# 阿里云 数据库审计

# 用户指南(A100)

文档版本: 20190807

为了无法计算的价值 | [] 阿里云

### <u>法律声明</u>

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。
- 3. 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

格式	说明	样例
•	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: 重置操作将丢失用户配置数据。
A	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。
	用于补充说明、最佳实践、窍门等,不 是用户必须了解的内容。	道 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。
##	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。	<pre>swich {stand   slave}</pre>

# 目录

法律声明	I
通用约定	I
1 启用数据库审计实例	1
2 管理数据库审计实例	3
3 登录数据库审计系统	5
4 添加数据库实例	7
5 部署Agent程序	
6 查看系统审计到的语句	24
7 查看SOL语句存储空间用量	
8 开启系统管理员和系统审计员角色	
9 常见问题	
9.1 安装Agent提示错误	
9.2 跨地域、VPC、账号部署场景常见问题	
9.3 无法打开云数据库审计控制台	
9.4 Windows安装Agent选项	

# 1 启用数据库审计实例

购买数据库审计实例后,您需要启用实例,才能登录数据库审计系统并使用审计服务。

操作步骤

- 1. 登录云盾数据库审计管理控制台。
- 2. 在我的审计页面,选择要启用的数据库审计实例,单击其操作列下的启用。
- 3. 在实例启用对话框中,完成以下配置,并单击确定。

配置项	说明
网络	单击选择安全组,并选择ECS实例的安全组,确保数据库审计系 统可以访问相应的ECS云服务器。
	<ul> <li>如果要审计的数据库是ECS上的自建数据库,选择ECS实例的 安全组。</li> <li>如果要审计的数据库是RDS云数据库,选择作为应用服务器连 接该数据库的ECS实例的安全组。</li> </ul>
内网访问控制	设置内网访问白名单。

配置项	说明
公网访问控制	选择公网访问控制策略,取值:
	<ul> <li>・ 不对公网开放</li> <li>・ 对公网白名单开放</li> <li>・ 对公网全网开放</li> </ul>

实例启用	×
* 网络:	经典网络类型和交换机在实例启用后将无法修改。
	■ 选择安全组
	请选择ECS对应的安全组,允许数据库审计通过该网络访问您的ECS,可多选,可修 改。
内网访问 控制:	请输入IP
	请输入VPN IP地址,以英文;分开,最多30个。
*公网访问	◎ 不对公网开放
控制:	◎ 对公网白名单开放
	受 对公网全部开放
注意:安全	:组+内网IP+公网白名单的总数量,不能超过30条!
	确定 关闭

数据库审计实例将自动开始初始化,初始化过程一般需要40分钟左右。

我的审计			(( 4 )) 2			的复数影响时
实例D	版本授权	地域	Rts	3040010	秋志(全部) マ	操作
dbaudit-cn-4590)bk6001	版本:32.36 专业版	印东 1	经典网络	2018-04-28 00:00:00	初始化中	清40分钟后刷新页面查看状态

4. 耐心等待系统初始化完成后,刷新页面。

### 预期结果

成功初始化数据库审计实例。

### 后续步骤

登录数据库审计系统

### 2 管理数据库审计实例

购买数据库审计实例后,您可以在云盾数据库审计管理控制台管理您的数据库审计实例。

背景信息

参照以下步骤管理您的数据库审核实例:

#### 操作步骤

- 1. 登录云盾数据库审计管理控制台。
- 2. 查看您已购买的数据库审计实例的套餐、版本号、地域、网络、到期时间、状态等信息。

1000401						RECEIPTION
880	8644297	354	194	200101	HSORE +	18.9
dault o	164:3236 9338	10.96 1	OARS		02	NG RGRX ISB
dault o	10(10) 32.12 6:500	1001	104/01		112	10 10 10
daudi ci	804:32.9 2008	100.1	10400		112	10 70 7052
dault c	新年:32.12 年末前	100.1	0488		112	RE Rest
dautho	制度:33.13 企业时	99/2	0400		<b>n</b> it	110 710 71052

- 3. 管理您的数据库审计实例。
  - · 网络配置:单击网络配置,您可以修改该数据库审计实例的安全组或者设置该数据库审计系统的内网和公网访问控制策略。



- 针对数据库审计系统设置的内网和公网访问控制策略均通过白名单方式配置。

网络配置	×
*网络:	经典网络类型和交换机在实例启用后将无法修改。
	<b>重新选择安全组</b> 已选择4个安全组
	请选择ECS对应的安全组,允许数据库审计通过该网络访问您的ECS,可多选,可修改。
内网访问 控制:	1.1.1.2,1.1.2.2
	请输入VPN IP地址,以英文; 分开,最多30个。
• 公网访问	◎ 不对公网开放
控制:	◎ 对公网白名单开放
	● 对公网全部开放
注意:安全	组+内网IP+公网白名单的总数量,不能超过30条!
	<b>確定</b> 关闭

#### - 安全组、内网白名单IP、公网白名单IP的访问控制规则总数量不能超过30条。

·升级:单击升级,并确认升级,可以将您的数据库审计系统升级到最新版本。如果您当前的 数据库审计系统已经是最新版本,升级按钮将不显示。

### 📃 说明:

升级过程中该数据库审计系统将停止服务,期间将无法该数据库审计系统中的数据库进行审 计,整个升级过程一般需要10分钟左右。

·续费:单击续费,您可以为该数据库审计实例续费,延长该实例的服务时长。数据库审计实例到期后将无法续费,请您关注您的数据库审计实例的到期时间及时续费。



您需要将数据库审计系统的版本升级到最新才可进行续费,续费时长仅支持选择一年。

# 3 登录数据库审计系统

数据库审计系统初始化完成后,您可以从云盾数据库审计管理控制台登录数据库审计系统。

#### 操作步骤

- 1. 登录云盾数据库审计管理控制台。
- 2. 在我的审计页面,选择要登录的数据库审计实例,单击其操作列下的管理。

1 R8241						PCENSIVE/2
880	804892	104	100	108101	955(88) +	16.7
diameter .	804:3235 1938	100.1	04000		91X	10 70 70 70 70
disult of	1011   3.2.12 \$2.010	0181	0405		11	10 70 70042
daadi ee	804 : 3.2.12 2008	1981	0405		912	UII Fill Product
daut et	80% : 3.2.12 \$1281	100	04001		92	110 7-0 700422
diandi en	804 : 52.52 0.080	05.2	04005		80	uti Fili Feedaa

3. 在管理对话框中,单击内网接入或公网接入。

### 蕢 说明:

如果选择内网接入,请确认本地客户端可连通该内网环境。如果所选择的数据库审计实例 在VPC专有网络中,您需要先通过VPN方式接入该VPC专有网络环境,再登录数据库审计系 统。

管理	×
请选择以私网(券 连接方式访问数1	效据库审计部署在VPC中,连接前您需先通过VPN接入VPC,再点私网连接)还是公网 居库审计控制台:
内网接入	公网接入
10	116
	取消

#### 预期结果

成功登录数据库审计系统。

云盾•数据库审计	<b>的</b> 戰況 國 报表	O℃配置 ▶维护			■(0) ▲1769112740192985 -   0+ 退出
	1940 <b>0</b> Patol <b>0</b> 4	0 \$1700 O			
<ul> <li>(2) 最近300910 最近2041 最近12041</li> </ul>	今天 昨天 本用 上用 本月 上月	自意义			4001
风险分布	第尺約 ■ 中尺約 ■ 任尺約	会话统计 ■ #i#	0.000 🔲 ARONR — MRONR	SQLSH	III DML IIII DCL III 并把规模作
4.7		1.0		4.0	
5		5	5	5	
00	50 10.00	009.40	09.50 10.00 0	0	09.50 10.00
+142055809					
数据版 的复数电子数 O	F地址个概 0	調査入実績学			

### 后续步骤

添加数据库实例

### 4 添加数据库实例

购买数据库审计实例后,您需要在数据库审计系统中添加云环境中的数据库进行审计。数据库审计 系统支持添加ECS云服务器自建数据库和RDS云数据库实例进行审计,您可以根据自身云环境中的 数据库的实际部署方式进行添加。

#### 添加ECS云服务器自建数据库

- 1. 登录数据库审计系统。
- 2. 在概况页面,单击添加数据库。

云盾•数据库审计	<b>必</b> 概況 国 服表	Q\$ 配置 ▶ 维护			■(0) ▲1769112740192985 -   (* 退出
	1600 <b>0</b> R120 <b>0</b>	今日高句 <b>0</b> 今日月始 <b>0</b>			
<ul> <li>(0) (0.0300)(0) (0.0520)(1)</li> <li>(0) (0.0520)(0) (0.0520)(1)</li> <li>(0) (0, 0) (0, 0) (0, 0)</li> <li>(0) (0, 0)<th>最近12小时 今天 昨天 本周 上周 本月 上川</th><th>) mæx</th><th></th><th></th><th>MIN .</th></li></ul>	最近12小时 今天 昨天 本周 上周 本月 上川	) mæx			MIN .
风险分布 10	#R01 +R01 = 65831	会话统计 ■ 1 10	нислик 🔲 якслик — мислик 10	SQL分布 10	DML DCL PRISIP/F
s		s	s	5	
0 09.40	09.50 10.00	009.40	09.50 10.00 0	009.40	09.50 10.00
+1820/0304					
NR RS	時个数 0 序地址个数 0	第第人文録字 Q			

3. 在添加数据库区域、填写要审计的数据库的相关信息、并单击保存。

+16100301							
添加較服库							
数据库名			0	多地址	1	描述	
数据库类型	Oracle	٠	IP地址				
数据库版本	9.1.0.0	٠	第口	日 助态		(84) <b>10</b> 56	0
选择字符集	ZHS16GBK	٠	实例名				
操作系统	Linux 64	۲					

- ·数据库名:为要审计的数据库指定一个名字。
- ·数据库类型:要审计的数据库的类型。
- ·数据库版本:数据库版本可以手动选择或者由系统自动获取。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,系统即可自动获取数据库的版本(对 于Oracle数据库同时会获取到字符集)。
- · IP地址:要审计的数据库的IP地址。
- ·端口:要审计的数据库的端口号。
- · 实例名:要审计的数据库实例的名称。



#### 此选项为选填项。如果不填写则对该ECS自建数据库下所有数据库实例进行审计。

· 描述: 要审计的数据库的注释。

#### 添加RDS云数据库实例

参照以下步骤添加RDS云数据库实例:

- 1. 登录数据库审计系统。
- 2. 在概况页面,单击添加数据库。

云后•数据库审计	<b>命</b> 脱況 国 服表	◎ 配置 ▶ 维护		<b>3</b> (0)	1769112740192985 -   0 退出
	HORE O RUCE O	0 4884 0 4884			
(0.000000 #552047 #5512048	今天 昨天 本周 上周 本月 上月	自定义			AREN
<b>风险分布</b> 10	<b>東天治 = </b> + 尺治 =	<b>会话统计 </b> #18:00.000	■ ARONA - NEGOIA 10	分布 ■ DML 10	III DCL III 并约第行
s		5	s	5	
0 09.40 09	50 10.00	009.40 09	0 1000	0 09.40 09.50	10:00
+ 16.00% EON					
<u>数据库</u> 和新市个权 0	17882-148 <b>0</b>	(清油入关键字) Q			

3. 在添加数据库区域中,填写要审计的数据库的相关信息,单击保存。

+163009309						
添加較緩库						
数据库名				) 多地址	厳密	
数据库类型	Oracle	• IP	地址			
数据库版本	9.1.0.0	•	皖口	□ 約5		· · · · · · · · · · · · · · · · · · ·
选择字符集	ZHS16GBK	· 33	例名			
操作系统	Linux 64	۲				

- ·数据库名:为要审计的RDS数据库实例指定一个名字。
- · 数据库类型:要审计的RDS数据库实例的类型。
- ·数据库版本:数据库版本可以手动选择或者由系统自动获取。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,系统会自动获取数据库的版本(对 于Oracle数据库同时会获取到字符集)。
- · IP地址:要审计的RDS数据库实例的URL连接串。
- ·端口:要审计的RDS数据库实例的端口号。
- · 实例名:要审计的RDS数据库实例的名称。



仅Oracle与Postgres类型的数据库需要填写,其他类型的数据库可以不填写。

· 描述: 为要审计的RDS数据库实例添加注释。

### 查看摘要信息

数据库添加成功后,可以在概况页面下方的数据库列表处看到已添加的数据库的摘要信息。

数据库	数据库个数 2	I	P地址个数 4	请输入关键字	Q
> sqlserver		🔪 dd			
当前		当前			
活跃会话	0 个	活跃会话	0 个		
语句压力	0 条/s	语句压力	0 条/s		
今天		今天			
风险总量	0 条	风险总量	0 条		
语句总量	0 条	语句总量	0 条		
全部		全部			
风险总量	27 条	风险总量	0 条		
语句总量	764,252 条	语句总量	0 条		
€ 信息 IP地址	t(2) 🦘 🗹 🗇	€ 信息	IP地址(2) ち 🗹 🗊		

#### 下一步

数据库添加完成后,您还需要为已添加的数据库部署Agent程序,数据库审计系统才能对您的数据 库进行审计。关于如何部署Agent程序,请参见部署Agent程序。

# 5 部署Agent程序

将数据库添加至数据库审计系统后,您需要将Agent程序部署到相应的数据库或应用服务器

上。Agent程序会获取访问数据库的流量,帮助数据库审计系统通过获取的流量实现数据库的分析 审计。

#### Agent程序部署位置

根据所添加的数据库在云环境中的实际部署方式,您需要将Agent程序部署在以下位置:

- · ECS云服务器自建数据库: Agent程序需要部署在数据库所在的ECS云服务器上。
- · RDS云数据库实例: Agent程序需要部署在对应的应用服务器上,通常为访问RDS数据库的应用系统所在服务器(ECS)。

**门** 说明:

RDS数据库里暂时无法安装配置Agent。

自动部署Agent程序

### - 说明:

Agent程序自动部署仅支持Linux系统。即对于ECS云服务器自建数据库的情况,数据库所 在的ECS云服务器必须使用Linux系统;对于RDS云数据库实例,对应的应用服务器必须 使用Linux系统。如果您需要审计的数据库所对应的服务器不是Linux系统,请查看手动部 署Agent程序。

参照以下步骤,自动部署Agent程序:

- 1. 登录云盾数据库审计系统。
- 2. 在维护页面,选择Agent管理,单击Agent自动部署。

云盾·数据库审计	48 概况	圖报表	0% 配置 ≯ 独护			🕿 (2) 🔺 secadmi	- 10-388
新聞餐台的集 Agent管理							
@ T-∰Agent	[下载Agent]下载需要	部署到被保护数	握库服务器上的Agent程序				
Agent自动部署	[Agent自动部署] 多点	用环境推荐使用	该功能部署Agent,只支持	nux®iA.			
Agent部署任置	[Agent部署配置	昰] Agent稽	i序所在服务器的IF	地址,请务必在此配置	i。如未配置,Agen	程序抓取的数据将不被审	it.

- 在Agent自动部署对话框中,按照格式填写需要部署Agent程序的服务器IP地址、ROOT用户 密码和SSH端口号,然后单击部署,即可将Agent程序自动部署到相应的服务器中。参数说明如 下:
  - ・审计服务器IP:填写数据库审计系统的IP地址,您可以在登录数据库审计系统时查看系统的内网和外网IP。如果数据库审计系统与Agent程序所在的服务器处于同一内网环境中,添加数据库审计系统的内网IP即可;如果两者不在同一内网中,则添加数据库审计系统的外网IP。
  - ・目标服务器:指需要自动部署Agent程序的服务器相关信息,格式为目标IP,root密码,ssh 端口。



Agent程序的自动部署需要服务器开通SSH端口,并且自动部署过程中需要使用ROOT用户 密码。

・如果应用服务与数据库部署在同一台服务器中,在自动部署Agent程序时,需要勾选本地回 环。

Anent自动部	3書		
Agent <b>配置:</b> □本地回环 ( ●审计服务器	应用程序与数据库在同一台机器上) 副P:		
目标服务器:	192.168.100.88,pwd,22 192.168.100.89,pwd,22	格式:	目标IP,root密码,ssh端口
查看执行日;	志		
			部署取消

4. Agent程序自动部署完成后,返回Agent管理页面,单击Agent部署配置。

5. 在Agent部署配置对话框中, 输入需要部署Agent程序的服务器IP地址, 然后单击添加。

Agent音	3零配置	
序号	IP地址	操作
1	172.17.71.212	Ð
2	192.168.0.1	8
3	192.168.0.111	<b>1</b>
IP地址:	192.168.100.88 192.168.100.89 添加	
		关闭



- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地址 即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服务器 的外网地址。
- ·如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。

手动部署Agent程序

Windows系统服务器部署Agent程序

对于Windows系统服务器,您需要根据云环境中数据库的实际部署情况选择相应的方式手动部署Agent程序。

- · 应用系统与数据库部署在不同的服务器
  - 1. 登录云盾数据库审计系统。
  - 2. 在维护页面,选择Agent管理,单击下载Agent。系统自动弹出Agent部署配置提示,单 击确定后浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下载至本地。

云后•数据库审计	的 概况 🕻	副报表 O	配置 ▶ 维护			🖴 (2) 🔺 secadmin	- 10-333
和日本的法室 Agent管理	1788年1月1日日 日本						
	(下载Agent)下载需要部	劉被保护数据库制	服务器上的Agent程序				
Agent自动部署	[Agent自动部署]多应用5	F 遺推荐使用设功者	能部署Agent,只支持inux系统。				
Agent2FEA2E	[ Agent部署配置 ]	Agent程序所	所在服务器的IP地址,	请务必在此配置。	如未配置,Agent	程序抓取的数据将不被审	it.

3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。

b)			
	说明:		

 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地 址即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服 务器的外网地址。

- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。
- 4. 将Agent程序(即rmagent.tar.gz)文件上传到需要部署Agent程序的服务器,并将其解

压缩。

L	t		-	o x
	単有	-	10	× (
$\leftarrow \rightarrow \land \downarrow$	magent >	~ O	搜索"rmagent"	م
	A 名称	修改日期	类型	大小
★ 快速访问	linux64	2017/10/31 16:01	文件夹	
	install.sh	2017/9/28 9:44	SH 文件	2 KB
🔸 下数 🕺	🐻 rmagent	2017/10/31 15:38	配置设置	1 KB
🗎 文档 🛛 🖈	궁 Rmagent_Setup	2017/9/28 9:44	应用程序	39,462 KB
No. 10 10 10 10 10 10 10 10 10 10 10 10 10	stop_rmagent.sh	2017/9/28 9:44	SH 文件	1 KB
02- 平数据库完全法				

- 5. 打开解压后的Agent程序文件夹,双击运行Rmagent\_Setup.exe程序文件。
- 6. 在Installer Language对话框中, 单击OK。

Installer l	anguage	Х
	Please select a language.	
	Chinese (Simplified) / Hanyu (Jiantizi)	$\sim$
	OK Cancel	

7. 在rmagent1.0安装对话框中,单击下一步,直到Agent程序开始安装。

<b>1</b> i	兑明:				
------------	-----	--	--	--	--

选择组件时,必须勾选VS 2015 Redistributable和WinPcap组件,在Agent程序安装过程中将自动运行相关组件的安装程序。

🌍 rmagent 1.0 安装		- 🗆 X			
<b>选择组件</b> 选择你想要安装 rmagent 1.0 的那些功能。					
勾选你想要安装的组件,并触 续。	<b>解除勾选你不希望安装的组件。</b>	单击 [下一步(Ŋ)] 继			
选定安装的组件:	<ul> <li>✓ rmagent core</li> <li>VS 2010 Redistributal</li> <li>✓ VS 2015 Redistributal</li> <li>✓ WinPcap</li> <li>npcap</li> </ul>	<b>描述</b> 停悬你的鼠标指针到 组件之上,便可见到 它的描述。			
所需空间: 28.0MB	< >>				
Nullsoft Install System v3.0	ob2场 〈上一步(P)	下一步(N) > 取消(C)			

8. 所有组件及Agent程序安装完成后,重新启动服务器,即完成Agent程序的部署。

·应用服务与数据库部署在同一台服务器的情况

- 1. 登录云盾数据库审计系统。
- 2. 在维护页面,选择Agent管理,单击下载Agent。系统自动弹出Agent部署配置提示,单 击确定后浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下载至本地。
- 3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。



 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地 址即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服 务器的外网地址。

- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。
- 4. 将Agent程序(即rmagent.tar.gz文件)文件上传到需要部署Agent程序的服务器,并将 其解压缩。
- 5. 打开解压后的Agent程序文件夹,双击运行Rmagent\_Setup.exe程序文件。
- 6. 在Installer Language对话框中,单击OK。
- 7. 在rmagent1.0安装对话框中,单击下一步,直到Agent程序开始安装。

### 📃 说明:

选择组件时,必须勾选VS 2015 Redistributable和npcap组件,在Agent程序安装过程中 将自动运行相关组件的安装程序。

💮 rmagent 1.0 安装	_		×
<b>选择组件</b> 选择你想要安装 rmagent 1.0 的那些功能。			
勾选你想要安装的组件,并解除勾选你不希望安装的组件。 续。	单击 [下—	步(N)] 维	1
送定安装的组件: 「 rmagent core 「 VS 2010 Redistributal 「 VS 2015 Redistributal WinPcap 「 mpcap	<b>描述</b> 停悬你的鼠 组件之上, 它的描述。	【标指针到 使可见到	
所需空间: 27.8MB < >			
Nullsoft Install System v3.Ob2	ऽ—步(№) >	取消	(C)

### 说明:

安装Npcap组件时,请务必勾选Install Npcap in WinPcap API-compatible Mode选项。

🌐 Npcap 0.93 Setup	– 🗆 X			
NMAP, ORG	Installation Options Please review the following options before installing Npcap 0.93			
Automatically start t	he Npcap driver at boot time			
Support loopback tra	affic ("Npcap Loopback Adapter" will be created)			
✓ Use DLT_NULL as the loopback interface' link layer protocol instead of DLT_EN10MB				
Restrict Npcap driver's access to Administrators only				
Support raw 802.11 traffic (and monitor mode) for wireless adapters				
Support 802. 1Q VLAN tag when capturing and sending data				
Install Npcap in Winf	Pcap API-compatible Mode			
Nullsoft Install System v2.51				
	< Back Install Cancel			

8. 所有组件及Agent程序安装完成后,修改C:\Users\<###>\AppData\Roaming\rmagent

\rmagent.ini文件,将其中#loopback=1一行中的#删除以解除注释,保存文件。

🥘 rmagent - 记事本	—	×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)		
[rms]		$\sim$
server_host=192.168.232.181		
#server_port=9266		
#device=eth2		
#device=tap0, tap1		
#buffer_size=200		
#queue_size=800000		
#pcap <sub>+</sub> file=e:\0_Download\rmagent.pcap		
#pcap_file_num=10		
#pcap_buffer=4		
loopback=1		
#web_server_port=80		
#nice=-20		

9. 重新启动服务器,完成Agent程序的部署。

Linux系统服务器部署Agent程序

对于Linux系统服务器,您也可以根据云环境中数据库的实际部署情况选择相应的方式手动部署 Agent程序。

- ·应用服务与数据库部署在不同的服务器的情况
  - 1. 登录云盾数据库审计系统。
  - 2. 在维护页面,选择Agent管理,单击下载Agent。系统自动弹出Agent部署配置提示,单 击确定后浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下载至本地。
  - 3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。

```
📕 说明:
```

- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地 址即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服 务器的外网地址。
- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审 计。
- 4. 以root用户登录需要安装Agent程序的服务器,将rmagent.tar.gz文件上传到服务器,并 将其解压缩。

```
[root@rsdsdf ~]# ls
anaconda-ks.cfg install.log install.log.syslog rmagent_.tar.gz
[root@rsdsdf ~]# tar -xvf rmagent_.tar.gz
./
./stop_rmagent.sh
./Rmagent_Setup.exe
./linux64/
./linux64/
./linux64/rmagent
./rmagent.ini
./install.sh
[root@rsdsdf ~]#
```

- 5. 执行chmod 755 install.sh命令,给install.sh文件增加权限。
- 6. 安装Agent程序。

```
[root@rsdsdf ~]#_./install.sh_
start rmagent ...
start rmagent success
[root@rsdsdf ~]# ^C
[root@rsdsdf ~]# _
```

7. 安装完成后, 启动Agent程序 (rmagent) 完成Agent程序的部署。

```
[root@mysql rmagent]# cd /usr/local//rmagent/
[root@mysql rmagent]# ./rmagent
[root@mysql rmagent]#
```

### ·应用服务与数据库部署在同一台服务器的情况

- 1. 登录云盾数据库审计系统。
- 2. 在维护页面,选择Agent管理,单击下载Agent。系统自动弹出Agent部署配置提示,单 击确定后浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下载至本地。
- 3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。



 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地 址即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服 务器的外网地址。

- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。
- 4. 以root用户登录需要安装Agent程序的服务器,将rmagent.tar.gz文件上传到服务器,并 将其解压缩。
- 5. 执行chmod 755 install.sh命令,给install.sh文件增加权限。
- 6. 安装Agent程序。



7. 安装完成后,进入rmagent安装目录,使用VI编辑器修改rmagent.ini配置文件,在文件 最后加入一行loopback=1,然后保存。



8. 执行./stop\_rmagent.sh命令停止rmagent进程后,执行./rmagent命令重启Agent程 序使配置更改生效,完成Agent程序的部署。



#### Agent部署注意事项

Agent程序默认连接数据库审计系统的内网IP,如果部署Agent程序的服务器与云盾数据库审计系统之间通过外网连接则需要修改rmagent.ini配置文件中的IP地址。

Windows系统服务器修改Agent程序连接地址

1. 登录数据库所在服务器或RDS数据库实例所对应的应用服务器。

2. 找到并修改C:\Users\###\AppData\Roaming\rmagent\rmagent.ini配置文件,将其中

server\_host一行的IP地址修改为云盾数据库审计系统的外网IP地址,保存文件。

🥘 rmagent - 记事本	_	×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)		
<pre>[rms] server_host=60. #server_port=9266 #device=eth2 #device=tap0, tap1 #buffer_size=200 #queue_size=800000 #pcap_file=e:\0_Download\rmagent.pcap #pcap_file=num=10 #pcap_buffer=4 #loopback=1 #web_server_port=80 #nice=-20</pre>		~

3. 重新启动rmagent服务,使配置变更生效。在服务管理器,选中Rmagent Service服务,单 击重启动此服务。

◎ 服务		-	
文件(F) 操作(A) 查看(V) 報助(H	)		
服务(本地)			
Rmagent Service	名称	描述	状态
	Remote Access Auto Con	无论什么时候,当某个程序引用一个远程 DNS 或者 N	
停止此服务	🗟 Remote Access Connecti	管理从这台计算机到 Internet 或其他远程网络的拨号…	正在运行
里后刘氏被安	Remote Desktop Configu	远程桌面配置服务(RDCS)负责需要 SYSTEM 上下文的	
	🔍 Remote Desktop Services	允许用户以交互方式连接到远程计算机。远程桌面和远…	
	🍓 Remote Desktop Service	允许为 RDP 连接重定向打印机/驱动程序/端口	
	🍓 Remote Procedure Call (	RPCSS 服务是 COM 和 DCOM 服务器的服务控制管	正在运行
	🍓 Remote Procedure Call (	在 Windows 2003 和 Windows 的早期版本中,远程…	正在运行
	Remote Registry	使远程用户能修改此计算机上的注册表设置。如果此服	
	🤹 Rmagent Service		正在运行
	Routing and Remote Acc	在局域网以及广域网环境中为企业提供路由服务。	
	🆏 RPC Endpoint Mapper	解析 RPC 接口标识符以传输端点。如果此服务被停止…	正在运行
	🆏 Secondary Logon	在不同凭据下启用启动过程。如果此服务被停止,这种	正在运行
	🖏 Secure Socket Tunneling	提供使用 VPN 连接到远程计算机的安全赛接字隧道协	正在运行
	Security Accounts Manag	启动此服务将向其他服务发出信号: 安全帐户管理器(SA	正在运行
	🖏 Security Center	WSCSVC(Windows 安全中心)服务监视并报告计算机	正在运行
	🆏 Sensor Data Service	从各种传感器传送数据	

### Linux系统服务器修改Agent程序连接地址

1. 登录数据库所在服务器或RDS数据库实例所对应的应用服务器。

2. 进入rmagent安装目录,使用VI编辑器修改rmagent.ini配置文件。



3. 将server\_host的值修改为云盾数据库审计系统的外网IP地址,然后保存。

server_host=60.205.188.19 <mark>.</mark>
~
Ne construction of the second s
Ne construction of the second s
N
•
•
~
~
INSERT

4. 执行./stop\_rmagent.sh命令停止rmagent进程后,执行./rmagent命令重启Agent程 度 使时累更改化效

序,使配置更改生效。

Agent程序部署测试

在数据库相应的服务器上成功部署Agent程序后,数据库审计系统就可以正常对您已添加的数据库 进行审计。

您可以通过使用已安装Agent程序的应用服务器访问被审计的数据库实例并执行SQL语句,然后登 录云盾数据库审计系统,查看是否已有审计信息。

- ・如果数据库审计系统正常记录了该数据库实例的审计信息,则说明数据库实例部署成功。
- ·如果数据库审计系统未能记录到审计信息,在相应的ECS云服务器上查看Agent程序的日志确认 连接是否正常。

查看Agent程序日志

Agent程序的日志一般存放在以下目录:

- Windows: C:\tmp\rmagent\rmagent\_info.log
- Linux: /tmp/rmagent/rmagent\_info.log

如果在Agent程序的日志中出现以下信息,表示Agent程序未能正确连接到数据库审计系统。

```
xml[INF0][tid=31235]20170322114351 rmagent.cpp:912:Rma_ConnectServer
connect <审计系统IP地址>:9266 failed, Connection timed out
```

解决方案

检查该数据库审计实例所在的安全组是否放开了内网入方向的9266端口。由于Agent程序与数据库 审计系统是通过9266端口进行通讯的,请确保在相关的安全组中放行该端口。

# 6 查看系统审计到的语句

将数据库接入数据库审计系统后,您就可以在系统中查看该数据库的详细审计信息。

背景信息

参照以下步骤查看审计信息:

#### 操作步骤

- 1. 登录数据库审计系统。
- 2. 在概况页面的数据库列表区域,选择已添加的数据库,单击信息,进入该数据库详细信息页面。

<mark>》</mark> sqlse <sup>当前</sup>	rver
活跃会话	0个
语句压力	0 条/s
今天	
风险总量	0条
语句总量	64,683 条
全部	
风险总量	27 条
语句总量	764,252 条
€ 信息	IP地址(1) ち 🕼 🗊

定位到语句 > 语句检索页面,选择查询时间范围,单击检索,查看符合所设置的检索条件的语句。

语句列表将以网格式报表的形式进行SQL语句检索分析结果。SQL语句分析项包括SQL语句、捕获时间、数据库用户、客户端IP、执行结果、影响行数等信息。



- ·通过单击列表右上角的列设置按钮,可以选择列表项展示内容。
- · 单击导出报表按钮,选择csv导出,可将当前语句列表导出到本地。

- 4. 定位到某条语句,进一步查看该语句的详细信息。
  - · 单击列表下方的展开语句信息,可概要地查看该SQL语句的相关信息,包括会话信息、客户 端信息、服务器信息、SQL信息等。
  - · 单击语句详情按钮,在语句详情页面查看该SQL语句的相关信息,包括访问来源、应用身份、SQL语句、受影响对象等。

语句详情							
访问来源信息							
客户))(P;	172.17.71.235	纳口:	42742		客户))IP名称:		
数据库用户:	SA	OS用户:	无信息		MAC地址:	EEFFFFFFFFF	
访问工具:	MICROSOFT JDBC DRIVER FOR SQL SERVER	主机名称:	无信息				
应用身份信息							
应用客户端IP:	N/A						
SQL语句信息							
SQL标识:	1	操作类型	: 数3	医提纵(DML)	)		
影响行数:	1	峭应时间	: 153	3µs			
命中规则:	N/A	语句捕获	时间: 201	18-01-10 11	55:15		
执行结果:	成功						*
受影响对象							
服勞器IP:	172.17.71.212	)9日:	1433		服务名 (实	ReportServer	
at Brancheda .				195. (#600/Alt 4	) : A) (		
医影响灯痕:	N/A			- minericent a			÷
SQL语句							
SELECT 1;							
4							•

・ 単击会话详情按钮,在会话详情列表中查看SQL语句所在通讯会话的会话信息以及此段会话 中审计到的所有SQL语句概况。

服务器IP/端口: 172.17.71.212:1433 客户端IP/端口: 172.17.71.235:42742 应用或工具: MICROSOFT JDBC DRIVER FOR SQL SERVER	数据库用户名: SA 客户端IP名称: 会话标识: 2532813110471000000	服务名 (实例) : mssqlserver 擾作系统用户: 无信息		
时间: 2018-01-10 11:55:11 到 Q查询 本导出 K 《 1 》 K Go 当前页1条/共 1条				
SELECT 1;				
◎ 2018-01-10 11:55:15 🛛 🗙 成功	j≡ 1 🛛 🕹 153µs	6	•	

### 📕 说明:

会话详情列表支持模糊查询审计到的SQL语句,并支持将会话详情列表导出到本地。

# 7 查看SQL语句存储空间用量

不同版本数据库审计服务提供的SQL语句存储空间不同,如果您发现您的SQL语句存储空间可用量 不足,您需要升级数据库审计实例版本。

#### 判断SQL语句存储空间是否够用

登录云数据库审计控制台,在首页即可看到已审计的语句量。

云盾•数据库审计	<b>企</b> 概况 III 报表	Q2 配置 ▶ 维护				
#H956 00 <sub>天</sub> 05 <sub>7</sub> 44	ROOM 1,158 ANON 9	৩৪জন 1,158 ৩৪৯৫ <mark>9</mark>				
<b>门</b> 说明	]:					
如果要查看	<b>f</b> 精确的磁	<b>盘容量,您可以</b>	使用系统管理员账	号,登录云数挑	居库审计系统	统进行查看。
压力 资源与引擎 数据中心监控	异常日志 系统日志					
<ul> <li>         · 回加30分钟         · 回加10月         ·····························</li></ul>	最近12小时 今天 許天 本周 上周	本月 上月 自定义			RM	
形统		— 内存	— CPU 逸量		— #0 — 202	
50% 0% 13.56 13.58 14.89	14.92' 14.94' 14.96' 14.96'	, <sup>6</sup> 53, <sup>3</sup> 63, <sup>3</sup> 63, <sup>3</sup> 63, <sup>5</sup> 73, <sup>6</sup> 73,	00 10 10 10 10 10 10 10 10 10	11.01 \$1.01 \$1.00 \$0.01 \$0.01 \$0.01 \$0.00		
		已使用		可用数	总数 最后更新时间	
系统分区 0	48%			20.15G	39.25G 2017-04-12 14:21:54	
数据中心分区 0 00				254.63G	254.82G 2017-04-12 14:21:54	
日志数据分区 🛛 💴				96.00G	96.00G 2017-04-12 14:21:54	
数据采集分区 ♀ 25				31.85G	32.00G 2017-04-12 14:21:54	
数据备份分区 9 22				109.20G	109.21G 2017-04-12 14:21:54	

下表显示了不同版本产品可用的存储量,您可以参照比对当前存储空间是否够用:

版本	可存储的SQL条数
专业版	301/2
高级版	301Z
企业版	3501Z

当您发现数据中心分区或数据备份分区的已使用量接近80%,则说明日志存储空间已满,需要升级 数据库审计实例版本扩容存储空间。

# 8 开启系统管理员和系统审计员角色

开启系统管理员和系统审计员角色后,您可以使用设置的角色信息进行登录。

背景信息

参照以下步骤设置系统管理员和系统审计员:

#### 操作步骤

- 1. 登录数据库审计控制台。
- 2. 选择配置 > 授权管理。
- 3. 在授权管理页面,单击开启密码登录。

元后-贵丽片市计		0.63	<b>M</b> 193	<b>0</b> \$8:22	F 10.11						
<u>190000</u> ===	128										
101-18	A656	15***#30		Mit102 64		66.098	88			sin	
sysadmin	NOTES:	2009-12-1	1 21.96.93				8	a.			
sysauthy	Silieur d	2009-12-3	11 21 16 13				90	æ	8		
								1	120560	TURNER	

4. 在开启登录对话框中分别设置系统管理员和系统审计员的初始密码。

开启登录	
WAR NAMES DAVIS	
2275H	2 (8-15 , PRMIA/REPROPID)
<b>街</b> 人堂码	¢
清淀量 新闻电计员 的名词变符	
22259	(8-16,100(加力的(940))
00.00G	¢
	200 200



首次登录会强制要求修改掉初时密码。

5. 单击保存,对应的开启密码登录按钮会变成关闭密码登录。

预期结果

启用密码登录后,您可以在浏览器地址栏输入https://审计系统的外网IP地址,进入登录页 面,并使用设置的系统管理员和系统审计员登录。

# 9 常见问题

### 9.1 安装Agent提示错误

在Windows上安装rmagent的时候,可能会报出下面的错误:

・安装VC运行库时报错

说明您的服务器上已经安装了更新版本的运行库,此时您只需单击关闭,关闭这个窗口,安装程 序会自动跳过这个步骤,继续下面的安装。

・安装WinPcap时报错

说明您已经安装了WinPcap,单击取消跳过WinPcap安装。

### 9.2 跨地域、VPC、账号部署场景常见问题

数据库审计系统支持跨地域、跨VPC、跨账号服务器的数据库审计。只需要RDS或ECS实例与数据 库审计系统之间网络互通,即可将不同地域、不同VPC网络、不同账号中的服务器接入数据库审计 系统进行审计。

例如,您在一个阿里云账号下有10多台服务器,分别在华北1、2、3三个不同地域。只要这些服务 器与数据库审计系统网络互通,您就可以使用一个数据库审计实例对这些服务器中的数据库进行审 计。

例如,您在一个阿里云账号下有13台ECS,其中9台使用经典网络,4台使用VPC专有网络。只要经 典网络和VPC中的服务器与数据库审计系统网络互通,您就可以使用一个数据库审计实例对这些服 务器中的数据库进行审计。

| ■ 说明:

如果服务器与数据库审计系统之间网络无法连通,则您可能需要多台数据库审计实例接入不同的服 务器进行数据库审计。

### 9.3 无法打开云数据库审计控制台

数据库审计系统控制台需要使用https进行访问,所以需要审计ECS所在的安全组打开443端口来进 行访问。

### 9.4 Windows安装Agent选项

Windows上安装Agent时,需要根据应用与数据库的环境选择不同的安装选项进行安装。 应用与数据库不在同一服务器的情况下,请按照下图,勾选WinPcap选项,选择安 装WinPcap,不安装npcap。

应用与数据库在统一服务器通过本机回环(loopback)进行访问的情况下,选择安装npcap,而 不安装WinPcap。请按照下图指示进行安装。

之后在安装npcap的时候,请按照下图选择Install Npcap in WinPcap API-compatible Mode。

安装完成后,修改C:\Users\<###>\AppData\Roaming\rmagent\rmagent.ini,将其中# loopback=1一行中的#删除以解除注释,保存文件。最后重启Windows。