阿里云 专有云Enterprise版 云盾(基础版)

安全管理员指南

产品版本: V3.1.0

文档版本: 20171129

为了无法计算的价值 | [-] 阿里云

| 序言 | 云盾(基础版)

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读 或使用本文档,您的阅读或使用行为将被视为对本声明全部内容的认可。

- 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档,且仅能用于自身的合法 合规的业务活动。本文档的内容视为阿里云的保密信息,您应当严格遵守保密义务;未经阿里云 事先书面同意,您不得向任何第三方披露本手册内容或提供给任何第三方使用。
- 未经阿里云事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分 或全部,不得以任何方式或途径进行传播和宣传。
- 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有任何通知或者 提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时发布更新后的用户文档。您 应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云网站上所有内容,包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站 画面的安排、网页设计,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标 权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使 用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此 外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或 复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、Aliyun"、"万网"等 阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、 产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或 其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

通用约定

按书	治明	±关///Ⅲ
		נילו דו
•	该类警示信息将导致系统重大变更甚至 故障,或者导致人身伤害等结果。	禁止:
	该类警示信息可能导致系统重大变更甚 至故障,或者导致人身伤害等结果。	▲ 警告 : 重启操作将导致业务中断,恢复业务所需 时间约10分钟。
!	用于警示信息、补充说明等,是用户必须了解的内容。	道 说明 : 导出的数据中包含敏感信息,请妥善保 存。
Ê	用于补充说明、最佳实践、窍门等,不是用户必须了解的内容。	说明 : 您也可以通过按 Ctrl + A 选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定 。
courier字 体	命令。	执行 cd /d C:/windows 命令,进 入Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid Instance_ID
[]或者[a b]	表示可选项,至多选择一个。	ipconfig [-all -t]
{}或者{a b}	表示必选项,至多选择一个。	swich {stand slave}

目录

法	上全声明	I
诵	所用约定	1
4		4
I	[既止]	1
2	配置要求	2
3	登录和注销	3
	3.1 登录	3
	3.2 注销	5
4	云盾基础版安全中心	7
-	41 概述	7
	4.2 云盾基础版安全中心界面	7
	4.3 基础信息	8
	4.3.1 总览	8
	4.3.1.1 简介	8
	4.3.1.2 查看网络流量信息	8
	4.3.2 威胁	10
	4.3.2.1 简介	10
	4.3.2.2 查看威胁攻击信息	10
	4.4 服务器安全	11
	4.4.1 主机防护	12
	4.4.1.1 登录安全	12
	4.4.1.1.1 登录记录	12
	4.4.1.1.2 查询登录记录	12
	4.4.1.1.3 暴力破解	13
	4.4.1.1.4 查询暴力破解事件	14
	4.4.1.2 木马查杀	15
	4.4.1.2.1 操作说明	15
	4.4.1.2.2 状态说明	15
	4.4.1.2.3 查询木马文件信息	15
	4.4.1.3 配置中心	17
	4.4.1.3.1 间介	17
	4.4.1.3.2 配直出名中	1/
	4.4.1.3.3	۵۲ مو
	4.4.2 土ル八位位渕	20
	4.4.2.1 旦旬乂汁泰以尹汁心求 / / 2 2 杏呑巳労进現记ヲ	∪∠ ^0
		∠∪ 20
	7.7.2.0 旦旬升市网泊灶攻儿米	20

	4.4.2.4 查看异常端口监听记录	21
4.5 🕏	安全审计	21
	4.5.1 审计一览	. 22
	4.5.2 审计查询	.23
	4.5.3 原始日志	. 23
	4.5.4 策略设置	. 23
	4.5.4.1 添加审计策略	.23
	4.5.4.2 添加审计类型	.24
	4.5.4.3 设置报警接收人	25
	4.5.4.4 管理事件日志存档	.25
	4.5.4.5 管理导出任务	.26
4.6 孨	系统管理	26
	4.6.1 管理阿里云账号	27
	4.6.1 管理阿里云账号 4.6.2 告警设置	27 28
	4.6.1 管理阿里云账号 4.6.2 告警设置 4.6.2.1 设置告警联系人	27 28 28
	4.6.1 管理阿里云账号 4.6.2 告警设置 4.6.2.1 设置告警联系人 4.6.2.2 设置告警信息	. 27 . 28 . 28 . 29
	 4.6.1 管理阿里云账号 4.6.2 告警设置 4.6.2.1 设置告警联系人 4.6.2.2 设置告警信息 4.6.3 全局设置 	27 28 28 28 29 30
	4.6.1 管理阿里云账号 4.6.2 告警设置 4.6.2.1 设置告警联系人 4.6.2.2 设置告警信息 4.6.3 全局设置 4.6.3.1 流量采集网段设置	27 28 28 29 30 .30
	 4.6.1 管理阿里云账号 4.6.2 告警设置 4.6.2.1 设置告警联系人	27 28 28 29 30 30 .30
	 4.6.1 管理阿里云账号 4.6.2 告警设置 4.6.2.1 设置告警联系人	27 28 28 29 30 30 .30 .30 .31
	 4.6.1 管理阿里云账号 4.6.2 告警设置 4.6.2.1 设置告警联系人	. 27 . 28 . 28 . 29 . 30 . 30 . 30 . 31 . 32
	 4.6.1 管理阿里云账号 4.6.2 告警设置	. 27 . 28 . 29 . 30 . 30 . 30 . 31 . 32 . 32
	 4.6.1 管理阿里云账号 4.6.2 告警设置	. 27 . 28 . 28 . 29 . 30 . 30 . 30 . 30 . 31 . 32 . 32 . 33

1 概述

云数据中心环境下,安全业务复杂多样,需要多种安全能力协同保证平台的安全和业务的安全,多 租户的场景下,租户的边界变得模糊,各租户的安全需求不一致,势必导致安全管理的不可控制。 统一的云安全管理成为迫切需求,将替代传统的单点安全管理,被云用户所接受。

云盾以阿里云互联网攻防技术为核心,为用户建设涵盖网络安全、应用安全、主机安全、安全态势 感知的全方位互联网安全攻防体系。不同于以往以检测技术为主的边界防护方式,云盾防护以泛安 全数据与情报联动分析为驱动,为用户提供全景的安全态势感知、攻击溯源回溯、基础安全防护等 功能。通过纯软件化的部署方式,云盾可以帮助您在自有 IDC、专有云、公共云、混合云等多种业 务环境获得与阿里云同等强度的互联网防护能力。

云盾对专有云环境中的网络安全、主机安全进行监控,并有效防护各类安全威胁。安全管理人员可 以通过专有云的云安全中心控制台实时了解专有云环境内的安全态势,并及时对安全风险项进行处 理。同时,专有云云盾还具备安全审计功能,对云服务操作日志进行展示和审计,以便安全审计员 及时发现并消除安全隐患。

阿里云专有云Enterprise V3.0中提供了云盾基础版及高级版。

2 配置要求

访问专有云云盾安全中心控制台时,本地PC需要满足如表 2-1: 配置要求表中要求才可以正常登录。

表 2-1: 配置要求表

内容	要求
浏览器	 Internet Explorer浏览器: 11及以上版本 Chrome浏览器(推荐): 42.0.0及以上版本 Firefox浏览器: 30及以上版本 Safari浏览器: 9.0.2版本及以上版本
操作系统	Windows XP/7 及以上版本Mac系统

3 登录和注销

3.1 登录

前提条件

在DTCenter的**系统管理>用户管理**页面,创建专有云云安全中心用户,并为该用户分配云安全中心相关的角色权限:

所有云安全中心角色均为默认角色,无法自定义添加。关于如何创建用户及授予角色权限,请参考 《管理员指南》中的创建用户。

- 云安全中心系统管理员:负责云安全中心系统管理设置,具备阿里云账号管理、告警设置、及全局设置的权限,但无法处理情报同步相关操作。
- 云安全中心安全管理员:负责检查整个专有云平台的安全状态,以及管理云盾各功能模块安全 策略的设置,包括态势感知、DDoS检测、服务器安全、资产管理各目录下的所有功能节点权 限,并且可以在系统管理目录下进行安全事件的告警设置。
- 部门安全管理员:负责检查用户所在部门下各云产品资源的安全状态,以及管理针对该部门的云 盾各功能模块安全策略的设置,包括态势感知、DDoS检测、服务器安全、资产管理各目录下的 所有功能节点权限。
- 云安全中心审计员:负责整个专有云平台安全审计工作,查看审计日志及相关审计策略设置,具 备安全审计目录下所有功能节点权限。

背景信息

登录专有云云盾安全中心有以下两种方式:

- 登录DTCenter,从DTCenter页面上跳转到专有云云盾安全中心页面。
 - a) 打开Chrome浏览器。
 - b) 在地址栏中,输入DTCenter的网站地址(例如:http://*DTCenter*网站地址),按**Enter**,进入DTCenter登录页面,如图 3-1: *DTCenter*登录页面所示。

图 3-1: DTCenter登录页面



- c)在DTCenter登录页面,输入已创建的专有云云盾安全中心用户的登录账号、密码及验证码。
- d) 单击**登录**。
- e) 登录DTCenter后,在菜单导航栏选择云安全中心。单击**安全中心**,进入云盾安全中心页面,如图 3-2:安全中心页面所示。

图 3-2: 安全中心页面

安全 全管	中心是以云平台安全资产和安全能力为核心,以安全事件管理为关键流程,协 理员进行安全事件风险分析,预警管理和应急响应的安全管理系统。	助安
	教会中心	

• 通过专有云云盾安全中心的网站地址,直接登录云盾安全中心页面。

说明:

从部署人员处获取相关网站地址信息,通过浏览器直接访问页面。

- a) 打开Chrome浏览器。
- b) 在地址栏中,输入专有云云盾安全中心的网站地址(例如:http://*DTCSC*网站地址),按**Enter**。
- c) 输入已创建的专有云云盾安全中心用户的登录账号、密码及验证码。
- d) 单击**登录**。

3.2 注销

在专有云云盾控制台页面,单击页面右上角的退出图标,如图 3-3:用户注销所示,即可退出登录。

图 3-3: 用户注销



4 云盾基础版安全中心

4.1 概述

云盾基础版是保障云计算服务平台正常运行的云安全运营平台。云盾基础版以云计算资源为基础防 护对象,以云上业务系统为防护核心,以安全事件管理为主要手段,及时准确地发现云平台的网络 异常行为和安全威胁,协助安全管理员进行安全管理、风险分析、应急响应和综合决策。

云盾基础版为用户提供异常流量分析检测、Web层攻击检测/防御、主机防入侵的实时防护能力,并 能够提供云计算平台的ECS、RDS、物理服务器、OpenAPI服务的安全审计,还支持对自定义的审 计类型进行审计。

4.2 云盾基础版安全中心界面

云盾基础版的云安全中心界面主要可以分为三大区域,如图 4-1: 云盾基础版安全中心界面图所示。



图 4-1: 云盾基础版安全中心界面图

表 4-1: Web 界面区域说明

区域	说明
操作按钮区	: 单击此按钮退出当前登录。
	: 単击此按钮进入修改个人信息页面。
	: 单击此按钮进入总览页面。

区域	说明
菜单导航树区	云安全中心管控平台包基础信息、服务器安全、安全审计、系统管理四个部 分,主要功能如下:
	 基础信息:根据网络流量情况对当前的安全态势进行概要性的展示,帮助管理员了解当前网络流量情况。 服务器安全:提供主机防护及主机入侵检测,保障服务器安全。 安全审计:对云服务操作日志展示和审计,以便安全审计员及时发现并消除安全隐患。 系统管理:安全事件报警接收人设置,以便安全管理员及时处理云服务的安全事件。云安全中心和云安全控制台登录和操作日志展示,以便系统管理员进行分析和审计。
操作视图区	当选择了菜单项后,该菜单项的功能配置界面就会显示在右侧的操作视图区中。

4.3 基础信息

基础信息集成了企业漏洞监控、黑客入侵监控、Web攻击监控、DDoS攻击监控、威胁情报监控、 企业安全舆情监控等安全态势监控手段,通过建模分析方法,从流量特征、主机行为、主机操作日 志等获取关键信息,识别无法单纯通过流量检测或文件查杀发现的入侵行为,借助云端分析模型输 入并结合情报数据,发现攻击威胁来源和行为,并评估威胁程度。

云盾基础版基础信息主要包含两个部分:

- 安全总览:展现安全的整体态势、网络流量情况和大屏相关信息。
- 威胁分析:展现业务系统中目前面临的安全风险和威胁来源。

4.3.1 总览

4.3.1.1 简介

总览页面根据网络流量情况对当前的安全态势进行概要性展示,让用户快速了解和掌握当前安全态势。

网络流量是对网络的出口、入口、QPS流量信息的分析,向用户展示流量的高峰、低谷、速率和地 域来源的分布规律。

4.3.1.2 查看网络流量信息

背景信息

网络流量页面通过折线图展示了过去一段时间的流量信息,通过查看不同时期、区域或单个IP的流量情况,可以定位流量的高峰和低谷时间、速率和地域等流量分布规律,同时通过展示TOP5流量的IP,可以有效甄别恶意的IP访问。

操作步骤

1. 单击总览,进入总览页面,如图 4-2: 总览页面所示。

图 4-2: 总览页面



2. 在总览页面,单击今天、最近30天、最近90天可以切换查看不同时间段的流量信息。

3. 在所属区域中可以选择区域信息,在搜索框中输入IP,可以分区域、分IP查询流量信息。

4. 将鼠标停留在流量折线图上,可以显示流量TOP5的 IP,如图 4-3: 查看流量 TOP5 的 IP所示。

图 4-3: 查看流量 TOP5 的 IP

	2015-12-01 21:57:	30								
	网络出口流量: 53.6	5M								
	流量TOP5							今天	最近30天	最近90天
	121.25.152.131	174.13G								
	112,74,86,810	60.06G								
网络	40.86269.00	43.50G								
	30.88.180.200	41.43G								
	112.74.128.00	25.41G								
\sim	᠕᠕᠕	ma m								
	0	N N M	•						\sim	\sim
hadh		· ^ ·	Am		A. A.		-	m		•
		\sim	\sim				~~~~	~~~	~~~~	\sim
12/01 1 20:00:00 21	2/01 12/01 :00:00 22:00:00	12/01 12/02 1 23:00:00 00:00:00 01	2/02 12/02 :00:00 02:00:00	12/02 03:00:00	12/02 04:00:00	12/02 05:00:00	12/02 06:00:00	12/02 07:00:00	12/02 08:00:00	12/02 09:00:00
一网络入口流雪	建 — 网络出口流生	2								

4.3.2 威胁

4.3.2.1 简介

云盾基础版**威胁**页面包括Web应用攻击和暴力破解两类安全信息:

- Web应用攻击:访问Web服务器的流量都会经过云盾的流量安全监控模块,流量安全监控模块对流量进行监测,提取流量中的攻击信息。
- **暴力破解**:当黑客针对某个资产进行暴力破解的时候,安骑士客户端能够及时监测到爆破的发生 并上报给云盾安全中心。

4.3.2.2 查看威胁攻击信息

操作步骤

1. 在威胁页面,单击 应用攻击,查看应用攻击信息及上报的应用攻击事件,如图 4-4: 应用攻击页面所示。

图 4-4: 应用攻击页面



您可以查看最近7日的攻击趋势、攻击的类型以及详细的攻击信息。

2. 单击暴力破解,查看暴力破解事件记录,如图 4-5: 暴力破解页面所示。

图 4-5: 暴力破解页面

威胁				
所属区域:全部 清输入要搜索的关键字	v 攻击分类: 应用攻击 墨力破解			
类型	威胁来源/受害资产	首次发现时间	最后发现时间	操作
• 暴力破解	(HINT) H. 20.4.90	2017-07-27 09:26:00	2017-07-27 13:33:01	展开▼
暴力破解	(MINT) 41.2014.201	2017-07-25 15:15:02	2017-07-25 15:18:02	展开▼
暴力破解	(0.002).00.010.0	2017-07-24 15:44:58	2017-07-25 14:14:29	展开▼
暴力破解	(8499) M (M (94))	2017-07-25 09:52:40	2017-07-25 09:52:40	展开▼
暴力破解	0409333333	2017-07-21 14:30:10	2017-07-21 14:30:13	展开▼
暴力破解	(HETELECHINE	2017-07-20 06:23:30	2017-07-21 03:51:30	展开▼
暴力破解	(MOT)(41.00.20.27)	2017-07-20 04:12:12	2017-07-20 23:18:37	展开▼
暴力破解	(mm)/ac.m.ac.av	2017-07-20 04:13:34	2017-07-20 23:17:46	展开▼

4.4 服务器安全

云盾能够防护每一台用户主机的安全,安骑士基础版是云盾的一个核心组件,提供了主机防护及主机入侵检测功能。安骑士分为客户端和服务器端。安骑士客户端配合安骑士服务器,监测系统层和 应用层的攻击行为,实时发现黑客入侵行为。

主机防护

主机防护具有以下功能:

- 登录安全:云盾登录安全防护包括异地登录提醒和暴力破解告警。
 - 异地登录提醒:云盾维护了每一台已安装安骑士客户端的主机的常用登录地,如果在非常用
 登录地有登录行为,会上报事件到安骑士服务器端。支持对RDP/SSH方式的异地登录告警。

- 暴力破解防护:安骑士客户端对所有的登录行为进行审计并实时上报到安骑士服务器端。服务器端进行汇总和分析,若匹配到暴力破解行为则会立即写进数据库并展示在云盾安全中心页面上。支持RDP/SSH等应用的密码破解攻击防护。
- **木马查杀**:恶意文件通过本地自动查杀及匹配服务器端样本库查杀。支持PHP、JSP等后门文件 类型。

主机入侵检测

主机入侵检测功能检测出所有服务器上发现的文件篡改、异常进程、异常网络连接、可疑端口监听 等行为,帮助用户及时发现服务器安全隐患。

4.4.1 主机防护

4.4.1.1 登录安全

登录安全主要分为异地登录和暴力破解两部分,管理员可以在云盾安全中心中查看异地登录和暴力 破解的告警信息,并查询登录记录和暴力破解的来源等详细信息,对异地登录和破解成功的记录进 行处理,处理后标记为已处理便不再进行告警。

4.4.1.1.1 登录记录

用户可以在配置中心设置服务器的常用登录地,如果发现不在常用登录地的登录行为,会在云盾安全中心提醒异地登录事件。在告警设置中可以为异地登录事件配置手机通知和邮箱通知。

常用登录地的设置请参见配置登录地,告警设置请参见告警设置。

原理简述

- 1. 安骑士客户端通过TCP协议上报登录信息到安骑士服务器端。
- 2. 安骑士服务器端通过消息模块将上报的信息发送到Defender模块。
- **3.** Defender模块分析登录信息,判断是否异地登录,并将结果写入Aegis-db。如果为异地登录,会将消息发送给态势感知模块进行进一步处理,判断是否通过手机、邮件提醒用户。

4.4.1.1.2 查询登录记录

背景信息

登录记录状态主要有异地登录、正常登录和已处理。支持通过主机IP、主机名进行模糊查询,并且 支持根据登录用户及登录时间进行筛选。

通过查询登录记录,管理员可以了解安骑士发现的异地登录事件,并及时进行排查处理,检查是否 有黑客入侵行为。

操作步骤

1. 在服务器安全 > 主机防护 > 登录安全页面,选择登录记录,如图 4-6: 登录记录页面所示。

图 4-6: 登录记录页面

所属	区域:全部	▼ 服务器IP/名称	, 支持模糊查询	输入对应用户名	登录时间: 起始时间	3	图 终止时间 按次			
分类:	登录记录17 暴力破解4									
	服务器IP/名称	所属用户	所属业务	所属区域	登录时间	型表表型	登录地点	对应用户名	状态(全部) ▼	操作
	2014/23		默认分组	未指定机房	2017-07-25 17:33:48	SSH	4500000(0r(114144))	root	异地登录	标记为已处理
	2014/02 127012/07/04/02.040		默认分组	未指定机房	2017-07-25 13:09:44	SSH	100000000(r(110000)	root	异地登录	标记为已处理
	2024/20 12702/2020/2020/2020		默认分组	未指定机房	2017-07-25 13:00:39	SSH	10000000000000000000000000000000000000	root	异地登录	标记为已处理
	30.2%3 1.364/0425		study	未指定机房	2017-07-18 17:21:15	SSH	9(15)(()) (maximum)	root	异地登录	标记为已处理
	20.2%3 1.364/0420		study	未指定机房	2017-07-18 10:08:23	SSH	(Sil(Another and	root	异地登录	标记为已处理

2. 设置查询条件。

3. 单击搜索,显示符合条件的登录记录。

4. 确认登录正常后,您可以单击标记为已处理。

5. 在弹出的对话框中单击确定。该事件状态被修改为已处理,并且不再在控制台提醒该记录。

4.4.1.1.3 暴力破解

用户可以在配置中心设置登录白名单,如果暴力破解成功且登录源IP不在白名单内,会在专有云云 盾控制台提醒暴力破解成功,在告警设置中可以为暴力破解配置手机通知和邮箱通知。

白名单的设置请参见配置白名单,告警设置请参见告警设置。

流程分析

- 安骑士客户端通过本地监控主机的登录记录来发现暴力破解事件,通过TCP协议上报暴破消息到 安骑士服务器端。
- 2. 安骑士服务器端通过消息模块将上报的信息发送到Defender。
- **3.** Defender分析暴破信息,判断暴破类型,以及是否暴力破解成功,并将暴破信息写入Aegis-db。 如果破解成功,会将消息发送给态势感知进行进一步处理,判断是否通过手机、邮件提醒用户。

暴力破解事件类型

暴力破解事件类型主要有破解成功、有威胁、无威胁和已处理,事件类型说明请参见表 4-7: 暴力破 解事件类型表。

表 4-2: 暴力破解事件类型表

事件类型	说明
破解成功	暴力破解已成功
有威胁	暴破次数较多
无威胁	暴破次数较少
已处理	已经解决的暴力破解成功事件

4.4.1.1.4 查询暴力破解事件

背景信息

通过查询暴力破解事件,用户可以了解暴力破解的攻击源、攻击次数以及拦截状态。当控制台显示 暴力破解成功意味着用户的主机已经被黑客暴力破解出密码并且成功登录了主机,管理员需要及时 进行排查处理。

暴力破解事件查询支持通过主机IP、主机名进行模糊查询,并且支持根据登录用户及登录时间进行 筛选。

操作步骤

在服务器安全 > 主机防护 > 登录安全页面,选择暴力破解,设置查询条件,单击搜索,查看暴力破解事件,如图 4-7:暴力破解事件页面所示。

图 4-7: 暴力破解事件页面

所履	区域:全部 🔻	服务器IP/名称,	支持模糊查询	输入对应用	1户名 攻击时间	記細间	至 终止时间	搜索			
9 9	登录记录12 暴力破解4										
	服务器IP/名称	所属用户	所属业务	所属区域	攻击时间	攻击类型	攻击源	对应用户名	攻击次数	拦截状态(全部) ▼	操作
	ERCETACI TELEBOORT	未指定机房	study	未指定机房	2017-07-18 17:21:15	SSH	1010(2) (an arrange)	root	100	破解成功	标记为已处理 帮助
	DORM NOT THE REPORT OF	未指定机房	test	未指定机房	2017-07-04 23:13:37	SSH	000(04440)	root	100	破解成功	标记为已处理 帮助
	DORM NORMAL INCOMES	未指定机房	test	未指定机房	2017-07-04 23:13:37	SSH	000(04440)	root	100	破解成功	标记为已处理 帮助
	DORM NOT STREET	未指定机房	test	未指定机房	2017-07-04 23:13:37	SSH	000(04440)	root	100	破解成功	标记为已处理 帮助
	MARK INCOME.	未指定机房	默认分组	未指定机房	2017-07-27 13:33:01	SSH	$\Phi(S(a),a,b)(a) = (a,a,a,a,a)$	root	500	有威胁	

 调查暴力破解的原因,排除风险后,单击标记为已处理,在弹出对话框中单击确定,该事件状态 被修改为已处理。

4.4.1.2 木马查杀

黑客入侵网站后,通常会将木马文件放在主机的Web服务目录下,和正常文件混在一起,然后通过 浏览器来访问恶意文件,从而达到控制网站服务器的目的。木马查杀功能及时检测木马文件并向管 理员告警,管理员可以在云盾安全中心查看已发现的木马文件,并对木马文件进行隔离、忽略、恢 复、移除信任文件操作。在已设置手机或邮件提醒的情况下,同一个木马文件只会在首次发现时推 送提醒,设置提醒请参见告警设置。

4.4.1.2.1 操作说明

■ 说明:

当移除信任文件后,该条告警将被删除,后续扫描将会重新上报木马信息。

操作	说明	操作前状态	操作后状态
忽略	忽略木马后,将不再提示风险。	待处理	信任文件
恢复	从FTP服务器把木马文件下载到本地。	已隔离	信任文件
移除信任文件	移除信任文件后,将会继续提示风险。	信任文件	无数据
隔离	把本地木马文件删除掉,上传到FTP服务器中 进行隔离。	待处理	已隔离/无需处理

表 4-3: 木马文件操作说明表

4.4.1.2.2 状态说明

表 4-4: 木马事件状态说明表

状态	说明
待处理	表明该文件是有危险的木马文件。
已隔离	表明该木马已被查杀。
信任文件	表明该文件已查明无危险。
无需处理	表明隔离时该木马已不存在。

4.4.1.2.3 查询木马文件信息

背景信息

木马查杀状态主要分为待处理、已隔离和信任文件,支持通过主机名称和主机IP进行模糊查询,并 且支持根据时间段进行筛选。木马事件列表可以按紧急程度排序,也可以按照组合服务器查看。

通过查询木马事件,用户可以了解安骑士发现的木马文件信息。

操作步骤

1. 在服务器安全 > 主机防护 > 木马查杀页面,设置查询条件,单击查询。

按紧急程度排序

优先展示待处理状态的木马查杀信息,再按发现时间降序排列展示,如图 4-8:按紧急程度排序 展示所示。

图 4-8: 按紧急程度排序展示

所属区域: 全部	▼ 服务器IP/名称,支持	F模糊查询 更新	耐间: 起始时间	至终止时间 搜索			
排序: 🖲 按紧急程度	◎ 组合相同服务器						
□ 服务器IP/名称	所属用户 所属业务	所属区域	更新时间	木马文件路径	木马类型	状态(全部) ▼	操作
 20,253 3400,000 	test	未指定机房	2017-07-26 19:27:19	/var/www/html/test_11_2.php	Webshell	待处理	隔离 忽略
 20.255 30000.005 	test	未指定机房	2017-07-26 19:27:19	/var/www/html/test_7_12.php	Webshell	待处理	隔离 忽略
 30.2584 304032305 	test	未指定机房	2017-07-26 19:27:19	/var/www/html/test_7_13_1.php	Webshell	待处理	隔离 忽略
 30.343 30.6400 	study	未指定机房	2017-07-26 19:20:54	/var/www/html/test123.php	Webshell	待处理	隔离 忽略
 SSLMJ Conversion 	study	未指定机房	2017-07-26 19:20:53	/var/www/html/webshell_test/8c6c5712-586f-4d1d-ab65-4fcda5755ce3.php	Webshell	待处理	隔离 忽略

组合相同服务器排序

按待处理个数降序排列,如图 4-9:组合相同服务器排序展示所示。

图 4-9: 组合相同服务器排序展示

所属区域:全部 🔻 服务器	P/名称,支持模糊查询 搜索					
排序: 🔍 按紧急程度 🖲 组合相同服务器						
服务器IP/名称	所属用户	所属业务	所属区域	已处理	待处理	操作
DESCO TO AMAGO		study	未指定机房	4个	15个	查看详情
DESCO PERCENSION		test	未指定机房	1个	3个	查若详情
DESCH SHREETERS		test	未指定机房	1个	3个	查看详情
H.2H.3 Internet investment		默认分组	cn-hangzhou-env5-d01	0个	3个	查看详情

 在组合相同服务器排序展示下,单击某个服务器所在行对应的查看详情,可以查看该服务器下所 有木马查杀的情况,根据发现时间按紧急程度排序,如图 4-10:查看服务器详情所示。

图 4-10: 查看服务器详情

	ē¥			
□ 更新时间	木马文件豁径	木马类型	状态(全部) ▼	操作
2017-07-26 19:20:54	/var/www/html/test123.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/webshell_test/8c6c5712-586f-4d1d-ab65-4fcda5755ce3.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/webshell_test/24a8cf3d-cbb4-4dbd-9318-dc4f6d78c69d.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/test_11_3.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/test_11_5.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/xx4.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/test_19_40.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/test_19_41.php	Webshell	待处理	隔离 忽略
2017-07-26 19:20:53	/var/www/html/test1948.php	Webshell	待处理	隔离 忽略

3. 单击返回木马查杀,可以回到木马查杀页面重新进行查询。

4.4.1.3 配置中心

4.4.1.3.1 简介

配置中心支持以下配置内容:

- **白名单设置**:登录IP白名单主要用于过滤暴力破解和暴力破解成功事件。如果访问源IP和目的IP在登录IP白名单中,暴力破解失败。
- 登录地设置:常用登录地主要用于异地登录的判断。如果不设置常用登录地,不管在哪里登录,都不是异地登录。如果设置了常用登录地,在非常用登录地登录的第一次和第五次会提醒此次登录为异地登录,其余都判定为正常登录。如果在一个登录地登录次数大于等于六,这个登录地会被自动加入到常用登录地,并在页面上展示出来。
- 基线检查设置: 支持设置周期性自动安全体检策略。

4.4.1.3.2 配置白名单

操作步骤

在服务器安全 > 主机防护,单击配置中心,单击白名单设置,进入白名单设置页面,如图 4-11:
 白名单设置页面所示。

图 4-11: 白名单设置页面

配置中心 1 返回				
白谷单设置 登录地设置 基线检查设置				
类型:全部▼ 输入源IP/网段 输入目的IP/网段	输入用户名			滚加
源IP	目的IP	用户名	类型	操作
LEARCEA.	ER.DECEOF	test	主机通用白名单	删除
Mark 202 and	01040	123456	主机登录记录白名单	删除
DESIN	191240	root	主机登录记录白名单	删除
PENKAP	P8.96237	qqq	主机暴力破解白名单	删除
PR-186-57	10.000	www	主机通用白名单	删除
DEMO22	18.166237	eee	应用攻击白名单	删除
P\$480.0	PE-66207	m	主机登录记录白名单	删除
00963408	0.001429	test	主机登录记录白名单	删除

- 2. 单击**添加**。
- 3. 在添加白名单对话框中,设置需要添加的白名单 IP,单击确认,添加白名单 IP,如图 4-12: 添加白名单对话框所示。

图 4-12: 添加白名单对话框

添加白名单		×
源IP	请输入IP/网段	
目的IP	请输入IP/网段	
用户名	请输入用户名,且用户名长度不超过64位	
 类型	主机暴力破解白名单	7
		确定 取消

4.4.1.3.3 配置登录地

操作步骤

在服务器安全 > 主机防护,单击配置中心,单击登录地设置,进入登录地设置页面,如图 4-13:
 登录地设置页面所示。

图 4-13: 登录地设置页面

白名单设置	登录地设置	基线检查设置						
常用登录地								
上海市2台	尼泊尔	1台 未	分配或者内网IP110台 印度尼西亚1台	2 巴基斯坦1台	泰国1台	呼和浩特市1台	深圳市1台	青岛市1台
十添加								

- 2. 单击添加。
- 3. 在添加常用登录地对话框中,设置需要添加的常用登录地,单击确认,添加常用登录地信

息,如图 4-14: 添加白名单对话框所示。

图 4-14: 添加白名单对话框

添加常用登录地			\times
请选择要添加的常用登录地:			
请选择 ▼ 请确认已选择	要添加的城市!		
所有服务器	送选	常用登录地为 <mark>请选择</mark> 的服务器	全选
请选择分组: 全部	•	输入服务器IP/名称进行搜索	Q
输入服务器IP/名称进行搜索	Q		
10.35.6.148 (a27d11008.cloud.d1			
10.35.6.84 (a27d08010.cloud.d08			
10.35.6.80 (a27d08101.cloud.d09			
10.35.6.146 (a27d11101.cloud.d1			
10.35.6.145 (a27d11014.cloud.d1			
10.35.6.83 (a27d08206.cloud.d10	-		
当前选中0条		共有0条	
		确认	取消

4.4.2 主机入侵检测

4.4.2.1 查看文件篡改事件记录

操作步骤

- 1. 在服务器安全 > 主机入侵检测页面,单击文件篡改。
- 2. 查看文件篡改事件记录,如图 4-15: 文件篡改事件记录所示。

图 4-15: 文件篡改事件记录

Ι±	几入侵检测								
分类	文件篡改 异常进	星 异常网络主接	可蜒端口监听						
状态	: 全部 ¥ 服	务器IP,支持模糊	直询 文件目录 , 支持	横湖查询 变素	时间: 起始时间	至终止时间	按案		
	服务器IP	区域	文件目录	变动类型	变动时间	原始文件创建时间	变动详情	状态	操作
	0.05.520	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:06	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理
	308409	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:13	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理
	303.04	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:07	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理
	10.00	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:06	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理
	20144	缺省机房	/etc/init.d/mysql	文件修改	2017-07-26 01:26:10	2017-06-23 21:56:03	遼文件md5:176bd7a935c0ebb8b308f65a4db3d441 修改后文件md5:176bd7a935c0ebb8b308f65a4db3d441	已标记处理	-

4.4.2.2 查看异常进程记录

操作步骤

- 1. 在服务器安全 > 主机入侵检测页面,单击异常进程。
- 2. 查看异常进程记录,如图 4-16:异常进程记录所示。

图 4-16: 异常进程记录

主机。	入侵检测								
分类:	文件篡改 异常进程 异常网络连	接 可疑端口监听							
状态:	全部 v 服务器IP , 支持撤	期查询 进程路径,支持模拟	期查询 启动时间: 起始	时间至	终止时间	搜索			
	服务器IP 区域	进程路径	进程类型	启动时间	文件大小	文件hash值	文件创建时间	状态	操作
	20240	/etc/rc.d/init.d/selinux	gate_backdoor_file	2017-07-17 17:30:17	8464	4a8e5735fefe17ec4410e5e4889dca3a	2017-06-29 16:15:44	未处理	标记为已处理
	10.00.025	/usr/bin/pamdicks	rootkitminer_file	2017-07-15 17:54:37	11128	f679115e75735c2de5937448b30242b8	2017-07-11 21:19:03	未处理	标记为已处理
	3538.60	/boot/vfpjyckqma	gate_xordoor_file	2017-07-15 19:50:06	8464	e0bc372135f57507a7689bd3069c705a	2017-06-29 16:15:56	未处理	标记为已处理
	0.08.63	/etc/rc.d/init.d/selinux	gate_backdoor_file	2017-07-17 17:30:17	8464	4a8e5735fefe17ec4410e5e4889dca3a	2017-06-29 16:15:44	未处理	标记为已处理
	30340	/usr/bin/pamdicks	rootkitminer_file	2017-07-15 17:54:37	11128	f679115e75735c2de5937448b30242b8	2017-07-11 21:19:03	未处理	标记为已处理
	103.61	/boot/vfpjyckqma	gate_xordoor_file	2017-07-15 19:50:06	8464	e0bc372135f57507a7689bd3069c705a	2017-06-29 16:15:56	未处理	标记为已处理

4.4.2.3 查看异常网络连接记录

操作步骤

1. 在服务器安全 > 主机入侵检测页面,单击异常网络连接。

2. 查看异常网络连接记录,如图 4-17:异常网络连接所示。

图 4-17: 异常网络连接

主机	1.入侵检测							
分类:	文件篇改 异常进程 异常网络	路主接 可疑调口监听						
状态:	全部 ▼ 服务器IP,支持	機糊查询 进程路径,支	持模糊查询 连接时间:	起始时间	至终止时间 機次			
	服务器IP 区域	事件类型	连接时间	对应进程	进程路径	连接详情	状态	操作
	10.00.04.0	Connect Internet	2017-06-16 17:42:25	7116	/apsara/cloud/app/tianji/TianjiClient#/proxyssl/237727/proxyssl	访问源:10.35.6.90:44231 访问目标:127.0.0.1:12344	未处理	标记为已处理
	H.H.HAD	Connect Internet	2017-06-16 17:42:31	7223	/apsara/cloud/app/tianji/TianjiClient#/p2p_worker/237727/p2p_worker	访问源:10.35.6.90:29686 访问目标:127.0.0.1:7070	未处理	标记为已处理
	N.N.M.F	Connect Internet	2017-06-16 20:13:26	3727	/apsara/cloud/app/tianji/TianjiClient#/proxyssl/237727/proxyssl	访问源:10.35.6.74:3078 访问目标:127.0.0.1:12344	未处理	标记为已处理
	10.20.207.0	Connect Internet	2017-06-16 20:13:32	3784	/apsara/cloud/app/tianji/TianjiClient#/p2p_worker/237727/p2p_worke r	访问源:10.35.6.74:12384 访问目标:127.0.0.1:7070	未处理	标记为已处理

4.4.2.4 查看异常端口监听记录

操作步骤

- 1. 在服务器安全 > 主机入侵检测页面,单击可疑端口监听。
- 2. 查看异常端口监听记录,如图 4-18:异常端口监听记录所示。

图 4-18: 异常端口监听记录

主机	入侵检测								
分类:	文件篡改 异常进程	异常网络连接 可数	路端口监听						
状态:	全部 • 服务器	IP , 支持模糊查询	総口	进程路径,支持模糊道	脑 变动时间: 起始时间	至终止时间按定	ξ.		
	服务器IP	区域	监听端口	开始监听时间	对应进程	进程路径	说明	状态	操作
	35/264-77	缺省机房	37308	2017-06-29 16:28:01	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	3636.677	缺省机房	51015	2017-06-29 16:28:03	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	1000.000	缺省机房	53638	2017-06-29 16:28:04	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	3628.613	缺省机房	45564	2017-06-29 16:28:01	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	0.00.001	缺省机房	53693	2017-06-29 16:28:01	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	36(5)+13	缺省机房	47402	2017-06-29 16:28:05	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理

4.5 安全审计

安全审计是指由专业审计人员根据有关法律法规、财产所有者的委托和管理当局的授权,对计算机 网络环境下的有关活动或行为进行系统的、独立的检查验证,并作出相应评价。在管理员需要对系 统过往的操作做回溯时,可以进行安全审计。

安全审计是一项长期的安全管理活动,贯穿云服务使用的生命周期。云盾的安全审计能够收集系统 安全相关的数据,分析系统运行情况中的薄弱环节,上报审计事件,并将审计事件分为高、中、低 三种风险等级,管理员关注和分析审计事件,从而持续改进系统,保证云服务的安全可靠。

4.5.1 审计一览

审计一览页面提供云平台日志趋势、审计事件趋势、审计风险分布、危险事件分布四种报表。四种 报表分别统计一周内发生的日志个数、事件个数、事件级别、事件类别分布,以趋势图或饼图的方 式直观地呈现给管理员,便于分析云服务面临的风险趋势。

- 云平台日志趋势的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的日志个数。通过云平台日志趋势,管理员可以了解系统产生的日志数量是否正常。
- 审计事件趋势的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的审计事件 个数。通过审计事件趋势,管理员可以了解系统产生的审计事件数量是否正常。
- 审计风险分布的数据是一周内高风险、中风险、低风险事件的个数。通过审计风险分布,管理员可以了解系统产生的审计事件级别是否正常。
- 危险事件分布的数据是一周内不同事件类型占总事件的比例。通过危险事件分布,管理员可以了 解什么类型的审计事件占比较多,识别高风险问题,做好预防措施。

在**安全审计 > 审计一览**页面,设置查询时间,单击**查询**,查看审计报表,如图 4-19:审计一览页 面所示。

说明:

默认情况下,显示一周的审计报表。

图 4-19: 审计一览页面



4.5.2 审计查询

审计查询页面可查看日志创建时间、日志内容、日志类型、事件类型、风险级别。日志的内容为对 应模块的日志调试信息。

送明:

如需了解日志的具体含义,请联系运维人员咨询相关内容。

审计查询生成的过程:将安全审计模块收集到的日志匹配审计规则,如果日志内容能匹配任意一条 审计规则的正则表达式,就会上报审计事件。用户可以根据需要在**安全审计 > 策略设置 > 审计策** 略查看默认的审计规则,也可以自己定义审计规则的正则表达式。

在安全审计 > 审计查询页面,设置查询条件,查看相关审计日志记录。

4.5.3 原始日志

原始日志页面中可查看应用在运行时产生的必要的调试信息,管理员可以根据这些调试信息定位系 统出现的故障。

单击**安全审计 > 原始日志**进入**原始日志**页面,选择审计类型、审计对象,通过输入查询关键字及起 始时间来设置查询条件,单击**查询**,查看原始日志记录。

4.5.4 策略设置

4.5.4.1 添加审计策略

背景信息

审计策略是正则表达式规则,当日志记录中的某个字符串匹配审计规则的正则表达式,就会上报审 计事件。

正则表达式描述了一种字符串匹配的模式,可以用来检查一个串是否含有某种子串。例如: ^\d{5, 12}\$ 表示匹配 5 到 12 位数字, load_file\(表示匹配 load_file(字符串。

安全审计模块根据发生审计事件时日志中输出的字符串,定义了默认的审计策略,管理员也可以根据受到攻击时日志输出的字符串自定义审计策略。

操作步骤

- 1. 选择策略设置 > 审计策略,选择审计类型及审计对象,可以进行审计策略的查询。
- 2. 单击新增,在新增规则对话框中输入相关信息可添加审计策略,如图 4-20:新增规则对话框所示。

图 4-20: 新增规则对话框

新增规则			×
策略	名称 请	输入策略名称	
审计类型:	数据库	 ▼ 审计对象: 全局 ▼ 操作类型: 阿萨德 	•
操作风险级	吸别: 高风	险事件 ▼ 是否告警: 告啓 ▼	
过滤条件:	:		
发起者	等于 🔻	输入发起者关键字 x +	
目标	等于 🔻	输入目标关键字 x +	
命令	等于 🔻	输入命令关键字 x +	
结果	等于 ▼	输入结果关键字	
原因	等于 ▼	输入原因关键字	
备注	备注		
			-
		添加	取消

3. 配置审计规则参数。

添加审计策略后,在指定的审计类型、审计对象、风险级别的审计日志中,如果出现匹配正则 表达式的内容,会发送一封告警邮件给下文中设置的报警接收人。例如设置了正则表达式:*hi hello*,并设置了ECS日志类型、登录尝试事件、高风险事件,那么在ECS日志中,如果出现hi或 者hello,会上报一个尝试登录高风险的审计事件,并发送告警邮件给告警接收人。

4.5.4.2 添加审计类型

操作步骤

1. 在策略设置 > 类型设置页面可以查看已经存在的审计类型列表。

- 2. 单击新增,在新增事件类型对话框中设置要添加的事件类型。
- 3. 单击确定,完成添加审计类型。

4.5.4.3 设置报警接收人

设置报警接收人的邮箱,在发生审计事件后,会将事件上报到告警人的邮箱。

操作步骤

 在安全审计 > 策略设置 > 告警设置页面,单击新增,弹出新增报警接收人对话框,如图 4-21:新 增报警接收人对话框所示。

图 4-21: 新增报警接收人对话框

新增报警接收人		×
邮箱	请输入有效邮箱eg:xxx@xxx	
姓名	请输入名称	
审计类型	全部	•
审计对象	全部	v
风险等级	全部风险	v
		确定取消

2. 在邮箱的输入框中,输入报警接收人的邮箱地址,在风险等级的下拉框中,选择风险等级。

3. 单击确定,添加报警接收人。

4.5.4.4 管理事件日志存档

操作步骤

选择策略设置 > 存档管理,可以查看存档列表,如图 4-22:存档管理页面所示。

图 4-22: 存档管理页面

市计策略 类型设置 告警设置 存档管理 导出管理				
审计类型: 全部 ▼ 归档类型: 全部 ▼ 发现时间: 起始时间 16	^ : 30 ^ 至 终止时间 16 ^ : 30 ^ 查询			
文件名	摘要值	归档类型	创建时间	操作
OPS/2017-07-17/OPSOPS-20170717162815.gz	7f9d4fc7b56d140c5b72c17798203af6	事件归档	2017-07-17 16:28:15	下载
OPS/2017-07-17/OPSOPS-20170717162815.gz	76cdb2bad9582d23c1f6f4d868218d6c	日志归档	2017-07-17 16:28:15	下载
OPS/2017-07-17/OPSOPS-20170717162815.gz	69a23bbea7c48baa20edbede9a7af337	事件归档	2017-07-17 16:28:15	下载

送 说明:

在输入框输入起始时间、终止时间可以根据发现时间段进行筛选。

4.5.4.5 管理导出任务

操作步骤

1. 选择策略设置 > 导出管理,可以查看已创建的导出任务,如图 4-23: 导出管理页面所示。

图 4-23: 导出管理页面

审计策略	类型设置	告警设置	存档管理	导出管理					
创建时间			Ę	出任务id	任务类型	过速条件	任务状态	格式	操作
2017-07-27 1	5:30:04		1	0302	审计事件导出	logType: 1 sourceid: q: name: 全部實證 from: 1501054260000 to: 1501140660000	0 6533	log	下载 翻除
2017-07-27 1	5:29:20		1	0301	日志导出	logType: 1 sourceld: 10155 q: name: 全部面询 from: 1501139700000 to: 1501140600000	0 6830	log	下载丨翻桥
								共有2条,每页5	显示:20条 《 < 1 > 》

2. 导出任务完成后,选择该导出任务,在操作栏单击**下载**可下载审计日志文件。

3. 选择导出任务,在操作栏单击删除可删除该导出任务。

4.6 系统管理

系统管理模块作为云盾安全中心不可或缺的部分,为管理员调整系统人员、配置提供了极大的便利。

系统管理主要包含四个部分:

- 用户管理:用于管理专有云云盾配套的阿里云账号。
- 情报同步:用于查看云盾情报库的更新方式及更新情况。

- 告警设置:用于配置各类安全事件、紧急信息等的告警方式以及联系人信息。
- 全局设置:用于配置云盾相关的网段信息,包括流量监控网段和区域网段两部分。

4.6.1 管理阿里云账号

操作步骤

 在系统管理 > 阿里云账号管理中,可以查看修改系统绑定的阿里云账号信息,如图 4-24: 阿里云 账号管理页面所示。

云盾中的资产均与阿里云账号绑定,请谨慎修改。

图 4-24: 阿里云账号管理页面

用户管理 阿里云乐导作	范围				
阿里云账号	甩户ID	Access Key	Access Secret		弱作
hh	1519714049632764	KIND MIRENAL	•••••	炒改	洋倩
			共有1条,每页显示:10条 🛛 <	1 >	>

2. 单击修改,弹出修改对话框,信息修改后单击确定,完成修改,如图 4-25: 账号修改对话框所示。

图 4-25: 账号修改对话框

帐号修改	\times
阿里云帐号	2018/06/06
用户ID	
Access Key	40780009804
Access Secret	•••••
	2014
	AK/N

3. 单击**详情**,查看阿里云账号详细信息,包括许可到期时间、安骑士许可数目,如图 4-26: 账号详 情所示。这些信息均是通过配置的用户ID、Access Key信息获取。

图 4-26: 账号详情

帐号详情		×
阿里云帐号:	1.00.00.004	
用户ID:	1-0020-01000-000	
Access Key:	x31300604	
Access Secret:	*****	
License到期时间:	2020-05-16	
安骑士license数目:	0	
		确定

4.6.2 告警设置

告警设置功能包括设置告警联系人和按照不同的安全事件设置告警通知方式。当发生对应的安全事件时,系统自动上报告警,以便管理员了解系统发生的安全事件。

4.6.2.1 设置告警联系人

背景信息

告警联系人是告警消息的接收人,告警消息的发送方式有手机短信和邮件。当监控数据满足报警规则时会发送告警信息给报警联系人。

操作步骤

1. 在系统管理 > 告警设置 > 告警联系人页面,单击添加联系人,如图 4-27:告警联系人页面所示。

图 4-27: 告警联系人页面

O ERESTO				<u>ه</u> .
	1 TEOR			
8	NEWE DEWSA			
G 8094				BARKA.
0 🚥	8:6A28	¥6.	Enal	80
(*) BR	ba	10000	har and the second	46 I DH
D 84				80.838
• 9880				
© 004958				I
D and the				I
6 B6512				I
- 8°88				I
H mron				I
- 5400				I
A #*##				I
0 8600 ·				I
@ 1028				I
0 1002				

2. 填写联系人信息,单击确认,添加告警联系人。

添加后的告警联系人可以通过页面上的编辑和删除按钮,进行相关联系人信息的编辑或删除。

4.6.2.2 设置告警信息

背景信息

告警设置可以对安全事件(登录安全-异地登录)、紧急事件告警(网页篡改、肉鸡行为、爆破成 功、发现后门、被DDoS攻击、黑客访问、异常网络连接和未授权下载)、攻击告警(暴力破解攻 击、高级威胁攻击和Web应用攻击)、弱点告警(发现弱口令、发现漏洞和应用配置项隐患)、情 报信息告警(人员信息泄露、重要漏洞、应急响应和行业新闻)进行告警,告警方式包括手机和邮 件。

在系统管理 > 告警设置 > 告警设置页面,选择每个安全事件的通知方式单击确认,如图 4-28:告
 警设置页面所示。

图 4-28: 告警设置页面

0 #####0			<u>ይ</u>
- 6990	1 894 X		
S en			
D. Koto	512.60		
۵ 🚥		0.48	0.48
() R A	18	適応が式	
D 84	建资业单位建建 排与不在现代和企业	0 #45	0.84
· 9287	198189	適応方式	
0 contaile Di antaire	現代開発 現代出産業務長に、会社会のの以外規模式(中心に)の定め代码	D 945	0.894
6 mmim	月後日 また2月17月10日のいかけた後年時1月、 米田田王王が必然市場的からう	0.45	0.84
- 8/88	926) Retornenent, næs-khtalendo	0.945	0.04
• SARE	9880) 2004-001.882102009800	0.945	0.64
2 8/82	MDOWER IL_MEREMONNE	0.445	0.814
A neca	TUNUGRADADADA REAL	0.45	0.04
0 1.94R	■第四本本書 11月7日11日本書品の日本の支援の月本の書法メ	0.945	0.64

4.6.3 全局设置

云盾安全中心提供全局设置,供管理员对云盾流量安全监控模块的网段范围以及安骑士模块上报检 测的区域进行设置。

📙 说明 :

流量安全监控模块的采集网段设置和区域设置中如果配置同一网段,则区域信息必须一致。

4.6.3.1 流量采集网段设置

网段设置主要针对流量安全监控模块进行网段配置,并且支持更改监控的网段范围,方便管理员根据需求调整监控的网段。配置的监控网段仅对所属区域机房生效。

网段设置更改后立即对流量监控生效,不需要管理员进行其他操作。

4.6.3.2 添加流量采集网段

操作步骤

在系统管理 > 全局设置 > 流量采集网段设置中,单击添加,弹出添加监控网段对话框,如图
 4-29:添加监控网段对话框所示。

图 4-29: 添加监控网段对话框

添加监控网段		×
网段 区域	请输入监控网段,例如:10.158.192.0/24	•
		政 演

- 2. 填写网段,要求必须是合法网段,并且不允许重复添加。
- 3. 选择所属区域。
- 4. 单击确定,完成添加。

4.6.3.3 管理流量采集网段

操作步骤

1. 选择区域,输入查询网段,单击查询,查看流量采集网段信息,如图 4-30: 全局设置页面所示。

图 4-30: 全局设置页面

生用必要		
REAL ROOM		
88 • 80.000 • 88		-
Rin	2.16	84
1010.00.000	Factor .	#31 \$54
100.00.00	1983	172x 850
100000	Farch .	1702 850
1.75.00.075	1000	1900 BDH
100.0010	11-12	1922 BDH
10000		1922 80e
1.12.10.00	1154	1722 859
10.00.000.000		1721 850
100.000		1721 850
10.08 (H.10)	10.00	1702 854
		月月10日, 40万世月:10日

2. 选择需要的网段,执行如下操作:

• 修改流量采集网段

单击**修改**,弹出**修改网段**对话框(只支持区域修改),修改所属区域后,单击**确定**,完成修改。

• 删除流量采集网段

单击删除,可以删除配置的监控网段。

4.6.3.4 区域设置

区域设置主要针对不同机房安骑士客户端的区域检测,配置后,所属区域对应网段下的安骑士主机 上报后,可以自动检测匹配对应的机房。

送 说明:

区域设置支持更改已配置网段的所属区域,但是更改后必须在资产总览中批量修改对应网段资产的 区域。

4.6.3.5 添加区域网段

操作步骤

 在系统管理 > 全局设置 > 区域设置中,单击添加按钮,弹出添加网段对话框,如图 4-31:添加网 段对话框所示。

图 4-31: 添加网段对话框

添加网段		×
网段 区域	请输入网段,例如:10.158.192.0/24	
	神 道	取消

- 2. 填写网段,要求必须是合法网段,并且不允许重复添加。
- 3. 选择所属区域。
- 4. 单击确定,完成添加。

4.6.3.6 管理区域网段

操作步骤

1. 选择区域,输入查询网段,单击查询,查看区域网段信息,如图 4-32: 区域设置页面所示。

图 4-32: 区域设置页面

全局设置		
RARRER SEARCH		
10 • 10 • 10 • 10	•	
84	RD	80
Terta	101003-0029	9.0. I 899
Testa .	0.7003-0.00	93 I 89
Conta de la conta	1000000	0.0 309
Testa (0.0000.000	9X 89
0.04	100.00.00	00 20
	10.000 000	5X 59
10.04	10000-00	04 20
	10,000,000	5X 50
	0.000.000	94 X0
0.00	101000-010	9X (89)
		月後10歳、報用型目:10歳 * (11歳 * * *

- 2. 选择需要的网段,执行如下操作:
 - 修改区域网段

单击**修改**,弹出修改网段对话框(只支持区域修改),修改所属区域后,单击**确定**,完成修改。

• 删除区域网段

单击删除,可以删除配置的网段区域。