**Система мониторинга**

Система мониторинга основана на Prometheus. Система состоит из различных экспортеров -мини серверов, расположенных на наблюдаемых машинах, и сервера Prometheus, который обрабатывает полученные данные от этих экспортеров. Экспортеры накапливают в себе огромное количество различных метрик, по которым можно следить за состоянием машины, на которой данный экспортер установлен.

Через определенное время, установленное в настройках файла конфигурации, Prometheus подключается к экспортерам и производит “снятие” метрик. Далее эти данные можно анализировать различными способами и по определенным параметрам можно установить пограничные значения, по достижению которых будет отправлено уведомление (различными способами). Собственно такие оповещения принято называть “Алертами”. За обработку алертов отвечает компонент Prometheus под названием Alertmanager.

В данном проекте сервер Prometheus контролирует свою машину, на которой он установлен (Monitoring), машину удостоверяющего центра (CA), машину с впн сервером (VPN) и машины резервного копирования ( Backup#1, Backup#2).

На каждой из машин, установлены следующие общие правила ( алерты):

* ((node\_filesystem\_avail\_bytes{job="node-ca", mountpoint="/",fstype!="rootfs"} / node\_filesystem\_size\_bytes{job="node-ca", mountpoint="/",fstype!="rootfs"}) \* 100) < 10 - объем свободного места на диске < 10%. При срабатывании данного алерта необходимо предпринять меры по увеличению свободного дискового пространства - очистка от старых ненужных файлов, установка доп.диска.
* ((node\_memory\_MemAvailable\_bytes{job="node-ca"} / node\_memory\_MemTotal\_bytes{job="node-ca"}) \* 100) < 10 - объем доступной оперативной памяти. При срабатывании данного алерта необходимо предпринять меры по увеличению доступной памяти - проверить на утечки памяти, зависшие процессы (зомби), физическое увеличение памяти.
* node\_load1{job="node-ca"} > 0.9 - loadaverage за минуту > 0.9. При срабатывании данного алерта необходимо проверить, что вызвало нагрузку на процессор и устранить данную причину.
* (rate(node\_network\_receive\_bytes\_total{job="node-ca", device="eth0"}[5m]) / 1024 / 1024) > 150 - Входящая нагрузка на порт > 150 Mb/s. В случае срабатывания алерта необходимо проверить, источник трафика. Если все работает в штатном режиме, то стоит задуматься об увеличении порогового значения срабатывания и/или увеличения пропускной способности канала (если текущий приблизился к своему максимуму). Так же, увеличение сетевой нагрузки может быть результатом вмешательства извне.
* (rate(node\_network\_transmit\_bytes\_total{job="node-ca", device="eth0"}[5m]) / 1024 / 1024) > 150 - Исходящая нагрузка на порт > 150 Mb/s. В случае срабатывания алерта необходимо проверить, источник трафика. Если все работает в штатном режиме, то стоит задуматься об увеличении порогового значения срабатывания и/или увеличения пропускной способности канала (если текущий приблизился к своему максимуму). Также, увеличение сетевой нагрузки может быть результатом вмешательства извне.
* up{job="node-СА"} == 0 - Данный алерт срабатывает при недоступности хоста. Причина может быть либо в “обрыве” канала или машина в выключенном состоянии.

Prometheus-exporter

* up{job="prometheus-monitor"} == 0 - процесс prometheus в статусе down. При срабатывании необходимо проверить причину остановки процесса.

VPN - exporter

* openVPN\_up == 0 - процесс openvpn в статусе down. При срабатывании необходимо проверить причину остановки процесса.
* openvpn\_server\_connected\_clients == 0 - количество подключенных клиентов. Если отсутствие подключенных клиентов по какой-то причине нормальное положение дел, то реагировать на данное срабатывание алерта, конечно, нет необходимости.