Документация системного администратора

**Общее описание системы.**

Система располагается в облаке серверов Yandex Cloud. Аккаунт [GeneralNameless@yandex.ru](mailto:GeneralNameless@yandex.ru), название облака cloudgeneralnameless, в облаке находятся две машины. Это единственный аккаунт, который имеет доступ к облаку. Доступ к виртуальным машинам осуществляется по ssh, с помощью ключа.

Ресурсы машин:

Privatevpn:

Платформа: Intel Ice Lake  
Гарантированная доля vCPU: 100%  
vCPU: 2  
RAM: 2 ГБ  
Объём дискового пространства: 20 ГБ  
Прерываемая: да

Backup-server:

Платформа: Intel Ice Lake  
Гарантированная доля vCPU: 50%  
vCPU: 2  
RAM: 2 ГБ  
Объём дискового пространства: 15 ГБ  
Прерываемая: да

Обе машины имеют динамический ip, так как это ознакомительный проект. Поэтому будем использовать 158.160.16.148 для обозначения vpn сервера, а 51.250.11.149 для обозначения бэкап сервера.

**Список имён в системе**

158.160.16.148 – хостовая машина vpn сервера  
158.160.16.148:1194 – интерфейс OpenVPN  
158.160.16.148:9090 – интерфейс Prometheus  
158.160.16.148:9093 – интерфейс Prometheus Alertmanager  
158.160.16.148:9100 – интерфейс Node exporter для Prometheus  
158.160.16.148:9176 ­– интерфейс OpenVPN exporter для Prometheus  
158.160.16.148:9256 – интерфейс Process exporter для Prometheus  
158.160.16.148:21 – интерфейс ftp соединения

51.250.11.149 – машина файлового/бэкап сервера  
51.250.11.149:9090 – интерфейс Prometheus  
51.250.11.149:9093 – интерфейс Prometheus Alertmanager  
51.250.11.149:9100 – интерфейс Node exporter для Prometheus  
51.250.11.149:9256 – интерфейс Process exporter для Prometheus  
51.250.11.149:21 – интерфейс ftp соединения

Полезные ссылки:

158.160.16.148:9090 – интерфейс Prometheus для хостовой машины vpn

51.250.11.149:9090 – интерфейс Prometheus для файлового/бэкап сервера

**Описание компонентов системы**

В системе есть несколько компонентов:

1. Easy-RSA
2. Verification Center
3. OpenVPN сервер
4. Prometheus
5. Prometheus Node Exporter
6. Prometheus Process Exporter
7. Prometheus OpenVPN Exporter
8. Prometheus Alertmanager
9. Vsftpd
10. Клиент
11. Электронный почтовый ящик
12. Бэкап сервер

Их взаимодействие показано на прилагаемой к документу схеме.

**Пошаговая настройка сервера**

Все скрипты и deb-пакеты, не входящие в официальные репозитории, находятся в свободном для скачивания доступе [ТУТ](https://github.com/EnragedShakal/PrivatePvn)

**Генерация SSH ключей:**

Перед началом работы Вам требуется пара ключей для подключения по ssh. Вы можете сгенерировать её в любой программе, которая предоставляет такую возможность. Я генерировал при помощи OpenSSH, эта утилита зачастую входит в состав Windows. Обратите внимание, что для большей безопасности следует вводить сложную кодовую фразу.

**Создание инстансов:**

Первым делом Вам необходимо завести аккаунт Yandex Cloud и создать два инстанса Compute Cloud. Первый инстанс будет в качестве бэкап сервера, а второй в качестве хостового сервера впн. Во время создания Вас попросят выбрать операционную систему, мощность вычислительных ресурсов, сетевые настройки и доступ. Операционную систему следует выбрать Ubuntu, ip-адрес статический, написать логин для входа по SSH и в поле SSH-ключ вставить публичный ключ, сгенерированный вами. Вычислительные ресурсы следует подбирать под нужды сервера. Чем больше загруженность сервера, тем больше потребуется вычислительной мощности для стабильной его работы.

**File and Backup server:**

Первым настройте бэкап сервер, так как он гораздо проще в настройке. Подключитесь к серверу по SSH с помощью закрытого ключа, сгенерированного Вами ранее, и приступайте к установке необходимого ПО:

1. Скачайте из официальных репозиториев следующие утилиты: prometeus, Prometheus-alertmanager, Prometheus-node-exporter, Prometheus-process-exporter, vsftpd.
2. Далее скачайте из репозитория GitHub deb-пакет ftp-server-config, Prometheus-config-for-file и скрипт iptables\_for\_file.sh.
3. Создайте папку /var/ftp, в которой так же создайте папки client, server и vcs. В папку client в будущем будет приходить запрос на подпись от клиента, в папку server будет приходить подписанный запрос от сервера, а в папку vcs бэкапы верификационных центров.
4. Запустите скрипт iptables\_for\_file.sh. Этот скрипт содержит набор команд для фаерволла iptables.
5. Установите deb-пакет ftp-server-config. Во время установки у вас запросят ip-адрес хостового сервера впн. Данный пакет содержит конфигурационный файл и скрипты для передачи файлов на хостовый сервер. Все скрипты выполняются в автоматическом режиме, из панели задач cron.
6. Установите deb-пакет Prometheus-config-for-file. Этот пакет содержит конфигурационные файлы и правила для Prometheus. Во время установки у Вас потребуют несколько данных, а именно: заголовок smtp сообщения (сообщения на почту будут приходить с этим заголовком), имя пользователя для smtp доступа и пароль для smtp доступа.

**VPN-сервер:**

Теперь приступите к настройке вашего основного сервера. Подключайтесь к нему по SSH и устанавливайте необходимое ПО:

1. Скачайте из официальных репозиториев следующие утилиты: easy-rsa, openvpn, prometeus, Prometheus-alertmanager, Prometheus-node-exporter, Prometheus-process-exporter, vsftpd.
2. Далее скачайте из репозитория GitHub следующие deb-пакеты и скрипты: OVPN-auto-backups, OVPN-server-generator, openvpn-exporter, Verification-Center, prometheus-config-for-vpn, iptables\_for\_file.sh.
3. Создайте папку /var/ftp, в которой создайте папку reqs. Именно в эту папку в будущем будут приходить сертификаты для подписи.
4. Установите deb-пакет Verification-Center. Данный набор скриптов поможет Вам развернуть удостоверяющий центр. В комплект deb-пакета так же входит конфигурационный файл для ftp сервера. Во время установки у Вас потребуют вести ip-адрес бэкап сервера. После установки выполняйте команду Verification-Center generate. У Вас потребуют ввести имя удостоверяющего центра, а также данные, такие как имя организации, страна, имэил и так далее. После ввода этих данных у Вас будет создан удостоверяющий центр. Этот удостоверяющий центр будет выбран центром по умолчанию для подписи сертификатов. Если Вы создали более одного удостоверяющего центра, то центр по умолчанию для подписи сертификатов можно поменять с помощью команды Verification-Center change. Как только пользователь оповестит Вам о том, что он отправил сертификат на подпись, вам необходимо выполнить команду Verification-Center sign, которая подпишет все неподписанные запросы. От Вам требуется только вводить кодовую фразу для подписи.
5. Установите deb-пакет OVPN-server-generator. Данный пакет поможет Вам развернуть OpenVPN сервер. После установки выполните команду OVPN-server-generator. У Вас запросят название удостоверяющего центра, с помощью которого нужно подписать сертификат для сервера и имя самого OpenVPN сервера. После завершения данной команды вам необходимо лишь добавить сервис сервера в автозапуск и запустить его.
6. Установите deb-пакет OVPN-auto-backups. Данный набор скриптов делает снапшоты Ваших удостоверяющих центров и отправляет их на бэкап сервер. Во время установки у Вам запросят ip-адрес бэкап сервера. Эти скрипты выполняются в автоматическом режиме, при помощи панели задач cron.
7. Установите deb-пакет openvpn-exporter. Данный пакет содержит в себе экпортер метрик OpenVPN для Prometheus. Дальнейших действий с этим пакетом не требуется.
8. Установите deb-пакет Prometheus-config-for-vpn. В данном пакете находятся конфигурационные файлы для Prometheus и Alertmanager. Во время установки у Вас запросят ввести заголовок для smtp сообщений (любой, который Вам удобен), логин почты, куда должны приходить smtp сообщения и пароль от неё.
9. Выполните скрипт iptables\_for\_file.sh. Данный скрипт содержит в себе набор правил для фаервола iptables.

Готово! Теперь у Вас есть рабочий сервер OpenVPN. Для того, чтобы клиент мог подключиться к нему, ему требуется скачать из репозитория GitHub deb-пакет OVPN-client-generator и инструкцию пользователя, в которой содержится пошаговая инструкция эксплуатации данного пакета.

**Система резервного копирования**

Система резервного копирования состоит из двух серверов. Первый сервер – хостовая машина vpn, из которой берутся файлы для резервного копирования. Вторая машина – бэкап сервер, на котором хранятся файлы бэкапов. На обеих машинах должен стоять vsftpd сервер, соответственно общение происходит по ftp. Скрипты для резервного копирования просты в работе. При установке пакета у Вас потребуют ip-адрес бэкап сервера. После установки файлы типа .crt и .key из директории удостоверяющего центра будут автоматически отправляться на бэкап сервер. Если нужен ручной бэкап, то его можно запустить командой OVPN-auto-backups manual. Ручной бэкап создаётся посредством архивирования всего удостоверяющего центра и отправки архива на бэкап сервер с временной меткой.

**Система мониторинга**

На обеих машинах используются идентичные алёрты, поэтому все алёрты будут описаны лишь единожды. Также эти описания алёртов приходят вместе с ними в SMTP сообщении на почту. В описании зачастую указывается корень проблемы. Например, какой именно system сервис крашится или какой конкретно Prometheus эуспортер не работает, что гораздо облегчает устранение проблемы.

1. PrometheusJobMissing – Prometheus по какой-то причине оффлайн. Требуется перезагрузить/включить Prometheus.
2. PrometheusTargetMissing – Один из экспортеров по какой-то причине оффлайн. В алёрте будет описано, какой именно экспортер не работает. Требуется перезагрузить/включить не работающий экспортер.
3. PrometheusAllTargetsMissing – Все экспортеры по какой-то причине оффлайн. Следует искать причину поломки. Возможно, что-то блокирует интерфейсы.
4. PrometheusTooManyRestarts – Prometheus по какой-то причине перезагрузился больше, чем два раза за последние 15 минут. Следует обратиться к логам и искать причину этого.
5. PrometheusNotConnectedToAlertmanager – Prometheus по какой-то причине не может подключиться к Alertmanager. Возможно, что-то блокирует интерфейсы или Alertmanager оффлайн.
6. PrometheusAlertmanagerNotificationsFailing – Alertmanager по какой-то причине не может отправить SMTP оповещение. Возможно что-то блокирует интерфейс или неправильно указаны настройки SMTP.
7. PrometheusRuleEvaluationFailures – Prometheus по какой-то причине не может обработать одно из правил. Скорее всего, стоит проверить его на ошибки в написании.
8. HostOutOfMemory – Память ноды заканчивается.
9. HostMemoryUnderPressure – Нода под тяжёлой нагрузкой, высокий уровень крупных сбоев страниц.
10. HostUnusualNetworkThrougputIn – Интерфейсы получают необычно большое количество данных. Стоит определить, на какой интерфейс поступает такое количество данных.
11. HostUnusualNetworkThrougputOut – Интерфейсы отправляют необычно большое количество данных. Стоит определить, какой интерфейс отправляет такое количество данных.
12. HostUnusualDiskReadRate – Диск читает слишком много данных. Стоит определить источник этого чтения.
13. HostUnusualDiskWriteRate – Диск записывает слишком много данных. Стоит определить источник этого.
14. HostOutOfDiskSpace ­– Заканчивается место на диске.
15. HostOutOfInodes – Заканчиваются доступные иноды.
16. HostInodesWillFillIn24Hours – Исходя из расчётов, иноды в файловой системе закончатся через 24 часа.
17. HostHighCpuLoad – Высокая загруженность процессора. Стоит определить процесс, который так сильно нагружает процессор.
18. HostSwapIsFillingUp – Свап память память заполнена.
19. HostSystemdServiceCrashed – Один из systemd сервисов не работает. Стоит перезапустить его или определить причину его выхода из строя.
20. HostPhysicalComponentTooHot – Один из физических компонентов сервера перегревается.
21. HostNetworkRecieveErrors – Один из интерфейсов выдаёт ошибки при получении информаци. Стоит найти и устранить причину ошибок.
22. HostNetworkTransmitErrors – Один из интерфейсов выдаёт ошибки при отправке информации. Стоит найти и устранить причину ошибок.
23. HostClockSkew – Смещение внутренних часов. Нужно убедиться, что протокол NTP настроен корректно.
24. HostClockNotSynchronising – Внутренние часы не синхронизированы. Нужно убедиться, что протокол NTP настроен на этой машине.
25. HostRequiresReboot – Машина требует перезагрузки. Перезагрузите её, пожалуйста С:
26. OpenVPNTargetMissing – OpenVPN выключен. Необходимо включить его.