

РЕД
СЛЁРМ

+



Southbridge

Проактивный мониторинг: Monit

slurm.io



Евгений Терешков

Инженер компании Southbridge

План

- Проблематика
- Область применения
- Устройство
- Настройка и эксплуатация

Проблематика



Было такое?

- Образовался перезапуска апача в кроне?
- Ночью OOM убил mysqld?
- SIGSEGV в закрытом бинарнике регулярно?
- Костыли, разброд, шатание, печаль, боль

Варианты решения

- Разные скрипты + крон
- `systemd`?
- Супервизоры

Что делает/не делает monit?

- Проактивный мониторинг без связи с центром
- Оперативный сбор информации
- Интеграционные тесты
- Интеграция с фабрикой
- Не сохраняет долгосрочную статистику
- Не умеет сложных формул проверки
- Не рисует графиков на заказ
- Не рассчитан на множество хостов

Устройство




```
[root@localhost /etc]# egrep -iv '^[ ]*(#|$)' monitrc
set idfile /var/monit/id
set statefile /var/monit/state
include /etc/monit.d/*
[root@localhost /etc]# tree monit.d/
```

monit.d/

```
├── alerts
├── crond
├── daemon
├── denyhosts
├── logging
├── messages
├── mmonit
├── ntpd
├── oom-messages
├── postfix
├── rsyslogd
├── system
├── template
│   ├── oom-messages
│   └── system
└── zabbix
```

1 directory, 15 files

Локальный оперативный МОНИТОРИНГ

Пришел ООМ, убил ~~кого-то~~ ~~попале~~ агент мониторинга:
МОНИТОРИНГ КОНЧИЛСЯ.

```
[root@localhost /etc/monit.d]# cat zabbix
```

```
check process zabbix with pidfile /var/run/zabbix/zabbix_agentd.pid
```

```
start program = "/bin/systemctl start zabbix-agent"
```

```
stop program = "/bin/systemctl stop zabbix-agent"  
if 3 restarts within 6 cycles then alert
```

Было: сервер без мониторинга
до ручного вмешательства

Стало: никто ничего не
заметил (но тикет про ООМ
заведён, см. далее)

Оперативный сбор информации

Ночью был LA over 9000, почему?

Собираем полезную информацию, шлём в стандартном виде на общую точку входа (+ ссылка на КБ внутри)

```
[root@localhost /etc/monit.d]# cat system
check system $HOST
    if loadavg (5min) > 5 for 2 cycles then exec "/srv/southbridge/bin/docker-highload-report.sh"
    if loadavg (5min) > 5 for 4 cycles then exec "/bin/bash -c '/usr/bin/monit unmonitor $HOST && /bin/sleep 1800
&& /usr/bin/monit monitor $HOST'"
```

Было: неясно, из-за чего была нагрузка, нет оперативных данных

Стало: зачастую из дампа очевиден виновник (IP/SQL/GET/POST/контейнер)

Интеграционные тесты

Превышение количества файлов в каталоге для ext4: ничего не создать, хотя место/inode есть

```
[root@localhost /etc/monit.d]# grep index messages
```

```
if match 'Directory index full' then alert
```

```
if match 'Directory index full' for 2 cycles then exec "/bin/bash -c  
'/usr/bin/monit unmonitor messages && /bin/sleep 3600 && /usr/bin/monit monitor  
messages' "
```

Было: клиент жалуется на подземный стук, надо идти на сервер и всё посмотреть

Стало: из тикета с сообщением очевидна проблема (а из КБ — пути решения)

Интеграция с фабрикой

Что-то случилось – оповещаем админа. \$HOST используем для сортировки по проектам.

```
[root@localhost /etc/monit.d]# cat alerts
```

```
set mailserver monitmail.slurm.io with timeout 30 seconds
```

```
set mail-format { subject: $HOST monit - $EVENT $SERVICE }
```

```
set alert monit@monitmail.slurm.io but not on { instance
```

```
    pid
```

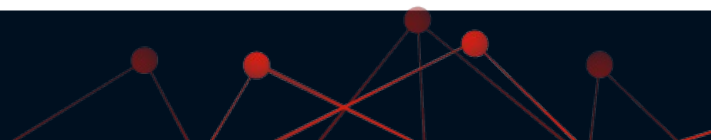
```
    ppid
```

```
    action }
```

Было: почта уходит куда попало, как попало, не сортируется

Стало: почта собирается в стандартном формате, раскладывается по проектам в виде тикетов

Установка, настройка, эксплуатация



Как ставим `monit` на машины?

- Руками (до первички, если у клиента зоопарк)
- SCM (`slack`, `ansible`) — всё само (первичка и далее)

Адаптация по месту

Monit из коробки не подстраивается под окружение (HW, софт). Варианты действий:

- ~~Ничего не делать~~
 - ~~Везде руками~~
 - Паковать monit со своим шаблонизатором
 - SCM (slack, ansible)
- } Мы здесь

```
[root@localhost /etc/monit.d]# cat template/system
check system $HOST
    if loadavg (5min) > __LA5__ for 2 cycles then exec "/srv/southbridge/bin/docker-highload-report.sh"
    if loadavg (5min) > __LA5__ for 4 cycles then exec "/bin/bash -c '/usr/bin/monit unmonitor $HOST && /bin/sleep 1800
&& /usr/bin/monit monitor $HOST'"
```


Обслуживание

Как обслуживать машину так, чтобы `monit` вам не мешал и не создавал лишних тикетов?

- `monit unmonitor all` (но можно забыть)/ `monit monitor all`
- `service monit stop` (+ внешний мониторинг процесса)/ `service monit start`

Можно и так и так, но рекомендуется второй вариант.

Вопросы?

