

Примечание: у сервера три ip-адреса, так как на нем находятся виртуальные машины.

|  |  |
| --- | --- |
| Название сервиса | Ip и порт |
| Vpn | 10.10.10.3:1194 |
| Prometheus | 10.10.10.2:9090 |
| Prometheus-node-exporter | 10.10.10.1 – 3:9100 |
| Prometheus-alertmanager | 10.10.10.2:9093, 25 |
| Prometheus-vpn-exporter | 10.10.10.3: 9176 |
| Gitlab | 10.10.10.1:80, 443, 22 |
| Anydesk | 10.10.10.3: 80, 443, 6568  10.10.11.1 – 8: 80, 443, 6568  10.10.12.1 – 8: 80, 443, 6568 |

Уважаемые коллеги! Для безопасного доступа к внутренним ресурсам компании (таким как [Название Wiki, CRM, etc.]) извне необходимо использовать корпоративный VPN. После подключения вы получите доступ так, как если бы находились в офисе.

**1. Получение сертификата и конфигурационного файла.**

Отправьте запрос на электронную почту vpn-support@example.com. В теме письма укажите "Запрос доступа к VPN", а в теле письма — ваше ФИО и операционную систему. В ответ вы получите архив с файлами:

* client.ovpn — конфигурационный файл для клиента.
* client.crt и client.key — ваш личный сертификат и ключ (уже могут быть встроены в .ovpn файл).
* ca.crt — корневой сертификат нашей компании (уже может быть встроен в .ovpn файл).

***Внимание! Файлы client.key и client.crt являются вашими цифровыми ключами. Не передавайте их третьим лицам!***

**2. Установка и настройка клиента.**

**Windows:**

1. Скачайте и установите официальный клиент OpenVPN GUI: https://openvpn.net/client/.
2. Скопируйте файл client.ovpn в папку C:\Users\[ВашеИмяПользователя]\OpenVPN\config\.
3. Запустите OpenVPN GUI от имени администратора (правая кнопка мыши -> "Запуск от имени администратора").
4. Щелкните правой кнопкой мыши на иконке клиента в трее и выберите "Connect".

**macOS:**

1. Скачайте и установите Tunnelblick: https://tunnelblick.net/.
2. Дважды щелкните на файле client.ovpn. Tunnelblick предложит его установить. Введите пароль вашей учетной записи для завершения установки.
3. Подключитесь, нажав на иконку Tunnelblick в строке меню и выбрав "Connect".

**Linux (Ubuntu/Debian):**

1. Установите пакеты: sudo apt update && sudo apt install openvpn
2. Скопируйте файл client.ovpn в удобное место, например, ~/vpn/.
3. Для подключения выполните в терминале: sudo openvpn --config ~/vpn/client.ovpn

Поддержка:

Если у вас возникли проблемы с подключением, пожалуйста, напишите на нашу почту поддержки: vpn-support@example.com. В письме обязательно укажите:

* Вашу операционную систему.
* Точное описание ошибки (текст из логов или скриншот).
* Время, когда произошла ошибка.

Руководство для администраторов:

Местоположение: локальное в здании компании.

Группы:

Admin-vlan – имеют доступ ко всем ресурсам сети. В данной группе состоят две учетные записи admin1 и admin2.

Staff – в ней состоят сотрудники имеющие ограниченный доступ к сетевым ресурсам. Учетные записи имеют в названии фамилии сотрудников.

В данной сети есть один сервер с ОС Ubuntu на котором находятся две виртуальные машины. Одна виртуальная машина является vpn-сервером, с которой производится подключение к другим компьютерам в офисах с помощью Anydesk, вторая нужна для сбора метрик серверов с помощью Prometheus. На основном сервере происходит хранение данных, бэкапов и скриптов в gitlab.

Сервисы:

Vpn - 10.10.10.3:1194

Prometheus - 10.10.10.2:9090

Prometheus-node-exporter - 10.10.10.1–3:9100

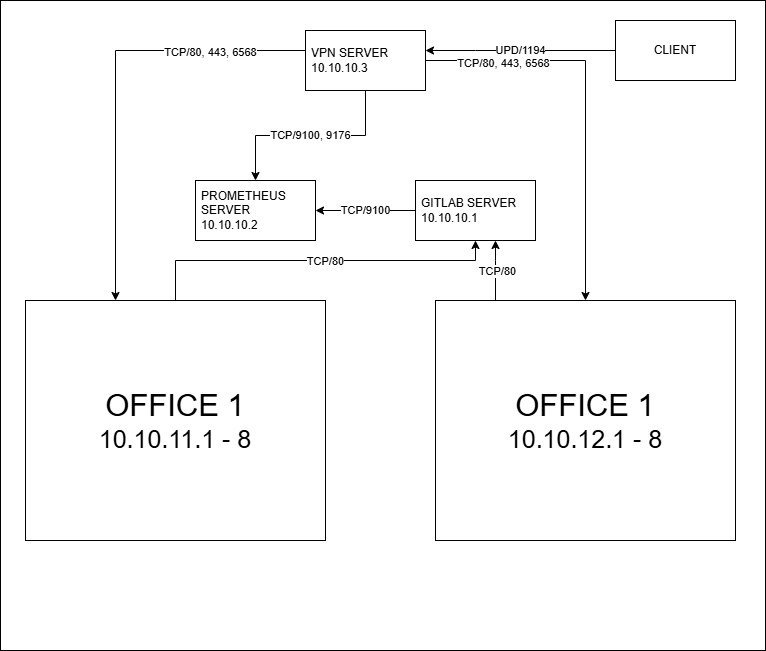
Prometheus-alertmanager - 10.10.10.2:9093, 25

Prometheus-vpn-exporter - 10.10.10.3: 9176

Gitlab - 10.10.10.1:80, 443, 22

Anydesk - 10.10.10.3: 80, 443, 6568 | 10.10.11.1–8: 80, 443, 6568 | 10.10.12.1–8: 80, 443, 6568

Схема взаимодействия компонентов сети:



Характеристики для двух виртуальных машин в virtualbox:

Образ ОС: Ubuntu Server 22.04 LTS

Размер ВМ: 4 vCPU, 4 GB RAM, 50 GB HDD

Сеть: Сетевой мост

Для настройки vpn сервера необходимо клонировать из gitlab репозиторий и запустить скрипт script\_for\_vpn.sh, далее нужно создать необходимые сертификаты для сервера и поместить их в директорию /etc/openvpn/server/. И перезапустить службу openvpn. После настройки openvpn нужно настроить резервное копирование. Для этого нужно установить duplicity с помощью команды «sudo apt-get install duplicity», далее нужно вставить строку «0 8 \* \* 0 duplicity –no-encryption /etc/openvpn sftp://admin1@10.10.10.1//backup-from-vpn/backup-$(date +%Y-%m-%d)» в crontab.

Для настройки сервера сбора метрик нужно клонировать репозиторий из gitlab и запустить скрипт script\_for\_metrics.sh, после этого нужно скопировать файл alerts.yml. После настройки prometheus нужно настроить резервное копирование. Для этого нужно установить duplicity с помощью команды «sudo apt-get install duplicity», далее нужно вставить строку «0 8 \* \* 0 duplicity –no-encryption /etc/prometheus sftp://admin1@10.10.10.1//backup-from-prometcheus/backup-$(date +%Y-%m-%d)» в crontab.

Бэкапы происходят в воскресенье в восемь часов.

Чтобы восстановить данные из бэкапа для prometcheus необходимо ввести «duplicity sftp:// sftp://admin1@10.10.10.1//backup-from-prometcheus/backup-(и нужную дату) /etc/prometcheus»

Чтобы восстановить данные из бэкапа для openvpn необходимо ввести «duplicity sftp:// sftp://admin1@10.10.10.1//backup-from-openvpn/backup-(и нужную дату) /etc/openvpn»

Компоненты системы мониторинга:

* Prometheus - сбор метрик и визуализация
* Node Exporter - системные метрики
* OpenVPN Exporter - метрики VPN
* Alertmanager - обработка и отправка уведомлений

Критические алерты и меры для устранения ошибок:

1. NodeDown (Узел недоступен)

Диагностика:

Сначала проверяем доступность узла через пинг. Если узел не отвечает, проверяем порт SSH. Затем через консоль VirtualBox смотрим, запущена ли виртуальная машина и в каком она состоянии. Проверяем, не произошел ли сбой питания или не исчерпаны ли ресурсы хоста.

Восстановление:

Если виртуальная машина остановлена, запускаем ее через консоль VirtualBox. Если она зависла, выполняем принудительный перезапуск. После восстановления подключения проверяем работу критических сервисов, особенно node\_exporter. Убеждаемся, что узел снова появляется в мониторинге.

2. HighCPUUsage (Высокая загрузка процессора)

Диагностика:

Определяем процессы с наибольшей загрузкой процессора. Проверяем общую нагрузку системы и утилизацию по ядрам. Если используются контейнеры, анализируем потребление ресурсов каждым контейнером. Смотрим историю нагрузки, чтобы понять, является ли это разовой ситуацией или постоянной проблемой.

Оптимизация:

Временно останавливаем некритичные сервисы, если это возможно. Для контейнеров ограничиваем выделенные ресурсы процессора. Повышаем приоритет критически важным процессам. Анализируем, можно ли оптимизировать работу ресурсоемких приложений.

3. OutOfMemory (Недостаток памяти)

Диагностика:

Проверяем общее использование памяти и доступную память. Ищем процессы с аномально высоким потреблением памяти. Анализируем использование swap-раздела. Проверяем, не вызвана ли проблема утечкой памяти в каком-либо приложении.

Немедленные действия:

Останавливаем процессы с утечкой памяти, если они не критические. Очищаем кэш памяти. Перезапускаем проблемные сервисы. В экстренных случаях временно создаем дополнительный swap-файл, чтобы выиграть время для решения проблемы.

4. DiskSpaceLow (Мало места на диске)

Диагностика:

Анализируем использование дискового пространства по разделам. Ищем крупные файлы и директории. Проверяем логи на предмет аномального роста. Если используются контейнеры, анализируем их использование диска. Смотрим, какие приложения генерируют много временных данных.

Очистка:

Очищаем старые логи, оставляя только актуальные данные. Удаляем кэш пакетов и временные файлы. Очищаем Docker от неиспользуемых образов и контейнеров. Архивируем и перемещаем старые данные на внешнее хранилище при необходимости.

5. HighNetworkErrors (Сетевые ошибки)

Диагностика:

Проверяем статистику сетевых интерфейсов на предмет ошибок приема и передачи. Анализируем, на каком именно интерфейсе возникают проблемы. Смотрим статистику повторной передачи пакетов. Мониторим сетевую активность в реальном времени для выявления аномалий.

Решение:

Перезапускаем проблемный сетевой интерфейс. Проверяем настройки сети в VirtualBox. Анализируем, не связана ли проблема с конфигурацией сетевого адаптера виртуальной машины.

Процесс обработки инцидента:

* Получить уведомление по email
* Проверить статус в Prometheus
* Зайти на проблемный сервер по SSH
* Выполнить диагностику согласно инструкциям выше
* После решения - отметить инцидент как обработанный в Alertmanager