DAS-SECUrity 支呈中国 恒态势感知 APT 配套人工服务 安 V5.0 恒态势感知 APT 配套人] L服务购买 B 安 文档版本: **01** 发布日期: 2023-06-14



www.dbappsecurity.com.cn



本文中出现的任何文字描述、文字格式、插图、照片、方法等内容,除另有特别注明,版权均属杭州安恒信息技术股份有限公司(简称"安恒信息")所有,受到有关产权及版权法保护。任何个人、机构未经安恒信息的书面授权许可,不得以任何方式复制或引用本文的任何片段。

经授权使用本文中内容的的单位或个人,应在授权范围内使用,并注明"来源:安恒信息"。违反上述声明者,安恒信息保留追究其法律责任的权利。

除杭州安恒信息技术股份有限公司的商标外,本手册中出现的其他商标、产品标识及商品名称,由各自权利人拥有。



文档说明

产品名称	安恒态势感知 APT 配套人工服务				
适用平台/版本	V5.0				
拟制人	评审组				
发布人	备注 受控				

修订记录

日期	修订版本	修改记录	修改人
2023-06-14	01	初次发布	



目 录

1. 安恒态势感知 APT 配套人工服务购买指导说明	1
1.1 说明	1
1.2 操作步骤	1
1.3 授权许可说明	5
2. 关于 SSH 登录安恒态势感知 APT 配套人工服务后台的补充说明	6
2.1 说明	6
2.2 操作方法	7



杭州安恒信息技术股份有限公司

L



1. 安恒态势感知 APT 配套人工服务购买指导

说明

1.1 说明

安恒态势感知 APT 配套人工服务采用大数据分析技术架构,为用户提供全局安全态势感知能力。构建

7*24h 持续主动、有效闭环的安全运营体系。

本文档主要介绍在市场如何进行购买安恒态势感知 APT 配套人工服务指导说明

1.2 操作步骤

1. 在市场搜索安恒态势感知 APT 配套人工服务软件镜像,选择对应的规格和推荐配置,确认购买方式进行

购买

姚 华为云	云商店 关于我们 商品分类。 热门专区。	最新活动 ~	解放中心 ~ 免難成用	C	天家中心 堂家中心 ~ 二 12 防約车	dbappsecurity 000 ~
	云南店 > 安全 > 安全服务 > 安信志势感知APT能在人工服务					
	AURACE 11 100 - 400 - 100 - 100 - 100 - 100 - 200	AILPHA	安恒态势感知APT配套人工服务 FF音率高 此意思为实际态势要犯APT配著的人工服务	+ 8 5		
	Annual and a set of the set of th	8tt	¥ 6923			
		1078	安福人にPHA大教課智報安全分析平台記書人工課券 安福明如APT攻击预奮平台記書人工課券			
		的天安里	- <u>1</u> +			
		购买方式	徽次			
						٠
	商品详情 商品规指定价 用户案例	服务支持	评价与问答			免 费 试 用
	商品亮点 - 全部的武振谋率与分析 - 开始的安全能力服合 - 深度的直影检测能力		₹555. Q ¥88	a		© 3
	·自动化安全研判则应 商品参数 交付方式 人工服务		MAS10111 (小) 1973			

2. 在自定义购买界面添加一块数据不小于 500G 的数据盘

系统盘	高IO ▼ 60 + GB IOPS上限1,560, IOPS突发上限5,000 ⑦
数据盘	○ 高IO ▼ - 500 + GB IOPS上限4,200, IOPS突发上限5,000 数量 - 1 + 展开∨
	④ 增加一块数据量 您还可以挂载 22 块磁盘 (云硬盘) 购买包年/包月弹性云服务器时添加的非共享盘磁盘不支持单独退订和续费,非共享的数据盘不支持挂载到其他云服务器。Linux实例添加的数据盘可使用脚本向导式初始化。\$

3. 自定义购买界面配置安全组规则

入方向规则中添加 TCP 443 和 UDP 514 端口的规则

く 単性云服务器	自定义购买快速购买									
① 基础配置 ———	- 2 网络配置 3	高级配置	- ④确认配置							
网络	vpc15bc99679ee64762(192.1 如需创建新的虚拟私有云,您可	68.0.0/16) 🔻 (前往控制台创建。	c subnet15bc996844a	a14954(192,168.0 💌	C 自动分配IPt	55 <u>1</u> •	可用私有IP数量	ŧ250个 ⊘		
扩展网卡	 · ·	011块网卡								
安全组	安全組 Sys-default (4798fa97-a31f-40fc-933d-5cc34bb8b28d) ● ○ 新建安全組 ⑦ 安全組製(防)火爆功能,是一个逻辑上的分组、用于设置网络访问控制, 谐铸等所选安全组已故通22講口 (Linux S5H登景), 3389端口 (Windows选择登景)和 ICMP 协议 (Ping) 配置安全组规则 展开安全組規則 >									
< Syn-default 基本信息 人方向规则 出	方向规则 关联实例						日春入規則	口导出规则		
通加規則 快速通加規則	· · · · · · · · · · · · · · · · · · ·	a.						С		
1 100000 7 ②		类型	源地址 ⑦		描述	1	9/1			
□ 全部		IPv4	Sys-default ⑦				sex seni ane			
CP : 22		IPv4	0.0.0.0/0 ⑦		Permit default Linux SSH po	rt. I	彩衣 裁制 删除			
TCP: 443		IPv4	0.0.0.0		122		8改 复制 副额			
UDP:514		IPv4	0.0.0.0/0 ③		-		9改 夏明 副除			

4. 设置 root 用户密码

く 弾性云服务器	自定义购买 快速购买
(1) 基础配置 ———	
云服务器名称	SOC
登录凭证	密 <mark>码</mark> 密钥对 创建后设置
用户名	root
密码	请牢记密码,如忘记密码可登录ECS控制台重置密码。
确认密码	

5. 确认购买的配置无误后,点击立即购买

く 弾性云服务器	自定文购买 快速	9 				English	inor 🛇 zere
① 基础配置 ——	- ② 网络配置						
₽.B.	基础配置 // 计规模式 规格 数项曲	包年/包月 通用计算型 52.slarge 2 49CPU5 8GB 1 块 案iO, 500GB	2% R\$	上海二 最大20个日志源(全国网络9合全位日志等计平均数件概念)	可用区。 系统曲	可用区1 面D,69G8	
	网络配置 2 建筑私寄云 潮性公园中	vpc15bc9675ee64762(192.168.0.0/16) 全改志のGP 计高方3C 的年間计算 専茂 5 Mbit/s	安全组	Sys-delault	主阿卡	subnet15bc996844a14954(192.168.0.0)24)	
	RQEE 2	500	BRAZ	電荷	云服务器组	-	
购买时长	1 2	3 4 5 6 7 8 91	1月 1年 2年 34	ŧ.			
购买数量 协议	 日动绕器 ② 1 + 労已经闲读并闻机 	》原参可以创建200台云服务器。由请更多云服务器和影响等 奏 (现金负责声明)	由申请扩大党额。				() () () () () () () () () () () () () (
							0
配照费用 ¥6,870.00 (参考价格,具体和表演以所等	已皆:¥1,374.00) 为难。了解计费详情						上一步 立即购买

6. 购买后在主机控制台使用控制台提供的 VNC 方式登录云主机后台,检查数据盘大小,数据盘用于存储

安恒态势感知 APT 配套人工服务数据

确认在云主机后台使用 lsblk 命令能看到新增的这块新增的大容量数据盘



HUAWEI	华为云 控制台										
≡	鼍 发送远程命令 ▼	🖵 Ctrl+Alt+Del	本地鼠标	日 复制粘贴	全屏模式						
٢				[root@ah [root@ah	soc ~]# soc ~]#	b 11 <i>c</i>					
ස				NAME Vda	500 1# 15	MAJ:MIN 253:0	RM Ø	SIZE 60G	RO Ø	TYPE disk	MOUNTPOINT
,000				l-vda1 `-vda2	oc-lu data	253:1 253:2 252:0	0 0 0	40G 20G 20G	0 0 0	part part	/
٢				vdb [root@ah	soc ~]# _	253:16	0	500G	0	disk	X
0											
0											
\odot											

联系安恒技术服务热线 4006059110 进行云主机数据盘磁盘在线扩容操作

服务方式:远程支持服务

客服电话: 4006059110 转7

邮箱: 400@dbappsecurity.com.cn

7.在 控制台,复制云主机的弹性公网 IP 地址,打开浏览器,输入 https:// 弹性公网 IP 地址,进入

WEB 界面

华为云 拉制台	♥ 上間	- •				設施の	豊用中心 う	127 工单	企业	开发工具	留宴	支持与服务	中文 (简体)
云服务離控制台		弹性云服务器 ③										☞ 最新动态	◎ 使用指
· (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		 或邀您参加P#位云服务器使用体验调研,您重要的意 	见和建议是我们持	续提升产品体验的源动力,	感谢您的参与!								
专属主机		开机 关机 重音运研 更多	•						1				C
裸金属服务器		默认按照名称搜索											
云硬盘		□ 名称/ID	道控	可用区 ▽	秋态 ⑦	规格/鏡像	IP地址		计费模	式了	企业项	i B	标签
专属分布式存储		ahsoc	3	可用区1	 遗行中 	4vCPUs 8GB s2.xlarge.2	119 37 (谢性公网	技需计 2020/1	费 1/13 12 10 0	defaul	t	-
镜像服务		200.570072804996-0096-406880518				MH_30C_V3.0_K30247_202011	192.100.1.211	(42344)	10107	1112 12 10 10 10	30 		
弹性伸缩													

系统检测完毕,发现2个异常,请	讀 看 检 查 结 果 及 描述 , 并 按 处 理 意 见 修 复 。	
检查内容	检查结果及描述	处理意见
许可文件检测	许可文件不存在	请导入许可文件,或联系技术支持。
日志审计系统线程检查	系统未发现服务进程,请启动服务	请启动日志审计系统服务。 修复
目录 / 空间检测	目录/,空间已经使用8%	
目录 /data 空间检测	目录/data,空间已经使用13%	

了安恒信息

点击许可导出,下载 license.RaC

31 37-明御综合日志审计	★ 下载内容 × +	
\leftrightarrow \rightarrow C (Shrome c	ome://downloads	
下载内容	Q、 搜索下载内容	
	今天	
	license.RaC https://1 ⁻ 37/soc?action=export 在文件夹中显示	

1.3 授权许可说明

购买完成后安恒态势感知 APT 配套人工服务实例会自动运行,需要购买许可方能使用。

license 购买流程 (购买前如有疑问请咨询客服 [客服电话: 4006059110]):

1、根据您单位情况,选择合适的规格,并购买支付;

2、支付成功后联系客服核对信息,验证支付;

3、登录安恒态势感知 APT 配套人工服务的 web 管理界面,点击"许可导出"按钮,会自动下载 license.RaC



文件;

4、在交付中心提交需求,上传 license.RaC 文件 (由于上传不支持此后缀名,请先压缩为.zip 或.rar 文件 上传) ;

5、服务商在交付中心提供许可文件,下载并解压出 license.RaU 文件;

6、在安恒态势感知 APT 配套人工服务的 web 管理界面,点击"许可导入"按钮,上传 license.RaU 文件;

7、导入成功后可以看到相应的 license 注册信息,请核实,如果有问题请联系客服。

8、如果导入失败,请使用谷歌浏览器重新导入许可,如果有问题请联系客服。

注意:购买许可前,请先购买安恒态势感知 APT 配套人工服务软件镜像

2. 关于 SSH 登录安恒态势感知 APT 配套人工 服务后台的补充说明

2.1 说明

由于安恒安恒态势感知 APT 配套人工服务镜像安全策略 SSH 服务设置了 root 用户不能直接 SSH

了安恒信息

登录,必须需要先创建普通用户登录 SSH 后再 su - root 切成 root 用户

2.2 操作方法

1、登录云服务器控制台,使用控制台提供的 VNC 方式登录

登录服务器控制台,在弹性云服务器界面选择对应的云主机,点击远程登录

-	华为云 12916	Q 上雨:					RE Q	素用中心 読録 工単	企业 开发工具	新菜 支持与服务	中文 (間体)	i 🖉
≡	云服务器控制台		弹性云服务器 ⑦							マ 最新功志	19 使用编辑	购买弹性云服务量
8	想范 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)			见和建议是我们转	懷護升产品体验的漂动力。	受制记的参与1						×
M ©	安屋主机		円町 天町 重加定明 更多 時にはAFFでかかか。	•							C	
Θ	云硬盘		名称/ID	监控	可用区 🏹	秋志 🏹	现档/销量	IP地址	计费模式 🍞	企业项目	标签	操作
0	安羅分布式存储 機像服务	•	D Million (M) with arts (c) Million.	•	190	•	44295, 838, 818982 44, 501, 511, 500,007, 20001	183429-081/A. 16781-9-555	按需计器 2020/11/09 16:25:2.	default		BRAR BS -
4	弹性伸缩											
0	面例对											
۲	云服务雕组											
	云煤云服务器 NEW	8										
	云偏份	ē.										
	云服务器备份											
	云硬盘备份	e										
	弹性负载均衡	2										
	弹性公网中	æ										e
	安全相	2										9
												•
												8

使用控制台提供的 VNC 方式登录



了安恒信息

⇒

2、 输入云服务器的 root 账号和 root 密码登录

🜺 AH SOC × + ■ console.huaweicloud.com/ecm/?instanceId=475cdcaa-9492-40d7-ae76-bd7dd3aeca? > C 华为云 控制台 Ξ 電 发送远程命令 ▼ Ctrl+Alt+Del 本地鼠标 ☐ 复制粘贴 全屏模式 6 CentOS Linux 7 (Core) Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64 B ah-soc login: root Password: MA Last login: Mon Nov 9 16:35:37 on tty1 Welcome to Huawei Cloud Service 6 [root@ah-soc ~]# LANG=en_US.UTF-8 [root@ah-soc ~]# useradd centos 0 Creating mailbox file: File exists [root@ah-soc ~]# passwd centos Changing password for user centos. 0 New password: \odot Retype new password: passwd: all authentication tokens updated successfully. [root@ah-soc ~]# usermod -G wheel centos [root@ah-soc ~]# _ 1

安恒信息

并输入如下命令

LANG=en_US.UTF-8

useradd centos

passwd centos

#给 centos 用户设置密码

usermod -G wheel centos

并将 centos 用户加到 wheel 组

3、使用 SSH 登录工具例如 SecureCRT 通过 centos 用户登录云主机的 SSH 后台

Enter Secu	re Shell Password	×
centos@119 enter a pass	requires a password. P word now.	lease OK Cancel
Username:	centos	
Password:	•••••	
Save pas	sword	Skip
New S	ession Wizard	name or IP address of the remote host?
*	The usernam	e can be left blank.
~	The usernam Hostname:	e can be left blank.
~	The usernam Hostname: Port:	e can be left blank.
~ ~	The usernam Hostname: Port: Firewall: Username:	e can be left blank.

了。安恒信息

4、登录成功后使用 sudo su - root 命令切换成 root 用户

Authorized users only. All activity may be monitored and reported. Last login: Mon Nov 9 16:42:26 2020 from 61.164.47.200 Welcome to Huawei Cloud Service [centos@ah-soc ~]\$ LANG=en_US.UTF-8 [centos@ah-soc ~]\$ sudo su - root [sudo] password for centos: Last login: Mon Nov 9 16:36:48 CST 2020 on tty2 [root@ah-soc ~]# [root@ah-soc ~]#