

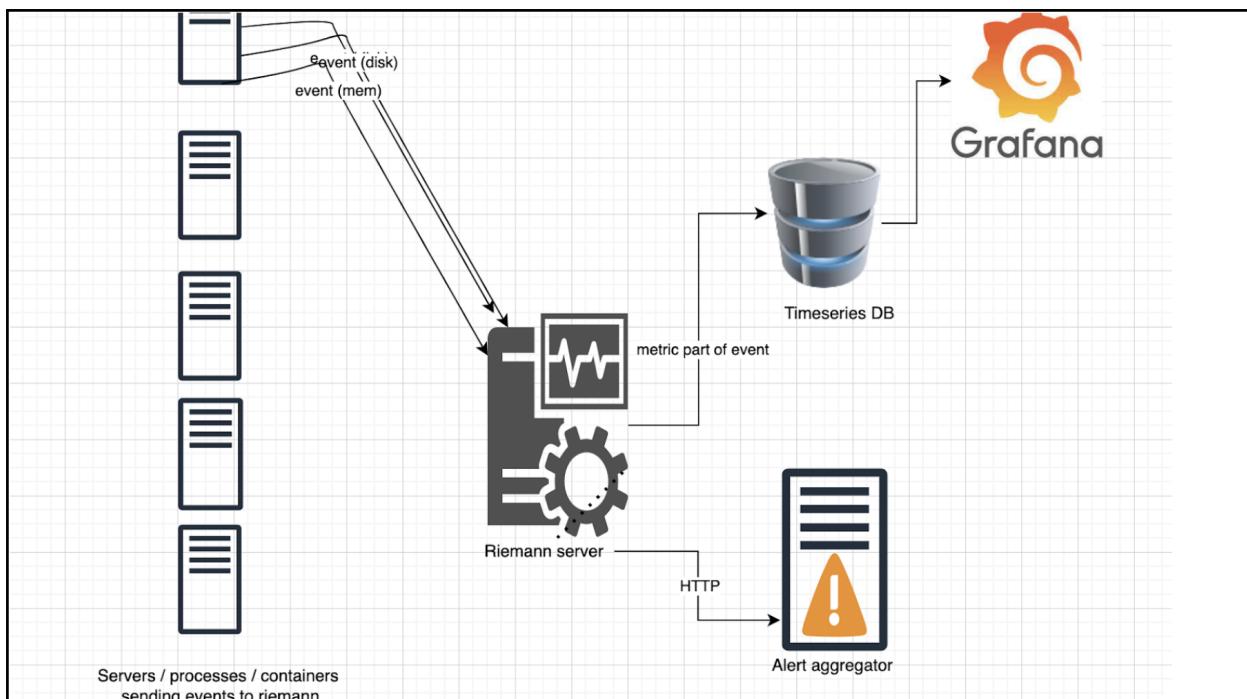
Infrastructure Monitoring

1. Who monitors the monitor?

According to the monitoring stack Riemann(an event processor) takes events as input from multiples Servers/containers and give out some metrics which are monitored with the help of grafana which is an open source visualisation system.(In the question monitor refers to the monitoring stats of all the Servers/containers which goes into Riemann as events and **grafana** monitors all these metrics).

2. Identify what could break monitoring?

After Processing of events Riemann server can send metrics/stats to a data-store(in case of time series data it can be influxDB or OpenTSDB) which can be visualised and monitored through grafana.If **Riemann server goes down** then it could break the monitoring because Riemann server will not be able to generate metrics/stats for monitoring the system and also it won't be able to communicate to Alert aggregator via HTTP cons which will result in sending no alerts to team for monitoring If anything goes down.



(3) How can you bring redundancy here

To bring in redundancy here we can setup multiple Riemann servers so that if one server goes down then our Containers/servers can send events to another Riemann server. Also to keep our data safe we can setup multiple Time series database which can backup the data of the primary Time-series DB so that in case DB failure another Database can be used for monitoring purpose.

Setup Riemann

Steps:-

1. Setup a Virtual Machine
2. Use the below command to download Riemann

```
riemann@riemann-VirtualBox:~$ wget https://github.com/riemann/riemann/releases/download/0.3.8/riemann-0.3.8.tar.bz2
--2022-03-24 23:01:25-- https://github.com/riemann/riemann/releases/download/0.3.8/riemann-0.3.8.tar.bz2
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com)|13.234.210.38|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/3385297/bb06ff23-047b-47c2-a63a-d529bd908f8c?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220324%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220324T173125Z&X-Amz-Expires=300&X-Amz-Signature=55468c8f1ceec246a1dcac1e9ecebe71d2bc867802261838ca7176cd2fa5890d&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=3385297&response-content-disposition=attachment%3B%20filename%3Driemann-0.3.8.tar.bz2&response-content-type=application%2Foctet-stream [following]
--2022-03-24 23:01:25-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/3385297/bb06ff23-047b-47c2-a63a-d529bd908f8c?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220324%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220324T173125Z&X-Amz-Expires=300&X-Amz-Signature=55468c8f1ceec246a1dcac1e9ecebe71d2bc867802261838ca7176cd2fa5890d&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=3385297&response-content-disposition=attachment%3B%20filename%3Driemann-0.3.8.tar.bz2&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91010548 (87M) [application/octet-stream]
```

3. Extract Riemann tar file using the below command:

```
riemann@riemann-VirtualBox:~$ tar xvfj riemann-0.3.8.tar.bz2
riemann-0.3.8/
riemann-0.3.8/bin/
riemann-0.3.8/bin/riemann
riemann-0.3.8/lib/
riemann-0.3.8/lib/riemann.jar
riemann-0.3.8/etc/
riemann-0.3.8/etc/riemann.config
riemann@riemann-VirtualBox:~$ cd riemann-0.3.8
riemann@riemann-VirtualBox:~/riemann-0.3.8$
```

4. Install some of the dependencies using the below commands:

```
riemann@riemann-VirtualBox:~$ sudo apt install build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu dpkg-dev fakeroot g++
  g++-9 gcc gcc-9 libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libasan5 libatomic1 libbinutils libc-dev-bin
  libc6-dev libcrypt-dev libctf-nobfd0 libctf0 libfakeroot libgcc-9-dev
  libitm1 liblsan0 libquadmath0 libstdc++-9-dev libtsan0 libubsan1
  linux-libc-dev make manpages-dev
Suggested packages:
  binutils-doc debian-keyring g++-multilib g++-9-multilib gcc-9-doc
  gcc-multilib autoconf automake libtool flex bison gcc-doc gcc-9-multilib
  gcc-9-locales glibc-doc libstdc++-9-doc make-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential dpkg-dev
  fakeroot g++ g++-9 gcc gcc-9 libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1
  libbinutils libc-dev-bin libc6-dev libcrypt-dev libctf-nobfd0 libctf0
  libfakeroot libgcc-9-dev libitm1 liblsan0 libquadmath0 libstdc++-9-dev
```

```
riemann@riemann-VirtualBox:~$ sudo apt install zlib1g-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  zlib1g-dev
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 155 kB of archives.
After this operation, 605 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 zlib1g-dev amd64 1:1.2.11.dfsg-2ubuntu1.2 [155 kB]
Fetched 155 kB in 0s (1,272 kB/s)
Selecting previously unselected package zlib1g-dev:amd64.
(Reading database ... 186497 files and directories currently installed.)
Preparing to unpack .../zlib1g-dev_1%3a1.2.11.dfsg-2ubuntu1.2_amd64.deb ...
Unpacking zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu1.2) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntu1.2) ...
Processing triggers for man-db (2.9.1-1) ...
```

5. Install ruby using the below commands:

```
riemann@riemann-VirtualBox:~$ sudo apt install ruby-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  fonts-lato javascript-common libgmp-dev libgmpxx4ldbl libjs-jquery
```

```
riemann@riemann-VirtualBox:~$ sudo apt install ruby
Reading package lists... Done
Building dependency tree
Reading state information... Done
ruby is already the newest version (1:2.7+1).
ruby set to manually installed.
The following package was automatically installed and is no longer required:
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
riemann@riemann-VirtualBox:~$
```

6. Install java using the below command:

```
sudo apt install default-jdk
```

7. Install Riemann tools

```
riemann@riemann-VirtualBox:~$ sudo gem install riemann-tools
Fetching json-1.8.6.gem
Fetching riemann-client-0.2.6.gem
Fetching optimist-3.0.1.gem
Fetching trollop-2.9.10.gem
Fetching beefcake-1.0.0.gem
Fetching riemann-tools-0.2.14.gem
Fetching mtrc-0.0.4.gem
Building native extensions. This could take a while...
Successfully installed json-1.8.6
Successfully installed optimist-3.0.1
Successfully installed mtrc-0.0.4
!     The 'trollop' gem has been deprecated and has been replaced by 'optimist'.
!     See: https://rubygems.org/gems/optimist
!     And: https://github.com/ManageIQ/optimist
Successfully installed trollop-2.9.10
Successfully installed beefcake-1.0.0
Successfully installed riemann-client-0.2.6
Successfully installed riemann-tools-0.2.14
Parsing documentation for json-1.8.6
Installing ri documentation for json-1.8.6
Parsing documentation for optimist-3.0.1
```

8. Install Riemann client

```
Installing ri documentation for riemann-tools-0.2.14
Done installing documentation for json, optimist, mtrc, trollop, beefcake, riemann-client, riemann-tools after 1 seconds
7 gems installed
riemann@riemann-VirtualBox:~$ sudo gem install riemann-client
Successfully installed riemann-client-0.2.6
Parsing documentation for riemann-client-0.2.6
Done installing documentation for riemann-client after 0 seconds
1 gem installed
riemann@riemann-VirtualBox:~$
```

9. Install Riemann dashboard

```
riemann@riemann-VirtualBox:~$ sudo gem install riemann-dash
Fetching multi_json-1.3.6.gem
Fetching webrick-1.3.1.gem
Fetching ffi-1.15.5.gem
Fetching rb-inotify-0.10.1.gem
Fetching rb-fsevent-0.11.1.gem
Fetching sass-listen-4.0.0.gem
Fetching sass-3.7.4.gem
Fetching rack-1.6.13.gem
Fetching riemann-dash-0.2.14.gem
Fetching rack-protection-1.5.5.gem
Fetching tilt-2.0.10.gem
Fetching sinatra-1.4.8.gem
Fetching erubis-2.7.0.gem
Successfully installed multi_json-1.3.6
Successfully installed webrick-1.3.1
Building native extensions. This could take a while...
Successfully installed ffi-1.15.5
Successfully installed rb-inotify-0.10.1
Successfully installed rb-fsevent-0.11.1
Successfully installed sass-listen-4.0.0
```

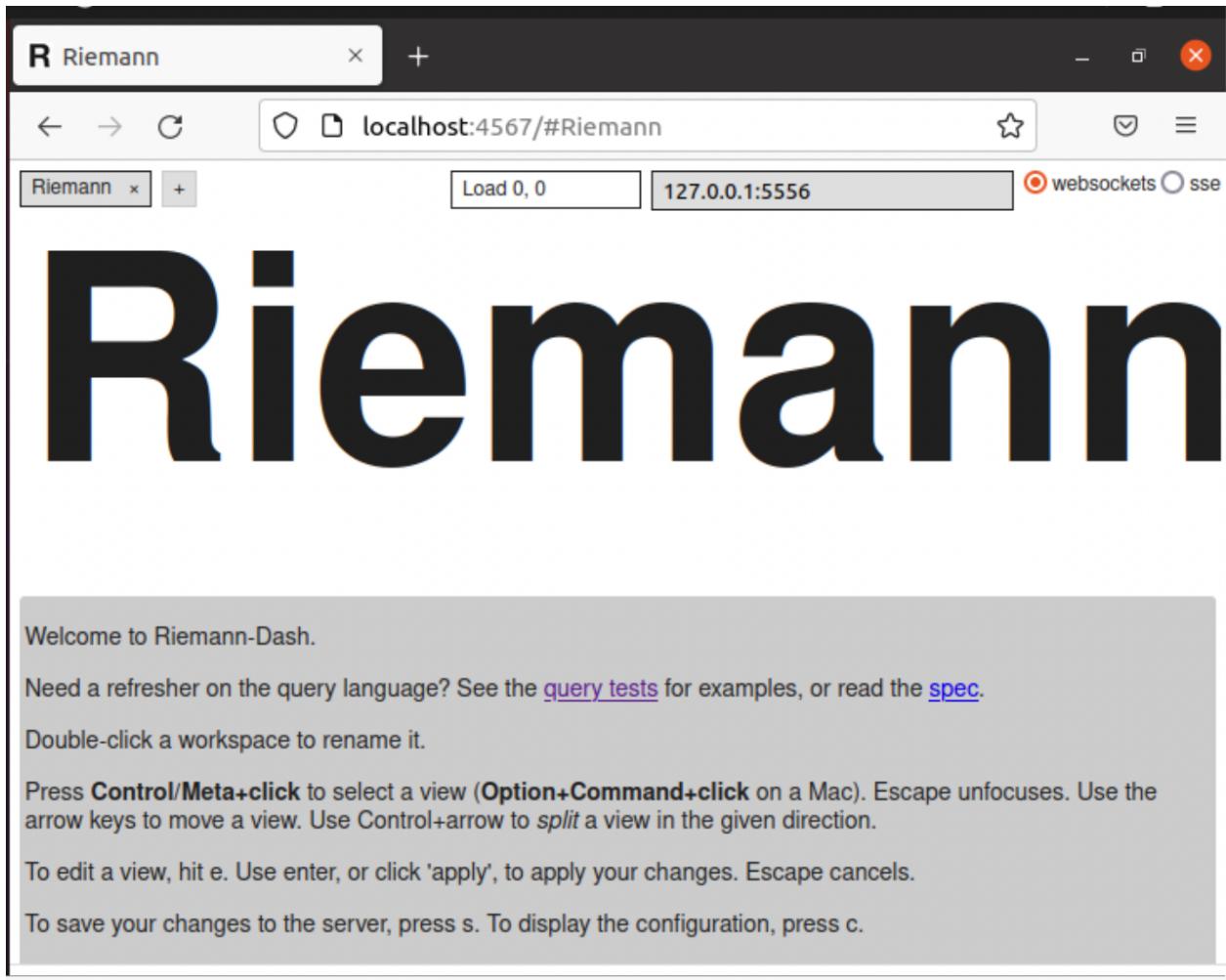
10. Now cd into riemann-0.3.8 and use the below command to start riemann server.

```
riemann@riemann-VirtualBox:~/riemann-0.3.8$ bin/riemann etc/riemann.config
INFO [2022-03-26 21:58:13,288] main - riemann.bin - Loading /home/riemann/riemann-0.3.8/etc/riemann
.config
INFO [2022-03-26 21:58:13,323] main - riemann.bin - PID 1930
INFO [2022-03-26 21:58:13,476] clojure-agent-send-off-pool-2 - riemann.transport.websockets - Webso
ckets server 127.0.0.1 5556 online
INFO [2022-03-26 21:58:13,514] clojure-agent-send-off-pool-0 - riemann.transport.tcp - TCP server 1
27.0.0.1 5555 online
I UbuntuSoftware 6 21:58:13,536] clojure-agent-send-off-pool-3 - riemann.transport.udp - UDP server 1
27.0.0.1 5555 16384 -1 online
INFO [2022-03-26 21:58:13,537] main - riemann.core - Hyperspace core online
INFO [2022-03-26 21:59:08,452] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
:@service disk /boot/efi, :state expired, :time 329662429689/200, :ttl 60}
INFO [2022-03-26 21:59:08,454] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
:@service disk /snap/snap-store/558, :state expired, :time 824156074227/500, :ttl 60}
INFO [2022-03-26 21:59:08,455] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
:@service disk /snap/gnome-3-34-1804/72, :state expired, :time 824156074227/500, :ttl 60}
INFO [2022-03-26 21:59:08,455] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
:@service disk /snap/bare/5, :state expired, :time 329662429691/200, :ttl 60}
INFO [2022-03-26 21:59:08,455] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
:@service memory, :state expired, :time 329662429691/200, :ttl 60}
INFO [2022-03-26 21:59:08,455] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
:@service disk /snap/snapd/15177, :state expired, :time 329662429691/200, :ttl 60}
INFO [2022-03-26 21:59:08,455] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
:@service disk /snap/snap-store/547, :state expired, :time 329662429691/200, :ttl 60}
INFO [2022-03-26 21:59:08,455] riemann task 3 - riemann.config - expired {:@host riemann-VirtualBox,
```

11. Use the below command to start riemann dash

```
riemann@riemann-VirtualBox:~$ riemann-dash
No configuration loaded; using defaults.
[2022-03-26 11:38:53] INFO  WEBrick 1.3.1
[2022-03-26 11:38:53] INFO  ruby 2.7.0 (2019-12-25) [x86_64-linux-gnu]
== Sinatra (v1.4.8) has taken the stage on 4567 for development with backup from WEBrick
[2022-03-26 11:38:53] INFO  WEBrick::HTTPServer#start: pid=13667 port=4567
localhost - - [26/Mar/2022:11:39:03 IST] "GET / HTTP/1.1" 200 2730
- -> /
localhost - - [26/Mar/2022:11:39:03 IST] "GET /vendor/toastr/toastr.css HTTP/1.1" 200 5259
http://localhost:4567/ -> /vendor/toastr/toastr.css
localhost - - [26/Mar/2022:11:39:03 IST] "GET /vendor/smoothie.js HTTP/1.1" 200 15858
http://localhost:4567/ -> /vendor/smoothie.js
localhost - - [26/Mar/2022:11:39:03 IST] "GET /vendor/lodash.min.js HTTP/1.1" 200 19265
http://localhost:4567/ -> /vendor/lodash.min.js
localhost - - [26/Mar/2022:11:39:03 IST] "GET /vendor/jquery/jquery.simplemodal.1.4.4.min.js HTTP/1.1" 200 9776
http://localhost:4567/ -> /vendor/jquery/jquery.simplemodal.1.4.4.min.js
localhost - - [26/Mar/2022:11:39:03 IST] "GET /vendor/jquery/jquery.quickfit.js HTTP/1.1" 200 4903
http://localhost:4567/ -> /vendor/jquery/jquery.quickfit.js
localhost - - [26/Mar/2022:11:39:03 IST] "GET /vendor/toastr/toastr.js HTTP/1.1" 200 8418
http://localhost:4567/ -> /vendor/toastr/toastr.js
localhost - - [26/Mar/2022:11:39:03 IST] "GET /css HTTP/1.1" 200 8535
```

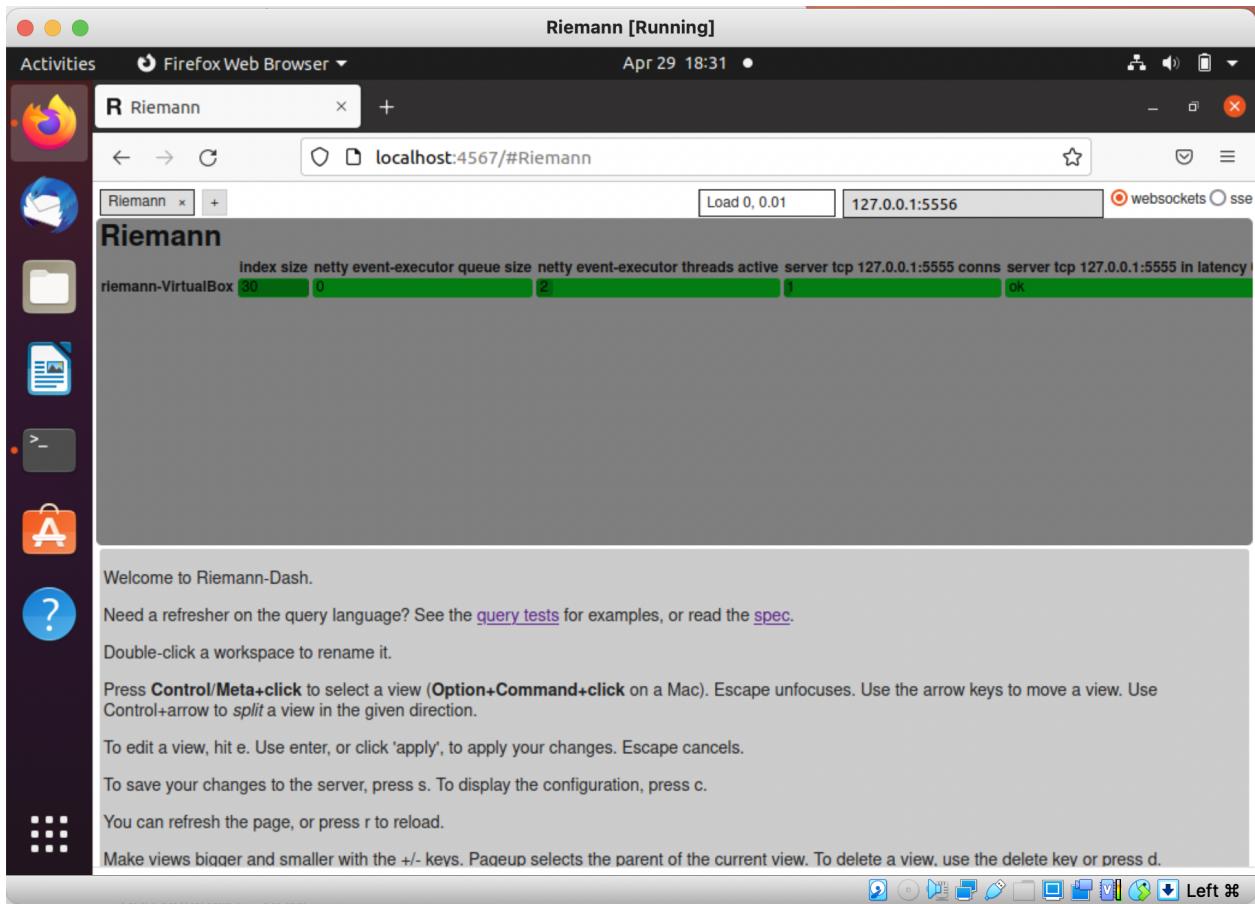
12. Now do your browser and type **localhost:4567** to open riemann dashboard.



Press Control + Click to select a view

Press e

Select Grid and write query as true and you will be getting this desired output.



- bring up toy riemann server whose job is to print/log events to stdout as events come

In the riemann.config file provide the (streams index) to print log events to stdout as events come.

```
(let [index (index)]
  ; Inbound events will be passed to these streams:
  (streams
    (default :ttl 60
      ; Index all events immediately.
      index

      ; Log expired events.
      (expired
        (fn [event] (info "expired" event))))))
```

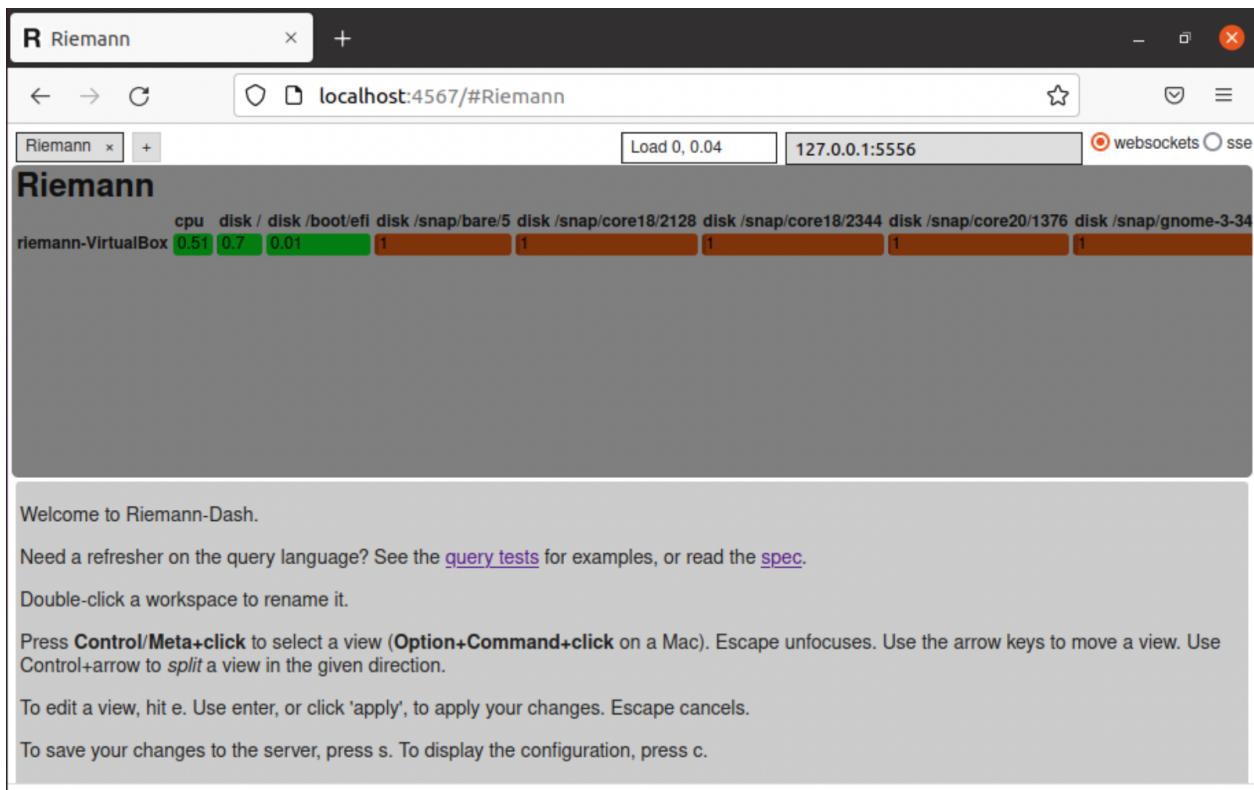
Write a plugin/script in a language of your choice to monitor server load avg every min and send as event to riemann

Plugin:

riemann-health daemon is a little Ruby program that submits events about the state of your CPU, memory, load, and disks to a Riemann server. If you switch back to the dashboard, you'll see your local host's state appear.

1. Set your dashboard in grid view Hold CTRL (or OPTION/META depending on your OS) and click the big title "Riemann" in the top pane. The title will be shaded grey to indicate that view is selected. Then, press "e" to edit, and change "Title" to "Grid" and type true in the query field and click on apply.
2. Now on your terminal use Riemann-health command to start the program which submits load avg every min to riemann dashboard.

```
riemann@riemann-VirtualBox:~/riemann-0.3.8$ riemann-health
```



Script:

1. Install these dependencies:-

```
pip3 install riemann-client
```

```
sudo pip install —upgrade pip
```

```
pip install psutil
```

```
pip3 install psutil
```

2. Write the below riemann_script.py

```
import time
import psutil
import riemann_client.client
from riemann_client.transport import TCPTTransport
from yaml import load

def send_event():
    load = psutil.cpu_percent(percpu=False)
    with riemann_client.client.Client(TCPTTransport("localhost",5555)) as client:
        if load<70:
            client.event(host="localhost",service="avg_server_load",state="ok",metric_f=load)
        if load>70 and load<90:
            client.event(host="localhost",service="avg_server_load",state="warning",metric_f=load)
        if load>90:
            client.event(host="localhost",service="avg_server_load",state="critical",metric_f=load)

if __name__ == "__main__":
    while True:
        send_event()
        time.sleep(10)
```

3. Run the script using python3 riemann_script.py and go to dashboard and Hold CTRL click the big title "Riemann" in the top pane. The title will be shaded grey to indicate that view is selected. Then, press "e" to edit and change title to gauge and type true in query and click on apply.

Setup riemann-dashboard that displays riemann's index (in memory state of current events) and create a dashboard to see load event being sent

1. Now you will be able to see Riemann Dashboard on localhost:4567

Welcome to Riemann-Dash.

Need a refresher on the query language? See the [query tests](#) for examples, or read the [spec](#).

Double-click a workspace to rename it.

Press **Control/Meta+click** to select a view (**Option+Command+click** on a Mac). Escape unfocuses. Use the arrow keys to move a view. Use Control+arrow to *split* a view in the given direction.

To edit a view, hit e. Use enter, or click 'apply', to apply your changes. Escape cancels.

To save your changes to the server, press s. To display the configuration, press c.

You can refresh the page, or press r to reload.

Make views bigger and smaller with the +/- keys. Pageup selects the parent of the current view. To delete a view, use the delete key or press d.

Welcome to Riemann-Dash.

Need a refresher on the query language? See the [query tests](#) for examples, or read the [spec](#).

Double-click a workspace to rename it.

Press **Control/Meta+click** to select a view (**Option+Command+click** on a Mac). Escape unfocuses. Use the arrow keys to move a view. Use Control+arrow to *split* a view in the given direction.

To edit a view, hit e. Use enter, or click 'apply', to apply your changes. Escape cancels.

To save your changes to the server, press s. To display the configuration, press c.

You can refresh the page, or press r to reload.

Make views bigger and smaller with the +/- keys. Pageup selects the parent of the current view. To delete a view, use the delete key or press d.