

# 阿里云 vDAS 部署实施指导书



深信服科技股份有限公司



		修订员	〕史		
编号	修订内容简述	修订日期	修订前版本号	修订后版本号	修订人
1	阿里云 vDAS 部署实施指导 书	20191031	1.0	1.0	Chenke
2					
3					

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容,除另有特别注明,版权 均属深信服所有,受到有关产权及版权法保护。任何个人、机构未经深信服的书面授权许可,不得 以任何方式复制或引用本文的任何片断。





# 目录

第1章	亡 儒才	专背景	4
第2章	ē 部署	暑概述	4
2.	1 阿里	<b>星云平台特性描述</b>	4
2.	2 镜像	象获取	4
2.	3 部署	署方式	4
2.	4 资源	原配置	4
2.	5 授校	双方式	5
第 <b>3</b> 章	育 部署	署指导	5
3.	<b>1</b>	平台配置	5
	3.1.1	创建 ECS 虚拟机	5
	3.1.2	配置网络和安全组	8
3.	2 网络	各配置	11
3.	<b>3</b> 登陆	击控制台	12
3.	4 云约	且件授权配置	12
	3.4.1	在线授权	13
	3.4.2	申请试用	14
	3.4.3	vDAS 授权说明	14
3.	5 数排	居库审计功能配置	16
	3.5.1	用户环境与需求	16
	3.5.2	配置步骤	16
第4章	亡 常见	1问题	





# 第1章 需求背景

目前大量用户为了减轻运维和数据不落地的需求采用了公有云托管业务,但是一直以来公有云 架构的安全防护方面一直处于劣势,需要借助第三方安全虚拟化组件来补齐短板。依托该需求深信 服推出了基于阿里云的数据库审计解决方案,实现阿里云上数据库审计的场景需求,解决客户痛点。

# 第2章 部署概述

## 2.1 阿里云平台特性描述

- ◆ 底层架构为 KVM
- ◆ 能够自定义上传镜像格式包括 raw
- ◆ 能够自定义安全规则
- ◆ 支持绑定浮动 IP
- ◆ 支持添加 1-2 块网卡

## 2.2 镜像获取

vDAS 镜像已经上传阿里云镜像市场,用户直接在阿里云镜像市场搜索"深信服数据库安全审计"就可以获取相应镜像。

## 2.3 部署方式

vDAS 支持旁路部署(需要在数据库服务器上安装 agent),不支持镜像部署。

# 2.4 资源配置

规格	配置参数	吞吐量	磁盘
			具体大小需要根据实际情况来配置,不少
VDA5-200	Z CFU,4G KAM	200Mb/s	于 81G.
		400Mb/s	具体大小需要根据实际情况来配置,不少
VDAS-400	4 CPU,86 RAM		于 81G.
vDAS-600	8 CPU,16G RAM	600Mb/s	具体大小需要根据实际情况来配置,不少

地址:深圳市南山区学苑大道1001号南山智园A1栋



于 81G.

# 2.5 授权方式

- 1、支持在线试用
- 2、支持在线授权

# 第3章 部署指导

# 3.1 云平台配置

深信服 vDAS 是以系统镜像的方式提供的, 部署深信服 vDAS 需要先提供一台独立的 ECS 主 机来安装 vDAS 镜像。

### 3.1.1 创建 ECS 虚拟机

登录阿里云中国站,点击购买 ECS 云服务器。





出现以下选择页面,参考【2.4资源配置】,按照实际需求选择对应的服务器,例如选择2核 CPU、4G内存的云服务器。实例类型需要选择(计算网络增强型 sn1n)型号,其他型号的 cpu 可 能会出现网卡适配不了网络配置无法生效的问题。

							₩ 1945年	丁市 お祝	的体中文 • 8	@sangtor.com
一键购买	自定义购买					« geiek	③ 购买历史	□ 产品价格	④ 购买云盘	0 产品控制台
1 基础配置		3 网络和安全组	③ 系統配置 (法項)		3 9900 (5)	0		- <b>()</b> #il	(JM	
计器方式	包年也月 🥥 注	会量付款 抢占式实	89							
地域 軟化活得地域	編欄1(案則) ▼ 開机名 不同地域的实例之间的网互不相通:选择	182 町用区E 町用 線近影響户的地域、可除低网络时程	区 0 可用区 C 可用区 A 可用区 B (1) . 通用可称户的访问追流 ①							Ħ
<b>实例</b> 染剂规格铁 场跟配置法型 可购买的地域 申请按振高配		购卖例规格 2 vCPU 4 GIB ▼ 指述规则的名称,知:ecs vCPU ↓ 内存 ↓ 平均基地 计算性能	্রান্দ্র <u>০</u> ১০ ৪/৫৯ম.্ <b>হর্মার • প্রশ্</b> র (CPV এইজেয়ন্	2. 处理爵主 成/會须 F	5网鞭魔 💠 内网收发行	D 🗘 GPU/FPGA 🕥	实例本地存 I 储 ○ I	Pv6 参考(i)	橋 ◎ ≑ ↓	
	・ ・ 計算同結増 弾型 snine ecssninelarge	2 vCPU 4 GiB -	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1Gbps 30万	PPS -	ч	. <u>.</u>	0.68 /87	
	○ 计算型(原 注章) sn1 ecs.sn1.medium	2 vCPU 4 Gi8 -	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.5 Gbps 10 75	PPS -	- 3	5 1	0.9 /81	
		2 vCPU 4 GiB 20 %	Intel(R) Xeon(R) Platinum 8269CY	2.5 GHz	0.08 Gbps 10 万	PPS -	- 3	2 × 0	236 /87	
	<ul> <li>完发性能致 ecs.t5- 例 t5 c1m2.large</li> </ul>	2 vCPU 4 Gi8 25 %	lintel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163 / Intel(R) Xeon(R) P atinum 8269CY	2.5 GHz	0.5 Gbps 10 万	PPS -	- 1		0.4 /8tj	
	· 現发性能实 ecst5- 例 t5 lclm2Jarge	2 vCPU 4 Gi8 20 %	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163 / Intel(R) Xeon(R) P atinum 8269CY	2.5 GHz	0.4 Gbps 10 万	PPS -	- 1	2 × 0	333 /0 <sup>1</sup>	
	共享计算型			25.004	0.5 Char 10 E	000			*	

镜像在镜像市场中搜索"深信服数据库安全审计"即可看到,选择2.0.2版本,点击 使用 按钮。

【说明】国外阿里云市场没有深信服数据库审计镜像,需要联系深信服工程师通过共享镜像的方式来提供。

镜像	公共镜像	自定义镜像	共享镜像	镜像市场	0
	从镜像市场获取更多选择	(含操作系统)			



	Q. 深信服 数据库			搜索	
有选镜像	全部操作系统	全部架构	$\sim$		
急後分类 へ	深信服虚拟化数据库安全	全审计		*****	¥0/时
✔ 全部	基础系统: linux 架构: ( 深信服数据库安全审计系统)	54位 DAS(Database security Audit S	2.0.2 V	12人已使用	使用
操作系统					
运行环境					
管理与监控					
管理与监控	公共造俸	白云以路後	士亨语佬	培施市场	0

存储选择按照需求选择高效云盘或者 SSD 云盘,存储选择 81G 以上,不需要选择额外的数据盘。

存储	系统盘					
云盘参数和性能	高效云盘	•	81	GiB	2448 IOPS	✔ 随实例释放
	不同云盘性能指标不同,	查看 各云盘性	館指标>	-		
	✓ 启用自动快照策略	(推荐)				
	当云盘数据逻辑错误时	(如误删、病毒	等),可通过	快照	恢复。大陆地	域 1 GB快照数据每月仅需 0.12 元,快照价格>
	请选择自动快照策略			C	)创建自动	快照策略>
	数据盘 你已选择 0 均	e盘,还可以选持	译 16 块 <u>盘</u>	-		
	+ 增加一块数据盘					



4

### 3.1.2 配置网络和安全组

云服务器 ECS	一键购买	自遠文時來			« igeithe	③ 购买历史	百 产品价格	四 购买云盘	⑦ 产品控制台
		2 网络和安全组	(3) 系統配置 (法编)	④ 分组设置 (选续)			③ 确认订加	n	
	网络	・             ・	LAN19 / van-wc99552202g11w623w7 で 0 円 EAN19 / van-wc99552202g11w623w7 EAN19/WC97用区: 94時1 可用匠 (1) 228M7/WG92 192106.190.24	网络类型选择专有网络, VPC根据用户需要选择 <sup>用追用问题量</sup> 21 个					
	公 <b>阿带克</b> 公阿带意计表	分離公開時4時起 不为应用分離公用時始出,如面内用公用,時配置并身	<b>和选举性公网 IP 地址</b> >,或者购买实的后升级实的的带意,系统会自动力实例						1. 約約年
	安全组 安全组限制 配要安全组	重新記録を全証     ③	2025年以初期世紀時期 新建会会場。 新発意味。 至少 写以近ね、2000 个気俗・編励用手) 日本登録登表にな、参可以送入にの設制保設量、前性必要。	需要开放TCP443、TCP4567端l					
	弹性网卡	eth0 主用+4 交通制 VLAN19 + 增加3%性质+4 初近可增加 1 映	✓ 自助分配 IP 地址 → 建实例释放						
	IPv6	您当前无法使用 (A6 (点主盘署原因))							

网络需要选择专有网络,需要选择业务虚拟机所在的 VPC, VLAN 可以是跟业务虚拟机同一个, 也可以是独立的 VLAN;

公网带宽根据实际情况选择,如果需要从公网直接访问 DAS 的控制台,则需要分配公网带宽;

安全组未配置默认进方向都是拦截,出方向都是放行的,若未定义则会导致创建好云主机后无法访问的情况,所以需要在安全组中放通 TCP443 端口(控制台管理)、TCP4567 端口(agent 同步日志端口)。

点击 新建安全组 跳转到新窗口设置安全组;

1972 **%**65.5

<ul> <li>安全组*</li> <li>安全組陽制</li> </ul>	<b>:</b> 重新选择安全组 ⑦ 安全	11美似防火增功能,用	于设置网络访问控制,	, 您也可以到管理控制	則合新建安全组>	較我选择>				
<ul> <li>配置安全组</li> </ul>	所选安全组: 默认安全组 (自定,	())								
			HTTPS 443 诫	10 🔽 22 第0	3389 1	✓ ICMP 协议 ⑦				
	項列応要开進的IPV4的加以/病日:(									

标签 100

安全组名称 • 输入安全组名称研销查询

模板选择自定义,名称按照实际情况填写,网络选择专有网络,最后点击 确定 按钮保存。 创建完成后,点击 配置规则 按钮添加规则;

① 没有查询到符合条件的记录

SANGFO 深信服科技	R	9	深信服智安 SANGFOR SECUR	全 mr				深信服,	让IT更简单,	更安全,	更有价值
安全组列表		接來 多标签							⑦安全追照制与规则	C 882228	
安全组印/名称	标签	所愿专有网络	相关实例	可加入IP数	网络类型(全部) マ	安全相类型	间建筑的	描述		援作	
sg-wz9iixeby39xzzkrsqt7 ssl	٠	vpc-wz98vfjtzz44uyek0siwo	0	2000	专有网络	普通安全组	2019年7月8日 19:03	12	修改 管理实例 配置规	売強 │ 还原规则 問 管理弾性网卡	
- 影除 编辑标签									共有1条、每页显示: 10条 。	< 1 × ×	

跳转到配置页面后,点击添加安全组规则按钮,然后在弹出的网页中逐个添加TCP443、 TCP4567端口。

注:规则方向选择入方向;授权动作选择允许;授权对象填写 0.0.0.0/0 (代表任意 IP, 若有其他需求则按需填写)

			Q 建能					調用 工節 昏窦 <u>企业</u> 支持与服务	🖸 🗸 🗑 🕲 🛱 🎝 🖸
<	DAS a VPC192 / VP	oc-wz9xihyvm2huz9uiiw8y		编辑安全组规则 ⑦ 添加	四安全组规则		×	教授设置 😋 透回 落加支全组织制	快速他建规则 添加ClassicLink安全组现则
安全组现则				网卡类型:	内网				* D) # D#-
安全组内实例列表	人方向 出方向			规则方向:	λ πith v				T av T art.
安全组内弹性网卡	HORE	协议舞型	論口范围					创建时间	援作
	🗹 允许	自定义 TCP	4567/4567	授权策略:	允许			2019年10月31日 19:15	修改   克隆   删除
				协议类型:	自定义 TCP 🔹				
	□ 允许	自定义 TCP	443/443	*	4567/4567	0		2019年10月31日 19:14	修改 克隆 影除
	e ese								
				0095582:	1	0			
				授权类型:	IPv4地址段访问 *				
				*接权对象:	0.0.0/0		0 ####		
				描述:	agent3≋⊡				
					长度为2-256个字符,不能以http	p://或https://开头。			
							NG ROA		

填写完成后回到配置云服务器的页面, 点击 重新选择安全组 的按钮, 选择刚刚创建的安全组, 然后选择下一步;

S 一键购买 I	自走义购买								《 返回旧版 (
		请选择	安全组						×
网络	专有网络	安全组	名称 ▼ 请输入安全组名	<u>称</u>					
教我选择网络	VPC192 / vpc-wz9xihyvn2hu		安全组名称ID	安全组名称	创建时间	实例+辅助网卡	专有网络ID	规则	
	如素创建新的专有网络、综	0	sg-wz92ujq5zpxrjfw93tjv	DAS	2019年10月31日 19:13:56	0	vpc-wz9xihyvn2huz9uiiw8y8	查看规则>	
			sg-wz92ihvsz4y7dzfyyqu1	sg-20191018das	2019年10月18日 18:15:11	1	vpc-wz9xihyvn2huz9uiiw8y8	查看规则>	
			sg-wz92ihvsz4y7buhrkkxu	sg-20191018	2019年10月18日 15:29:29	0	vpc-wz9xihyvn2huz9uiiw8y8	查看规则>	
公网审党 公网审党计费	DIECZYMIPVARAL X		sg-wz90k9jt7wa6purboz4q	SSLVPN	2019年10月14日 11:16:27	0	vpc-wz9xihyvn2huz9uiiw8y8	查看规则>	
			sg-wz959be577h69utnj1v5	sg-wz959be577h69utnj1v5	2018年10月17日 18:03:05	0	vpc-wz9xihyvn2huz9uiiw8y8	查看规则>	
安全组	重新选择安全组 ③							1 >	
安全组限制 配置安全组	所选安全组: DAS/so-~								
	请确保所远安全组开放包							选择 取消	1
弹性网卡	eth0 主网卡		交换机 VLAN19	✓ 自动分配 IF	地址 ~ 肺实例释放				
	+ 增加弹性网卡 您还	可增加1							

后面的配置按照实际情况选择即可,一般情况下保持默认即可。



#### 深信服,让IT更简单,更安全,更有价值

	MINDREN	3 系統配置 (活識)	▲ 分组设置 遮如	3 确认订单
登录凭证:	● 密钥对 ○ 自定义密码 ○ 创建后设置			
密铜对: ③	诸违译密钥对	<ul> <li>〇 洋橋参考(新建面明)</li> </ul>		
	著不适迭 密钥对 / 目虚义密码,则默认为创建后再设置。			
实例名称:	launch-advisor-20191031	如何自定义有序实例结察		
	2-128个字符,以大小写字母或中文开头,可包含数字。**。	17. Yata		
描述:			长度为2-256个字符,不能以http://或https://开头	
主机名: ⑦	摄作系统内部的计算机名,选续项	如何自定义有序主机名 -		
	Linux 韓興他變作系築:长度为 2-64 个字符,允许使用点号	(1)分標字符成多段、每段允许使用大小写字母、数字或注字符(-),但不能注埃使用点号(1)或这	生学符(-)。不翻以点号()或注字符(-)开头或地尾。	
有序后缀:	为实例名称和主机名添加有序后缀 ②			
实例释放保护:	」防止通过控制给取API 決劃除释放()			
高级选项(实例 RA	AM 角色 & 实例自定义数据 cloud-init) (可点击展开)			
[础配置]		🗸 系統配置 (法壇)	4 分组设置 低陶	5 确认
東組 道道 	四月四週間 一 〇 ⑦ 雪创連新的波源組、忽可以点击 主動語>			
<b>東山</b> (市) 丸田 御 御 一 短 日 一 一 二 一 二 二 一 二 二 二 二 二 二 二 二 二 二 二 二	5月日 月前日 第回経営的の実現は、安可以供由 主会経 2日前市石田会 日日 1日日 1日日 1日日 1日日 1日日 1日日 1日日			
教祖 1953 第2章 2015 第2章 2015 第2章 2015 第1章 注利 2015	高時完新組			
新知	ARE 2011 毎回選条的波源線 ( 切可以供由 ま会理) 居由現新設備 和印成有法社教術( 智慧部編集・ 可以供社社教術) 創建発展集上的>			
数组 前日 初日 現集 前日 一 第二章 日 第二 第二 第二 第 第 二 第 二 第 二 第 二 第 二 第 二 第				天历史 団 产品が増 尚 和天王皇
新祖	AR (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本)		< 2000 0 192 • 2000 0 192	天历史 国 产品が後 (8) 和天三皇 (3) 確认订年
数组	AR (日本) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	<ul> <li>承統起置 (3)改)</li> <li>無結: 40年1可用反 E(1)</li> <li>職種: 40年1可用反 E(1)</li> <li>職種: 二次指現最好に試現年安全等計 2.0.2</li> </ul>	<ul> <li>※ 図田田田 ● 第5</li> <li>※第1: 计第三点 / ec.dlarge2ACPU 4GB</li> <li>※第1: 计第三点 / ec.dlarge2ACPU 4GB</li> <li>※第2: 第3:52:8 3163 [第三時間]</li> <li>第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章</li></ul>	天历史 图 产型价格 80 和天云盘 ③ 确认订单
数组 第3 等重 第 事査 第 可 可 可 可 可 可 可 可 可 可 可 可 可	A将更高级     ・      ・     ・      ・     ・     ・      ・     ・     ・     ・      ・     ・     ・     ・     ・     ・     ・     ・     ・	<ul> <li>              新命政策 (35年)      </li> <li>             北島: 34年13月回日(1)             秋田: 可用回日(1)      </li> <li>             秋田: 7月回日(1)      </li> <li>             北島: 34年13月回日(1)         </li> <li>             北島: 54年13月回日(1)      </li> <li>             北島: 54年13月回日(1)         </li> <li>             北島: 54年13月回日(1)         </li> <li>             北島: 54年13月回日(1)         </li> </ul> <li>             大学校(1)             大学校(1)             北山市(1)         </li> <li>             北島: 54年13月回日(1)         </li> <li>             Ж: 54年13月回日(1)         </li> <li>             Ж: 54年13月回日(1)         </li> <li>             Ж: 54年13月回日(1)         </li> <li>             Ж: 54年143月回日(1)         </li>	《 図面日服 ① 取 ② 分指设置 (3年) ※第1: 计算1 6 / ecc.diage(3/2014/36) 系统: 第25元章 (35年) 系统: 第25元章 (35年) 系统: 第25元章 (35年) 系统: 11(3/108-mcd952522(35/11/12))	平原史 国 产品が格 (8) 和天王皇 ③ 確认订単 業業 7天 168-19-80-24
新祖 二部 新祖 二部 新藤主 初 一部 5 一世時天 「「「「「「」」」 「「「」」」 「「」」」 「「」」」 「」 「	AR (日本) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	<li>         展続記書 (354)          展続記書 (354)              地域: ※明目可用区 (1)         ・         ・         ・</li>	《 図面日服 ① 取 の 取 の 対理定置 (3項) の 第 の 対理に置 (3項) の 第 の 対理に置 (3項) の 第 の 1 (40) ( 予 の 1 (40) ( の 第 の 1 (40) ( の 第 の 1 (40) ( の 第 の 1 (40) ( の 第 の 1 (40) ( の 来      の 考 の 5 の 5	REA: 国 产品が客 (3) 和天王皇 (3) 論(LIJ和 製工 7天 168,19.8/24
新祖 二部 東京 二部 京都主が、 201 5 一様的交 第 本紀記堂 単純記堂 2 単純記堂 2 単純記堂 2 単純記堂 2 単純記堂 2		● 系統配置 (334)           ・ 必有1可用区 (1)           ・ 地理: 「東田道島KicK200年年金海谷・20.02           ・ VTC: 192/192-vs2billyvs2bud5killeの6月           ・ SNNKKP: lbanch-advisor-020191021	《 図田田服 ① 第3 ② 分指设置 (34) ② 分指设置 (34) ※第1 计算数 d / eco.diage(2),CU 40(8) 減度: 第25元者 91(36 現在分析版) 単位また所成版 自然的策略 / dbatt,polory (東天 140) ( 文読者: VLAN19/198-wd3955222)(11/e528/m7/192)	<ul> <li>平成的 他 和天王会</li> <li>第二、11年</li> <li>第二、11年</li> <li>第二、11年</li> <li>第二、11年</li> <li>11年</li> <li>11年</li> <li>11年</li> <li>11年</li> <li>11年</li> </ul>
<ul> <li>第組</li> <li>第</li> <li>●確約束</li> <li>●</li> <li>■</li> <li>■</li> <li>●</li> <li>■</li> <li>■</li> <li>●</li> <li>●</li></ul>		<ul> <li>● 系統配置 (30年)</li> <li>● 熟練工業 (30年)</li> <li>● 熟練工業 (30年)</li> <li>● 第二 東京総連邦/428年号金章1+2.0.2</li> <li>● WTC: 19C182/19C+04284(4594)</li> <li>● S2重用: DAS / sp-wt324(4594)(4924)</li> <li>■ S3 / sp-wt324(4594)(4924)</li> <li>■ WTC: 19C182/19C0/19C31</li> </ul>	<ul> <li>(※ 図目日回 ① 用目</li> <li>(※) 外目以至 (350)</li> <li>(※) : 計算型, 6 / ecc.diregt/ACU 408)</li> <li>(※) : : : : : : : : : : : : : : : : : : :</li></ul>	<ul> <li>平品が市 高 和天王会</li> <li>③ 執い丁年</li> <li>第二 7 天</li> <li>168 19.0/24</li> </ul>

2 単語表明: ¥ 0.430 /ct 現象表明: ¥ 0.000 /ct 上一歩: 分類収置 例はため

最后确认订单支付即可完成云主机的创建,创建完成后可以在实例列表里看到新建的 vDAS 主机的相关信息,包括运行状态、内网 IP 地址、EIP 地址、配置信息等。

196424





## 3.2 网络配置

由于 DAS 不支持 DHCP, 所以需要手工配置 DAS 的 IP 地址, 具体配置方法如下:

首先在实例列表里查看 vDAS 实例的私网 IP,如下例,阿里云平台给 DAS 分配的私网地址是 192.168.1.133。

≡ (-)阿里云 🐲	町1 (深圳) ▼		Q 搜索					房用 工单 倫置 企业	支持与服务 🖸 🗳	10		城中文 🌔	
云服务器 ECS	实例列表								⑦ ECS控制台操作指南	C	创建实例	批惠設作	
概选	<ul> <li>选择实例履性项搜索,或者输入</li> </ul>	大健李识别搜索	0 Q	标签							高级搜索	2 0	
專件	□ 实例ID/名称	标签 监控 可用区 *	IP地址	状态 🗸	网络美型 -	10.201	实例规格族	专有网络歴性	付務方式 👻	倾藏方式 🕶		操作	E
标签 🔤	Isunch-advisor-2	🦠 🛡 🤷 🔛 华南1可用区C	2(公) 192.168.1.133(私術)	<ul> <li>通行中</li> </ul>	专有网络	2 vCPU 4 GiB (I/O优化) ecs.sn1neJarge SMbps ()隆值)	ecs.snlne.large 计算网络增强型	vpc-wz? ; ? :9uiiw8y8 vsw-wz? ?	按量 2019年11月1日 10:48 创建		三百万万万	理 透程连接  照悟   更多 •	
实例与销量	i-wz9d6z27o4rxgyegljp4 launch-advisor-2	🦠 🗢 🤷 🐱 🕸 埠南1可用区E	192.168.19.22(私有)	●已停止	专有网络	2 vCPU 4 GiB (I/O优化) ecs.c6.large 5Mbps (峰值)	ecs.c6.large ecs.c6	vpc-wz9xihyvn2huz9uiiw8y8 vsw-wz99o52ziz2yl1vr62bw7	按量 2019年11月1日 10:14 创建		更改实例	管理  現格   更多 •	-
实则	i-wz9505h9bgsb2bcezmnv vAF808-2	≫ © <mark>∆</mark> 唑 柴南1可用区8	10.223.69.243(私有)	④已停止	专有网络	2 vCPU 4 GiB (I/O优化) ecs.t5-c1m2Jarge 1Mbps (譜道)	ecs.t5-c1m2.large ecs.t5	vpc-942kzjhdy vsw-wz9vuzhqmf43cssy0vj9j	按量 2019年10月30日 15:13 创建		更改实例	間格   更多 -	-

然后点击远程连接,进入到以下界面。

× C3 管理终期 htm?spm=5176.2020	<b>≭ ×</b> 520101.107.d515.68314d	+ f5u0ojn3&instanceId=i-bp1gpdc9x4o06990leo0&regionId	l=cn-hangzhou
	Counton DAS Cotu		提示:如果出现持续黑
		P=	
		Appliance Manager is at https://	
		Management Setup Wizard 2 Show Current Settings 3 Reboot	

选择第一项 Management Setup Wizard, 然后配置 DAS 的 IP、掩码和网关, 其中 IP 配置成阿 里云平台分配的私网 IP 地址, 掩码配置成 VPC 设置的掩码, 网关配置成 x.x.x.253, 然后点击 OK 保存配置生效。



# 3.3 登陆控制台

IP 地址配置生效后,用户就可以通过私网 IP 或云平台给 DAS 分配的公网 IP (如果有)登陆 DAS 的 WEB 控制台页面了,登陆方式是 <u>https://x.x.x.x</u>。



默认的用户名和密码均为 admin, 建议登录后及时修改密码。

# 3.4 云组件授权配置

首次使用 vDAS 系统, 需要先给 vDAS 授权。vDAS 授权分以下为三种, 使用云主机只需关注 "在线授权"和 "申请试用"即可。

- ▶ 在线授权:需要先购买获得序列号,然后将序列号信息填写到对应的位置
- ▶ 本地授权服务器授权:需要在本地搭建一个授权服务器 (VLS),使用授权服务器对 vDAS



来授权。

▶ 申请试用:只要填写申请信息即可通过短信方式获得授权序列号,把序列号填入【在线授

权】即可,使用此序列号可以免费试用 30 天。

【在线授权】与【申请试用】都需要 vDAS 能够连接互联网,与 vls.sangfor.com.cn 的 443 端口保持通信。

● 数据库安全审计系统	V2.0.2		系统尚未获得授权、您可使用以下任 本问证(2) + ++ + 医可使用以下任	意方式获得授权:	⑥ 帮助文档   🏯 发起求助   🥃 在线笛询 社区编句、资料搜索 🔍 🔗 admin
导航菜单	首页		CERERC   4-ADD CARD BERCK   443	915.4H9	
🍰 系统状态	首页 Dashboard				🔯 本間・ 🔮 选择显示媒块
▶ 返行状态	系统资源		\$ B	新型SQL模版	\$ <b>0</b> 0
Q. 数据库风险					
显 日志查询					
	1.	20.6 *	5.3 %	袋	
★ 系统管理	CPU占用率	内存占用率	磁曲占用率	山榄瓶小	
				SQ	
	_	总日志数	风险日志数		
		0	<u>0</u>		SQL構版个数
	风险告替		\$ <b>□</b> @	风脸操作	\$ E 0

#### 3.4.1 在线授权

在线授权需要填写授权 ID 和序列号,请联系当地销售或致电 400-806-6868 进行咨询购买。 点击控制台的在线授权,将购买的授权序列号填写到对应位置,提交后等待设备进程重启后即可变 为授权状态。

● 数据库安全审计系统	V202	新始成年表得感況、認可使用以下任意方式获得感況:	⑥ 帮助文档   🍰 发标求助   💭 在线齿间 社区经问、资料搜索 🔍 🔗 admin・
导航菜单 《	第页		
🎂 系统状态	首页 Dashboard		📅 本周 🔹 🧶 选择显示模块 🔹
▶ 运行状态	系统资源	◆ ◎ 新型SQL機版	\$ <b>0</b> 8
Q. 数据库风险	$\sim$		
m 日志重時			
🔮 报表中心	1. 20.6.		
★ 系统管理	CPU占用憲 内存占用庫	在城市规产品	
	0.0 EX 0 7/255	- 第200日99号機能系加速機能変更4400-80-684日7番機時天、 第200日99号機能系加速機能を加速した。 第21日、1、回該規制業務は準期的場合下でお出行。 2、通过20世紀の日本規構要素が成功的場合下でお出行。 3、5000日99号骨和総合一を集体や差徴、近世的規模の1419字号目が正確的合金差 現 	■ Souttes Att

授权成功后在授权信息页面会有【更改授权】、【删除授权】和【授权服务器授权】三个选项。 【删除授权】和【授权服务器授权】都是删除掉当前的授权信息,使设备变为初始化状态;【更改 授权】则是将新的序列号覆盖掉当前的,授权 ID 不会更改。



### 3.4.2 申请试用

点击 申请试用, 填写对应信息。

	中頃以用	
联系人:		
手机号码:		获取验证码
验证码:		
公司名称:		
推荐人:		
推荐人电话:		
温馨根示:		
the last with Table and	2011年保持连接网络的情况下,免费使用产品3	0天。

【姓名】、【手机号码】、【短信验证码】、【公司名称】和【产品用途】是必填项,提交申请后, 会有审核人审批,审批完成后,会收到授权 ID 和授权序列号,把授权 ID 和授权序列号填入【在线 授权】,填写成功后控制台会有提示:您还可以免费试用 30 天,您可以使用【在线授权】或【本地 授权服务器授权】。

SANGFOR		人生前咨询 400-806-6868
	<b>申请试用表</b> APPLY FOR TRIAL 请填写您的联系方式以及需求,我们会第一时间响应您的需求!	•

重新登录 vDAS 控制台,系统就会显示可以免费试用 30 天。

### 3.4.3 vDAS 授权说明

授权成功后, vDAS 控制台有授权客户和授权有效期的提示。



数据库安全审计系统	V2.0.2	您还可以免费试用30天,您可以使用 在线接权 或 本地	10000000000000000000000000000000000000	- 帮助文档   🏯 发始求助   🤎 在线咨询 社区疑问、资料提案 🔍 🔍 admin・
导航菜单 · · ·	首页			
叠 系统状态	首页 Dashboard			📓 本周・ 🔮 选择型示媒块・
▶ 运行状态	系统资源	∿ ⊜	新型SQL模板	\$ = s <sup>*</sup>
Q. 数据库风险				
圖 日志查询				
🕒 报表中心	3 * 22.3 *	5.3 %	휫	
🥔 策略管理	CPU占用率 内存占用率	磁盘占用率	に残疾	
<b>父</b> 系统管理			SC	
	888X	风险日志数		
		<u>0</u>		SQU機能个數
	风险告答	¢□©	风险操作	4 🗆 🛛

查看【系统管理】-【系统设置】页面,即可显示授权信息。

数据库安全审计系统	充 V2.0.2	您还可以免费试用30天,您可以使用 在线接权 或 半地接权服务器接权	⑥ 帮助文指   🍰 发始求助   🤍 在线路线 社区絕问、资料搜索 🔍 📯 admin・
导航菜单 《	首页 × 接权信息 ×		
🙆 系统状态	您还可以免费试用30天		
Q. 数据库风险	设备序列号		
■ 日志重領	● 网先序号: CD310977 ● 序列号状态: 有效 过期时间: 2019-12-01		
接来中心			
💣 策略管理	软件升级授权 ①		
★ 系統管理	序列号状态: 複效 过期时间: 2019-12-01		
▶ 部署模式 >			
▶ 系统设置 ~			
接权信息			
系统时间			
管理员			
服务器配置			
白彩达火			
200 P			
• Electron >			

若因为某种原因 (网络不可达等),连续 7 天未收到授权服务器的心跳信息,此时 vDAS 从授 权切换到非法状态,非法状态时控制台不可配置业务,但原有的业务还可以继续使用。非法状态的 设备登录后在首页头部有非法状态的提示。

导致非法状态的原因有序列号过期、授权资源与实际资源不匹配、序列号被禁用、序列号失效 等,在控制台头部都会有对应的提示信息。

如果非法状态的设备经过 **30** 天还是没有收到正确的授权则都会变为初始化状态。由于设备是 由已经授权过的设备转变为初始化状态,因此将不会再有免费试用的选项。





# 3.5 数据库审计功能配置

### 3.5.1 用户环境与需求

A 公司在阿里云上部署了若干数据库服务器,现在需要对所有访问数据库的行为进行记录。

#### 3.5.2 配置步骤

#### 配置步骤如下:

数据库审计可以记录常见的数据库操作日志,包括 Mysql、Oracle、SQL、DB2、Informix、 KingBase、Dameng 等数据库的查询、修改、新增、删除等日志。

#### windows 主机数据库配置

Windows 主机仅仅支持 64 位 Windows 2008 、64 位 Windows 2012。保证 windows 主机和 数据库审计是可达的。



#### 1) 新增一个业务系统,并配置对应的审计策略

🤤 S/ 🐺	ANG 信服科技	FOR 5		言服智安全 SFOR SECURITY				深信服,	让IT更简单,	更安全,	更有价值
数据库安全	审计系统	V2.0.1							🐍 帮助文档   🤽 发帖求助   🚦	■ 在线咨询 社区期间	
导航菜单	**	首页	× 数据库审计日志 ×	策略列表 ×	<u>41</u> 49	5系统 ×					
🙆 系统状态		C 刷新 + 淡加	★ 删除								
Q. 数据库风险		□ 序号	业务系统		描述	1			类型		
		1	cssp						Mysq		
<ul> <li>・</li> <li>・</li></ul>					_						
★ 系统管理					编辑业	务系统	×				
<ul> <li>部唇模式</li> </ul>	~				名称:	win2012					
运行模式					描述:						
网口配置					<b>类型</b> :	Mysq	*				
静态路由					编码:	UTF-8	*				
业务系统					主机:	199.201.91.22					
<ul> <li>系統设置</li> </ul>	>										
▶ 系統維护	>										
						提交	取消				

可以审计安全策略,审计功能和安全功能配置,同时还可以配置权限控制策略。

		and the	MEANINE CONTRACTOR	(R407)	LDDA	a a sectores a				
SKHO	0	87 + 3320+	X 209: V 100	Ø 頭用 <b>會</b> 上移	484					CONCESS:
Q 数据库风险		序号	名称	191P	空気系	克 功能配置	×	生效时间	10/1	状态
🔤 日志重的	10 KUS	1	aa	승명	期相申日女王永	18 /		<b></b>	1.4	7
() 服務中心	9 mit	・ 安全策略(2祭)			医胎周			201		
		1	all	全部	名称:	默认策略		全天	+ +	4
₩ 策略管理	×	2	RELIMEN	全部	課約P:	全部	8	全天	₹ 4	1
					业务系统:	所有	0			
▶ 安全规则					生然时间:	全天	*			
	w				审计功能		1			
IPH					☑ WEB审计:	所有	8			
#100218					☑ 数据库审计:	所有	8			
> 审计白名单					安全功能					
<ul> <li>他的资源法语</li> </ul>					☑ 数据库安全:	非常见运维工具或业务系统使用grant.sp_adc				
					□ 账号安全:		7			
X 3588世纪					Bby/E :	212R68 05850 058				
					告誓对象:	系统新认	*			

- 2) 通过下载 agent 安装文件
- 3) 进入到下载页面, 支持 windows: 64 位 Windows 2008 、64 位 Windows 2012;



4) 下载 windows 的 agent 安装文件到 windows, 并安装成功;



port = 4567

[capture]

#网卡配置(linux 下配置为网口名称, win 下面配置为本机网口 ip 地址)

dev = 199.201.91.22

#抓包过滤条件(配置为 shutdown 则停止抓包)

filter = tcp

#缓存包个数

prod\_cons\_cnt = 42000

#### [sender]

#ip 头替换为此 ip 地址以适应 DAS 业务系统的配置

conn cnt=1



地址:深圳市南山区学苑大道1001号南山智园A1栋



5) 然后重启一下 eps 服务,双击重启服务

a WannaCry® FlashFXP	10M process.ba								r.	
				EPS				X		
文件 主页 共享	查若							~ 0		
	这台电脑 > 本地磁盘 (C:)	<ul> <li>Program Files</li> </ul>	Sangfor + AC + El	×s •		× ¢	搜索"EPS"	Q		
☆ 收藏夾	名称	*	修改日期	美型	大小					
👪 下载	1.0.000000		2016/10/19 8:22	文件夹						
二 点面	🚳 7z.dll		2016/9/2 15:24	应用程序扩展	1,052 KB					
💹 最近访问的位置	Tz.exe		2016/9/2 15:24	应用程序	273 KB					
<b>党</b>	agent_win.tgz		2016/10/19 16:29	WinRAR 压缩文件	3,305 KB					
📜 这台电脑	installer.bat		2016/9/28 15:32	Windows 批处理	2 KB					
🔒 视频	restart.bat	执行重启eps服务	2016/9/19 10:03	Windows 批处理	1 KB					
1 图片	i uninstall.bat		2016/8/27 20:35	Windows 批处理	2 KB					
1 文档	wget.exe		2016/9/2 15:24	巡用程序	821 KB					
下数										
1 mm										
11 合 <b>两</b>										
- 木地炭泉(())										
-POINTER (CI)										
<b>9</b> 网络										
8 个项目										
Navicat EPS2.0_Bui										
1								Wind	lows Server 2	<b>012 R2</b> 激活 Windo

### linux 主机数据库配置

Linux 主机支持 linux: 64 位的 CentOS 5/6/7、Debian 6/7、Ubuntu 10.04-14.4、RHEL 5/6/7。 首先保证 Linux 可以与数据库审计可达;

root@CSSP4.0.3:~/vdas/bin\$
1001@C55F4.0.3:~/V0a5/010\$
root@CSSP4.0.3:~/vdas/bin\$ping 8.8.0.23
PING 8.8.0.23 (8.8.0.23) 56(84) bytes of data.
64 bytes from 8.8.0.23: icmp_seq=1 ttl=63 time=2.88 ms
64 bytes from 8.8.0.23: icmp_seq=2 ttl=63 time=5.30 ms
64 bytes from 8.8.0.23: icmp_seq=3 ttl=63 time=11.4 ms
64 bytes from 8.8.0.23: icmp_seq=4 ttl=63 time=6.70 ms
8.8.0.23 ping statistics
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.885/6.578/11.425/3.114 ms
root@CSSP4.0.3:~/vdas/bin\$

1) 新增一个业务系统,并配置对应的审计策略

<b>3</b>	信服科	技	$\overline{\mathbf{e}}$	涂信版省女王 SANGFOR SECURITY					深信服,让IT更简单,更安全	,更有价值
♥ 数据库安全市	审计系统	V2.0.1							G 帮助文档   🚨 发标求助   🛄 在线音询 社区短问,资料搜索 🔍	1
导航菜单	**	NG.	× Bilişeiti Bil	×	为系统 × 日	建高硼化石 ×	网口腔器	×		
🔗 系统状态		S 聯新 + 潮加	× 80%						(6)6	<b>南</b> 道
		□ 序号	业务系统	描述	£				天型	
		2 1	cssp						Mysql	
		2	win2012						wysą	
· 提表中心										
2 策略管理				10+0-IL	AR XI II:		×			
* 系统管理				2013132	955500		_			
▶ 部務機式				名称:	Cisp					
运行模式				振送:						
网口和田				类型:	Mysql		~			
经合新由				编码:	UTF-8		*			
业劳系统				主机:	8.8.0.1					
▶ 系統设置	>									
• 550000	>									
						载	RCA			

可以审计安全策略,审计功能和安全功能配置,同时还可以配置权限控制策略。

数据库安全审计	系统 V2.0.1						(3) 帮助文档   22 发始求助   1	在线咨询 社区地可、资料授	朱 Q A admin
导航菜单	·· 首页	× mexant	18 × 100	1 <b>8 × -</b> 1193	a x merena x				
🔗 SiSK5	Ø Ref. + 25.	10・ × 細冷 × 点月	日 🥝 筑用  🚖 上総	🗣 T85					植桃查宗
Q 数据库风险	日 序号	名称	191P	293	統 功能影響		生效时间	10/11	状态
🔜 日志香狗	■ 权限控制策略 (1	約	승명	编辑审计安全策	16 10		<b>4</b> ∓		1
	日 审计安全策略 (2	9) 9)		図応用		_			
₩ 策能管理	0 1	all	全部	名称:	默认策略 企可	-	金天	± 4	1
) 策略列表	¥ 2	默认为服	全部		In P 所有	0	金天	<b>*</b> 1	~
• 安全规则				生物时间:	全天	~			
• 2000定义	-			审计功能					
PH				₩EB#it:	所有	0			
B 100 2 1 Br				☑ 数据库率计:	所有	8			
告報対象				安全功能					
<ul> <li>集整密设法历</li> </ul>				☑ 数据库安全:	非常见运维工具或业务系统使用grant,sp_adc	0			
* ****				□账号安全:					
				Bh/E :	※ IBREま □告報通知 □拒绝				
				告誓对象:	Riceria Y	1			
					握交	ROA			

2) 通过下载 agent 安装文件

SANGFOR CALL TO WERREA

数据库安全审计	系统 V2.0.1		
导航菜单	<b>**</b> 首页	× 业务系统 × 运行模式	×
2 系统状态			
Q、数据库风险	运行模式:	<ul> <li>         ● 单机模式         <ul> <li></li></ul></li></ul>	
圖 日志查询			Internet
🕒 报表中心	配置网口		
❷ 策略管理	管理口: IP地址:	eth0 *	
* 系統管理		8.8.0.21/255.255.255.240	① DAS(管理協名英集團)
▶ 部署模式	风关:	10.252.252.254	单机模式,DAS设备在网络中以旁路方式部署,一体化提供策略配置、日志
运行模式	首选DNS:	8.8.8	采集、查询报表等功能。适用于仅需要在一个采集点上进行数据采集的场 县。
静态路由 业务系统	田 <u></u> 近0143 .		
▶ 系统设置	~		
授权信息			部署模式配置完成后请 配置业务系统,设备采集数据才开始生效
系统时间			♀ 当web服务器、数据库部署在同一台主机或者部署在虚拟机环境中时,请部署 数据库Anept零户选并行日主义集 配管方式参考要助文档
管理员			

3) 进入到下载页面, 支持 linux: 64 位的 CentOS 5/6/7、Debian 6/7、Ubuntu 10.04-14.4、 RHEL 5/6/7。



4) 下载 Linux 的 agent 安装文件到 Linux, 并安装成功;



5) 给安装文件可执行权限 chmod +x agent\_installer.bin

./agent\_installer.bin /root/vdas (可选择需要安装路径)

```
SSP4.0.3:~/vdas/config$pwd
/root/vdas/config
root@CSSP4.0.3:~/vdas/config$ls
 aflog.proto appversion das_agent.ini machineid not5 reslimit_das_agent.ini reslimit_logcli.ini sfguardpath
 [server]
 #das_agent 连接服务端地址
 host = 8.8.0.23
 port = 4567
 [capture]
 #网卡配置(linux 下配置为网口名称, win 下面配置为本机网口 ip 地址)
 dev = eth1
 #抓包过滤条件(配置为 shutdown 则停止抓包)
 filter = tcp
 #缓存包个数
 prod_cons_cnt = 42000
 [sender]
 #ip 头替换为此 ip 地址以适应 DAS 业务系统的配置
 conn cnt=1
```





6) 然后重启一下 eps 服务, 双击重启服务

#### rootgCSSP4.0.3:-/vdas/configScd../bin/ rootgCSSP4.0.3:-/vdas/configScd../bin/ rootgCSSP4.0.3:-/vdas/binSls agent\_List cpulinit enable\_sshd\_execmen eps\_monitor eps\_services\_check.sh eps:test ipc\_probe ipc\_proxy luadbg resmon\_export.sh sfginject sfglogs sfgpromote.bashrc agent\_List. Ldsa\_genet eps\_app eps\_services eps\_uninstal[.sh get\_appversion ipc\_probe.l lloader patchelf sfgconfig sfginject.bin sfgpromote sfgpromote.l eps stortsuccess eps start success eps start success

7) 通过数据库审计日志查询对应的日志

# 第4章 常见问题

1、实例类型需要选择(计算网络增强型 sn1n)型号,其他型号的 cpu 可能会出现网卡适配不了网络配置无法生效的问题。