# Система Мониторинга

## Описание

Мониторинг за состоянием виртуальных машин и сервисов проекта осуществляется при помощи системы Prometheus

Для сбора метрик используются следующие экпортеры (агенты):

* *prometheus-node-exporter*
* *prometheus-nginx-exporter*
* *prometheus-blackbox-explorer*
* *openvpn-exporter* v0.3.0 (https://github.com/kumina/openvpn\_exporter/releases )

Для отправки уведомлений о проблемах используется prometheus-alertmanager.

Сервисы Prometheus и Alertmanager развернуты на виртуальной машине **vm-mon-srv**. Агенты распределены по виртуальным машинам следующим образом:

**vm-mon-srv**

* *prometheus-node-exporter*
* *prometheus-nginx-exporter*
* *prometheus-blackbox-explorer*

**vm-ovpn-srv**

* *prometheus-node-exporter*
* *openvpn-exporter*

**vm-pckg-srv**

* *prometheus-node-exporter*
* *prometheus-nginx-exporter*

В целях минимизации рисков информационной безопасности мониторинг виртуальной машины, на которой развернут удостоверяющий центр, не производится.

## TARGETS

Обмен данными сервера Prometheus со всеми экспортерами (за исключением openvpn-exporter) осуществляется по защищенному соединению (TLS), аутентификация осуществляется по сертификатам, заверенным нашим УЦ.

В системе мониторинга настроены следующие цели (targets):

node – получает данные о состоянии хостов со следующих виртуальных машин:

* *vm-mon-srv*
* *vm-ovpn-srv*
* *vm-pckg-srv*

nginx - получает данные о состоянии сервиса nginx со следующих виртуальных машин:

* *vm-mon-srv*
* *vm-pckg-srv*

blackbox-http - получает данные о состоянии HTTP и SSL, сертификатов со следующих виртуальных машин:

* *vm-mon-srv*
* *vm-pckg-srv*

ovpn - получает данные о состоянии сервера OpenVPN со следующих виртуальных машин:

* *vm-ovpn-srv*

Targets сконфигурированы в файле настройки Prometheus: prometheus.yml

## Система оповещения (Alertmanager)

В системе настроены следующие уведомления (alerts):

|  |  |
| --- | --- |
| **/etc/prometheus/rules.yml > network** | **Описание** |
| HostNetworkReceiveErrors | Количество ошибок при приеме на сетевом интерфейсе превышает 1 % |
| HostNetworkTransmitErrors | Количество ошибок при передаче на сетевом интерфейсе превышает 1 % |
| Unusual\_Network\_Activity | Необычная сетевая активность. Количество принятых данных за 1 мин превышает 10Mb |
| **/etc/prometheus/rules.yml > nginx** |  |
| NginxInstanceDown | Сервис nginx недоступен более 1 минуты |
| nginx\_high\_number\_active\_connections | Подозрительно много сетевых соединений в течение 3 мин. В нашем проекте nginx используется только в служебных целях, поэтому кол-во > 5 |
| nginx\_not\_all\_connections\_are\_handled | Не все соединения приняты нашим сервером nginx |
| **/etc/prometheus/rules.yml > node** |  |
| Node\_Down | Сервис экспортера недоступен более 1 минуты |
| DiskSpaceCriticallyLow | Свободное дисковое пространство заканчивается, <n% |
| HostClockNotSynchronising | На хосте не синхронизировано время (разница > 16 c) |
| HostInodesWillFillIn24Hours | В течение 24 часов закончатся свободные Inodes |
| HostMemoryUnderMemoryPressure | Количество аппаратных отказов страницы памяти превышает заданное значение (возможно, какой-то из процессов работает некорректно) |
| HostOomKillDetected | Обнаружен out of memory kill |
| HostOutOfMemory | Доступно менее 10% оперативной памяти |
| HostUnusualDiskWriteRate | Очень интенсивная запись на диск (более 50 Mb) за 2 мин |
| NodeRequiredReboot | Сервер необходимо перезагрузить |
| ServiceFailed | Запуск сервиса Systemd невозможен |
| **/etc/prometheus/rules.yml > openvpn** |  |
| OVPN\_no\_Сlient\_Сonnections | Нет клиентских соединений (возможно проблема) |
| OVPN\_Instance\_Down | Сервер OpenVPN недоступен более 1 минуты |
| **/etc/prometheus/rules.yml > ssl\_cert\_expire** |  |
| SSLCertExpiringSoon | Срок действия сертификата из цепочки SSL-сертификатов истекает через 30 дней |

При срабатывании (firing) вышеописанных алертов уведомления направляются по электронной почте администратору. Настройки smtp - сервера для отправки уведомлений находятся в конфигурационном файле Alertmanager: alertmanager.yml