安华金和云数据库防火墙 接入文档



北京安华金和科技有限公司

二〇一九年一月

版权申明

本文档包含了来自北京安华金和科技有限公司的技术和商业信息,提供给北京 安华金和科技有限公司的客户或合作伙伴使用。接受本文档表示同意对其内容保密 并且未经北京安华金和科技有限公司书面认可,不得复制、泄露或散布本文档的全 部或部分内容。

本文档及其描述的产品受有关法律的版权保护,对本文档内容的任何形式的非法复制,泄露或散布,需承担相应的法律责任。

北京安华金和科技有限公司保留在不另行通知的情况下修改本文档的权利,并保留对本文档内容的解释权。



目 录

1.	产	品部署	L	4
2.	产	品初始	化	9
	2.1	导入	、LICENSE 文件	9
	2.1	1	登录系统管理员界面	9
	2.1	2	导入 License 文件	10
	2.2	设置	代理端口	11
	2.2	2.1	登录系统管理员界面	11
	2.2	2.2	添加代理端口	11
	2.3	配置	住集群	13
	2.3	8.1	负载均衡配置	13
	2.3	8.2	分区管理	14
	2.3	8.3	节点管理	15
	2.4	KERN	IEL 节点配置	16
	2.5	添加]被保护数据库实例	19
	2.5	5.1	登录安全管理员界面	19
	2.5	5.2	添加被保护数据库实例	19
	2.6	设置	_昆 虚拟补丁规则	24
	2.7	设置	【防火墙规则	26
	2.8	配置	负载均衡	28
	2.9	部署	?测试	30



1.产品部署

1、打开阿里云云市场,搜索"安华金和",如下图所示。

〕阿里云			Q ② 中国站 ~ 控制台 备室 邮幕	최 전국 오프 티
云市北		发布定制需求▼	来家中心▼	
云市场分类	基础软件 建网站 安全 商业软件 物联网 API 数	据智能 开发者软件 是	品牌馆 聚沙姆 云市场头条	
違宗 5	华金和 ×			
产品分类	软件市场 服务市场 罐站市场 云安全市场 企业应用 解决方案 API市场 物研阅市场 数据智能			
价格:	全部 免票 1-96 99-198 199-1998 1999-2998 2998以上			
REGULT/F	上編时间章 价格章 评分章		为您找到 11条结果	
Ø	乙数提準审计_企业版(DBAudit-EnCloud) 文行方式:環像 基础系统:Lnux 安培会低语于明显示于台、正地推出学会合式资源率审计(图称DBAudit-EnCloud),限时支持RD 声音 服务者:2代学业会任何起发展及句 思示会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社	保障: (金)(帝)(金)(御) (平分: ***** (人政: 153	¥ 0/月 + ECS明期期	RU
	乙数据库加密_体验版(MysqITDE) 灸疗药法:瞬间 基定统计:CentOS 安华金约定或爆动使用线的现象化,在不要除MySOL原有效能的基础上,实现对常能很可要 局质者: 2.在身边全行动性最限之句 例	19月月年 : (16) (16) (17) 1月月 : (14) 1月月 : (14) 1月月 : (14)	¥ 0/月 + ECS使用鹿用	

2、在搜索结果中查找到需要购买的云数据库防火墙产品,然后点击该产品,如下图所示。

<u> 云数据库防火墙_企业版(DBFirewall-EnCloud)</u> 交付方式: 環像 基础系统: CeriOS 5.8	平台保障: 🏨 🛞 俄 📵	¥ 0/月
云数据库防火壤系统(简称DBFIrewall-Encloud)能够实时监控云上的数据库活动,使用全面的访问… 服务商: 北京安华金和科技有限公司	产品评分: ★★★★★★ 使用人数: 0	+ ECS使用费用
企业 安全 防火墙		

3、在打开的产品详情页面中点击"立即购买",如下图所示。

云市场	在此榆入您需要的! 病毒清除 网站搬游	2 9 https 故障 恢复 堡垒机 VPN	<u>接全部</u> 該者 发布定制需求 ▼ JAVA 全能环境	英家中心▼● 素家中心▼
云市场分类 云安全市场 > 数据安全 > 数	基础软件 建网站	安全 商业软件 物理	关网 API 数据智能 开发者软件	牛 品牌馆 照划 间 云市场头条
天数	如据库防火墙_企业版(DBFII 调库防火墙系统(简称DBFIrewall-E 和外部对数据的攻击,是保护数据库	ewall-EnCloud) ncloud)能够实时监控云上的数据 安全的最后一道防线。	库活动,使用全面的访问控制,防止来自	服务 電 北京安华金印料技有限公司 联系報报:●元代集报 ●加速集报 ●面前集報版 不確認明 17 代目 800-2200
*	2 0 月 突费:* 0/月 按量价格:* 0/小时		用户评分: ★★★★★ 使用人数:0人	电话: 4008005185は10134 13702007105 1552228284 邮箱: support@dbsec.cn
\langle	立即购买	G		云市场免费提供线上担保交易、全程服务监管, 保障您的资金安全和服务质量,90%的职作、纠
保) 交易过程担保	(退) 不满意全额退款	(监) 服务全程监管	(优) 优质服务商	紛. 资金盗取均由线下交易导致,请勿线下交易! 易!

4、在打开的"选择配置"页面根据用户实际使用情况设置"地域"相关选项,如下图所示。



C	阿里云									
		选择	全配置							
		地域	地域 可用区	华北 1 华北 2 可用区 A	华北 2 【	华北 3	华东 1	华东 2	华南 1	
5,	在打开的 说明: 在	"选择 选择领	配置"	〔面选择需 时需要与客	要购买的 :服人员过	镜像版才 挂行沟通,	本,如下日 , <mark>以确保</mark>	图所示。 所选择的	版本是最	新的。
镜像	镜像名称 镜像版本	云数据库 DBF-C	昉火墙_企业版 _V3.2.4.0.1 ▼	(DBFirewall-EnClo	ud)			\triangleright		
6,	在打开的	"选择	配置" 页	〔面,设置	云服务器	相关配置	₽ III. o			

第一步:设置网络类型,根据实际情况选择专有网络,如下图所示。

网络类型	专有网络		
	如果您需要弹性公网IP , 请单独购买后	,再绑定到专有网络类型的ECS实例上 >> 弹性公网IP	
	DBSCloud-Encrypt -	switch1 👻	
	如需使用其他专有网络,请选择已有考	<mark>≠有网络</mark> ,也可以自行到 控制台创建 >>	

第二步:设置实例规格,根据所购买的产品规格选择相应的实例规格,防火墙高可用版需要购买一个管理端和两个节点共三个实例,产品规格说明详见下方"说明"部分内容。此处以企业版中一台实例的购买为例,选择 8 核 16G 的实例规格,如下图所示。

定例至列	হ নি। ।	조진 미
201201	系9] II	————————————————————————————————————
I/O优化	I/O 优化实例 ②	
实例规格:	(默认配置)8核	16GB:计算型
	田多实例规模 田多实例规模 田参会の 田参会の 日参会の 日参会の	8

说明:产品规格、购买时长和配置需按以下要求进行选择。

序号	产品规格	购买方式	云服务器最低配置	价格
1	标准版	默认1年	CPU: 4核 内存: 8G	云市场标示的价格

云上数据资产所有权捍卫者 北京安华金和科技有限公司



			数据盘: 1T	
			CPU: 8 核	
2	企业版	按年购买	内存: 16G	咨询客服人员
			数据盘: 2T	
			CPU: 16 核	
3	专业版	按年购买	内存: 32G	咨询客服人员
		.0	数据盘: 4T	
		OUE	CPU: 16 核	
4	旗舰版	按年购买	内存: 64G	咨询客服人员
	Car th		数据盘: 8T	102 7

第三步: 设置公网带宽, 根据用户实际情况设置"带宽", 如下图所示。

说明:如果被保护数据库与云数据库防火墙系统在同一个 VPC(专有网络)内,通过内网 通信,且通过内网管理云数据库防火墙系统,则可选择不使用外网流量,在"带宽"项中设 置为 0Mbps 即可。如果需要通过外网访问或管理云数据库防火墙系统,则需要购买外网流 量,带宽建议设置为 5Mbps。

公网带宽	按固定带宽					
带宽	1	50M	100M	150M	5	Mbps ×
	阿里云免费提供	最高 5Gbps 的恶意	就量攻击防护, 了解	释更多>> 提升防护能力>>		

第四步:设置磁盘容量,系统盘默认即可,然后点击"增加一块"图标,添加一块类型为"高效云盘"的数据盘,根据所购买的产品规格设置相应的磁盘容量,产品规格相关内容详见第二步"说明"部分内容。此处以企业版为例,磁盘容量设置为2000G,如下图所示。

系统盘	高效云盘 🔫	40 (GB	1240 IOPS 系统盘设备名:/dev/xvda	
	如何选择 SSD云盘 / 副	副 人 金辺 (音道	甩云盘	1,请看 详细说明>>	
数据盘	高效云盘 🔻	2000	GB	自动分配设备名	×
	+ 増加一块 您还	还可选配 3 块;f	包年包	一 同 高效云盘 不支持卸载;	

7、在打开的"选择配置"页面,设置购买量。根据所购买的产品规格,选择相应的付费方式和 购买时长,产品规格相关内容详见第6步骤中的第二步"说明"部分内容。此处以企业版为 例,选择付费方式为包月套餐,购买时长为1年,如下图所示。

说明: 云数据库防火墙系统以提供镜像方式提供服务,镜像文件内部默认内置7天试用授权, 用户可选择"按量"模式进行产品试用。



			1					
购买	付费方式	包月套餐	按量					
量	购买时长	1个月	2个月	3个月	4个月	5个月	6个月	7个月
		8个月	9个月	1年	2年	3年		

8、在打开的"选择配置"页面右侧,勾选"同意《云服务器 ECS 服务条款》",然后点击"立即 购买",如下图所示。

选	择配置		
地域	地域 可用区		当前配置 地域 华北 2(陳刊分配) 猿参 云ઝ雪库防火道 企业版 (DBFirewall-EnCloud)
镜像	镜像名称 镜像版本	云数据库防火墙_企业版(DBFirewall-EnCloud) DBF-C_V3.2.4.0.1 ▼	 云服易器 8 岐 (1608 5所売氏(9本同知) 1 株売改三盘(2000GB) 阿天量 1年X1台 9 免费开通安骑士基础版 ② 2011
	网络类型	专有网络 如果您需要现在公网IP,请单独购买后,再绑定到专有网络类型的ECS实例上 >> 弹性公网IP DBSCloud-Encrypt ▼ switch1 ▼ 如當使用其他专有网络、请选择已有专有网络、也可以自行到控制台创建>>	镜暈: ¥0 云慰易谱:¥18596.64 颈付台調用:¥18596.64
	实例系列	派列 II 系列 III	☑ 同意《云服务器ECS服务条款》
	1/0优化	I/O 优化实例 ⑦	<u> 立即购买</u>
7	实例规格:	(默认配置) 8 核 16GB : 计算型(原独字) sn1,ecs.sn1.xlarge	实际扣费以账单为准 购买和计费说明>>
服		₩ 更多实例规格	

9、在打开的"确认订单"页面,核对购买产品信息,如下图所示。

荀	秋订单 * 返回					
	确认订单	支付			开通成功	
	产品名称	付费方式	购买周期	数量	优惠	资费
	服务商: 阿里云计算有限公司					
1.	支服务器 ECS 地域: %412 可用区: %412 0.9 (KU2KW) (10) (KU2KW) </td <td>包年包月</td> <td>1年</td> <td>1台</td> <td>會:¥ 3903.36 1) 芳酒 時年立章軍阿伦他总5所代重(集條曲) 芳酒 時立章軍阿伦他总5所代重(定應) 芳酒 時立章軍阿伦他总5所代重(PC实例) 芳酒 1年立章軍阿伦他总1所代重(PC实例)</td> <td>¥ 18596.64</td>	包年包月	1年	1台	會:¥ 3903.36 1) 芳酒 時年立章軍阿伦他总5所代重(集條曲) 芳酒 時立章軍阿伦他总5所代重(定應) 芳酒 時立章軍阿伦他总5所代重(PC实例) 芳酒 1年立章軍阿伦他总1所代重(PC实例)	¥ 18596.64
2.	税像市场 服装等:北京安华金和科技有限公司 地域 4/32 関連名称: 元安國軍的火境 <u>全世球</u> (DBFirewall-EnCloud) DBF-C_V3.2.4.0.1 現象 [D: m-2ze905avpr25g0grtzm	包年包月	1年	1台		¥ 0.00

10、在打开的"确认订单"页面,设置云服务器 ECS 操作系统 root 账户的密码。然后点击"去

下单",如下图所示。



设置密钥	设置密码	创建后设置	
28%所设置的密码,如遗忘	河登录 ECS 控制台重置密码		
名: root			
密码:		8 - 30 个字符,且同时包含三项(大写字母、小写字母、数字	e、特殊符号)
容码 : •••••••			
<u> </u>			
: 规则及操作说明>			
对应的发票信息,请在 管理 品默认禁用 TCP 25 端口和	整制台-费用中心-发票管理 中设 基于此端口的邮箱服务,特殊情》	置。 元需报备审核后使用, 查 置详情 ≻	
			() 使用推荐4
			应付款: ¥ 15026.64 ≝i¥ 3273.3
			去下单
			✔ 《云服务器 ECS 服务条款》
			 ✔ (云服务器 ECS 服务条款) ✔ (镇像商品使用条款)

11、在打开的"支付"页面,选择支付方式,然后点击"确认支付"完成购买,如下图所示。

合井支付 2確订単 应付费用: ¥ 15026.64 订算: 201339037290997 ¥ 15026.64 乙酸勞器EC5(包月) 数量: 1 时长: 1年 ※ 实例: 8 & 16 G6 系列 IH 計量回(原始意) sin1 //0 优化实例: 1/0 优化实例 系统曲: /dev/xvda调效云血 ¥ 0.00 乙数据库防火墙 企业版 (DBFirewall-EnCloud) 数量: 1 时长: 1年 ¥ 0.00 函數即: 44 ½ 2_0BC-5kd.V3.2.4.0.1 所圖回應: 44½ 2 受問照推: ecs.sn1.xlarge ¥ 0.00 ① 使用储值卡抵扣 抵扣: ¥ 14920.63 订算: 201339037290997 ¥ 14920.63;适用产盾 ◆ 2 取金余额 (¥ 0.08) 当前使用 0.08 元 如果您有正在使用中的后付妻产品,请保证有足够余额。 支付: ¥ 0.08 其他支付方式 页付重 个人网限 企业网限 支付 ¥ 105.93 ● 乙託ご ●	确认订单	支付	支付成功
订单: 201339037290997 ¥ 15026.64 云服务器ECS(包月)数量: 1 时长: 1年 实例: 8 核 16G8系列 II-计算型(原独享) sn1 \/O 优化实例: 1/O 优化实例 系统曲: /dev/xvda高效云曲 ¥ 0.00 ブ単: 201340035280997 ¥ 0.00 云数据库防火墙_企业版 (DBFirewall-EnCloud) 数量: 1 时长: 1年 ¥ 0.00 酸@ID: 华北 2_DBC-Std.V3.2.4.0.1 所服区地: 华北 2 安例规格: ecs.sn1.xlarge ¥ 14920.63 过单: 201339037290997 编号-Q-d5342c21e7a7;余额:14920.63;适用产言 ▼ ¥ 14920.63 过单: 201339037290997 編号-Q-d5342c21e7a7;余额:14920.63;适用产言 ▼ ¥ 14920.63 梁 现金余额 (¥ 0.08) 当前使用 0.08 元 如果您有正在使用中的后付票产品,请保证有定够余载. 支付: ¥ 0.08 其他支付方式 支付室 个人网根 企业网根 支付 ¥ 105.93 ② 泛忙 E	合并支付 2笔订单		应付费用: ¥ 15026.64
订单: 201340035280997 ¥ 0.00 云数据库防火墙 企业版 (DBFirewall-EnCloud) 数量: 1 時长: 1年 頃金D: 华北 2_DBC-Std V3.2.4.0.1 所服区域: 华北 2 至例期待: ecs.sn1.xlarge 抵扣: ¥ 14920.63 谜 使用储值卡瓶扣 抵扣: ¥ 14920.63 订单: 201339037290997 编号:Q-d5342c21e7a7;余额:14920.63;适用产言 ◆ ☑ 现金余额 (¥ 0.08) 当前使用 0.08 元 如果您有正在使用中的后付票产品,请保证有定够余额。 支付: ¥ 0.08 其他支付方式 支付: 个人网根 企业网根 支付: ¥ 105.93 ④ 泛红宝 ● 泛红宝 ●	订单: 201339037290997 云服务器ECS(包月) 数量: 1 时长: 1年 实例: 8 核 16GB系列 I\计算型(原独事) sn1 I/O	优化实例: I/O 优化实例 系统曲: /dev/xvda高效云曲	¥ 15026.64
 ● 使用储值卡抵扣 抵扣: ¥ 14920.63 □ ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ① ①	订单:201340035280997 云数据库防火墙_企业版(DBFirewall-En 镜像ID: 华社 2_DBC-Std.V3.2.4.0.1 所屬医婊 4	Cloud)数量: 1 时长: 1年 松北 2 实例规格: ecs.sn1.xlarge	¥ 0.00
 「戸羊: 201339037290997 「第号:Q-d5342c21e7a7;余懸:14920.63;道用严言 ・ ¥14920.63 「迎金余额(¥0.08)当前使用 0.08 元 如果忽有正在使用中的后付妻产品,请保证有足够余额. 支付:¥0.08 其他支付方式 支付宝 个人网根 企业网根	☑ 使用储值卡抵扣		抵扣:¥ 14920.63
 図 现金余额(¥0.08)当前使用 0.08 元 如果您有正在使用中的后付费产品,请保证有足够余额. 支付:¥0.08 其他支付方式 支付宝 个人网银 企业网银 支付 ¥105.93 ● 支付宝 	订单:201339037290997	编号:Q-d5342c21e7a7;余额:14920.63;适用产指 👻	¥ 14920.63
其他支付方式 支付室 个人网線 企业网線 支付 ¥105.93	☑ 现金余额(¥ 0.08)当前使用 0.0	8 元 如果您有正在使用中的后付费产品,请保证有足够	\$余额。 支付:¥0.08
	其他支付方式 支付宝 个人网银	企业网報	支付 ¥105.93

12、联系厂商客服人员获取 License 文件。

说明: 云数据库防火墙标准版镜像内置1年 License 授权,购买后即可正常使用,其他版本 需与厂商客服人员联系获取 License 文件。



2.产品初始化

管理控制台 (Manager) 443 Web控制台HTTPS服务通讯端口 管理控制台 (Manager)、 集群节点 (Kernel) 22 Web控制台SSH服务通讯端口 集群节点 (Kernel) 22 Web控制台SSH服务通讯端口 集群节点 (Kernel) 10000-11000 此处端口需根据2.2.2章节所 设置的具体端口号开放。 管理控制台 (Manager) 9901、9311、 9207 应用服务器管理端和节点之前 的通信端口 集群节点 (Manager) 9301 健康检查端口		节点	端口	备注
管理控制台 (Manager)、 集群节点 (Kernel) 22 Web控制台SSH服务通讯端口 集群节点 (Kernel) 10000-11000 此处端口需根据2.2.2章节所 设置的具体端口号开放。 管理控制台 (Kernel) 9901、9311、 9207 应用服务器管理端和节点之前 的通信端口 集群节点 (Manager) 9301 健康检查端口		管理控制台 (Manager)	443	Web控制台HTTPS服务通讯端口
集群节点 (Kernel) 10000-11000 此处端口需根据2.2.2章节所 设置的具体端口号开放。 管理控制台 (Manager) 9901、9311、 9207 应用服务器管理端和节点之前 的通信端口 集群节点 (Kornel) 9301 健康检查端口		管理控制台 (Manager)、 集群节点 (Kernel)	22	Web控制台SSH服务通讯端口
管理控制台 (Manager) 9901、9311、 9207 应用服务器管理端和节点之前 的通信端口 集群节点 (Kornal) 9301 健康检查端口		集群节点 (Kernel)	10000-11000	此处端口需根据2.2.2章节所 设置的具体端口号开放。
集群节点 (Kornol) 9301 健康检查端口		管理控制台 (Manager)	9901、9311、 9207	应用服务器管理端和节点之前 的通信端口
		集群节点 (Kernel)	9301	健康检查端口
	14			

说明:在系统使用之前需要在安全组中开放以下端口。

2.1 导入 License 文件

登录系统管理员界面 2.1.1

1、打开 Google Chrome 或 Firefox 浏览器,在地址栏内输入 https://云数据库防火墙系统管理节 点IP地址。进入登录页面后,输入用户名: sysadmin 默认密码: sysadmin1234,点击【登录】 进入系统管理员界面。



云数据库防火墙系统 DBFirewall-EnCloud
▲ 〈 mmbaya → ····································
注意:首次登录系统需要修改安全管理员默认密码。

2.1.2 导入 License 文件

 进入系统管理员界面,点击"系统",然后选择"证书管理",在打开的"证书管理"页面, 点击"浏览",选择获取到的License 文件存放路径,然后点击"上传",校验通过后系统方 可正常使用。

证书状态:	正常
证书类型:	试用版
产品型号:	DBF-C-PRO
序列号:	0A72-E5D8-0BCA-1FC4
功能模块:	云数据库防火墙 (3)实例[注:1个数据库实例=1组(IP+Port)]
颁发对象:	user
本期服务起始日期:	2017年07月30日
本期服务终止日期:	2017年08月07日
	浏览



2.2 设置代理端口

2.2.1 登录系统管理员界面

1、打开 Google Chrome 或 Firefox 浏览器,在地址栏内输入 <u>https://云数据库防火墙系统管理节</u> <u>点 IP 地址</u>。进入登录页面后,输入用户名: sysadmin 默认密码: sysadmin1234,点击【登录】 进入系统管理员界面。

2.2.2 添加代理端口

1、进入系统管理员界面后点击【网络管理】->【网卡管理】,进入网卡列表页,如下图所示。

云数据库 防火墙系统	◎ 益控 戌 网络管理	G 系统 O 集群				¢ °	(A) sysadr
■ 「「「」 「」 「」 「」 「」 「」 「」 「」 」 」 」 「」 」 」 」 … 」 … … … … … … … … … … … … …	防路由						
主机名称							
主机名称: iZ2ze759k33ab0jhda3	5r9Z *5	R允许数字、字母、连字符、下划线并	且不親超过64个字符 🕒				
网卡列表							
网卡名称		MAC地址	连接状态	连接速率 (Mbps)	同卡组	授	ffe
Eth0		00:16:3E:0E:32:BB	注股	0	管理接口	C	3 8 +

2、然后点击"查看代理端口"图标,如下图所示。

云数据库 防火墙系统	<u>ه انتق</u>	63、网络管理	₲ 系统	O 集群				¢ ⁰ (⊉) sysadm
网卡管理 管理接口	静态路由							
主机名称								
主机名称: IZ2ze759k33	ab0jhda35r9Z	*Rf	允许数字、字母、	進字符、下划线并且不能超过84个字符 🚦	3			
网卡列表								
同卡名称			MACIBL		连接状态	连接速率(Mbps)	阿卡组	操作 🚽
Eth0			00:16:3E	0E:32:88	注报	0	管理接口	🗹 R +
								_

3、进入代理组页面,点击"编辑"图标,如下图所示。



云数据库 G 监控 d 网络 防火墙系统	管理 G系统 O集群				♀ ⁰ ④ sysadmin [+ 過出
岡卡管理 管理接口 静态路由				1	
主机名称					×
主机名称: IZ2ze759k33ab0jhda35r9Z	*只允许数字、字母、连字符、下划线并且不能超过64个字符	# 🕒		网卡名称: Eth0	
网卡列表				部署模式: 代理	•
-				代理各称: 管理接口	
P#K646	MACIBIE 00.620000000	连接状态	送报送年(Mbps)	IP地址: 192.168.235.201	PING
Emu	00:10:36:06:32:88	267章	0	子阿掩码: 255.255.0.0	
				网关: 192.168.255.253	
				启用状态: 🧹	
				第日设置	
				端口号(推荐范围10000-11000)	状态 操作
				表中数据为空	

4、进入端口设置界面,点击"添加端口"图标,如下图所示。

大数据库 の 磁控 61 网络管理 G	· 系统 O 集群) ⁰ 🙆 sysadmin	
阿卡管理 管理接口 静态路由							
主机名称				88			×
主机系称: [222x755ik33ab0jhda35r92]*风光神	数字、字母、连字符、下划线并且不能超过64个字符 🕒			网卡名称	Eth0		
网卡列表				部署模式	代理		,
94-52 b	MACINH	16.18.18.75	法编译率 (Mhos)	代理名称	管理接口		
Eh0	00 16 3E 0E 32 8B	3510	0	IP地址	192.168.235.201		PING
				子周掩码	255.255.0.0		
				宛笑	192.168.255.253		
				日用状态			
				端口号(推荐范围1000	0-11000)	状态	副作
				表中数据为空	1		
)	
					\sim	6	

5、在"端口设置"<mark>页</mark>中输入可用的端口号,如下图所示。

注意:可以添加多个端口号,每个端口号对应一个被保护的数据库实例,端口号可用范围为:

10000-11000

	云数据库 方火墙系统	◎ 监控	の 网络管理	G 系统	O 集群								¢ º	(a) sysadmin	E• iBH
网卡管理	管理接口	静态路由													
主机名称									B	ά (×
主机名称:	iZ2ze759k33ab	0jhda35r9Z	*5	R允许数字、字母、	進字符、下划线并	3不能超过64个字符 🗎				网子	·名称:	Eth0			
网卡列表										部署	模式	代理			٣
B420				MACIE			10.10.52171	MIRING (Mhos.)		代理	1名称	管理接口			
Ftb0				00:16:38	-0E-32-88		No.12	(mops)		IF	地址: [192.168.235.201			PING
							42.08			子网	掩码:	255.255.0.0			
											同 关: [192.168.255.253			
										島用	状态:	v			
									1	第日设置					
									编口	号(推荐范围	000-1	11000)		秋志	操作
									100	00					a
												添加時日	1		

6、点击"保存"图标,完成添加代理端口。如下图所示。



	云数据库 防火墙系统	の話法	战 网络管理	G 系统	0	£Ħ							۵.0	eysadmin	E+ ass
网卡管理	管理接口	静态路由								+					
主机名称										8					×
主机名称	iZ2ze759k33ab	oljhda35r9Z		"只允许数字、李	喝、 连字符	3、下泡底并且不	範續过64个字符	3			同卡名称	Eth0			
网卡列表											印石模式	代理			
同主名称				MAC	inter .			连接联办	许接连来 (Mbos)		代理名称	管理接口			
Eth0				00.1	6.3E.0E.32	68		3618	0		IP地址	192.168.235.201			PING
											子间履货	102 169 255 253			
											周用状态	. 192.100.200.200			
										1.0	日記書				
										SREEK.	(推荐范围1000	0-11000)		秋志	操作
										10000					
										100	1				1
												(15.103	e 🗆		
2.3	酉	置	 耗群	9P)											

2.3.1 负载均衡配置

1、进入系统管理员界面后点击【集群】->【负载均衡配置】,如下图所示。

	云数据库 防火墙系统	6 监控	63 网络管理	☞ 系統	O 集群			۵ م	Sysadmin	D+ 通出
负载均衡	配置 分区管理	节点管理								
负载均衡	冽表									+
序号	负载均衡名称				宾例 ID	IP 地址	操作			
表中数据	为空									

2、点击"添加"按钮图标,如下图所示。

云数据库 の 脳控 成 网络管理 G 系統 O	D 生町			💿 sysadmin 🛛 🗜 छिस
负载均衡配置 分区管理 节点管理				1
负载均衡列表				(+
序号 负载均衡名称 实例 ID	D	IP mble	19/11	
素中数编为空				

3、在弹出的"添加负载均衡"页,添加负载均衡相关信息,并保存,如下图所示。



	◎ 监控	63、网络管理	G 系统	O 集群						¢ 0	Sysadmin	[→ 退出
负载均	射配置	分区管理	节点管理									
负载均	衡列表											+
序号	负载均衡名	郗		实例 ID			IP 地址		操作			
表中数	据为空											
				添加负载均	衡			×				
					负载均衡名称	SLB1		1				
					实例 ID	lb-2ze5z1kgya6	y4qw85cd6d					
					地址	192.168.235.11	5					
							1	·				
							保存	返回				

2.3.2 分区管理

1、进入系统管理员界面后点击【集群】->【分区管理】,如下图所示。

	◎ 监控	战 网络管理	🔓 系統	O 集群				¢ º	Sysadmin	[→ 退出
负载均	衡配置	分区管理	节点管理							
分区列	表									+
ID	负载均衡	i			名称		操作			
表中数	如据为空									

2、点击"添加"按钮图标,如下图所示。

	◎ 监控	战 网络管理	🔓 系統	O 集群			¢ 0	🙆 sysadmin	[→ 退出
负载	均衡配置	分区管理 节	ち点管理						+
分区	列表								+
ID	负载均衡				名称	操作			
表中	数据为空								

3、在弹出的"添加分区"页,选择负载均衡,并输入分区名称,保存,如下图所示。



a 🖻	控 战网络管理	☞ 系统	○ 集群				¢ 0	🔕 sysadmin	[→ 退出
负载均衡配置	分区管理	节点管理							
分区列表									+
ID 负编	說均衡			名称		操作			
表中数据为空									
			潇加分区	负戦均衡 SLB1 名称 分区1	•	×			
2.3.3	大 古 広	管理							

2.3.3 节点管理

1、进入系统管理员界面后点击【集群】->【节点管理】,如下图所示。

	◎ 监控 64、网络	各管理 口子系统	O 集群						¢ 0	Sysadmin	[→ 退出
负载均	新配置 分区管理	节点管理									
节点列	表										1 0
每页 10) ▼ 项										
序号	负载均衡名称	分区名称	地址/(实例ID)	节点描述	状态	证书信息	上次操作	操作结果		操作	
表中数	据为空										
上页下列	Į										

2、点击"添加"按钮图标,如下图所示。

	◎ 监控	61 Mat	ஊ	₲ 系統	O 集群						¢ 0	Sysadmin	[→ 退出
负载均	衡配置	分区管理	节点	管理									1
节点列	表												(C) +
每页 1	〕▼ 项												
序号	负载均衡名	称	分区名称		地址/(实例ID)	节点描述	状态	证书信息	上次操作	操作结果		操作	
表中数	据为空												
上页下了	τ												

3、在弹出的"添加节点"页,输入节点的实例 ID,选择负载均衡、分区,输入节点的 IP 地址, 保存,如下图所示。



	◎ 监控	6 3 网络1	管理	₲ 系統	O 集群								¢	0 🙆 sysadmin	[→ 退出
负载均衡	新配置	分区管理	节	点管理											
节点列制	表														1 0
每页 10	▼ 项														
序号	负载均衡名	称	分区名称	۶¢	地址/(实例ID)	节点描述		状态	证书信息		上次操作	操作结果	操作	
表中数据	属为空					添加节点						×			
上页下页	ī						Γ	实例ID	i-2zehvlnilb22rzngnxl						
								负载均衡	SLB1	•					
								分区	分区1	¥					
								地址	192.168.235.202						
								节点描述							
							L								
											1				
										_	<u>♥</u>				
										6	游				
													Y-		

2.4 kernel 节点配置

1、通过阿里云控制台远程连接到 kernel 节点后台, 输入后台用户名, 密码, 进入系统管理界面, 如下图所示。

5CLOUD
5CL H
To The
38
1/10
1000
549
14
1

2、选择序号7,并回车,进行集群管理配置,如下图所示。



####	***************************************	########
##		##
##	系统管理	##
##		##
####	*******	#########
#		#
#	1.系统初始化	#
#		#
#	2. 维护工具	#
#		#
#	3. 诊断工具	#
#		#
#	4. 杏看系统信息	#
#		#
#	5、黄新启动系统	#
#		#
#	6、关闭系统	#
#		#
#	7. 华群管理	#
#	·· (() a · 2	
####	***************************************	#########
# -	请洗择[1->7,q:退比]: 7 ━━━	

3、选择序号2,并回车,设置管理节点地址,如下图所示



4、输入管理节点地址,如下图所示。

诸龄入签理节于中		194
192.168.235.201	μ. •	>

5、敲回车键, kernel 会去 ping 管理节点 IP, ping 通后, 提示重启机器, 如下图所示。



蒲翰入管理节点地址: 192.168.235.201 PING 192.168.235.201 (192.168.235.201) 56(84) bytes of data. 64 bytes from 192.168.235.201: icmp_seq=1 ttl=64 time=1.61 ms --- 192.168.235.201 ping statistics ---1 packets transmitted, 1 received, 0% packet loss, time 1ms rtt min/avg/max/mdev = 1.612/1.612/1.612/0.000 ms 设置管理节点地址 '192.168.235.201' 成功,诸重启机器! -

6、敲回车键,退回到集群管理界面,并输入q,返回到系统管理界面,如下图所示。

	4###
##	##
## 集群管理	##
##	##
	<i>4###</i>
##	##
## 1.查看管理节点地址	##
## 2.设置管理节点地址	##
##	##
	4###
	27
	8
# 请选择 1,2, q:返回, x:直接退出 : q	5

7、退回到系统管理界面后,输入5重新重启系统,并回车,如下图所示。

##		#########
##	+	##
##	* 系统管理	##
##	ŧ	##
##	******	#########
#		#
#	1. 系统初始化	#
#		#
#	2. 维护工具	#
#		#
拼	3. 诊断工具	#
拼		#
Ħ	4. 查看系统信息	Ħ.
Ħ		Ħ,
并	5. 重新启动系统	Ħ,
Ħ		Ŧ
H H	6. 天闭系统	# #
#	o Merita ma	# #
#	7. 采杆宫壁	# #
17 14 H	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	<i>⁷⁷ AAAAAAAAAA</i>
mn		*****
Ħ	+ 浅沙城[1>7 の・泥山]・[5]	

8、在重新启动系统的提示中,输入 yes,并回车,如下图所示。



## ##	
## 重新启动系统 ##	
## ##	

# $#$ $#$ $#$ $#$ $#$ $#$ $#$ $#$ $#$	
# 你确定重启主机?(yes/no): yes	
	10
	12

9、待 kernel 节点启动完成后,防火墙管理页面查看节点状态正常,如下图所示。

	◎ 监控 🕺	网络管理 😽 😽 系统	O 集群					¢ º	🙆 sysadmin	[→ 退出
负载均	衡配置 分区管	理节点管理								
节点列	表									1 0
每页 1	0 ▼ 项									
序号	负载均衡名称	分区名称	地址/(实例ID)	节点描述	状态	证书信息	上次操作	操作结果	操作	
1	SLB1	分区1	192.168.235.202 (i-2zehvlnilb22rzngrxxl)		I.R	正常详情	Get license info	-	İ	
上页1下	页									

2.5 添加被保护数据库实例

2.5.1 登录安全管理员界面

1、打开 Google Chrome 或 Firefox 浏览器,在地址栏内输入 <u>https://云数据库防火墙系统管理节</u> <u>点 IP 地址</u>。进入登录页面后,输入用户名: secadmin 默认密码: secadmin1234。

注意: 首次登录系统需要修改安全管理员默认密码。

2.5.2 添加被保护数据库实例

系统支持对云服务器自建数据库实例和云服务商提供的云数据库实例的防护。用户需根据自 身云环境下数据库的实际部署方式进行添加。具体添加方式如下:



2.5.2.1 添加云服务器自建数据库实例

1、进入安全管理员界面后点击【配置】->【数据库】,进入数据库列表页,然后点击"增加数据 库"图标,如下图所示。

云数据库 防火墙系统	♠ 概況	办 风险	🛛 行为	■ 报表	🕲 規则	📄 库安全		₩ 419			۵ ۵	🙆 secadnin	
数据库 ● 用户管理	角色管理 告	書设置	应用身份	IP名称管理									
查询条件													
数据库类型: 证	计选择数据类型		*		数据库名称	请输入数据库存	172						
数据库列表												•(
数据库名称	3	數据库类型		数据	库版本		防护状态		部署模式	操作			
表中數据为空													
	上页 下页												

2、在弹出"添加数据库"页面中填写被保护的数据库实例相关信息。如下图所示。

B		×
数据库名称:	mysql	
数据库类型:	MySql	¥
数据库版本:	5.6 • 自动获取	
部署模式:	代理	¥
防护状态:	○ 学习中 ○ 保护中	
学习截止日:	2017-10-25 16:08:32	
描述:	请输入描述	

注意:

1、Oracle 数据库需要正确选择该数据库所使用的字符集,其他数据库不需要设置。

2、点击【自动获取】输入数据库主机 IP、数据库主机端口、数据库实例名、用户名、密码, 单击"确认"按钮,可以自动获取数据库版本, 0racle 数据库同时会获取到字符集。

3、防护状态: 云数据库防火墙系统默认保护模式为学习模式,并且默认 7 天后自动切换为 保护模式。学习模式下所有的数据库访问行为都将被放行。即使命中了规则,语句也不会被 阻断,以保证业务系统的正常行为,但系统会记录下所有的 SQL 语句,同时也将记录下语句 被哪些策略所命中。学习模式下脱敏规则仍会正常执行。系统默认 7 天为一个学期周期,学 习期满自动切换至保护模式。也可在此直接设置为保护模式,但是不建议这样设置,因为直 接进入保护模式系统就无法建立应用系统的特征模型,很可能使正常的应用系统行为被误 判,导致被中断会话或拦截。建议按照应用系统使用的周期来设置学习模式的学习周期。

3、在"网络设置"页中输入被保护数据库实例 IP 址和端口号,"代理组"列中选择"管理接口"



和"端口号",如下图所示。

网络设置		IP
地址:端口号(动态端口)	代理组	操作
60.205.117.149 : 3306	管理接口	
	10 10	000
	10	002

4、然后点击"操作"列中的"保存"图标,如下图所示。

			14 T
网络设置			IP
地址:端口号(动态端口)	代理组		揭作
60.205.117.149 : 3306	管理接口	v	
		10000	
		10001	
		10002	

5、点击"保存"图标,如下图所示。

DP				
				×
数据库名称:	mysql			
数据库类型:	MySql			٣
数据库版本:	5.6		•	自动获取
部署模式:	代理			•
防护状态:	🧿 学习中 🔘	保护中		
学习截止日:	2017-10-2	5 16:08:32		
描述:	请输入描述			
网络设置				IP
地址:端口号(动态端口)		代理组		操作
60.205.117.149: 3306		192.168.233.245: 10000		l i
				0

2.5.2.2 添加云服务商提供的数据库服务实例(如 RDS 数据库)

1、进入安全管理员界面后点击【配置】->【数据库】,进入数据库列表页,然后点击"增加数据 库"图标,如下图所示:

云数据库 防火墙系统	♠ 概況	📩 风险	🛛 行为	■ 报表	🖲 規则	🔤 康安全		G6 维护			🙆 secadain	
数据库 ── 用户管理	角色管理	告警设置	应用身份	IP名称管理								
查询条件												
数据库类型: 请	选择数据类型 .		٣		数据库名称:	请输入数据库名	积					
数据库列表											 •(
数据库名称		数据库类型		数据	牟版本		防护状态		部署模式	操作		
表中数据为空												
					E	页下页						

2、在弹出"添加数据库"页面中填写被保护的数据库实例相关信息。如下图所示:

8		X
数据库名称:	mysql-RDS111	
数据库类型:	MySql	¥
数据库版本:	5.6	
部署模式:	代理	T
集群分区:	SLB1_分区1	•
防护状态:	● 学习中 🔹 保护中 7天后切换为保护状态	
学习截止日:	2019-01-30 15:49:41	
建模分组:		
学习规则:	▼ 默认规则	
	自动添加学习期未命中规则	
描述:	「清輸入描述	
* * *		

注意:

1、Oracle数据库需要正确选择该数据库所使用的字符集,其他数据库不需要设置。

2、点击【自动获取】输入数据库主机 IP、数据库主机端口、数据库实例名、用户名、密码, 单击"确认"按钮,可以自动获取数据库版本,0racle数据库同时会获取到字符集。

3、防护状态:云数据库防火墙系统默认保护模式为学习模式,并且默认7天后自动切换为保护模式。学习模式下所有的数据库访问行为都将被放行。即使命中了规则,语句也不会被阻断,以保证业务系统的正常行为,但系统会记录下所有的 SQL 语句,同时也将记录下语句被哪些策略所命中。学习模式下脱敏规则仍会正常执行。系统默认7天为一个学期周期,学



习期满自动切换至保护模式。也可在此直接设置为保护模式,但是不建议这样设置,因为直 接进入保护模式系统就无法建立应用系统的特征模型,很可能使正常的应用系统行为被误 判,导致被中断会话或拦截。建议按照应用系统使用的周期来设置学习模式的学习周期。

3、在"网络设置"页中的"地址:端口号(动态端口)"列中输入被保护云服务商提供的数据库服务(如 RDS 数据库)实例的连接字符串域名和端口号,"代理组"列中选择"管理接口"和"端口号",如下图所示。

网络设置		ЯI
地址:端口号(动态端口)	代理组	操作
rm-2ze6rp09t67mjn: 3306	管理接口 ▼ 10001 ▼	

4、点击"操作"列中的"保存"图标,如下图所示。

网络设置		₽
地址:端口号(动态端口)	代理组	操作
rm-2ze6rp09t67mjr : 3306	管理接口 ▼ 10001	• • •

5、点击"保存"图标,如下图所示。





			>
数据库名称:	mysql-RDS111		
数据库类型:	MySql		۲
数据库版本:	5.6	▼	自动获取
部署模式:	代理		•
集群分区:	SLB1_分区1		•
防护状态:	⊙ 学习中 🔵	保护中 7天后切换为保护状态	
学习截止日:	🛅 2019-01-30 ⁻	15:49:41	
建模分组:	マ客户端IP		
学习规则:	✔──默认规则		
	自动添加学习期	未命中规则	
描述:	请输入描述		
网络设置			₽
地址:端口号(动态端口)		代理组	操作
	ql.rds.aliyuncs.co	192.168.235.201: 10001	

2.6 设置虚拟补丁规则

1、进入安全管理员界面,点击【规则】->【虚拟补丁管理】,进入虚拟补丁列表页,然后在"查 询条件"项中的"数据库名称"下拉列表中选择被保护的数据库实例。如下图所示。

	会 #	既 👍 风险 🖙 行为	学习期	■ 报表	◎ 规则 🔡	应用 🖌 配置	G 维护		¢ º	(3) secadmi	n E+	退出
虚拟	补丁查试	虚拟补丁管理 规则	管理 规则启用	语句规则								
查询	条件										(查询
*	如据库名和	R : mysql-RDS111	漏洞库类	型: 全部	•	风险级别	: 全部	▼ 启用状态:	全部		•	
	CVE标识	R:) *	称:		CNNVD标识	CNNVD					
虚拟	补丁列目	请选择数据库 ▼									00	8
ALLIN		R Mysq+RDS111										
	序号	漏洞名称	CVE标识	CNNVD	漏洞类型	<u>9</u>	影响范围	风险组	別 告警通知	控制动作	状态	
	1	GEOMETRYCOLLECTIONFROMWKB存储	过程 CVE-2009-4019	CNNVD-200911	-313 拒绝服务	All MySQL		4	. –	放行	0	-
	2	UpdateXML或ExtractValue中存在拒绝	CVE-2009-0819	CNNVD-200903	-100 拒绝服务	All MySQL		4		放行	0	
	3	带有ROLLUP的IN或CASE语句存在拒绝	【务】 CVE-2010-3678	CNNVD-201101	-112 拒绝服务	All MySQL		4	. –	放行	0	
	4	CREATE TEMPORARY TABLE中存在拒绝	限例 CVE-2010-3680	CNNVD-201101	-114 拒绝服务	All MySQL		4		放行	0	
	5	语句"SELECT UNION ORDER BY	SELE CVE-2010-3682	CNNVD-201101	-116 拒绝服务	All MySQL		4	. –	放行	0	
	6	LOAD_FILE存在漏洞			未知类型	All MySQL		4	. –	放行	0	
	7	可能的数据提取			未知类型	All MySQL		4		放行	0	
	8	对information_schema.user_privilege	表的		访问敏感组件	All MySQL		4	. –	放行	0	
	9	对information_schema.schemata表的	可疑问		访问敏感组件	All MySQL		4	. –	放行	0	
	10	对mysql.db表的可疑访问			访问敏感组件	All MySQL		4		放行	0	
	11	对mysql.user表的可疑访问			访问敏感组件	All MySQL		4	. –	放行	0	
	12	对information_schema.tables表的可能	访问		访问敏感组件	All MySQL		4	-	放行	0	
	13	对information_schema.columns表的可	礙访		访问敏感组件	All MySQL		4	-	放行	0	
	14	INDEX DIRECTORY, DATA DIRECTORY, O	REA1 CVE-2007-5969	CNNVD-200712	-083 权限提升	All MySQL		4	-	放行	0	-

^{2、}在"虚拟补丁列表"页中即会显示未启用的系统默认规则,然后选择需要启用的规则,点击



"启用"图标,如下图所示。

	合 概	兄 🛕 风险 🖙 行为	学习期	■ 报表 🤇	⑤ 规则 🔡 应归	用 🌶 配置	G 维护			¢ 0	(3) secadmin	[→ 退出
虚拟	补丁查询	虚拟补丁管理 规则	管理 规则启用	语句规则								
查询]条件											童洵
1	数据库名称	mysql-RDS111	漏洞库类	월: 全部	•	风险级别:	全部	• 5	自用状态: 全i	部		•
	CVE标识	: CVE	名称	\$:		CNNVD标识:	CNNVD					
虚拟	は补丁列表										[000
	序号	漏洞名称	CVE标识	CNNVD	漏洞类型		影响范围		风险级别	告警通知	控制动作	状态
۲	1	GEOMETRYCOLLECTIONFROMWKB存储	过程 CVE-2009-4019	CNNVD-200911-3	13 拒绝服务	All MySQL			A	-	放行	O ^
	2	JpdateXML或ExtractValue中存在拒绝的	段务社 CVE-2009-0819	CNNVD-200903-1	00 拒绝服务	Att MySQL			A	-	放行	0
	3	带有ROLLUP的IN或CASE语句存在拒绝的	長寿	CNNVD-201101 1	12 拒绝服务	All MySQL			4	-	放行	0
	4	CREATE TEMPORARY TABLE中存在拒绝	服务 CVE-2010-3680	CNNVD-201101-1	14 拒绝服务	All MySQL			4	-	放行	0
	5	春句"SELECT LIN ION ORDER BY (SELE CVE-2010-3682	CNNVD-201101-1	16 拒绝服务	All MySQL			4	-	放行	0
	6	_OAD_FILE存在漏洞			未知类型	All MySQL			A	-	放行	0
	7	可能的数据提取			未知类型	All MySQL			4	-	放行	0
	8	对information_schema.user_privilege	表的		访问敏感组件	All MySQL			4	-	放行	0
	9	对information_schema.schemata表的	可疑问		访问敏感组件	All MySQL			4	-	放行	0
	10	对mysql.db表的可疑访问			访问敏感组件	All MySQL			4	-	放行	0
	- 11	对mysql.user表的可疑访问			访问敏感组件	All MySQL			A	-	放行	0
	12	对information_schema.tables表的可编	1 1 519		访问敏感组件	All MySQL			A	-	放行	0
	13	对information_schema.columns表的可	疑论		访问敏感组件	All MySQL			4	-	放行	0
	14	INDEX DIRECTORY, DATA DIRECTORY, C	REA1 CVE-2007-5969	CNNVD-200712-0	83 权限提升	All MySQL			4	-	放行	•

3、点击"立即应用新的防护规则"图标,如下图所示。

	合概	兄 👍 风险 🔅	🛛 行为	学习期	田 报表	18 AQU 🔡 I	立用 🖌 配置	い いちゅう ほう ほう ほう ほう ほう ほう ほう しゅう しゅう しゅう しゅう しゅう しゅう しゅう しゅう しゅう しゅ	V	¢ 0	ecadmin	· E·	• 退出
虚拟	小丁查询	虚拟补丁管理	规则管理	规则启用	语句规则				[点击]	立即应用新的	的防护规则! X		
查询	条件											[查询
ž	据库名称	mysql-RDS111	•	漏洞库类型	: 全部	•	风险级别	全部	▼ 启用状态: 全	部		•	
	CVE标识	: CVE		名称	:		CNNVD标识:	CNNVD					
-													
虚拟	补」列表											00	9
	序号	漏洞名称		CVE标识	CNNVD	漏洞类型	1	影响范围	风险级别	告警通知	控制动作	状态	
	1 (GEOMETRYCOLLECTIONFROM	WKB存储过程	CVE-2009-4019	CNNVD-200911-	313 拒绝服务	All MySQL		A	-	放行	\bigcirc	-
	2	JpdateXML或ExtractValue中有	存在拒绝服务)	CVE-2009-0819	CNNVD-200903-	100 拒绝服务	All MySQL		A	-	放行	\odot	
	3 1	带有ROLLUP的IN或CASE语句有	F在拒绝服务》	CVE-2010-3678	CNNVD-201101-	112 拒绝服务	All MySQL		A	-	放行	\odot	
	4 (CREATE TEMPORARY TABLE	存在拒绝服务	CVE-2010-3680	CNNVD-201101-	114 拒绝服务	All MySQL		A	-	放行	\odot	
	5 i	吾句"SELECT UNION ORI	DER BY (SELE	CVE-2010-3682	CNNVD-201101-	116 拒绝服务	All MySQL		A	-	放行	\bigcirc	
	6 1	_OAD_FILE存在漏洞				未知类型	All MySQL		A	-	放行	\bigcirc	
	7	可能的数据提取				未知类型	All MySQL		A	-	放行	\bigcirc	
	8 5	∃information_schema.user_p	privileges表的			访问敏感组件	All MySQL		A	-	放行	\bigcirc	
	9 3	dinformation_schema.schem	ata表的可疑i			访问敏感组件	All MySQL		A	-	放行	\bigcirc	
	10 3	时mysql.db表的可疑访问				访问敏感组件	All MySQL		A	-	放行	\bigcirc	
	11 5	对mysql.user表的可解访问				访问敏感组件	All MySQL		A	-	放行	\bigcirc	
	12 5	ಠinformation_schema.tables	表的可疑访问			访问敏感组件	All MySQL		A	-	放行	\bigcirc	
	13	तिinformation_schema.colum	ns表的可疑访			访问敏感组件	All MySQL		A	-	放行	\bigcirc	
	14	NDEX DIRECTORY, DATA DIREC	TORY,CREAT	CVE-2007-5969	CNNVD-200712-	083 权限提升	All MySQL		A	-	放行	\odot	-

4、在弹出的窗口上点击"确定",如下图所示。



	合相	院 🎄 风险 🖙 行为	学习期	■ 报表 🛛 🔞	规则 📲 应用	▶配置	译 维护	Ø	¢ 0	💧 secadmii	n E+i	退出
虚拟	补丁查询	」 虚拟补丁管理 规则管	理 规则启用	语句规则				[点击]	立即应用新的	的防护规则 ×		
查询	条件										童	询
큀	如据库名称	: mysql-RDS111	漏洞库关型	1: 全部	•	风险级别: 全部	β •]	启用状态: 全i	BB		-	
	CVE标识	: CVE	名称	•		CNNVD标识: CN	NVD					
虚拟	补丁列录	Ę										₽
	序号	漏洞名称	CVE标识	CNNVD	漏洞类型		影响范围	风险级别	告警通知	控制动作	状态	
	1	GEOMETRYCOLLECTIONFROMWKB存储过程	CVE-2009-4019	CNNVD-200911-313	気体的な	ALL HUGOL		A	-		\odot	4
	2	UpdateXML或ExtractValue中存在拒绝服务	CVE-2009-0819	CNNVD-200903-100	信息	×		Δ	-		\bigcirc	
	3	带有ROLLUP的IN或CASE语句存在拒绝服务	CVE-2010-3678	CNNVD-201101-112	· · · · · · · · · · · · · · · · · · ·	±000 2		A	-		\odot	
	4	CREATE TEMPORARY TABLE中存在拒绝服	第 CVE-2010-3680	CNNVD-201101-114	441人5元 主众	16230		A	-		\odot	
	5	语句"SELECT UNION ORDER BY (SEL	E CVE-2010-3682	CNNVD-201101-116		确认 取消		A	-		\odot	
	6	LOAD_FILE存在漏洞				·		A	-		\odot	
	7	可能的数据提取			未知类型	All MySQL		A	-		\odot	
	8	对information_schema.user_privileges表	r:		访问敏感组件	All MySQL		A	-		\odot	
	9	对information_schema.schemata表的可影	Êì		访问敏感组件	All MySQL		A	-		\odot	
	10	对mysql.db表的可疑访问			访问敏感组件	All MySQL		A	-		\odot	
	11	对mysql.user表的可疑访问			访问敏感组件	All MySQL		A	-		\odot	
	12	对information_schema.tables表的可疑访	ē,		访问敏感组件	All MySQL		A	-		\odot	
	13	对information_schema.columns表的可疑	ź		访问敏感组件	All MySQL		A	-		\odot	
	14	INDEX DIRECTORY, DATA DIRECTORY, CREA	CVE-2007-5969	CNNVD-200712-083	权限提升	All MySQL		A	-		\odot	-

2.7 设置防火墙规则

1、进入安全管理员界面,点击【规则】->【规则启用】,然后在"查询条件"页中的"数据库" 下拉列表中选择被保护的数据库实例。如下图所示。

	合 概況	📩 风险	🖾 行为	学习期	■ 报表	◎ 规则	■ 应用	₽ 配置	G 维护			¢ º	🕒 se	cadmin	[→ 退出
虚找	补丁査询	虚拟补丁管理	规则管理	规则启用	语句规	则	_								
查询	除件														查询
	数据库 : (mysql-RDS111	•	规则名称	: 规则名称			规则类型:	全部	¥	规则组:	全部		٣	
	风险级别:	请选择数据库 mysql-RDS111		是否启用	: 巳启用		٣								
规则	列表													<u>⊼ ⊻</u>	0 4
	序号					规	则名称					规则类型	风险级别	操作	乍
							当前查	间无数据							

2、在"查询条件"页的"是否启用"下拉列表选项中选择"未启用",如下图所示。

	🚖 概況	📩 风险	🕑 行为	学习期	■ 报表	⑧ 规则	■ 应用	≁ 配置	尾 维护		¢ º	ecadmin	[→ 退出
虚拟补丁	「查询	虚拟补丁管理	规则管理	规则启用	语句规则	I							
查询条件	4												童询
đ	数据库:	mysql-RDS111	Ŧ	规则名称	: 规则名称			规则类型:	全部	Ŧ	规则组: 全部		¥
×.	检级别:	全部	٣	是否启用	: 未启用		*						
规则列表	表				日启用	V							0

3、"规则列表"页中即会自动显示未启用的规则,然后选择需要启用的规则,点击"启用"图标,



如下图所示。

	٨	概況	📥 风险	🕑 行为	学习期	■ 报表	စ 規则	₩ 应用	₽ 配置	☞ 维护			Ļ	© 0	secadmin	[→ 退出
虚拟	补丁查	询	虚拟补丁管理	规则管理	规则启用	语句规	则									
查询	条件															查询
	数据	罅:[mysql-RDS111	•	规则名利	: 规则名称			规则类型:	全部	¥	规则组:	全部		•	
	风险级	题: [全部	•	是否启用	: 未启用		Ŧ								
规则	列表															
	夜号						±6101	28					011216780	Fil 80483 201	操作	
	1	\$E87	间内实力登录失败[涌日	840 DI 481				H400					今政击	0		
	2	MyS	ql-数据库用户密码泄露	[MySql默认规则组]					_				「「「「「「「「」」」	0	0	
	3	MyS	ql·系统表非法操作[MyS	ql默认规则组]								括	作规则	0	0	
	4	商危	操作[通用规则组]									括	作规则	0	0	
	5	权限	变更[通用规则组]									括	作规则	0	0	
	6	批量	数据篡改[通用规则组]									括	能作规则	0	0	
	7	批量	- 数据泄露[通用规则组]									拔	作规则	0	0	
	8	无w	here更新或删除[通用规	[[[]])组]								括	作规则	0	0	
	9	可難	的创建存储过程和包操	作[通用规则组]								报	1作规则	0	0	
1	10	可幾	的视图操作[通用规则缘	3)								扬	作规则	0	0	
	-11	MyS	ql-系统表查询操作[MyS	ql默认规则组]								括	作规则	Ø	0	
	12	MyS	ql-SQL中包含注入常用的	的时间函数[MySql默	认规则组]							注	入攻击	U	0	
	13	MyS	ql-SQL中包含注入常用的	的字符串函数[MySql	【默认规则组】							注	入攻击	0	0	
	14	MyS	ql-SQL中包含获取数据原	车用户名的函数[My!	5ql默认规则组]							注	入攻击	0	0	•

4、点击"立即应用新的防护规则"图标,如下图所示。

	😭 概況	📩 风险	🖾 行为	学习期	🖬 报表	စ 规则	■ 应用	₽ 配置	G 维护		¢ 🗹	1 ⁰ 🙆 s	secadmin	[→ 退出
虚拟	补丁查询	虚拟补丁管理	规则管理	规则启用	语句规	LAI					[点击]立即。	应用新的防护	舰则! ×	
查询	条件													童询
	数据库:	mysql-RDS111	Ŧ	规则名	称: 规则名称			规则类型:	全部	T	规则组: 全部		٣	
	风险级别:	全部	٣	是否启	用: 未启用		¥							
规则	列表													\bigcirc
	序号					规则	名称				规则类型	风险级别	操作	
							当前查	间无数据						

5、在弹出的窗口上点击"确定",如下图所示。

	合 概況	📩 风险			田 报表	囫 规则	🔡 应用	₩ 配置	G 维护		ې ا	. ⁰ (5) se	ecadmin	
虚拟	补丁查询	虚拟补丁管理	规则管理	规则启用	语句规	LQJ					[点击]立即的	应用新的防护规	则 ×	
查询	条件													查询
	数据库:	mysql-RDS111	¥	规则名	称 : 规则名称			规则类型:	全部	* #	2014:全部		٣	
	风险级别:	全部	¥	是否启	用:(未启用		Y							
规则	列表													Ø
	序号					规则	名称				规则类型	风险级别	操作	
						信	息		×					
						72		wo l						
						94	10.8%—±30.989							
								确认 取消	θ					



2.8 配置负载均衡

1、创建一个负载均衡 SLB, 创建完成后, 点击"点我开始配置", 如下图所示。

实例名称/ID	服务地址 🏹	状态 🏹	监控	端□/健康检查/后端服务器 >>	操作
防火墙集群 Ib-2zeo1xtnfvj0vll55zcea 未设置标签	192.168.235.115(专有网络) vpc-2ze5zzip65nhatf4j8qc4 vsw-2zekxu4l7stcv4gpa0zzy	●已停止	1	点我开始配置	监听配置向导 添加后端服务器 更多 >>

2、选择负载均衡协议为 TCP, 配置负载均衡对外服务提供的端口为 10001, 高级配置中根据实际 情况选择适当的调度算法, 其他参数默认,, 点击"下一步", 如下图所示。

协议&监听	后端服务器	健康检查	配置审核
选择负载均衡协议			
TCP UDP HTTP HTTPS			
后端协议			
TCP			
• 监听端口 🔘			-
10001			
高級配置 收起 《			
• 调度算法			
<u>加权給询 (WRR)</u> 加权最小连接数 (WLC)	\$论词 (RR)		
开启会话保持 🔘			
启用访问控制 💿			
开启监听带宽限速 💿			
连接超时时间 🔘			
900	Đ		
TCP語時時间輸入范围为10-900秒			
监听名称 🌚			

负载均衡支持如下三种调度算法如下,可以根据实际情况调整:

加权轮询:权重值越高的后端服务器,被轮询到的次数(概率)也越高;

加权最小连接数(WLC):除了根据每台后端服务器设定的权重值来进行轮询,同时还考虑后端服务器的实际负载(即连接数)。当权重值相同时,当前连接数越小的后端服务器被轮询到的次数(概率)也越高;

轮询 (RR): 按照访问顺序依次将外部请求依序分发到后端服务器。

3、添加后端服务器用于处理负载均衡接收到的访问请求,选择默认服务器组,并将相应的 kernel 节点添加到该服务器组中,根据实际需要,配置每台 kernel 节点的端口和权重,点击"下一步",如下图所示。



非择将监听请求转发至哪类后端服务器					
虚拟服务器组	默认服务器组 主备	服务器组			
ā加服务器					_
云服务器ID/名称	公网/内网IP地址	第日	权重	操作	
kernel-1 -2zehvinitb22rzngnod	47.93.51.127(公) 192.168.235.202(私有) vpc-2ze5zzip65nhatf4j8qc4 vsw-2zeiocu4(7stcv4gpa0zzy	10001	50	859	
kernel-2 2zechx5nf4cg40nyj513	39.96.15.180(公) 192.168.235.199(私告知 vpc-2ze5zzip65nhatf4j8qc4 vsw-2zelxxu4/7stcv4gpa0zzy	10001	50 4 h#×	###	
Sections, Hanks , Hebris	9259-1971				

4、配置健康检查,健康检查端口配置为9301,其他健康检查参数可以使用默认值,或者根据实际需要进行配置,点击"下一步",如下图所示。

配置健康检查		⑦ 配置健康检查	
① 配置健康检查能够让负载均衡自动排除健康状况异常的后端服务器			
开启健康检查			
			_
高级配置 收起 《			1
• 健康检查协议 💿			
● TCP ◯ HTTP			
健康检查端口 💿			
9301			
·			
•健康检查响应超时时间 💿			
5	砂		
输入范围1-300秒, 默认为5秒			
•健康检查问隔时问 💿			
2	秒		
输入范围1-50秒,默认为2秒			t
•健康检查健康间值 💿			1
3	次		1
健康检查健康调值为2-10			1
• 健康检查不健康阈值 💿			
3	次		
健康检查不健康调度为2-10			
上一步 取消			

5、配置审核,所有配置信息审核通过后,点击'提交'按钮,如下图所示。



负载均衡业务配置向导	1週回						③监听介
	协议&监听	后旗服务器		健康检查		配置車核	
配置审核							
协议&监听							修改
负载均衡协议 TCP			监听跳口 10001				
加权轮询			安运保持 关闭				
访问控制 关闭			带觉峰值 不限制				
连接超时时间 900 秒							
健康检查							修改
健康检查 已开启			健康检查协议 TCP				
健康检查施口 9301			健康检查响应超时时间 5 秒				
健康检查间隔时间 2秒			健康检查健康调值 3 次				
健康检查不健康阈值							
后洪服务器							修改
默认服务器组							
云服务器(D/名称		公网/内网IP地址	第日		权重		
kernel-1 i-2zehvlnilb22rzngnod		47,93.51.127(公) 192.168.235.202(信/約) vpc-2ze5:22565hat#14jqc4 vsw-2zekxu4/Tstcv4gpa0zzy	10001		50		
kernel-2 i-2zechx5nf4cg40nyj513	8	39.96.15.180(☆) 192.168.235.198(私/約) yep-22es52pt65matf49gp4 vsw-2zekou4/7stcv4gpa0zzy	10001		50		
1	E78						

6、负载均衡配置并启动监听成功后,如下图所示。

负载均衡业务配置向	导う返回		
ł	办议&监听	后端服务器	
配置审核			
默认服务 器 组			成功
四层负载均衡			成功
启动监听			成功

2.9 部署测试

修改应用或使用 Navicat 等客户端工具,配置连接信息,将连接到数据库的 ip 和端口指定为 SLB 的 ip 和代理端口,通过代理转发的方式访问数据库。执行相关操作,查看防护效果。

注意:必须连接代理服务器,而不是原数据库。原则上原数据库应该不允许代理服务器及应 用系统之外的地址访问。