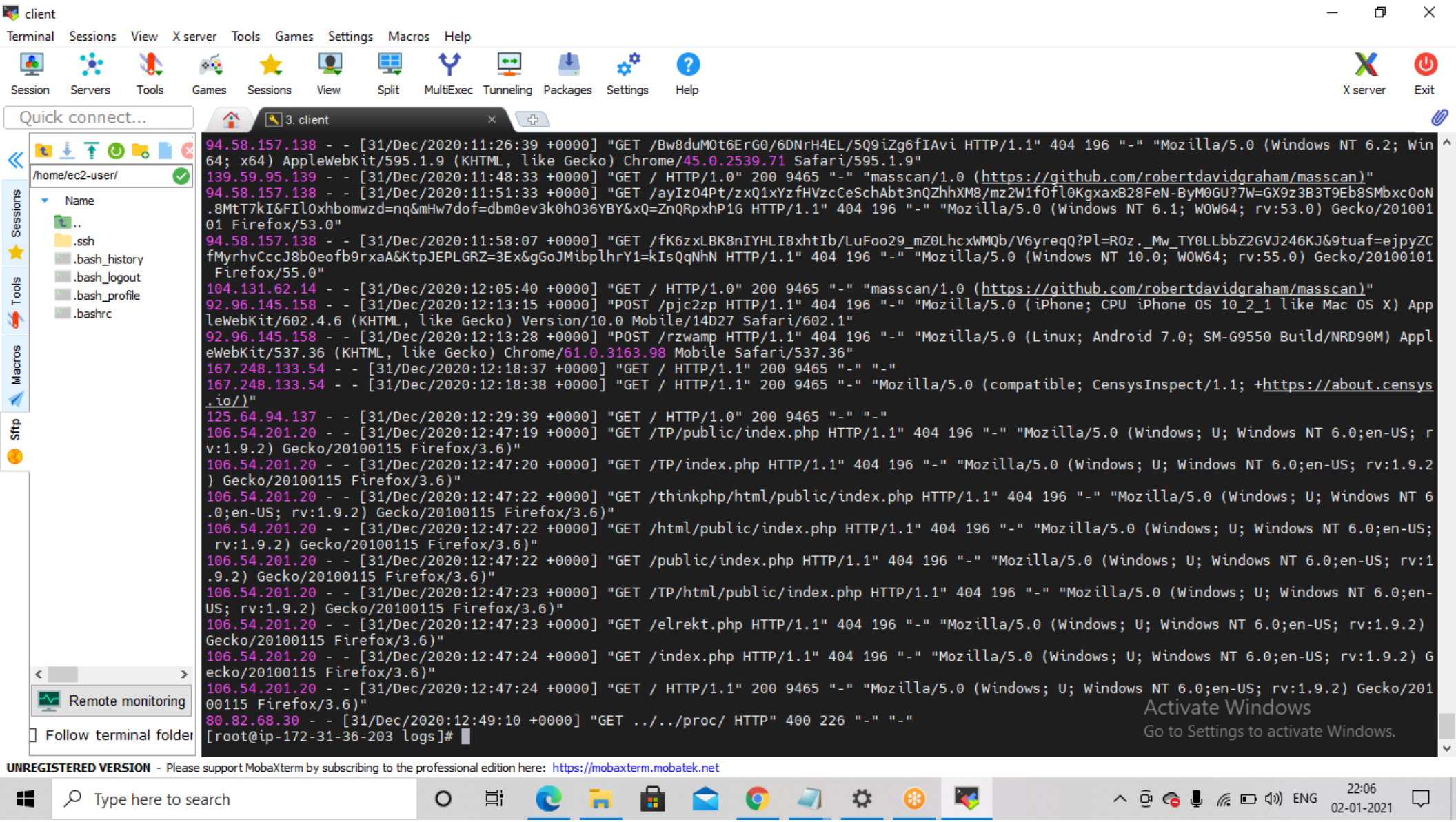
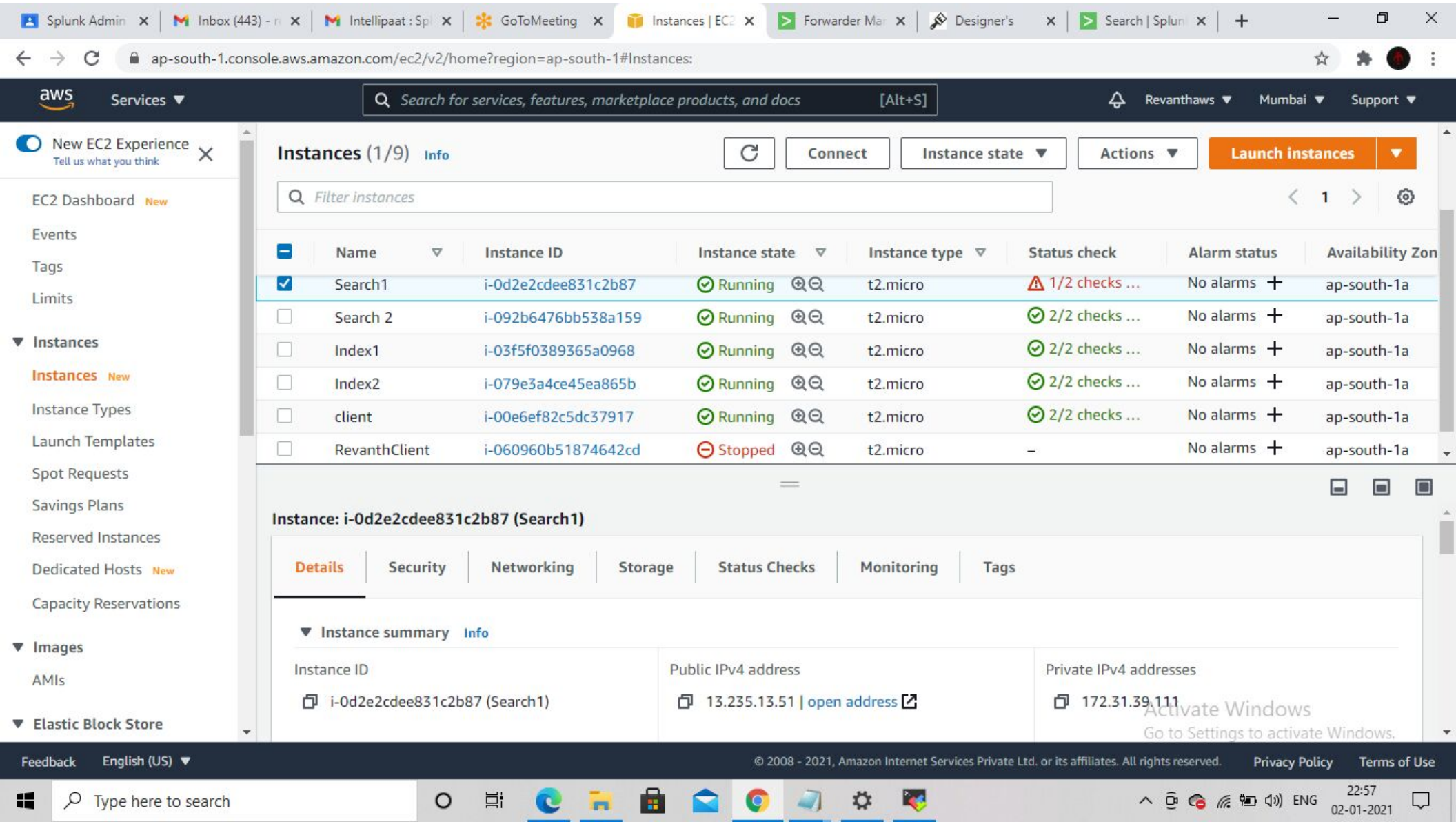
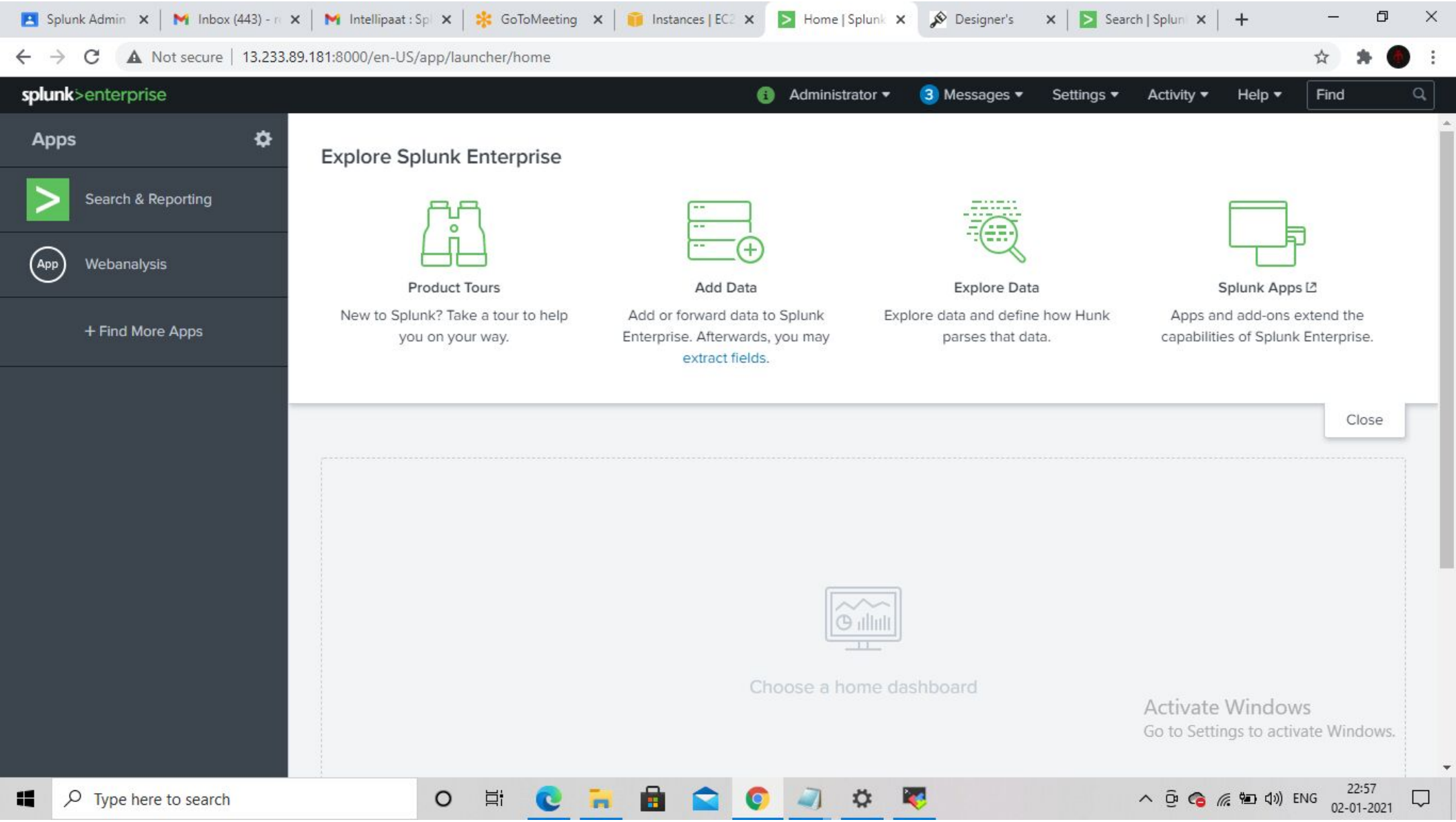
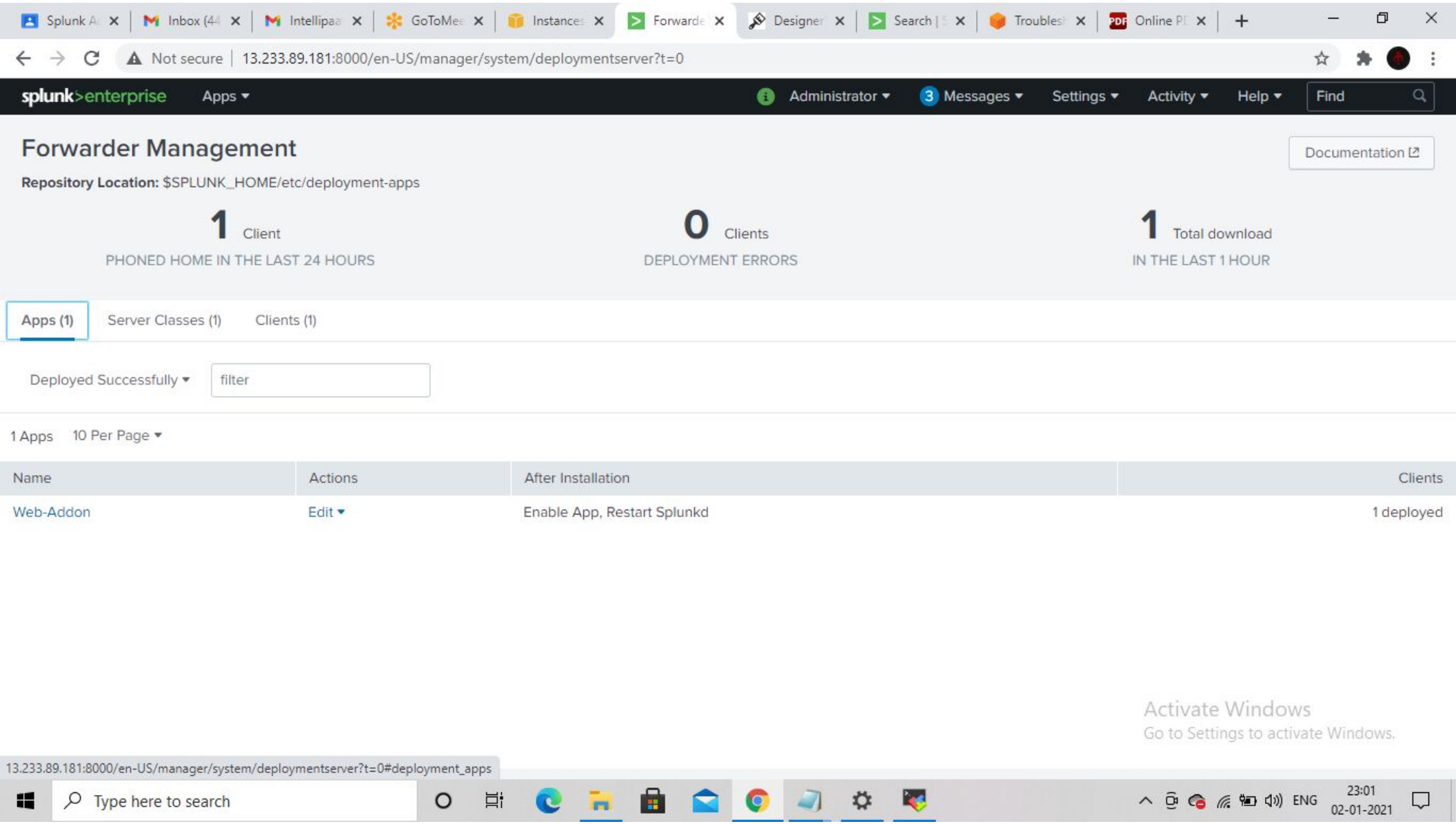
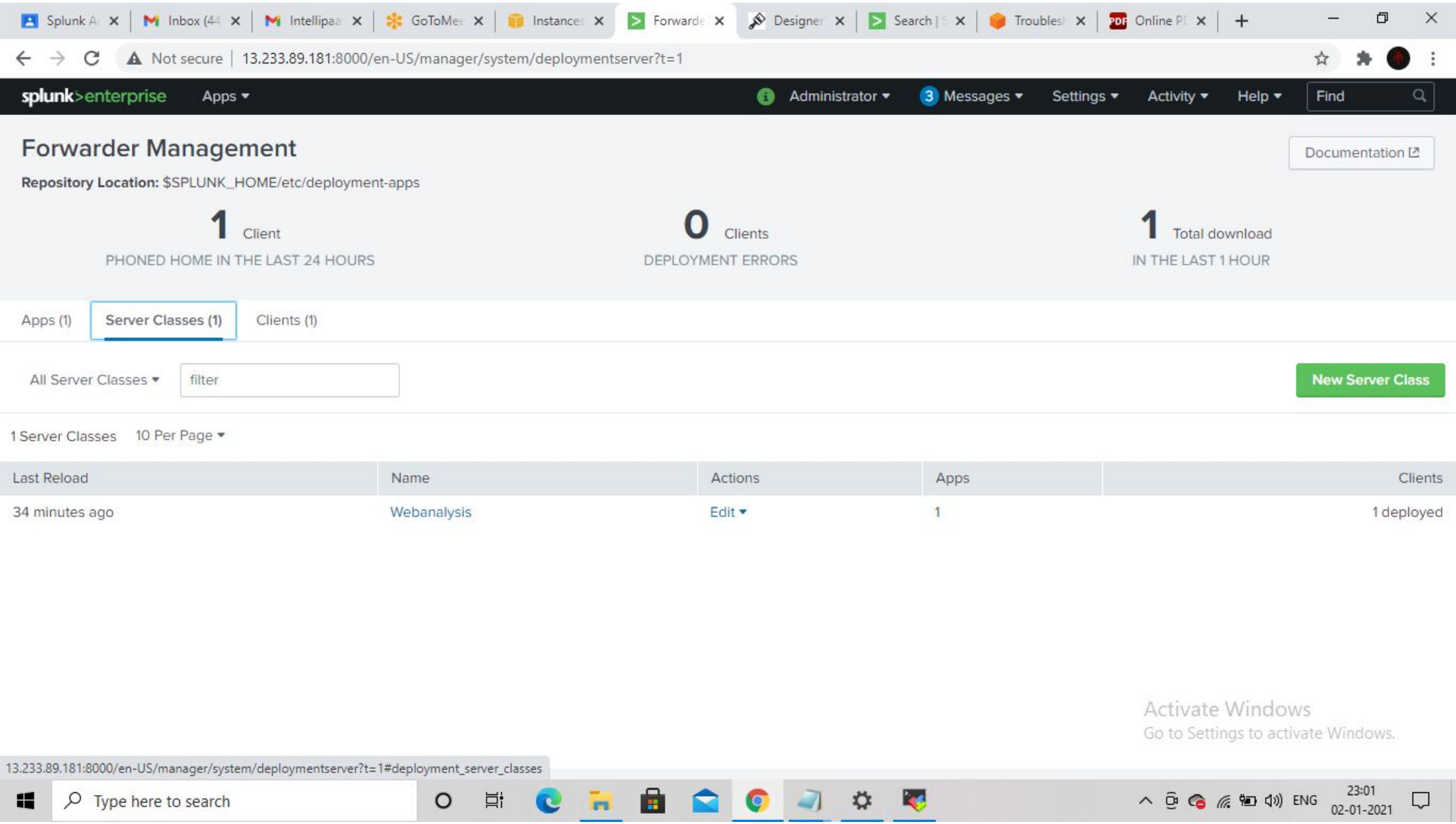
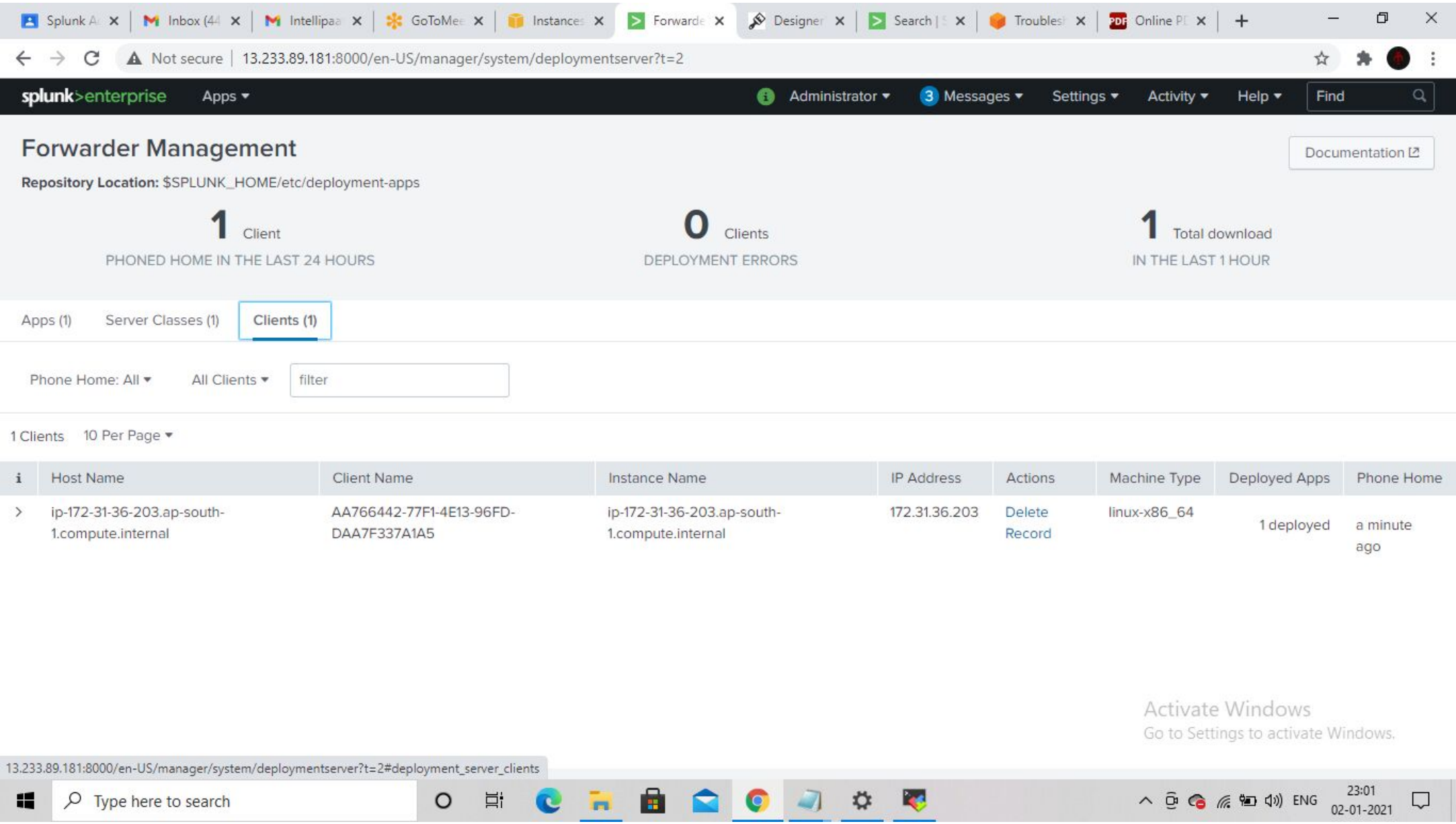

client
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
3. client
/home/ec2-user/
Name
..
.ssh
.bash_history
.bash_logout
.bash_profile
.bashrc
Sessions Tools Macros Sftp
Remote monitoring
Follow terminal folder
94.58.157.138 - - [31/Dec/2020:11:26:39 +0000] "GET /Bw8duMOt6ErG0/6DNrH4EL/5Q9iZg6fIAvi HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/595.1.9 (KHTML, like Gecko) Chrome/45.0.2539.71 Safari/595.1.9"
139.59.95.139 - - [31/Dec/2020:11:48:33 +0000] "GET / HTTP/1.0" 200 9465 "-" "masscan/1.0 (https://github.com/robertdavidgraham/masscan)"
94.58.157.138 - - [31/Dec/2020:11:51:33 +0000] "GET /ayIzO4Pt/zxQ1xYzfHVzcCeSchAbt3nQZhhXM8/mz2W1fOfl0KgxaxB28FeN-ByM0GU?7W=GX9z3B3T9Eb8SMbxcOoN.8MtT7kI&FIlOxhbomwzd=nq&mHw7dof=dbm0ev3k0hO36YBY&xQ=ZnQRpxhP1G HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0"
94.58.157.138 - - [31/Dec/2020:11:58:07 +0000] "GET /fK6zxLBK8nIYHLI8xhtIb/LuFoo29_mZ0LhcxWMQb/V6yreqQ?Pl=ROz._Mw_TY0LLbbZ2GVJ246KJ&9tuaf=ejpyZCfMyrhvCccJ8bOeofb9rxaA&KtpJEPLGRZ=3Ex&gGoJMibplhrY1=kIsQqNhN HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0"
104.131.62.14 - - [31/Dec/2020:12:05:40 +0000] "GET / HTTP/1.0" 200 9465 "-" "masscan/1.0 (https://github.com/robertdavidgraham/masscan)"
92.96.145.158 - - [31/Dec/2020:12:13:15 +0000] "POST /pjc2zp HTTP/1.1" 404 196 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 10_2_1 like Mac OS X) AppleWebKit/602.4.6 (KHTML, like Gecko) Version/10.0 Mobile/14D27 Safari/602.1"
92.96.145.158 - - [31/Dec/2020:12:13:28 +0000] "POST /rzwamp HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Linux; Android 7.0; SM-G9550 Build/NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.98 Mobile Safari/537.36"
167.248.133.54 - - [31/Dec/2020:12:18:37 +0000] "GET / HTTP/1.1" 200 9465 "-" "-"
167.248.133.54 - - [31/Dec/2020:12:18:38 +0000] "GET / HTTP/1.1" 200 9465 "-" "Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)"
125.64.94.137 - - [31/Dec/2020:12:29:39 +0000] "GET / HTTP/1.0" 200 9465 "-" "-"
106.54.201.20 - - [31/Dec/2020:12:47:19 +0000] "GET /TP/public/index.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:20 +0000] "GET /TP/index.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:22 +0000] "GET /thinkphp/html/public/index.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:22 +0000] "GET /html/public/index.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:22 +0000] "GET /public/index.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:23 +0000] "GET /TP/html/public/index.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:23 +0000] "GET /elrekt.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:24 +0000] "GET /index.php HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
106.54.201.20 - - [31/Dec/2020:12:47:24 +0000] "GET / HTTP/1.1" 200 9465 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0;en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6)"
80.82.68.30 - - [31/Dec/2020:12:49:10 +0000] "GET ../../proc/ HTTP" 400 226 "-" "-"
[root@ip-172-31-36-203 logs]#
Activate Windows
Go to Settings to activate Windows.
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
ENG
22:06
02-01-2021

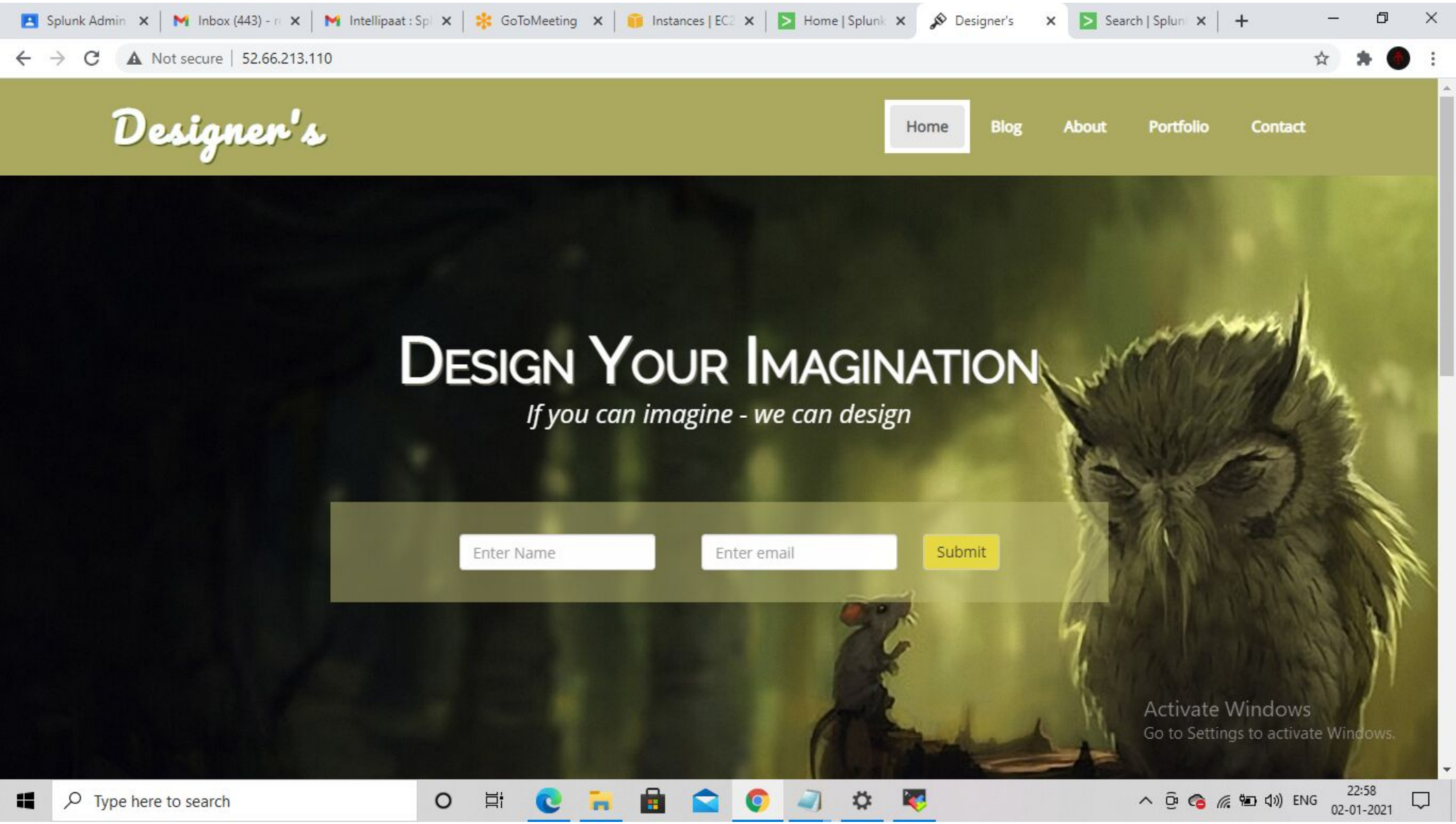

Splunk Admin
Inbox (443) -
Intellipaat : Spl
GoToMeeting
Instances | EC2
Forwarder Mar
Designer's
Search | Splun
ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#Instances:
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Revanthaws
Mumbai
Support
New EC2 Experience
Tell us what you think
EC2 Dashboard New
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Capacity Reservations
Images
AMIs
Elastic Block Store
Instances (1/9) Info
Connect
Instance state
Actions
Launch instances
Filter instances
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zon
Search1 i-0d2e2cdee831c2b87 Running t2.micro 1/2 checks ... No alarms ap-south-1a
Search 2 i-092b6476bb538a159 Running t2.micro 2/2 checks ... No alarms ap-south-1a
Index1 i-03f5f0389365a0968 Running t2.micro 2/2 checks ... No alarms ap-south-1a
Index2 i-079e3a4ce45ea865b Running t2.micro 2/2 checks ... No alarms ap-south-1a
client i-00e6ef82c5dc37917 Running t2.micro 2/2 checks ... No alarms ap-south-1a
RevanthClient i-060960b51874642cd Stopped t2.micro – No alarms ap-south-1a
Instance: i-0d2e2cdee831c2b87 (Search1)
Details
Security
Networking
Storage
Status Checks
Monitoring
Tags
Instance summary Info
Instance ID
i-0d2e2cdee831c2b87 (Search1)
Public IPv4 address
13.235.13.51 | open address
Private IPv4 addresses
172.31.39.111
Activate Windows
Go to Settings to activate Windows.
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
ENG
22:57
02-01-2021

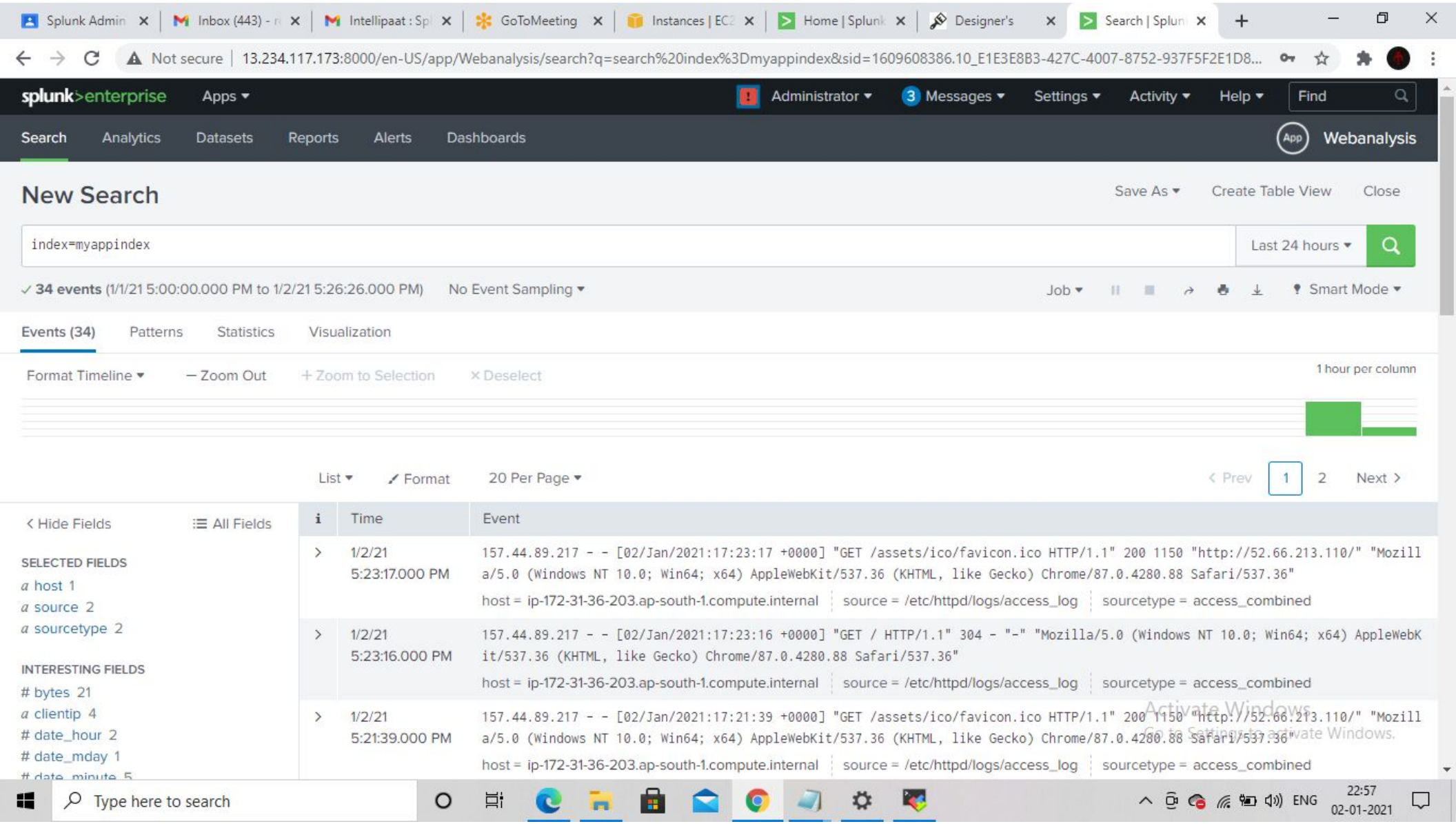

Splunk Admin
Inbox (443) -
Intellipaat : Sp
GoToMeeting
Instances | EC2
Home | Splunk
Designer's
Search | Splun
Not secure
13.233.89.181:8000/en-US/app/launcher/home
splunk>enterprise
Administrator
3 Messages
Settings
Activity
Help
Find
Apps
Search & Reporting
Webanalysis
+ Find More Apps
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Explore Data
Explore data and define how Hunk parses that data.
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.
Close
Choose a home dashboard
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
22:57
02-01-2021

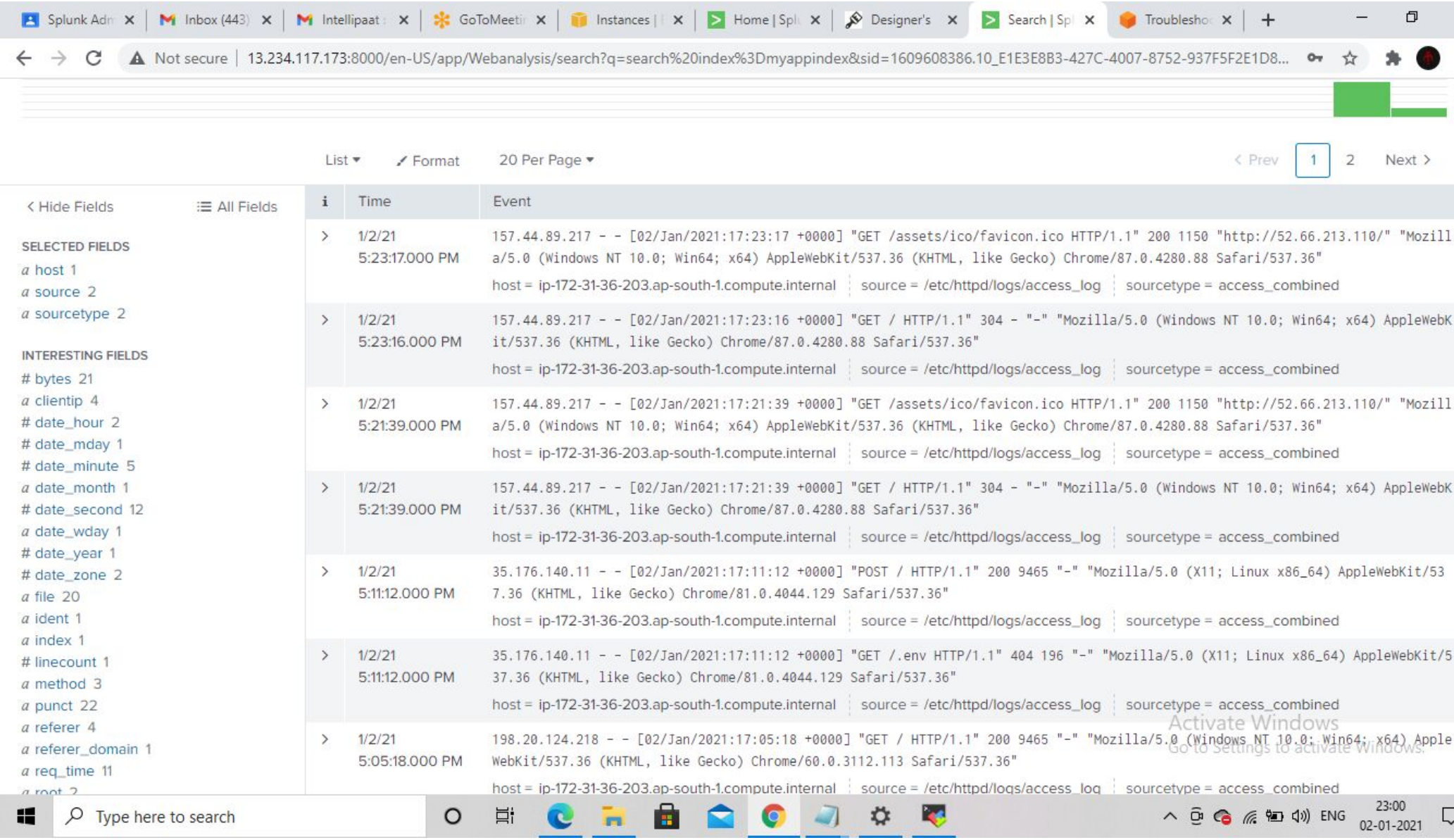

Not secure | 13.233.89.181:8000/en-US/manager/system/deploymentserver?t=0
splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Forwarder Management
Documentation
Repository Location: $SPLUNK_HOME/etc/deployment-apps
1 Client
PHONED HOME IN THE LAST 24 HOURS
0 Clients
DEPLOYMENT ERRORS
1 Total download
IN THE LAST 1 HOUR
Apps (1)
Server Classes (1)
Clients (1)
Deployed Successfully
filter
1 Apps
10 Per Page
Name
Actions
After Installation
Clients
Web-Addon
Edit
Enable App, Restart Splunkd
1 deployed
Activate Windows
Go to Settings to activate Windows.
13.233.89.181:8000/en-US/manager/system/deploymentserver?t=0#deployment_apps
Type here to search
ENG
23:01
02-01-2021

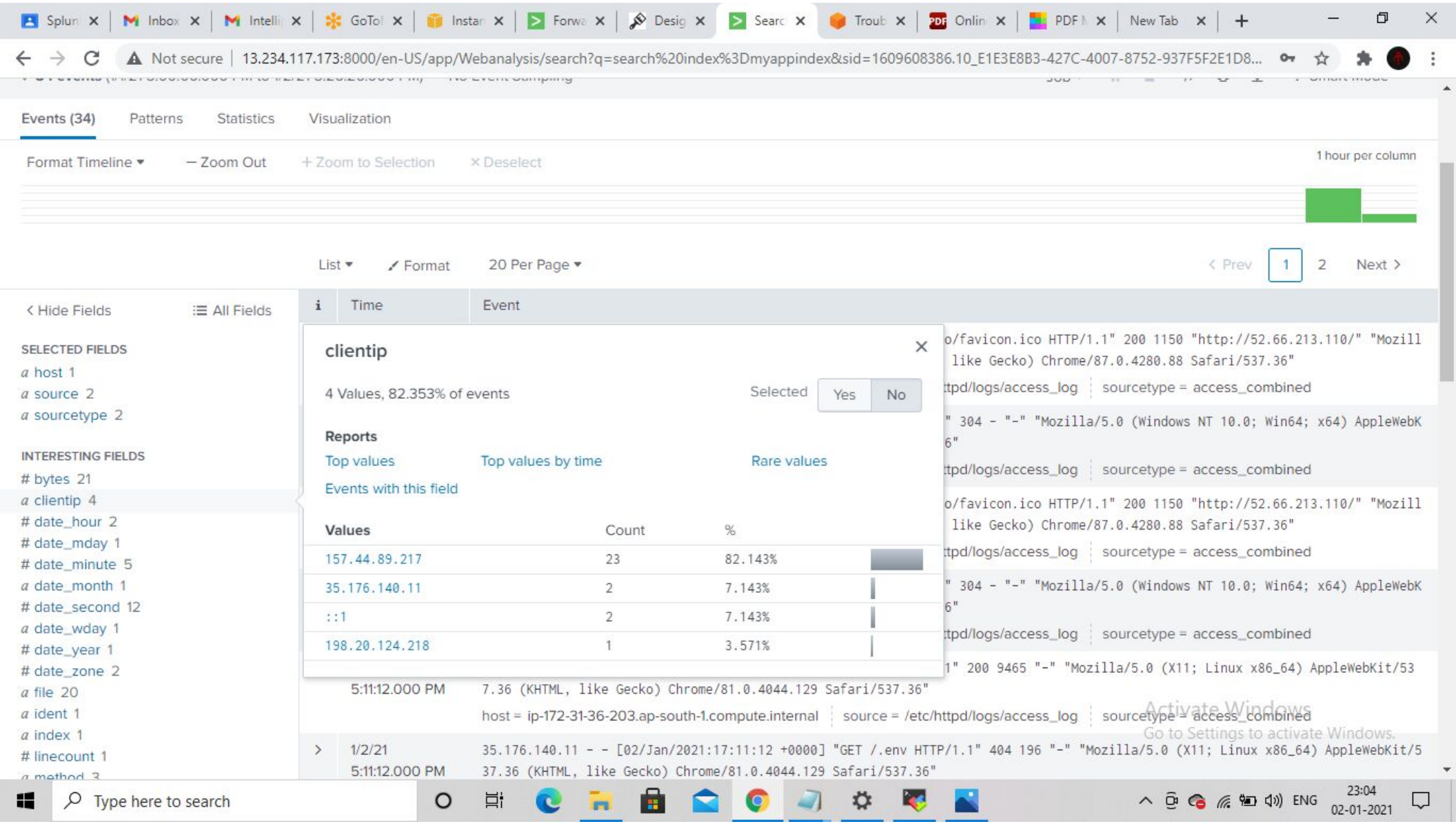

Not secure | 13.233.89.181:8000/en-US/manager/system/deploymentserver?t=1
splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Forwarder Management
Documentation
Repository Location: $SPLUNK_HOME/etc/deployment-apps
1 Client
PHONED HOME IN THE LAST 24 HOURS
0 Clients
DEPLOYMENT ERRORS
1 Total download
IN THE LAST 1 HOUR
Apps (1)
Server Classes (1)
Clients (1)
All Server Classes
filter
New Server Class
1 Server Classes
10 Per Page
Last Reload
Name
Actions
Apps
Clients
34 minutes ago
Webanalysis
Edit
1
1 deployed
Activate Windows
Go to Settings to activate Windows.
13.233.89.181:8000/en-US/manager/system/deploymentserver?t=1#deployment_server_classes
Type here to search
ENG
23:01
02-01-2021

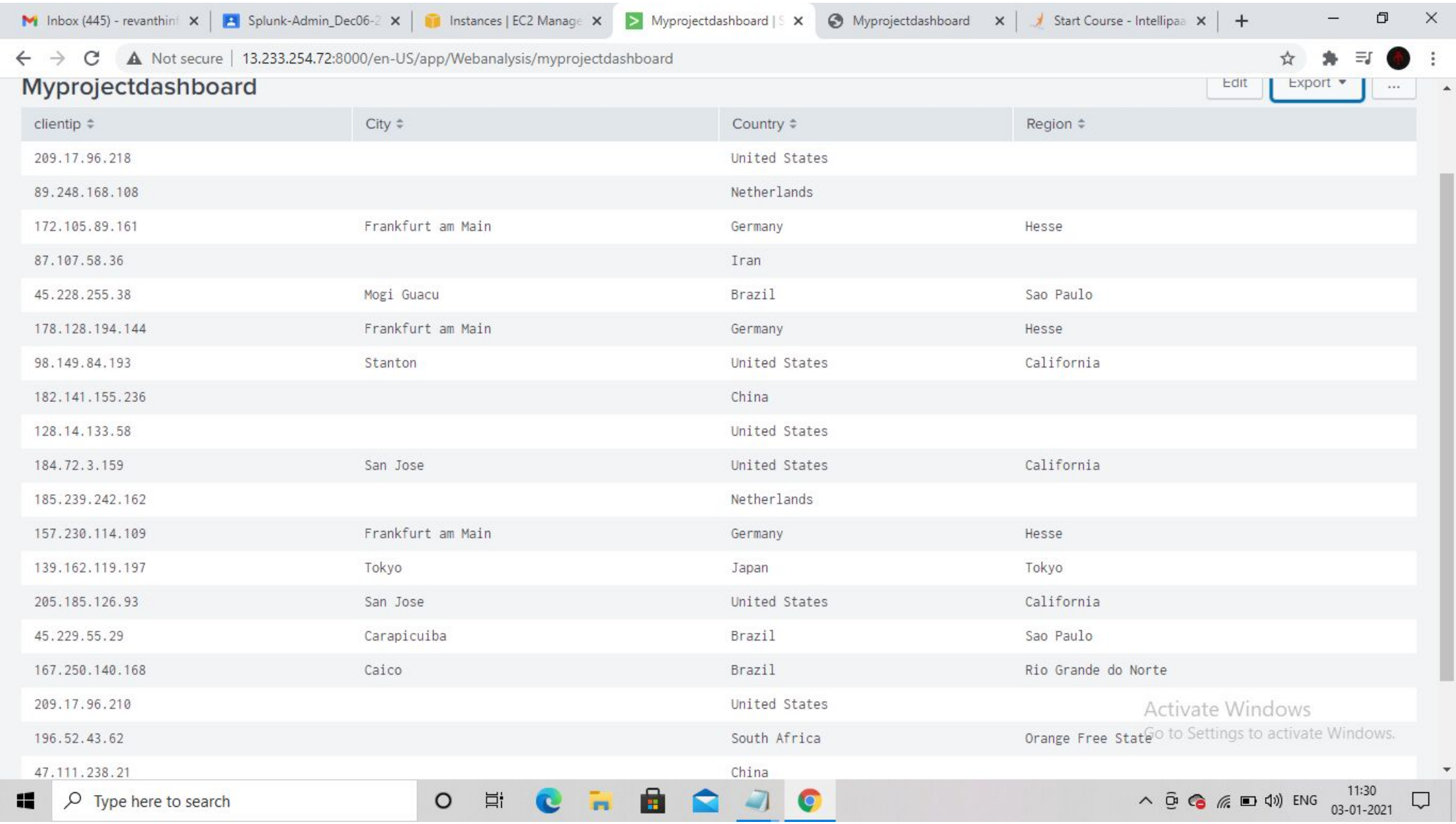

Not secure | 13.233.89.181:8000/en-US/manager/system/deploymentserver?t=2
splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Forwarder Management
Documentation
Repository Location: $SPLUNK_HOME/etc/deployment-apps
1 Client
PHONED HOME IN THE LAST 24 HOURS
0 Clients
DEPLOYMENT ERRORS
1 Total download
IN THE LAST 1 HOUR
Apps (1)
Server Classes (1)
Clients (1)
Phone Home: All
All Clients
filter
1 Clients
10 Per Page
i
Host Name
Client Name
Instance Name
IP Address
Actions
Machine Type
Deployed Apps
Phone Home
ip-172-31-36-203.ap-south-1.compute.internal
AA766442-77F1-4E13-96FD-DAA7F337A1A5
ip-172-31-36-203.ap-south-1.compute.internal
172.31.36.203
Delete Record
linux-x86_64
1 deployed
a minute ago
Activate Windows
Go to Settings to activate Windows.
13.233.89.181:8000/en-US/manager/system/deploymentserver?t=2#deployment_server_clients
Type here to search
ENG
23:01
02-01-2021


Splunk Admin
Inbox (443) -
Intellipaat : Sp
GoToMeeting
Instances | EC2
Home | Splunk
Designer's
Search | Splun
Not secure
52.66.213.110
Designer's
Home
Blog
About
Portfolio
Contact
DESIGN YOUR IMAGINATION
If you can imagine - we can design
Enter Name
Enter email
Submit
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
22:58
02-01-2021


Splunk Admin
Inbox (443) -
Intellipaat : Spl
GoToMeeting
Instances | EC2
Home | Splunk
Designer's
Search | Splun
Not secure
13.234.117.173:8000/en-US/app/Webanalysis/search?q=search%20index%3Dmyappindex&sid=1609608386.10_E1E3E8B3-427C-4007-8752-937F5F2E1D8...
splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
App
Webanalysis
New Search
Save As
Create Table View
Close
index=myappindex
Last 24 hours
34 events (1/1/21 5:00:00.000 PM to 1/2/21 5:26:26.000 PM)
No Event Sampling
Job
Smart Mode
Events (34)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1
2
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 2
a sourcetype 2
INTERESTING FIELDS
bytes 21
a clientip 4
date_hour 2
date_mday 1
i
Time
Event
1/2/21 5:23:17.000 PM
157.44.89.217 - - [02/Jan/2021:17:23:17 +0000] "GET /assets/ico/favicon.ico HTTP/1.1" 200 1150 "http://52.66.213.110/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal
source = /etc/httpd/logs/access_log
sourcetype = access_combined
1/2/21 5:23:16.000 PM
157.44.89.217 - - [02/Jan/2021:17:23:16 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal
source = /etc/httpd/logs/access_log
sourcetype = access_combined
1/2/21 5:21:39.000 PM
157.44.89.217 - - [02/Jan/2021:17:21:39 +0000] "GET /assets/ico/favicon.ico HTTP/1.1" 200 1150 "http://52.66.213.110/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal
source = /etc/httpd/logs/access_log
sourcetype = access_combined
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
22:57
02-01-2021


Not secure 13.234.117.173:8000/en-US/app/Webanalysis/search?q=search%20index%3Dmyappindex&sid=1609608386.10_E1E3E8B3-427C-4007-8752-937F5F2E1D8...
List
Format
20 Per Page
Prev
1
2
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 2
a sourcetype 2
INTERESTING FIELDS
bytes 21
a clientip 4
date_hour 2
date_mday 1
date_minute 5
a date_month 1
date_second 12
a date_wday 1
date_year 1
date_zone 2
a file 20
a ident 1
a index 1
linecount 1
a method 3
a punct 22
a referer 4
a referer_domain 1
a req_time 11
Time
Event
1/2/21 5:23:17.000 PM
157.44.89.217 - - [02/Jan/2021:17:23:17 +0000] "GET /assets/ico/favicon.ico HTTP/1.1" 200 1150 "http://52.66.213.110/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal source = /etc/httpd/logs/access_log sourcetype = access_combined
1/2/21 5:23:16.000 PM
157.44.89.217 - - [02/Jan/2021:17:23:16 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal source = /etc/httpd/logs/access_log sourcetype = access_combined
1/2/21 5:21:39.000 PM
157.44.89.217 - - [02/Jan/2021:17:21:39 +0000] "GET /assets/ico/favicon.ico HTTP/1.1" 200 1150 "http://52.66.213.110/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal source = /etc/httpd/logs/access_log sourcetype = access_combined
1/2/21 5:21:39.000 PM
157.44.89.217 - - [02/Jan/2021:17:21:39 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal source = /etc/httpd/logs/access_log sourcetype = access_combined
1/2/21 5:11:12.000 PM
35.176.140.11 - - [02/Jan/2021:17:11:12 +0000] "POST / HTTP/1.1" 200 9465 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal source = /etc/httpd/logs/access_log sourcetype = access_combined
1/2/21 5:11:12.000 PM
35.176.140.11 - - [02/Jan/2021:17:11:12 +0000] "GET /.env HTTP/1.1" 404 196 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal source = /etc/httpd/logs/access_log sourcetype = access_combined
1/2/21 5:05:18.000 PM
198.20.124.218 - - [02/Jan/2021:17:05:18 +0000] "GET / HTTP/1.1" 200 9465 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal source = /etc/httpd/logs/access_log sourcetype = access_combined
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
23:00
02-01-2021


Not secure
13.234.117.173:8000/en-US/app/Webanalysis/search?q=search%20index%3Dmyappindex&sid=1609608386.10_E1E3E8B3-427C-4007-8752-937F5F2E1D8...
Events (34)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1
2
Next
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
a host 1
a source 2
a sourcetype 2
INTERESTING FIELDS
bytes 21
a clientip 4
date_hour 2
date_mday 1
date_minute 5
a date_month 1
date_second 12
a date_wday 1
date_year 1
date_zone 2
a file 20
a ident 1
a index 1
linecount 1
clientip
4 Values, 82.353% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
157.44.89.217
23
82.143%
35.176.140.11
2
7.143%
::1
2
7.143%
198.20.124.218
1
3.571%
o/favicon.ico HTTP/1.1" 200 1150 "http://52.66.213.110/" "Mozill
like Gecko) Chrome/87.0.4280.88 Safari/537.36"
ttpd/logs/access_log
sourcetype = access_combined
" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
6"
ttpd/logs/access_log
sourcetype = access_combined
o/favicon.ico HTTP/1.1" 200 1150 "http://52.66.213.110/" "Mozill
like Gecko) Chrome/87.0.4280.88 Safari/537.36"
ttpd/logs/access_log
sourcetype = access_combined
" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
6"
ttpd/logs/access_log
sourcetype = access_combined
1" 200 9465 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/53
5:11:12.000 PM
7.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"
host = ip-172-31-36-203.ap-south-1.compute.internal
source = /etc/httpd/logs/access_log
sourcetype = access_combined
1/2/21
5:11:12.000 PM
35.176.140.11 - - [02/Jan/2021:17:11:12 +0000] "GET /.env HTTP/1.1" 404 196 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/5
37.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
23:04
02-01-2021


Inbox (445) - revanthini
Splunk-Admin_Dec06-2
Instances | EC2 Manage
Myprojectdashboard | S
Myprojectdashboard
Start Course - Intellipaa
Not secure | 13.233.254.72:8000/en-US/app/Webanalysis/myprojectdashboard
Myprojectdashboard
Edit
Export
...
clientip
City
Country
Region
209.17.96.218 United States
89.248.168.108 Netherlands
172.105.89.161 Frankfurt am Main Germany Hesse
87.107.58.36 Iran
45.228.255.38 Mogi Guacu Brazil Sao Paulo
178.128.194.144 Frankfurt am Main Germany Hesse
98.149.84.193 Stanton United States California
182.141.155.236 China
128.14.133.58 United States
184.72.3.159 San Jose United States California
185.239.242.162 Netherlands
157.230.114.109 Frankfurt am Main Germany Hesse
139.162.119.197 Tokyo Japan Tokyo
205.185.126.93 San Jose United States California
45.229.55.29 Carapicuiba Brazil Sao Paulo
167.250.140.168 Caico Brazil Rio Grande do Norte
209.17.96.210 United States
196.52.43.62 South Africa Orange Free State
47.111.238.21 China
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
11:30
03-01-2021