

Інструкція зі встановлення програмного комплексу Metrix

Copyright 2015-2023 Metrix-totalAPI

Склад комплекту:  
  
1. База даних зберігання телематичних даних Apache Cassandra

2. Налаштування та встановлення програм на ОС Windows

3. Сервіс роботи з телематичними даними **TotalApi**

**4.** База даних для Web-додатку **Metrix**

**5.** Web-додаток **Metrix**

**1. База даних зберігання телематичних даних Apache Cassandra**

Покрокова інструкція встановлення бази даних Apache Cassandra версії 3.x на операційній системі Ubuntu:

* **Відключення запиту пароля SUDO (якщо потрібно):**

Додати в файл /etc/sudoers:

%sudo ALL=NOPASSWD: ALL

* **Встановлення Java OpenJDK**

Apache Cassandra потребує OpenJDK 8 для роботи в системі Ubuntu. Спочатку оновіть свій репозиторій пакетів:

sudo apt update

Коли процес завершиться, інсталюйте OpenJDK 8 за допомогою такої команди:

sudo apt install openjdk-8-jdk –y

Коли інсталяція завершиться, перевірте, чи Java інстальовано успішно, перевіривши версію Java:

java -version

* **Встановлення apt-transport-https Package**

Далі встановіть транспортний пакет apt-transport-https Package. Вам потрібно додати цей пакет до вашої системи, щоб увімкнути доступ до репозиторіїв за допомогою HTTPS. Введіть цю команду:

sudo apt install apt-transport-https

* **Додайте репозиторій Apache Cassandra та імпортуйте ключ GPG**

Для <release series> укажіть номер основної версії без крапки та з додаванням «x».

Останній <release series> — 41x.

Для старіших випусків <release series> може мати значення 40x, 311x, 30x або 22x.

Додайте репозиторій Apache Cassandra до /etc/apt/sources.list.d/cassandra.sources.list, наприклад, для останньої версії 3.11.

echo "deb https://debian.cassandra.apache.org 311x main" | sudo tee -a /etc/apt/sources.list.d/cassandra.sources.list

Додайте ключі репозиторію Apache Cassandra:

curl https://downloads.apache.org/cassandra/KEYS | sudo apt-key add -

* **Встановлення Apache Cassandra**

Тепер ви готові встановити Cassandra на Ubuntu.

Оновіть список пакетів сховища:

sudo apt update

Якщо ви зіткнулися з цією помилкою:

GPG error: http://www.apache.org 311x InRelease: The following signatures couldn't be verified because the public key is not available: NO\_PUBKEY A278B781FE4B2BDA

Тоді додайте відкритий ключ A278B781FE4B2BDA таким чином:

sudo apt-key adv --keyserver pool.sks-keyservers.net --recv-key A278B781FE4B2BDA

Повторіть sudo apt-get update. Фактичний ключ може бути іншим, ви отримуєте його з самого повідомлення про помилку.

Щоб отримати повний список відкритих ключів Apache, ви можете звернутися до Cassandra KEYS.

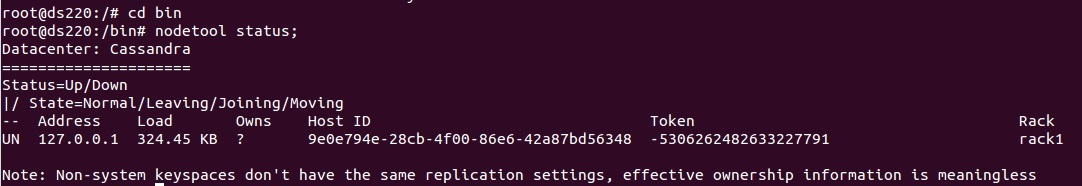
Зараз виконайте команду встановлення:

sudo apt install cassandra

* **Перевірте встановлення Apache Cassandra**

Нарешті, щоб переконатися, що процес встановлення Cassandra завершився належним чином, перевірте стан кластера:

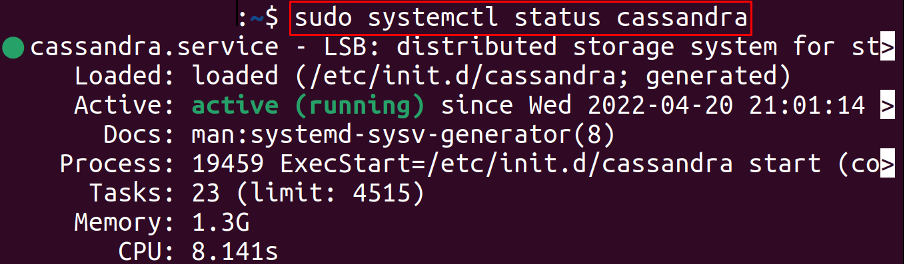
nodetool status



Літери «UN» у виході сигналізують про те, що кластер працює.

Ви також можете перевірити статус Cassandra, ввівши:

sudo systemctl status cassandra або sudo service cassandra status



Стан має відображатися як активний (працює) зеленим кольором.

* **Команди для запуску, зупинки та перезапуску служби Cassandra**

sudo systemctl start cassandra

sudo systemctl stop cassandra

sudo systemctl restart cassandra

* **Автоматичний запуск служби Apache Cassandra під час завантаження Ubuntu**

Коли ви вимикаєте або перезавантажуєте систему, служба Cassandra стає неактивною. Щоб запустити Cassandra автоматично після завантаження, скористайтеся такою командою:

sudo systemctl enable cassandra

Тепер, якщо ваша система перезавантажується, служба Cassandra вмикається автоматично.

* **Розташування основних файлів Cassandra:**

Конфігурація: /etc/cassandra/cassandra.yaml

База даних: /var/lib/cassandra/data

Логи роботи: /var/log/cassandra

* **Налаштування конфігураційного файлу:**

listen\_address: xxx.xxx.xxx.xxx # localhost

rpc\_address: xxx.xxx.xxx.xxx # localhost

file\_cache\_size\_in\_mb: 2048 # 512

auto\_snapshot: false # true

#incremental\_backups: false # false

# clustering support

#endpoint\_snitch: GossipingPropertyFileSnitch # SimpleSnitch

seed\_provider:

- class\_name: org.apache.cassandra.locator.SimpleSeedProvider

parameters:

- seeds: "xxx.xxx.xxx.xxx"

* Використання окремого диска для БД Cassandra

Якщо є можливість, слід розділити диск, на якому знаходиться Commit Log і диск з даними. Найпростіший спосіб - зробити каталог БД посиланням на інший диск:

sudo systemctl stop cassandra

sudo mount -t ext4 /dev/sdb1 /var/lib/cassandra/data

sudo chown -R cassandra:cassandra /var/lib/cassandra/data

sudo systemctl start cassandra

Для постійного монтування необхідно додати файл /etc/fstab рядок

/dev/sdb1 /var/lib/cassandra/data auto defaults,nofail 0 2

або:

UUID={uuid} /var/lib/cassandra/data auto defaults,nofail 0 2

Краще вказувати диск за його UUID, дізнатися який можна командою:

sudo blkid

* **Поліпшення продуктивності**

Вимкнення SWAP:

Нездатність повністю вимкнути swap може серйозно знизити продуктивність. Оскільки Cassandra має кілька реплік і прозоре перемикання після відмови, бажано, щоб репліка була знищена негайно, коли пам’яті мало, а не переходила в обмін. Це дозволяє негайно перенаправляти трафік до функціонуючої репліки замість того, щоб продовжувати потрапляти на репліку, яка має високу затримку через підкачку. Якщо у вашій системі багато DRAM, заміна все одно значно знижує продуктивність, оскільки ОС замінює виконуваний код, щоб більше DRAM було доступно для кешування дисків.

Якщо ви наполягаєте на використанні swap, ви можете встановити vm.swappiness=1. Це дозволяє ядрузамінити абсолютно найменш використовувані частини.

sudo swapoff –all

Далі видаліть усі записи файлу підкачки з /etc/fstab

* Налаштування TCP

Щоб обробляти тисячі одночасних з’єднань, які використовує Cassandra, DataStax рекомендує ці налаштування для оптимізації мережевого стеку Linux.

Додайте ці налаштування до /etc/sysctl.conf (або /etc/sysctl.d/filename.conf):

net.core.rmem\_max = 16777216

net.core.wmem\_max = 16777216

net.core.rmem\_default = 16777216

net.core.wmem\_default = 16777216

net.core.optmem\_max = 40960

net.ipv4.tcp\_rmem = 4096 87380 16777216

net.ipv4.tcp\_wmem = 4096 65536 16777216

vm.max\_map\_count = 1048575

Щоб задіяти негайно (залежно від вашого дистрибутива):

sudo sysctl -p /etc/sysctl.conf

#OR...

#sudo sysctl -p /etc/sysctl.d/filename.conf

* Оптимізація SSD

Конфігурації SSD за замовчуванням у більшості дистрибутивів Linux не є оптимальними. Виконайте такі кроки, щоб забезпечити найкращі налаштування для SSD:

Переконайтеся, що для параметру SysFS встановлено значення false (нуль). Це вимикає будь-яке виявлення операційною системою, щоб гарантувати, що диск вважається SSD.

Застосуйте ті самі налаштування для будь-яких блокових пристроїв, створених із накопичувачів SSD, наприклад mdarrays.

Налаштуйте планувальник вводу-виведення данних значення deadline або noop:

Noop-планувальник є правильним вибором, коли цільовим блоковим пристроєм є масив твердотільних накопичувачів з висококласним контролером вводу-виводу, який виконує оптимізацію вводу-виводу.

Планувальник deadline оптимізує запити, щоб мінімізувати затримку введення-виведення. Якщо сумніваєтеся, скористайтеся планувальником deadline.

Встановіть для блокового пристрою значення 8 КБ. Цей параметр повідомляє операційній системі не зчитувати зайві байти, що може збільшити час введення-виведення та забруднити кеш байтами, які не запитував користувач.

Наприклад, якщо SSD є /dev/sda, у /etc/rc.local:

echo deadline > /sys/block/sda/queue/scheduler

#OR...

#echo noop > /sys/block/sda/queue/scheduler

touch /var/lock/subsys/local

echo 0 > /sys/class/block/sda/queue/rotational

echo 8 > /sys/class/block/sda/queue/read\_ahead\_kb

Якщо /etc/rc.local відсутній, ви повинні створити його:

sudo echo '#!/bin/sh -e' > /etc/rc.local

sudo chmod u+x /etc/rc.local

Негайно застосувати та перевірити налаштування:

systemctl start rc-local

systemctl status rc-local

* **Встановлення обмеження ресурсів користувача**

Використовуйте команду ulimit -a, щоб переглянути поточні обмеження. Хоча обмеження також можна тимчасово встановити за допомогою цієї команди, DataStax рекомендує зробити зміни постійними:

Встановлення пакетів: переконайтеся, що такі параметри включено у файл /etc/security/limits.d/cassandra.conf:

<cassandra\_user> - memlock unlimited

<cassandra\_user> - nofile 100000

<cassandra\_user> - nproc 32768

<cassandra\_user> - as unlimited

У RHEL версії 6.x переконайтеся, що такі параметри включено у файл /etc/security/limits.conf:

<cassandra\_user> - memlock unlimited

<cassandra\_user> - nofile 100000

<cassandra\_user> - nproc 32768

<cassandra\_user> - as unlimited

Якщо ви запускаєте Cassandra як root, деякі дистрибутиви Linux, такі як Ubuntu, вимагають встановлення обмежень для root замість використання cassandra\_user:

root - memlock unlimited

root - nofile 100000

root - nproc 32768

root - as unlimited

Для систем на базі RHEL 6.x також установіть обмеження nproc у /etc/security/limits.d/90-nproc.conf:

cassandra\_user - nproc 32768

Для всіх установок додайте такий рядок до /etc/sysctl.conf:

vm.max\_map\_count = 1048575

Для встановлення в операційних системах Debian і Ubuntu модуль pam\_limits.so не ввімкнено за замовчуванням. Відредагуйте файл /etc/pam.d/su та розкоментуйте цей рядок:

session required pam\_limits.so

Ця зміна у файлі конфігурації PAM гарантує, що система читає файли в каталозі /etc/security/limits.d. Щоб зміни вступили в силу, перезавантажте сервер або виконайте таку команду:

sudo sysctl –p

Щоб переконатися, що обмеження застосовано до процесу Cassandra, виконайте таку команду, де {pid} — це ідентифікатор поточного процесу Cassandra:

cat /proc/{pid}/limits

* **Встановіть розмір для оптимального збирання сміття Java у Cassandra**

Див. [Ресурси налаштування Java](https://docs.datastax.com/en/cassandra-oss/2.1/cassandra/operations/ops_tune_jvm_c.html).

* **Вимкнути режим zone\_reclaim\_mode у системах NUMA**

Ядро Linux може бути непослідовним у ввімкненні/вимкненні zone\_reclaim\_mode. Це може призвести до дивних проблем з продуктивністю.

Великі випадкові скачки ЦП, що призводять до значного збільшення затримки та пропускної здатності. Програми зависають на невизначений час, очевидно, нічого не роблять. Симптоми раптово виникають і зникають. Після перезавантаження симптоми зазвичай не проявляються протягом деякого часу. Щоб переконатися, що режим zone\_reclaim\_mode вимкнено виконайте наступне:

echo 0 > /proc/sys/vm/zone\_reclaim\_mode

* **Застосуйте оптимальні параметри blockdev --setra для RAID на звичайних жорстких дисках**

Зазвичай рекомендовано значення 128 для readahead. Переконайтеся, що для setra не встановлено значення 65536:

sudo blockdev --report /dev/spinning\_disk

для встановлення параметру setra:

sudo blockdev --setra 128 /dev/spinning\_disk

Примітка. Рекомендоване налаштування для RAID на SSD є таким самим, як і для SSD, які не використовуються в RAID.

* **Синхронізація годинників**

Синхронізуйте годинник на всіх вузлах, використовуючи NTP (протокол мережевого часу) або інші методи. Це потрібно, оскільки Cassandra перезаписує стовпець, лише якщо існує інша версія, позначка часу якої є новішою.

* **Встановлення Fail2Ban**

Протокол SSH дозволяє віддалено керувати пристроями, проте як і будь-який відкритий для публічного доступу сервіс, він уразливий для різноманітних атак. Одна з найбільш очевидних та поширених уразливостей – добір паролів.

У цьому посібнику ми розглянемо захист SSH від підбору паролів за допомогою пакету fail2ban, який ставиться на Ubuntu 16.04.

Принцип роботи fail2ban є простим. Спеціальний сервіс шукає в системних журналах (логах) записи про невдалі спроби автентифікації та за певних умов за допомогою iptables блокує IP-адреси, з яких ведеться атака.

Усі команди, що наводяться нижче, повинні виконуватися від імені root-користувача або за допомогою sudo.

Спочатку встановіть пакет fail2ban:

apt-get install fail2ban

Тепер потрібно зробити так, щоб сервіс fail2ban автоматично запускався під час завантаження системи:

systemctl enable fail2ban

Файли налаштувань fail2ban розташовані в каталозі /etc/fail2ban/:

fail2ban.conf – дефолтні налаштування сервісу fail2ban;

fail2ban.d/\*.\* – налаштування користувача сервісу fail2ban;

jail.conf – дефолтні налаштування для сервісів, що захищаються;

jail.d/\*.\* – налаштування користувача для сервісів, що захищаються;

filter.d/\*.\* – налаштування шаблонів пошуку у системних журналах (логах);

action.d/\*.\* – налаштування виконуваних дій;

paths\*.conf – налаштування шляхів для різних операційних систем.

Щоб ваші налаштування не перезаписувалися при оновленні пакетів, рекомендуємо замість редагування файлів з дефолтними налаштуваннями створювати власні (користувацькі) файли налаштувань.

Вам необхідно видалити дефолтні налаштування захисту sshd:

cat /dev/null >/etc/fail2ban/jail.d/defaults-debian.conf

Потім створіть файл /etc/fail2ban/jail.d/sshd.conf. Додайте до файлу такі записи:

[sshd]

enabled = true

bantime = 600

findtime = 650

maxretry = 5

Тепер якщо параметр enabled буде мати значення true, сервіс **fail2ban** заблокує відповідну IP-адресу на кількість секунд, прописану у параметрі bantime, за умови, що за період, вказаний у секундах у параметрі findtime, з цієї адреси буде проведено задане параметром maxretry або більше невдалих спроб ssh-автентифікації. Після періоду, прописаного у параметрі bantime, заблокована IP-адреса автоматично розблокується.

У нашому прикладі IP-адреса буде блокуватися на 600 секунд, якщо протягом останніх 650 секунд з неї було здійснено 5 і більше невдалих спроб аутентифікації.

Налаштування сервісу fail2ban завершено, необхідно його перезапустити:

systemctl restart fail2ban

**2. Налаштування та встановлення програм на ОС Windows**

1. **Необхідні компоненти для встановлення на чистій системі:**

* [.NET Framework 4.8 (ndp48-x86-x64-allos-enu.exe)](https://go.microsoft.com/fwlink/?LinkId=2018531)
* [dotnet-hosting-2.2.8-win.exe](https://download.visualstudio.microsoft.com/download/pr/ba001109-03c6-45ef-832c-c4dbfdb36e00/e3413f9e47e13f1e4b1b9cf2998bc613/dotnet-hosting-2.2.8-win.exe)
* [UrlRewrite2 (перенаправлення http -> https)](https://github.com/TotalApi/Installations/raw/main/Redist/Tools/urlrewrite2.exe)
* [WinAcme (автоматичне створення/подовження SSL-сертифікатів)](https://github.com/TotalApi/Installations/raw/main/Redist/Tools/win-acme.v2.1.13.978.x64.pluggable.zip)
* [tcp\_setup (збільшення кількості одночасних TCP-з’єднань)](https://github.com/TotalApi/Installations/raw/main/Redist/Tools/tcp_setup.reg)

1. **Додаткові інструменти**

* [Chrome](https://www.google.com/intl/en_us/chrome)
* [7z](https://www.7-zip.org/download.html)
* [Process Hacker 2](https://processhacker.sourceforge.io/downloads.php)
* [[FAR Manager](https://github.com/TotalApi/Installations/raw/main/Redist/Tools/Far%20Manager.zip)]
* [[Remote Debugger](https://github.com/TotalApi/Installations/raw/main/Redist/Tools/Remote%20Debugger.zip)]

1. **Сервіс роботи з телематичними даними TotalApi**

* Розпакувати вміст архіву в будь-яку папку;
* Копіювати [зразки конфігураційних файлів](https://github.com/TotalApi/Installations/raw/main/Configs/Default/TotalApi) до папки TotalApi;
* Налаштувати [сервіс у конфігураційному](https://github.com/TotalApi/Installations/blob/main/Configs/TotalApi_Config.md) файлі;
* Налаштувати [модулі прийому координат](https://github.com/TotalApi/Installations/blob/main/Configs/TotalApi_DevicePlugins.md);
* Встановити сервіс як службу Windows, виконавши команду в командному рядку TotalApi.Server.Host.exe /i з правами адміністратора.

1. **База даних для Web-додатку Metrix**

* встановити БД MS SQL Server 2012 R2 x64 або вище. (Використання інших редакцій теоретично можливе, але не перевірялося);
* (опційно) встановити [SQL Server Management Studio](https://aka.ms/ssmsfullsetup).

1. **Web-додаток Metrix**

* Встановити на сервері IIS 7+ (у разі встановлення обов'язково вибрати опцію підтримки Web-socket);
* Для автоматичного старту програми виконати рекомендації, описані [тут](https://www.taithienbo.com/how-to-auto-start-and-keep-an-asp-net-core-web-application-and-keep-it-running-on-iis/) та [тут](https://docs.hangfire.io/en/latest/deployment-to-production/making-aspnet-app-always-running.html);
* Розпакувати вміст архіву в будь-яку папку;
* Копіювати зразки [конфігураційних файлів](https://github.com/TotalApi/Installations/raw/main/Configs/Default/MetriX) у папку Metrix;
* Налаштувати сервіс у [конфігураційному файлі](https://github.com/TotalApi/Installations/blob/main/Configs/Metrix_Config.md);
* Створити в IIS Web-додаток, вказавши папку Metrix як кореневу;