**基础监控报警表达式参考：**

**CPU使用率**：**100 - (avg by (instance) (irate(node\_cpu{instance="xxx", mode="idle"}[5m])) \* 100)**

**CPU 各 mode 占比率：avg by (instance, mode) (irate(node\_cpu{instance="xxx"}[5m])) \* 100**

**机器平均负载：node\_load1{instance="xxx"} // 1分钟负载**

**node\_load5{instance="xxx"} // 5分钟负载**

**node\_load15{instance="xxx"} // 15分钟负载**

**内存使用率：100 - ((node\_memory\_MemFree{instance="xxx"}+node\_memory\_Cached{instance="xxx"}+node\_memory\_Buffers{instance="xxx"})/node\_memory\_MemTotal) \* 100**

**磁盘使用率：**

**100 - node\_filesystem\_free{instance="xxx",fstype!~"rootfs|selinuxfs|autofs|rpc\_pipefs|tmpfs|udev|none|devpts|sysfs|debugfs|fuse.\*"}/node\_filesystem\_size{instance="xxx",fstype!~"rootfs|selinuxfs|autofs|rpc\_pipefs|tmpfs|udev|none|devpts|sysfs|debugfs|fuse.\*"} \* 100**

**网络io**：// 上线带宽**sum by (instance) (irate(node\_network\_receive\_bytes{instance="xxx"device!~"bond.\*?|lo"}[5m])/128)**// 下行带宽**sum by (instance) (irate(node\_network\_transmit\_bytes{instance="xxx",device!~"bond.\*?|lo"}[5m])/128)**

**网卡出入包**：// 入包量**sum by (instance) (rate(node\_network\_receive\_bytes{instance="xxx",device!="lo"}[5m]))**// 出包量**sum by (instance) (rate(node\_network\_transmit\_bytes{instance="xxx",device!="lo"}[5m]))**

**Rule文件格式：**

groups:

- name: monitor

rules:

- alert: xx非200告警

annotations:

description: 域名{{ $labels.host}}出现大量:{{ $labels.status}}状态码异常,当前值{{$value}}

summary: 域名{{ $labels.host}}出现大量:{{ $labels.status}}状态码异常

expr: sum(irate(nginx\_http\_requests\_total{host=~"xxx",status!="200"}[1m]))

by (host,status) >30

for: 1m

labels:

project: monitor

severity: disaster

- alert: xxx非200告警

annotations:

description: 域名{{ $labels.host}}出现大量:{{ $labels.status}}状态码异常,当前值{{$value}}

summary: 域名{{ $labels.host}}出现大量:{{ $labels.status}}状态码异常

expr: sum(irate(nginx\_http\_requests\_total{host=~"xxxx",status!="200"}[1m]))

by (host,status) >30

for: 1m

labels:

project: monitor

severity: high

alertmanager集群模式：