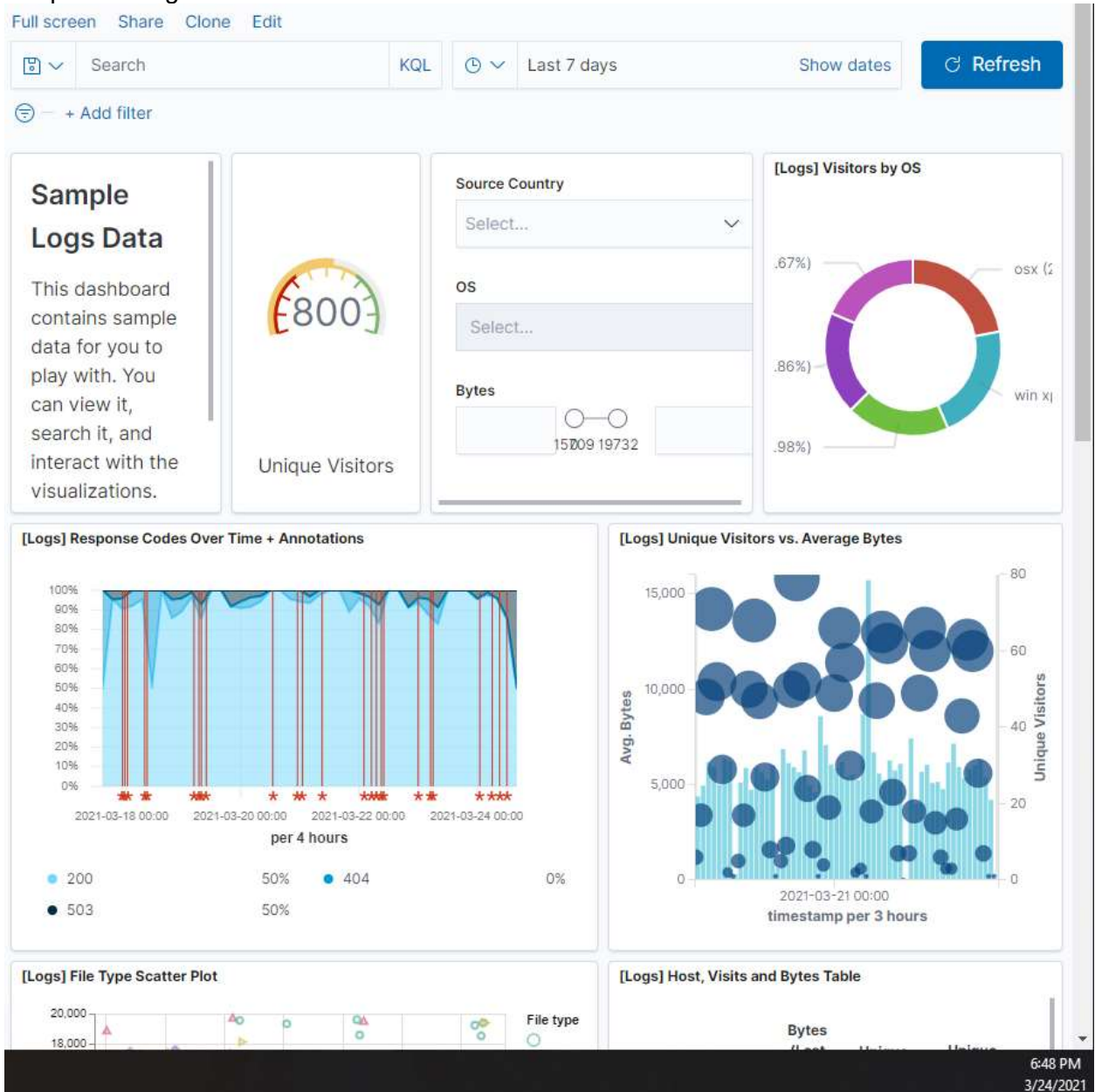


Exploring Kibana

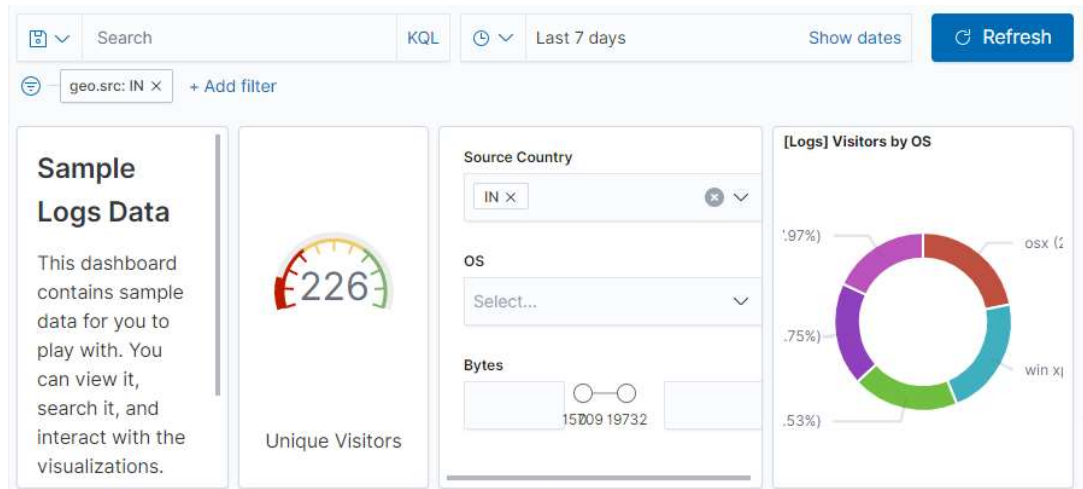
By: Walter Pan

1. Add sample web log data to Kibana.

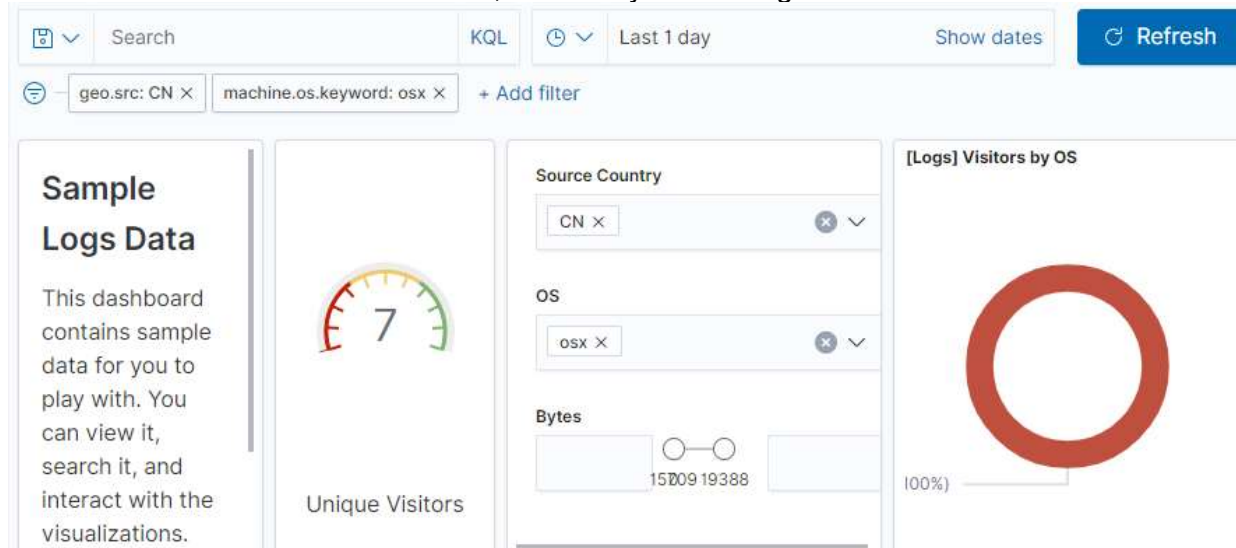


2. Answer the following questions:

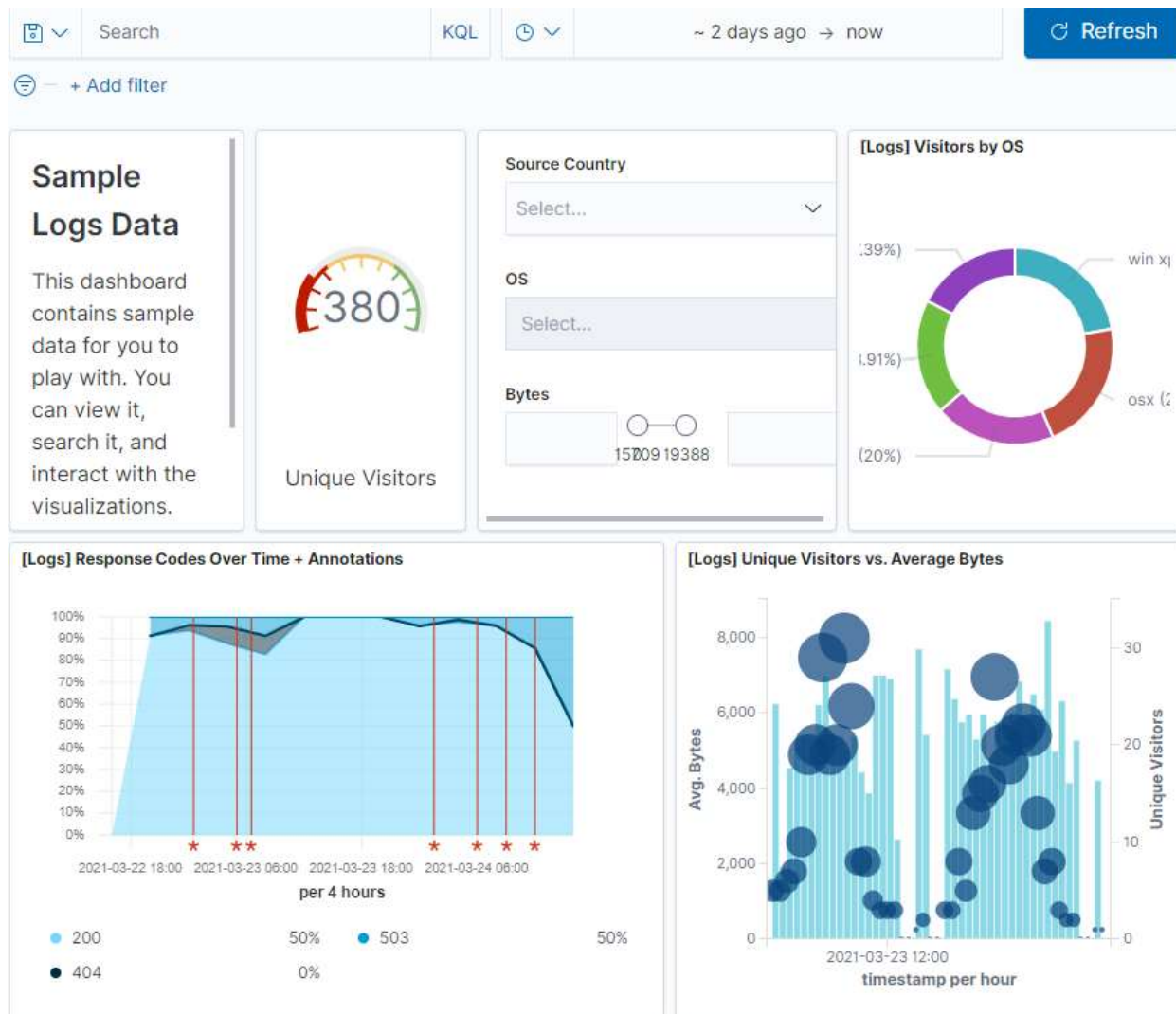
- In the last 7 days, how many unique visitors were located in India? 226



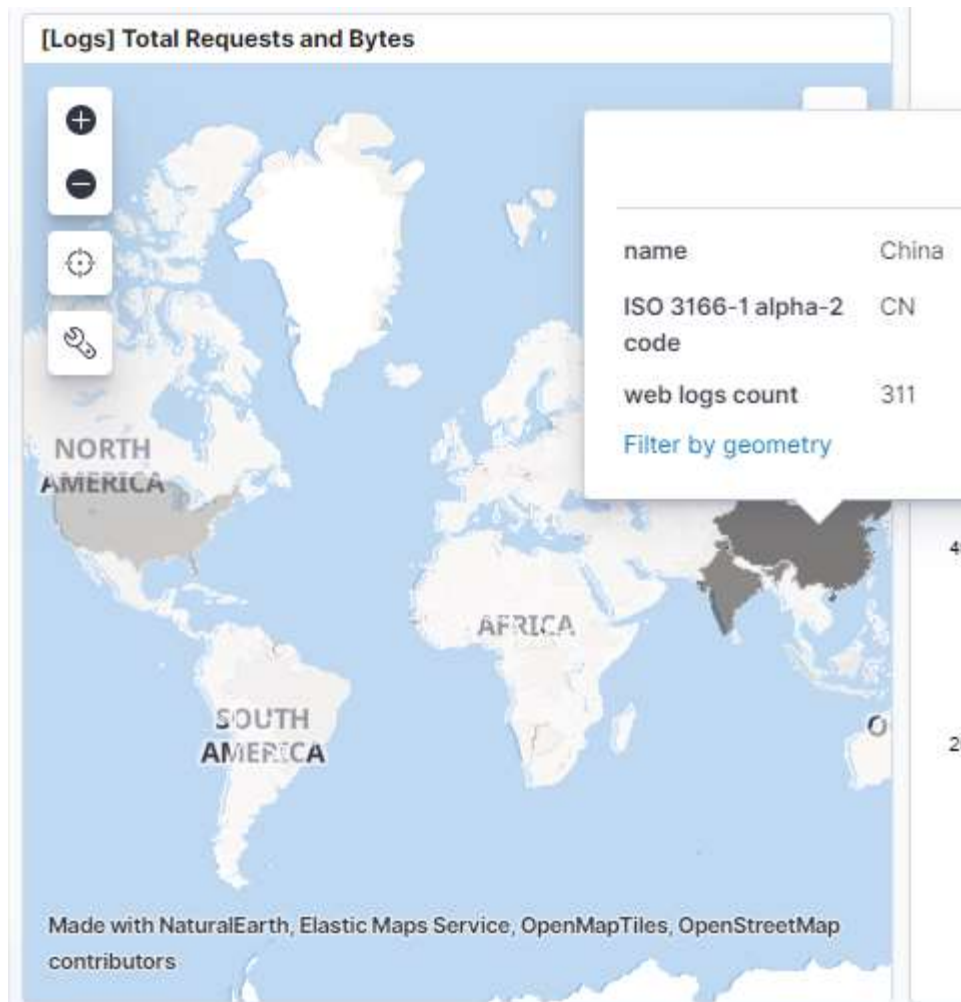
- In the last 24 hours of the visitors from China, how many were using Mac OSX? 64



- In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors? 404 errors - 0%, 503 errors - 50%

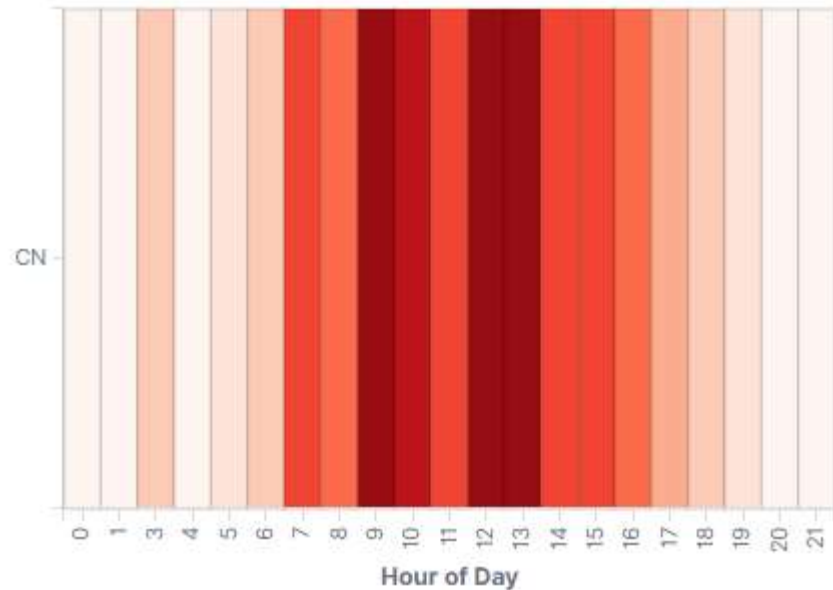


- In the last 7 days, what country produced the majority of the traffic on the website?
China



- Of the traffic that is coming from that country, what time of day had the highest amount of activity? Of the traffic that is coming from CN, 13:00 had the highest amount of activity.

[Logs] Heatmap



- List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you are not sure about a particular file type).

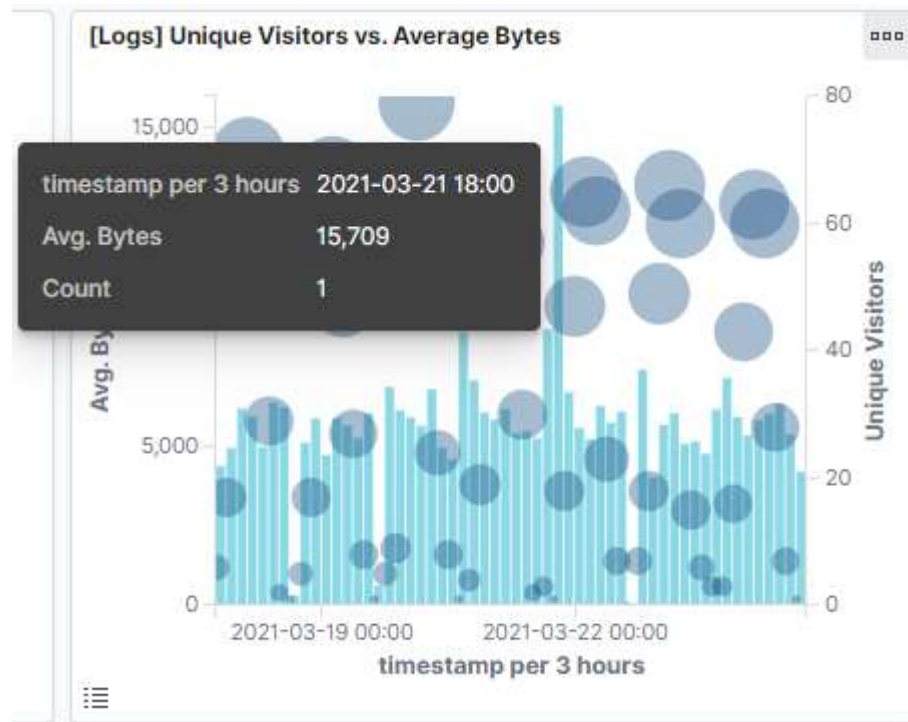
[Logs] Host, Visits and Bytes Table

Type ↑	Bytes (Total)	Hour)	Visits (Total)	Visits (Last Hour)
	2.9MB	0B	591 ↓	1 ↓
gz	1.7MB	0B	298 ↓	0 ↓
css	1.4MB	0B	254 ↓	0 ↓
zip	1.2MB	0B	210 ↓	0 ↓
deb	1.1MB	0B	178 ↓	0 ↓
rpm	473.9KB	0B	80 ↓	0 ↓

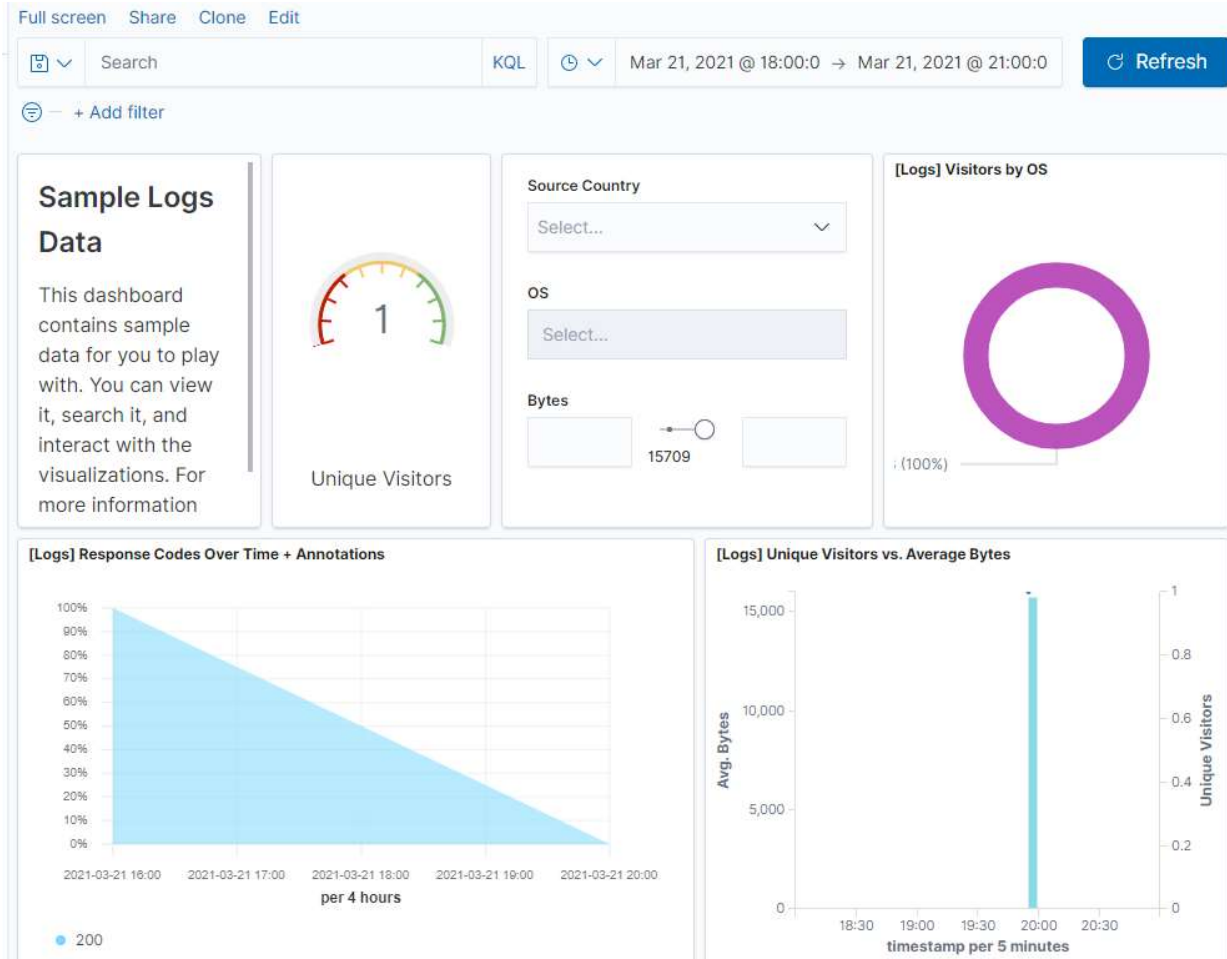
- gz: Compressed file created using gzip compression utility.
- ccss: Files for defining text format of HTML information on a webpage.
- zip: a lossless compression format file.
- deb: A Debian software package file.
- rpm: Red hat software package file.

3. Unique Visitors Vs. Average Bytes

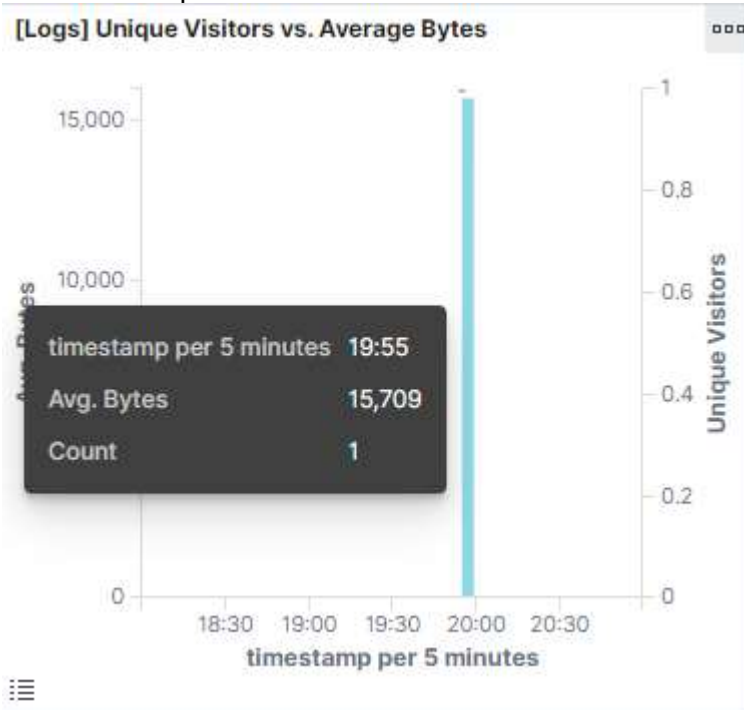
- Locate the time frame in the last 7 days with the most amount of bytes (activity).



- In your own words, is there anything that seems potentially strange about this activity?
 - At 18:00, one user used an abnormal amount of data.
4. Filter the data by this event.



- What is the timestamp for this event?

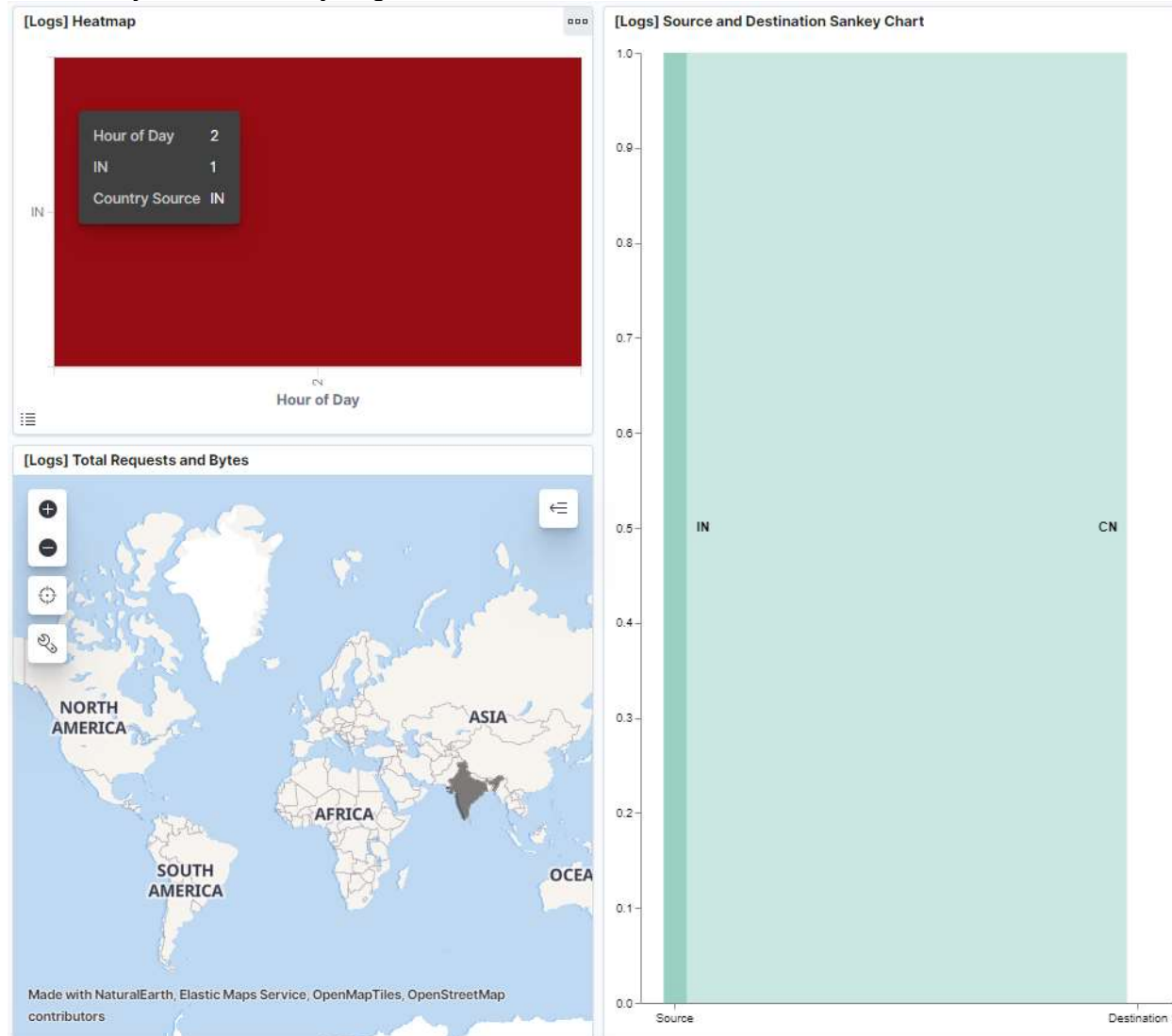


- The time stamp is 19:55.
- What kind of file was downloaded?

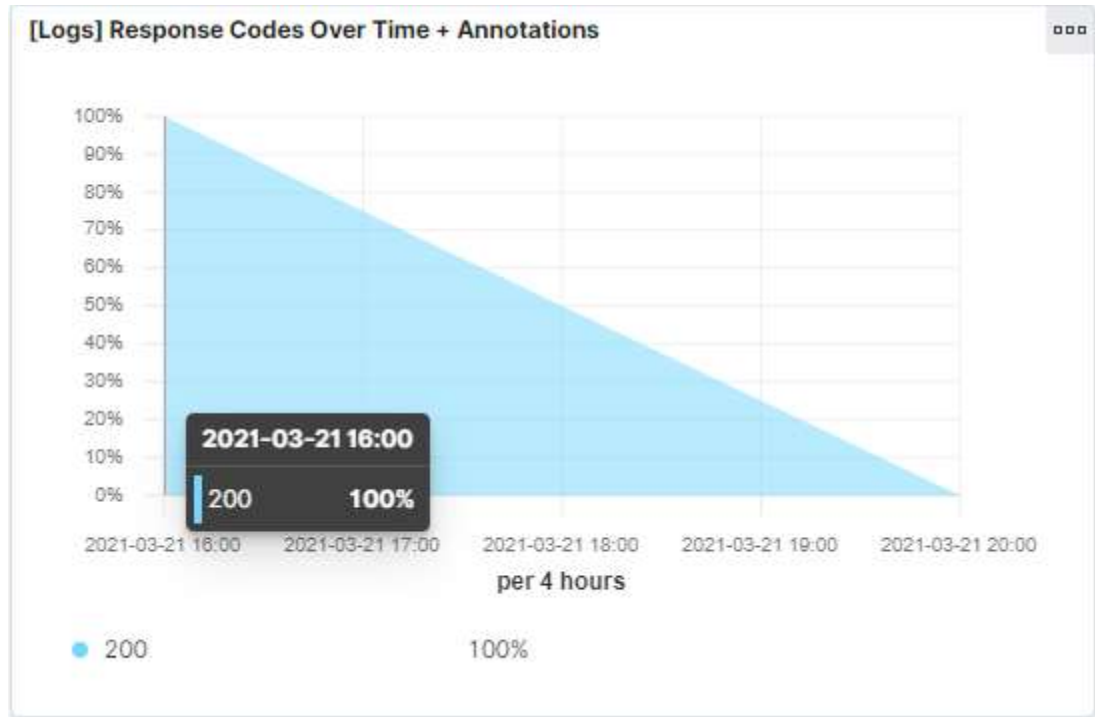
[Logs] Host, Visits and Bytes Table

Type	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
rpm	15.3KB	0B	1 ↓	0 ↓

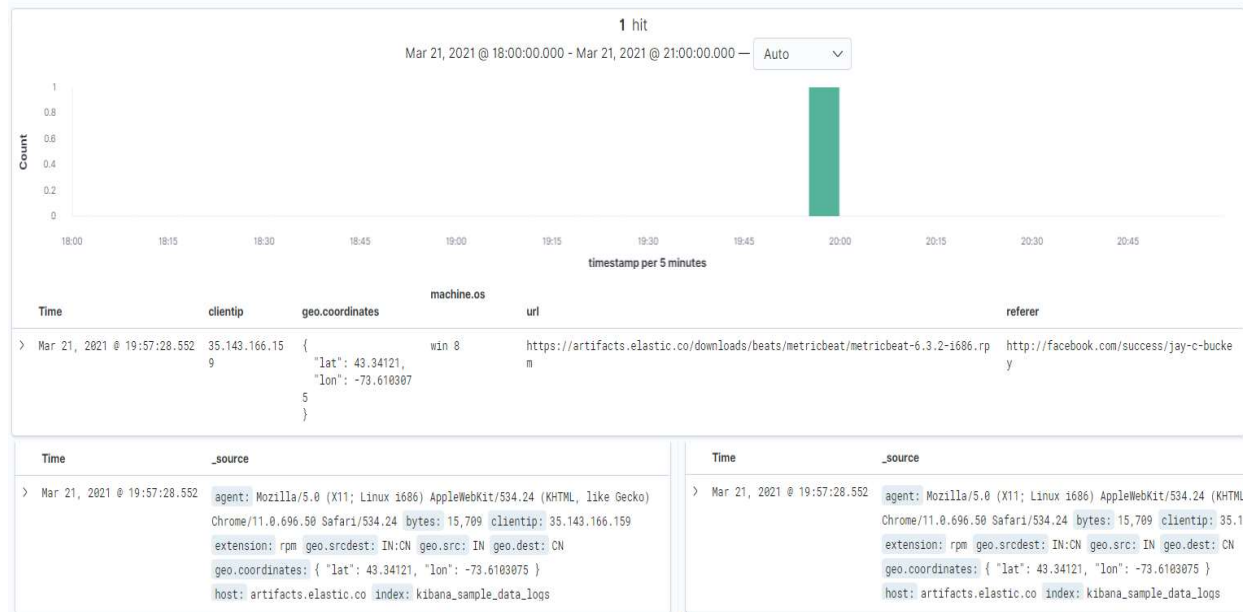
- rpm: Red hat software package file
- From what country did this activity originate?



- India
- What HTTP response codes were encountered by this visitor?



- The HTTP response code encountered by this visitor is 200.
5. Switch to the Kibana Discover page to see more details about this activity.



- What is the source IP address of this activity?

ip x

35.143.166.159

- What are the geo coordinates of this activity?

Time ↕	geo.coordinates	geo.dest	geo.src	geo.srcdest
> Mar 21, 2021 @ 19:57:28.552	{ "lat": 43.34121, "lon": -73.6103075 }	CN	IN	IN:CN

- What OS was the source machine running?

machine.os

win 8

- What is the full URL that was accessed?

url

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

- From what website did the visitor's traffic originate?

referrer

http://facebook.com/success/jay-c-buckey

6. Finish your investigation with a short overview of your insights.

- What do you think the user was doing?
 - The user was downloading Linux packages.
- Was the file they downloaded malicious?
 - There was no indication on whether the Linux packages were malicious or not.
- If not, what is the file used for?
 - The user may be performing an update or downloading a large module.
- Is there anything that seems suspicious about this activity?
 - The amount of data used by one user is suspicious.
- Is any of the traffic you inspected potentially outside of compliance guidelines?
 - The referral link from Facebook is of concern.

Kibana-Continued

SSH Barrage

SSH barrage script. /Linux/ SSH_Barrage.sh

```
#!/bin/bash
for i in {1..10}
do
    ssh hacker@10.0.0.5
done
```

```
root@5aff091c7f32:/tmp# nano SSHB.sh
root@5aff091c7f32:/tmp# chmod +x SSHB.sh
root@5aff091c7f32:/tmp# ./SSHB.sh
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
hacker@10.0.0.5: Permission denied (publickey).
root@5aff091c7f32:/tmp# |
```

GNU nano 2.9.3

SSHB.sh

```
#!/bin/bash
for i in {1..10}
do
ssh hacker@10.0.0.5
done
```


Logs

StreamSettings

hacker

CustomizeHighlights03/24/2021 8:11:27 PMStream live










Mar 24, 2021event.datasetMessage

No additional entries found

20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33848 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33850 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33852 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33854 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33856 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33858 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33860 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33862 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33864 [preauth]
20:11:27.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:11:27.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33866 [preauth]
20:12:48.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:12:48.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33976 [preauth]
20:12:48.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:12:48.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33978 [preauth]
20:12:48.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:12:48.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33980 [preauth]
20:12:48.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:12:48.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33982 [preauth]
20:12:48.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined
20:12:48.000	system.auth	Connection closed by invalid user hacker 10.0.0.4 port 33984 [preauth]
20:12:48.000	system.auth	[System][auth][ssh] Invalid user undefined from undefined

Log event document details

Actions  

Field	Value
@timestamp	 2021-03-25T03:11:27.000Z
_id	 -EFdZ3gB2VRYEJJ0tsu6
_index	 filebeat-7.4.0-2021.03.23-000001
agent.ephemeral_id	 c31d8d34-2515-419d-a296-105e56f82033
agent.hostname	 Web-1
agent.id	 8d68d879-94df-45ec-9565-511cbaf1d5f5
agent.type	 filebeat
agent.version	 7.4.0
ecs.version	 1.1.0
event.dataset	 system.auth
event.module	 system
event.timezone	 +00:00
fileset.name	 auth
host.hostname	 Web-1
host.name	 Web-1
input.type	 log
log.file.path	 /var/log/auth.log
log.offset	 76460
message	 Connection closed by invalid user hacker 10.0.0.4 port 33866
message	 Connection closed by invalid user hacker 10.0.0.4 port 33866 [preauth]
process.name	 sshd
process.pid	 16909
service.type	 system

Linux Stress

SSH into Web-1 from jump box


```

root@5aff091c7f32:~# ssh sysadmin@10.0.0.5
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1043-azure x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Fri Mar 26 17:14:54 UTC 2021

System load:  0.3               Processes:            126
Usage of /:   13.3% of 28.90GB   Users logged in:     0
Memory usage: 23%               IP address for eth0:  10.0.0.5
Swap usage:   0%                IP address for docker0: 172.17.0.1

* Introducing self-healing high availability clusters in MicroK8s.
  Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

  https://microk8s.io/high-availability

10 packages can be updated.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Fri Mar 26 17:11:37 2021 from 10.0.0.4
sysadmin@Web-1:~$

```

Install stress on Web-1

```

sudo apt install stress

sysadmin@Web-1:~$ sudo apt-get install stress
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  stress
0 upgraded, 1 newly installed, 0 to remove and 10 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 (86.6 kB/s)
Selecting previously unselected package stress.
(Reading database ... 120988 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) ...

```

Check number of cores on Web-1 VM

Web-1 Virtual machine

Search (Ctrl+F) < > Connect Start Restart Stop Capture Delete Refresh Open in mobile

Advisor (1 of 5): Disk encryption should be applied on virtual machines →

Subscription (change) : Azure subscription 1 virtual network/subnet : neo-team-net/uea-net
Subscription ID : 0bbee373-d6e7-4a43-a18f-93215e3cde67 DNS name : Configure
Tags (change) : Click here to add tags

Properties Monitoring Capabilities (7) Recommendations (5) Tutorials

Virtual machine

Computer name	Web-1
Operating system	Linux (ubuntu 18.04)
Publisher	Canonical
Offer	UbuntuServer
Plan	18.04-LTS
VM generation	V1
Agent status	Ready
Agent version	2.2.53.1
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A

Availability + scaling

Availability zone	-
Scale Set	-

Networking

Public IP address	52.183.66.168
Public IP address (IPv6)	-
Private IP address	10.0.0.5
Private IP address (IPv6)	-
Virtual network/subnet	RedTeamNet/default
DNS name	Configure

Size

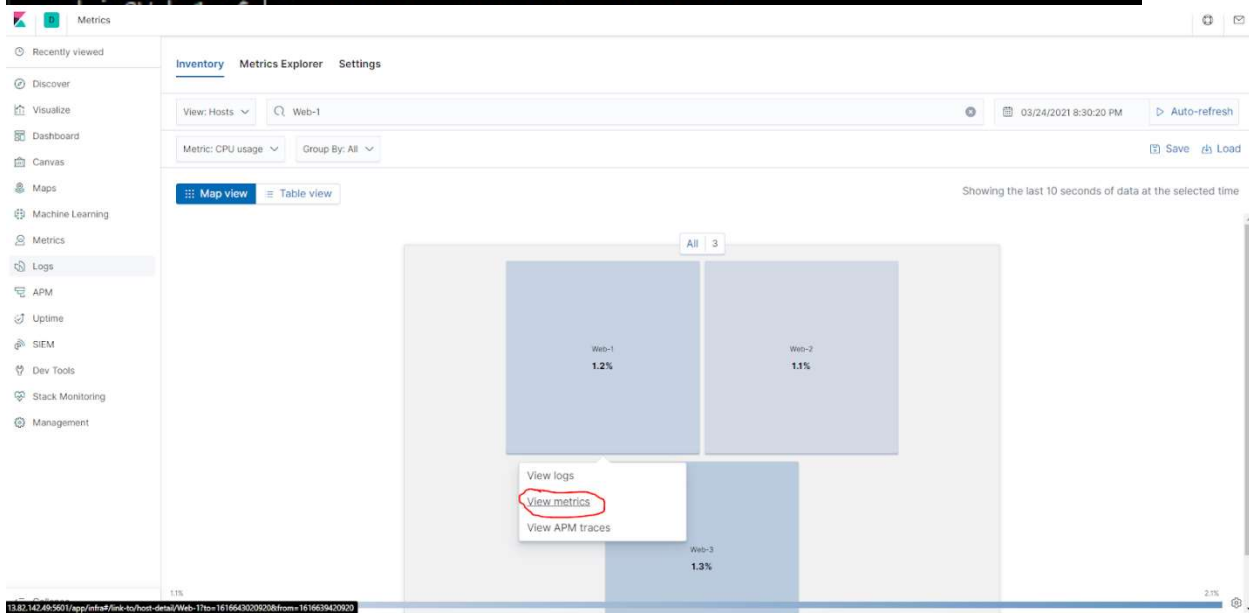
Size	Standard B1ms
vCPUs	1
RAM	2 GiB

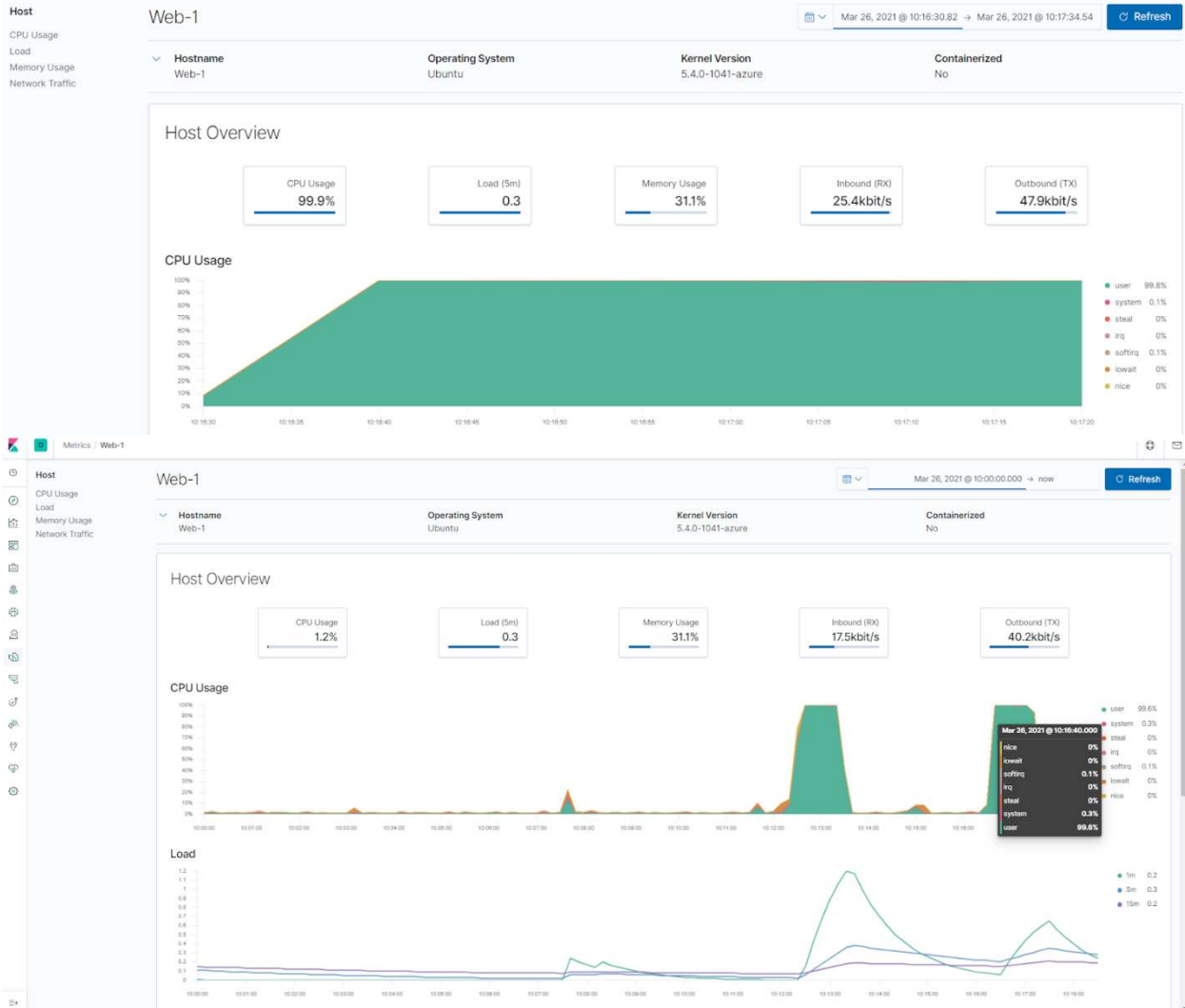
Disk

OS disk	Web-1_OsDisk_1_ccd12ede102e4f9cb5a5fe88ec5ad489
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

Stress tests the 1 core on Web-1

```
sysadmin@Web-1:~$ stress --cpu 1 --timeout 60
stress: info: [5975] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5975] successful run completed in 60s
```





wget-DoS

wget-Dos Script /Linux/ wget-DoS.sh

```
sysadmin@web-1:~$ sudo apt-get install wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version (1.19.4-1ubuntu2.2).
wget set to manually installed.
The following packages were automatically installed and are no longer required:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 10 not upgraded.
```

```

sysadmin@Web-1:/tmp/testfiles$ for i in {1..100}
> do
> wget https://google.com
> done
--2021-03-26 17:35:38-- https://google.com/
Resolving google.com (google.com)... 142.251.33.78, 2607:f8b0:400a:803::200e
Connecting to google.com (google.com)|142.251.33.78|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/ [following]
--2021-03-26 17:35:38-- https://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.14.196, 2607:f8b0:400a:808::2004
Connecting to www.google.com (www.google.com)|172.217.14.196|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

index.html.1          [ <=>          ] 12.55K  --.-KB/s    in 0s

2021-03-26 17:35:38 (50.5 MB/s) - 'index.html.1' saved [12849]

```

