FITERBYTE
01001110

Программное обеспечение «Клаудвизор»

Инструкция по установке

Содержание

Требования к системе

Минимальные

- Windows 10 (Home/Pro) или Debian-based Linux, или Windows Server 2012
- 4 vCPU
- 8 Гб RAM
- 300 MB HDD для установки
- 10 GB HDD для поисковых метаданных
- Дисковое пространство для загружаемых файлов логов
    - только при выборе локального жесткого диска для хранения логов
    - не требуется при поиске в логах на внешних хранилищах

Рекомендуемые

- Windows 10 или 11 (Home/Pro) или Ubuntu Linux 20.2 и выше, или Windows Server 2018
- 8-64 vCPU, в зависимости от требований к скорости поиска в логах
- 16-256 GB RAM, в зависимости от требований к скорости поиска в логах
- 300 MB SSD для установки
- 10-100 GB SSD для поисковых метаданных, в зависимости от количества событий в просматриваемых логах.
- Дисковое пространство для загружаемых файлов логов
    - только при выборе локального жесткого диска для хранения логов

Установка на ОС Windows

Установка

1. Скачиваем дистрибутив (файл MSI) с сайта Правообладателя ПО «Клаудвизор» и копируем его на установочную машину. Дистрибутив ПО предоставляется пользователю (покупателю, клиенту заказчику) после приобретения ПО «Клаудвизор».
2. Устанавливаем под административным пользователем.

   Результат: откроется окно браузера с адресом https://localhost:9991, с приглашением ввести имя пользователя и пароль.

3. Вводим данные по умолчанию: пользователь: admin, пароль: admin.
4. В правом верхнем углу экрана, заходим в профиль пользователя и меняем пароль администратора.

   Если Вы планируете использовать ПО локально в однопользовательском режиме, то на этом можно закончить установку.

Если Вы планируете использовать ПО в режиме многопользовательского веб-сервера, то см. ниже.

Настройка URL и порта

1. Определяемся с URL, по которому пользователи будут заходить в ПО «Клаудвизор»:
   i. Можем использовать IP адрес
   ii. Можем использовать DNS имя, например *myserver.mycompany.corp*, если в DNS создана такая запись.

2. Выбираем номер порта, на котором будет отвечать ПО.
   i. По умолчанию, установлен порт 9991, то есть URL для доступа к ПО «Клаудвизор» будет например: https://myserver.mycompany.corp:9991
   ii. Вы можете использовать другой номер порта, например 8888, тогда URL для доступа к ПО «Клаудвизор» будет: https://myserver.mycompany.corp:8888
   iii. Если на этой машине нет других более важных веб серверов, то можно использовать основной https порт 443, тогда URL для доступа к ПО «Клаудвизор» будет: https://myserver.mycompany.corp

3. Открываем выбранный порт в Windows Firewall: создаем новое разрешающее правило для входящих соединений на выбранный номер порта (тип порта - TCP) и всех (либо диапазона) IP адресов.

4. Если Вы используете виртуальную машину в облаке, - открываем выбранный порт в сетевой группе безопасности, в которую входит эта машина: создаем новое разрешающее правило для входящих соединений на этот номер порта и всех (либо диапазона) IP адресов.

5. Меняем номер порта в файле конфигурации. Открываем (с помощью notepad) файл конфигурации C:\Program Files\CloudVyzor\Logpad\LogpadService.exe.config, находим строку
   <add key="url" value="https://localhost:9991" /> , заменяем в ней:
   - localhost – на внутренний IP адрес машины в сети.
     - если машина находится в облаке или корпоративной сети, и к ней доступаются из Internet, то внутренний IP-адрес отличается от внешнего.
   - номер порта 9991 - на выбранный номер порта.

   Новая строчка может выглядеть так:
   <add key="url" value="https://10.129.0.31:8888" />
   Сохраняем файл.

6. Открываем Менеджер Задач, вкладку Службы и перезапускаем службу «CloudVyzorLogpadServer».

Результат: при навигации на https://myserver.mycompany.corp:8888, после согласия на небезопасное соединение, - видим страницу входа в ПО «Клаудвизор».

Установка сертификата для HTTPS

1. Подготавливаем сертификат в формате PFX (это можно сделать при помощи библиотеки **OpenSSL**), выданный **на выбранный ранее домен**, например *myserver.mycompany.corp*.

2. Устанавливаем данный сертификат в хранилище сертификатов Windows (правой кнопкой мыши на pfx-файле, выбрать «Установить»)

3. Открываем хранилище сертификатов Windows и находим данный сертификат.

4. По правой кнопке -> Все задачи -> Экспорт, - экспортируем публичный ключ в формате Base 64 Encoded X.509 (CER) в файл с именем certificate.cer.

5. Копируем файл certificate.cer в папку C:\Program Files\CloudVyzor\Logpad, перезаписав файл, установленный по умолчанию.

Результат: при навигации на https://myserver.mycompany.corp:8888, - соединение должно быть квалифицировано браузером как безопасное.

Установка на ОС Linux (Debian-based)

Установка пакета

1. Скачиваем дистрибутив для Debian Linux (файл DEB) с сайта Правообладателя ПО «Клаудвизор».

2. Копируем дистрибутив на установочную машину, например:
scp -i mysshkeyfile cloudvyzor-logpad_2.15.0_amd64.deb myadmin@51.250.71.56:/home/myadmin

3. Устанавливаем SSH сессию под административным пользователем, например:
ssh -i mysshkeyfile myadmin@51.250.71.56

4. Устанавливаем пакет, например:
sudo apt-get install /mnt/cloudvyzor-logpad_2.15.0_amd64.deb

5. Запускаем службу:
   cd /usr/share/Megatrace.WebServerCore
   sudo Megatrace.WebServerCore

6. В локальном браузере (если таковой есть), набираем https://localhost:8443

   Результат: откроется страница ПО, с приглашением ввести имя пользователя и пароль.

1. Вводим данные по умолчанию: пользователь: admin, пароль: admin.

2. В правом верхнем углу экрана, заходим в профиль пользователя и меняем пароль администратора.

   Если Вы планируете использовать ПО локально в однопользовательском режиме, то на этом можно закончить установку.

   Если Вы планируете использовать ПО в режиме многопользовательского веб-сервера, то см. ниже.

Настройка URL и HTTPS порта

1. Определяемся с URL, по которому пользователи будут заходить на этот сервер:
   i. Можем использовать IP адрес
   ii. Можем использовать DNS имя, например *myserver.mycompany.corp*, если в DNS создана такая запись.

2. Выбираем номер порта, на котором будет отвечать ПО.
   i. По умолчанию, установлен порт 8443, то есть URL для доступа к ПО «Клаудвизор» будет например: https://myserver.mycompany.corp:8443
   ii. Вы можете использовать другой номер порта, например 8888, тогда URL для доступа к ПО «Клаудвизор» будет: https://myserver.mycompany.corp:8888
   iii. Если на этой машине нет других более важных веб серверов, то можно использовать основной https порт 443, тогда URL для доступа к ПО «Клаудвизор» будет: https://myserver.mycompany.corp

2. Открываем выбранный порт в файерволле, например:
   sudo ufw allow 8888

3. Если Вы используете виртуальную машину в облаке, - открываем выбранный порт в сетевой группе безопасности, в которую входит эта

машина: создаем новое разрешающее правило для входящих соединений на этот номер порта и всех (либо диапазона) IP адресов.

4. Редактируем файл конфигурации:
   cd /usr/share/Megatrace.WebServerCore
   sudo nano /usr/share/Megatrace.WebServerCore/appsettings.json

   Находим строку:
   "Url": "https://localhost:8443", заменяем в ней:
   - localhost – на **внутренний IP адрес машины**
     - если машина находится в облаке или корпоративной сети и к ней доступаются из Internet, то внутренний IP-адрес отличается от внешнего.
   - номер порта 8443 - на выбранный номер порта, например 8888.

   Новая строчка может выглядеть так:
   "Url": "10.129.0.31:8888"
   Сохраните файл.

5. Перезапустите машину
   sudo reboot

Результат: при навигации на https://myserver.mycompany.corp:8888, после согласия на небезопасное соединение, - видим страницу входа в ПО «Клаудвизор».

Установка сертификата для HTTPS

1. Подготовьте сертификат в формате PFX (это можно сделать при помощи библиотеки **OpenSSL**), выданный на выбранное ранее DNS имя машины, например *myserver.mycompany.corp*.

2. Копируем PFX файл в папку сервиса, например:
   scp -i mysshkey mycertificate.pfx myadmin@51.250.71.56:
   /usr/share/Megatrace.WebServerCore

3. Прописываем имя сертификата и пароль в файле конфигурации:
   cd /usr/share/Megatrace.WebServerCore
   sudo nano /usr/share/Megatrace.WebServerCore/appsettings.json

   Находим:
   ```
   "Https": {
       "Certificate": {
        "Password": "",
        "Path": ""
       },
   ```
   Меняем значение установок

- Password - на пароль от сертификата, если он задан
- Path – на “*/usr/share/Megatrace.WebServerCore/mycertificate.pfx*”

4. Перезагружаем машину
   sudo reboot

Результат: при навигации на https://myserver.mycompany.corp, - соединение должно быть квалифицировано браузером как безопасное.

Настройка хранилища для загружаемых логов

ПО «Клаудвизор» поддерживает поиск по логам:
- загружаемых в него через веб клиента или API
- на внешних файловых хранилищах

Для загружаемых логов, можно выбрать тип хранилища:
- локальный или сетевой диск
- S3
- Blob Storage

По умолчанию, хранилище для загружаемых логов сконфигурировано на локальном диске:
- Windows: *C:\Program Files\CloudVyzor\Logpad\Data\Storage*
- Linux: */usr/share/Megatrace.WebServerCore/Data/Storage*

Настойка в Windows

1. Останавливаем службу *CloudVyzorLogpadServer*

2. **Для использования сетевой папки в качестве хранилища:**
   a. предварительно создаем на разделяемой папке *MyFileShare* папку *CloudVyzor/Data/Storage/admin/logs*
   b. Открываем (с помощью notepad) файл конфигурации *C:\Program Files\CloudVyzor\Logpad\ LogpadService.exe.config*, находим строку *<add key="Storage" value="file://./Data/Storage" />*, заменяем в ней: *value="file://MyFileShare/CloudVyzor/Data/Storage"*

3. **Для использования S3 в качестве хранилища:**
   a. В хранилище S3, предварительно создаем бакет *admin-logs-d*
   b. Открываем (с помощью notepad) файл конфигурации *C:\Program Files\CloudVyzor\Logpad\ LogpadService.exe.config*, находим строку *<add key="Storage" value="file://./Data/Storage" />*, заменяем в ней: *value="type=ya;key=<S3_key_value_here>;secret=<s3_key_secret_here>;region =ya;bucket= admin-logs-d"*

4. **Для использования Blob storage в качестве хранилища:**
   a. В хранилище Blob, предварительно создаем контейнер *admin-logs-d*

b. Открываем (с помощью notepad) файл конфигурации *C:\Program Files\CloudVyzor\Logpad\ LogpadService.exe.config*, находим строку *<add key="Storage" value="file://./Data/Storage" />*, заменяем в ней:

value="DefaultEndpointsProtocol=https;AccountName=<accountname>;AccountKey=<accountkey>;EndpointSuffix=core.windows.net"/>

5. Запускаем службу *CloudVyzorLogpadServer*

Результат: При создании в ПО новых баз логов, папки под них будут созданы в новом хранилище. При загрузке логов, файлы логов будут загружены в эти папки.

Настойка в Linux

1. **Для использования сетевой папки в качестве хранилища:**
   a. предварительно создаем на сетевой папке *MyFileShare* папку *CloudVyzor/Data/Storage/admin/logs*.
   Маунтим сетевую папку как “/mnt/MyFileShare”
   Для этого: если сетевая папка на машине под Linux используйте **SSHFS** клиент. Если сетевая папка на машине под Windows используйте пакет Samba для реализации сетевого протокола SMB / CIFS.

   b. Открываем файл конфигурации
   cd /usr/share/Megatrace.WebServerCore
   sudo nano /usr/share/Megatrace.WebServerCore/appsettings.json

   Находим строку: *"DatabaseFolder": "/usr/share/Megatrace.WebServerCore/Data/Database"*
   заменяем в ней:
   "DatabaseFolder": “/mnt/MyFileShare/CloudVyzor/Data/Storage"

2. **Для использования S3 в качестве хранилища:**
   a. В хранилище S3, предварительно создаем бакет *admin-logs-d*
   b. Открываем файл конфигурации
   cd /usr/share/Megatrace.WebServerCore
   sudo nano /usr/share/Megatrace.WebServerCore/appsettings.json

   Находим строку: *"DatabaseFolder": "/usr/share/Megatrace.WebServerCore/Data/Database"*
   заменяем в ней:
   "DatabaseFolder": "type=ya;key=<S3_key_value_here>;secret=<s3_key_secret_here>;region=ya;bucket= admin-logs-d"

3. **Для использования Blob storage в качестве хранилища:**

---

a. В хранилище Blob, предварительно создаем контейнер *admin-logs-d*
b. Открываем файл конфигурации
cd /usr/share/Megatrace.WebServerCore
sudo nano /usr/share/Megatrace.WebServerCore/appsettings.json

Находим строку: *"DatabaseFolder": "/usr/share/Megatrace.WebServerCore/Data/Database"*
заменяем в ней:
"DatabaseFolder": "DefaultEndpointsProtocol=https;AccountName=<accountname>;AccountKey=<accountkey>;EndpointSuffix=core.windows.net"

4 **Перезагружаем машину**
sudo reboot

Результат: При создании в ПО новых баз логов, папки под них будут созданы в новом хранилище. При загрузке логов, файлы логов будут загружены в эти папки.

Дополнительная информация по использованию ПО «Клаудвизор» содержится в Руководстве пользователя ПО «Клаудвизор».

Настройка лицензии

Свяжитесь со службой поддержки support@piterbyte.com