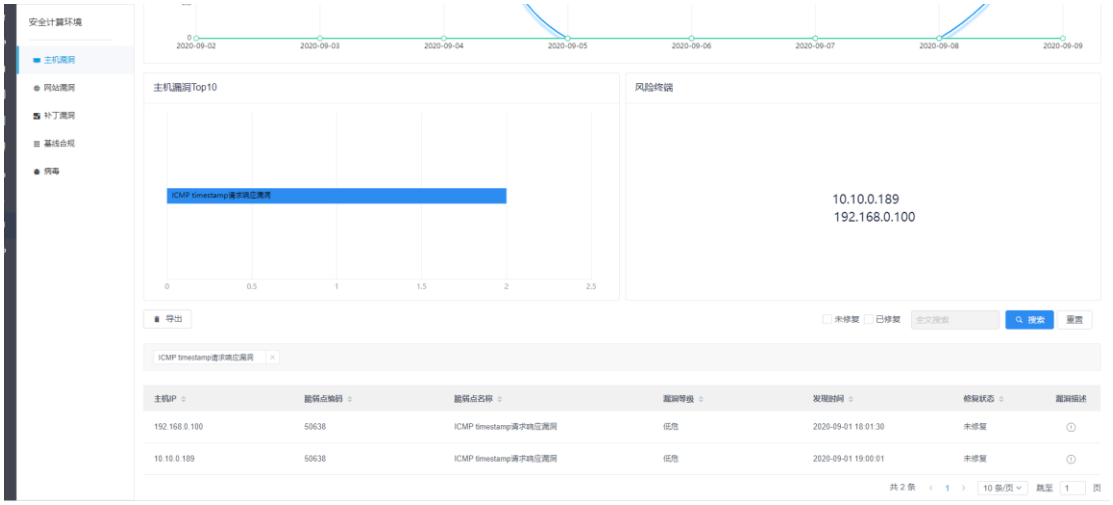
安全管理中心记录漏洞状态、漏洞所存在风险值，对时间段内所存在漏洞进行趋势分析

点击『未处理漏洞数量』或者『风险项』（风险项颜色标注高、中、低风险）

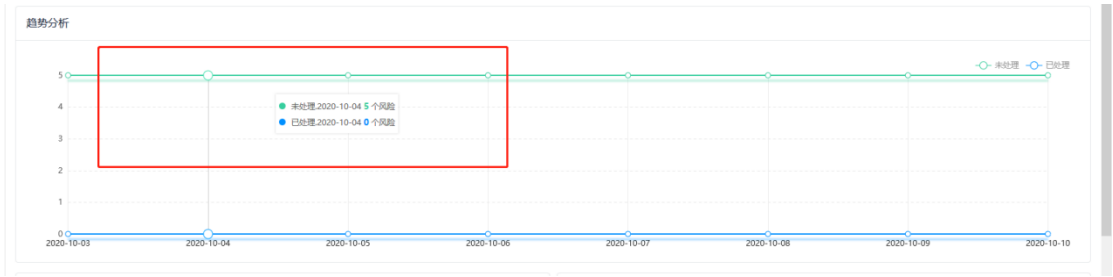
点击柱状图可筛选出相应的数据



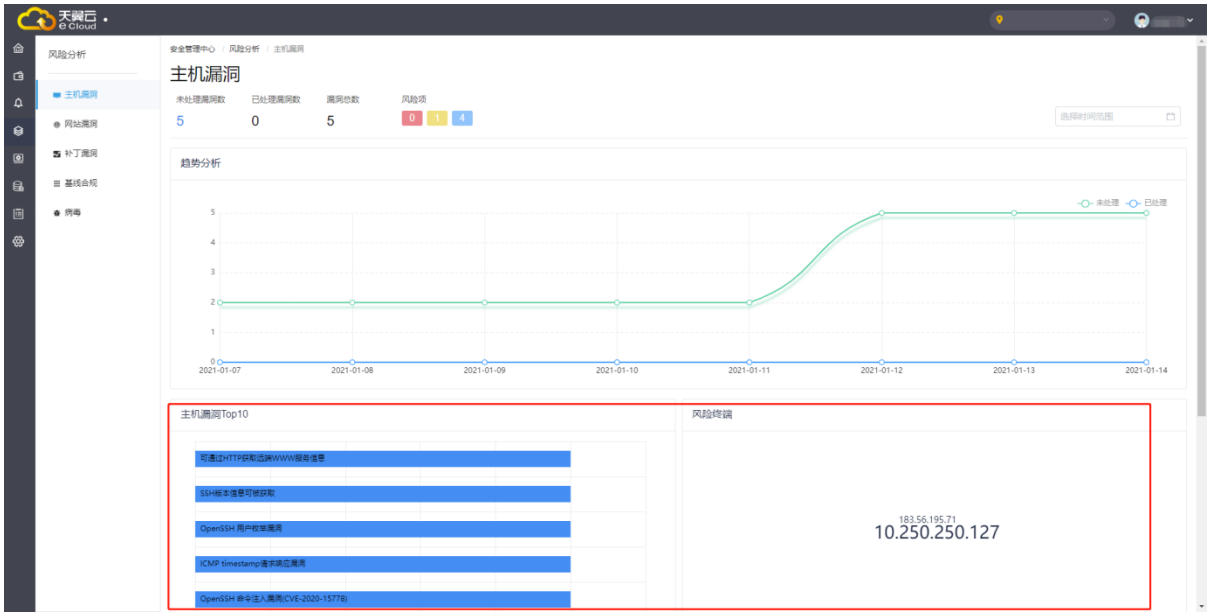
筛选出相应结果



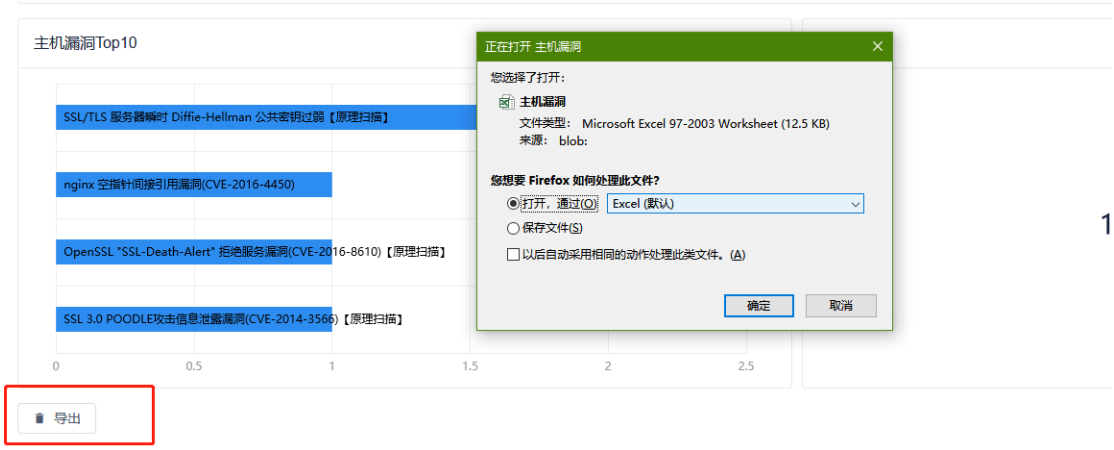
鼠标移至『趋势分析』中的曲线上，即可查看已处理漏洞、未处理漏洞、产生时间和处理时间。



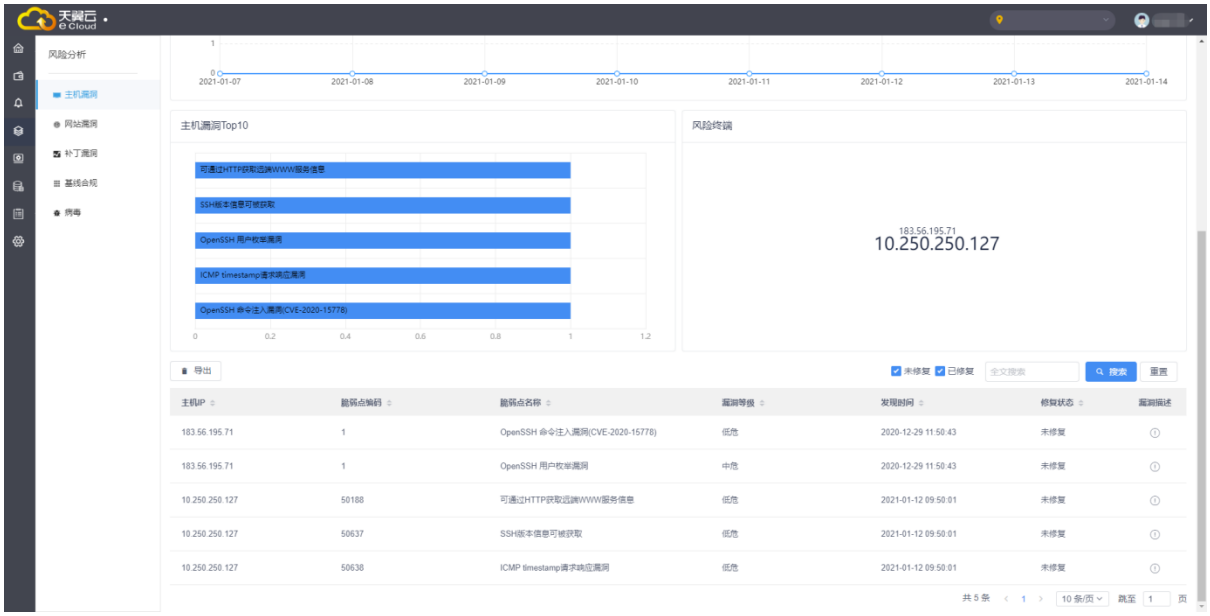
点击『主机漏洞 Top10』，查看详细漏洞分析、漏洞产生原因。



选择导出漏洞信息文件，确定保存即可。



对于某一个特定的风险终端进行精准定位，展示主机漏洞产生原因并记录扫描方案。

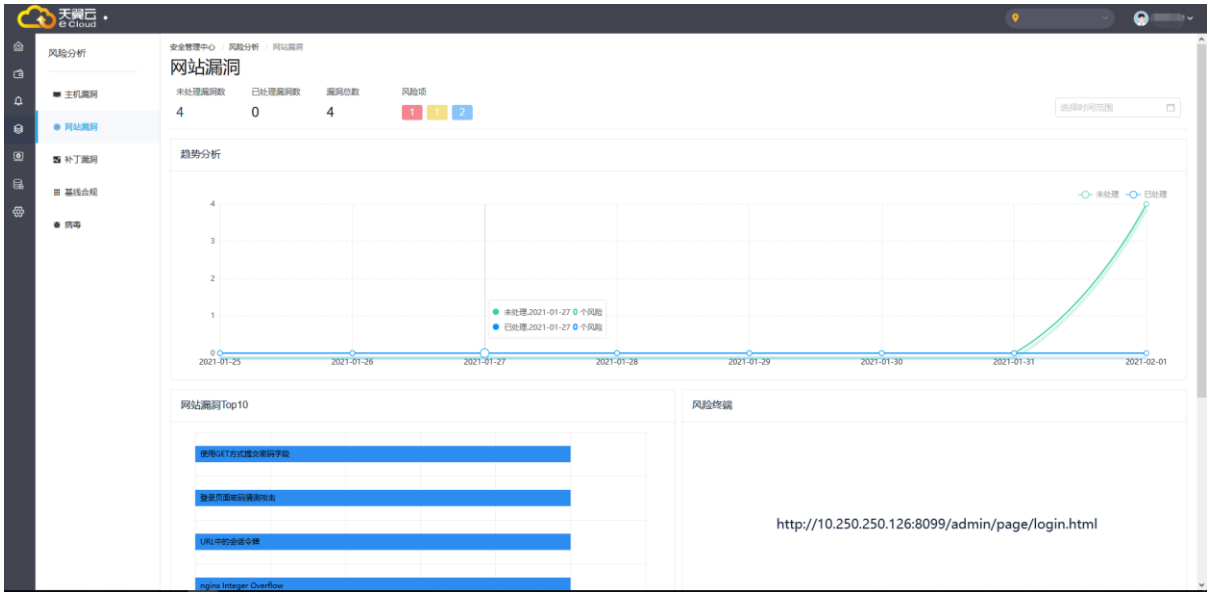


点击漏洞描述下的查看设置，展示风险的具体描述及其解决方案。

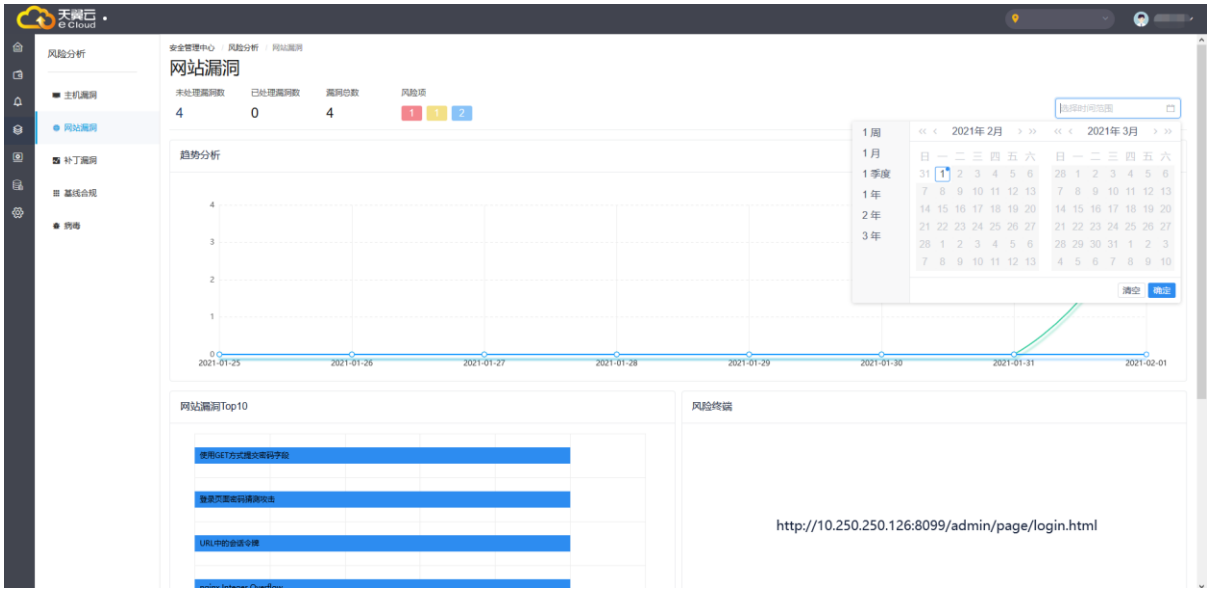
4.4.2 网站漏洞

网站漏洞扫描主要是针对 WEB 应用的 SQL 注入、跨站、远程挂马、跨站请求伪造 CSRF、OWASP top 10 等漏洞进行扫描进行网站漏洞扫描，实时将数据反馈到安全专区，进行动态展示。

网站漏洞数据来源：点击『资产管理』→『域名』，扫描后，如果该网站有漏洞则会同步到【网站漏洞】模块



选择时间范围内，进行趋势分析。

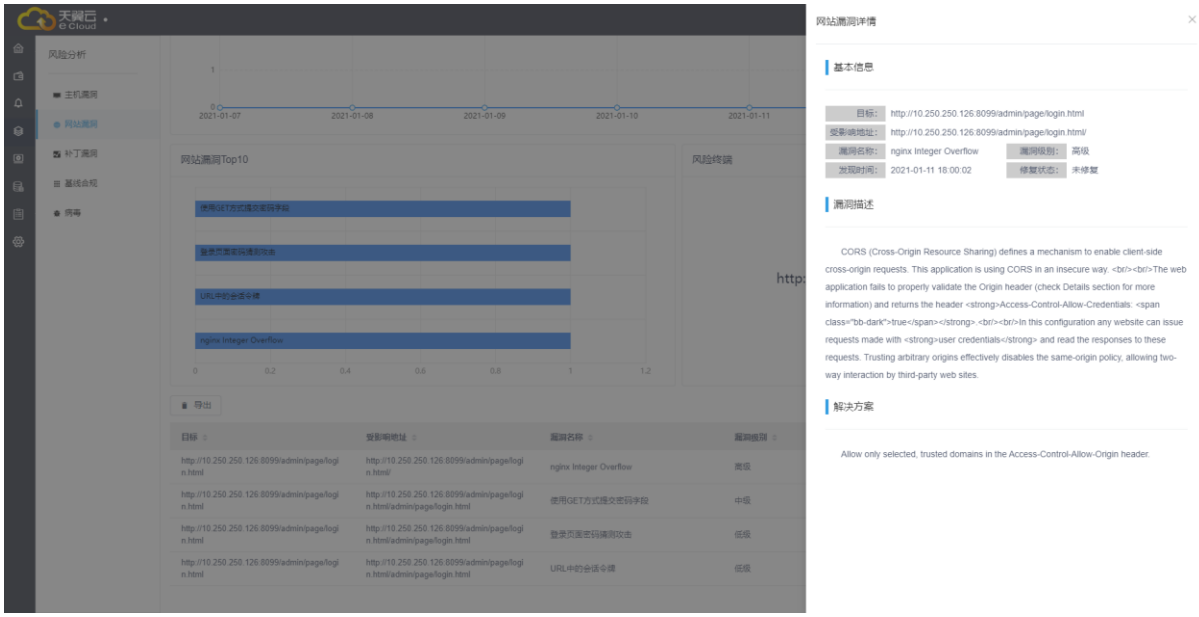


风险终端：

可以实时分析、日志追溯等方式进行数据查找和分析，记录站点来源信息以及网站网页信息类型，记录网站漏洞名称、漏洞等级、漏洞发现时间、漏洞处理状态及漏洞具体描述。

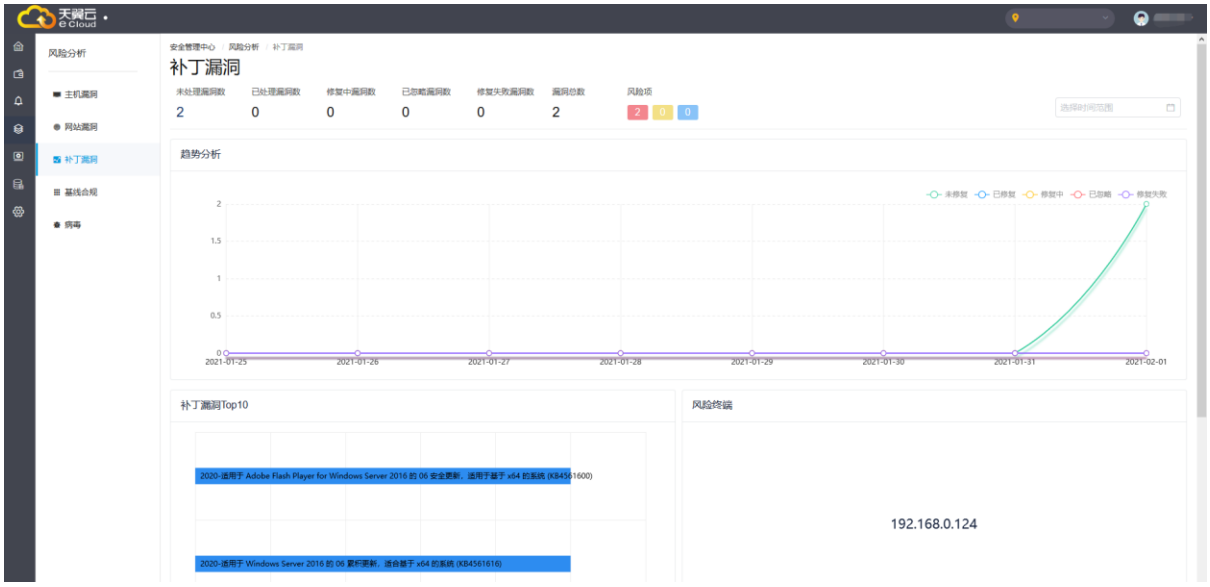
点击『导出』，即下载网站漏洞扫描报告。

点击『漏洞描述』即展示网站漏洞具体域名地址、网站漏洞详情

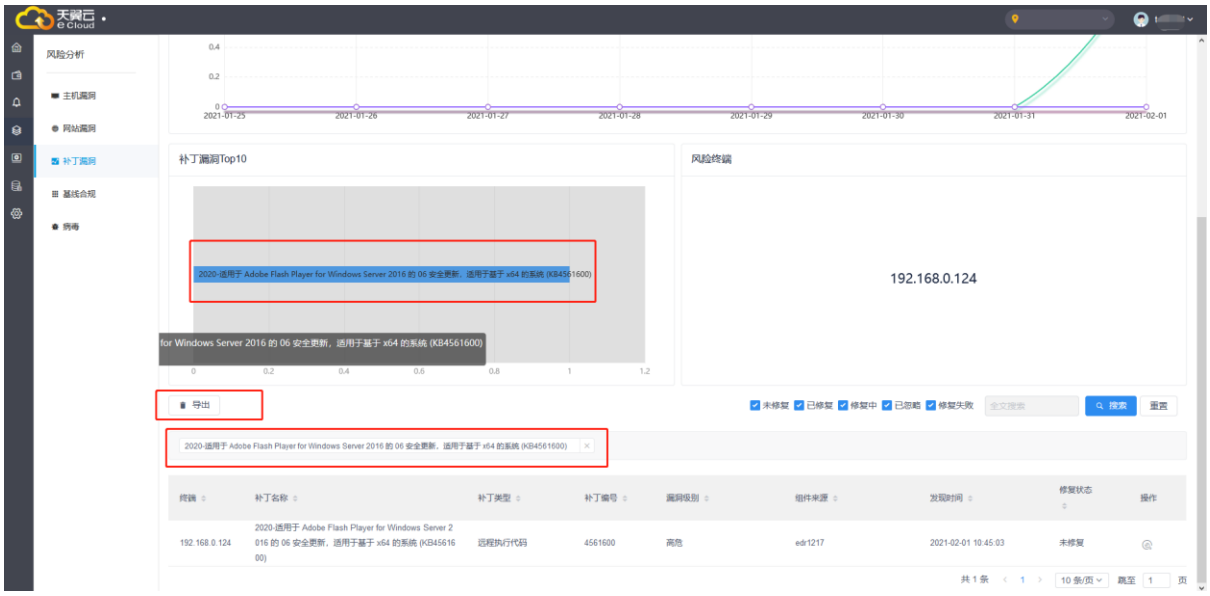


4.4.3 补丁漏洞

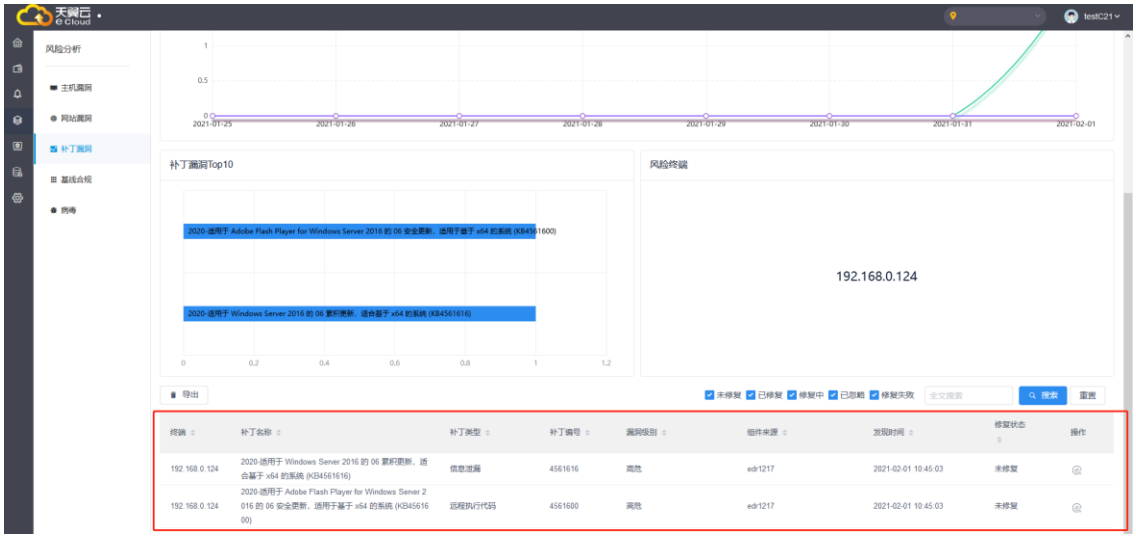
补丁漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。安全专区整合外部漏洞扫描服务，实时返回补丁漏洞扫描数据。



点击『补丁漏洞』中的一项漏洞，进行单项查询以及漏洞详细展现，导出扫描出来的补丁漏洞文件。



记录该数据返回（即风险终端），分析补丁漏洞所产生原因。

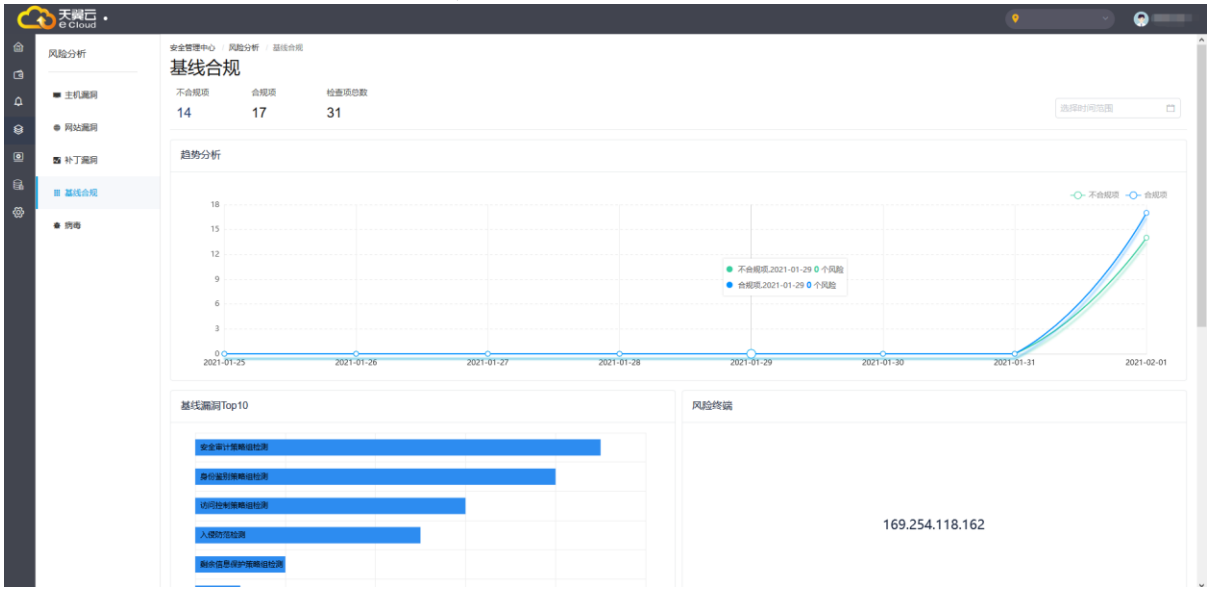


选择修复补丁漏洞，点击右侧『操作』，页面跳转组件系统进行管理。

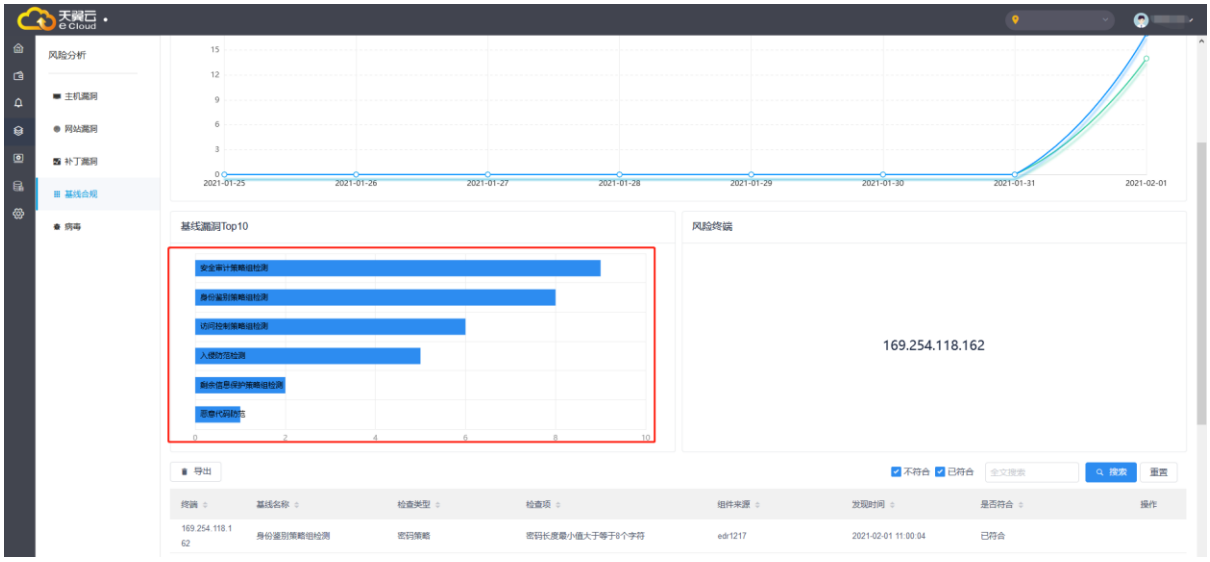
4.4.4 基线合规

基线核查主要是针对主机的操作系统、数据库、虚拟化设备、软件基础、应用程序的配置合规性进行检查，并提供检测结果说明和加固建议。

基线检查功能进行系统安全加固，降低入侵风险并满足安全合规要求。



展示基线漏洞详细信息以及漏洞发生 IP 地址



记录基线合规相关风险信息，其中包括终端 IP 地址、基线名称、基线检查类型、发现时间及是否修改符合。

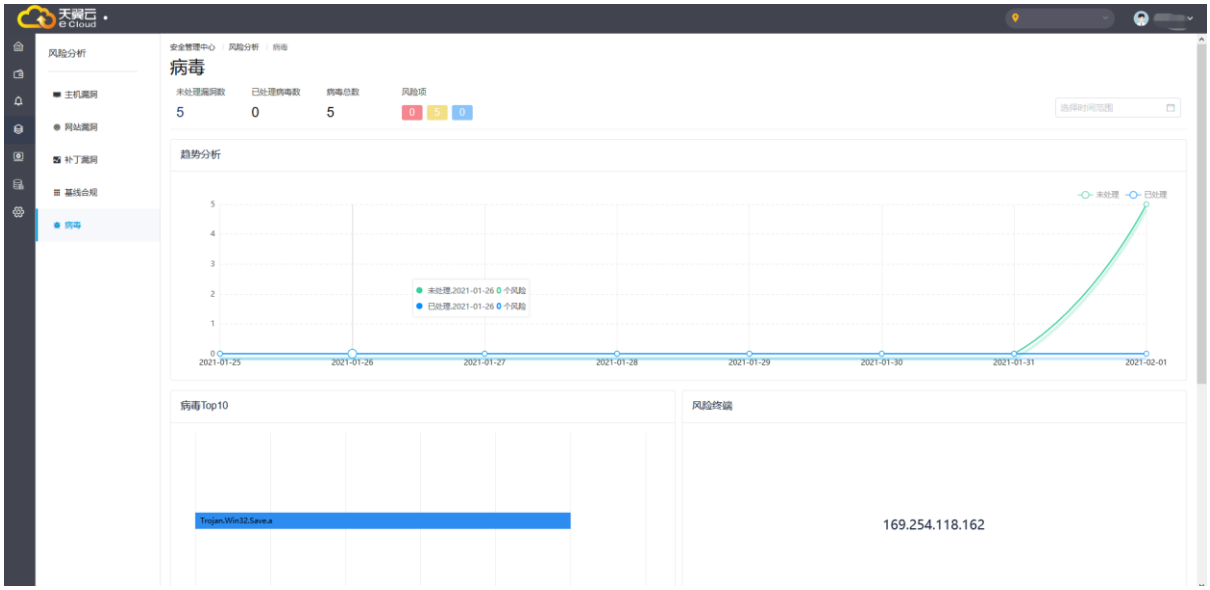
终端	基线名称	检查类型	检查项	发现时间	是否符合	操作
192.168.0.124	身份鉴别策略组检测	密码策略	密码长度最小值大于等于8个字符	2021-01-07 12:20:01	已符合	
192.168.0.124	身份鉴别策略组检测	密码策略	密码最短使用期限大于等于2天	2021-01-07 12:20:01	不符合	
192.168.0.124	身份鉴别策略组检测	密码策略	密码最长使用期限小于等于90天	2021-01-07 12:20:01	不符合	
192.168.0.124	身份鉴别策略组检测	密码策略	保留密码历史数量大于等于5个	2021-01-07 12:20:01	不符合	
192.168.0.124	身份鉴别策略组检测	账户策略	复位账户锁定计数器大于等于15分钟	2021-01-07 12:20:01	已符合	
192.168.0.124	身份鉴别策略组检测	账户策略	账户锁定时间大于等于15分钟	2021-01-07 12:20:01	已符合	
192.168.0.124	身份鉴别策略组检测	账户策略	账户锁定阈值小于等于10次	2021-01-07 12:20:01	不符合	
192.168.0.124	身份鉴别策略组检测	自动登录	自动登录账户	2021-01-07 12:20:01	已符合	
192.168.0.124	访问控制策略组检测	账户检测	空密码账户	2021-01-07 12:20:01	已符合	
192.168.0.124	访问控制策略组检测	账户检测	弱密码账户	2021-01-07 12:20:01	已符合	

共 31 条 1 2 3 4 10 条/页 跳至 1 页

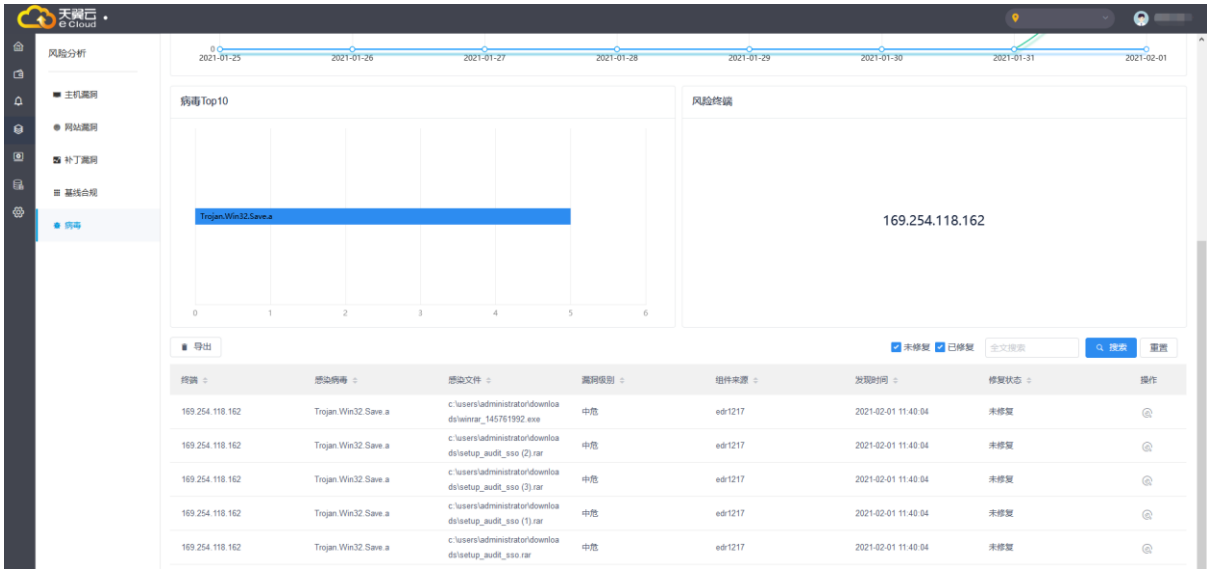
4.4.5 病毒检测

针对病毒处理，安全专区自动检测主流木马病毒、勒索软件、挖矿病毒、DDoS 木马并自动隔离查杀，通过提供扫描、告警、深度查杀及病毒修复能力，可有效预防病毒入侵服务器。

趋势分析图默认展示当前一周的数据，通过右上角可筛选不同的时间段查看趋势图

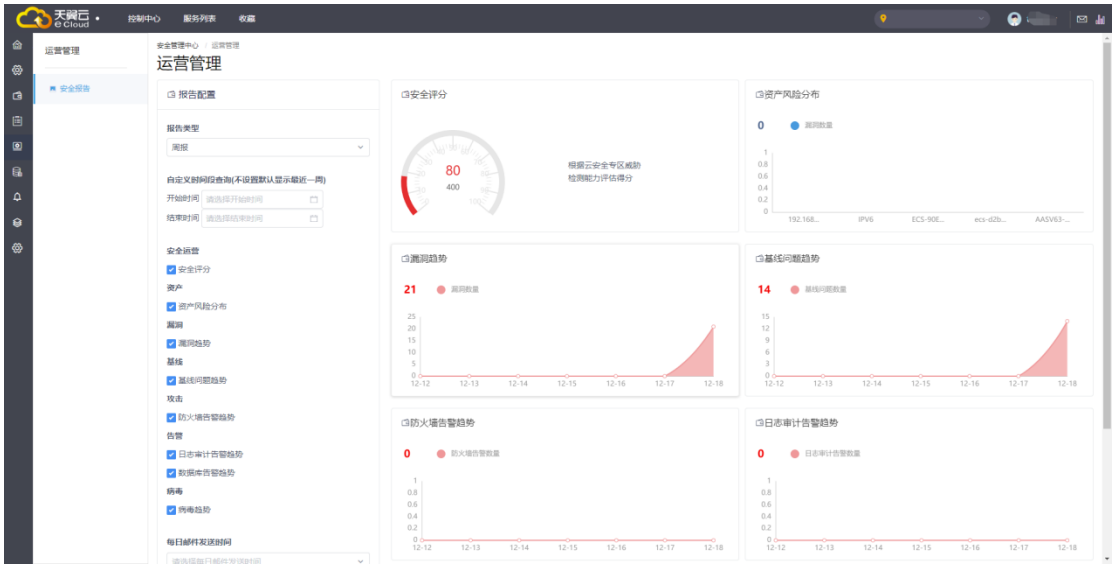


展示病毒漏洞详细信息以及漏洞发生 IP 地址



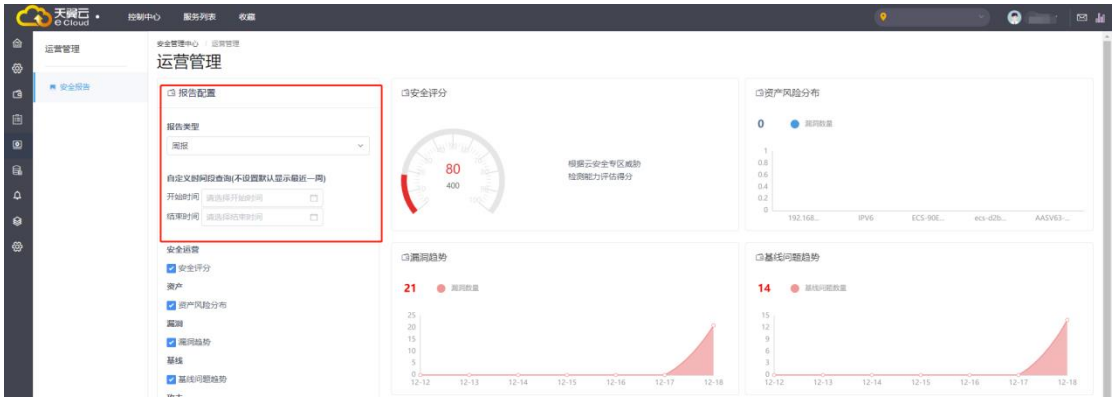
4.5 运营管理

安全专区支持安全报告功能，支持对安全报告进行自定义配置。通过自定义报告内容、报告展示的数据类型和接收人邮箱地址，满足告警资产安全状况数据的需求。



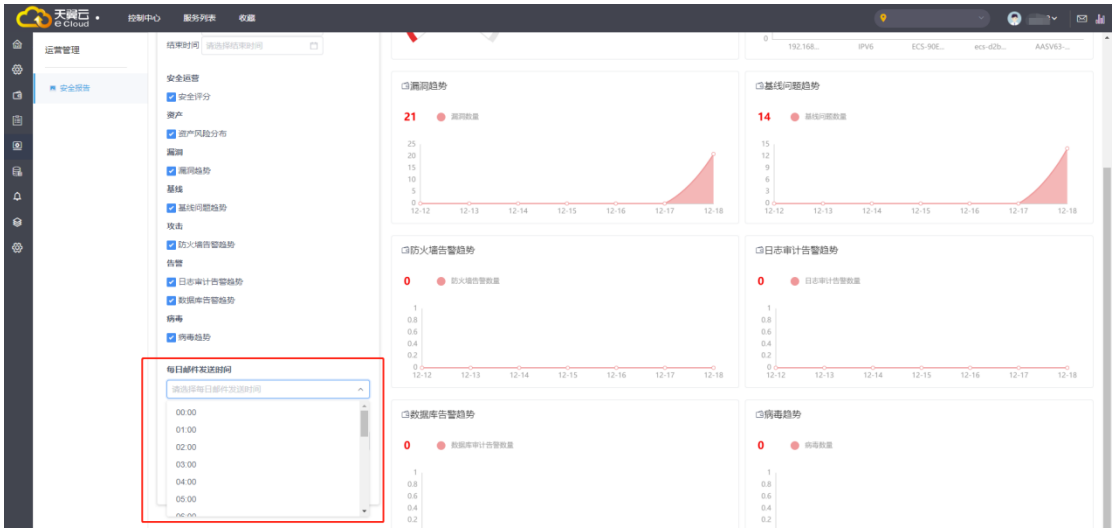
运营管理支持报告类型分不同种类，例如周报、月报、季报、年报。存在自定义时间段查询，根据开始时间和结束时间进行查询并对安全运营模块进行实时监控和检查，该功能模块支持邮件定期发送及指定特定接收人。

自定义时间查询报告，默认展示一周的漏洞趋势数据，可选择时间段，选择开始时间和结束时间进行查询。



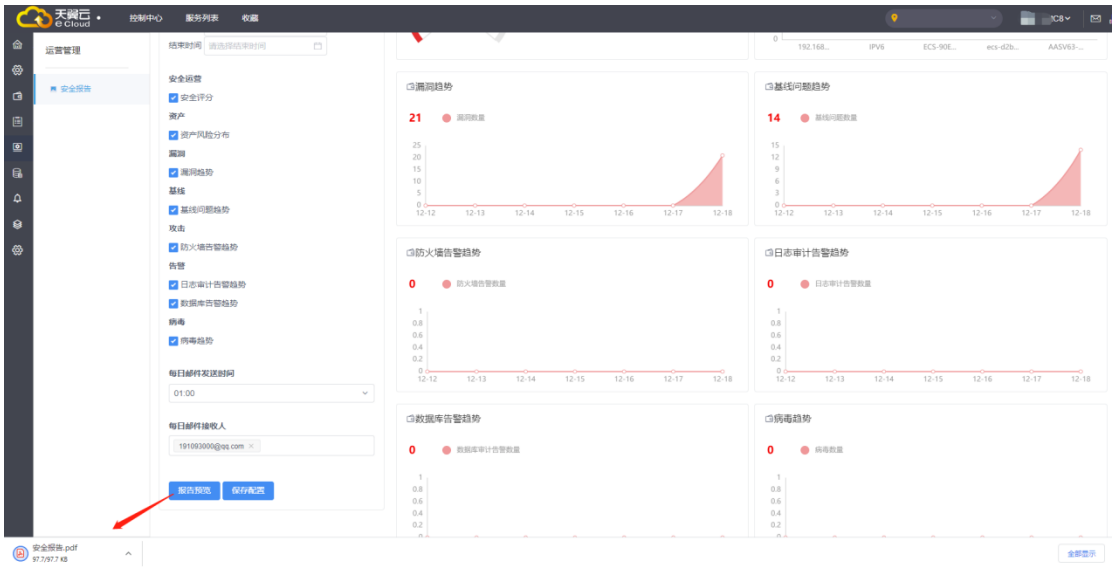
对于查询，可点击“安全运营”，点击所查询事项，将可在右侧展示栏获取相关信息。

确定每日邮件发送时间，设置为定时任务，确定好每日邮件接收人，提交『保存配置』即可完成。（系统则按该时间每天进行发送）



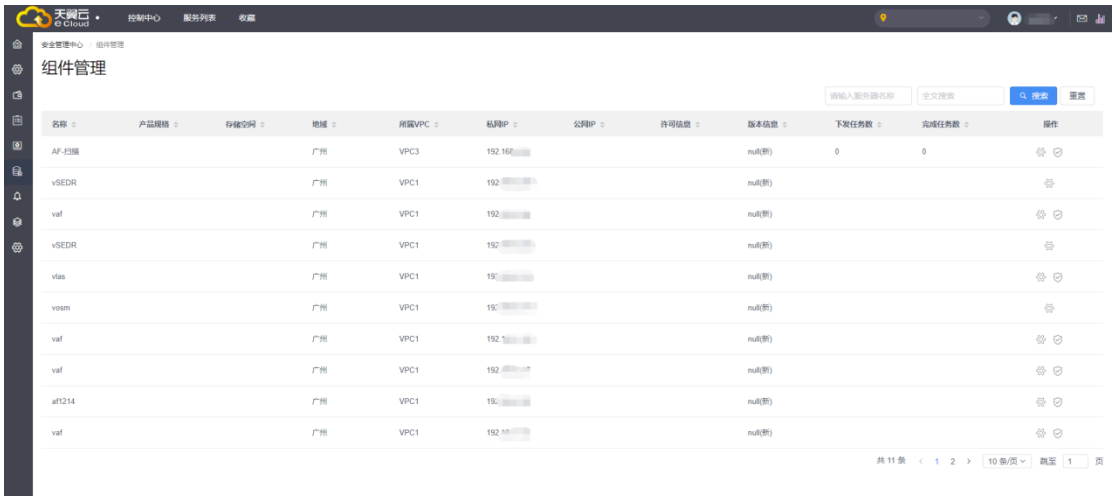
在每日邮件接收人编辑框，输入要接收的邮箱后确认添加，点击『保存配置』按钮

点击『报告预览』按钮，系统会下载一份 pdf 格式的安全报告



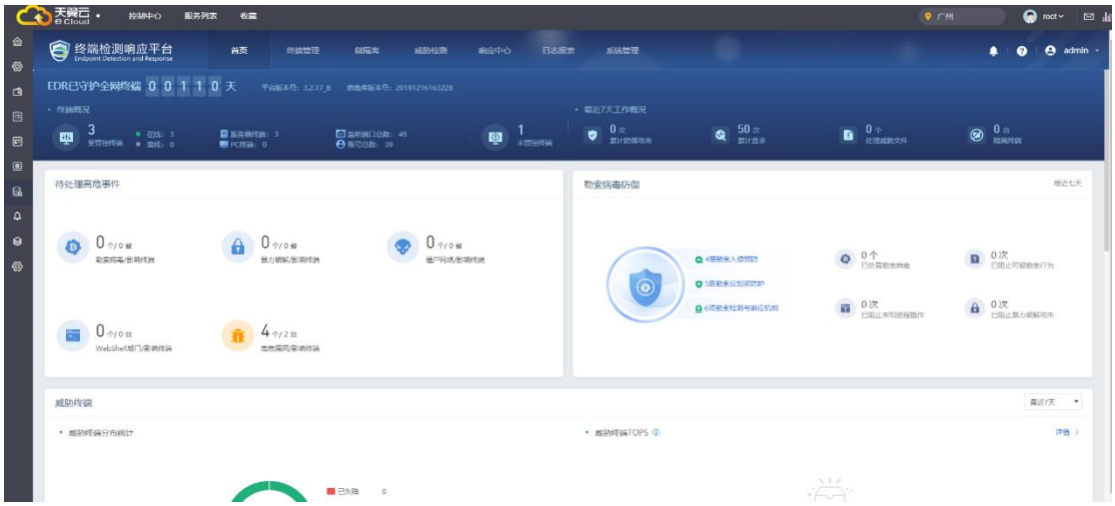
4.6 组件管理

组件管理作为安全专区的核心区域，展示云防火墙、云日志审计、云堡垒机、终端安全 EDR、云数据库审计等组件产品的状态信息，作为安全专区组件的入口，满足单点登录、统一管理的功能。



组件管理提供详细的安全组件信息，包括安全产品的产品规格、可存储空间、所属地域、所属 VPC 组、许可信息时间、版本信息及在线状态。

点击『操作』下的设置，即自动进入云日志审计 web 管理界面。



如果需要选择恢复组件管理的配置，可选择点击『操作』→『配置恢复』，点击配置恢复按钮（只有终端安全 EDR、云防火墙、云数据库审计才有恢复功能），显示组件的备份记录，选择所需恢复状态。

点击『恢复』，确定提交即可，则可成功恢复到备份时状态。

4.7 系统管理

4.7.1 角色权限说明

根据等级保护 2.0 要求，对系统管理员、审计管理员和安全管理员的管理主体、权限控制和管控过程提出明确要求，同时要求安全管理中心内的管理系统符合“三权分立”权限管理模式。

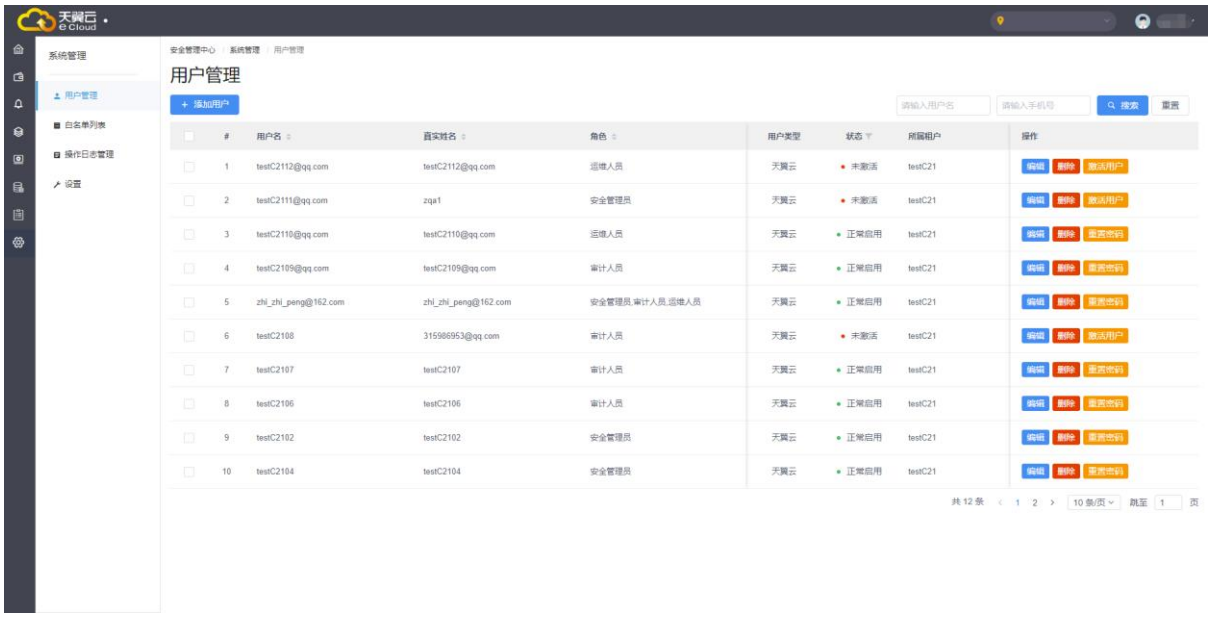
安全管理中心默认以下权限分配：

模块名称/角色名称	租户系统管理员	租户安全管理员	租户运维管理员	租户审计管理员
总览	√	√		√
系统管理				
用户管理	√			
白名单	√			
操作日志管理	√	√		√
资产管理	√	√		√
总览	√	√		√
服务器	√	√		√
域名	√	√		√
运营管理	√	√		√
安全报告	√	√		√
组件管理	√	√		√
安全组件	√	√		√
威胁分析	√	√		√
风险分析	√	√		√
主机漏洞	√	√		√
网站漏洞	√	√		√
补丁漏洞	√	√		√
基线合规	√	√		√
病毒	√	√		√
设置	√			

4.7.2 用户管理

按照角色权限说明，进行管理员权限分配及设置。

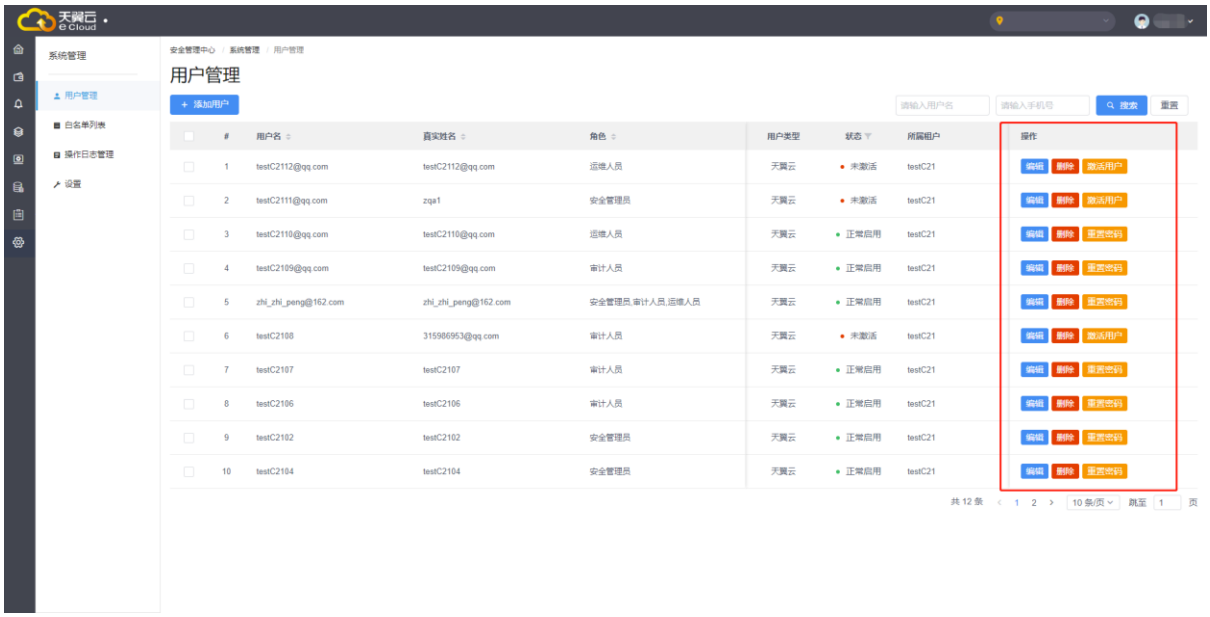
对系统管理员可进行添加、编辑、查询和删除用户信息选项操作。



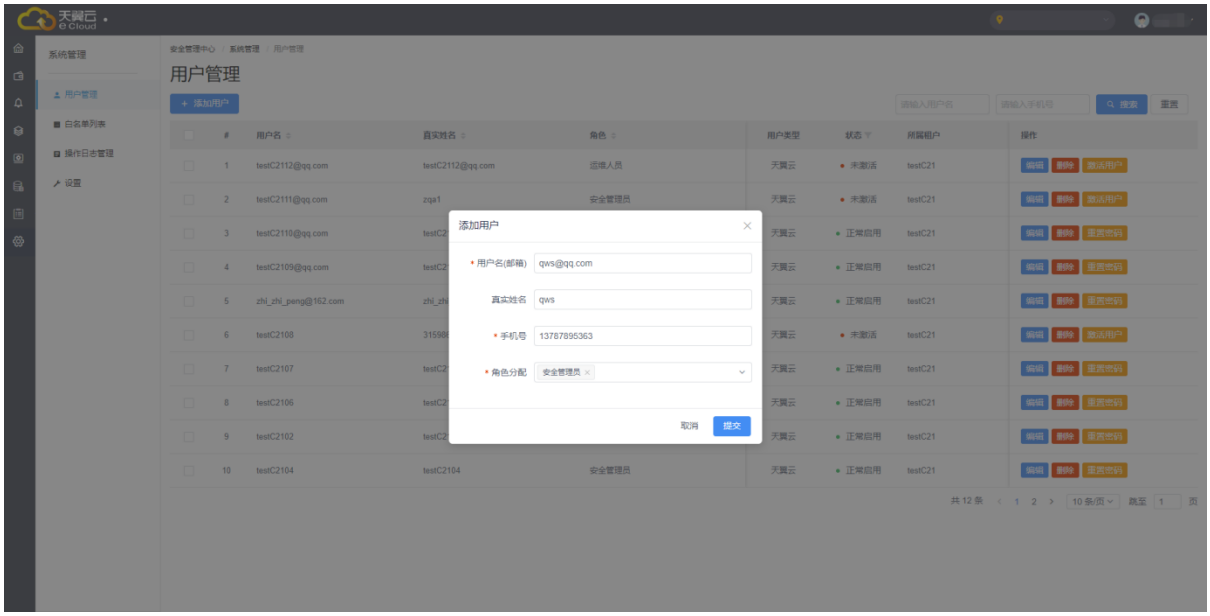
添加用户

管理员：是从天翼云平台同步到安全管理平台的天翼云用户

普通管理员：在安全管理平台【系统管理】-【用户管理】新增的系统用户



点击『添加用户』按钮可创建或者添加用户需填写信息（用户名、真实姓名、密码、邮箱、手机号码、角色分配选择），填写完成、点击『提交』即可添加成功。

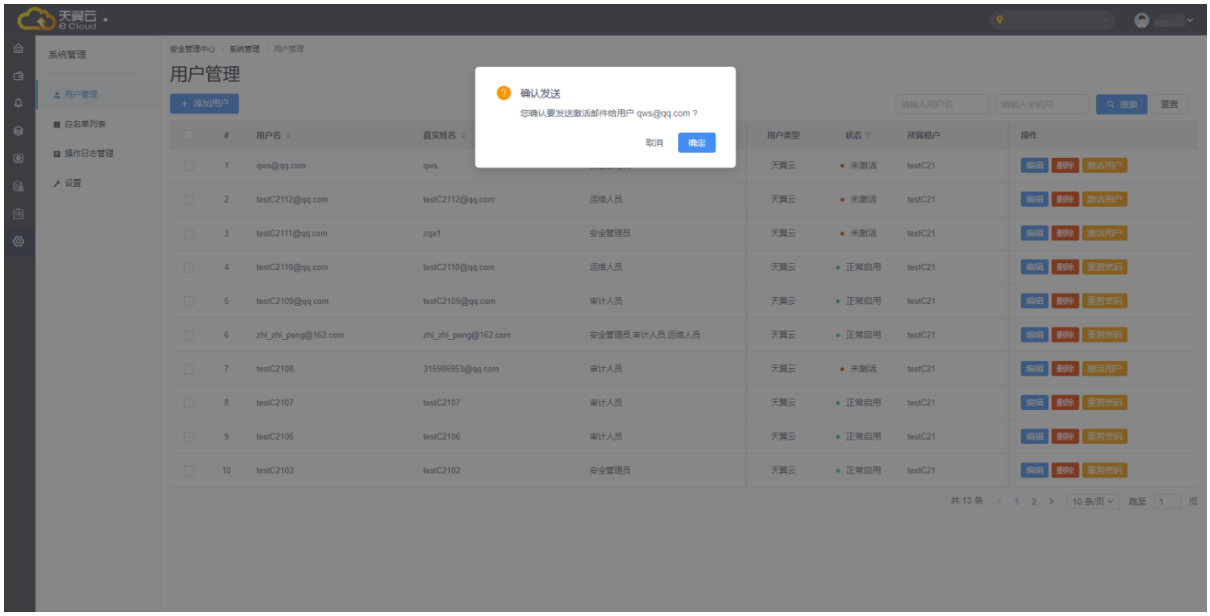


注：[用户名]：填写用户邮箱作为用户名（系统将发送邮件到该邮箱）

[手机号]：填写用户手机号（登录接收验证码）

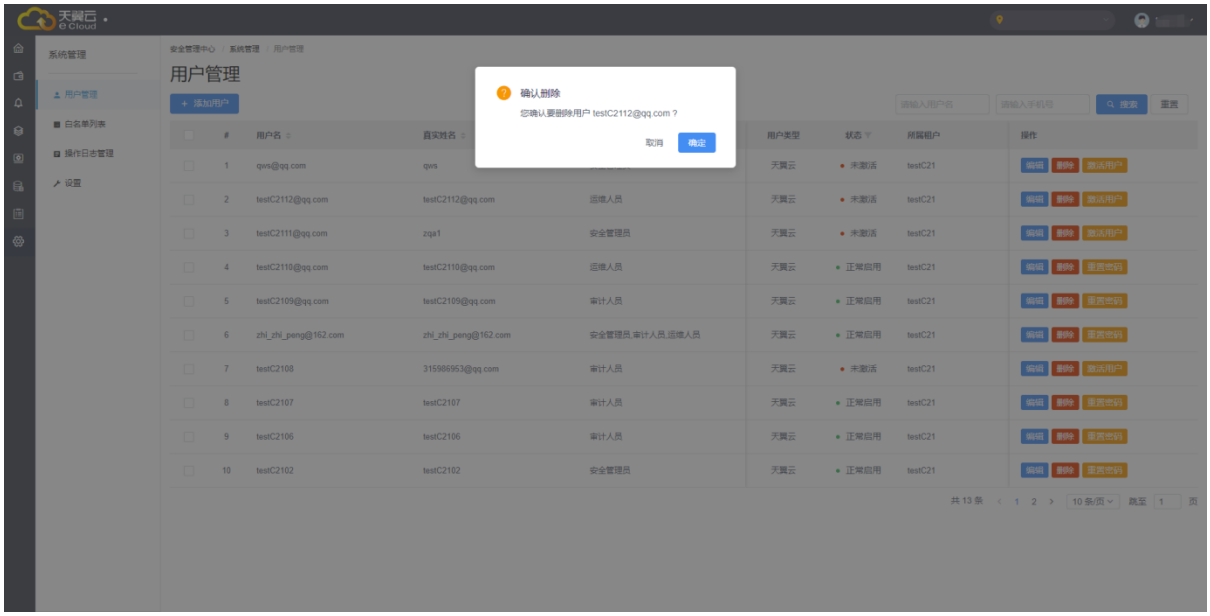
激活用户

点击『激活用户』，发送邮件到用户邮箱，进行激活

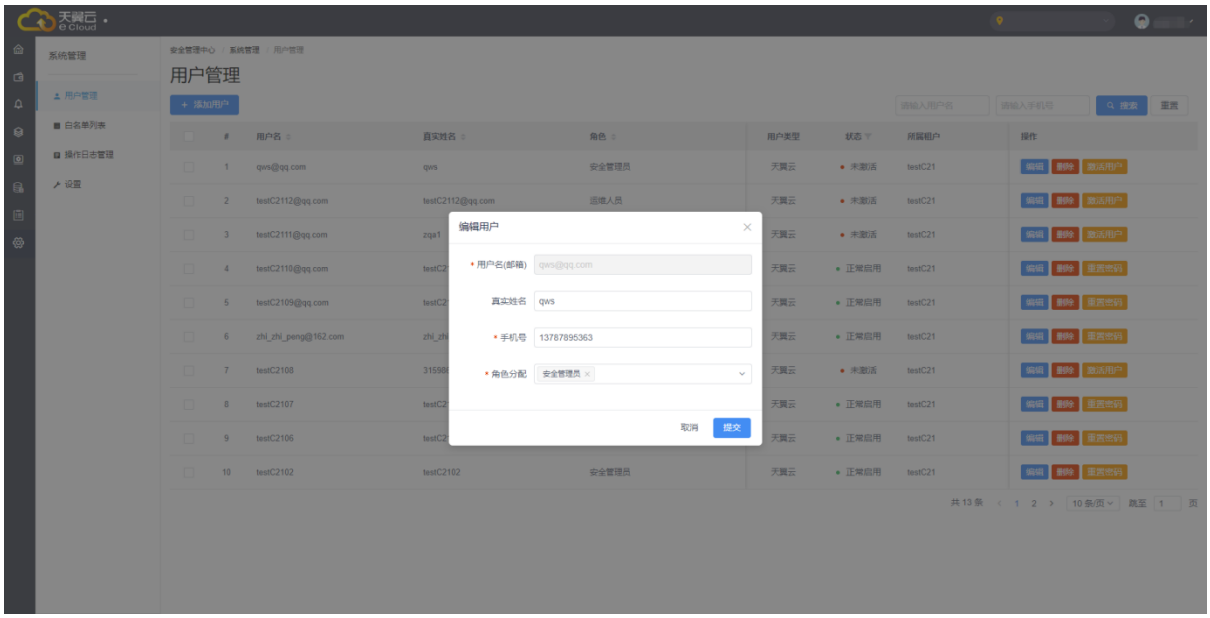


删除用户：

点击『删除』或『批量删除』按钮（只有用户系统类型为“系统”的用户登录系统，才有该按钮权限），删除用户；点击『确认』，即可删除用户



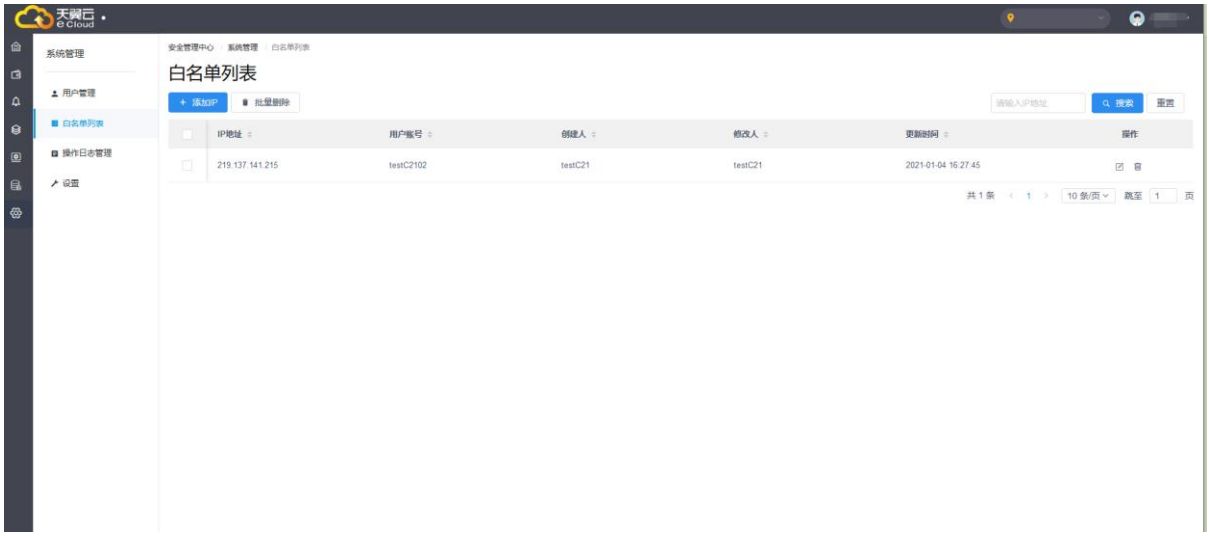
选择要进行编辑的用户，点击『编辑』，即可更改用户的相关信息，修改提交即显示操作成功。



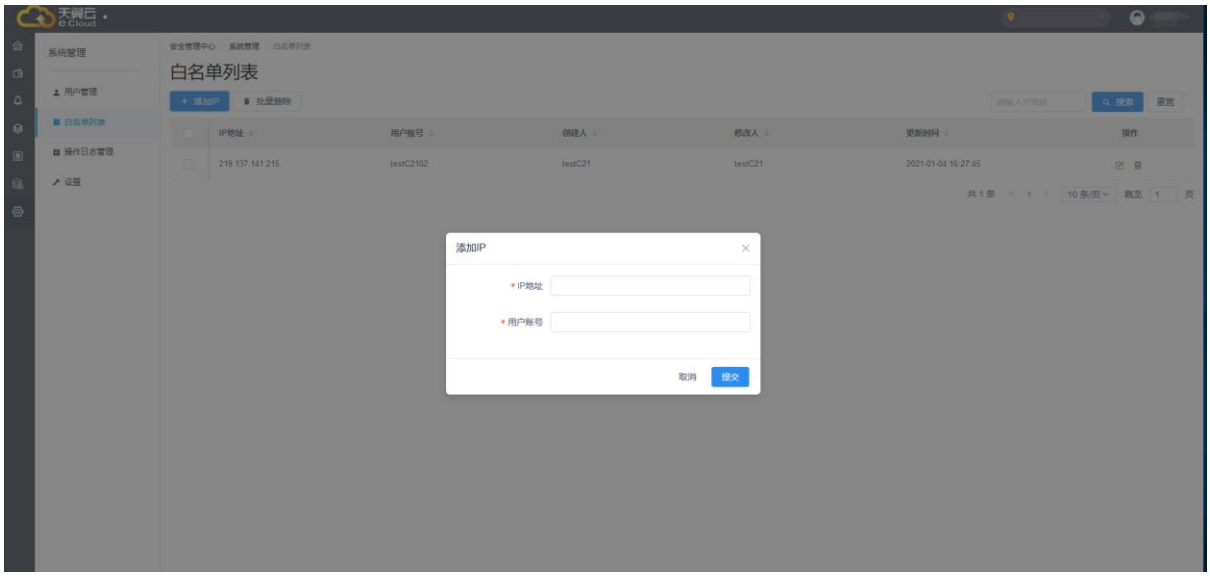
4.7.3 登录控制

安全管理中心将自动检测系统中是否存在可疑或恶意登录，对未出现在白名单中的用户登录进程进行拦截提示。

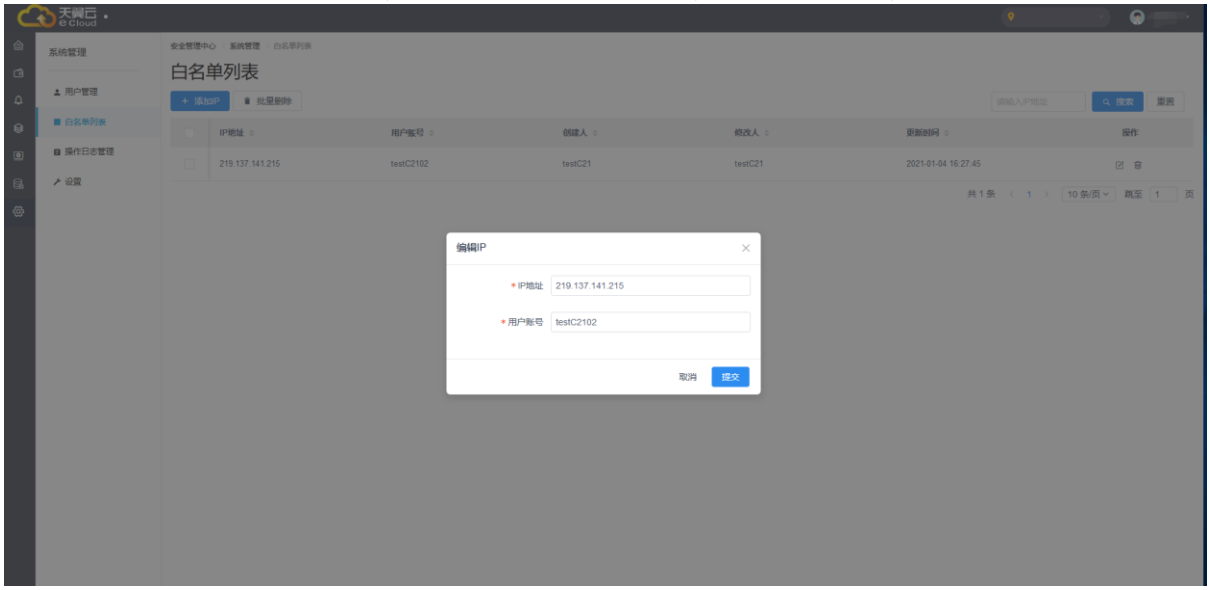
点击『系统管理』→『白名单列表』，创建白名单策略后，选择在需要重点防御的服务器中应用该策略。



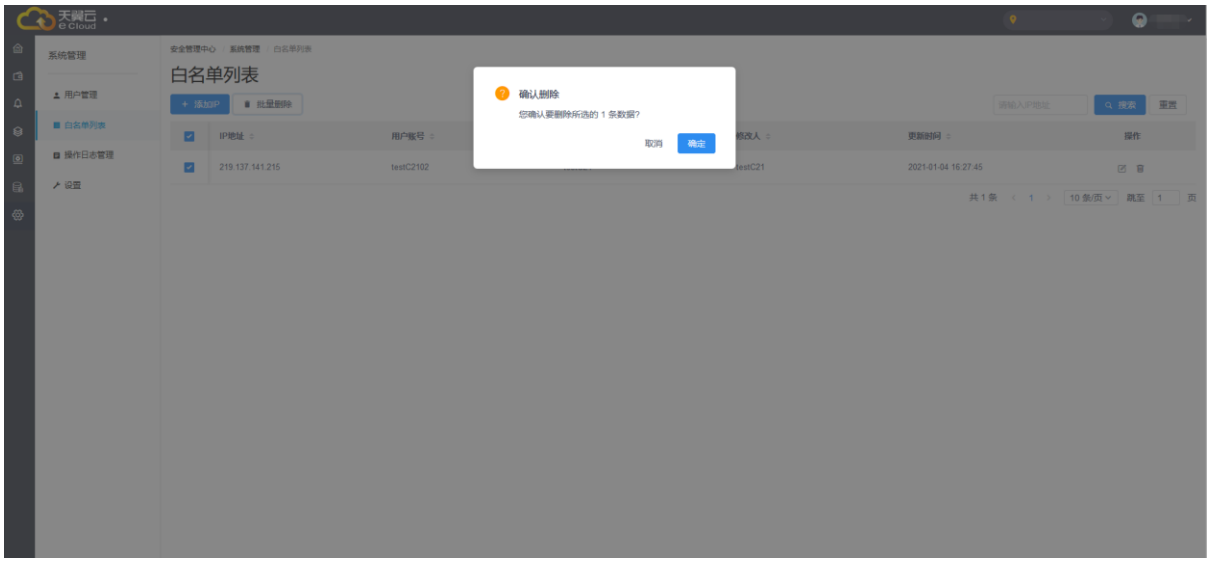
点击『白名单列表』→『添加 IP』，在弹出的编辑框中填上 IP 地址、用户账号，确认提交，自动同步加载更新时间。



可点击右侧『操作』→『编辑』，对白名单用户进行编辑，更改账号信息，同步更新时间。

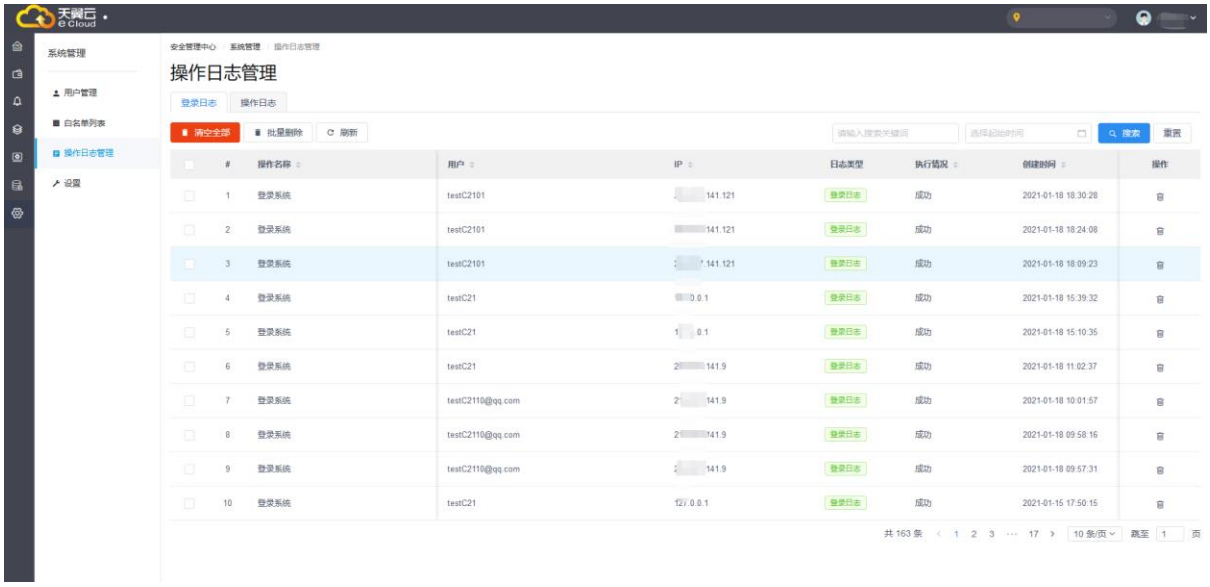


可选择『批量删除』，对白名单进行管理，点击『确定』即可删除（删除后该账号不被 IP 地址所限制）

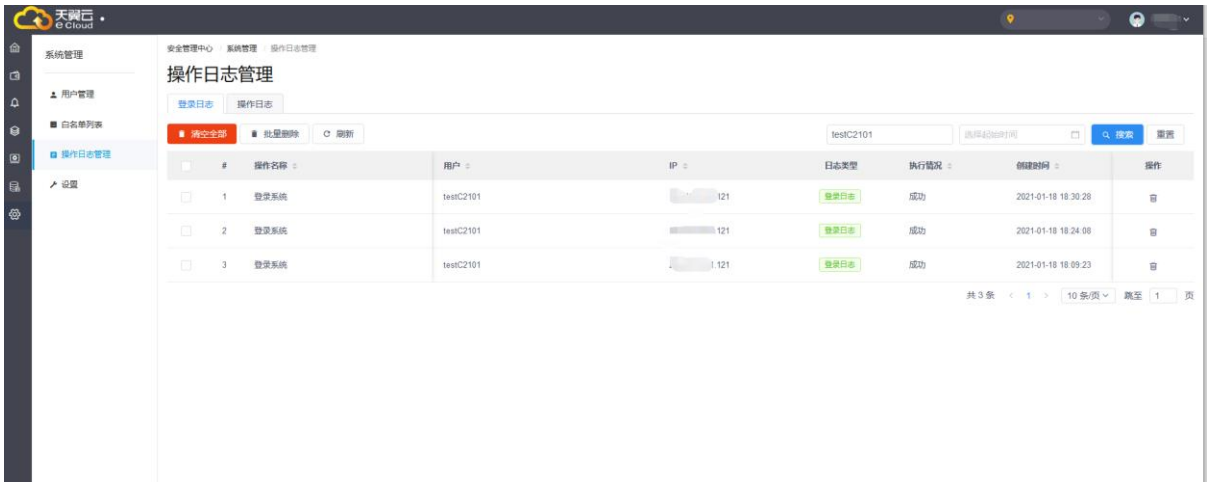


4.7.4 操作记录

对于日志的操作管理，分为登录日志和操作日志两个方面，操作日志记录具有追根溯源的功能，其记录用户在安全专区的执行操作。



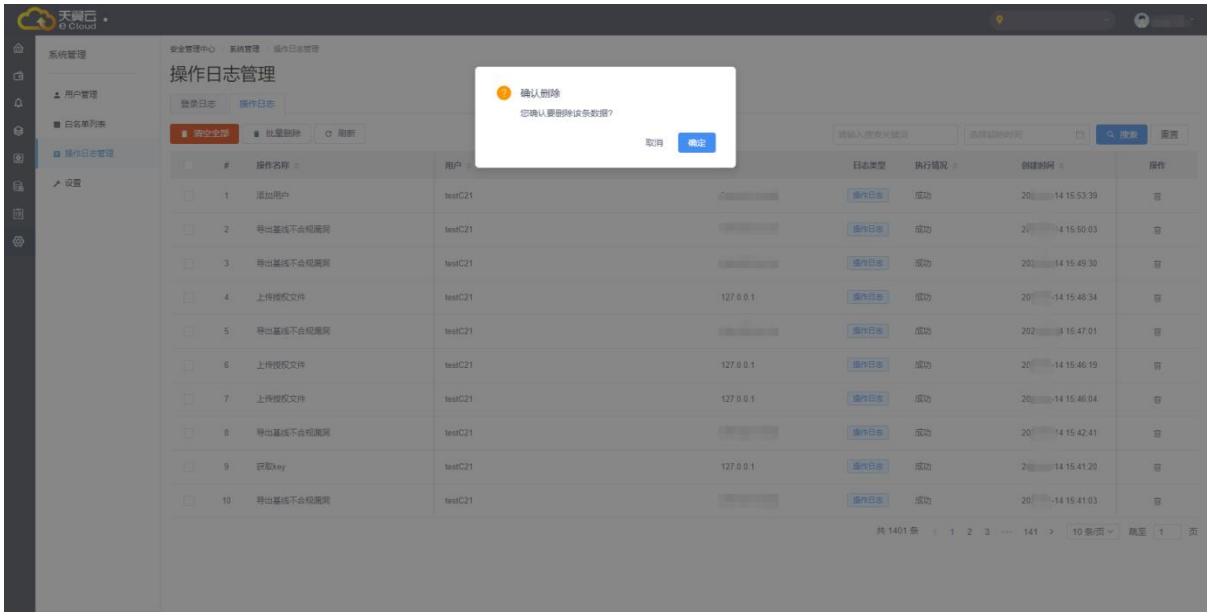
搜索功能：可采用关键词搜索、日志起始时间设置，进行筛选和查询



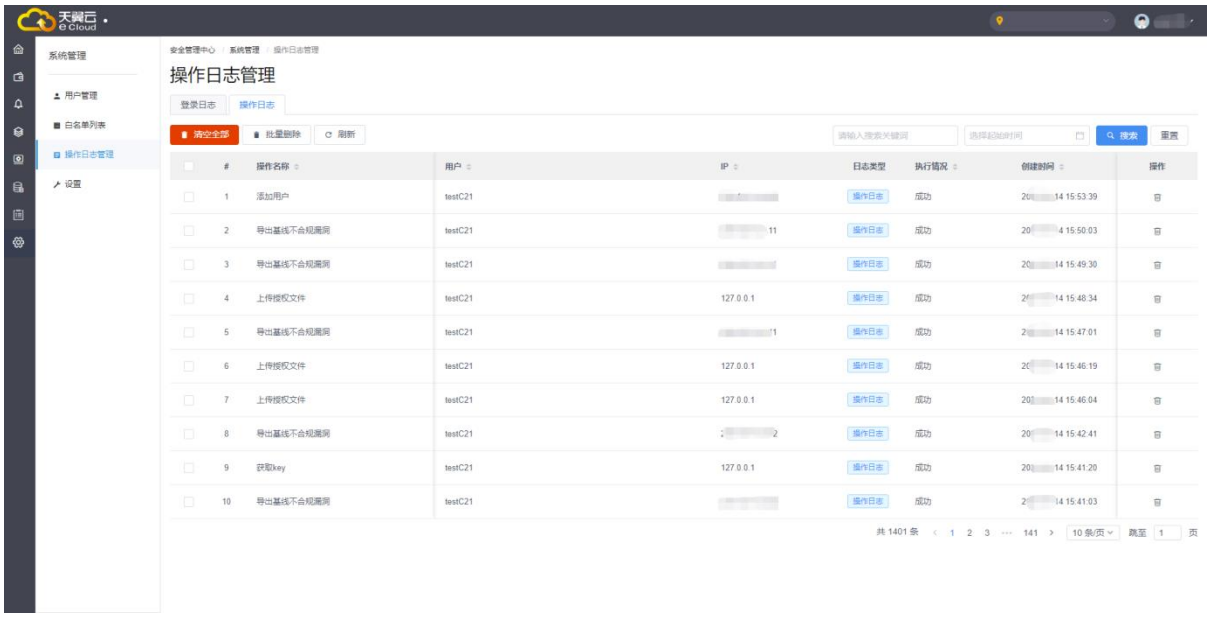
在登录日志 / 登录日记中可采用“清空全部”，点击『清空全部』，请谨慎做此操作。

支持批量删除，勾选所需删除项，进行批量删除。

可进行单个操作处理，点击右侧边栏，点击『删除』单个操作



在操作日志方面，记录的操作日志较为清楚，具有清空全部、批量删除及操作下单个删除的操作。操作名称记录系统所进行的操作，记录登录用户及 IP 地址等功能。



5 常见问题

（1）为减低云主机风险，仅开放最少端口，如何为安全组件云主机加固

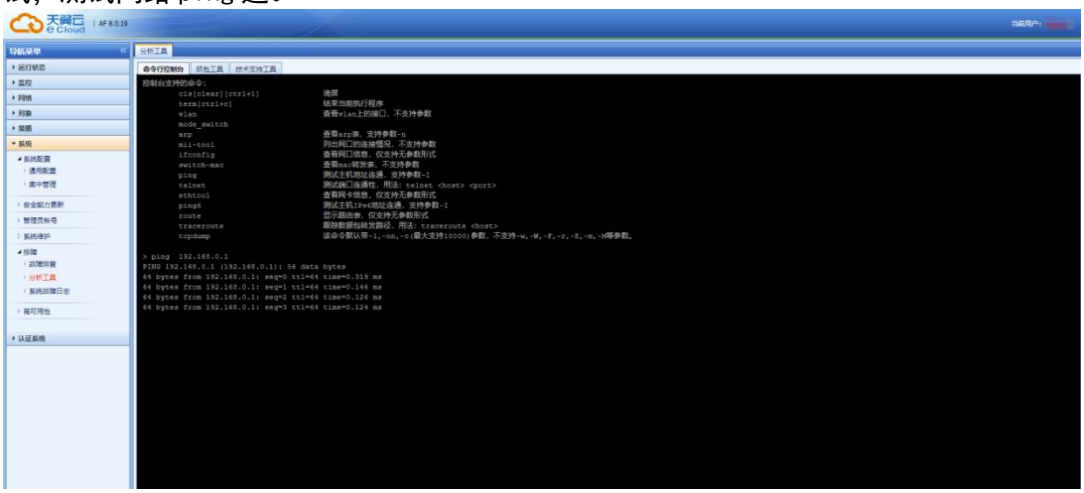
可通过设置云主机安全组，为每个安全组件云主机开放以下端口。

安全组件云主机	端口	端口作用
AQZQ-AF-***（云防火墙）	业务端口	网络通信
AQZQ-OSM-***（云堡垒机）	20/21	FTP
	22	ssh
	443	https、协议代理（web）
	444	数字证书登陆
	1521	Oracle 数据库
	3306	Mysql 数据库
	3389	RDP
	8080	http
	9443	Web 客户端
	12021	协议代理（FTP 协议）
	12024	协议代理（字符客户端：xshell、putty、crt、winscp、filezilla）
	12025	协议代理（RDP 客户端）
AQZQ-LAS-***（云日志审计）	TCP22	访问后台命令行
	UDP161	snmp query 设备状态
	UDP162	接收 snmp trap 日志
	UDP514	接收 syslog 日志
	TCP8082	访问设备管理控制台
	TCP8443、443	访问业务控制台
AQZQ-EDR-***（终端安全 EDR）	443	Agent 下载端口
	8083	业务端口
	54120	管理端口
AQZQ-DAS-***（云数据库审计）	TCP22	ssh 服务
	TCP80	web 服务

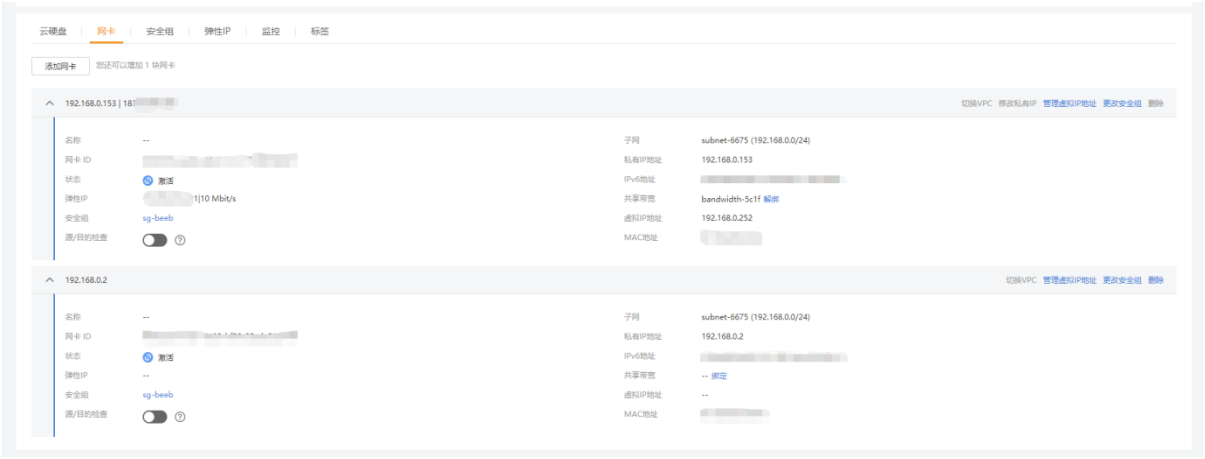
AQZQ-CSSP-***（安全专区服务）	TCP443	安全的 web 服务
	TCP8443	安全的 web 数据服务
	TCP9092	kafka 发送数据
	TCP9999	Agent 审计服务端口
	TCP5672	rabbitmq 客户端
	TCP10000	综合治理相互监听端口
	TCP15672	rabbitmq 服务端
	TCP4430	API 通信端口
	TCP4433	单点登录
	UDP4500、UDP500	用来创建扫描隧道与执行扫描
	TCP7443	API 通信端口，用来授权与部署扫描任务
	TCP8888	代理组件后端
	TCP8989	单点登录
	TCP9999	自动升级

（2）设置防火墙网络链路时，如果网络不通，该怎么排错

1、检查云防火墙内部的接口、路由是否设置与云主机上的信息一致。确认一致后，可在云防火墙组件管理页面的【系统】-【排障】-【分析工具】中 ping 子网网关（该用户所使用 VPC）测试，测试网络 ping 通。

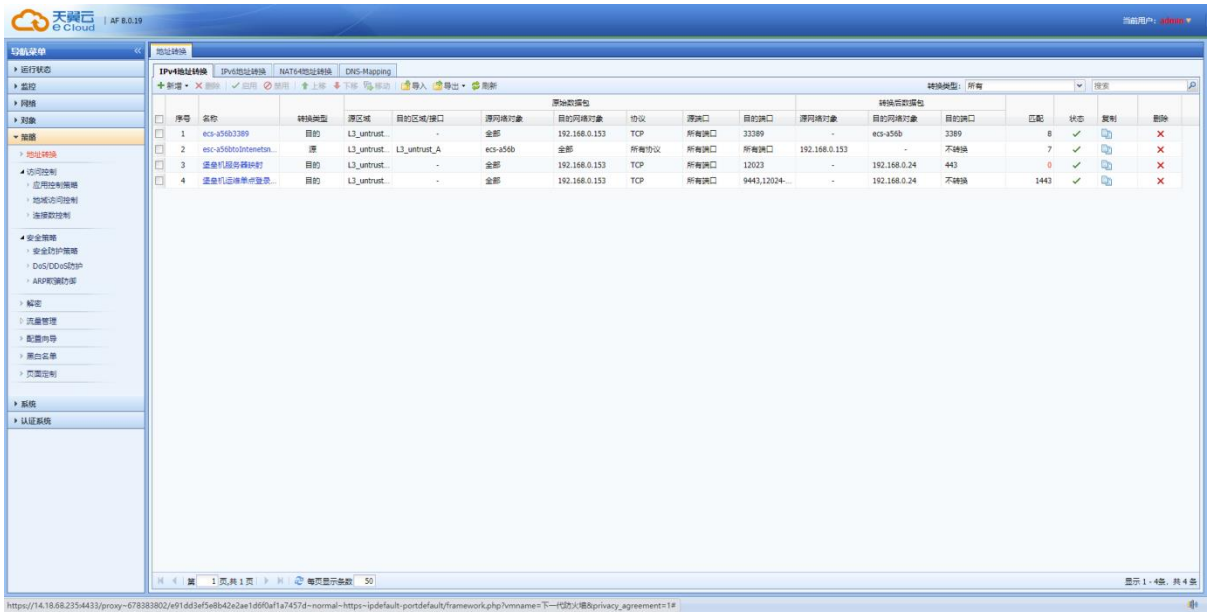


2、检查云防火墙网卡是否已绑定弹性公网 IP、检查 VPC 路由表是否已设置默认路由。



3、检查云防火墙到互联网及业务云主机是否网络互通，也可在命令行工具 ping 互联网地址与业务云主机地址查看是否可达，如果测试可达，则弹性公网 IP 设置正确。

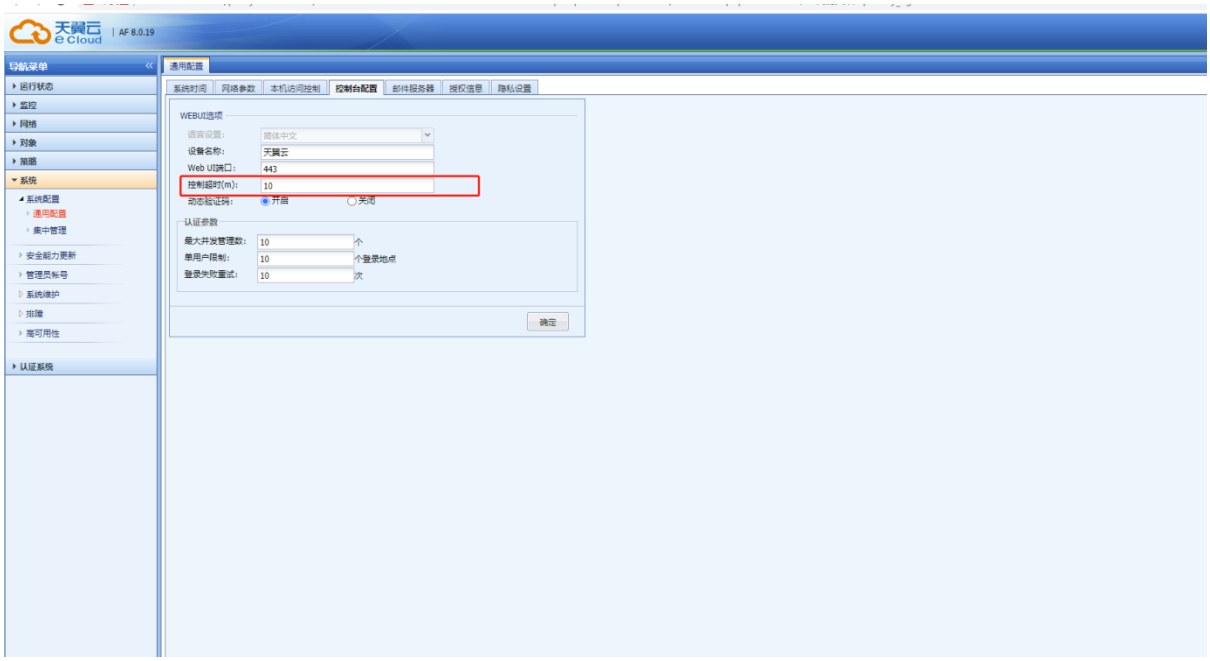
4、检查地址映射策略的转换前地址是否为云防火墙绑定弹性公网 IP 的私网地址或虚拟 IP 地址，测试从互联网访问弹性公网 IP 地址的端口，若测试成功，则证明网络策略正确。若仍无法访问，请检查虚拟私有云的安全组、访问控制，是否放通网络流量。



（3）云防火墙自动退出登录或登录超时

1. 重新在安全管理中心登录云防火墙组件

2. 在【系统】-【系统配置】-【通用配置】-【控制台配置】，进行控制超时设置



（4） 云防火墙授权时，显示授权信息失败

请等待 15 分种，超过 15 分钟仍未显示获取授权，需联系客服人员进行调整。

（5）云堡垒机无法进行 SSO 单点跳转

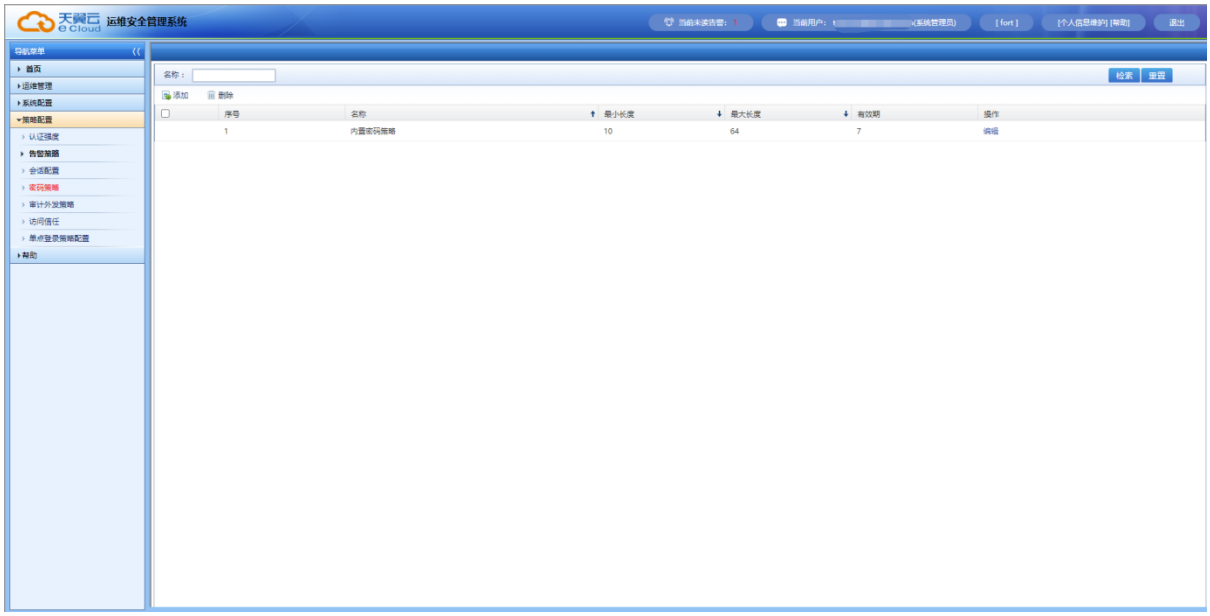
请按照 3.6.5 章节登录运维，进行插件下载安装。

（6）云堡垒机进行扩容，出现异常

云堡垒机的云主机附加磁盘后，如未看到系统存储空间扩容，请重启云主机后再查看

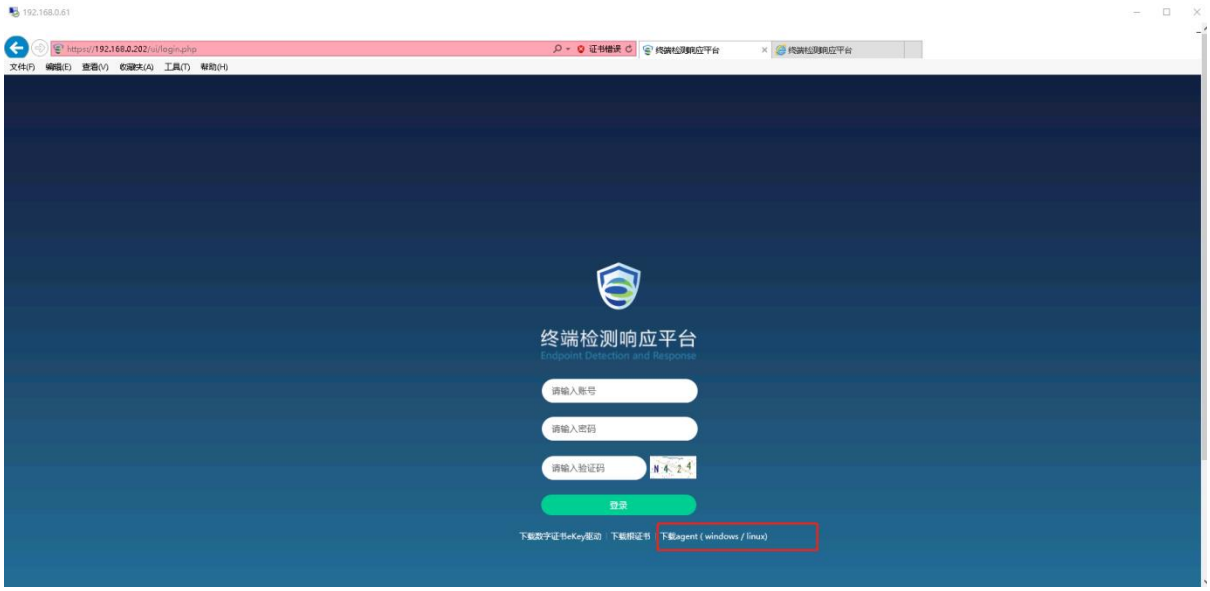
（7）云堡垒机的密码更换时间较短

云堡垒机更换密码较短，让用户登录系统管理员登录云堡垒机，然后在【策略】-【密码策略】进行策略调整，设置密码更换天数



（8）终端安全 EDR 安装客户端失败问题

请进入内网地址（https://AQZQ-EDR-XXX 云主机 IP）登录终端安全 EDR 组件，进行安装文件下载。



（9）终端安全 EDR 无法联网

A：在云防火墙添加终端安全 EDR 允许访问互联网的应用控制策略及源地址转换策略，详情请参考 3.6.4 映射端口。

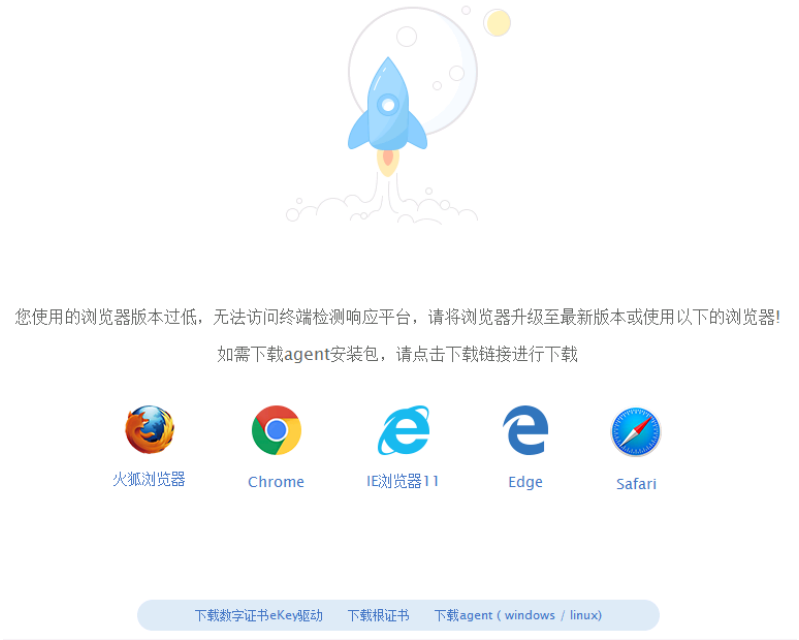
（10）安装过程中出现下图提示。

出现上图提示，说明安装程序文件名被改。在上图填写终端安全 EDR 地址及 443 端口即可完成安装，或者也可以重新下载安装程序（不能修改安装程序文件名）进行安装。

（11）安装过程中弹出提示“检测到安装了其它安全软件，可能与终端安全 EDR 客户端存在冲突”

卸载电脑上其它的安全软件后继续安装终端安全 EDR 客户端。

（12）使用 IE 浏览器打开 EDR 管理平台控制台，无法登录控制台，提示如下图



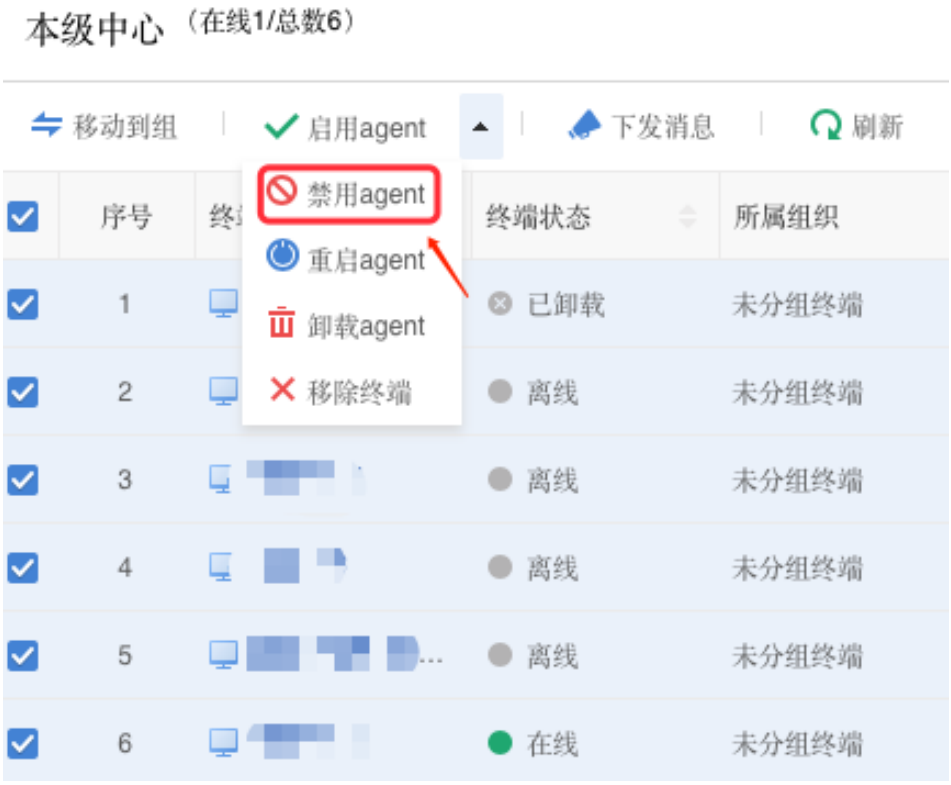
出现上图提示，说明 IE 浏览器版本太低。请使用 IE11 或其它浏览器登录。

（13）病毒库无法自动升级

请确保 EDR 管理平台 IP 地址、网关、DNS 配置正确。仍无法升级，请联系服务提供商处理。

（14）电脑安装终端安全 EDR 后出现异常情况

通过终端安全 EDR 管理平台[终端管理/终端分组管理]，禁用问题电脑的 agent，如下图，如果禁用后故障恢复，则联系服务提供商进一步处理。



（15）下发病毒查杀后，发现业务文件被误报为病毒

通过以下任一种方法将误报文件的业务文件加入信任名单。

1、通过终端安全 EDR 管理平台将误报文件加入信任名单。在[终端管理/策略中心/信任名单]页面下，如下图所示。

2、通过终端安全 EDR 客户端加入信任名单，如下图。

（16） 终端安全 EDR 是否可以支持 U 盘文件、网络共享路径下的文件进行查杀

终端安全 EDR 支持对 U 盘文件扫描查杀，不支持对网络共享路径下的文件进行查杀。

（17）电脑性能不足，终端安全 EDR 下发病毒扫描时，CPU 使用率高

打开终端安全 EDR 管理平台[终端管理/策略中心/病毒查杀]，启用“资源优化模式”，如下图。

（18）微隔离策略不生效的问题

请按如下检查，如果仍然不生效，请联系服务提供商处理。

微隔离功能不支持终端操作系统为 Windows XP 或 Windows Server 2003，如果终端操作系统是上述版本，则微隔离不生效。

打开终端安全 EDR 管理平台[微隔离/微隔离策略]，检查“微隔离生效开关”是否启用状态，如下图。

（19）微隔离流量状态无法显示

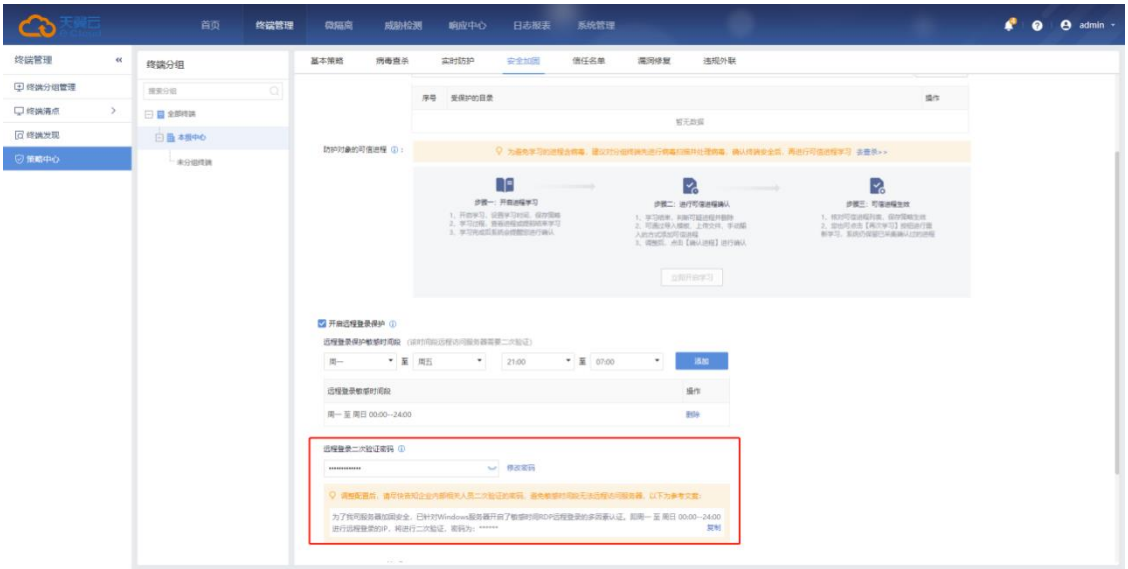
请按如下检查，如果无法解决，请联系服务提供商处理。

打开终端安全 EDR 管理平台[微隔离/微隔离设置]，检查“流量上报”开关是否启用状态，如下图。

打开终端安全 EDR 管理平台[微隔离/流量状态]，检查“过滤流量”条件是否启用，如下图。

（20） 终端安全 EDR 客户端安装后重新登录需要输入密码

在终端安全 EDR 组件中，在【终端管理】-【策略中心】-【安全加固】可查看终端登录密码

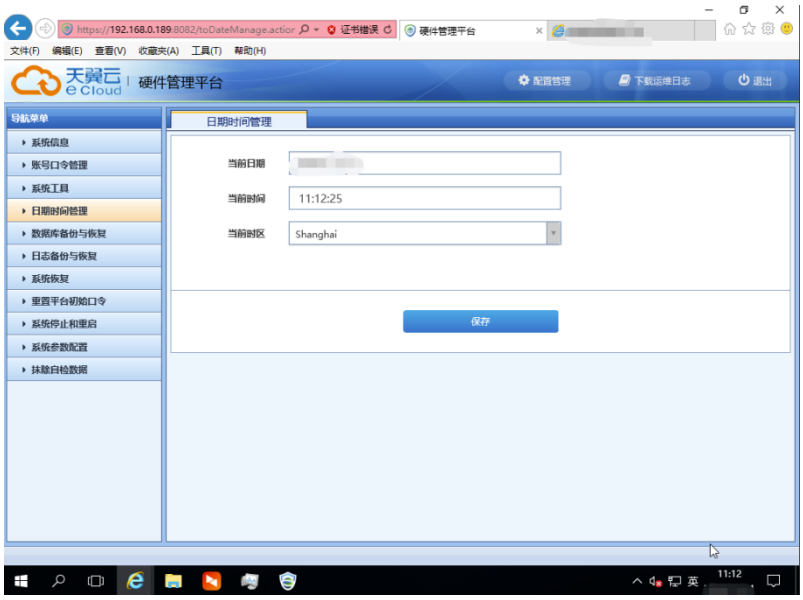


（21）终端安全 EDR 管理平台管理问题

如果有如下需求，如修改终端安全 EDR 管理平台 443 端口、恢复终端安全 EDR 管理平台控制台登录密码、终端安全 EDR 管理平台需要迁移至其它服务器等需求，请联系服务提供商处理。

（22）云日记审计系统日记时间不同步

登录同网段 windows 系统，访问云日志审计 8082 的 https 端口，初始密码为 admin/admin，当前目录设置新密码，在【日期时间管理】，设置与本地同步或者手动调整时间。

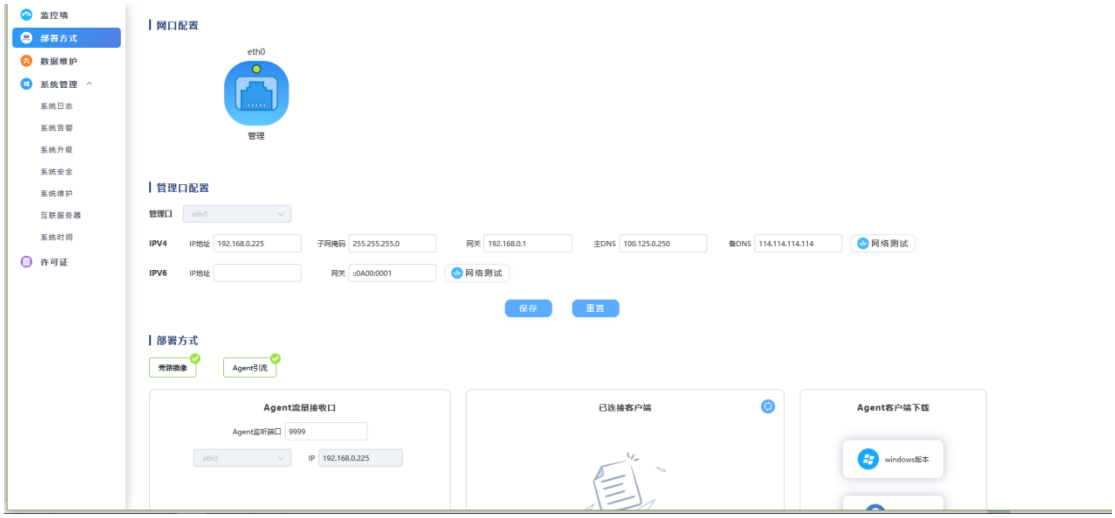


（23）如何查看是在云主机内成功安装安全组件 Agent 客户端

查看安全专区的资产或者总览页面，查看所添加资产是否已进行防护。

（24） 如何测试云数据库审计与互联网联通

进入云数据库审计管理页面，可控制网口运行状态，更改管理口（eth0）配置。点击【部署方式】，进行管理口配置，填写子网掩码和网关并保存。


监控墙
部署方式
数据维护
系统管理
系统日志
系统告警
系统升级
系统安全
系统维护
互联服务器
系统时间
许可证
网口配置
eth0
管理
管理口配置
管理口
eth0
IPV4
IP地址
192.168.0.225
子网掩码
255.255.255.0
网关
192.168.0.1
主DNS
100.125.0.250
备DNS
114.114.114.114
网络测试
IPV6
IP地址
网关
::0A00:0001
网络测试
保存
重置
部署方式
旁路镜像
Agent引流
Agent流量接收口
Agent监听端口
9999
eth0
IP
192.168.0.225
已连接客户端
Agent客户端下载
windows版本