|  |
| --- |
| OAMLab |
| 运维实验·夜莺v4监控系统安装使用介绍 |
| 部署、使用 |

|  |
| --- |
| 李渊荣 584194788@qq.com  2022-10-1  基于GPL v3 |

目录

[一、 硬件环境 2](#_Toc120435327)

[1 、虚拟机一台 2](#_Toc120435328)

[1.1 虚拟机硬件要求 2](#_Toc120435329)

[二、 操作系统及软件版本 2](#_Toc120435330)

[1 、操作系统 2](#_Toc120435331)

[1.1 操作系统类型以及版本 2](#_Toc120435332)

[2 、中间件 2](#_Toc120435333)

[2.1 中间件类型以及版本 2](#_Toc120435334)

[三、 部署 2](#_Toc120435335)

[1 、夜莺server主机安装配置 2](#_Toc120435336)

[1.1 检查 selinux 是否关闭以及防火墙策略是否异常，如下命令可关闭 selinux 和防火墙。 2](#_Toc120435337)

[1.2 配置ntp服务器 2](#_Toc120435338)

[1.3 安装mysql、nginx和redis 3](#_Toc120435339)

[1.4 下载夜莺软件包，并进行环境初始化 3](#_Toc120435340)

[1.5 前端静态资源文件 3](#_Toc120435341)

[1.6 时序数据存储部署 3](#_Toc120435342)

[1.7 将夜莺相关服务进行systemd管理, 启动相关进程。 4](#_Toc120435343)

[1.8 访问夜莺主页，并登录查看 5](#_Toc120435344)

[1.9 配置夜莺告警短信脚本 5](#_Toc120435345)

[2 、夜莺agent主机安装配置 6](#_Toc120435346)

[2.1 检查 selinux 是否关闭以及防火墙策略是否异常，如下命令可关闭 selinux 和防火墙。 6](#_Toc120435347)

[2.2 配置ntp服务器 6](#_Toc120435348)

[2.3 下载夜莺软件包，部署agent服务 6](#_Toc120435349)

[2.4 将夜莺相关服务进行systemd管理, 启动相关进程。 7](#_Toc120435350)

[四、 使用说明 7](#_Toc120435351)

[1 、使用概览 7](#_Toc120435352)

[2 、资产管理系统 7](#_Toc120435353)

[3 、服务树：节点和叶子节点 7](#_Toc120435354)

[4 、用户管理、团队管理 9](#_Toc120435355)

[5 、角色管理（用户权限）：资源角色和页面角色 10](#_Toc120435356)

[6 、采集中间件 10](#_Toc120435357)

[7 、采集端口 12](#_Toc120435358)

[8 、进程采集 13](#_Toc120435359)

[9 、日志采集 13](#_Toc120435360)

[10 、告警策略 14](#_Toc120435361)

[五、 排错 16](#_Toc120435362)

[1 、n9e-v4版本常见安装问题 16](#_Toc120435363)

[1.1 系统安装好了，也能看到指标，但是点击指标看不到图 16](#_Toc120435364)

[1.2 server模块进程虽然在，但是server的两个端口都没有在监听 16](#_Toc120435365)

[1.3 设备管理的列表里缺少了本机设备 16](#_Toc120435366)

# 硬件环境

## 、虚拟机一台

* 1. 虚拟机硬件要求

Cpu： x86

内存： 最少4G

硬盘： 20G

# 操作系统及软件版本

## 、操作系统

* 1. 操作系统类型以及版本

Centos7.6

## 、中间件

* 1. 中间件类型以及版本

建议版本如下：

nginx：1.22.1

Mysql：5.7.40

Redis： 5.0.14

n9e(夜莺监控)： 4.0.3

# 部署

## 、夜莺server主机安装配置

* 1. 检查 selinux 是否关闭以及防火墙策略是否异常，如下命令可关闭 selinux 和防火墙。

setenforce 0

sed -i 's#SELINUX=enforcing#SELINUX=disabled#' /etc/selinux/config

systemctl disable firewalld.service

systemctl stop firewalld.service

* 1. 配置ntp服务器

为避免主机采集数据不上报，需配置ntp时间同步服务器

yum install ntpdate ntp –y

使用ntp同步所有机器时间

#192.168.0.101为ntp服务端ip地址

ntpdate -u 192.168.0.101

将时间同步命令写入定时任务

crontab -e

#192.168.0.101为ntp服务端ip地址

\* \* \* \* \* ntpdate -u 192.168.0.101

* 1. 安装mysql、nginx和redis

yum install -y redis mariadb nginx net-tools

启动服务

systemctl start mysqld

systemctl start redis

systemctl start nginx

systemctl enable redis

systemctl enable mysqld

systemctl enable nginx

设置mysql 数据库 root用户密码为1234

mysqladmin -u root -p password 1234

* 1. 下载夜莺软件包，并进行环境初始化

mkdir -p /data/n9e

cd /data/n9e

wget http://116.85.64.82/n9e-4.0.3.tar.gz

tar xf n9e-4.0.3.tar.gz

初始化数据库，这里假设使用 root 账号，密码为 1234，如果不是这个账号密码，需要修改 /data/n9e/etc/mysql.yml

cd sql

mysql -uroot -p1234 < n9e\_ams.sql

mysql -uroot -p1234 < n9e\_hbs.sql

mysql -uroot -p1234 < n9e\_job.sql

mysql -uroot -p1234 < n9e\_mon.sql

mysql -uroot -p1234 < n9e\_rdb.sql

redis请不要配置密码， 如果redis设置了密码，需要修改/home/n9e/etc/server.yml，把密码改对

* 1. 前端静态资源文件

静态资源文件放到/home/n9e下，请不要随意更换目录结构，否则还要自行修改nginx.conf

mkdir -p /home/n9e

cp -a pub /home/n9e

覆盖nginx.conf。如果静态资源文件不是放到/home/n9e下的，就要先修改nginx.conf了

cp etc/nginx.conf /etc/nginx/nginx.conf

systemctl restart nginx

* 1. 时序数据存储部署

这里选择使用单机版本的m3db

mkdir -p /data/m3db

cd /data/m3db

wget https://s3-gz01.didistatic.com/n9e-pub/tarball/m3dbnode-single-v0.0.1.tar.gz

tar zxvf m3dbnode-single-v0.0.1.tar.gz

cd m3dbnode-single

./scripts/install.sh

# 使用下面的curl初始化M3DB，这一步千万不能少！！！

# retentionTime 表示历史监控数据存储时长，使用m3一般建议最长不要超过3个月

# M3DB安装需要几分钟时间，需要等待几分钟再执行以下命令，若执行太早会报ERROR

curl -X POST http://localhost:7201/api/v1/database/create -d '{

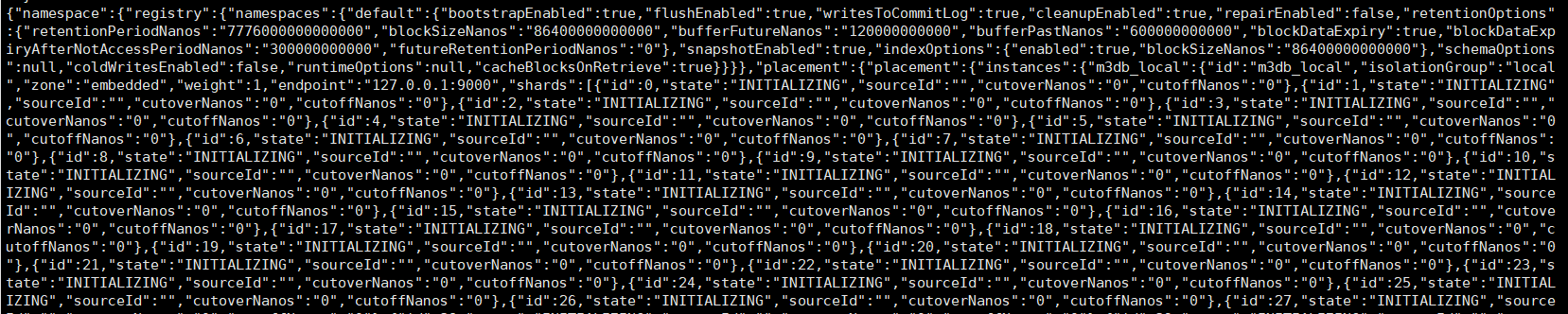
"type": "local",

"namespaceName": "default",

"retentionTime": "2160h"

}'

# 弹出以下内容说明M3DB初始化完成

****

将M3DB加入开机自启

systemctl enable m3dbnode.service

将M3DB数据目录缓存目录改为数据盘

mkdir -p /data/m3db

cp –a /opt/data/m3db/\* /data/m3db/

cp -a /opt/data/m3kv /data/m3kv

sed -i 's/opt//g' /opt/m3db/etc/m3dbnode.yml

systemctl restart m3dbnode.service

* 1. 将夜莺相关服务进行systemd管理, 启动相关进程。

cd /data/n9e/etc/service

sed -i 's/home/data/g' \* .service

cp \*.service /etc/systemd/system/

systemctl start agentd.service ;systemctl enable agentd.service

systemctl start prober.service ;systemctl enable prober.service

systemctl start server.service ;systemctl enable server.service

启动完成后，即可访问nginx看效果了

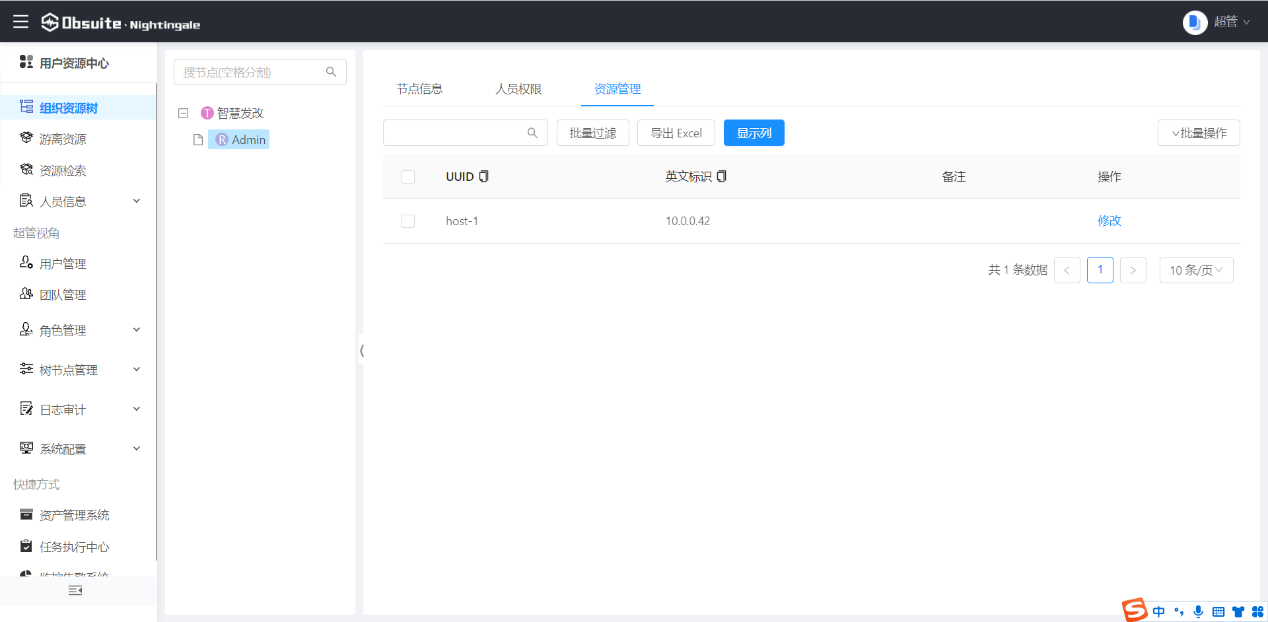
* 1. 访问夜莺主页，并登录查看

#尽量使用最新版谷歌浏览器访问

访问夜莺主页， 输入默认账号root 密码root.2020



登录成功



* 1. 配置夜莺告警短信脚本

修改n9e-server的配置文件

vim /data/n9e/etc/server.yml

sender:

mail:

# three choice: smtp|shell|api

way: smtp

worker: 10

api: http://127.0.0.1:2008/mail

sms:

# two choice: shell|api

#将sms中的way改成shell模式

way: shell

worker: 10

api: http://127.0.0.1:2008/sms

由于默认没有夜莺sms模块对接短信脚本的脚本，需要我们手动编写

vim /data/n9e/script/send\_sms

#!/bin/bash

# $1 传参电话号码 $2 传参短信内容

# sendsms.py短信脚本需要自行编写

/usr/bin/python /data/sendsms.py "$1" "$2"

echo "$1" >> /tmp/send\_sms.txt

echo "$2" >> /tmp/send\_sms.txt

echo "" >> /tmp/send\_sms.txt

给/data/n9e/script/send\_sms脚本添加执行权限

chmod +x /data/n9e/script/send\_sms

## 、夜莺agent主机安装配置

* 1. 检查 selinux 是否关闭以及防火墙策略是否异常，如下命令可关闭 selinux 和防火墙。

setenforce 0

sed -i 's#SELINUX=enforcing#SELINUX=disabled#' /etc/selinux/config

systemctl disable firewalld.service

systemctl stop firewalld.service

* 1. 配置ntp服务器

为避免主机采集数据不上报，需配置ntp时间同步服务器

yum install ntpdate ntp –y

使用ntp同步所有机器时间

#192.168.0.101为ntp服务端ip地址

ntpdate -u 192.168.0.101

将时间同步命令写入定时任务

crontab -e

#192.168.0.101为ntp服务端ip地址

\* \* \* \* \* ntpdate -u 192.168.0.101

* 1. 下载夜莺软件包，部署agent服务

mkdir -p /data/n9e

cd /data/n9e

wget http://116.85.64.82/n9e-4.0.3.tar.gz

tar xf n9e-4.0.3.tar.gz

修改address.yml中数据上报地址为server主机地址

# 10.0.0.42 为本文档试验server主机，读者请将此ip修改为生产server主机的ip地址

sed -i 's/127.0.0.1/10.0.0.42/g' /data/n9e/etc/address.yml

* 1. 将夜莺相关服务进行systemd管理, 启动相关进程。

cd /data/n9e/etc/service

sed -i 's/home/data/g' \* .service

cp \*.service /etc/systemd/system/

systemctl start agentd.service ;systemctl enable agentd.service

systemctl start prober.service ;systemctl enable prober.service

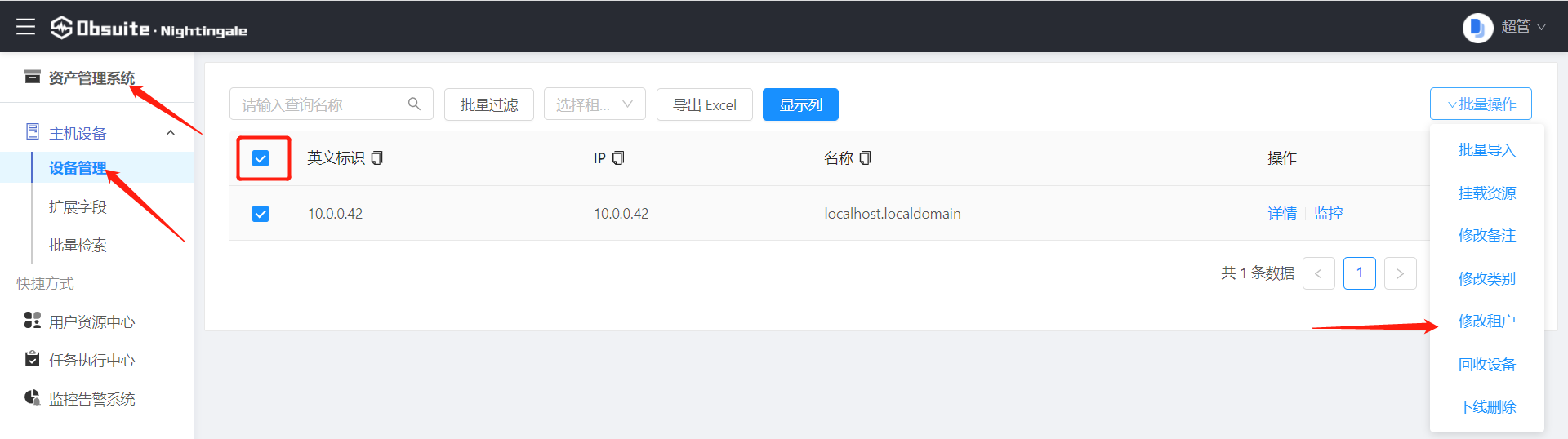
# 使用说明

## 、使用概览

夜莺server端和agent端安装完成后，首先先在资产管理系统中将所有监控设备的租户改为inner，然后建设服务树，添加叶子节点扩展信息，将监控设备挂载至叶子节点，检查叶子节点是否有监控数据，检查完成后完善扩展信息内容，然后添加需要接收短信或使用夜莺的用户，并将用户添加至对应团队，配置用户权限，完成后配置需要监控的采集项，例如配置监控首页url返回码，配置监控error日志等，最后配置告警策略即可。

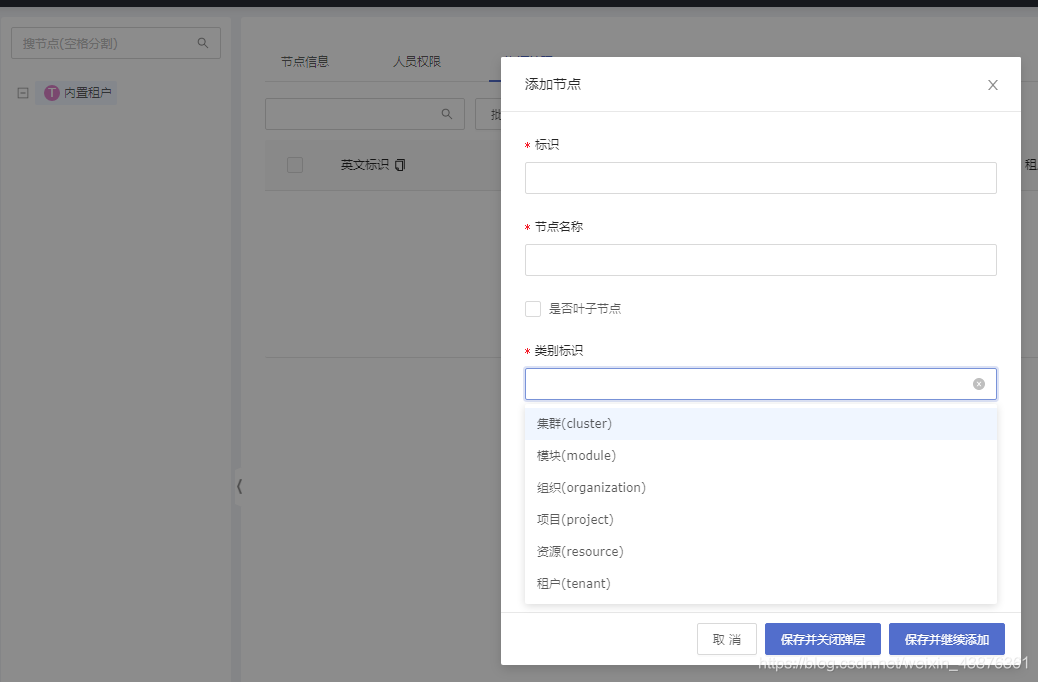
## 、资产管理系统

资产管理系统，是安装完成后的第一个需要操作的模块，需要第一时间将所有监控设备租户修改成inner



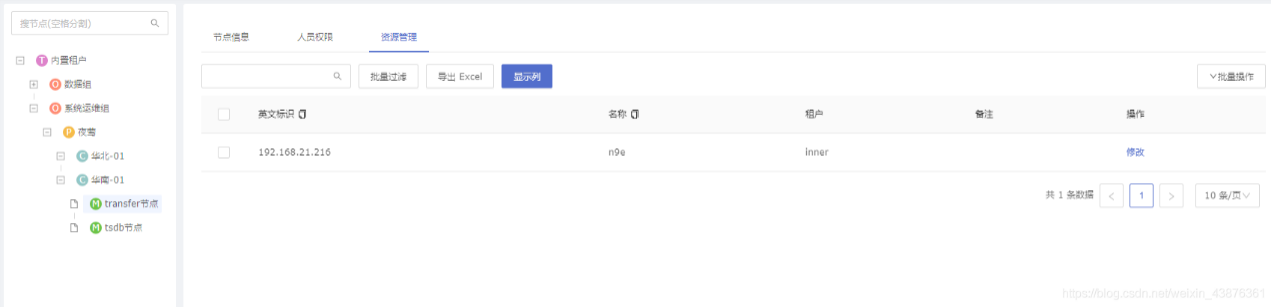
## 、服务树：节点和叶子节点

节点：是根据各个公司自己的规则来进行设计，类别可分为租户、资源、项目、组织、模块、集群，现在集群是有设置一个默认租户，小团队一般不用改租户，直接在下面创建节点就好，服务树这个功能还是比较好用的；



注意：资源权限可根据设计挂在某个父节点，则可拥有父节点下的子节点的相关权限

子节点：终端挂载的具体节点，且终端只能挂载在叶子节点下；挂载以后，就可以看到该节点的机器，如下图



注意：夜莺是需要先在资产管理系统给机器分配租户以后，才能在用户资源中心挂载，否则是无法识别到的；

挂载方式有两种：一种是在节点下，点击右上角的批量操作进行挂载；一种是在左侧的【游离资源】处进行挂载

服务树搭建样例：

#可根据实际情况进行灵活修改格式

-项目名 --默认只需修改名称

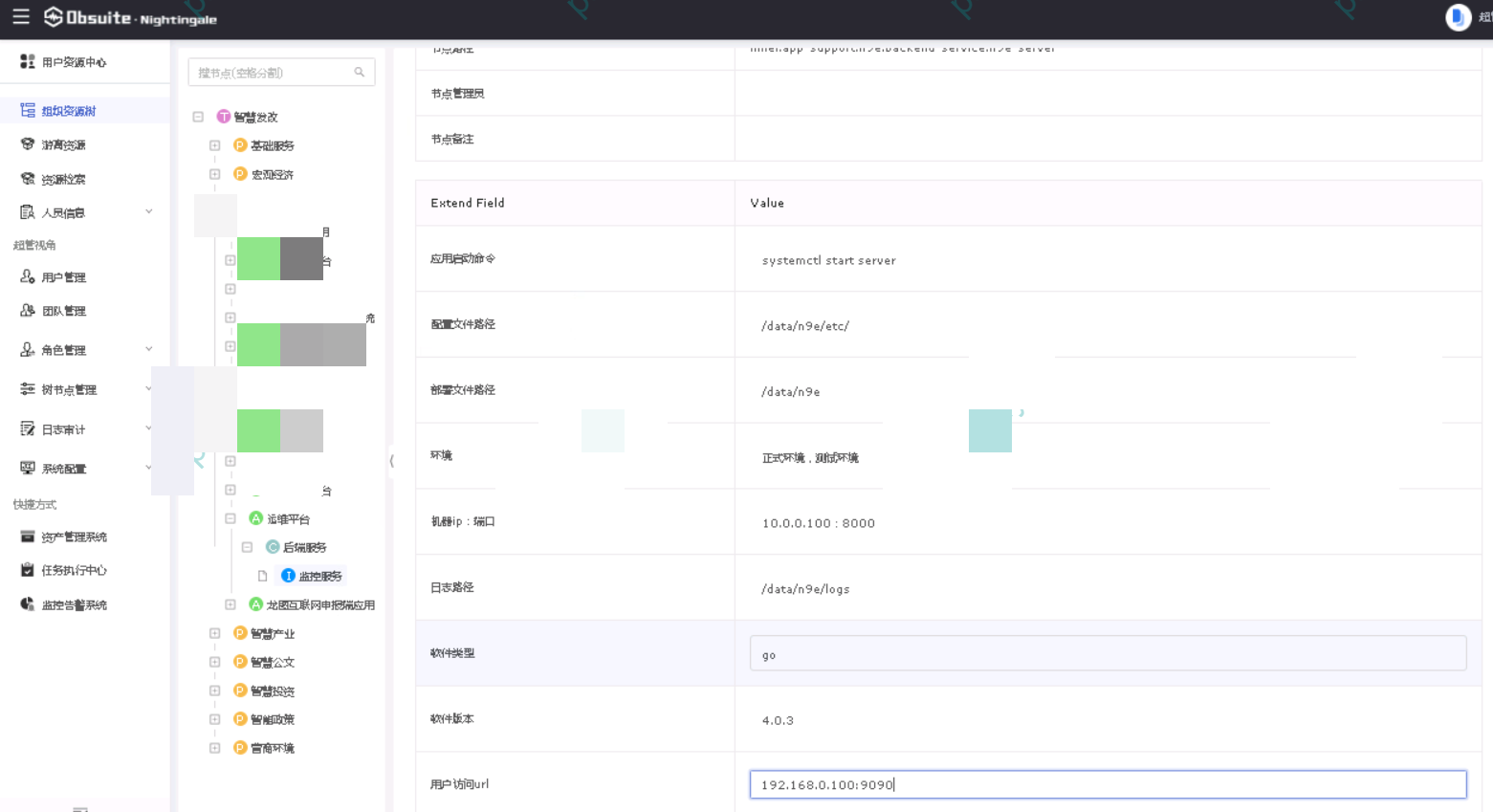
-子项目名 --项目（project）

-应用名 --应用（app）

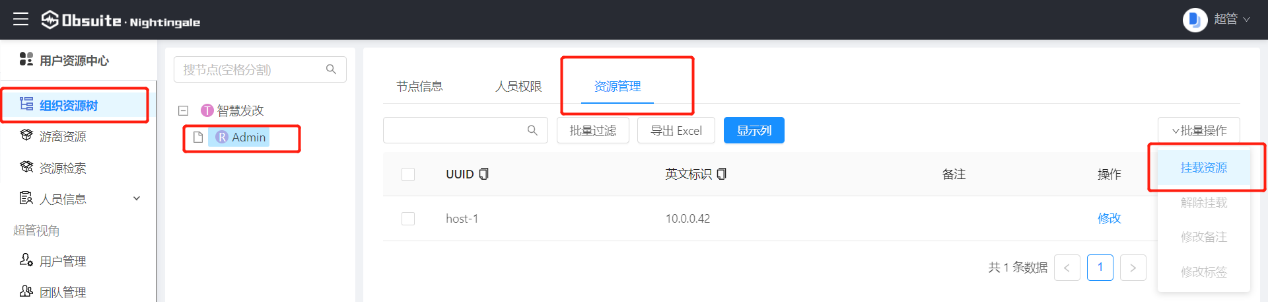
-后端服务 --集群（cluster）

-后端服务名称 --实例（instance）此节点需设置为叶子节点模式

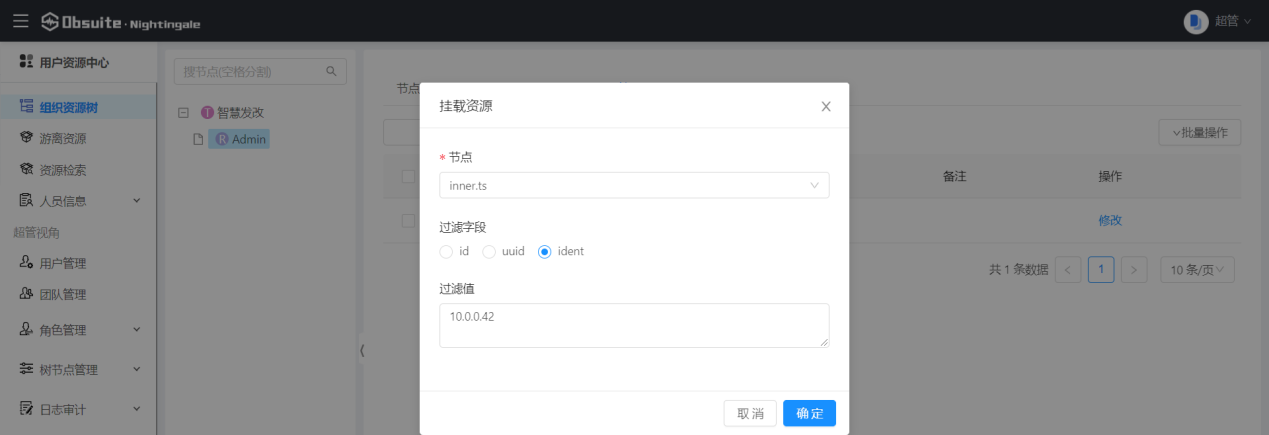
服务树样例图：



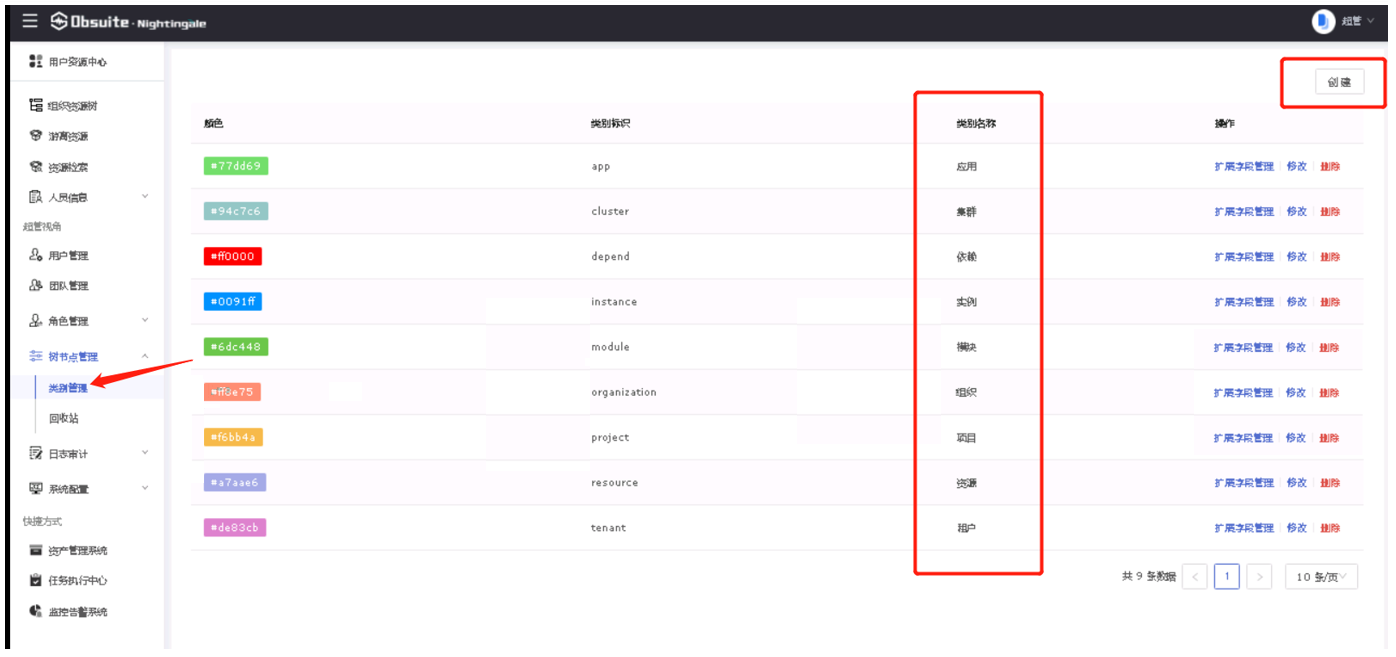
服务树节点挂载 用户资源中心-组织资源树-叶子节点-资源管理-批量操作-挂载资源



点击挂载资源后，进入以下页面



叶子节点扩展信息填写前需要在 用户资源中心-树节点管理-类别管理 中新建需要的信息

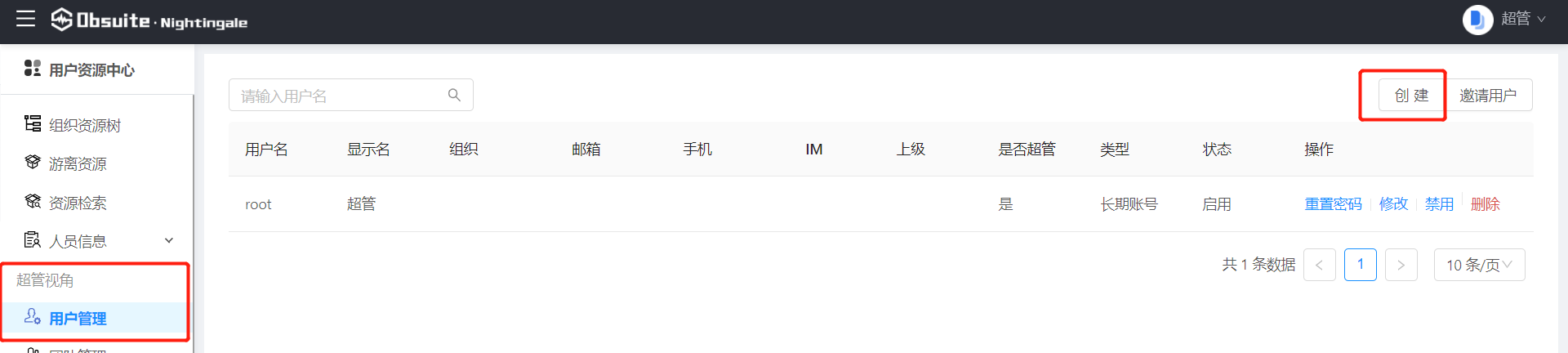


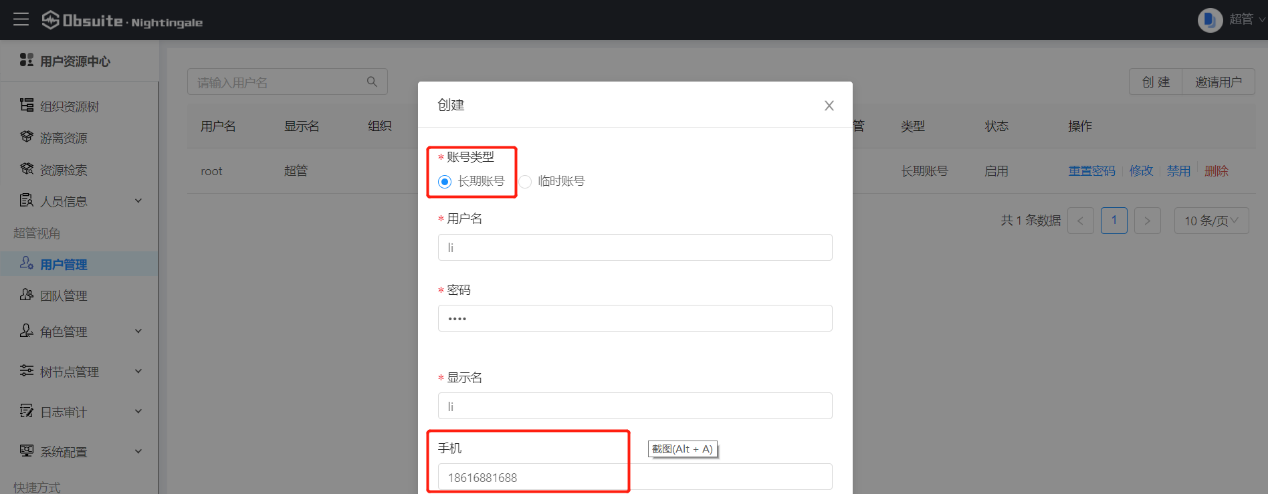
点击 实例-扩展字段管理 进入以下页面并进行添加配置



## 、用户管理、团队管理

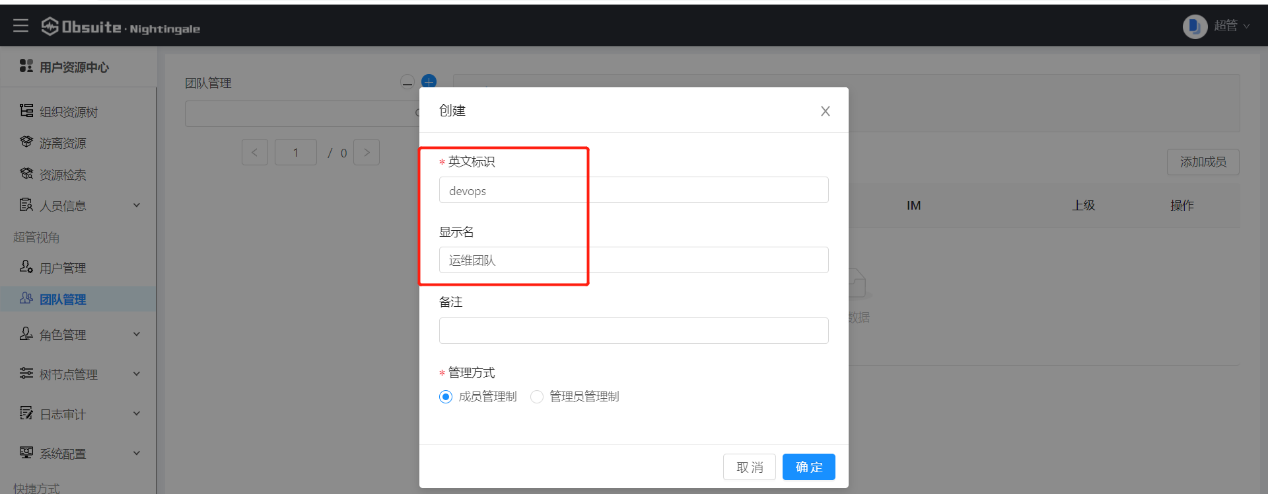
创建用户





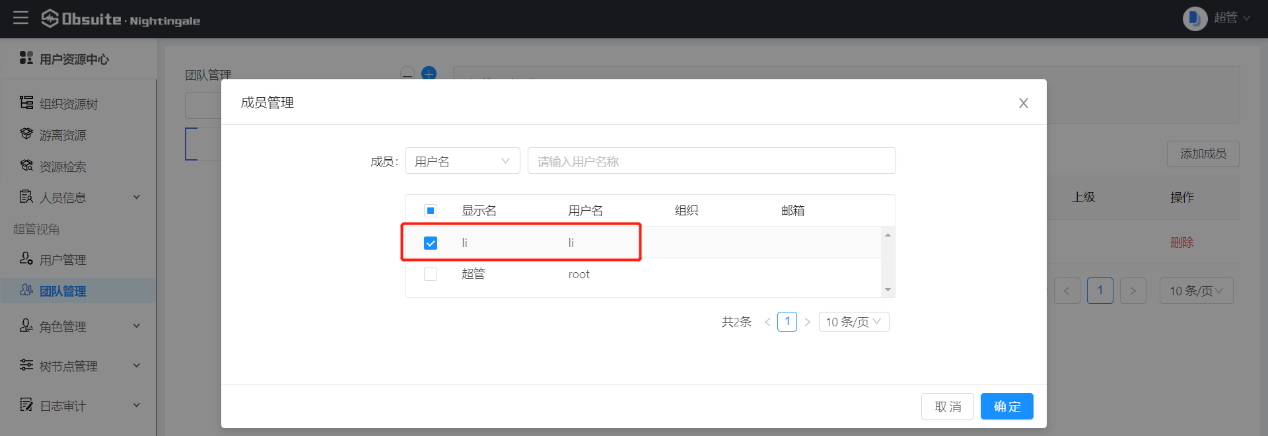
创建团队，并添加用户进入团队





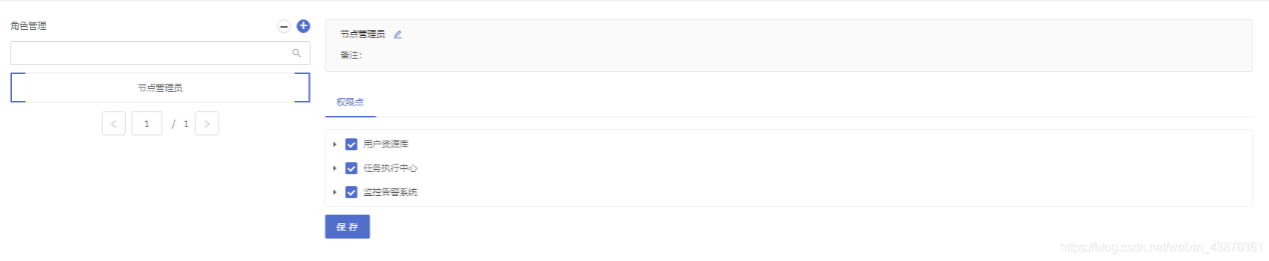
添加用户进入团队





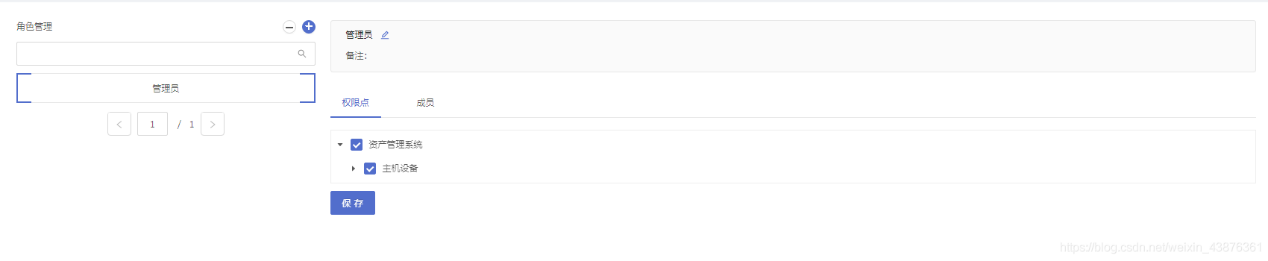
## 、角色管理（用户权限）：资源角色和页面角色

资源角色：主要是针对各节点来进行管理，设置好资源角色权限后，就可以在具体节点挂载用户时选择。例如，A用户负责夜莺集群的运维，那就可以直接把用户挂载在夜莺的节点下即可；





页面权限：页面权限主要是给资产管理页面的相关权限；

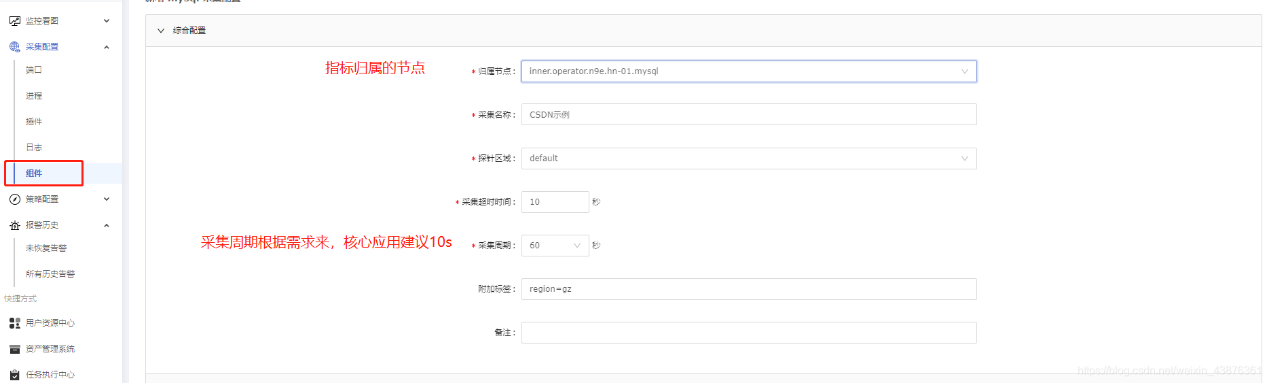


## 、采集中间件

夜使用Prober采集

部署好Prober以后，只需要在页面上进行配置即可；

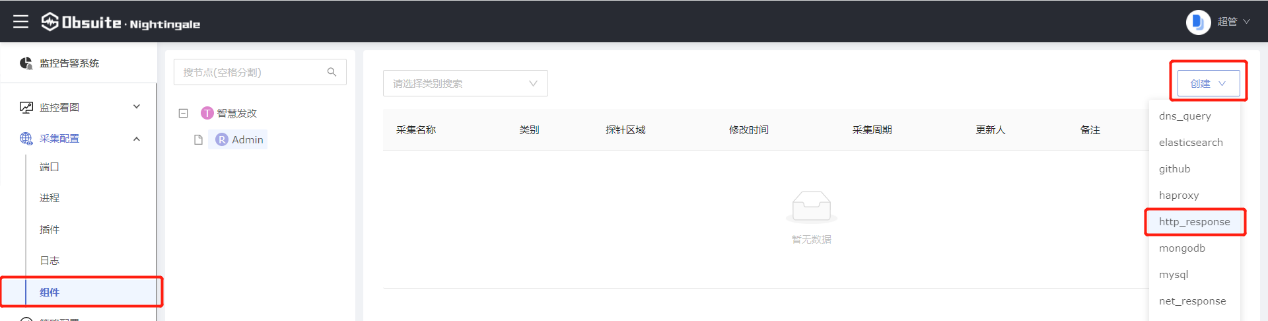
监控msyql：

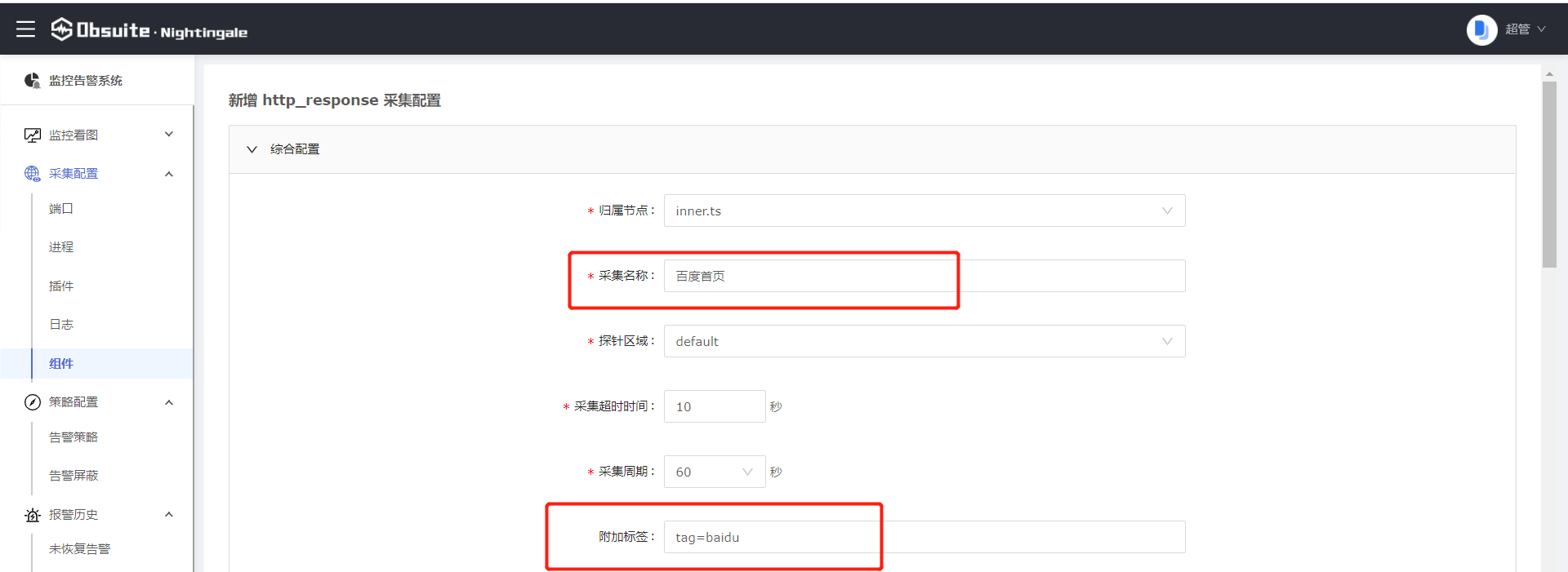




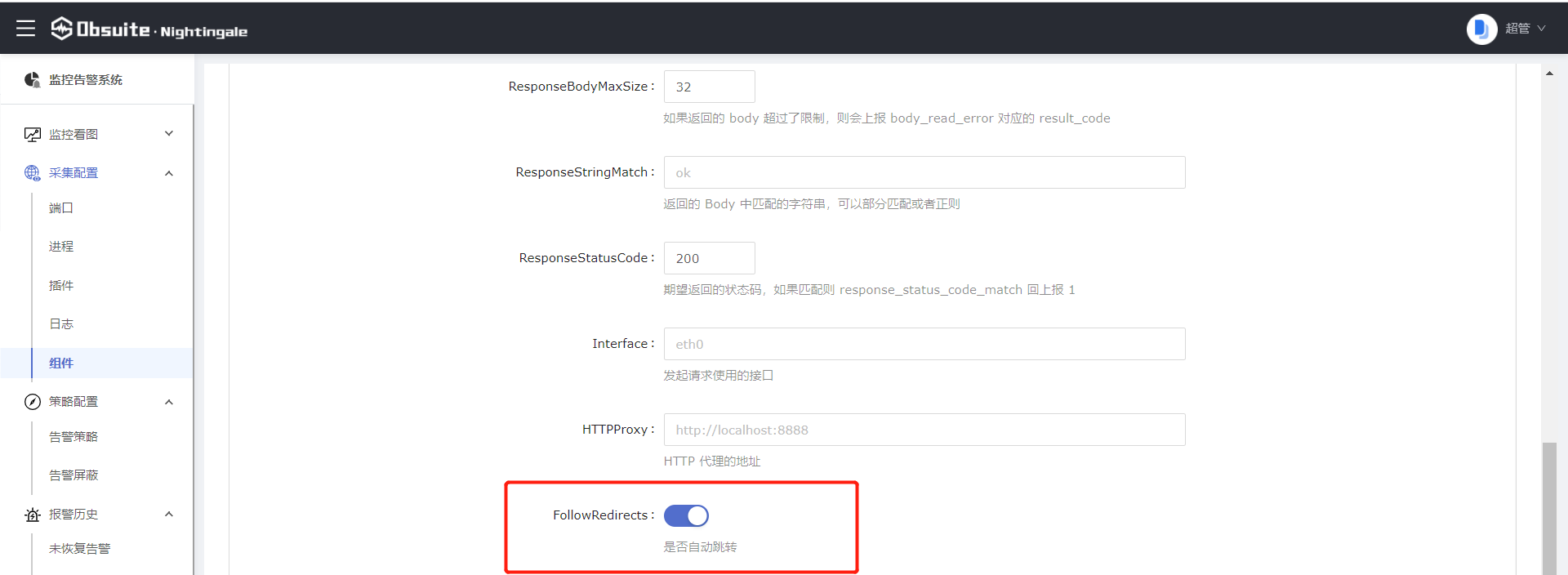
监控url返回码

注意：只需要填写红框中的内容



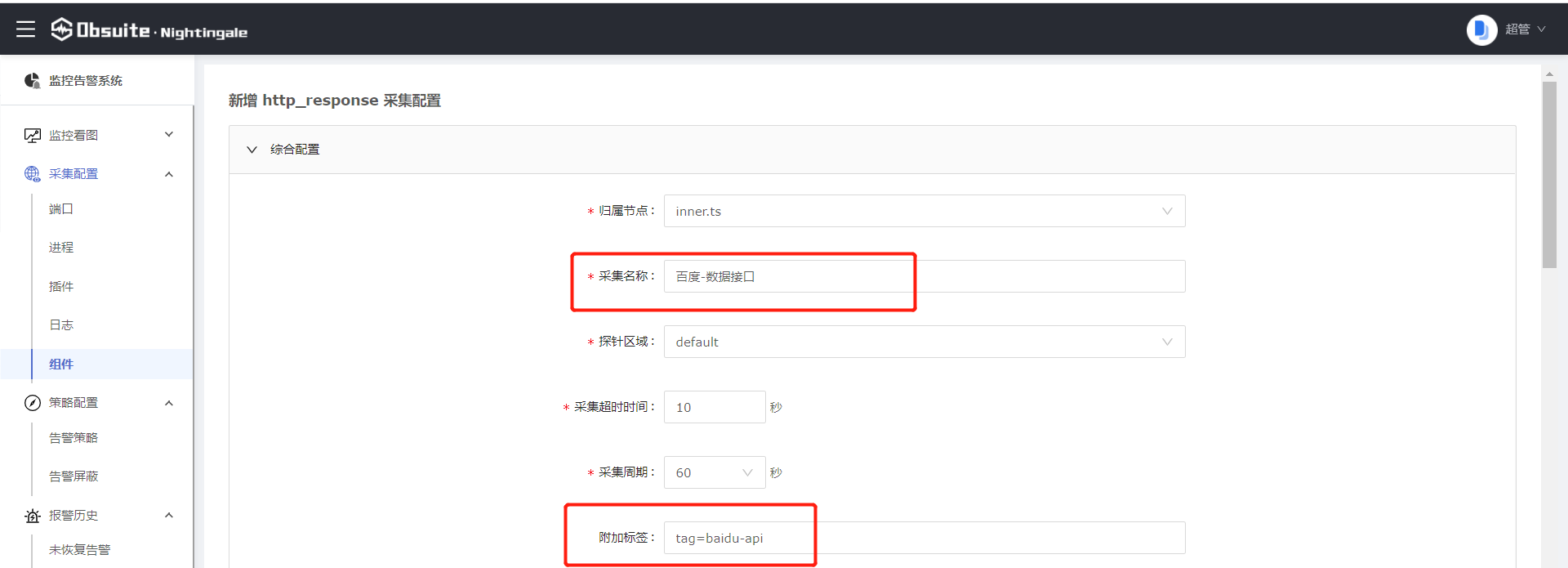




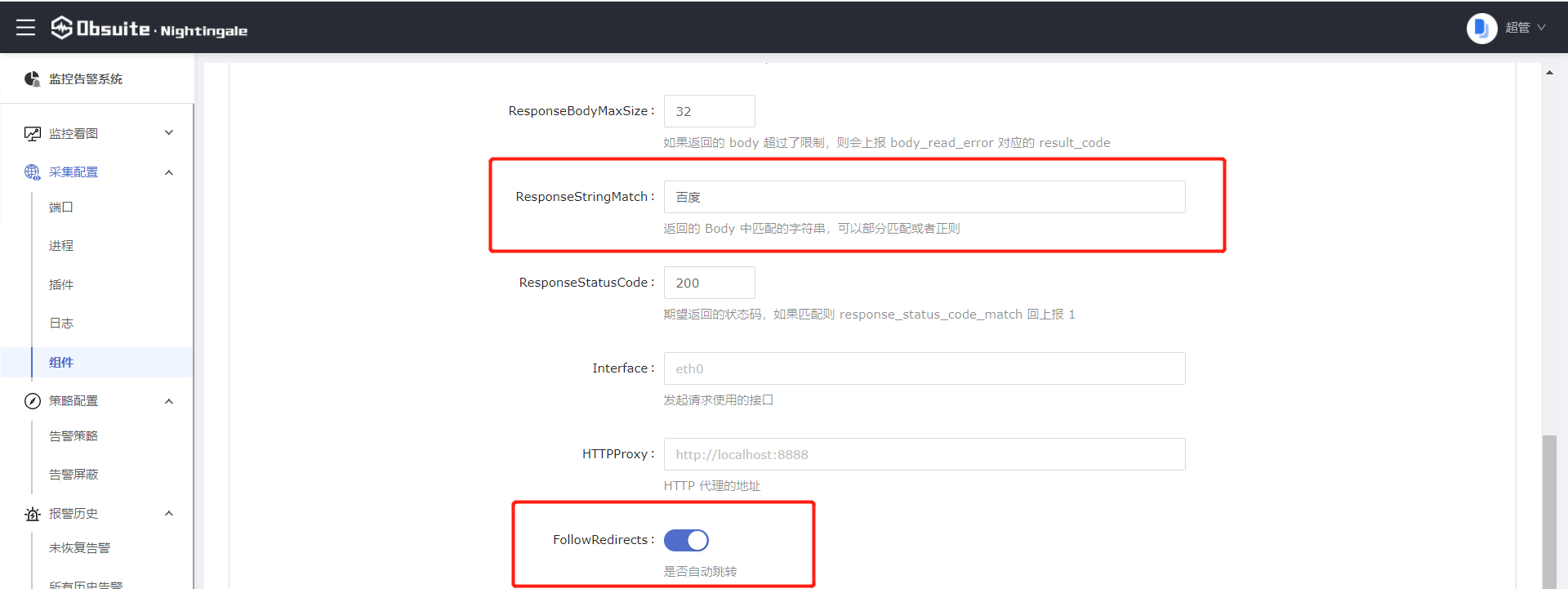


监控数据接口是否有关键字返回

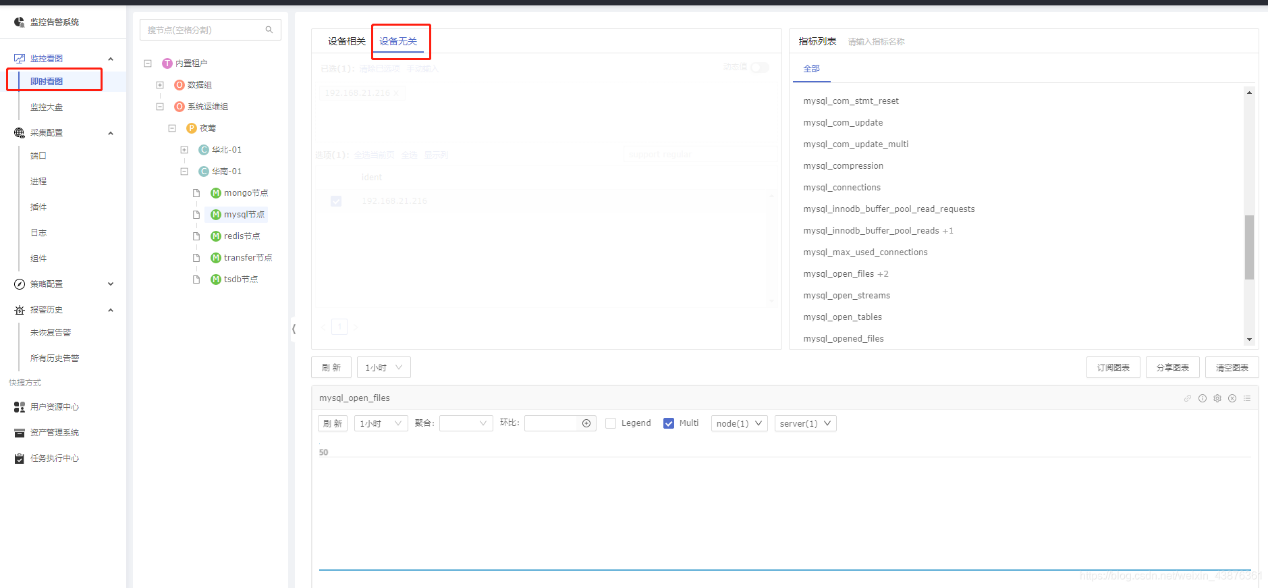
注意：操作与监控url一样，只需添加数据接口监控字段







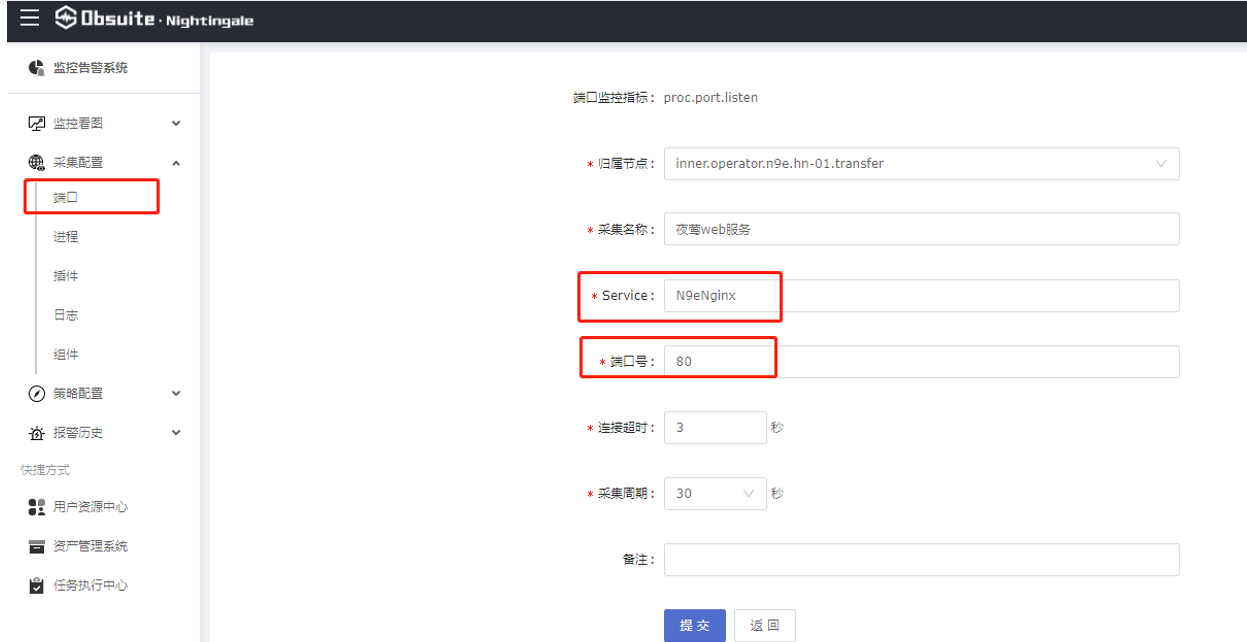
通常配置完根据你的采集周期，大概等个1-2min就可以看到指标了，这个指标位于节点下的【设备无关】里，如果长时间没有指标出现，可以重启下prober组件；



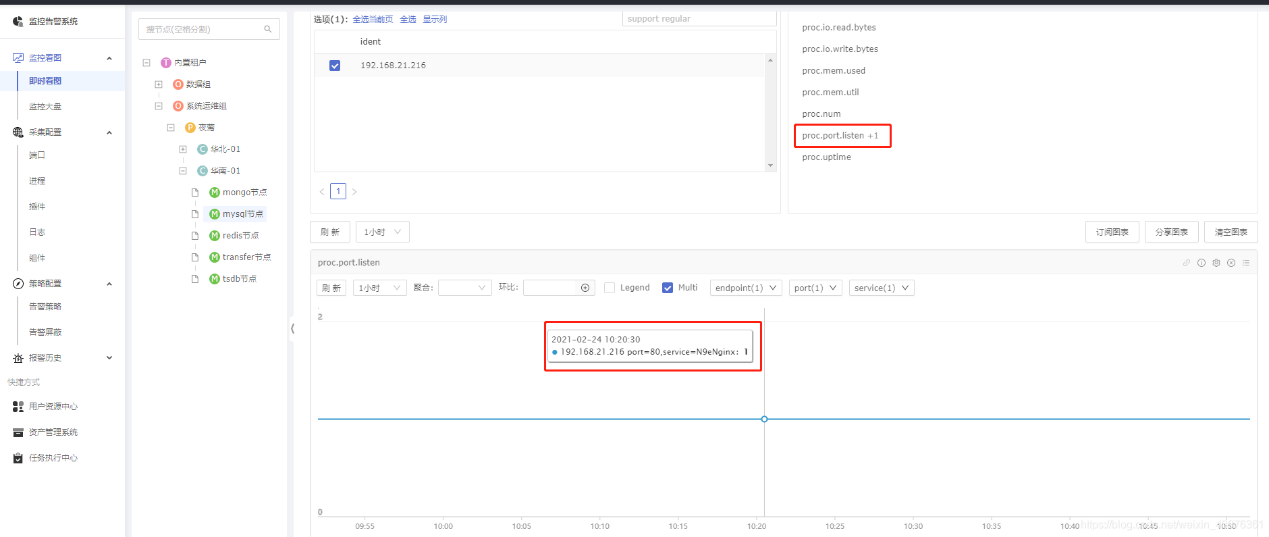
使用prober采集的指标，可以在夜莺的目录下etc/plugin的各.yml文件里查看，由于telegraf采集的指标较多，所以Prober组件实际上是使用了白名单上报的方式，可以自行添加白名单，或者切换成all模式上报；

## 、采集端口

Service是后面会作为tag上报

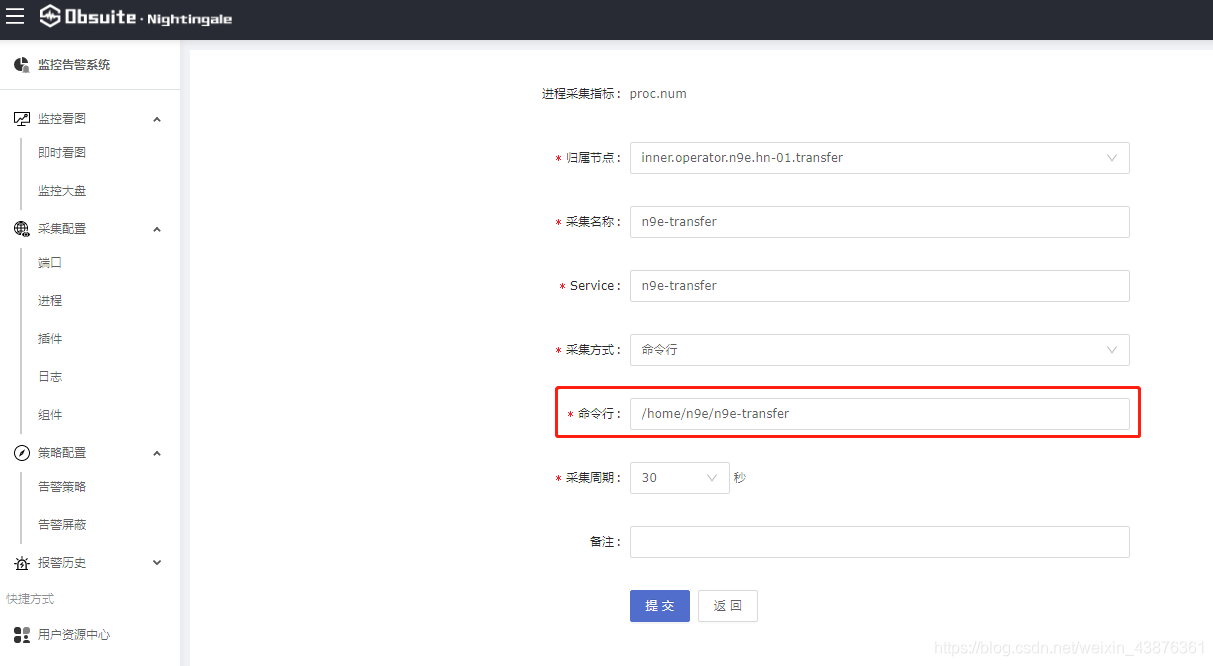


指标查看，指标是位于【归属节点】下的，【进程】内proc.port.listen指标下；注意，如果一个节点下有采集多个端口，监控信息都会汇聚到一条指标下，然后根据tag来区分，也就是上面的【Service】和【端口号】；

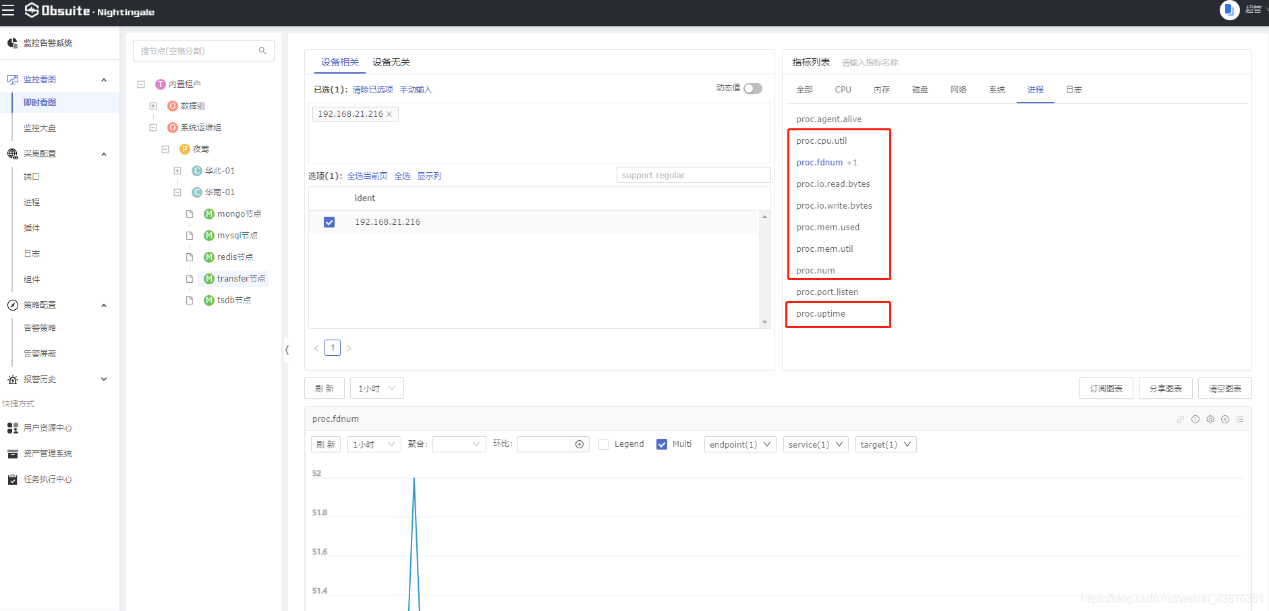


## 、进程采集

进程采集支持命令行和进程名，主要是为了进程重名下的区分



采集策略设置好以后，等待大概2-3s后，可以在【进程】下看到下图红框内新增的指标，夜莺支持采集进程的具体cpu, mem等指标。（如果一个节点下配置了采集多个进程，则不同进程通过tag来区分）



## 、日志采集

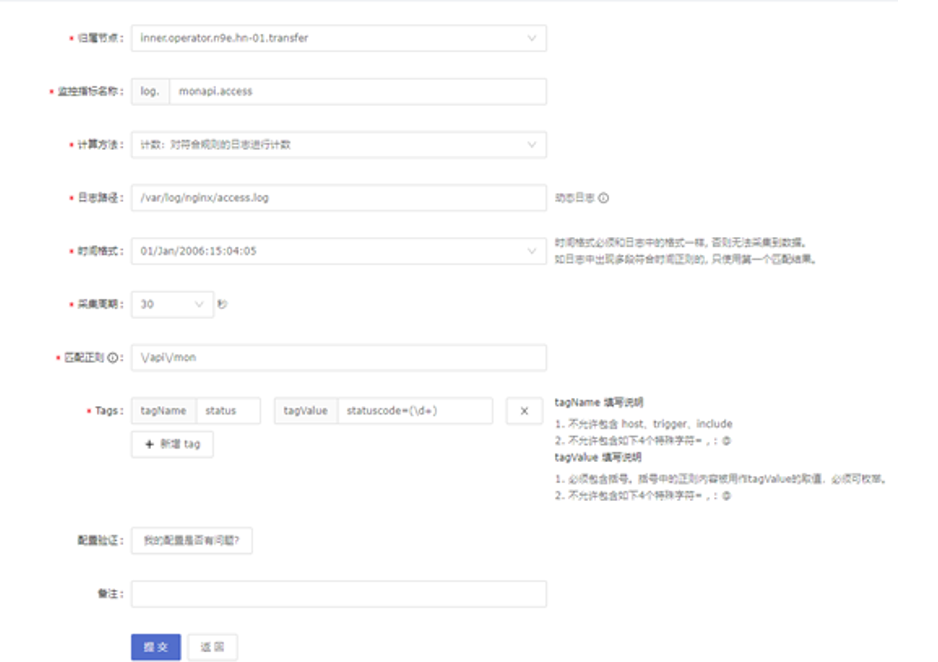
夜1，确认需要采集日志的相关信息；

–日志路径：（示例：/var/log/nginx/access.log）

–时间格式: （示例：DD/MM/YY:hh:mm:ss）

–正则匹配行 （示例：/api/mon，指的是匹配到/api/mon这一行）

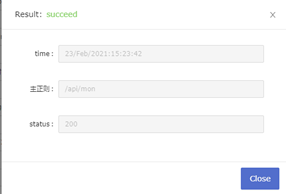
–指标名称 （示例：log.monapi.access）



(tagvalue指的是从/api/mon这一行里提取对应的tag出来使用，示例里是提取了请求的状态码作为tag来显示，注意采集周期)

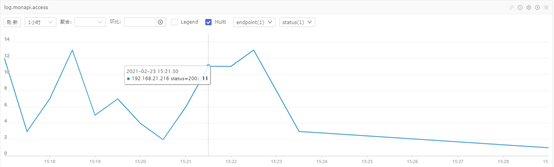
2，验证正则是否匹配

写好以后，可以复制日志行出来配置验证。



3，查看指标

设置完成后，等待大概1~2分钟，就可以在节点下看到设置的log.monapi.access（自定义不重复即可）指标出来了。



4，夜莺支持的汇总方式：

cnt avg sum max min 举例如下：

假设正则表达式配置为 Return Success : (\d+)s Used

某一个周期内日志滚动：

2017/12/01 12:12:01 Return Success : 1s Used

2017/12/01 12:12:02 Return Success : 2s Used

2017/12/01 12:12:03 Return Success : 4s Used

2017/12/01 12:12:04 Return Success : 2s Used

2017/12/01 12:12:05 Return Success : 1s Used

首先，根据正则获取到括号内的值：1、2、4、2、1 接下来，

根据不同的计算方式，会得到不同的结果：

avg : (1 + 2 + 4 + 2 + 1) / 5 = 2

cnt : 5 sum : (1 + 2 + 4 + 2 + 1) = 10

max : Max(1, 2, 4, 2, 1) = 4

min : Min(1, 2, 4, 2, 1) = 1

## 、告警策略

Nightingale的告警策略与Open-Falcon的配置有很大区别。首先取消了策略模板的机制，每一条策略都可以单独配置告警接收人，其次，策略可以直接绑定到服务树节点上，节点下的所有机器都会继承生效，另外还增加了一些字段，下面挨个字段解释：

策略名称：描述这条策略的作用，比如“CPU利用率超过85%”

生效节点：关联的服务树节点，节点下所有机器都会应用这条策略

排除节点：生效节点下面的部分子节点可能较为特殊需要排除，可以用此配置解决

报警级别：分三级，P1最严重，报警之后事件通过所有报警通道推送，P3不严重，只用部分通道

统计周期：判断报警的时候使用最近多长时间以内的数据

触发条件：支持与条件，即两个条件都满足才报警

Tag过滤：可以配置只生效监控指标的部分tag，或者排除部分tag，比如disk.io.util只监控sda

执行动作：配置报警收敛策略和报警接收人，也支持配置回调，与自动化逻辑打通

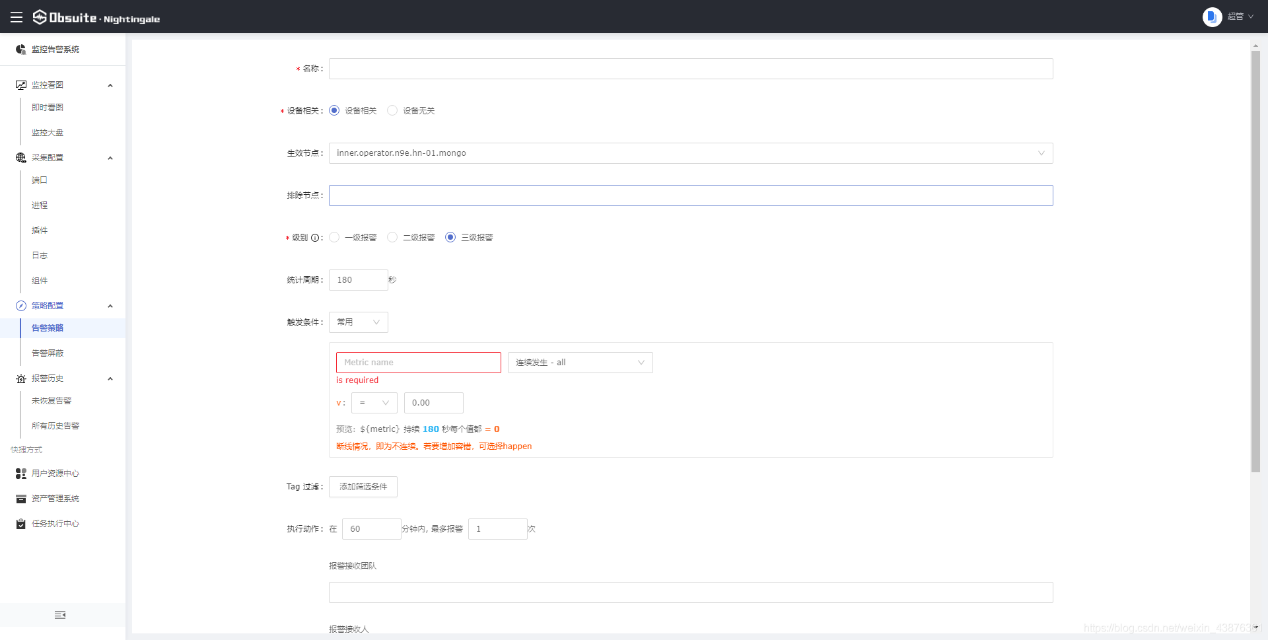
留观时长：告警恢复后持续观察多少秒，称为留观时长，未再触发阈值才发送恢复通知

静默恢复：即只发送告警消息，不发送恢复通知，默认会发送，即不开启静默恢复

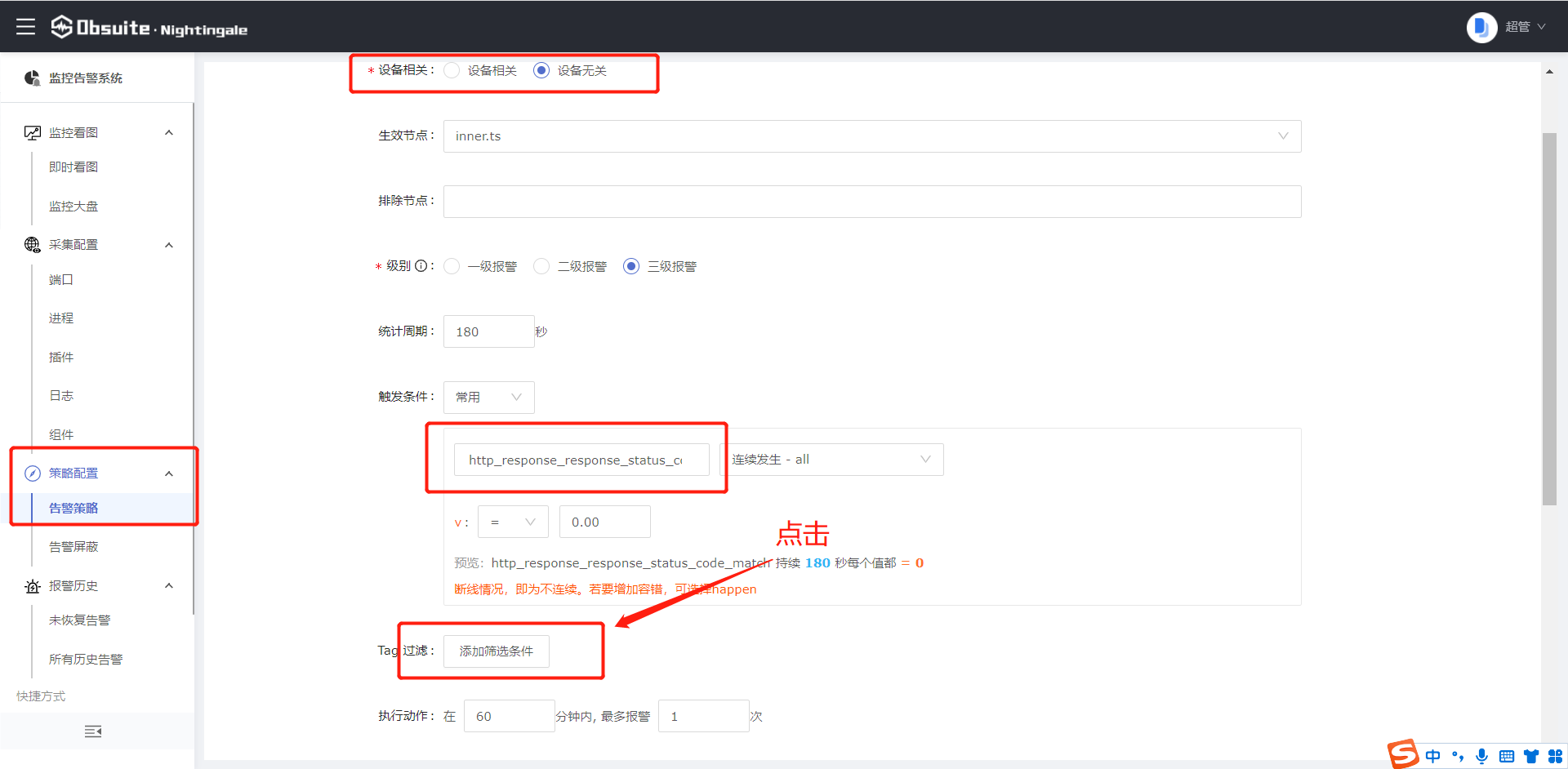
生效时间：即策略生效时间，默认7\*24生效，可以配置只生效部分时间段

配置页面如下

注意：告警接收这里优先设置团队接收

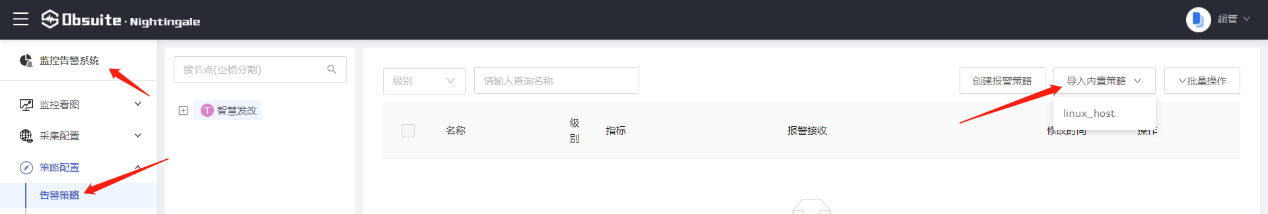


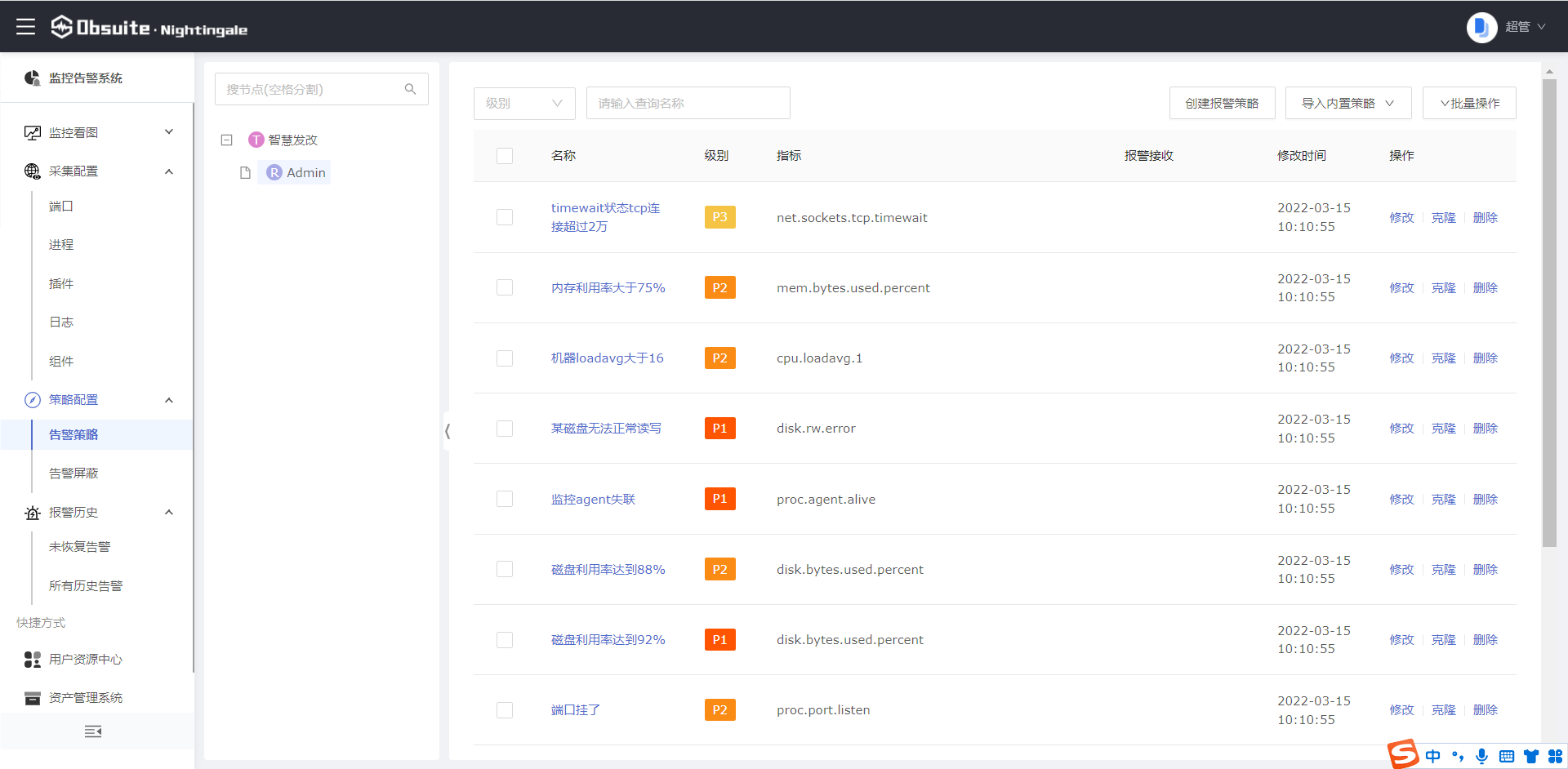
例如端口，进程，url等有打tag的监控指标需要添加tag过滤



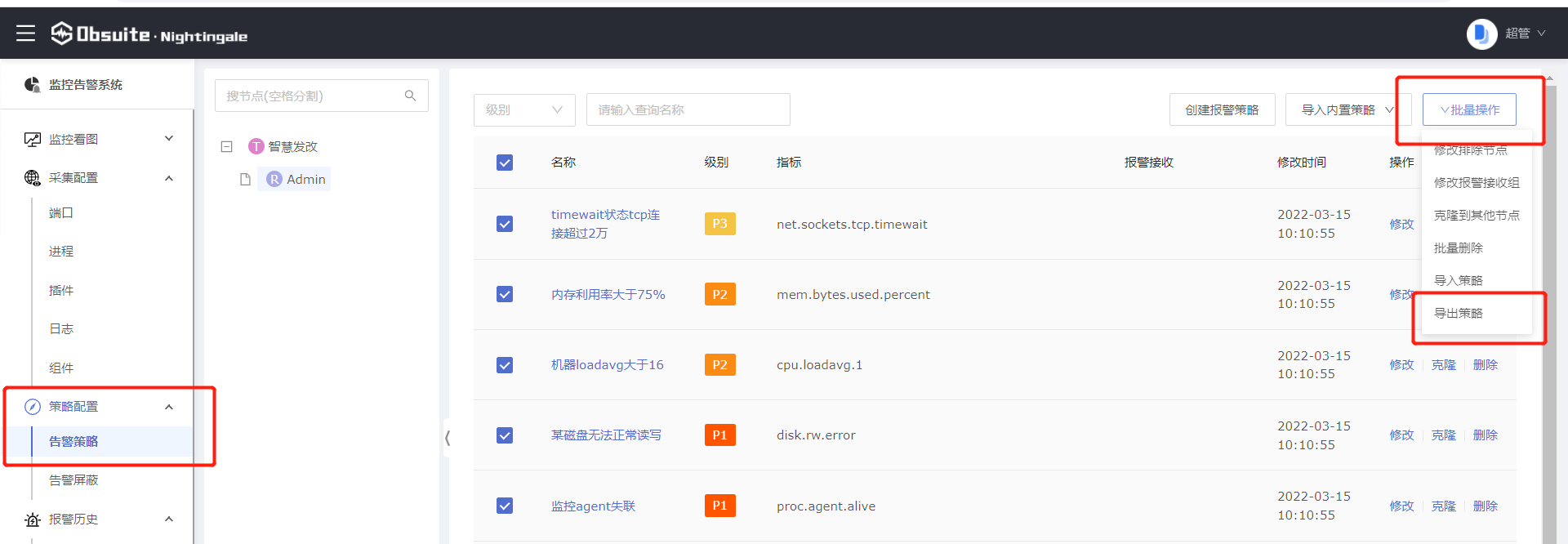


策略配置页面支持导入，这里整理了一些常见策略，可以一键导入，然后批量修改一下报警接收人就可以用起来了





告警策略可以批量导出为json格式



Json内容可以直接拷贝粘贴使用



# 排错

## 、n9e-v4版本常见安装问题

* 1. 系统安装好了，也能看到指标，但是点击指标看不到图

很可能是系统时间没有校准，检查ntp服务器是否生效

* 1. server模块进程虽然在，但是server的两个端口都没有在监听

这说明server模块没有正常启动，可以查看logs/server/stdout.log查看是否有一些有用的信息，大概率是m3没有安装好，或者m3没有用那个curl指令初始化。另外如果用的pve，可能会因为指令集导致m3进程起来，过一会就挂了，所以不要用pve

* 1. 设备管理的列表里缺少了本机设备

说明agentd没有成功注册到server，需要检查agentd和server的日志来排查