阿里云
安全管家

常见问题

文档版本：20200629

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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。
	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。
	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。
	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。	执行cd /d C:/window命令，进入Windows系统文件夹。
斜体	表示参数、变量。	bae log list --instanceid 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。	switch {active|stand}

目录

1 安全管家服务售前咨询

尊敬的“准”安全管家服务用户您好：

如果您准备购买阿里云安全管家服务，但是遇到如安全管家服务范围、规格、服务选择等售前方面的问题，您可以通过钉钉与我们联系，您将“当面”获得阿里云安全服务专家的建议。

说明：

- **售前咨询时间**：5*8小时（不含法定节假日）。如果您在非正常咨询时间内遇到紧急问题，仍可通过该方式与阿里云专家进行沟通。
- 售前咨询服务仅帮助您解答安全管家服务的**售前**问题。

2 购买专业版后如何绑定服务器？

在购买安全管家专业版后，您需要进入云盾安全管家控制台，绑定需要进行安全检测的服务器。本文介绍如何绑定服务器。

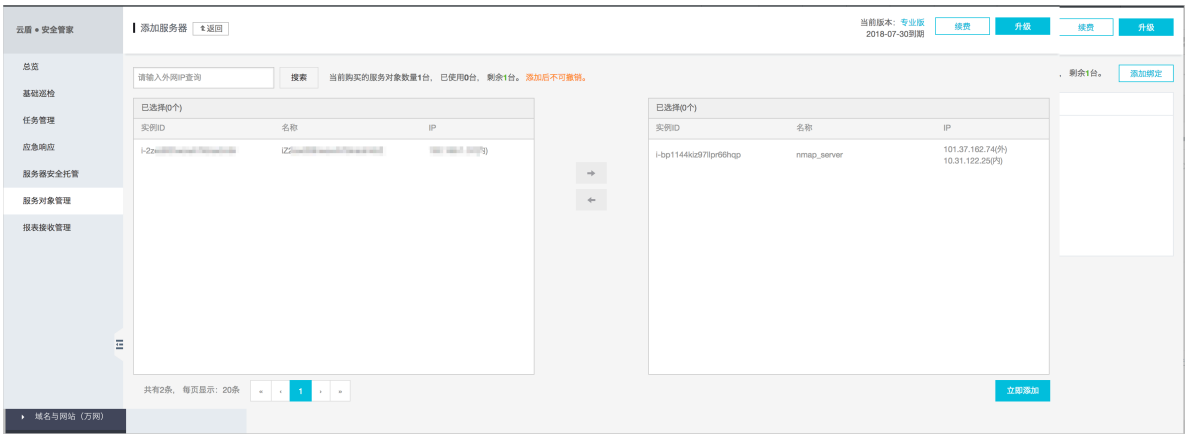
以下是绑定服务器详细的操作步骤：

1. 进入安全管家服务器绑定页面。

2. 选择需要绑定的服务器，单击**确定**。

说明：

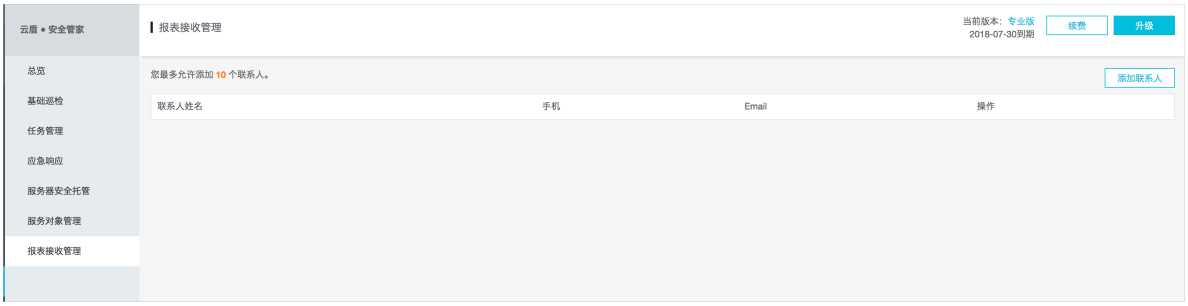
服务器绑定后将无法进行解绑，请确认选择的服务器是需要被安全管家检测的服务器。

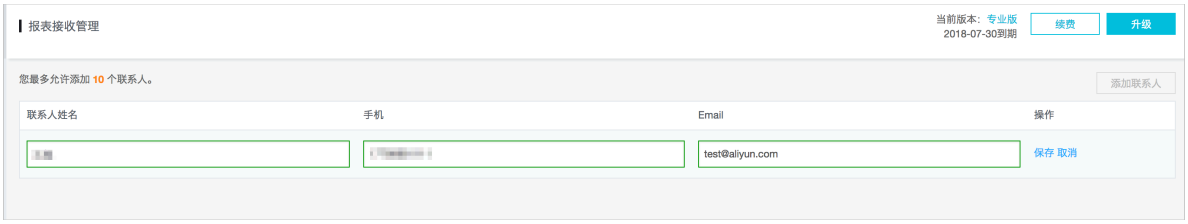


3. 确认服务器已经添加。

4. 添加邮件接收人。

> **说明:**
> 专业版的报表是通过邮件自动发送到管理员邮箱的，您需要在控制台添加接收人的邮件地址。





3 用户购买了安全管家应急服务后，如何响应？

购买应急服务后，安全管家将通过电话联系您，并为您建立应急响应处理工作的沟通联系渠道。

安全管家应急服务的具体流程如下图所示：

4 如果用户第一次使用了应急响应服务，再次发生问题后怎么办？

目前安全管家应急服务有效期限为15天。在应急响应服务期（5天）结束后，如果在有效期（15天）内再次发生安全事件，安全管家应急服务将为您继续提供服务，如果超过了服务有效期（15天）需要重新购买或选用其他的方案。

5 不理解或对应急响应报告内容存在疑问

如果您对报告有任何疑问，可以在线咨询安全管家或以远程电话的方式提供专业答疑，以便于您能够真正理解报告内容。

6 安全管家提供现场服务吗？

安全管家原则上不提供现场服务，安全管家通过远程技术支持的方式提供服务。

7 安全管家应急服务提供安全事件溯源服务吗？

安全管家应急服务不提供安全事件溯源服务。如果需要该服务，请提交阿里云工单咨询客服。

说明：

安全事件溯源服务是指，根据安全事件分析和调查的数据，溯源追查定位到入侵黑客的具体人员身份信息。

8 安全管家应急服务能提供数据恢复服务吗？

因安全问题而导致的数据损坏，安全管家应急服务根据不同的用户场景评估和提供解决方案，并协助客户进行数据修复，但由于数据恢复难度高，安全管家应急服务不承诺和保证数据恢复的效果。

关于数据备份与恢复问题，阿里云建议客户做好日常数据备份，包括本地备份和异地备份。

9 安全管家服务能排查到安全事件原因吗？

寻找安全事件事发原因是理想结果，但由于该结果取决于客户的IT基础环境保存的分析信息的完整性，例如：包括服务器登录访问日志、应用服务访问日志等方面的日志完整性方面因素，安全管家会尽力收集安全事件各方面的信息帮助客户排查分析出造成安全事件的根本原因，从根本上发现安全技术问题和安全管理问题，为制定安全解决方案提供信息输入，防止后续再次发生安全事件。

10 安全管家应急服务处理非安全问题吗？

服务不提供非安全问题分析和处理服务。安全管家应急服务专门针对以下定义的突发安全事件提供应急响应处理服务，客户的软件问题、基础网络问题、云服务器问题不在此范围内，如果您有其他问题，您可以提交工单，阿里云售后人员会为您服务。

您可以根据发生的事件判断是否属于安全事件，安全事件定义如下：

事件类别	描述
有害程序事件	计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件
网络攻击事件	后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件
信息破坏事件	信息篡改事件、信息伪造假冒的冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件
信息内容安全事件	通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件

说明：

以上安全事件定义参照《信息安全技术-信息安全事件分类分级指南》-GB/Z 20986-2007标准。