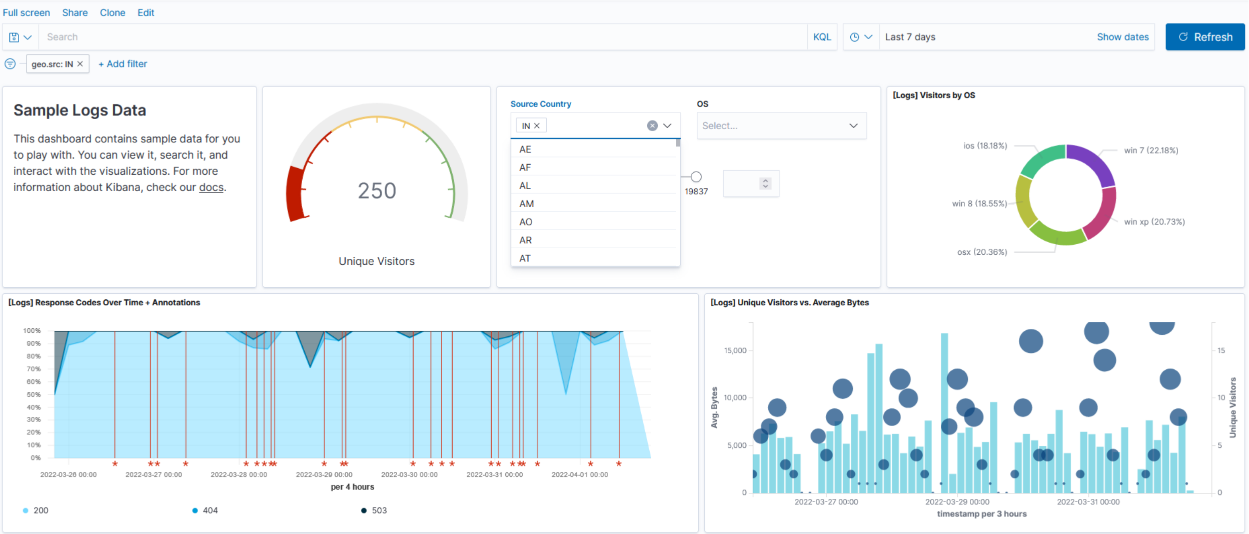
1. In the last 7 days, how many unique visitors were located in India?

250



Last 7 days

geo.src: IN ×

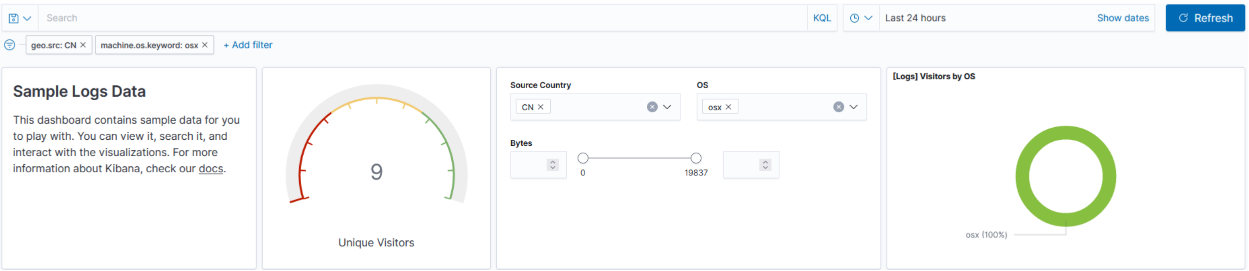
Source Country: IN ×

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

2. In the last 24 hours, of the visitors from China, how many were using Mac OSX?

9 individuals were using Mac OSX (17.31%) from China



Last 24 hours

geo.src: CN × machine.os.keyword: osx ×

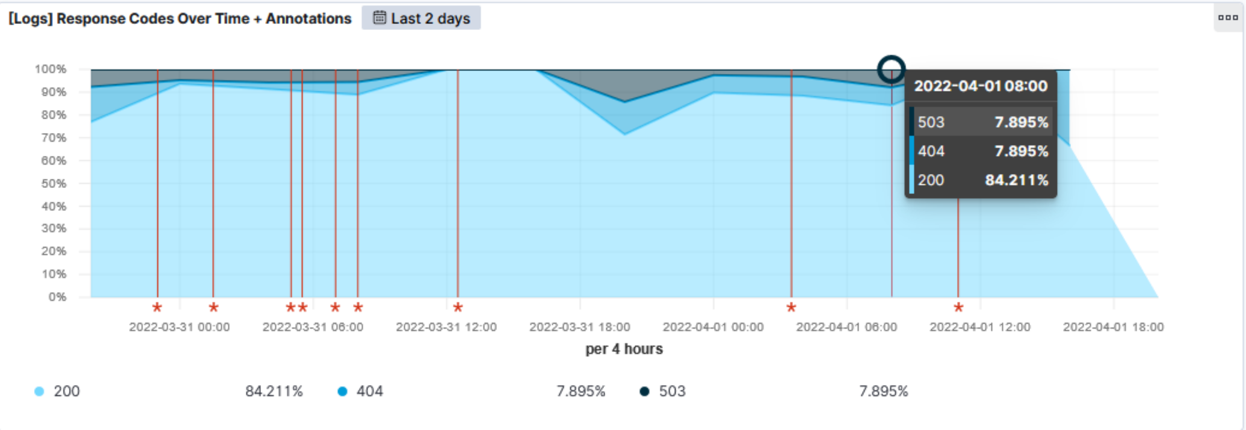
Source Country: CN × OS: osx ×

Sample Logs Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

3. In the last two days, what percentage of visitors received 404 errors? How about 503 errors?

In the last two days, there were 7.895% of 404 errors and 7.895% of 503 errors.



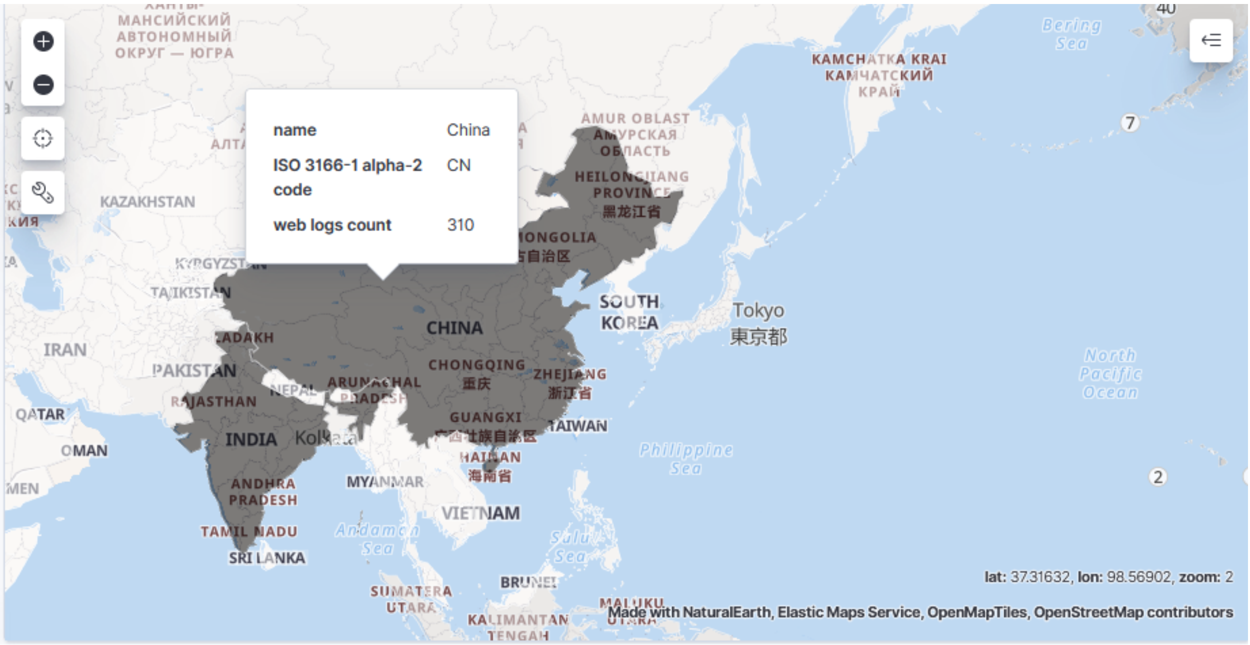
2022-04-01 08:00

```
503   7.895%
404   7.895%
200   84.211%
```

```
● 200        84.211%    ● 404        7.895%    ● 503        7.895%
```

4. In the last seven days, what country produced the majority of the traffic on the website?

China produced the most traffic in the last seven days.



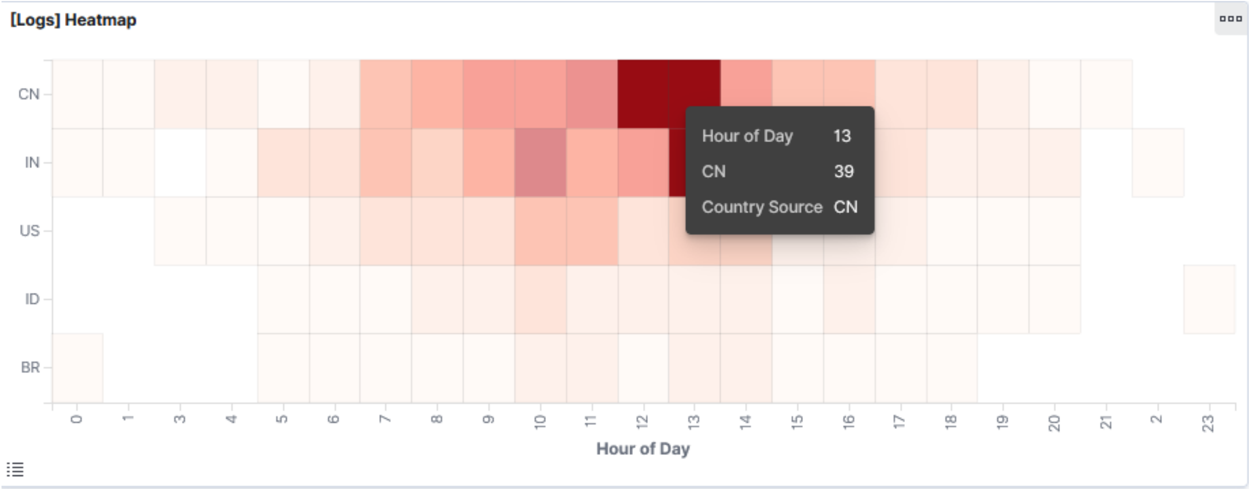
name	China
ISO 3166-1 alpha-2 code	CN
web logs count	310

lat: 37.31632, lon: 98.56902, zoom: 2

Made with NaturalEarth, Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

5. Of the traffic that's coming from that country, what time of day had the highest amount of activity?

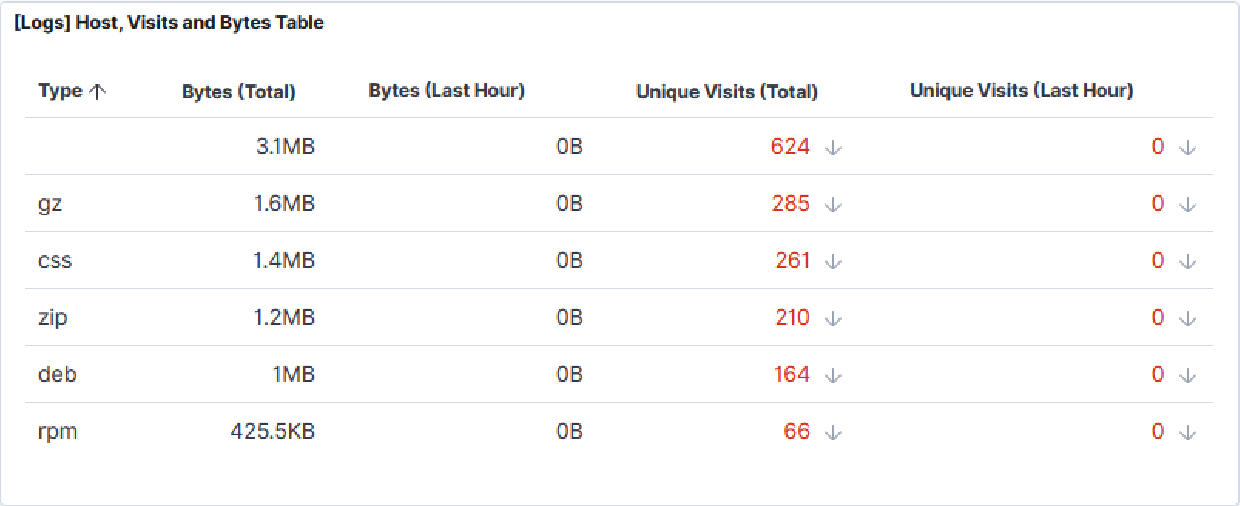
Between hours 12 and 13 as shown on the heat map.



[Logs] Heatmap

Hour of Day	13
CN	39
Country Source	CN

6. List all the types of downloaded files that have been identified for the last 7 days and a short description of each.



[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
	3.1MB	0B	624 ↓	0 ↓
gz	1.6MB	0B	285 ↓	0 ↓
css	1.4MB	0B	261 ↓	0 ↓
zip	1.2MB	0B	210 ↓	0 ↓
deb	1MB	0B	164 ↓	0 ↓
rpm	425.5KB	0B	66 ↓	0 ↓

Gz: compressed archive files by using gzip

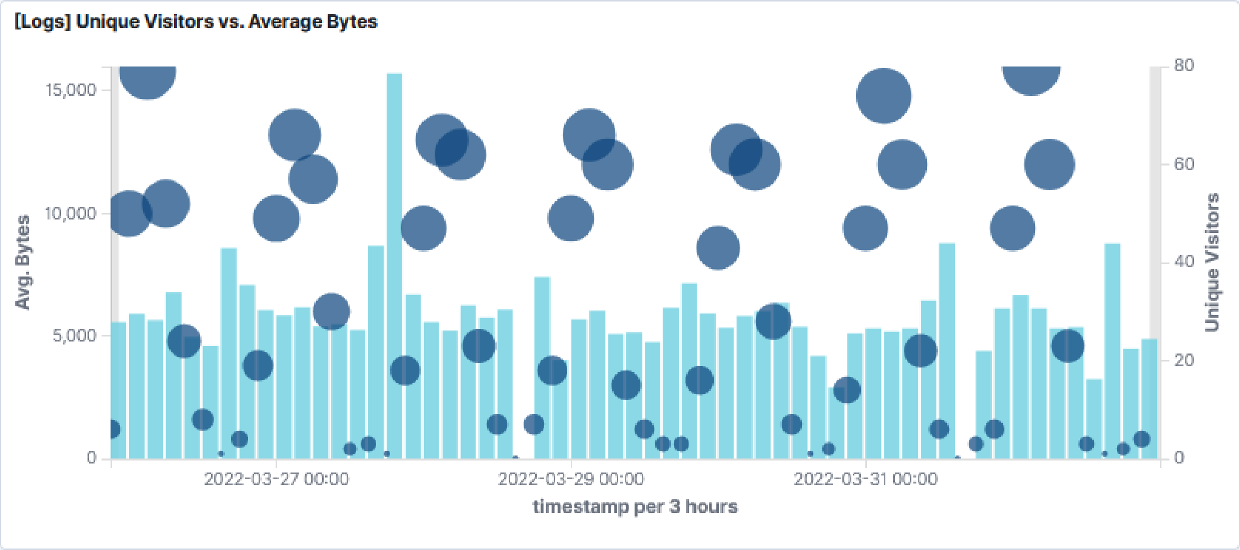
Css: a cascading style sheets file describes HTML elements

Zip: several files that are compressed together into one location

Deb: a debian software package file that installs or updates applications

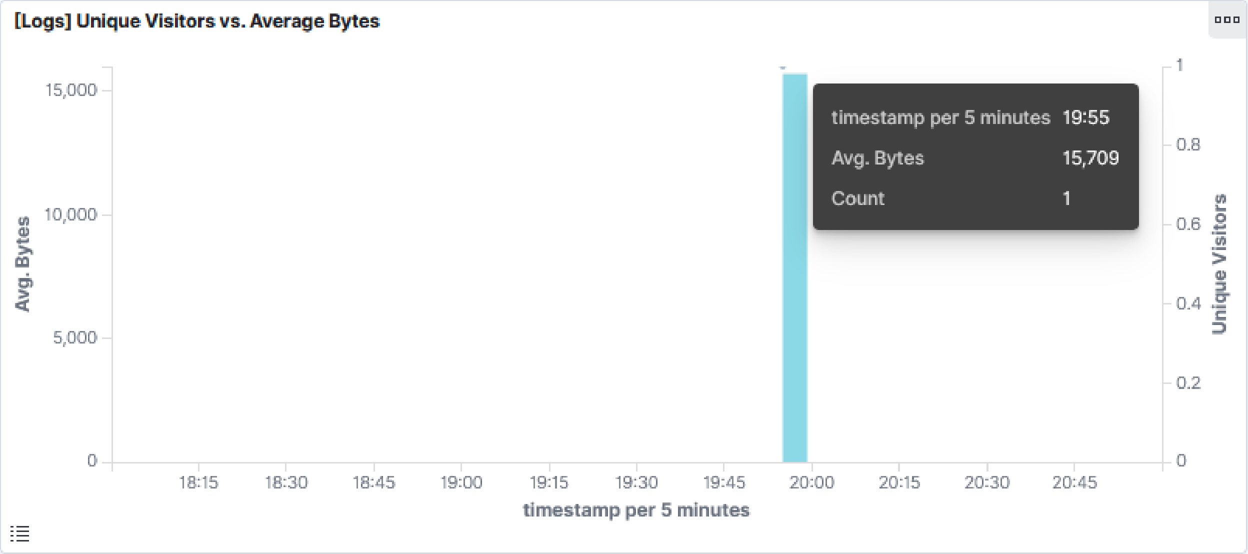
Rpm: a file that is connected to the Red Hat Package Manager and used to store installation packages

7. Unique Visitors vs. Average Bytes in the last seven days. Is there anything that seems potentially strange about this activity?



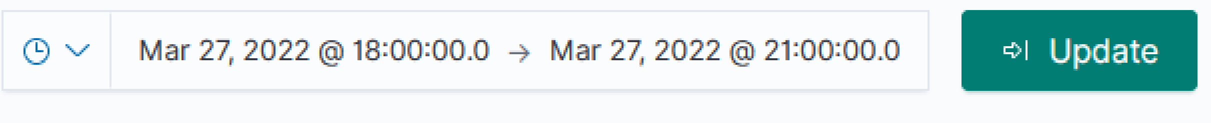
[Logs] Unique Visitors vs. Average Bytes

The photo below shows one visitor using an exorbitant amount of bytes (15,709) compared to all other unique visitors



Filtered Data

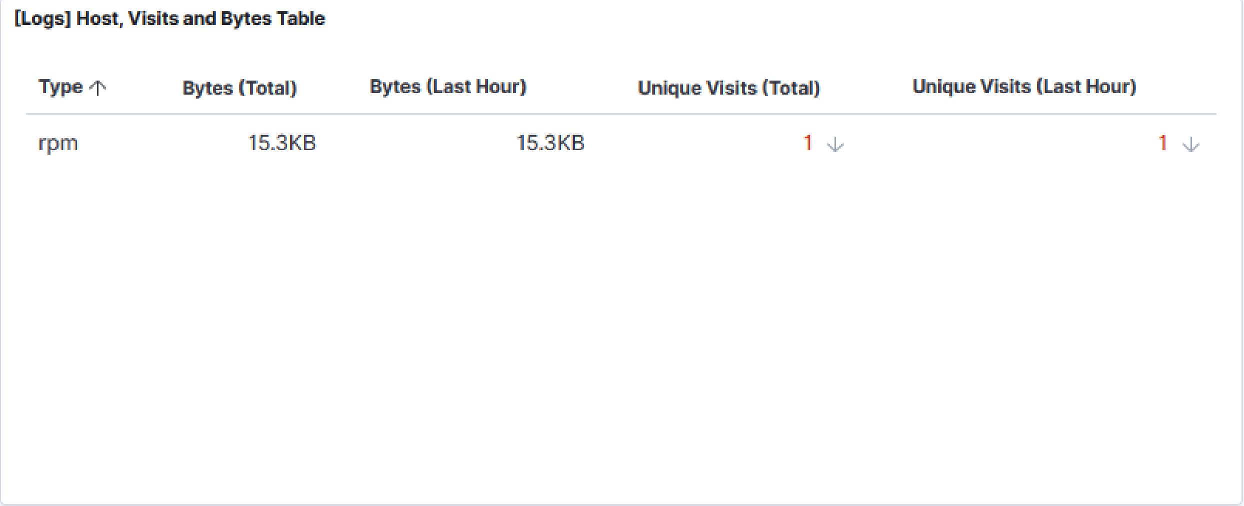
1. What is the timestamp for this event?



Mar 27, 2022 @ 18:00:00.0 → Mar 27, 2022 @ 21:00:00.0

2. What kind of file was downloaded?

RPM file

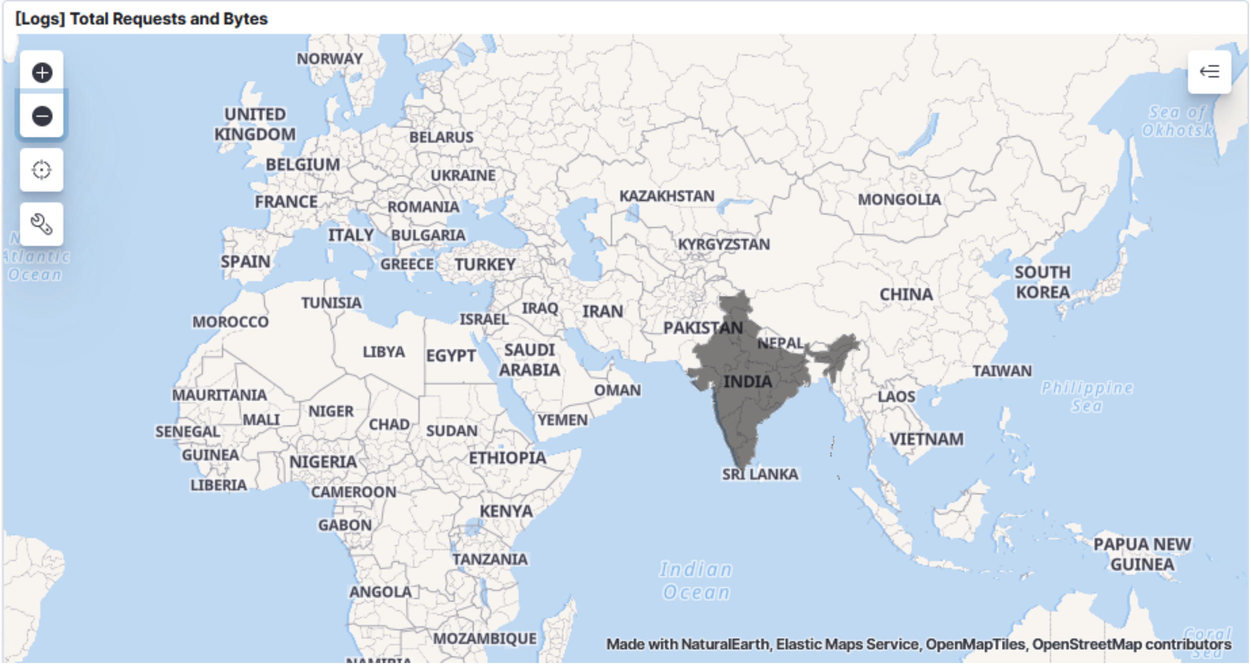


[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
rpm	15.3KB	15.3KB	1 ↓	1 ↓

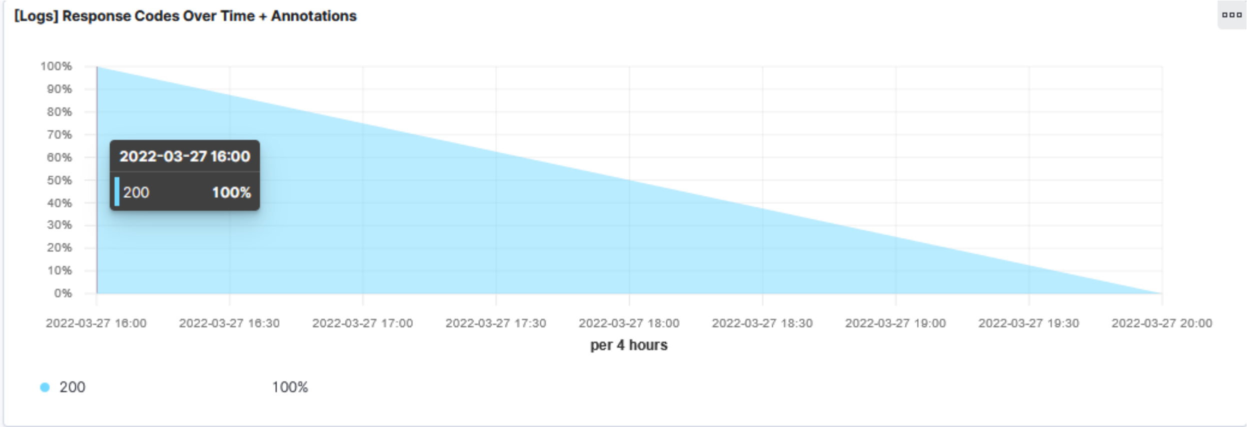
3. From what country did this activity originate from?

India.



4. What HTTP response codes were encountered by this visitor?

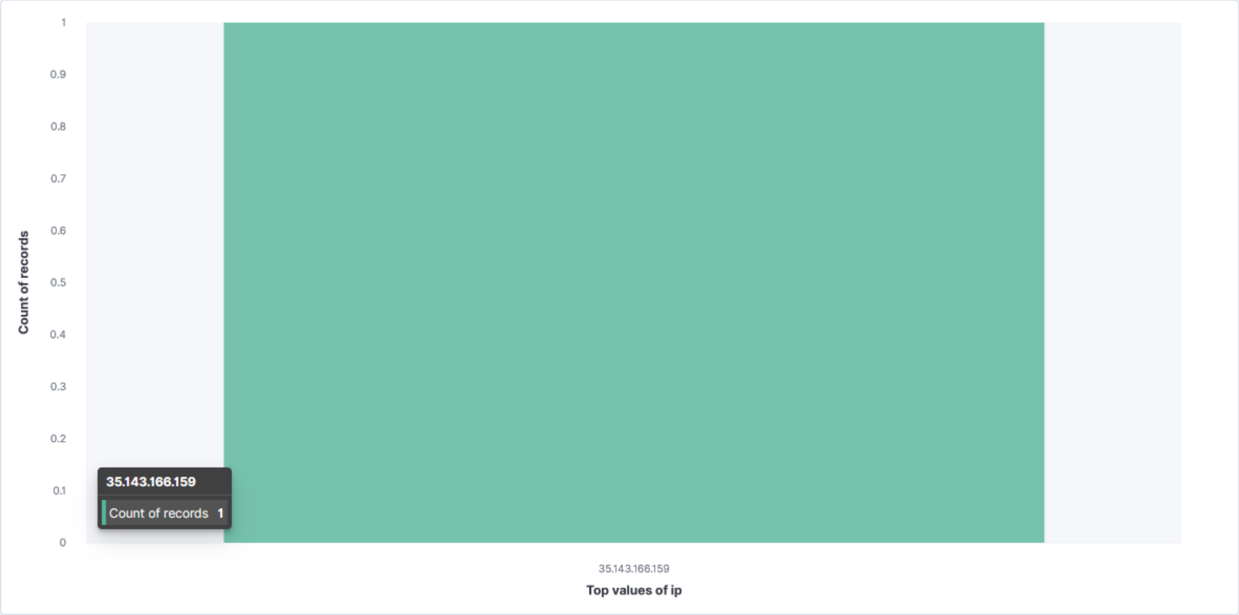
200



Kibana Discover Page

1. What is the source IP address of this activity?

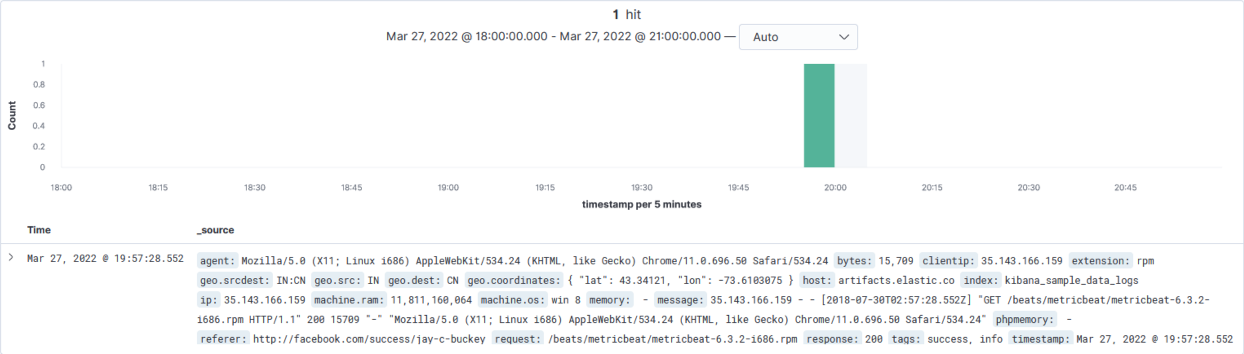
The IP is 35.143.166.159.



2. What are the geo coordinates of this activity?

The geo coordinates are lat: 43.34121, lon: -73.6103075

3. What OS was the source machine running?

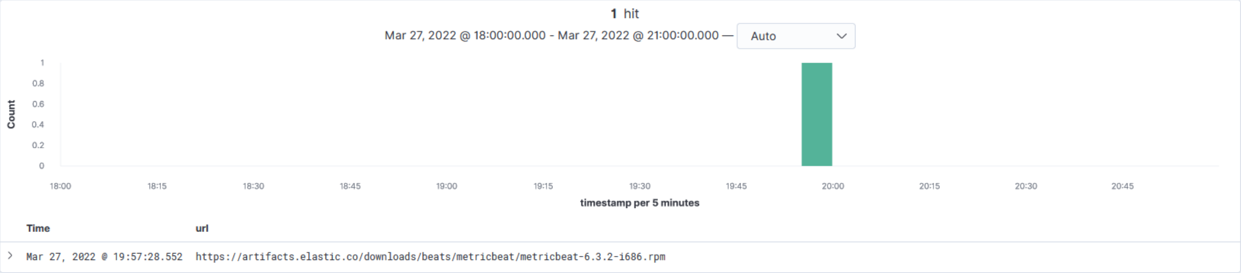


```
Time                          _source
> Mar 27, 2022 @ 19:57:28.552 agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 bytes: 15,709 clientip: 35.143.166.159 extension: rpm
                              geo.srcdest: IN:CN geo.src: IN geo.dest: CN geo.coordinates: { "lat": 43.34121, "lon": -73.6103075 } host: artifacts.elastic.co index: kibana_sample_data_logs
                              ip: 35.143.166.159 machine.ram: 11,811,160,064 machine.os: win 8 memory:  - message: 35.143.166.159 - - [2018-07-30T02:57:28.552Z] "GET /beats/metricbeat/metricbeat-6.3.2-
                              i686.rpm HTTP/1.1" 200 15709 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24" phpmemory:  -
                              referer: http://facebook.com/success/jay-c-buckey request: /beats/metricbeat/metricbeat-6.3.2-i686.rpm response: 200 tags: success, info timestamp: Mar 27, 2022 @ 19:57:28.552
```

The machine is running “win 8”, Windows 8.

4. What is the full access URL that was accessed?

https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm



Time	url
Mar 27, 2022 @ 19:57:28.552	https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm

5. From what website did the visitor's traffic originate?

The traffic originated from facebook: http://facebook.com/success/jay-c-buckey

Investigation Overview

1. What do you think the user was doing?

I believe the user was attempting to download a Linux package from the site.

2. Was the file they downloaded malicious? If not, what is the file used for?

It doesn't appear to be initially malicious since Linux packages usually perform updates or other non-malicious tasks. They could be hiding something malicious though depending on the source website.

3. Is there anything that seems suspicious about this activity?

Yes because it's very strange they would use/find a package update link from facebook. It doesn't make sense in terms of average traffic, so I would investigate it further.

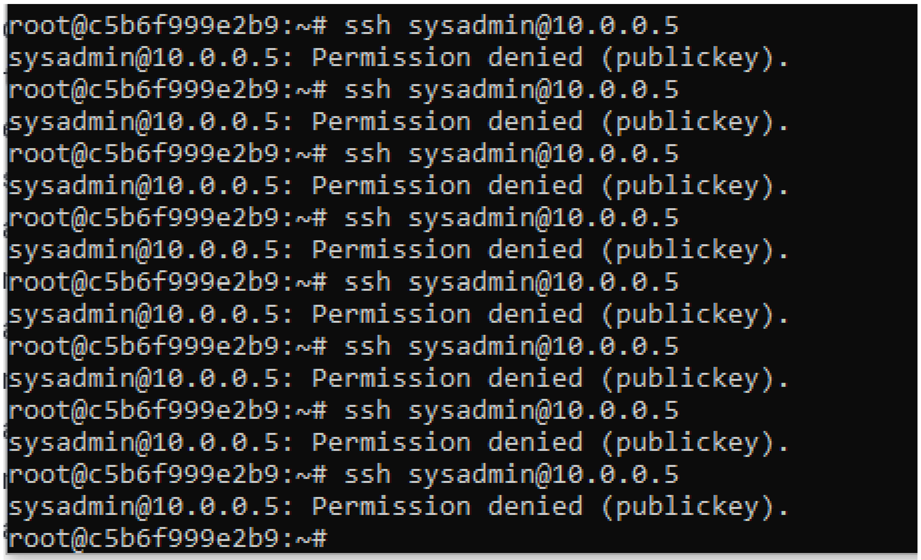
4. Is any of the traffic you inspected potentially outside of compliance guidelines?

I believe so, as it doesn't seem like good practice to allow posts with links about package updates due to high risk of spam/malicious links. It's a social network, not a software update site or otherwise.

KIBANA CONT. - SSH BARRAGE

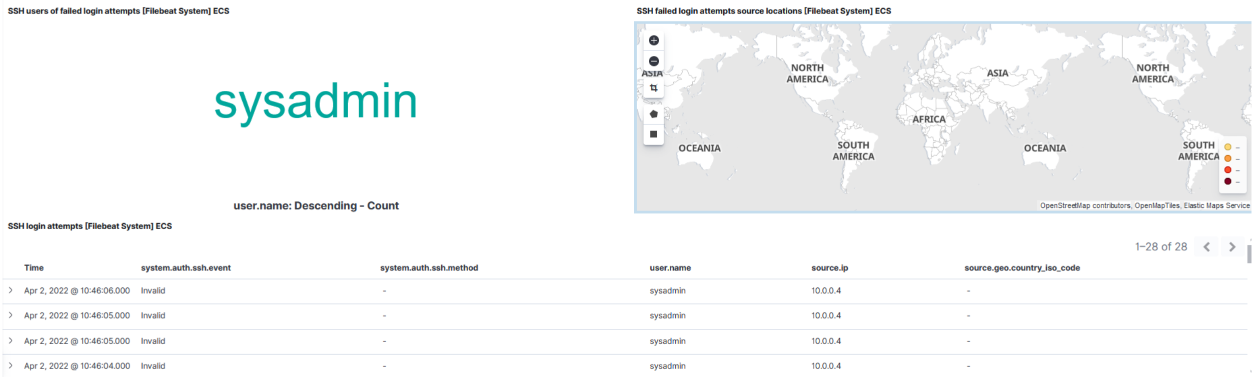
Failed Attempts on Command Line:

Use jump box to attack web machines



```
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~# ssh sysadmin@10.0.0.5
sysadmin@10.0.0.5: Permission denied (publickey).
root@c5b6f999e2b9:~#
```

SSH Login Attempts Data:



SSH users of failed login attempts [Filebeat System] ECS

sysadmin

user.name: Descending - Count

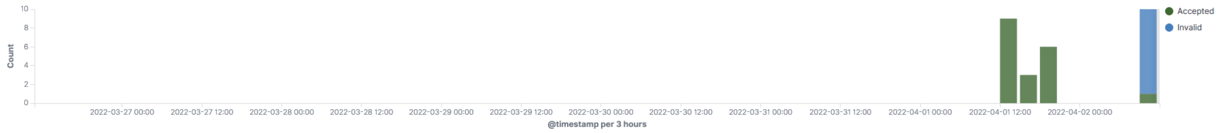
SSH failed login attempts source locations [Filebeat System] ECS

SSH login attempts [Filebeat System] ECS

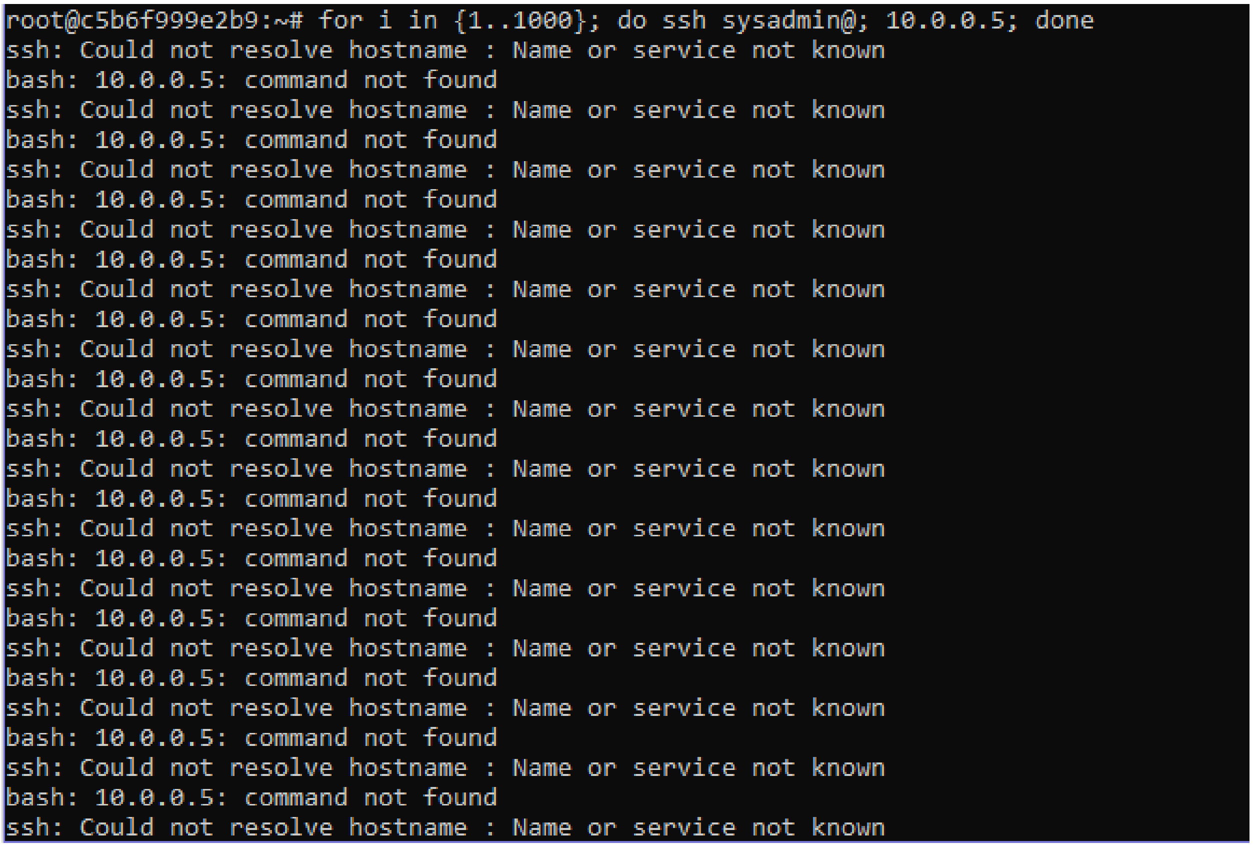
1–28 of 28

Time	system.auth.ssh.event	system.auth.ssh.method	user.name	source.ip	source.geo.country_iso_code
Apr 2, 2022 @ 10:46:06.000	Invalid	-	sysadmin	10.0.0.4	-
Apr 2, 2022 @ 10:46:05.000	Invalid	-	sysadmin	10.0.0.4	-
Apr 2, 2022 @ 10:46:05.000	Invalid	-	sysadmin	10.0.0.4	-
Apr 2, 2022 @ 10:46:04.000	Invalid	-	sysadmin	10.0.0.4	-

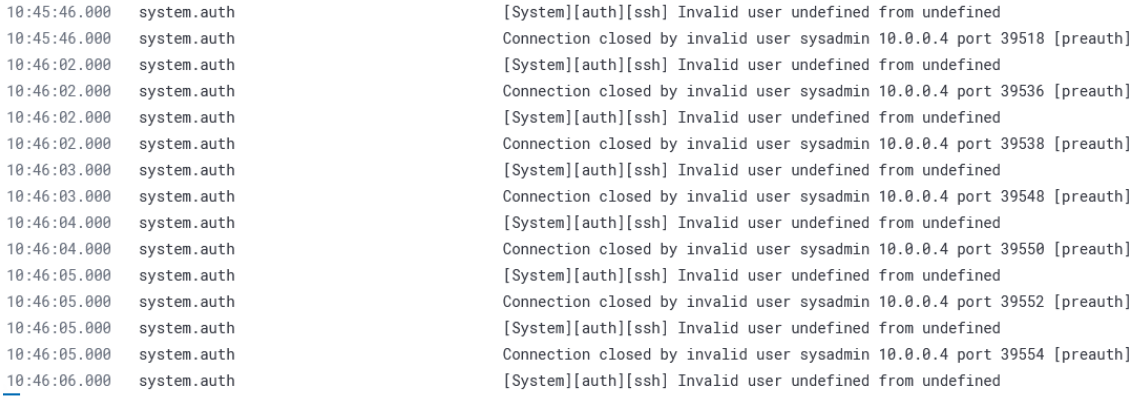
SSH login attempts [Filebeat System] ECS



FAILED LOGIN LOG ENTRIES



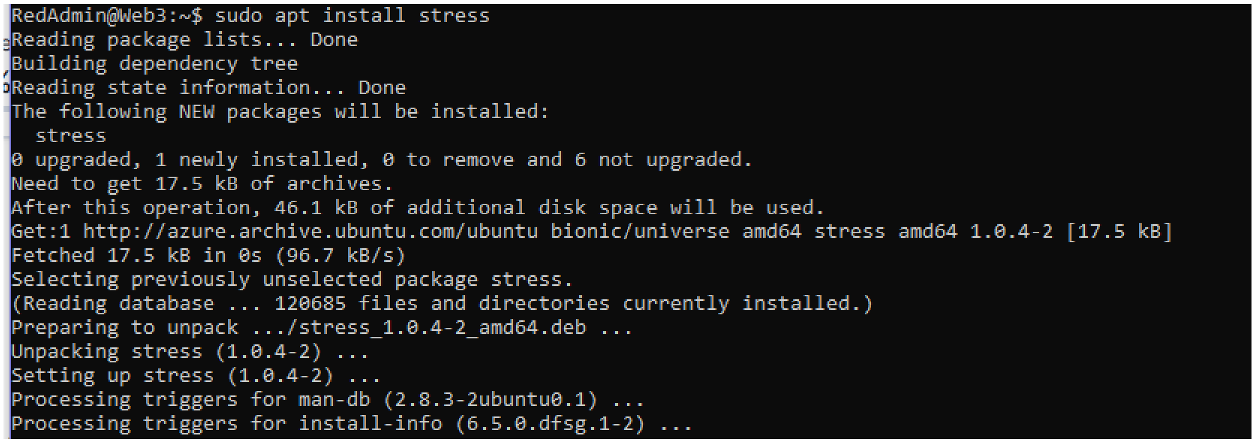
```
root@c5b6f999e2b9:~# for i in {1..1000}; do ssh sysadmin@; 10.0.0.5; done
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
bash: 10.0.0.5: command not found
ssh: Could not resolve hostname : Name or service not known
```



```
10:45:46.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
10:45:46.000   system.auth          Connection closed by invalid user sysadmin 10.0.0.4 port 39518 [preauth]
10:46:02.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
10:46:02.000   system.auth          Connection closed by invalid user sysadmin 10.0.0.4 port 39536 [preauth]
10:46:02.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
10:46:02.000   system.auth          Connection closed by invalid user sysadmin 10.0.0.4 port 39538 [preauth]
10:46:03.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
10:46:03.000   system.auth          Connection closed by invalid user sysadmin 10.0.0.4 port 39548 [preauth]
10:46:04.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
10:46:04.000   system.auth          Connection closed by invalid user sysadmin 10.0.0.4 port 39550 [preauth]
10:46:05.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
10:46:05.000   system.auth          Connection closed by invalid user sysadmin 10.0.0.4 port 39552 [preauth]
10:46:05.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
10:46:05.000   system.auth          Connection closed by invalid user sysadmin 10.0.0.4 port 39554 [preauth]
10:46:06.000   system.auth          [System][auth][ssh] Invalid user undefined from undefined
```

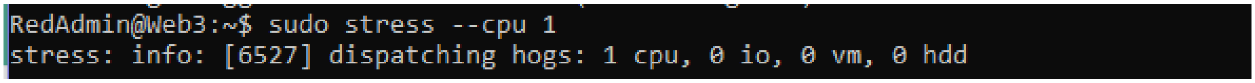
LINUX STRESS

Sudo apt install stress



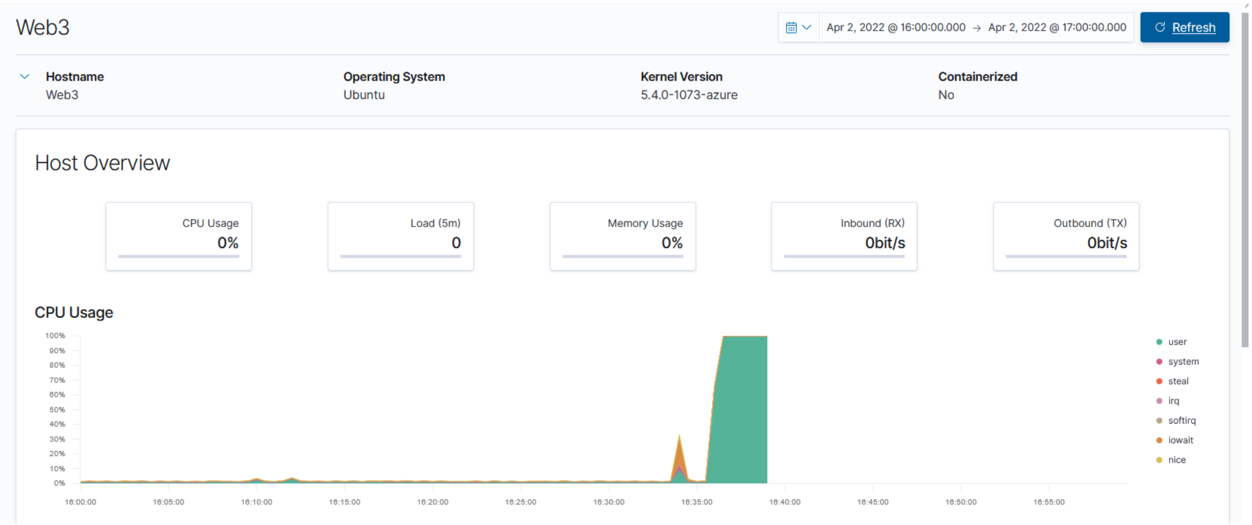
```
RedAdmin@Web3:~$ sudo apt install stress
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  stress
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.
Need to get 17.5 kB of archives.
After this operation, 46.1 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 stress amd64 1.0.4-2 [17.5 kB]
Fetched 17.5 kB in 0s (96.7 kB/s)
Selecting previously unselected package stress.
(Reading database ... 120685 files and directories currently installed.)
Preparing to unpack .../stress_1.0.4-2_amd64.deb ...
Unpacking stress (1.0.4-2) ...
Setting up stress (1.0.4-2) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for install-info (6.5.0.dfsg.1-2) ...
```

Sudo stress



```
RedAdmin@Web3:~$ sudo stress --cpu 1
stress: info: [6527] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
```

Web 3 Usage Change



Web3

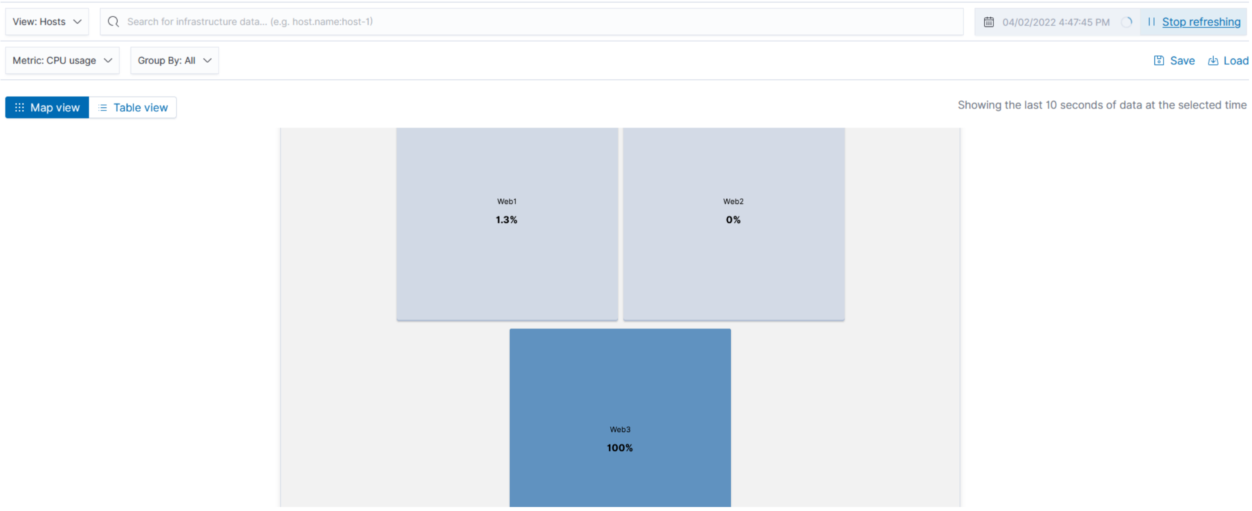
Apr 2, 2022 @ 16:00:00.000 → Apr 2, 2022 @ 17:00:00.000

Hostname	Operating System	Kernel Version	Containerized
Web3	Ubuntu	5.4.0-1073-azure	No

Host Overview

CPU Usage	Load (5m)	Memory Usage	Inbound (RX)	Outbound (TX)
0%	0	0%	0bit/s	0bit/s

CPU Usage



View: Hosts

Metric: CPU usage

Group By: All

04/02/2022 4:47:45 PM

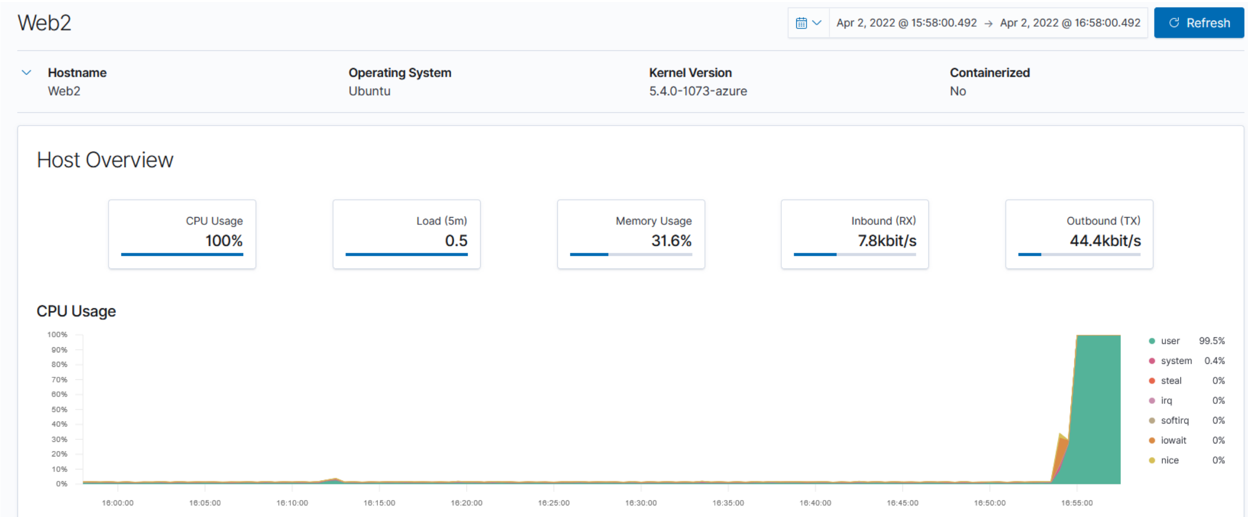
Showing the last 10 seconds of data at the selected time

Web1
1.3%

Web2
0%

Web3
100%

Web 2 Usage



Web2

Apr 2, 2022 @ 15:58:00.492 → Apr 2, 2022 @ 16:58:00.492

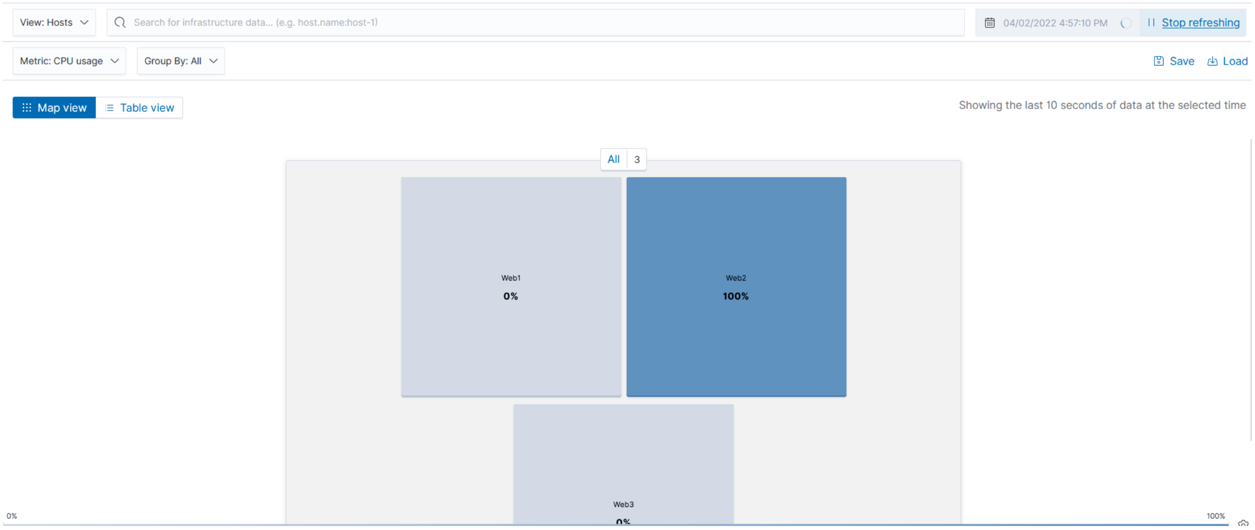
Hostname	Operating System	Kernel Version	Containerized
Web2	Ubuntu	5.4.0-1073-azure	No

Host Overview

CPU Usage	Load (5m)	Memory Usage	Inbound (RX)	Outbound (TX)
100%	0.5	31.6%	7.8kbit/s	44.4kbit/s

CPU Usage

● user	99.5%
● system	0.4%
● steal	0%
● irq	0%
● softirq	0%
● iowait	0%
● nice	0%

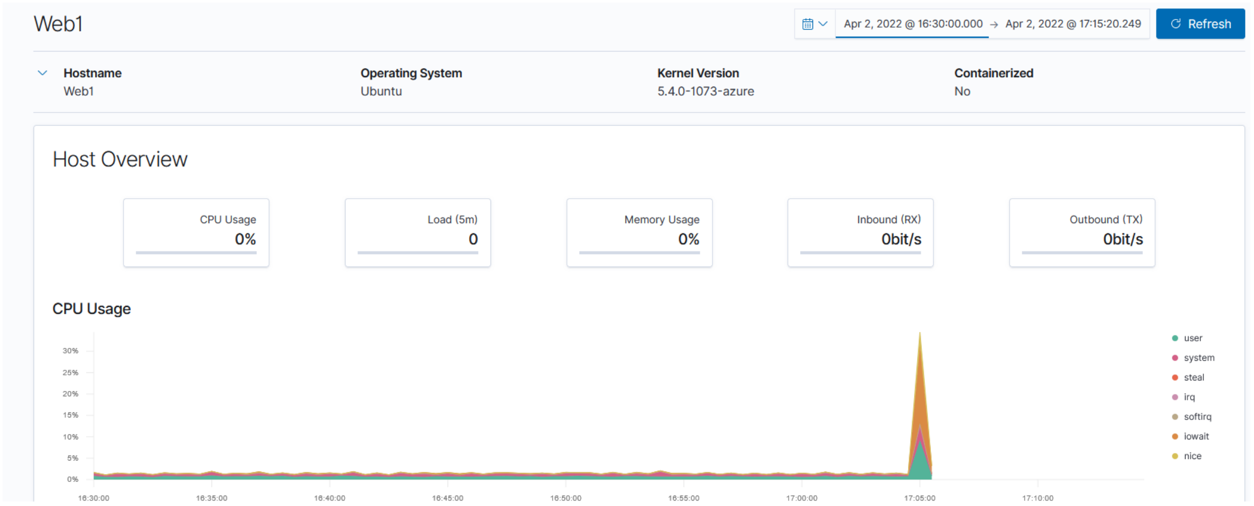


View: Hosts | Search for infrastructure data... (e.g. host.name:host-1) | 04/02/2022 4:57:10 PM | Stop refreshing

Metric: CPU usage | Group By: All | Save | Load

Map view | Table view | Showing the last 10 seconds of data at the selected time

Web 1 Usage



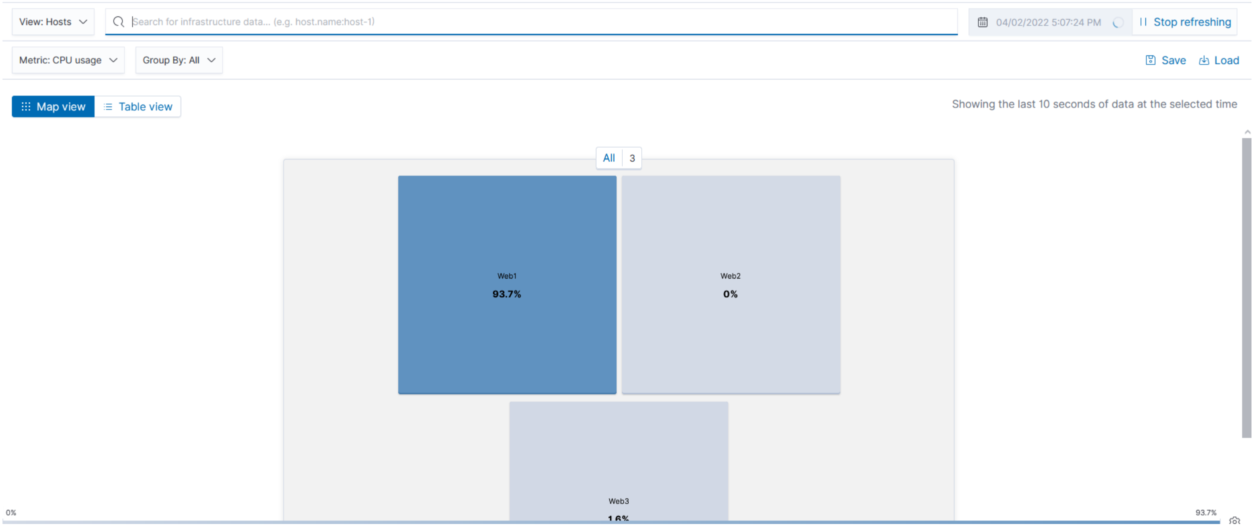
Web1 | Apr 2, 2022 @ 16:30:00.000 → Apr 2, 2022 @ 17:15:20.249 | Refresh

Hostname	Operating System	Kernel Version	Containerized
Web1	Ubuntu	5.4.0-1073-azure	No

Host Overview

CPU Usage	Load (5m)	Memory Usage	Inbound (RX)	Outbound (TX)
0%	0	0%	0bit/s	0bit/s

CPU Usage



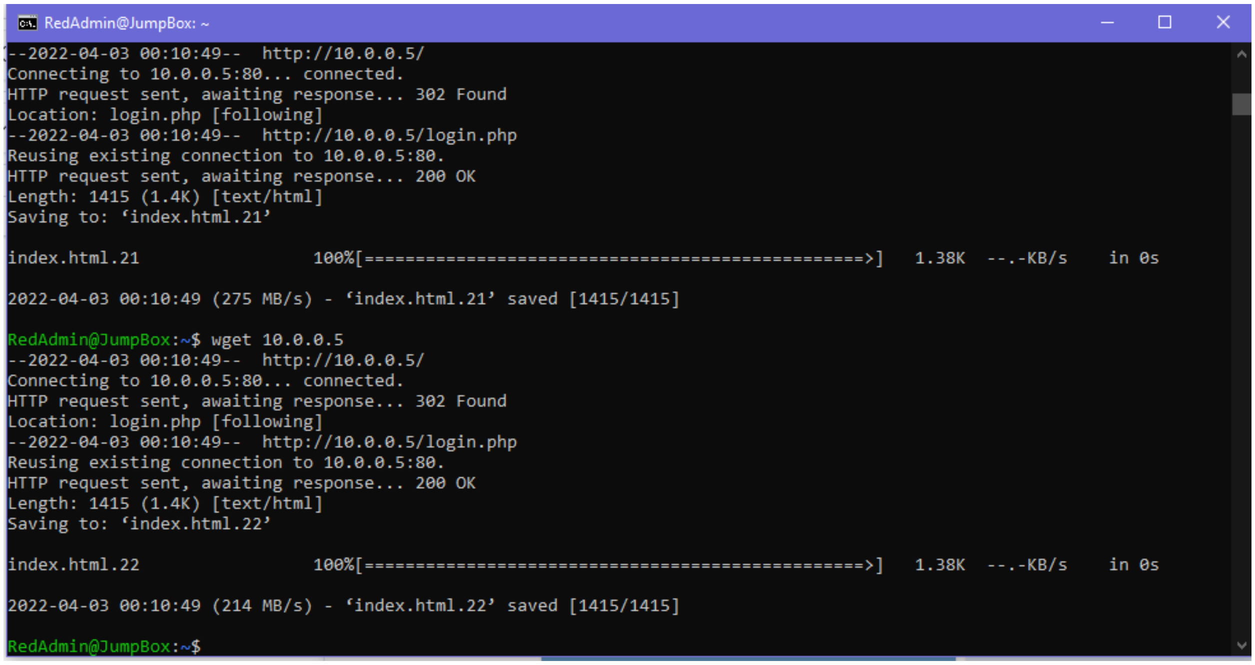
View: Hosts | Search for infrastructure data... (e.g. host.name:host-1) | 04/02/2022 5:07:24 PM | Stop refreshing

Metric: CPU usage | Group By: All | Save | Load

Map view | Table view | Showing the last 10 seconds of data at the selected time

Wget-DoS

Wget 10.0.0.5
Ls (view files downloaded from web vm to jump box)
Wget [ip] loop (many files are created):



```
--2022-04-03 00:10:49--  http://10.0.0.5/
Connecting to 10.0.0.5:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: login.php [following]
--2022-04-03 00:10:49--  http://10.0.0.5/login.php
Reusing existing connection to 10.0.0.5:80.
HTTP request sent, awaiting response... 200 OK
Length: 1415 (1.4K) [text/html]
Saving to: ‘index.html.21’

index.html.21                100%[===============================================>]   1.38K  --.-KB/s    in 0s

2022-04-03 00:10:49 (275 MB/s) - ‘index.html.21’ saved [1415/1415]

RedAdmin@JumpBox:~$ wget 10.0.0.5
--2022-04-03 00:10:49--  http://10.0.0.5/
Connecting to 10.0.0.5:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: login.php [following]
--2022-04-03 00:10:49--  http://10.0.0.5/login.php
Reusing existing connection to 10.0.0.5:80.
HTTP request sent, awaiting response... 200 OK
Length: 1415 (1.4K) [text/html]
Saving to: ‘index.html.22’

index.html.22                100%[===============================================>]   1.38K  --.-KB/s    in 0s

2022-04-03 00:10:49 (214 MB/s) - ‘index.html.22’ saved [1415/1415]

RedAdmin@JumpBox:~$
```

Then all files were deleted when done.