

夜莺专业版介绍

前言

夜莺有三个版本：开源版、专业版、企业版。

- 开源版：免费的、代码公开的，可以在 github (<https://github.com/ccfos/nightingale>) 下载使用
- 专业版：对开源版本做了一些功能增强，具体在后文介绍
- 企业版：即 [快猫 Flashcat 平台](#)，提供一整套的稳定性治理框架和可观测性能力，包含北极星、灭火图、事件墙、多维日志分析等商业模块，也包含专业版的所有能力

本文介绍的专业版相较开源版的功能增强。

概要

功能		开源版	专业版
告警管理	Metrics 指标阈值告警	✓	✓
	Host 机器失联、时间偏移告警	✓	✓
	ElasticSearch 日志告警		✓
	智能告警引擎（利用算法做智能告警）		✓
	规则管理：屏蔽规则、订阅规则、记录规则	✓	✓
	活跃告警、历史告警管理	✓	✓
	全局屏蔽、服务日历		✓
通知渠道	内置支持阿里云电话、短信通知渠道		✓
	内置支持腾讯云电话、短信通知渠道		✓

扩展数据源	SLS数据源（告警、看图）		√
	InfluxDB数据源（告警、看图）		√
	ClickHouse数据源（告警、看图）		√
	Zabbix数据源（看图）		√
数据可视化	指标即时查询	√	√
	指标快捷视图	√	√
	自定义仪表盘+内置常用仪表盘	√	√
	ElasticSearch 可视化	√	√
	指标预聚合		√
机器管理	机器分组打标签	√	√
	基础metadata信息展示	√	√
	扩展metadata信息展示		√
	catgraf 采集规则管理下发		√
基础设施	网络设备		√
	拨测		√
	Pingmesh		√
人员组织	用户管理、团队管理、业务组管理	√	√
	角色管理、权限管理	√	√
系统配置	数据源管理	√	√
	通知媒介、渠道、模板配置	√	√
	单点登录（OIDC、CAS等）	√	√
操作审计	告警规则修改审计记录		√

技术支持	以上商业模块技术支持		✓
	开源夜莺技术支持 仓库: github.com/ccfos/nightingale		✓
	Catgraf技术支持 仓库: github.com/flashcatcloud/catgraf		✓

增强功能详解

告警管理

ElasticSearch 日志告警

ElasticSearch 通常用于存储日志，我们经常需要对异常关键字做告警，或者从日志中提取指标对指标做告警（很多业务没有直接埋点，使用日志来暴露各类指标），指标、日志相关的告警规则都可以集成到夜莺来统一管理。

The screenshot displays the configuration interface for an ElasticSearch alert rule. The '数据预览' (Data Preview) button is highlighted with a red arrow, pointing to a line chart showing the count of data points over time. The chart shows a steady increase in the count, reaching a peak of 903 at 13:10. Below the chart is a table with columns for Series (1), Max, Min, Avg, Sum, and Last. The values are: Series (1) is _count, Max is 903, Min is 9, Avg is 850.508, Sum is 51.881k, and Last is 9.

告警规则的配置原理，就是填写 ElasticSearch 查询 API 所需要的各类参数，包括索引、查询条件等，夜莺就会拿着这些查询条件去查询 ElasticSearch，如果查询到了数据并触发了阈值，则告警。对于 ElasticSearch 触发的告警，在告警详情页面会提供快捷入口，方便地查看告警时刻相关的日志。

查询面板

规则标题: 有监控对象失联

业务组: telegraf-host

规则备注:

所属集群: Default

告警级别: S1

事件状态: Triggered

事件标签: __name__=target_up ident=tt-fo-dev01.nj region=tencent rulename=有监控对象失联

对象备注:

触发时间: 2022-08-03 14:12:24

触发时值: 0 [日志详情](#)

告警方式: 阈值告警

2022-08-17 00:00 - 2022-08-17 23:59

结果数 10

结果数 10

Document

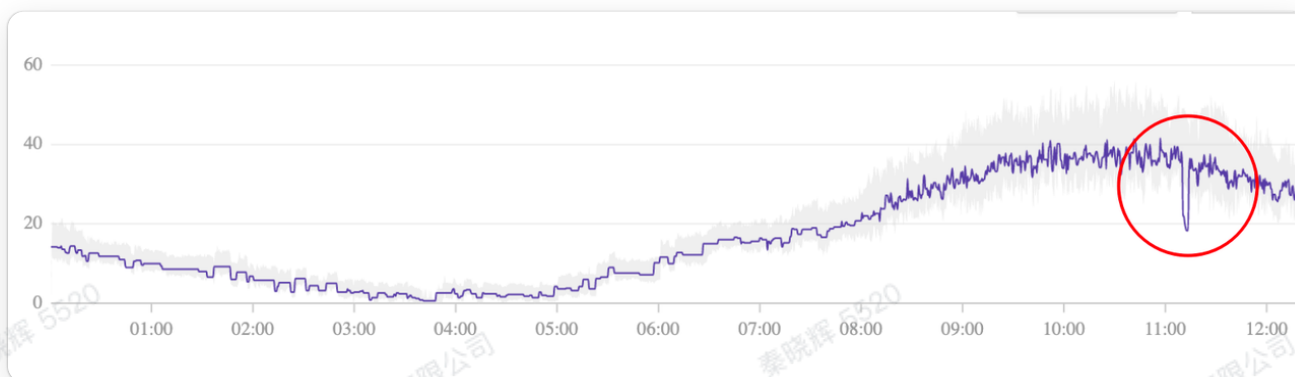
```

> @timestamp: Aug 25, 2022 @ 00:00:28.687 app_name: vn log_level: INFO log_message: NetService.java,173 网络变更:ws4zs开始,变更时间戳:中间有空格 前一位
thread_name: Net_Business_Thread_1-4-1 _id: Y2WVEI8_MIECFdW-7 _index: ds_1a631e33_20220825 _score: 1 _type: .doc
> @timestamp: Aug 25, 2022 @ 00:00:29.686 app_name: vn log_level: INFO log_message: NetService.java,173 网络变更:ws4zs开始,变更时间戳:中间有空格 前一位
thread_name: Net_Business_Thread_1-4-1 _id: Y2WVEI8_MIECFdW-7 _index: ds_1a631e33_20220825 _score: 1 _type: .doc
> @timestamp: Aug 25, 2022 @ 00:00:29.688 app_name: vn log_level: INFO log_message: NetService.java,173 网络变更:ws4zs开始,变更时间戳:中间有空格 前一位
thread_name: Net_Business_Thread_1-4-1 _id: Y2WVEI8_MIECFdW-7 _index: ds_1a631e33_20220825 _score: 1 _type: .doc
> @timestamp: Aug 25, 2022 @ 00:00:31.684 app_name: vn log_level: INFO log_message: NetService.java,173 网络变更:ws4zs开始,变更时间戳:1655363298514 @
thread_name: Net_Business_Thread_1-4-1 _id: Y2WVEI8_MIECFdW-7 _index: ds_1a631e33_20220825 _score: 1 _type: .doc
> @timestamp: Aug 25, 2022 @ 00:00:38.687 app_name: vn log_level: INFO log_message: NetService.java,173 网络变更:ws4zs开始,变更时间戳:1655363298514 @
thread_name: Net_Business_Thread_1-4-1 _id: ZM0VEI8_MIECFdW-7 _index: ds_1a631e33_20220825 _score: 1 _type: .doc
> @timestamp: Aug 25, 2022 @ 00:00:32.687 app_name: vn log_level: INFO log_message: NetService.java,173 网络变更:ws4zs开始,变更时间戳:1655363298514 @
thread_name: Net_Business_Thread_1-4-1 _id: 60WVEI8_MIECFdW-7 _index: ds_1a631e33_20220825 _score: 1 _type: .doc
> @timestamp: Aug 25, 2022 @ 00:00:33.687 app_name: vn log_level: INFO log_message: NetService.java,173 网络变更:ws4zs开始,变更时间戳:1655363298514 @

```

智能告警引擎

有些指标具有很强的规律，而且不适合配置固定的阈值，此时就可以引入智能告警引擎，通过算法自动计算动态阈值，如果真实数据偏离动态阈值过多，则告警。比如下图灰色部分，就是通过算法预测的动态阈值范围，紫色的线是真实数据，在红圈位置因为有个下跌，跌破了动态阈值范围，就自动告警了。



如果采买智能告警引擎，需要单独部署一个机器学习的训练模块，整个架构如图所示：



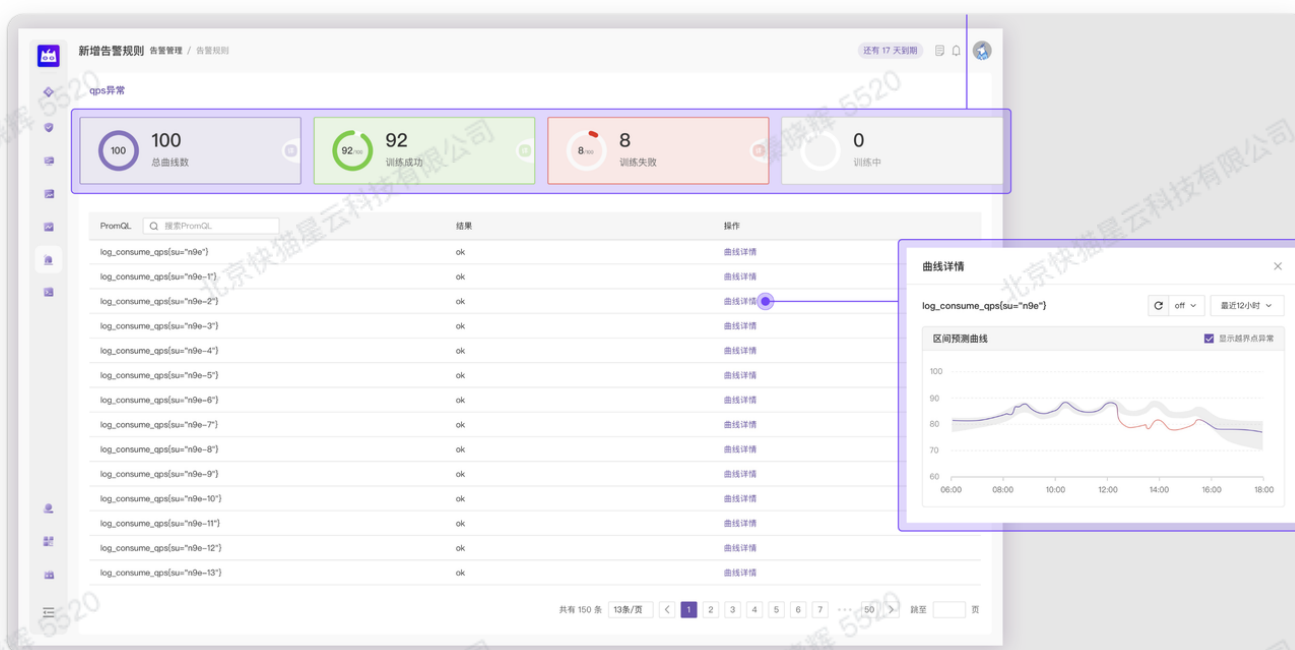
智能异常检测模块安装完成之后，在夜莺告警规则配置页面，会多出一个智能告警的选项，如下图所示：



选择智能告警之后，只需填写要监控的指标，不需要填写阈值，点击保存即可，之后在告警规则列表页，智能告警的规则右侧会有一个“训练结果”的按钮：

集群	级别	名称	告警接收者	附加标签	更新时间	启用	操作
<input type="checkbox"/>	Default	S2	alert_test		2022-07-08 16:54:07	<input checked="" type="checkbox"/>	克隆 删除 训练结果
<input type="checkbox"/>	Default	S2	compare_test41		2022-06-15 15:53:22	<input checked="" type="checkbox"/>	克隆 删除 训练结果

点击“训练结果”，可以进入训练结果详情页，点击曲线详情，可以看到曲线学习出来的动态基线。如果曲线偏离到基线之外，夜莺的告警引擎会发出告警通知。



全局屏蔽

使用全局屏蔽，管理员可以一键对整个平台的告警进行屏蔽，做一些计划性维护工作时，可以更方便地屏蔽告警。

启用

屏蔽时间类型 固定时间 周期时间

屏蔽开始时间: 2023-10-11 17:56:53 屏蔽时长: 2h 屏蔽结束时间: 2023-10-11 19:56:53

屏蔽事件标志Key: 运算符: 标志Value:

排除业务组:

排除数据源:

屏蔽原因:

服务日历

对于一些业务，会有交易日和非交易日的场景，在非交易日的时候，服务会关闭，期间不需要告警通知。此时可以使用服务日历的功能，配置好哪些是非交易日，在告警规则中关联了服务日历之后，只有在交易日告警规则才会生效，不再需要频繁地修改规则的生效时间。

日历详情

一月 2023							二月 2023							三月 2023							四月 2023						
日	一	二	三	四	五	六	日	一	二	三	四	五	六	日	一	二	三	四	五	六	日	一	二	三	四	五	六
1	2	3	4	5	6	7				1	2	3	4														
8	9	10	11	12	13	14	5	6	7	8	9	10	11	2	3	4	5	6	7	8							
15	16	17	18	19	20	21	12	13	14	15	16	17	18	9	10	11	12	13	14	15							
22	23	24	25	26	27	28	19	20	21	22	23	24	25	16	17	18	19	20	21	22							
29	30	31					26	27	28					23	24	25	26	27	28	29							

五月 2023							六月 2023							七月 2023							八月 2023						
日	一	二	三	四	五	六	日	一	二	三	四	五	六	日	一	二	三	四	五	六	日	一	二	三	四	五	六
						6						1	2	3													
7	8	9	10	11	12	13	4	5	6	7	8	9	10	2	3	4	5	6	7	8	6	7	8	9	10	11	12
14	15	16	17	18	19	20	11	12	13	14	15	16	17	9	10	11	12	13	14	15	13	14	15	16	17	18	19
21	22	23	24	25	26	27	18	19	20	21	22	23	24	16	17	18	19	20	21	22	20	21	22	23	24	25	26
28	29	30	31				25	26	27	28	29	30		23	24	25	26	27	28	29	27	28	29	30	31		

九月 2023							十月 2023							十一月 2023							十二月 2023							
日	一	二	三	四	五	六	日	一	二	三	四	五	六	日	一	二	三	四	五	六	日	一	二	三	四	五	六	
						2							1	2	3	4												
						9	1	2	3	4	5	6	7	8	9	10	11											
10	11	12	13	14	15	16	8	9	10	11	12	13	14	5	6	7	8	9	10	11	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	15	16	17	18	19	20	21	12	13	14	15	16	17	18	17	18	19	20	21	22	23	24
24	25	26	27	28	29	30	22	23	24	25	26	27	28	19	20	21	22	23	24	25	24	25	26	27	28	29	30	31

基础配置

日历名称: 年份:

备注:

假期停服日期 是否包含周末

日期	备注	操作
09-29, 09-30, 10-01, 10-02, 10-03, 10-04, 10-05, 10-06	国庆	编辑 删除
10-15, 10-16, 10-17, 10-18, 10-19		编辑 删除

假期服务在线日期

日期	备注	操作
10-06		编辑 删除

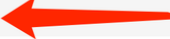
生效配置

立即启用

生效时间 开始时间 结束时间

00:00 00:00

服务日历


2023 

2024

通知渠道

内置阿里云电话、短信通知媒介

开源版本也可以做到，不过需要自行编写 notify.py 脚本，商业用户只需要在页面配置认证信息就可以自动打通了，更加便捷。

通知设置 

回调地址 通知脚本 通知媒介 联系方式 SMTP 设置 腾讯云短信 腾讯云语音 阿里云短信 阿里云语音

```
1
2 AlibabaCloudAccessKeyId = "xxx"
3 AlibabaCloudAccessKeySecret = "xxx"
4 AlibabaCloudEndpoint = "dyvmsapi.aliyuncs.com"
5 TtsCode = "TT"
6 PlayTimes = 3
7
```

保存

内置腾讯云电话、短信通知媒介

开源版本也可以做到，不过需要自行编写 `notify.py` 脚本，商业用户只需要在页面配置认证信息就可以自动打通了，更加便捷。

扩展数据源

SLS 数据源

SLS 是阿里云的日志产品，如果您有些数据是在 SLS，也可以在夜莺里配置管理告警规则（和 ElasticSearch 告警引擎的原理类似），可以在夜莺里绘图可视化。

数据源类型: 阿里云SLS * 生效集群: sls_test

查询统计: A 项目: grafana-test 日志库: test 查询区间: 最近 5 分钟 SQL增强

查询条件: *|select avg(body_bytes_sent) as size, count(1) as count

辅助配置

数据预览

告警条件: 简单模式 表达式模式

A > 0

关联 Label: 触发 一级告警

ElasticSearch 中您要选择索引，在 SLS 中您要选择项目、日志库等信息，这是 SLS 特有的概念。

InfluxDB 数据源

InfluxDB 和 ElasticSearch、SLS 的告警类似，也是输入一个查询条件获得输出，对输出的结果进行阈值判断，当然了，这里的查询条件需要使用 Influx 的 QL。

数据源类型 * 生效集群

InfluxDB lim_20230314 x

查询统计计 ⊕

A 数据库 test

查询条件 `select count(usage_idle) from cpu` 查询区间 最近 1 分钟

> 查询辅助

告警条件 ⊕

简单模式 表达式模式

A > 0

关联 Label: ⊕

触发 一级告警

ClickHouse 数据源

ClickHouse 因为其优秀的性能被越来越多的公司采用，夜莺专业版也可以接入 ClickHouse 作为数据源，对 ClickHouse 的数据进行查询告警和可视化

数据源类型 * 生效集群

ClickHouse test_ck x

查询统计计 ⊕

A SQL `select count() cnt, event_time, type from system.query_log where toUnixTimestamp(event_time) >= toUnixTimestamp(now()) - 10 GR`

时间字段 时间格式 DateTime 查询区间 最近 1 分钟

辅助配置

ValueKey cnt LabelKey type x

数据预览

告警条件 ⊕

简单模式 表达式模式

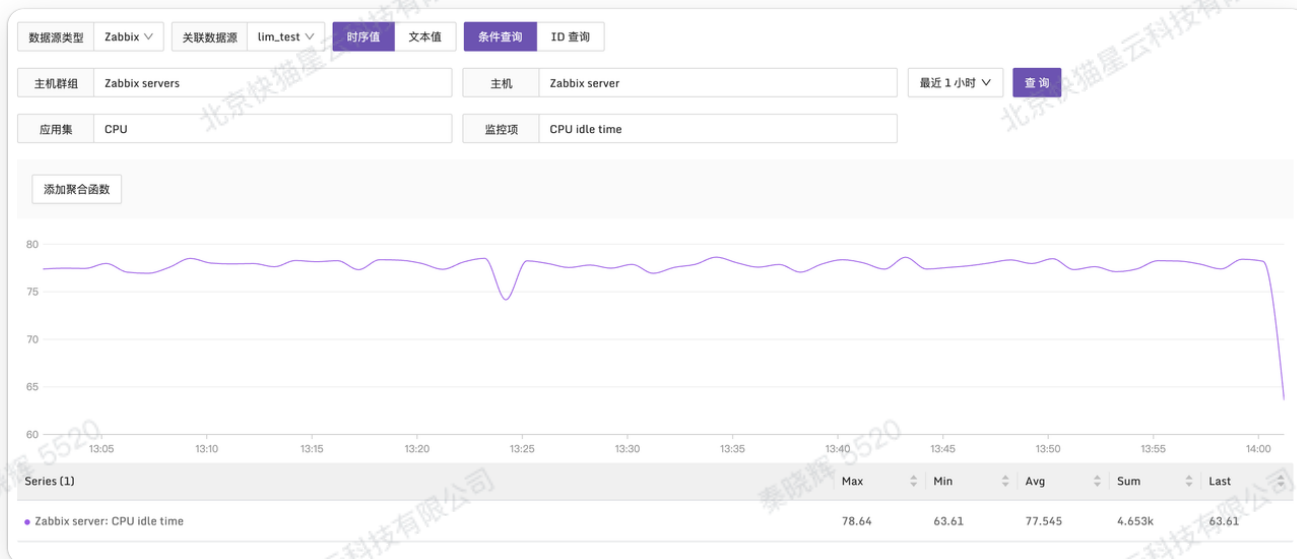
A > 0

关联 Label: ⊕

触发 三级告警

Zabbix 数据源

Zabbix 作为老牌的监控工具，仍然被很多公司采用，作为机器、网络设备监控的首选工具，夜莺可以接入 Zabbix 作为数据源，目前可以对 Zabbix 数据做可视化，告警引擎尚未对接 Zabbix。



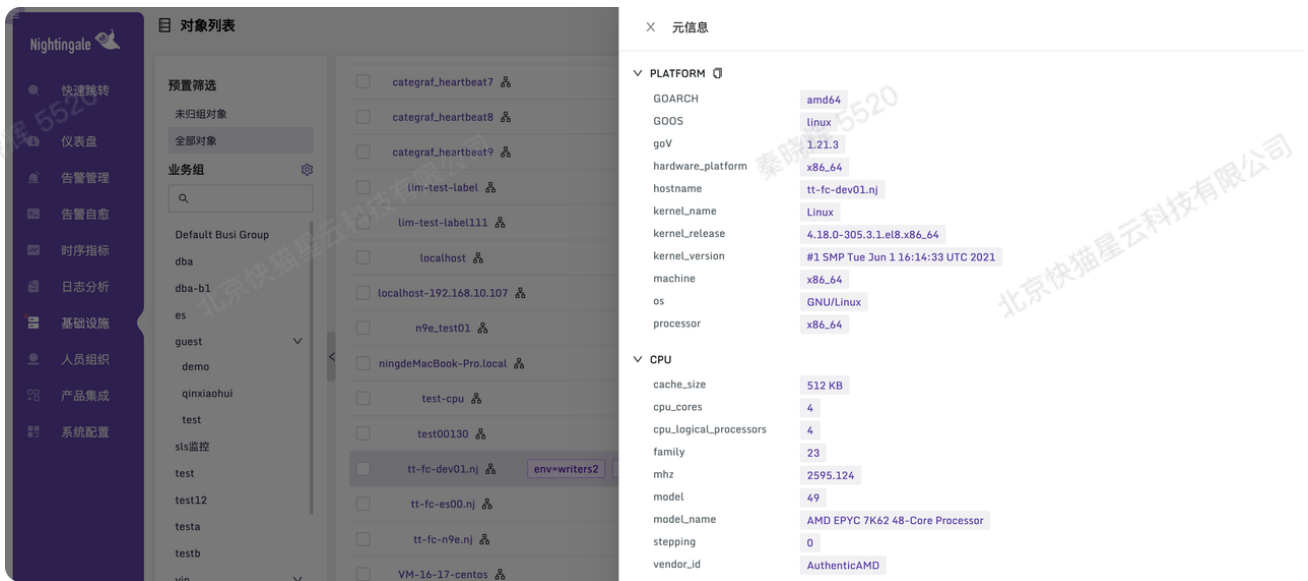
机器管理

扩展 metadata 信息展示

默认开源版本的机器列表，只有少量信息展示，如下图：

<input type="checkbox"/>	标识	标签	业务组	状态	内存	CPU	时间偏移	心跳时间	来源IP
<input type="checkbox"/>	bogon		board	DOWN	83.8%	81.8%	222 ms	2023-04-27 20:12:09	10.206.0.13
<input type="checkbox"/>	localhost	service=mon	board	DOWN	82.5%	24.1%	125 ms	2023-05-12 13:59:24	10.206.0.13
<input type="checkbox"/>	ningdeMacBook-Pro.local		未归组	DOWN	77.5%	22%	209 ms	2023-04-28 17:01:01	10.206.0.13
<input type="checkbox"/>	tt-fc-es00.nj		Default Busi Group	UP	unknown	unknown	unknown	unknown	unknown
<input type="checkbox"/>	tt-fc-n9e.nj	mod=mon	Default Busi Group	UP	47.4%	5%	6 ms	2023-05-16 14:03:50	10.206.16.17

商业版本采集了更多更详细的机器 metadata 信息，点击某个机器即可看到详情。



Catgraf 采集规则管理下发

开源版本的 Catgraf 采集监控数据，是需要修改本地配置文件的，每次修改完成配置之后，还需要手工重启 Catgraf 或者发送 HUP 信号，很不方便。专业版提供了页面上中心化管理采集策略的能力。比如 mysql、redis、进程、端口、ping 等等所有插件的采集配置，都可以在页面上管理。



创建采集规则的时候，可以选择生效的机器范围，采集的插件，以及采集配置。右侧还会有个 Markdown 的提示信息，作为文档辅助。

筛选条件 ⊕

全部机器 ⌵ ⊖

[机器预览](#)

采集配置

* 插件类型

mysql ⌵

```

1 # # collect interval
2 # interval = 15
3
4 # [[queries]]

```

[测试](#)

基础设施

网络设备监控

开源的 `catgraf` 也提供了采集网络设备监控数据的能力，不过配置起来非常复杂，需要自己整理各种oid，专业版的网络设备管理，提供了网络设备管理和监控数据采集两个能力，可以在网络设备页面添加待监控的网络设备，选择使用哪个采集agent、以及内置的采集模板，实现非常方便地采集设备的监控数据。

C
采集 Agent
采集模板
🔍 请输入关键字搜索
新增 ⌵ 更多操作 ⌵

<input type="checkbox"/>	IP	设备名称	机房	设备型号	采集 Agent	附加标签	监控采集	更新时间	更新人	操作
<input type="checkbox"/>	10.206.0.16	tt-fc-dev01.nj	shanghai	Linux tt-fc-dev01.nj 4.18...	VM-16-17-centos	mod+n9e	<input checked="" type="checkbox"/>	2023-10-13 13:12:23		编辑 克隆 删除
<input type="checkbox"/>	10.206.0.2		shanghai				<input type="checkbox"/>	2023-10-19 13:20:39		编辑 克隆 删除

基础配置

* IP: 机房:

附加标签: 仪表盘链接:

备注:

监控采集

立即启用

采集 Agent: 采集模板:

SNMP 版本: SNMP 协议: SNMP 端口: 超时时间(s):

Community:

下图是采集模板样例

<input type="checkbox"/> Ruijie Device Status	2023-10-11 17:26:55	root	编辑 克隆 删除
<input type="checkbox"/> Huawei Test	2023-10-11 18:02:56	root	编辑 克隆 删除
<input type="checkbox"/> Huawei BGP Prefix	2023-10-09 15:30:34	root	编辑 克隆 删除
<input type="checkbox"/> Huawei BGP	2023-10-09 15:32:05	root	编辑 克隆 删除
<input type="checkbox"/> Airsta Device Status	2023-10-09 15:32:18	root	编辑 克隆 删除
<input type="checkbox"/> Huawei CE Device Status	2023-10-10 15:22:03	root	编辑 克隆 删除
<input type="checkbox"/> H3C Device Status	2023-09-19 18:41:32	root	编辑 克隆 删除
<input type="checkbox"/> Generic SNMPv2	2023-10-09 15:30:01	root	编辑 克隆 删除
<input type="checkbox"/> Juniper BGP	2023-10-19 11:28:32	root	编辑 克隆 删除
<input type="checkbox"/> Juniper Device Status	2023-10-09 15:29:37	root	编辑 克隆 删除

拨测

拨测是一种用于监测和评估网络性能的技术。它通过模拟真实用户的行为，定期发送测试数据包到目标网络或服务器，并收集关于网络延迟、丢包率等指标的信息。

夜莺专业版的拨测功能，提供了 HTTP(s)、ICMP、TCP、UDP、WSDL等多种协议，对目标进行探测，可以从**平均时延**、**连接超时**、**成功率**等维度展示探测目标的可用性

* 任务名称

flashcat.cloud

任务描述

请输入任务描述

* 协议类型

HTTP

协议方法

GET

字符编码

utf8

HTTP

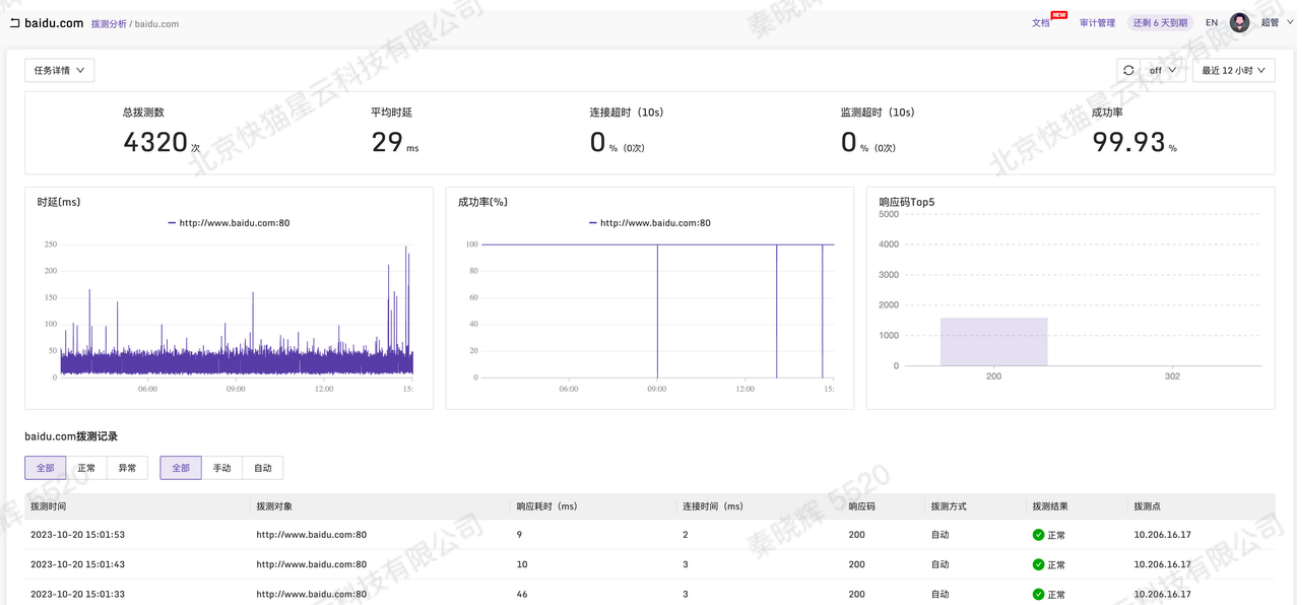
ICMP

TCP

UDP

WSDL

请求参数

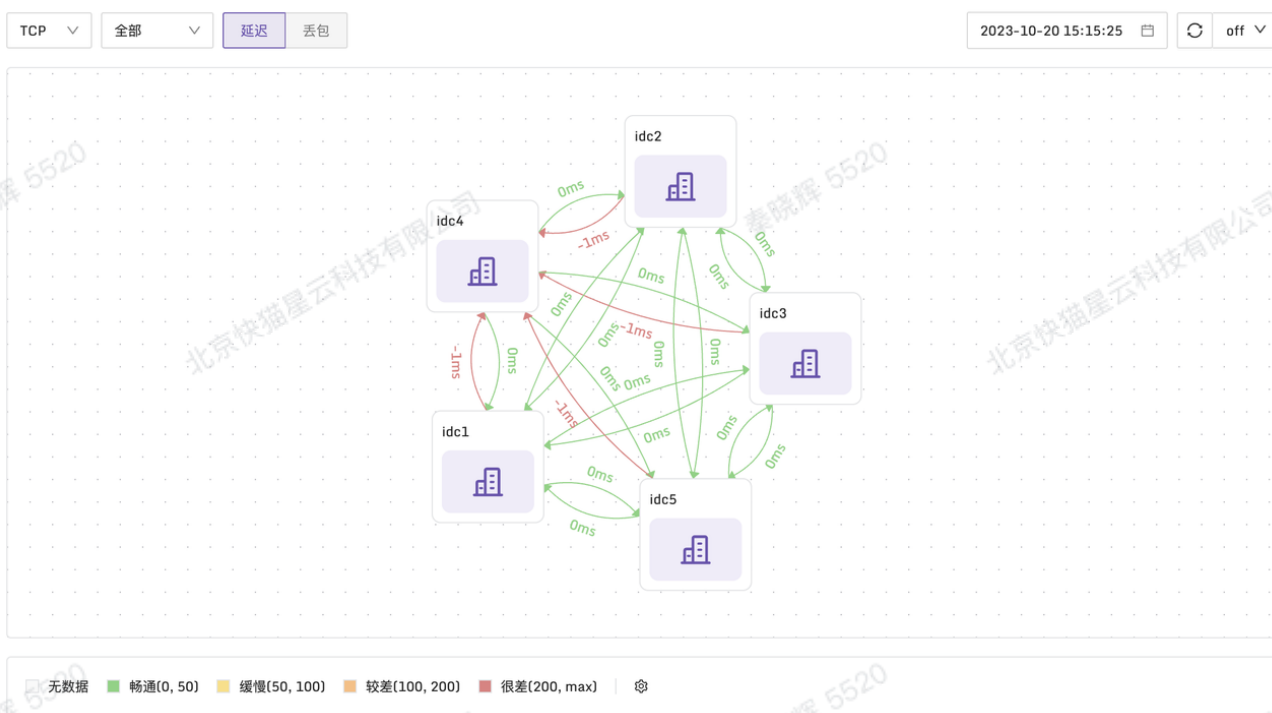


Pingmesh

Pingmesh 是一种用于测量和监控网络性能的技术，通过在一组通信对等体之间执行 ping 测试来评估网络的可用性和延迟。

夜莺专业版的 Pingmesh 功能，提供了 TCP、UDP、ICMP 三种协议，在设备之间进行互相探测，并绘制各个层面的连通性视图，从全局视角观测整个网络的连通性

IDC之间连通性



机柜之间连通性

目标	源	结果
rack4#41-44	rack1#11_11	网络不通
rack2#21-22	rack1#11_11	0
rack1#11_11	rack1#11_11	网络不通
rack3#31-33	rack1#11_11	0
rack5#51-55	rack1#11_11	0

机器之间连通性

目标	源	结果
10.206.0.13:8080	10.206.16.7	0

操作审计

告警规则修改审计记录

有时告警规则改出问题，难以追根溯源，通过审计功能可以记录所有规则修改，知道何时新增、删除了规则，何时修改了规则以及修改了具体什么内容。并且可以对比改了具体哪些字段。

