

ALIBABA CLOUD

阿里云

数据库审计 用户指南（A100）

文档版本：20220216

 阿里云

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。

1. 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。
2. 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
 危险	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。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会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，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	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。	单击设置>网络>设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

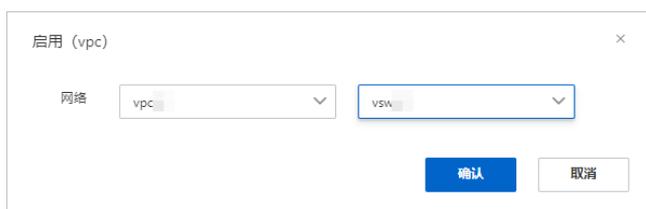
- 1. 启用数据库审计实例 ----- 05
- 2. 管理数据库审计实例的标签 ----- 06
- 3. 管理数据库审计实例 ----- 10
- 4. 登录数据库审计系统 ----- 13
- 5. 添加数据库实例 ----- 14
- 6. 部署Agent程序 ----- 18
- 7. 查看系统审计到的语句 ----- 27
- 8. 查看SQL语句存储空间用量 ----- 29
- 9. 开启系统管理员和系统审计员角色 ----- 30
- 10. 配置数据库审计告警邮件 ----- 31
- 11. 常见问题 ----- 35
 - 11.1. 安装Agent提示错误 ----- 35
 - 11.2. 跨地域、VPC、账号部署场景常见问题 ----- 35
 - 11.3. 无法打开云数据库审计控制台 ----- 36
 - 11.4. Windows安装Agent选项 ----- 36

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. 在顶部菜单栏，选择数据库审计实例所在地域。
3. 在左侧导航栏，单击**A100实例**
4. 在**A100实例**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**。
5. 在**启用 (VPC)**对话框中，在对应的下拉列表中为该数据库审计实例选择VPC和交换机，并单击**确认**。



该操作完成后，数据库审计实例将自动开始初始化，实例的状态将更新为**创建中**。初始化过程一般需要40分钟左右。

6. 耐心等待系统初始化完成后，刷新页面。

执行结果

成功启用实例后，实例的状态将更新为**运行中**。您可以在**A100实例**页面，从状态下拉列表中选择**运行中**确认该实例的状态是否为**运行中**。



后续步骤

启用数据库审计实例后，您可以登录数据库审计系统。具体操作，请参见[登录数据库审计系统](#)。

2. 管理数据库审计实例的标签

数据库审计提供标签管理功能，方便您标记数据库审计实例资源，实现分类批量管理。本文介绍为实例添加标签、选择已有标签、删除标签等操作。

使用限制

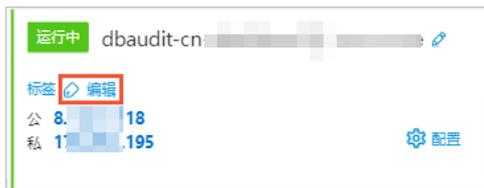
每个标签都由一对键值对（标签键和标签值）组成，数据库审计实例标签存在以下使用限制：

- 一个实例最多可以绑定20个标签。
- 一个实例的每个标签的标签键必须唯一，相同标签键的标签值会被覆盖。
- 不支持未绑定实例的空标签存在，即标签必须绑定在某个数据库审计实例上。

为实例添加新标签

参考以下操作步骤，为数据库审计实例添加标签：

1. 登录[云盾数据库审计管理控制台](#)。
2. 在左侧导航栏，单击**A100实例**。
3. 定位到需要添加标签的数据库审计实例，鼠标移动到实例的**标签**处，单击**编辑**。



4. 在**标签设置**面板的**新建标签**区域，输入键和值并单击**确定**。



说明 您可以为当前数据库审计实例添加多个标签。

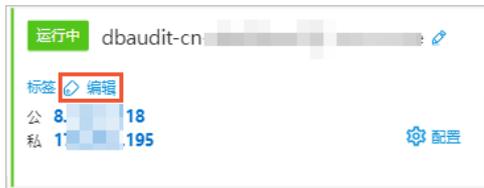
5. 在**标签设置**面板下方，单击**确认**。
标签设置完成后，您可以将鼠标放在当前实例的标签处，查看当前实例绑定的标签。



为实例选择已有的标签

参考以下操作步骤，为数据库审计实例选择已有的标签：

1. 登录[云盾数据库审计管理控制台](#)。
2. 在左侧导航栏，单击A100实例。
3. 定位到需要添加标签的数据库审计实例，鼠标移动到实例的标签处，单击编辑。



4. 在标签设置面板的添加标签区域，选择已有的标签键和值。



 **说明** 您可以为当前实例选择多个已有标签。

5. 单击确认。

通过标签搜索实例

参考以下操作步骤，搜索拥有指定标签的数据库审计实例：

1. 登录[云盾数据库审计管理控制台](#)。
2. 在左侧导航栏，单击A100实例。
3. 在A100实例页面，从全部标签的下拉列表中选择标签键和标签值。



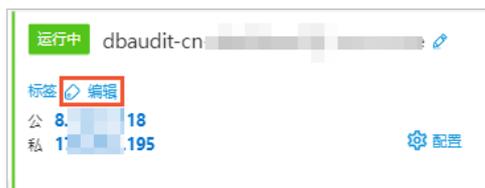
4. 在实例列表中，查看绑定该标签的所有实例。

删除实例的标签

说明 数据库审计不支持批量删除多个实例的标签，您只能单独删除某一个实例的标签。

参考以下操作步骤，删除指定数据库审计实例的标签：

1. 登录[云盾数据库审计管理控制台](#)。
2. 在左侧导航栏，单击**A100实例**。
3. 定位到需要删除标签的数据库审计实例，鼠标移动到实例的**标签**处，单击**编辑**。



4. 在**标签设置**面板的**标签**区域，定位到需要删除的标签，单击 **×** 图标。

标签设置

标签

信息安全部: 数据脱... ✕

添加标签

MySQL数据库 >	01
信息安全部 >	

新建标签

确认 取消

5. 在**标签设置**面板下方，单击**确认**。

? **说明** 当标签从实例上移除后，如果其他实例也没有使用该标签，系统将自动删除该标签。

3. 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。

操作步骤

1. 登录[云盾数据库审计管理控制台](#)。
2. 在顶部菜单栏，选择数据库审计实例所在地域。
3. 在左侧导航栏，单击A100实例。
4. 在A100实例页面，查看已开通的数据库审计实例的网络、版本、规格、到期时间等信息。



5. 管理数据库审计实例。

在A100实例页面。您可以根据需要进行以下操作：

- 配置网络：在数据库实例名称下方，单击**配置**。您可以在**配置 (VPC)** 面板，修改该数据库审计实例的网络、安全组、内网和公网访问控制策略。

公网访问控制策略支持以下选项：

- **公开模式**：该模式下，您通过内网和公网都可以访问数据库审计实例。
- **白名单访问模式**：该模式下，您可以通过配置白名单限制对数据库审计实例的访问，仅支持白名单内的IP地址访问数据库审计实例。
- **内网访问模式**：该模式下，您只能通过内网访问数据库审计实例。

说明

- 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。
- 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。



- 规格升级：您需要升级数据库审计实例的规格时，可以参考以下步骤操作：
 - a. 在规格区域，单击升配。
 - b. 在规格升级购买对话框中，单击确定。
 - c. 在变配页面，选择您需要升级的版本并选中数据库审计服务协议，单击立即购买。
 - d. 支付完成后，返回A100实例页面。
 - e. 定位到需要升级的数据库审计实例，在该实例右侧单击启用升级。
 - f. 在规格升级对话框中，单击确认。

 **注意** 升级过程中数据库审计将停止服务，整个过程预计需要15分钟，建议在对您影响最小的时间段内执行该操作。

- 续费：在到期时间区域，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。

 注意

- 数据库审计实例到期后将无法续费，请您及时关注数据库审计实例的到期时间，并在实例到期前续费。
- 您必须将数据库审计系统的版本升级到最新版本后，才可进行续费。

4. 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。

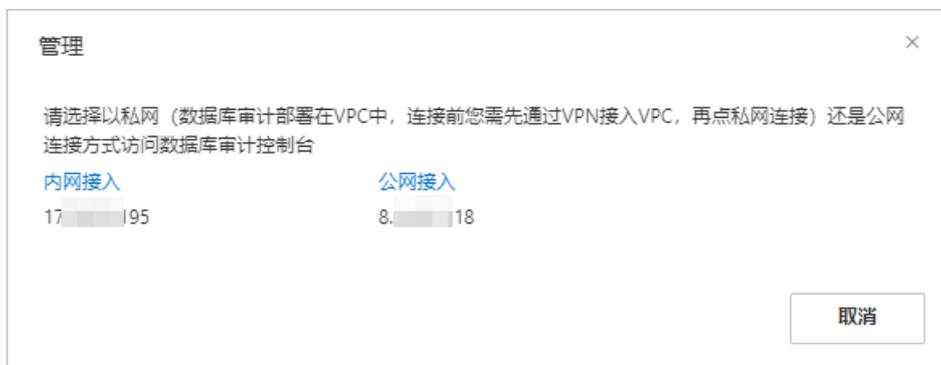
操作步骤

1. 登录[云盾数据库审计管理控制台](#)。
2. 在左侧导航栏，单击A100实例。
3. 在A100实例页面，定位到需要登录的实例，单击该实例最右侧的管理。



4. 在管理对话框中，单击内网接入或公网接入。

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。



执行结果

成功登录数据库审计系统。



后续步骤

登录数据库审计系统后，您可以添加需要审计的数据库实例。具体操作，请参见[添加数据库实例](#)。

5. 添加数据库实例

数据库审计系统支持审计ECS自建数据库和RDS云数据库实例。购买数据库审计实例后，您需要根据数据库的部署方式，将其添加至数据库审计系统中。

背景信息

关于数据库审计系统支持审计的数据库类型，请参见[支持审计的数据库](#)。

添加ECS自建数据库

参照以下步骤添加ECS自建数据库：

1. 登录数据库审计系统。
具体操作，请参见[登录数据库审计系统](#)。
2. 在概况页面，单击添加数据库。



3. 在添加数据库区域，参考以下表格填写要审计的数据库的相关信息。

数据库名	<input type="text"/>	<input type="checkbox"/> 多地址	描述	<div style="border: 1px solid #ccc; height: 30px;"></div>
数据库类型	Oracle	IP地址	<input type="text"/>	
数据库版本	10.1.0.5	端口	<input type="text"/> <input type="checkbox"/> 动态	
选择字符集	ZHS16GBK	实例名	<input type="text"/>	
操作系统	Linux 64			<input type="button" value="保存"/> <input type="button" value="取消"/>

参数	说明
数据库名	为要审计的数据库指定一个名字。
数据库类型	选择要审计的数据库的类型。 数据库审计服务支持审计的数据库类型，请参见 支持审计的数据库 。
数据库版本	从下拉列表中选择要审计的数据库的版本。

参数	说明
选择字符集	从下拉列表中选择要审计的数据库的字符集。
操作系统	从下拉列表中选择要审计的数据库所在服务器的操作系统。
多地址	需要审计的数据库有多个地址时，您需要选中 多地址 。
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。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> ? 说明 如果您的Oracle数据库是10.1.0.5版本或该版本之前的版本，并且数据库开启了动态端口功能，您需要选中端口右侧的动态。 </div>
实例名	要审计的数据库实例的名称。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> ? 说明 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。 </div>
描述	要审计的数据库的注释。

4. 单击保存。

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。
具体操作，请参见[登录数据库审计系统](#)。
2. 在概况页面，单击添加数据库。



3. 在添加数据库区域，参考以下表格填写要审计的数据库的相关信息。

添加数据库

数据库名

数据库类型 MySQL

数据库版本 4.0

选择字符集 Latin

操作系统 Linux 64

多地址

IP地址

端口

实例名

描述

保存 取消

参数	说明
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，数据库审计服务支持审计的数据库类型，请参见 支持审计的数据库 。
数据库版本	从下拉列表中选择要审计的数据库的版本。
选择字符集	从下拉列表中选择要审计的数据库的字符集。
操作系统	从下拉列表中选择要审计的数据库所在服务器的操作系统。
多地址	需要审计的数据库有多个地址时，您需要选中 多地址 。
IP地址	要审计的RDS数据库实例的连接地址。 例如：rm-bpxxxxxxxxxxxxxxxx.mysql.rds.aliyuncs.com
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。 <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;"> ? 说明 仅Oracle与Postgres类型的数据库需要填写，其他类型的数据库无需填写。 </div>
描述	为要审计的RDS数据库实例添加注释。

4. 单击**保存**。

执行结果

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。



后续步骤

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](#)。

6.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）。

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。



3. 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`。

说明

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自动部署

Agent配置:

本地回环 (应用程序与数据库在同一台机器上)

审计服务器IP:

目标服务器: 格式: 目标IP,root密码,ssh端口

[查看执行日志](#)

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

序号	IP地址	操作
1	172.17.71.212	<input type="button" value="删除"/>
2	192.168.0.1	<input type="button" value="删除"/>
3	192.168.0.111	<input type="button" value="删除"/>

IP地址:

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。

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

- i. 登录云盾数据库审计系统。
- ii. 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。

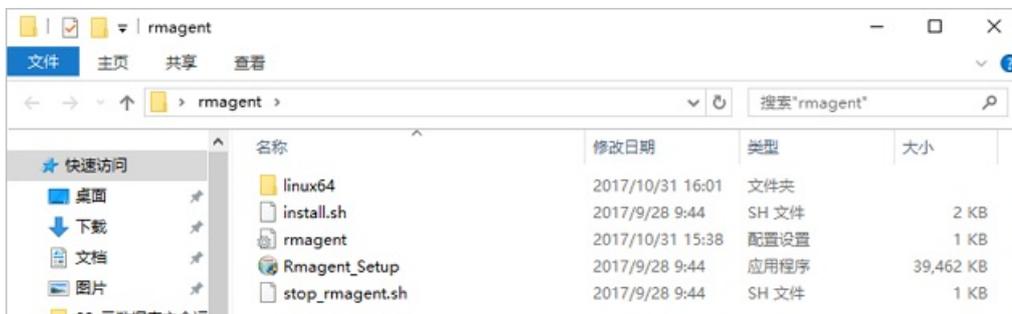


- iii. 在Agent部署配置对话框中，输入需要部署Agent程序的服务器IP地址，然后单击添加。

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。

- iv. 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。



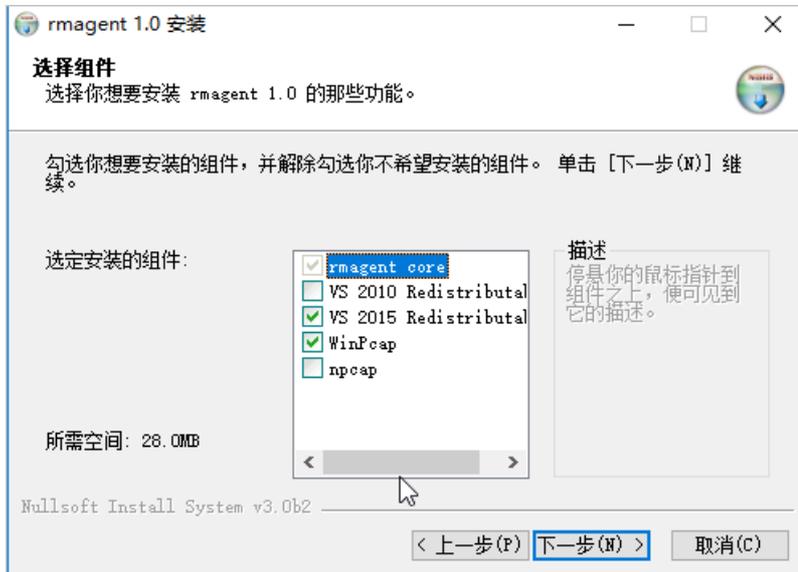
- v. 打开解压后的Agent程序文件夹，双击运行Rmagent_Setup.exe程序文件。
- vi. 在Installer Language对话框中，单击OK。



- vii. 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。



viii. 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

i. [登录云盾数据库审计系统](#)。

ii. 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。

iii. 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。

iv. 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。

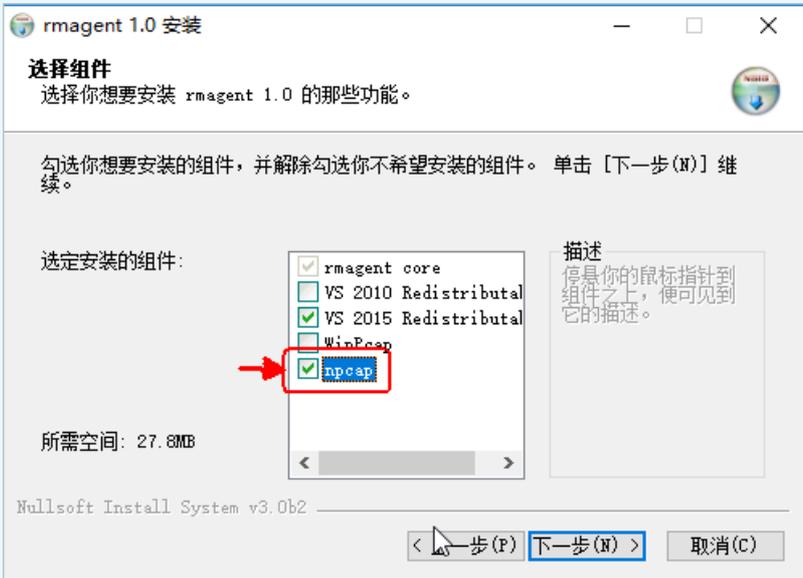
v. 打开解压后的Agent程序文件夹，双击运行 *Rmagent_Setup.exe* 程序文件。

vi. 在 **Installer Language** 对话框中，单击 **OK**。

vii. 在 **rmagent 1.0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

选择组件
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。单击 [下一步(N)] 继续。

选定安装的组件:

- rmagent core
- VS 2010 Redistributable
- VS 2015 Redistributable
- WinPcap
- npcap

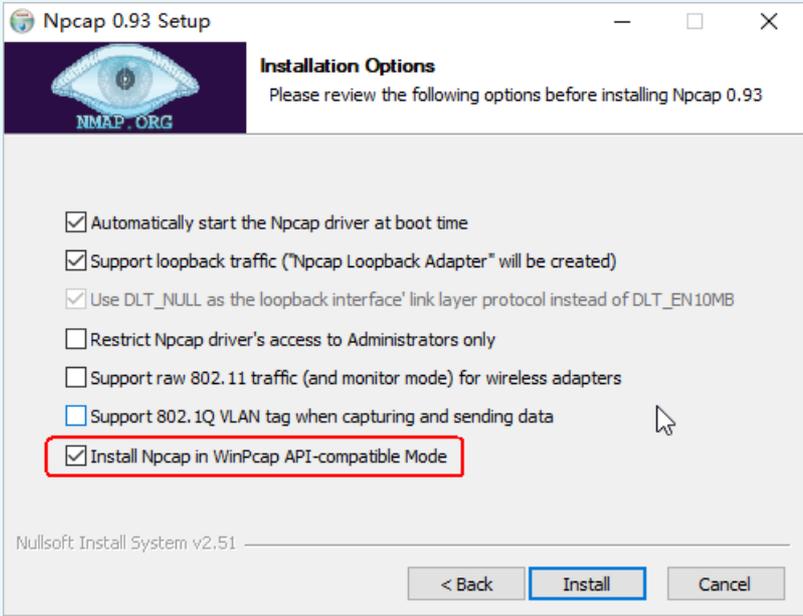
所需空间: 27.8MB

Nullsoft Install System v3.0b2

< 上一步 (P) **下一步 (N) >** 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

Installation Options
Please review the following options before installing Npcap 0.93

- Automatically start the Npcap driver at boot time
- Support loopback traffic ("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 WinPcap API-compatible Mode**

Nullsoft Install System v2.51

< Back **Install** Cancel

viii. 所有组件及Agent程序安装完成后，修改 `C:\Users\<用户名>\AppData\Roaming\rmagent\rmagent.in` 文件，将其中的 `#loopback=1` 一行中的 `#` 删除以解除注释，保存文件。

loopback=1 表示监听回环网卡。

```

rmagent - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
[rms]
server_host=192.168.232.181
#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
  
```

ix. 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

- i. 登录云盾数据库审计系统。

- ii. 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。

- iii. 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。

- iv. 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/rmagent
./rmagent.ini
./install.sh
[root@rsdsdf ~]#
  
```

chmod 755

- v. 执行 `install.sh` 命令，给 `install.sh` 文件增加权限。

vi. 安装Agent程序。

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

vii. 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

- i. 登录云盾数据库审计系统。
- ii. 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。
- iii. 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。

iv. 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。

v. 执行 `chmod 755 install.sh` 命令，给install.sh文件增加权限。

vi. 安装Agent程序。

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

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

`loopback=1` 表示监听回环网卡。

```
server_host=60.205.188.19
loopback=1
~
~
~
~
~
```

- viii. 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。

```
[root@mysql ~]# cd /usr/local//rmagent/
[root@mysql rmagent]# ./stop_rmagent.sh
find pid: 1352, exe: /usr/local/rmagent/rmagent
[root@mysql rmagent]# ./rmagent
[root@mysql rmagent]#
```

Agent部署注意事项

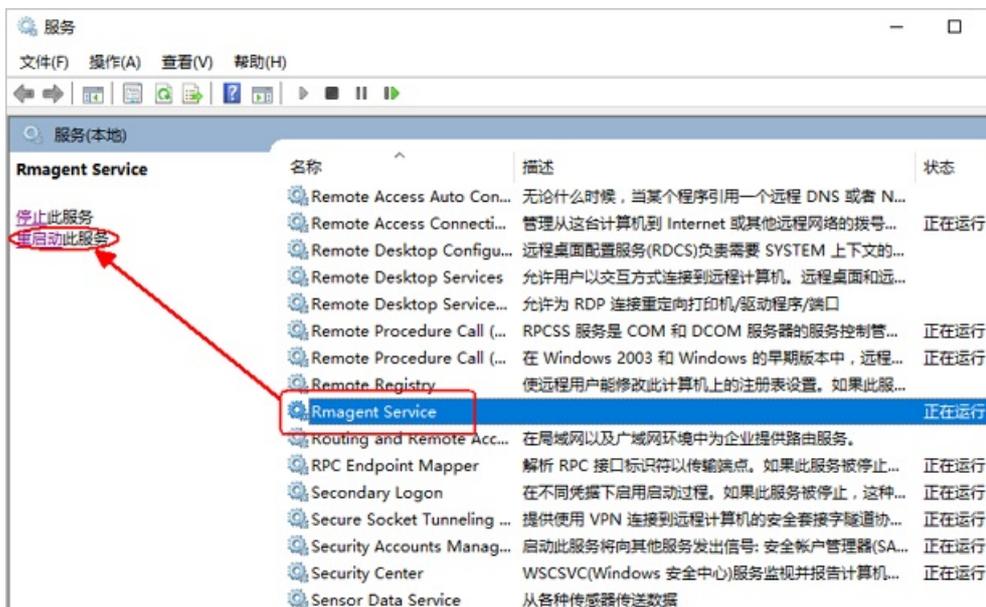
Agent程序默认连接数据库审计系统的内网IP, 如果部署Agent程序的服务器与云盾数据库审计系统之间通过外网连接则需要修改`rmagent.in`配置文件中的IP地址。

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\用户名\AppData\Roaming\rmagent\rmagent.in` 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。



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, 单击重新启动此服务。



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。

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

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
~
~
~
~
~
~
-- INSERT --
```

4. 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。

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[INFO][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。

7. 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。

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。



3. 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。

说明

- 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

客户端IP: 172.17.71.235 端口: 42742 客户端IP名称: 无信息
数据库用户: SA OS用户: 无信息 MAC地址: EEEEEEEEEEE
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: 数据操纵(DML)
影响行数: 1 响应时间: 153µs
命中规则: N/A 语句捕获时间: 2018-01-10 11:55:15
执行结果: 成功

受影响对象

服务器IP: 172.17.71.212 端口: 1433 服务名 (实例): ReportServer
受影响对象: N/A 截图(Alt + A)

SQL语句

SELECT 1;

- 单击会话详情按钮，进入会话详情列表。在列表中，您可以查看SQL语句的会话信息和会话中审计到的所有SQL语句的概况。

服务器IP/端口: 172.17.71.212:1433 数据库用户名: SA 服务名 (实例): mssqlserver
客户端IP/端口: 172.17.71.235:42742 客户端IP名称: --- 操作系统用户: 无信息
应用或工具: MICROSOFT JDBC DRIVER FOR SQL SERVER 会话标识: 2532813110471000000
时间: 2018-01-10 11:55:11 到 查询 导出

1 << 1 >> 1 Go 当前页1条/共1条

SELECT 1;

2018-01-10 11:55:15 成功 1 153µs

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。

8. 查看SQL语句存储空间用量

不同版本的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。

您可以通过查看审计的语句总量或磁盘容量判断SQL语句存储空间是否够用。

- 安全管理员查看已审计的语句量

登录云盾数据库审计系统，在首页的概况中直接查看已审计的语句量。



- (可选) 系统管理员查看精确的磁盘容量

说明 默认情况下，数据库审计系统不启用系统管理员，如何开启系统管理员请参见[开启系统管理员和系统审计员角色](#)。

如果要查看精确的磁盘容量，您可以使用系统管理员账号，登录云盾数据库审计系统进行查看。



您可以参考[计费方式](#)中不同版本的性能参数，参照比对当前存储空间是否够用。

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将近存满；这时，您需要升级数据库审计实例版本，对数据盘空间进行扩容。具体如何升级数据库审计实例版本，请参见[管理数据库审计实例](#)。

9. 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，您可以使用已设置的用户名和密码进行登录。

操作步骤

1. 登录数据库审计系统，具体操作，请参见[登录数据库审计控制台](#)。
2. 在顶部菜单栏，选择配置，并单击授权管理页签。
3. 在授权管理页签，单击开启密码登录。



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

请设置系统管理员的初始密码

登录密码 ☆ (8~16, 同时包含数字和字母)

确认密码 ☆

请设置系统审计员的初始密码

登录密码 ☆ (8~16, 同时包含数字和字母)

确认密码 ☆

② 说明 首次登录时，系统会强制要求修改初始密码。

5. 单击保存，可保存登录密码。

② 说明 授权管理页面中开启密码登录按钮会变成关闭密码登录。

执行结果

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，并使用已设置的系统管理员（或系统审计员）的用户名和密码进行登录。

10. 配置数据库审计报告邮件

数据库审计支持配置告警邮件。配置告警邮件后，数据库审计服务将以邮件的方式向您发送告警信息。本文介绍配置数据库审计报告邮件的具体操作。

前提条件

已开启数据库审计系统的系统管理员角色，具体操作，请参见[开启系统管理员和系统审计员角色](#)。

配置流程

您需要参照以下流程配置数据库审计报告邮件：

1. **步骤一：配置邮件服务器**：使用数据库审计的系统管理员sysadmin账号设置发送告警邮件的服务器。
2. **步骤二：配置告警邮件接收地址**：使用数据库审计的管理员账号配置用户接收告警邮件的邮箱地址。
3. 使用数据库审计的管理员账号配置告警邮件信息。

在数据库审计系统环境产生的告警为系统告警，由数据库审计的语句命中告警规则产生的告警为规则告警。

- 如果您需要接收系统告警通知邮件，请配置系统告警邮件信息。具体操作，请参见 **(可选) 步骤三：配置系统告警邮件信息**。
- 如果您需要接收规则告警通知邮件，请配置规则告警邮件信息。具体操作，请参见 **(可选) 步骤四：配置规则告警邮件信息**。

步骤一：配置邮件服务器

1. 在浏览器地址栏输入 `https://数据库审计IP`，进入登录页面，并使用系统管理员sysadmin的用户名和密码登录数据库审计控制台。
2. 在顶部菜单栏，选择**系统 > 通知管理**。
3. 在**告警通知管理 > Email设置**页面的Email设置区域，设置发送告警邮件服务器的相关参数。

Email设置

SMTP服务器地址:	<input type="text"/>	用户名:	<input type="text"/>
端口:	<input type="text"/> (1 - 65535)	密码:	<input type="text"/>
加密连接类型:	<input type="text" value="无"/>	发件人地址:	<input type="text"/>

发信测试

收件人地址:	<input type="text"/>	<input type="button" value="发送测试邮件"/>
--------	----------------------	---------------------------------------

参数	说明
SMTP服务器地址	发送告警邮件的SMTP服务器的IP地址。
用户名	数据库审计实例访问发送告警邮件的服务器的用户名。

参数	说明
端口	数据库审计实例对接发送告警邮件的服务器的端口。 端口范围1~65535。
密码	数据库审计实例访问发送告警邮件服务器的密码。 如果邮件服务器要求第三方客户端登录时使用授权码，此处需要填写客户端授权码。
加密连接类型	数据库审计实例连接发送告警邮件服务器时使用的加密类型。取值： <ul style="list-style-type: none">无SSLTLS
发件人地址	邮件中显示的发送告警邮件的邮箱地址。

4. 在发信测试区域的收件人地址中，填写接收告警邮件的邮箱地址。

如需校验接收告警邮件的邮箱有效性，可单击发送测试邮件。如果测试邮箱接收到测试邮件，表示收件人地址信息填写正确。

5. 单击保存。

步骤二：配置告警邮件接收地址

请参见以下步骤为需要接收告警邮件的用户配置邮箱地址。

1. 登录数据库审计系统。
2. 单击页面右上角的用户名，并在下拉列表中单击用户资料。
3. 在用户资料对话框中，输入用户对应的邮件地址，单击保存。

4. 在提示对话框中，单击确定。

(可选) 步骤三：配置系统告警邮件信息

如果您需要接收系统告警通知邮件时，请参考以下步骤配置系统告警邮件信息：

1. 登录数据库审计系统。
具体操作，请参见[登录数据库审计系统](#)。
2. 在顶部菜单栏，选择配置 > 系统告警设置。

- 在邮件通知页签的用户列表中，选中需要接收告警邮件的用户所在行的通知列。
您可以选择为多个用户开启告警邮件接收通知，未选中的用户将不会接收到告警邮件。



- 配置系统告警邮件的邮件标题及告警周期，选中邮件中需要显示的系统告警信息。
- 单击确定。
- 在提示对话框中，单击确定。

(可选) 步骤四：配置规则告警邮件信息

如果您需要接收规则告警通知邮件时，请参考以下步骤配置规则告警邮件信息：

- 在数据库审计系统概况页面的数据库区域，单击已添加数据库的信息。
- 在数据库详情页面，单击配置。
- 在规则告警通知的邮件通知页签，选中所有需要接收告警邮件的用户所在行的通知列。



4. 配置规则告警邮件的**邮件标题**及**告警周期**，选中告警邮件中发送的内容。
5. 单击**确定**。
6. 在提示对话框中，单击**确定**。

执行结果

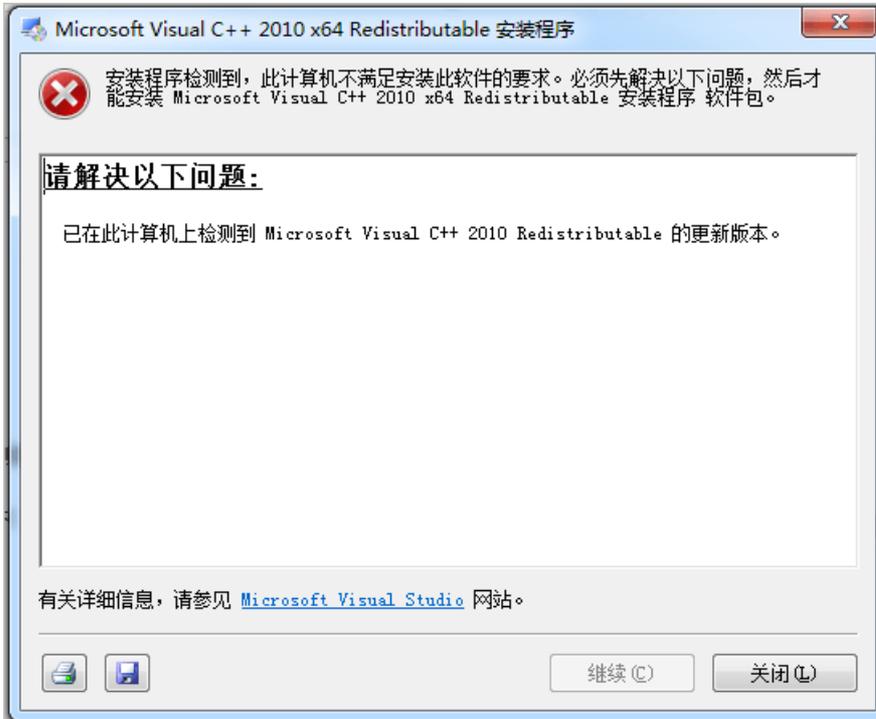
配置数据库审计系统告警邮件后，当数据库审计系统环境发生告警时，您设置的邮箱接收地址会收到系统告警邮件通知。配置数据库审计规则告警邮件后，当审计的语句命中告警规则时，您设置的邮箱接收地址会收到规则告警邮件通知。

11. 常见问题

11.1. 安装Agent提示错误

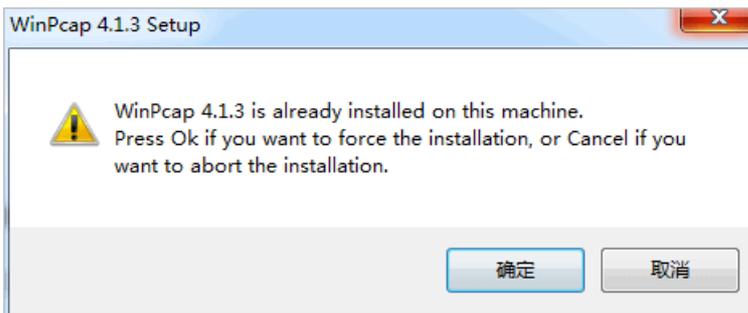
在Windows上安装ragent的时候，可能会报出下面的错误：

- 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。

11.2. 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。

11.3. 无法打开云数据库审计控制台

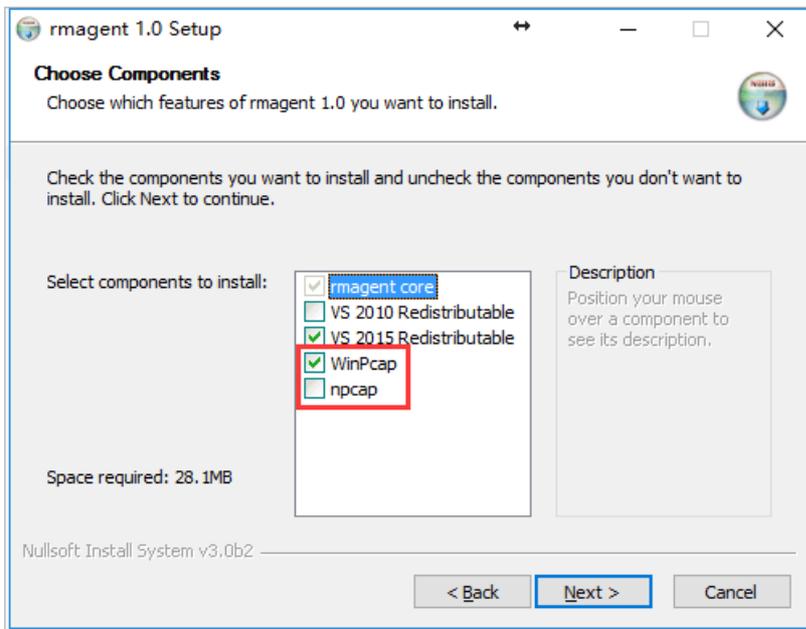
数据库审计系统控制台需要使用HTTPS进行访问，所以需要审计ECS所在的安全组打开443端口来进行访问。

11.4. Windows安装Agent选项

在Windows操作系统中安装Agent时，您需要根据应用与数据库的环境选择不同的安装选项。本文介绍在不同的情况下如何选择安装选项。

应用与数据库不在同一台服务器上

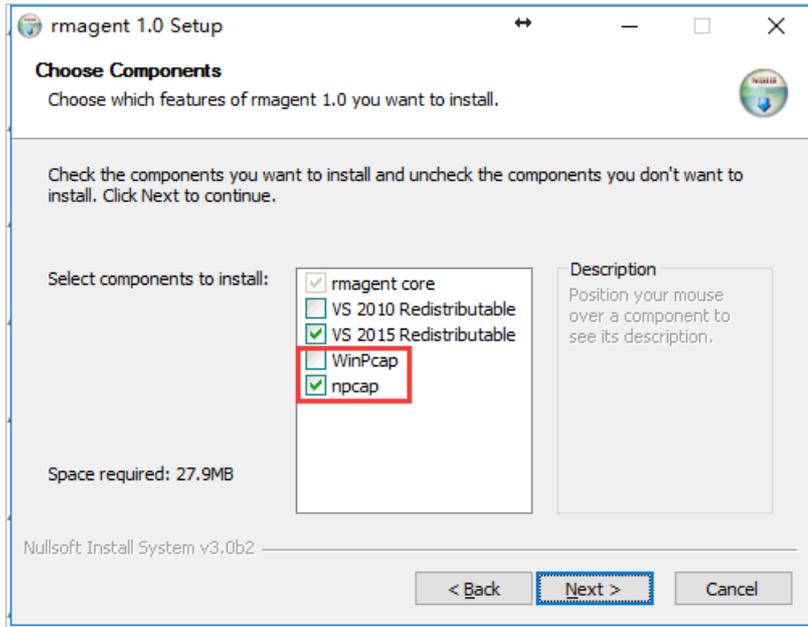
在此情况下，选中WinPcap复选框，取消选中npcap复选框。使用默认选项安装WinPcap。



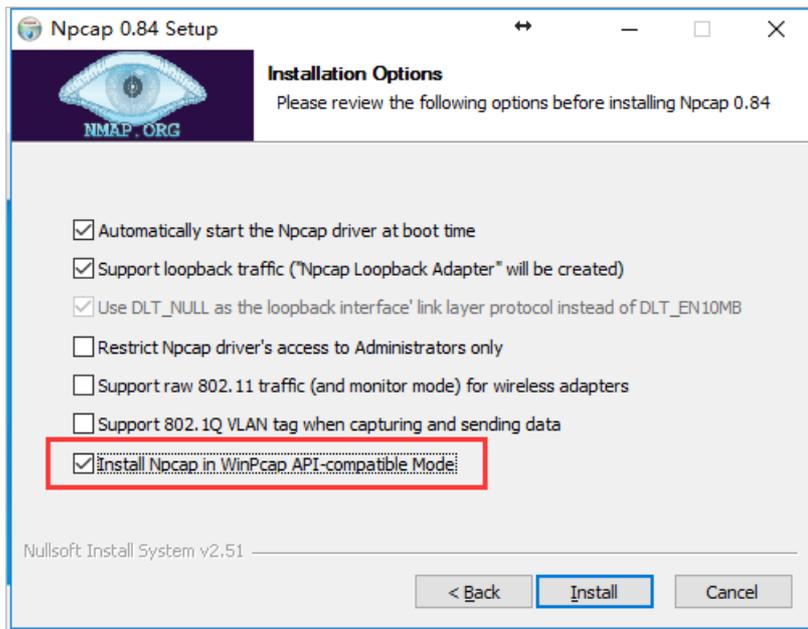
应用与数据库在同一台服务器上

应用与数据库在同一台服务器上并通过本机回环（Loopback）进行访问的情况下，选择安装npcap。请按照以下步骤设置安装选项：

1. 选中npcap复选框，取消选中WinPcap并单击Next。



2. 在安装Npcap时，选中Inst all Npcap in WinPcap API-compatible Mode复选框后单击Inst all。



3. 安装完成后，执行以下步骤修改 *rmagent.ini* 文件。

- i. 在 *C:\Users\<用户名>\AppData\Roaming\rmagent* 目录下打开 *rmagent.ini* 文件。
- ii. 去掉 *rmagent.ini* 文件中 `#loopback=1` 所在行的 `#`，并保存该文件。
- iii. 重启Windows服务器。