

夜莺日志插件

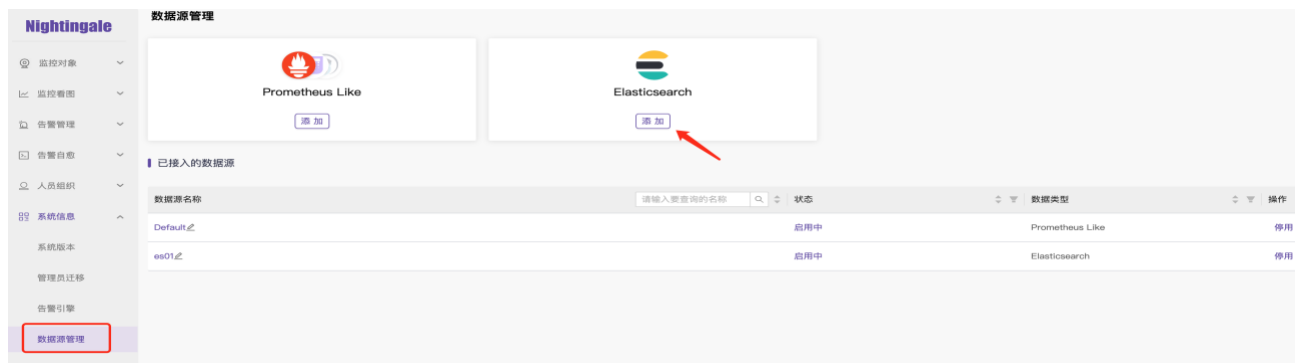
把 ELASTICSEARCH 作为数据源，在夜莺里配置告警规则

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

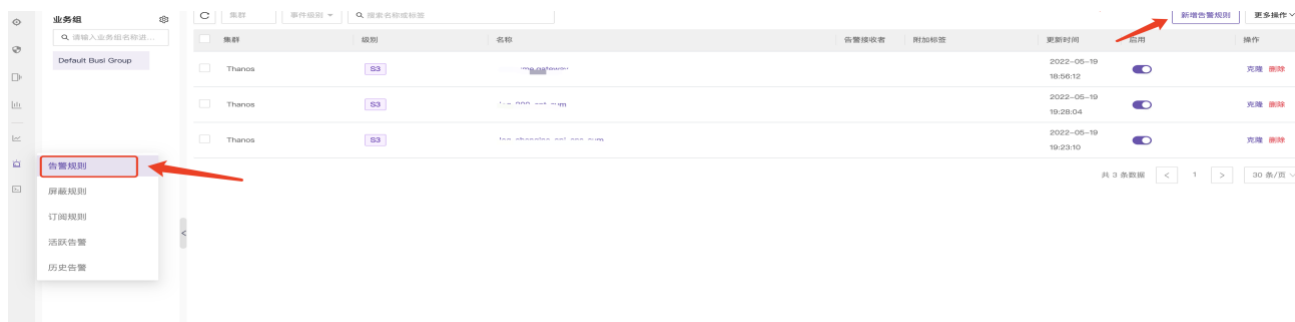
添加 ES 数据源

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

基本配置

* 规则标题: 规则备注:

* 告警级别: 一级告警 二级告警 三级告警

数据源类型: * 生效集群:

* 索引: 过滤条件:

数值提取:

Group By: 时间颗粒度: 分

数据预览

告警条件: 触发:

字段说明:

索引: 支持多种配置方式

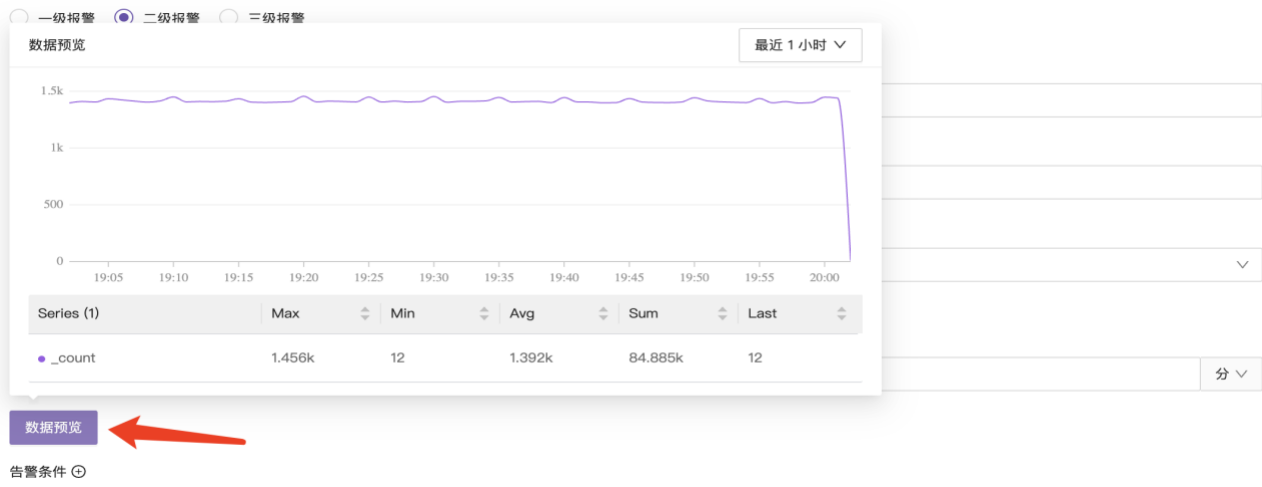
1. 指定单个索引 gb 在 gb 索引中搜索所有的文档
2. 指定多个索引 gb,us 在 gb 和 us 索引中搜索所有的文档
3. 指定索引前缀 g*,u* 在任何以 g 或者 u 开头的索引中搜索所有的文档

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

The screenshot shows a monitoring interface with a sidebar on the left containing navigation items like '监控对象', '告警管理', and '历史告警'. The main area displays a table of alert events. At the top, there are filters for '最近 6 小时', 'Elasticsearch' (highlighted with a red box), '集群', '业务组', and '事件级别'. Below these, a table lists events for cluster 'es01'. Each event row includes a small bar chart and several tags: '.__name__.process.pid_avg', 'ecs.version=1.12.0', and 'rulename=test5'. The last event also includes 'agent.hostname=tt-fc-dev00.nj' and 'ecs.ver'.

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

The screenshot shows the '告警事件详情' (Alert Event Details) page. At the top, there's a refresh button and a time range selector set to '2022-10-29 08:32 ~ 2022-10-29 09:32'. Below this is a line chart with a y-axis from 0 to 150k and an x-axis from 08:15 to 09:10. A vertical dashed red line marks the trigger time at approximately 09:02. Below the chart, the following details are shown:

- 规则标题: test5
- 业务组: ES日志告警
- 规则备注:
- 所属集群: es01
- 告警级别: S2
- 事件状态: Triggered
- 事件标签: .__name__.process.pid_avg, ecs.version=1.12.0, rulename=test5
- 对象备注:
- 触发时间: 2022-10-29 09:02:00
- 触发时值: 30993.4134 (with a '日志详情' button)
- 告警方式: 阈值告警

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

告警详情

告警事件详情

2022-10-29 08:15

规则标题: test5

业务组: ES日志告警

规则备注:

所属集群: es01

告警级别: S2

事件状态: Triggered

事件标签: __name__=pr

对象备注:

触发时间: 2022-10-29 09:03:00

触发时值: 30993.4134

告警方式: 推送告警

× 日志详情

2022-10-29 09:00:00 ~ 2022-10-29 09:03:00 结果数 10 筛选字段

Document

```

> @timestamp: 2022-10-29T01:00:01.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:00:02.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:00:02.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:00:02.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:02:01.000Z agent.ephemeral_id: bc159ebd-4e83-4baf-9f9d-a9009aa90243 agent.hostname: tt-fc-log00.nj agent.id: 961531c2-2b91-4dde-989e-bf72ecfd908b8c agent.name: tt-fc-log00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:02:05.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:02:05.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:00:44.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:
> @timestamp: 2022-10-29T01:00:44.000Z agent.ephemeral_id: a27722a0-dc7c-4798-ae41-c378d1d7f409 agent.hostname: tt-fc-dev00.nj agent.id: e87f0265-5d0f-4fea-93c4-f72ecfd35806 agent.name: tt-fc-dev00.nj agent.type: filebeat agent.version: 7.15.2 ecs.version:

```

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