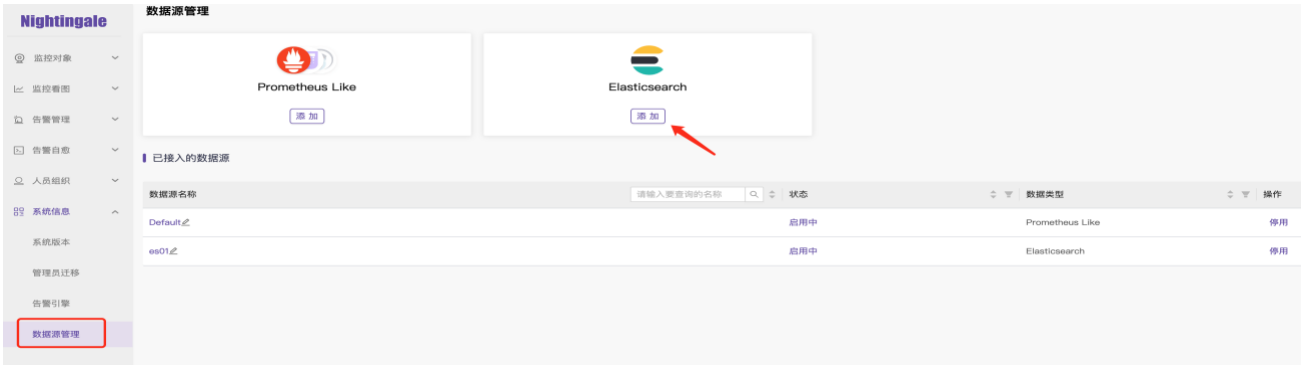
夜莺日志插件

把 ELASTICSEARCH 作为数据源，在夜莺里配置告警规则

北京快猫星云科技有限公司
FLASHCAT.CLOUD | 北京市海淀区用友产业园东区 19A

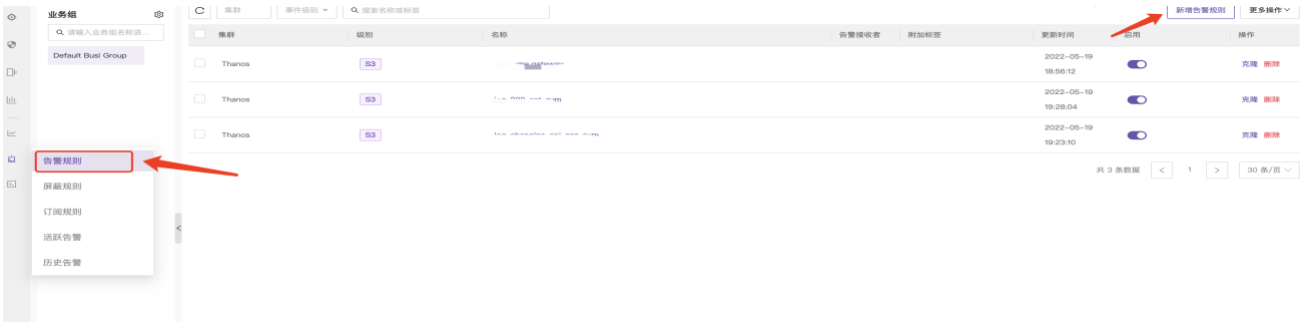
添加 ES 数据源

进入数据源管理页面，添加 ElasticSearch 数据源，按要求填写完表单之后，点击保存。

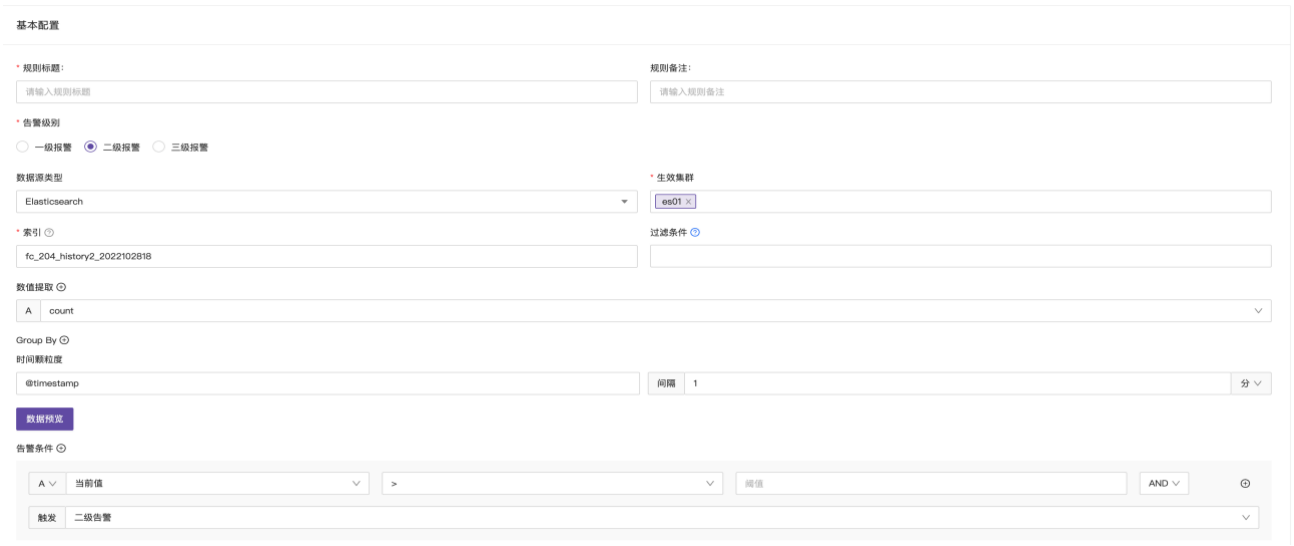


配置告警规则

左边菜单选择告警规则，点击 “新增告警规则”



数据源选择 ElasticSearch，生效集群填写刚才配置的集群



字段说明：

索引：支持多种配置方式

1. 指定单个索引 gb 在 gb 索引中搜索所有的文档

2. 指定多个索引 gb,us 在 gb 和 us 索引中搜索所有的文档

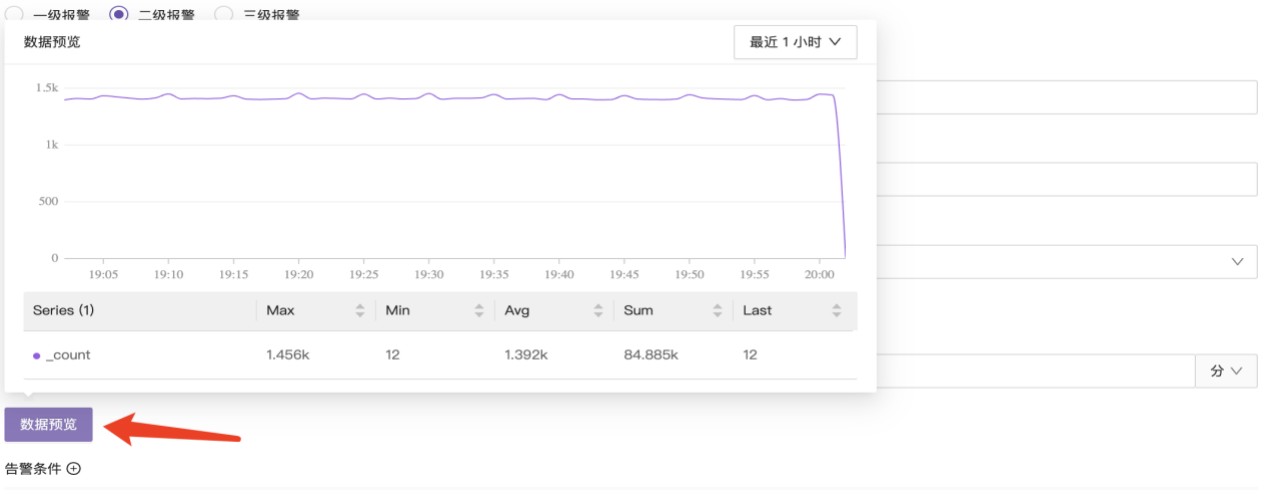
3. 指定索引前缀 g*,u* 在任何以 g 或者 u 开头的索引中搜索所有的文档

过滤条件：查询语法可参考 es 官方文档

数值提取：统计匹配的日志条数（count），提取选取字段的数值进行计算（avg max min sum p90 p95 p99 ）

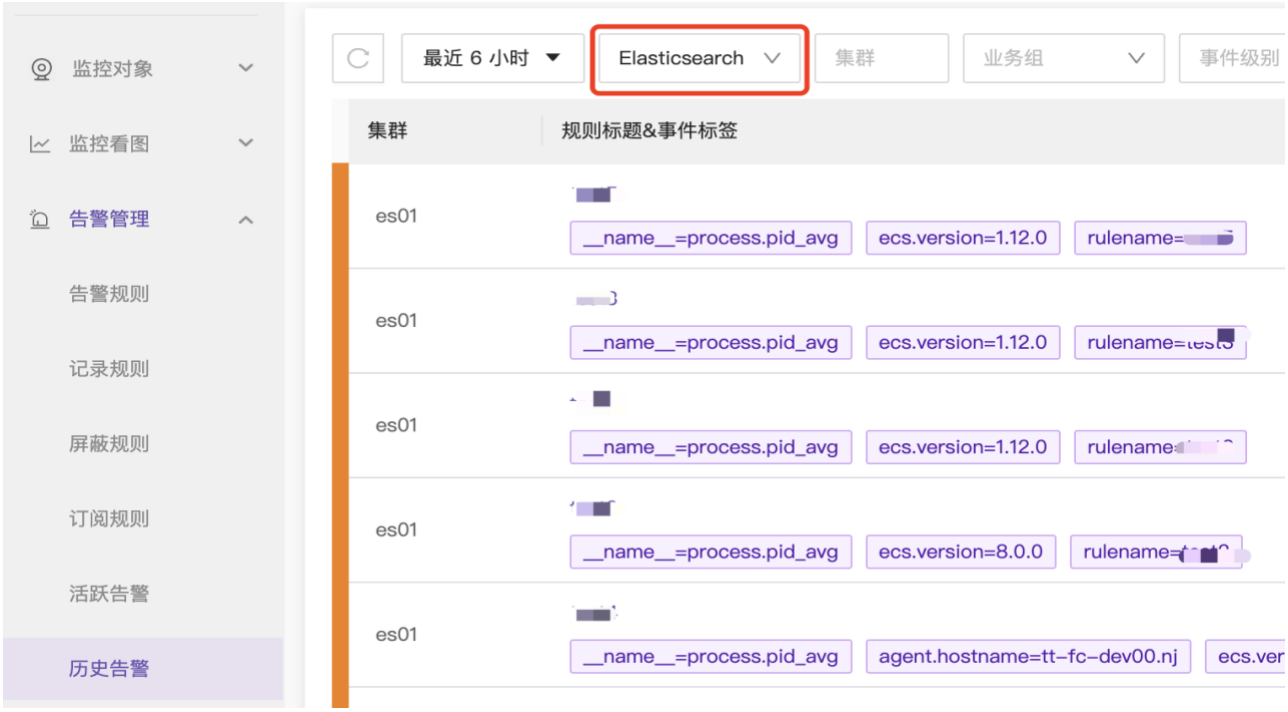
GroupBy：对查询的结果按照指定的分组单独处理，类似于 SQL 中的 group by

过滤条件填写完成之后，可以点击数据预览，检测填写是否正确，确认正确之后，填写其他告警规则配置，点击保存即可



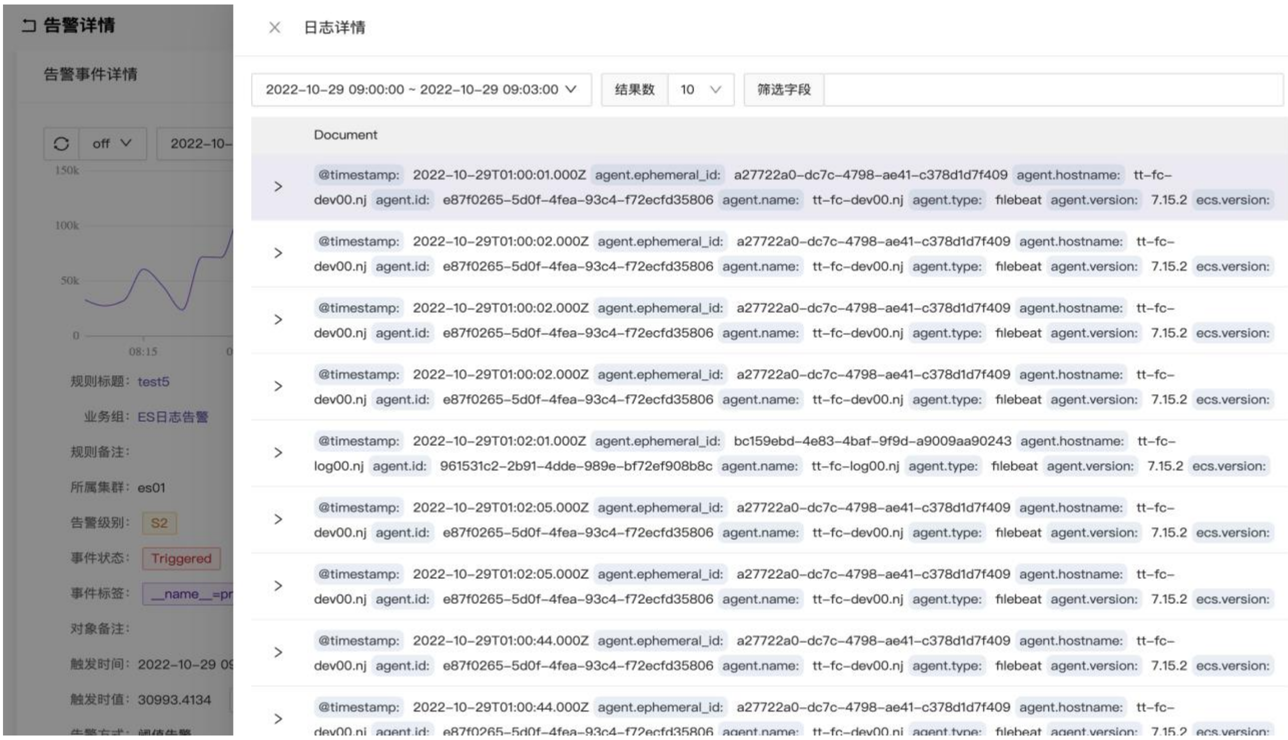
告警事件详情

点击“历史告警” 菜单，数据源类型选择 ElasticSearch ，即可查看 ES 告警事件列表



点击选择的告警事件，进入详情页，即可查看对应告警时刻的数值变化曲线

点击 日志详情 按钮，可以查看告警触发时刻和规则相关的日志原文



其他告警规则参数说明：

规则标题：告警规则标题，例如 “磁盘需要清理了-利用率达到 92%”

规则备注：填写额外的说明备注

生效集群：要监控的指标，所属的集群

执行频率：检测曲线是否异常的频率

持续时长：曲线持续异常多久才触发告警

附加标签：告警规则的额外说明，会追加到生成告警事件中

预案链接：如果有规则对应的预案 wiki，可以把 wiki 地址写到这里，发送通知的时候，可以把预案链接带上

生效时间：即规则生效时间，默认 7*24 生效，可以配置只生效部分时间段

通知媒介：通知的渠道

接收组：通知的对象，接收组在人员组织菜单管理

恢复通知：可以设置是否发送恢复通知

留观时长：持续 n 秒没有再次触发阈值才发送恢复通知

发送频率：如果告警持续未恢复，间隔 60 分钟之后重复提醒告警接收组的成员

回调地址：会将告警事情发送给填写的 webhook 地址

联系我们：contact-us@flashcat.cloud