阿里云
云安全中心（态势感知）

自定义告警

文档版本：20200506

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 限制条件说明

云安全中心的自定义告警功能目前处于公测阶段，如果使用自定义告警服务需要单独申请开通该服务。提交的公测申请需要人工审批，审批周期为5至7个工作日。

2 规则设置

云安全中心支持自定义的告警规则，帮助您更全面和深入地获取您服务器中存在的威胁信息。本文档介绍了如何创建自定义告警规则并配置告警通知策略。

步骤一：创建自定义告警规则

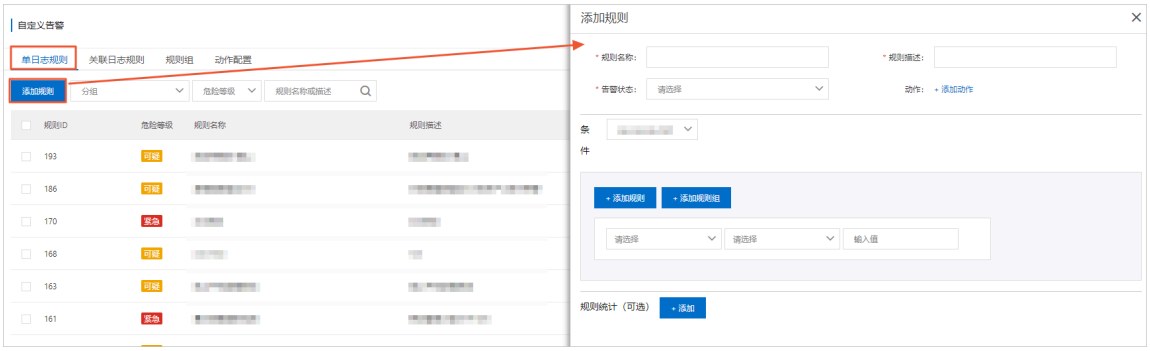
- **单日志规则**是指在创建告警规则时匹配单个日志。
- **关联日志规则**是指在创建告警规则时匹配两个日志。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**自定义告警** > **规则设置**。

3. 在**自定义告警**页面，选择**单日志规则**或**关联日志规则**页签，创建自定义告警规则。

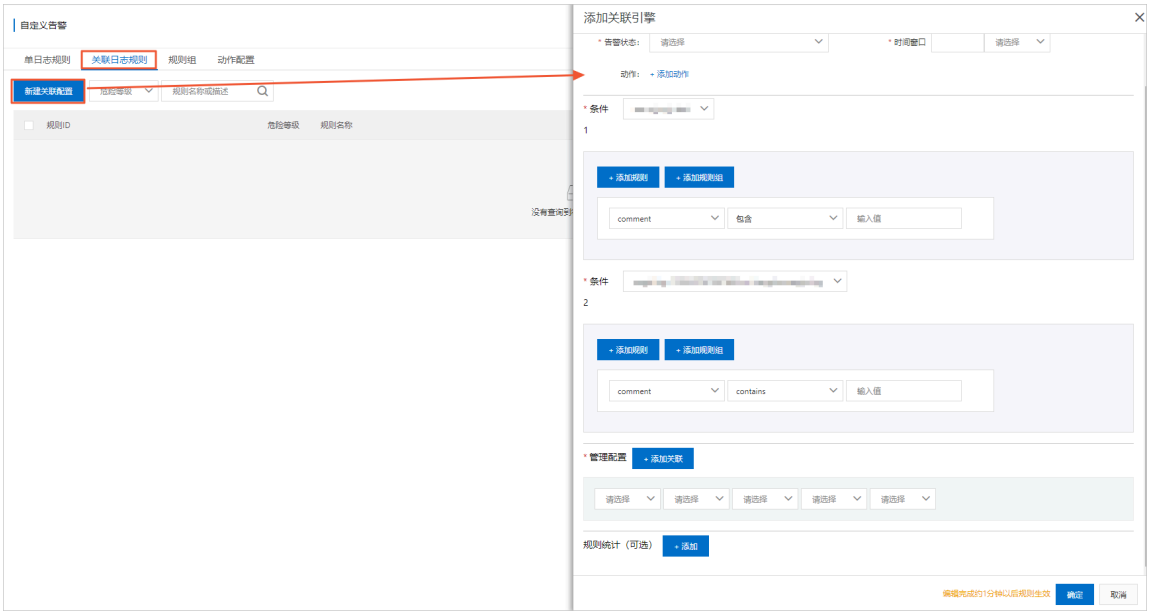
- **单日志规则**

  单击**添加规则**，配置单日志规则参数（见下表）。



- **关联日志规则**

  单击**新建关联配置**，配置关联日志告警参数（见下表）。



规则类型	参数	配置说明
单日志规则/关联日志规则	**规则名称**	自定义该规则的描述性名称，不得少于2个字符。
	告警状态	设置该告警规则的严重等级，可选项为**紧急**、**可疑**和 **提醒**。
	规则描述	自定义该规则的说明描述信息。

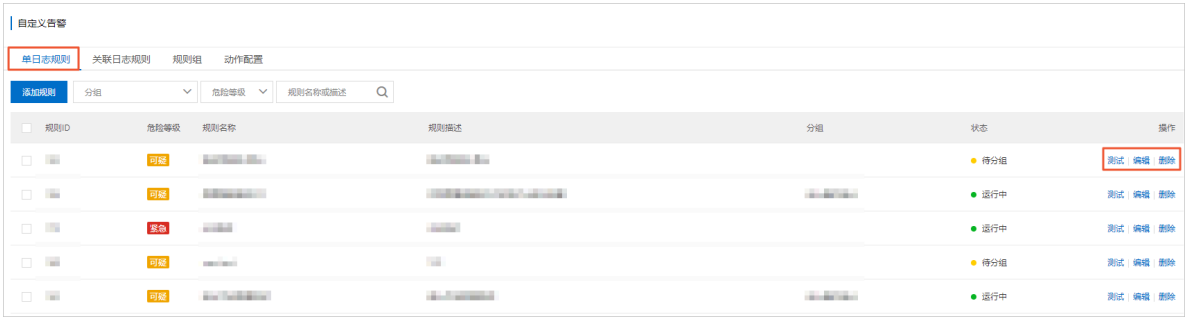
规则类型	参数	配置说明
	动作	设置该规则命中的告警事件通知方式。可选项： • **钉钉通知**：通过钉钉群机器人发送告警通知 • **事件存储**：通过**自定义告警 > 日志及事件管理**页面展示告警信息。 您可配置**钉钉通知+事件存储**的方式来展示告警事件。 钉钉通知支持选择多个钉钉群机器人。钉钉群机器人配置请参见动作配置。
	统计规则	可选配置。设置自定义时间范围内命中多少次该规则才会进行告警， 时间单位可选**天**、**小时**、**分钟**或**秒**。 例如：**时间间隔**设置为1天，**阈值**为100，表示1天内命中该规则超过100次会产生告警。
单日志规则	**条件**	选择应用该规则的日志，并配置对应的规则内容。 支持配置多个规则或规则组，一个规则组至少需要配置2个规则。 规则或规则组之间，需要设置规则关系： • **AND**：多个规则或规则组之间是**与**的关系。 • **OR**：多个规则或规则组之间是**或**的关系。
关联日志规则	**时间窗口**	设置该告警规则通知的间隔时间。 时间单位可选小时、分钟或秒。例如：设置为5小时，代表5小时内只发送一次告警通知。
	条件1/条件2	选择关联规则的日志名称，并配置对应的规则内容。
	管理配置	配置两个日志间的关联参数。

4. 单击**确定**完成规则创建。

说明：

- 单日志规则创建完成后还需将该规则添加到分组中，规则才能生效。详细内容请参见步骤二：创建规则组并添加自定义告警规则。
- 关联日志规则创建完成，无需添加分组，立即生效。

5. （可选）您可在**单日志规则**列表最右侧**操作**栏，单击**测试**对已创建的规则进行测试；单击**编辑**修改规则配置；或单击**删除**对已创建的规则进行删除。

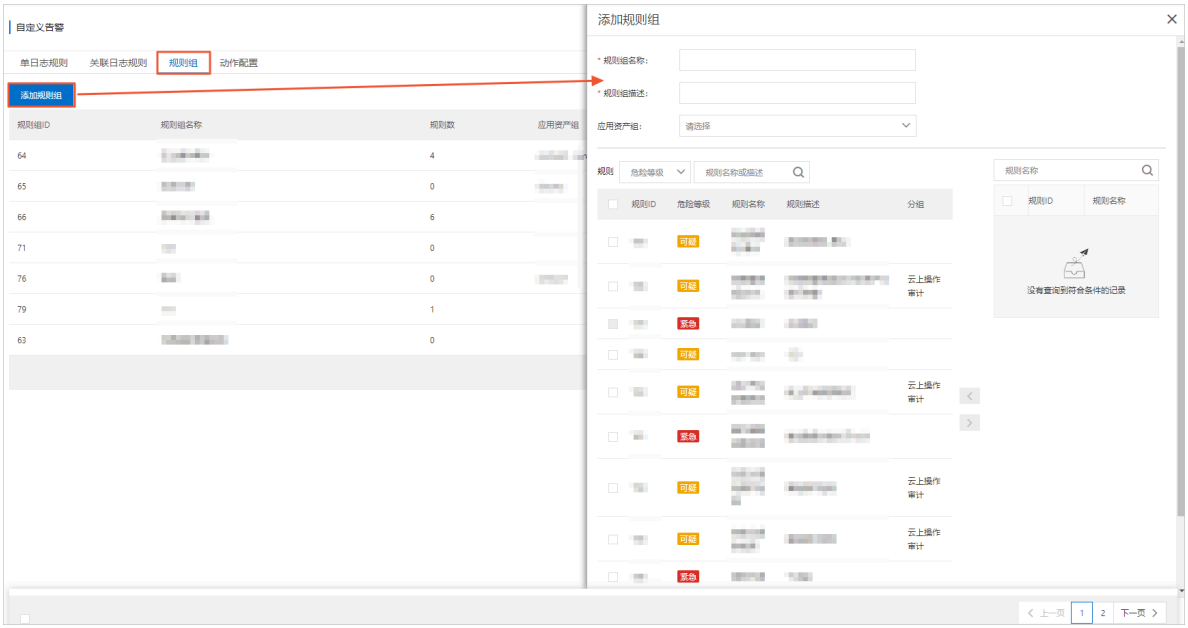


6. （可选）您可在**关联日志规则**列表最右侧**操作**栏，单击**编辑**修改规则配置；或单击**删除**对已创建的规则进行删除。

步骤二：创建规则组并添加自定义告警规则

单日志规则创建完成后，需要将该规则添加到规则分组中，该规则才能生效。

1. 在**自定义告警**页面，选择**规则组**页签，并单击**添加规则组**。



2. 在**添加规则组**页面中完成规则组的配置，并将您定义好的检测规则添加到该规则组中。

参数	配置说明
规则组名称	自定义该规则组的描述性名称，不得少于2个字段。

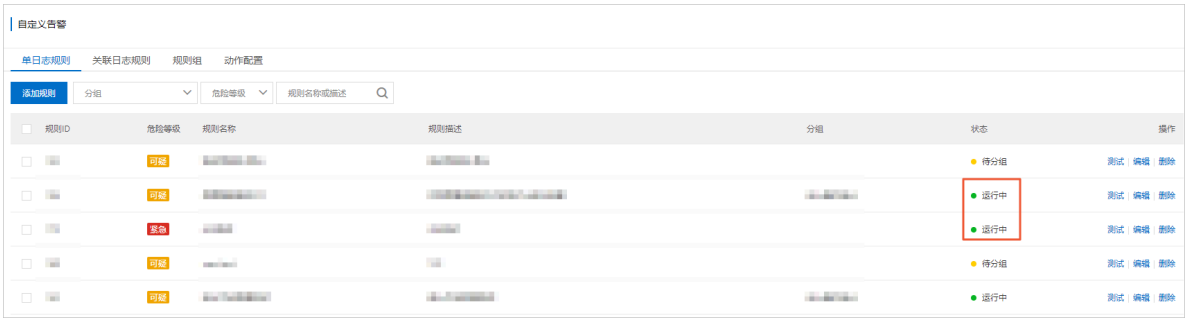
参数	配置说明
规则组描述	自定义该规则组的说明描述信息。
应用资产组	从下拉列表中勾选应用该规则组的资产组名称。 您可在云安全中心控制台**资产中心**页面使用资产分组管理功能添加或修改资产分组。详细内容请参见#unique_5。
规则	勾选要添加到该组的规则，并添加到右侧**规则名称**列表中。 

3. 单击**确定**完成规则组创建。

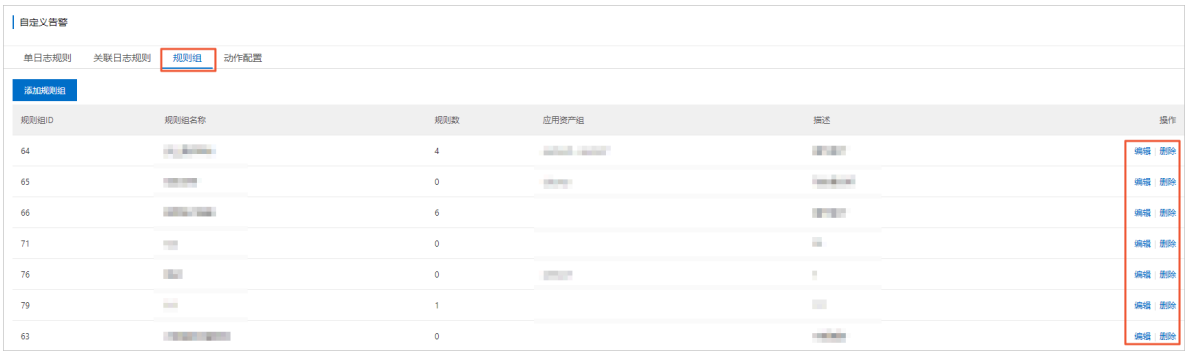
说明:

规则组中如果未添加任何规则，**规则数**将显示为0。

新创建的规则添加到规则组后，该规则的状态才会变为**运行中**。**运行中**表示该规则已生效。



4. （可选）您可在规则组列表最右侧**操作**栏，单击**编辑**修改规则组，或单击**删除**对已创建的规则组进行删除。



说明：

删除的规则组不可恢复，并且该规则组中添加的规则将失效。

步骤三：查看告警通知

自定义告警可通过以下两种方式查看。

- 钉钉群机器人通知。
- 云安全中心控制台**自定义告警** > **日志及事件管理**查看所有的告警通知。

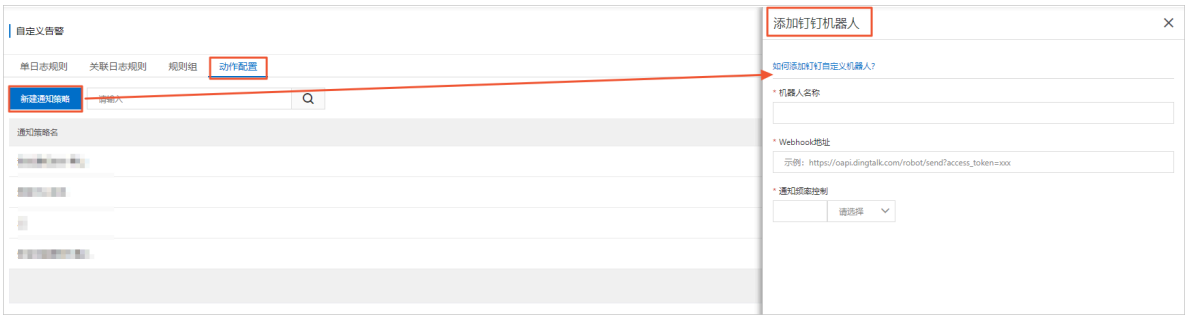
动作配置

自定义告警规则创建完成后，您还需配置告警通知策略，确定钉钉群机器人自动发送告警通知的配置信息。

说明：

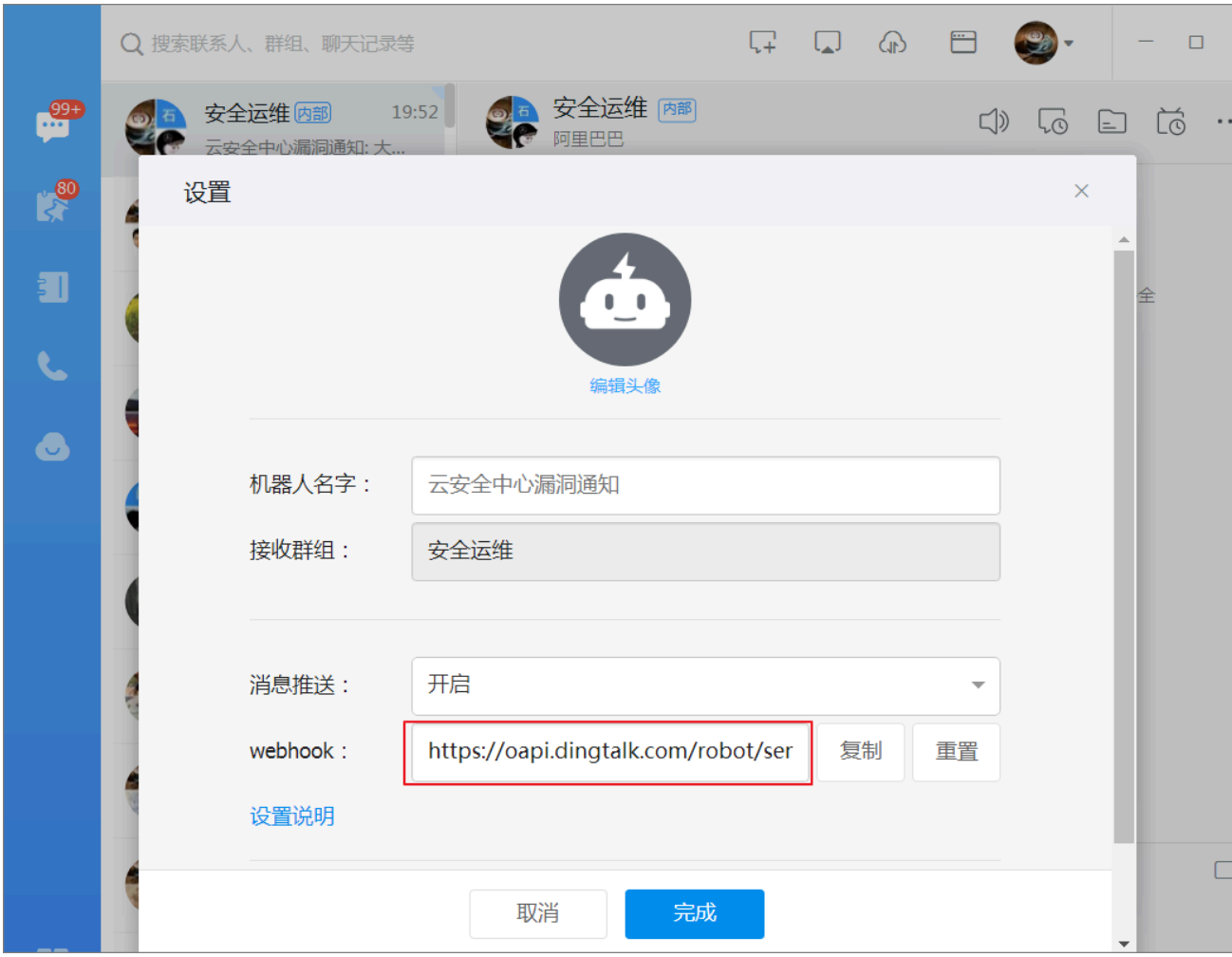
告警通知策略仅支持钉钉群机器人通知。如未安装钉钉，请到**自定义告警** > **日志及事件管理**页面手动查看自定义告警通知事件。

1. 在**自定义告警**页面，选择**动作配置**页签，并单击**新建通知策略**。



2. 在**添加钉钉机器人**页面，为您自定义的告警规则设置钉钉通知方式。

   - **机器人名称**：设置钉钉群自动通知机器人的名称。
   - **Webhook地址**：在要应用该钉钉机器人通知的钉钉群中，找到机器人的Webhook链接，复制粘贴到**Webhook地址**输入栏中。



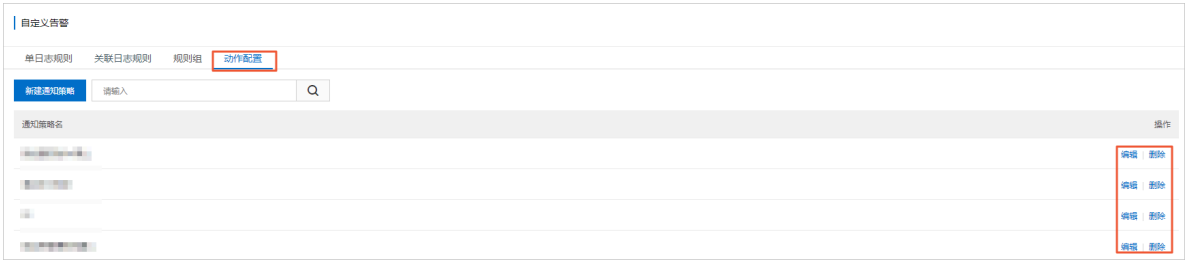
> **说明：**
> 未安装钉钉并建立钉钉群的用户，无法使用钉钉机器人通知。如果已有钉钉群中未添加钉钉机器人，需要在钉钉群**群设置 > 群机器人 > 添加群机器人 > 自定义（通过Webhook接入自定义服务）**，添加自定义机器人。

   - **通知频率控制**：设置钉钉机器人通知触发的频率 。频率范围为10分钟-1天。 例如：通知频率设置为10分钟，表示每间隔10分钟通知一次。

3. 单击**创建**，完成钉钉群机器人通知策略的创建。

   完成通知策略创建后，您可在**单日志规则**和**关联日志规则**中添加已创建好的钉钉机器人策略。

4. 您可在通知策略列表最右侧**操作**栏，单击**编辑**修改策略配置，或单击**删除**对已创建的通知策略进行删除。



3 日志查询

云安全中心支持查询自定义告警规则相关的进程告警日志。您可通过日志分析功能搜索和查看更多类型的日志。

操作步骤

1. 登录云安全中心控制台。
2. 单击左侧导航栏**自定义告警**打开自定义告警页面。
3. 单击**日志查询**跳转到**日志**页面。
4. 单击**增加一组**打开搜索条件配置框。

   支持配置多条搜索条件。

5. 在**请选择日志源**下拉框中选择**进程告警日志**。

> **说明：**
> 云安全中心全要素日志目前已开放，您可在日志分析模块查看更多类型的日志信息。日志分析提供的日志类型请参见#unique_7。

6. 选择需要查询的日志字段、匹配条件并输入搜索**关键字**。

   支持使用自定义的告警规则名称或描述信息搜索相关规则命中日志。

7. 设置查询时间范围。

说明：

您可设置查询24小时内、7天内或一个月内的进程告警日志信息。

8. 单击**搜索**查看日志。