Hyperbase监控告警系统

安装文件

- jmx exporter: **jmx_prometheus_javaagent-0.11.0.jar**
- node exporter: **node_exporter-0.17.0.linux-amd64.tar.gz**
- prometheus: **prometheus-2.7.2.linux-amd64.tar.gz**
- alertmanager: **alertmanager-0.16.1.linux-amd64.tar.gz**
- grafana: **grafana-6.0.0.linux-amd64.tar.gz**

配置文件

- prometheus.yml
- hyperbase_rules.yml
- hyperbase-dashboard.json

具体部署

jmx exporter部署

1. 在hyperbase配置文件夹**conf**下 (例如/etc/hyperbase1/conf)，存放jmx_prometheus_javaagent-0.11.0.jar，并新建空文件jmx_emp_conf.yml
2. 编辑 hbase-env.sh中的HBASE_MASTER_OPTS & HBASE_REGIONSERVER_OPTS。新增如下两行命令，分别指定master和regionserver暴露jmx属性的端口 (可根据需要更改)。(hyperbase conf path) 为hyperbase配置文件夹conf的路径。空jmx_emp_conf.yml暴露全部的jmx属性，可根据需要修改。

```
export HBASE_MASTER_OPTS="$HBASE_MASTER_OPTS -javaagent:(hyperbase conf
path)/jmx_prometheus_javaagent-0.11.0.jar=7070:(hyperbase conf
path)/hbase_emp_conf.yml"

export HBASE_REGIONSERVER_OPTS="$HBASE_REGIONSERVER_OPTS -javaagent:(hyperbase conf
path)/jmx_prometheus_javaagent-0.11.0.jar=7071:(hyperbase conf
path)/hbase_emp_conf.yml"
```

3. 重启hbase master与regionserver，即可使用 `curl localhost:7070(or 7071)/metrics` 查看到jmx exporter暴露的hbase jmx属性。也可在浏览器中输入 http://serverIP:port/metrics 查看

node exporter部署

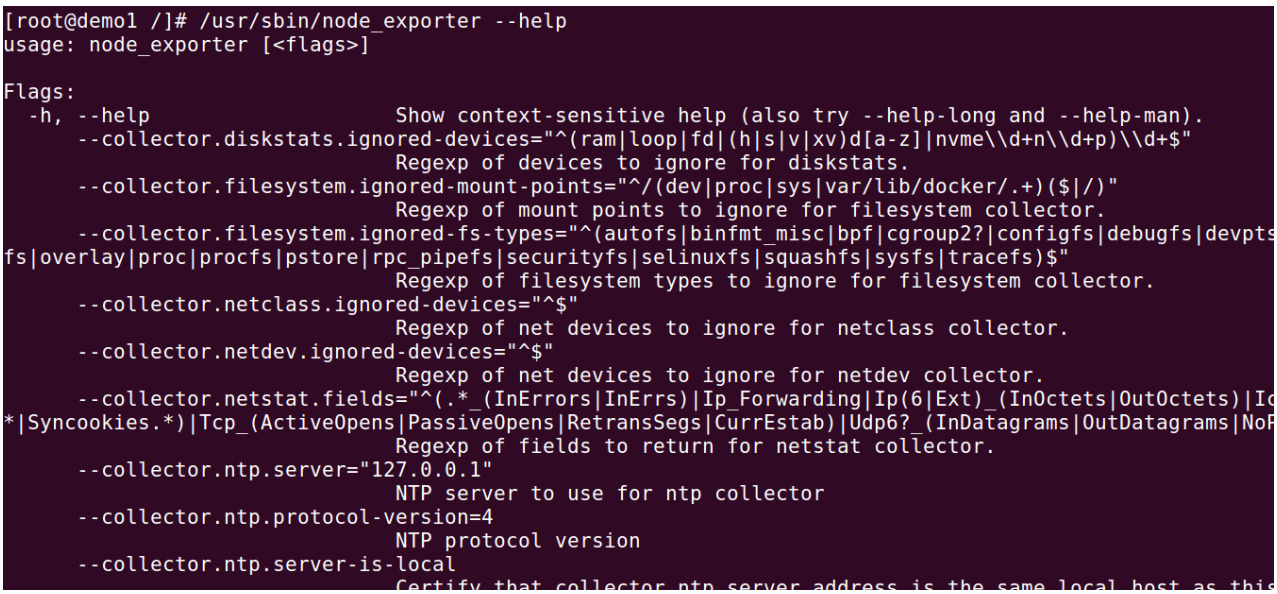
1. 在服务器上创建无特权node_exporter用户：`sudo useradd node_exporter -s /sbin/nologin`
2. 解压node_exporter-0.17.0.linux-amd64.tar.gz，将其下的node_exporter拷贝进/usr/sbin目录下
3. 创建systemd service文件/etc/systemd/system/node_exporter.service，内容为：

```
[Unit]
Description=Node Exporter

[Service]
User=node_exporter
EnvironmentFile=/etc/sysconfig/node_exporter
ExecStart=/usr/sbin/node_exporter $OPTIONS

[Install]
WantedBy=multi-user.target
```

4. 创建sysconfig文件/etc/sysconfig/node_exporter，内容为：

```
OPTIONS="--collector.textfile.directory /var/lib/node_exporter/textfile_collector"
```

5. 检测上述步骤是否正确，以终端运行`/usr/sbin/node_exporter --help`可见如下图为准。



6. 重新加载systemd配置:

```
sudo systemctl daemon-reload
sudo systemctl enable node_exporter
```

7. 后台无挂起启动node_exporter服务，9101为建议端口，可自行根据需要更改：

```
nohup node_exporter --web.listen-address=":9101" > /var/log/node_exporter/logs 2>&1 &
```

其中，/var/log/node_exporter存放node_exporter运行日志

8. 运行命令`curl localhost:9101/metrics`即可看到系统metrics信息，同样可在浏览器中键入url观察

Prometheus部署

1. 在服务器上创建无特权prometheus用户：`sudo useradd prometheus -s /sbin/nologin`

2. 创建两个文件夹，/etc/prometheus与/var/lib/prometheus，前者存放prometheus配置文件，后者存放prometheus运行数据。将新目录的用户和组所有权设置为prometheus用户

```
sudo chown prometheus:prometheus /etc/prometheus
sudo chown prometheus:prometheus /var/lib/prometheus
```

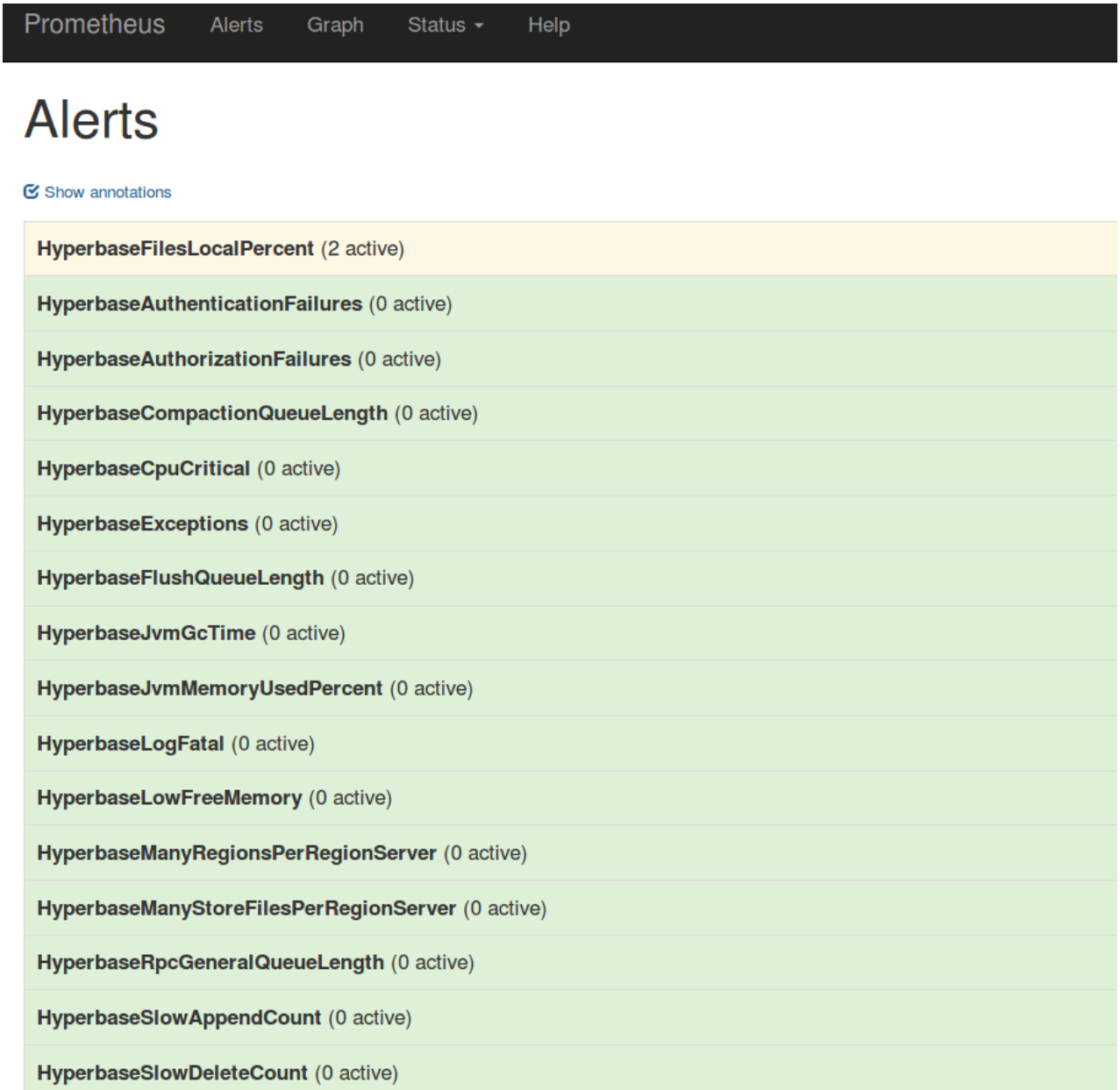
3. 解压prometheus-2.7.2.linux-amd64.tar.gz，将其下的prometheus和promtool文件拷贝进/usr/sbin目录下，并将consoles和console_libraries目录复制到/etc/prometheus目录
4. 将目录上的用户和组所有权设置为prometheus用户。使用该`-R`标志将确保对目录内的文件设置所有权。

```
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries
```

5. 在/etc/prometheus目录下添加prometheus.yml配置文件
6. **prometheus.yml修改说明**：
    1. 修改alertmanager的配置，把172.26.0.37:9093改成对应的alertmanager的主机和端口（alertmanager配置见后面）
    2. rule_files部分配置的是使用哪些告警规则文件，这里可以不用修改，详细指标请参考：hyperbase监控告警指标
    3. 修改scrape_configs，将每个job_names下对应的targets，如172.26.0.37:7070 改成对应jmx exporter或node exporter进程所在的主机和端口，然后还可以为每个job单独添加 scrape_interval（prometheus获取search metrics的频率）和 evaluation_interval（prometheus检查告警规则的频率），否则使用的是global下的scrape_interval和evaluation_interval
7. 后台无挂起的启动prometheus，可在9090端口(默认)查看prometheus拉取的信息：

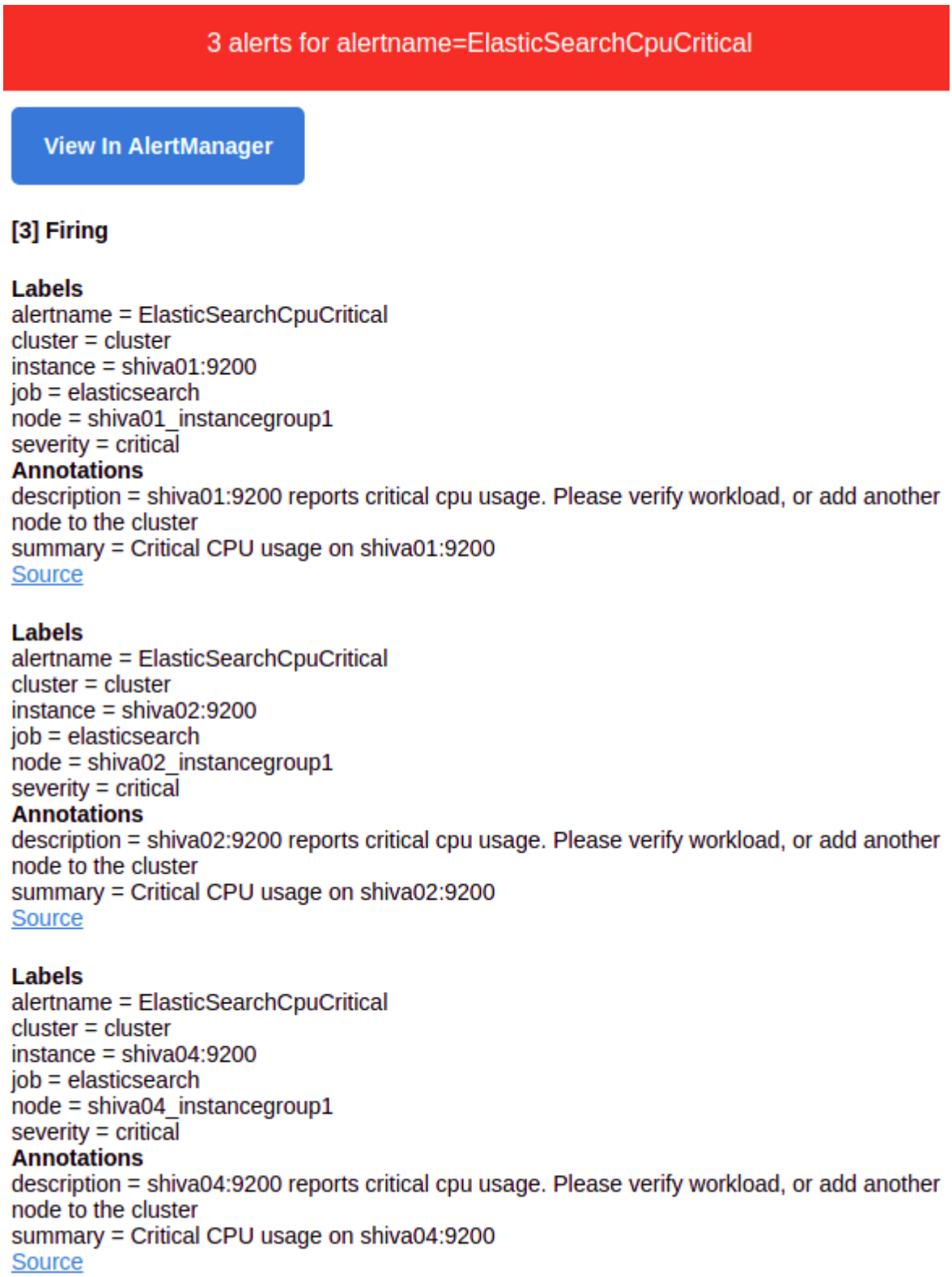
```
nohup prometheus --config.file=/etc/prometheus/prometheus.yml >
/var/log/prometheus/logs 2>&1 &
```

   /var/log/prometheus目录下存放prometheus运行日志
8. 添加告警规则文件hyperbase_rules.yml，与prometheus.yml集成，规范prometheus以怎样的频率拉取哪些进程的数据，以怎样地规则告警。prometheus网页端上点击alerts可查看告警信息。



Alertmanager部署

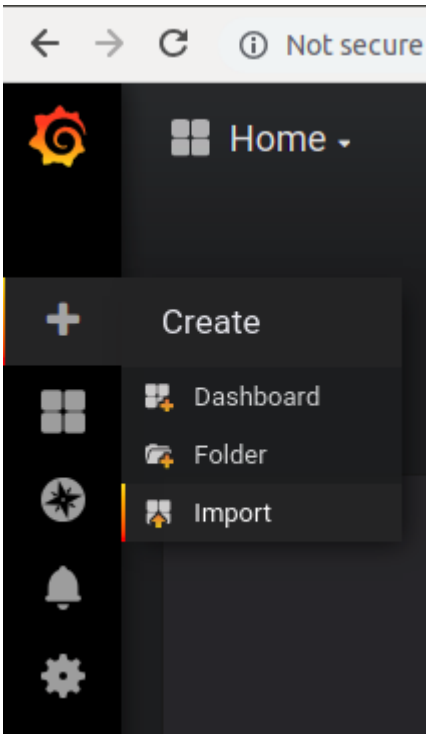
1. 解压alertmanager-0.16.1.linux-amd64.tar.gz，进入alertmanager-0.16.1.linux-amd64文件夹
2. 修改alertmanager.yml里的email_configs配置项，用来接收告警邮件。需要把 from，to，auth_username，auth_identity，auth_password都改成对应的transwarp邮箱地址和密码。如果不想用transwarp邮箱，那么还需要修改smarthost和hello
3. 修改完配置后，执行类似 nohup ./alertmanager > logs 2>&1 & 的命令，在后台启动alertmanager
4. 启动如果成功，可以在浏览器里访问9093端口打开alertmanager界面；如果不成功，可以看logs文件看报错原因
5. 目前alertmanager只配置了发送邮件的动作，如还需别的动作可参考官方文档。邮箱中收到的告警邮件样例如下图：



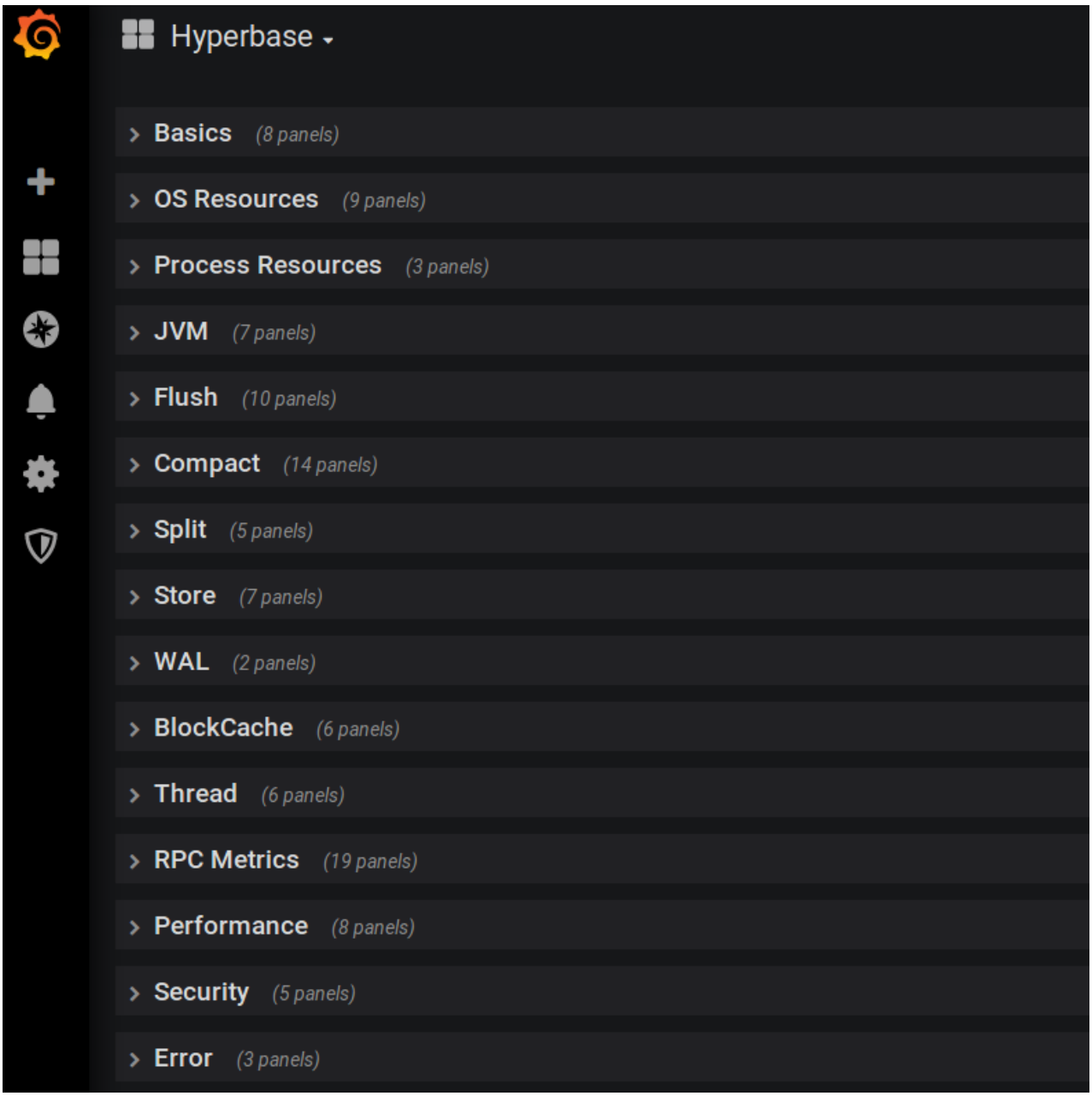
Grafana Dashboard配置

1. 解压grafana-6.0.0.linux-amd64.tar.gz，进入grafana-6.0.0文件夹
2. 进入bin，执行类似 nohup ./grafana-server web > logs 2>&1 & 的命令，在后台启动grafana
3. 启动如果成功，可以在浏览器里访问3000端口打开grafana界面，默认用户名密码：admin/admin；如果不成功，可以看logs文件看报错原因

4. 启动成功后，选择 "Add data source" -> "Prometheus"，在页面上填上对应的prometheus配置项（其中Name必须填上Prometheus，否则会影响下一步；还可以指定Scrape interval，配置grafana去prometheus获取metrics的频率），配置完后点 Save & Test 会提示是否成功
5. 步骤4成功后，再选择左上角的 "Create" -> "Import"（如下图），将dashboard配置文件hyperbase-dashboard.json文件导入，生成dashboard



6. 导入成功后，可以看到如下的dashboard



监控和告警指标

https://www.zybuluo.com/cyfcooler/note/1494848