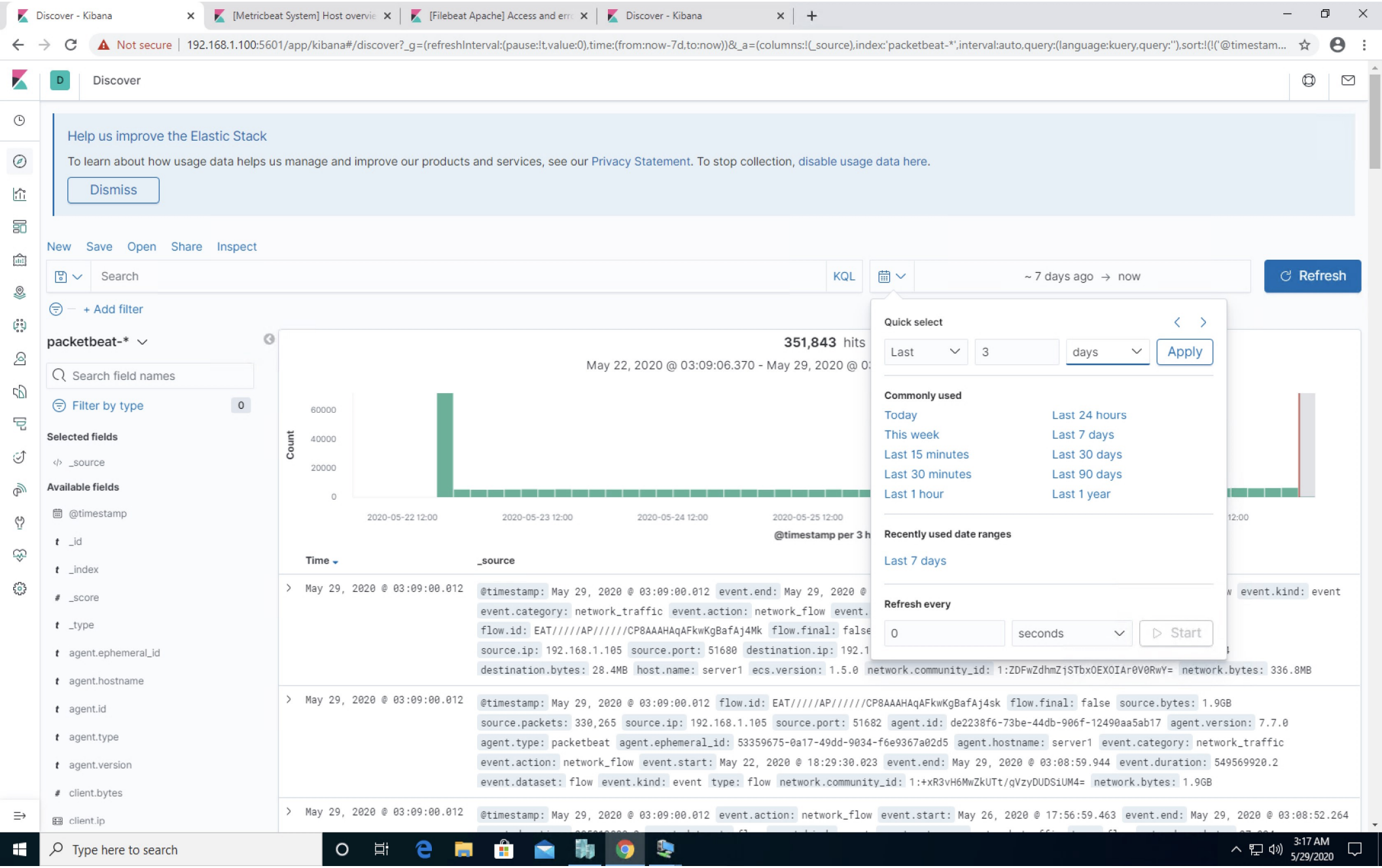
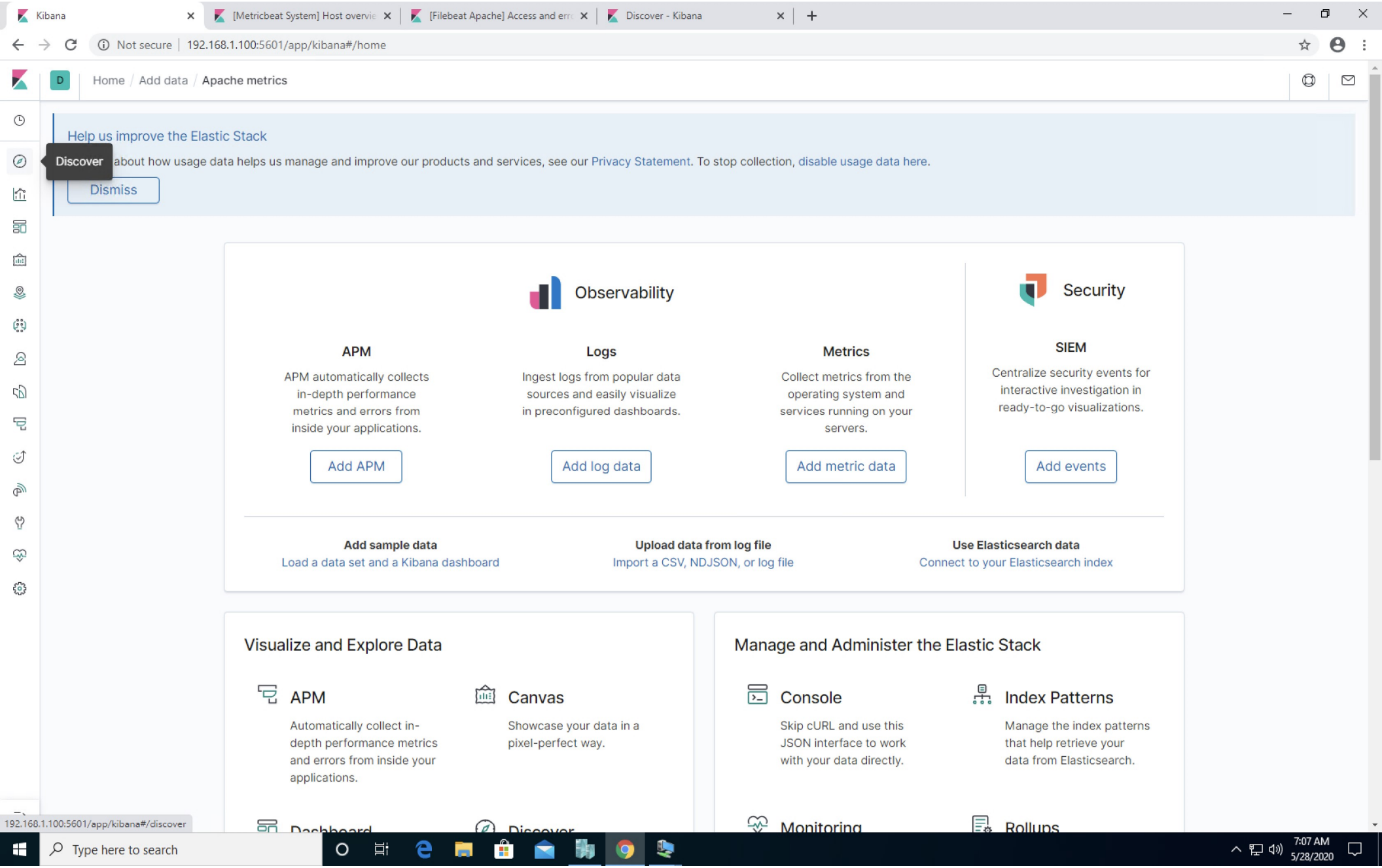
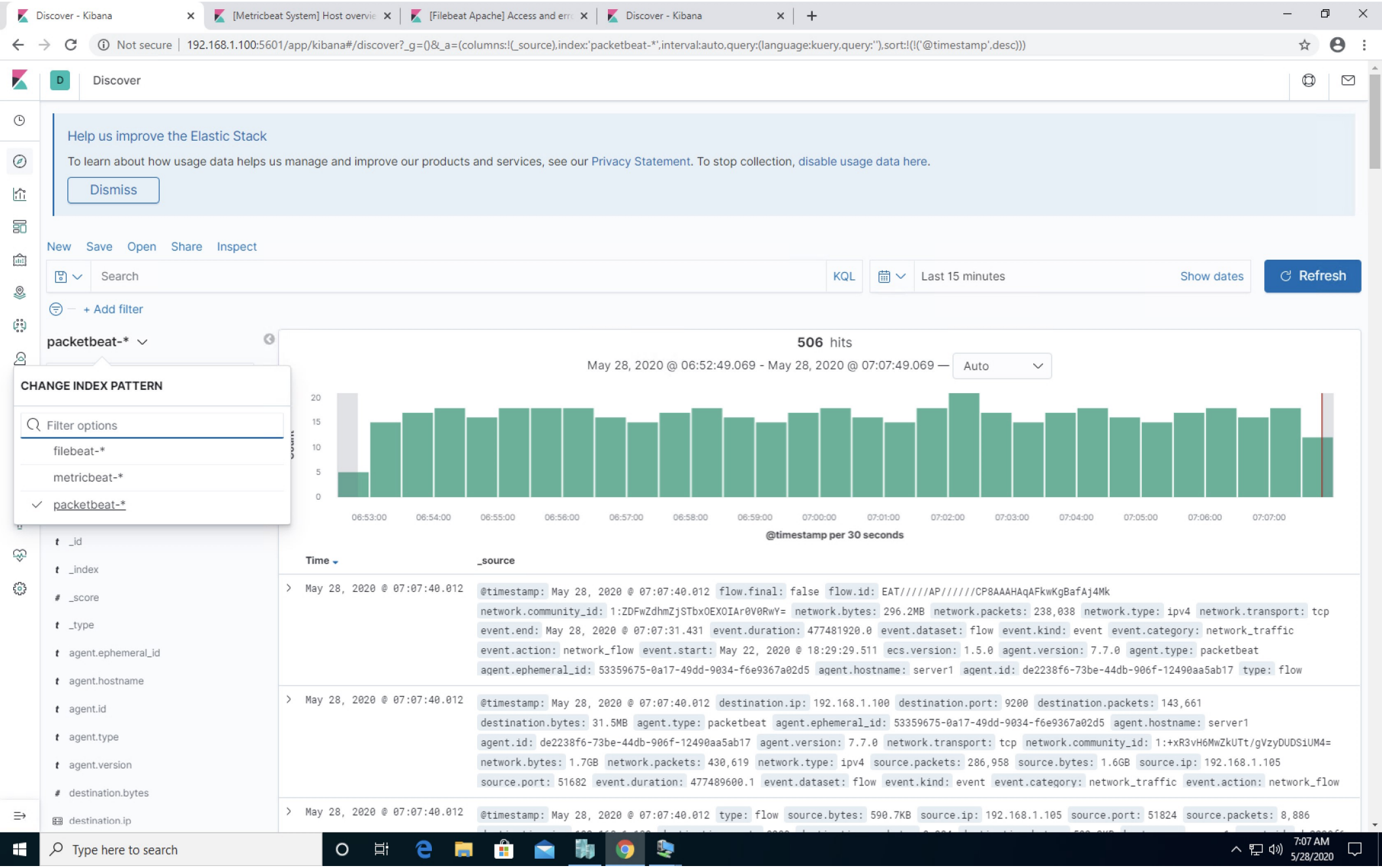

Discover - Kibana
[Metricbeat System] Host overvie
[Filebeat Apache] Access and err
Discover - Kibana
Not secure
192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(_source),index:'packetbeat-*',interval:auto,query:(language:kuery,query:''),sort:!(!('@timestam...
Discover
Help us improve the Elastic Stack
To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.
Dismiss
New
Save
Open
Share
Inspect
Search
KQL
~ 7 days ago → now
Refresh
+ Add filter
packetbeat-*
Search field names
Filter by type
0
Selected fields
_source
Available fields
@timestamp
_id
_index
_score
_type
agent.ephemeral_id
agent.hostname
agent.id
agent.type
agent.version
client.bytes
client.ip
351,843 hits
May 22, 2020 @ 03:09:06.370 - May 29, 2020 @ 0
Count
60000
40000
20000
0
2020-05-22 12:00
2020-05-23 12:00
2020-05-24 12:00
2020-05-25 12:00
@timestamp per 3 h
Time
_source
May 29, 2020 @ 03:09:00.012
@timestamp: May 29, 2020 @ 03:09:00.012 event.end: May 29, 2020 @
event.kind: event
event.category: network_traffic event.action: network_flow event.
flow.id: EAT/////AP//////CP8AAAHAqAFkwKgBafAj4Mk flow.final: false
source.ip: 192.168.1.105 source.port: 51680 destination.ip: 192.1
destination.bytes: 28.4MB host.name: server1 ecs.version: 1.5.0 network.community_id: 1:ZDFwZdhmZjSTbxOEXOIAr0V0RwY= network.bytes: 336.8MB
May 29, 2020 @ 03:09:00.012
@timestamp: May 29, 2020 @ 03:09:00.012 flow.id: EAT/////AP//////CP8AAAHAqAFkwKgBafAj4sk flow.final: false source.bytes: 1.9GB
source.packets: 330,265 source.ip: 192.168.1.105 source.port: 51682 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0
agent.type: packetbeat agent.ephemeral_id: 53359675-0a17-49dd-9034-f6e9367a02d5 agent.hostname: server1 event.category: network_traffic
event.action: network_flow event.start: May 22, 2020 @ 18:29:30.023 event.end: May 29, 2020 @ 03:08:59.944 event.duration: 549569920.2
event.dataset: flow event.kind: event type: flow network.community_id: 1:+xR3vH6MwZkUTt/qVzyDUDSiUM4= network.bytes: 1.9GB
May 29, 2020 @ 03:09:00.012
@timestamp: May 29, 2020 @ 03:09:00.012 event.action: network_flow event.start: May 26, 2020 @ 17:56:59.463 event.end: May 29, 2020 @ 03:08:52.264
Quick select
Last
3
days
Apply
Commonly used
Today
Last 24 hours
This week
Last 7 days
Last 15 minutes
Last 30 days
Last 30 minutes
Last 90 days
Last 1 hour
Last 1 year
Recently used date ranges
Last 7 days
Refresh every
0
seconds
Start
Type here to search
3:17 AM
5/29/2020


Kibana
[Metricbeat System] Host overvie
[Filebeat Apache] Access and err
Discover - Kibana
Not secure | 192.168.1.100:5601/app/kibana#/home
D
Home / Add data / Apache metrics
Help us improve the Elastic Stack
Discover
about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.
Dismiss
Observability
APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM
Logs
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Add log data
Metrics
Collect metrics from the operating system and services running on your servers.
Add metric data
Security
SIEM
Centralize security events for interactive investigation in ready-to-go visualizations.
Add events
Add sample data
Load a data set and a Kibana dashboard
Upload data from log file
Import a CSV, NDJSON, or log file
Use Elasticsearch data
Connect to your Elasticsearch index
Visualize and Explore Data
APM
Automatically collect in-depth performance metrics and errors from inside your applications.
Canvas
Showcase your data in a pixel-perfect way.
Manage and Administer the Elastic Stack
Console
Skip cURL and use this JSON interface to work with your data directly.
Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.
Monitoring
Rollups
192.168.1.100:5601/app/kibana#/discover
Type here to search
7:07 AM
5/28/2020


Discover - Kibana
[Metricbeat System] Host overvie
[Filebeat Apache] Access and err
Discover - Kibana
Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:'packetbeat-*',interval:auto,query:(language:kuery,query:''),sort:!(!('@timestamp',desc)))
Discover
Help us improve the Elastic Stack
To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.
Dismiss
New Save Open Share Inspect
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
packetbeat-*
CHANGE INDEX PATTERN
Filter options
filebeat-*
metricbeat-*
packetbeat-*
506 hits
May 28, 2020 @ 06:52:49.069 - May 28, 2020 @ 07:07:49.069 —
Auto
Count
20
15
10
5
0
06:53:00
06:54:00
06:55:00
06:56:00
06:57:00
06:58:00
06:59:00
07:00:00
07:01:00
07:02:00
07:03:00
07:04:00
07:05:00
07:06:00
07:07:00
@timestamp per 30 seconds
Time
_source
May 28, 2020 @ 07:07:40.012
@timestamp: May 28, 2020 @ 07:07:40.012 flow.final: false flow.id: EAT/////AP//////CP8AAAHAqAFkwKgBafAj4Mk
network.community_id: 1:ZDFwZdhmZjSTbxOEXOIAr0V0RwY= network.bytes: 296.2MB network.packets: 238,038 network.type: ipv4 network.transport: tcp
event.end: May 28, 2020 @ 07:07:31.431 event.duration: 477481920.0 event.dataset: flow event.kind: event event.category: network_traffic
event.action: network_flow event.start: May 22, 2020 @ 18:29:29.511 ecs.version: 1.5.0 agent.version: 7.7.0 agent.type: packetbeat
agent.ephemeral_id: 53359675-0a17-49dd-9034-f6e9367a02d5 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 type: flow
May 28, 2020 @ 07:07:40.012
@timestamp: May 28, 2020 @ 07:07:40.012 destination.ip: 192.168.1.100 destination.port: 9200 destination.packets: 143,661
destination.bytes: 31.5MB agent.type: packetbeat agent.ephemeral_id: 53359675-0a17-49dd-9034-f6e9367a02d5 agent.hostname: server1
agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 network.transport: tcp network.community_id: 1:+xR3vH6MwZkUTt/gVzyDUDSiUM4=
network.bytes: 1.7GB network.packets: 430,619 network.type: ipv4 source.packets: 286,958 source.bytes: 1.6GB source.ip: 192.168.1.105
source.port: 51682 event.duration: 477489600.1 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow
May 28, 2020 @ 07:07:40.012
@timestamp: May 28, 2020 @ 07:07:40.012 type: flow source.bytes: 590.7KB source.ip: 192.168.1.105 source.port: 51824 source.packets: 8,886
_id
_index
_score
_type
agent.ephemeral_id
agent.hostname
agent.id
agent.type
agent.version
destination.bytes
destination.ip
Type here to search
7:07 AM
5/28/2020

Discover - Kibana | [Metricbeat System] Host overvie | [Filebeat Apache] Access and err | Discover - Kibana

Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(_source),index:'packetbeat-*',interval:auto,query:(language:kuery,query:'source.ip%20:%2019...

D Discover

Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Dismiss

New Save Open Share Inspect

source.ip : 192.168.1.90 KQL ~ 7 days ago → now Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

@timestamp
_id
_index
_score
_type
agent.ephemeral_id
agent.hostname
agent.id
agent.type
agent.version
client.bytes
client.ip

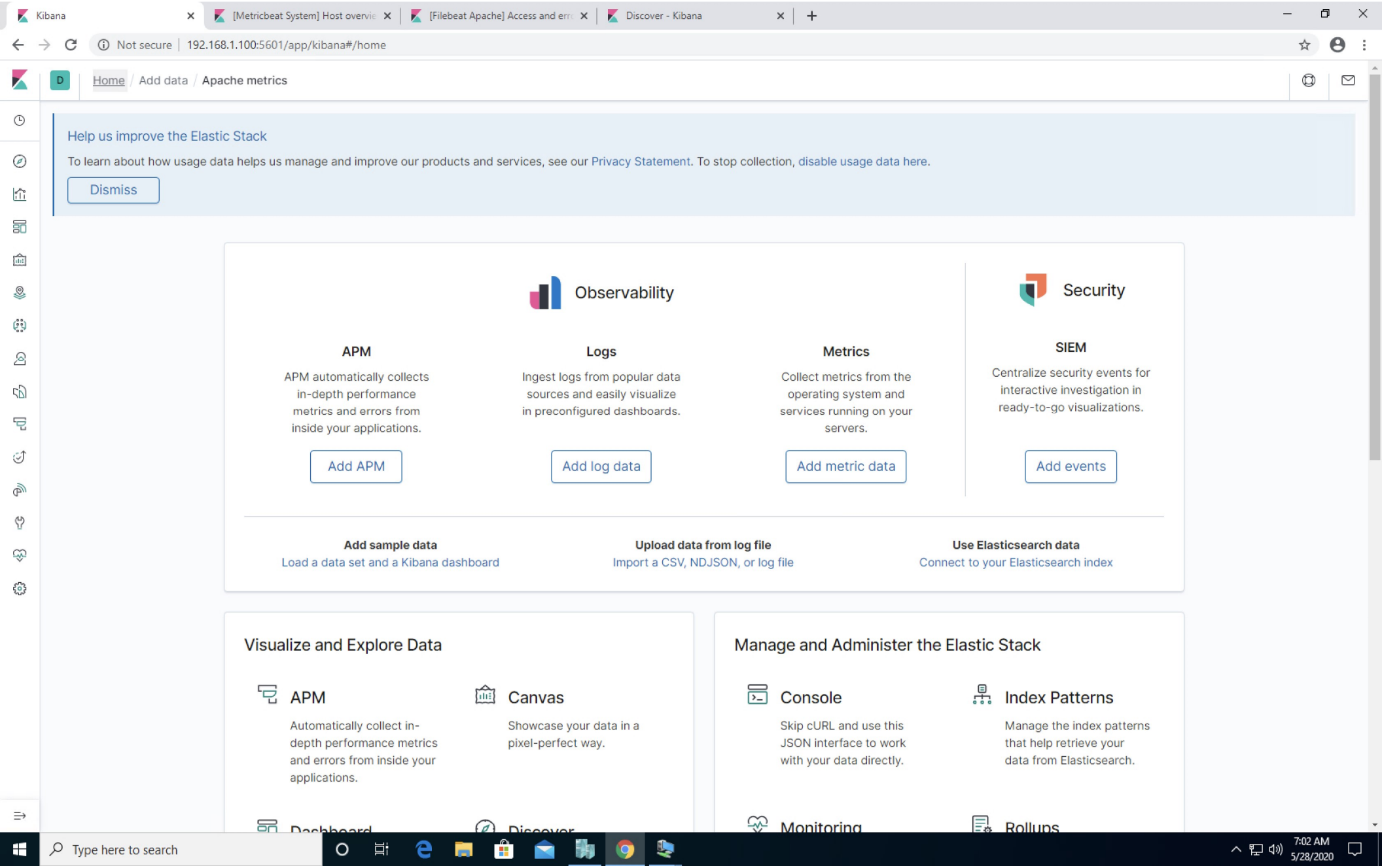
67,026 hits

May 22, 2020 @ 03:33:23.525 - May 29, 2020 @ 03:33:23.525 — Auto

Time	_source
May 26, 2020 @ 18:02:00.012	@timestamp: May 26, 2020 @ 18:02:00.012 destination.packets: 8 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 3.2KB host.name: server1 network.type: ipv4 network.transport: tcp network.community_id: 1:g+55eUgfq3ZGGa2WO4RqL6uIQUo= network.bytes: 5.5KB network.packets: 19 event.duration: 11264.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: May 26, 2020 @ 18:00:50.407 event.end: May 26, 2020 @ 18:01:01.671 flow.final: true flow.id: EAz/////AP//////CAwAAAHAqAFawKqBaSzhUABaJwAAAAAAAA type: flow ecs.version: 1.5.0 agent.id: de2238f6-73be-44db-906f-12490aa5ab17
May 26, 2020 @ 18:01:50.012	@timestamp: May 26, 2020 @ 18:01:50.012 destination.ip: 192.168.1.105 destination.port: 80 destination.packets: 8 destination.bytes: 3.2KB event.duration: 11264.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: May 26, 2020 @ 18:00:50.407 event.end: May 26, 2020 @ 18:01:01.671 host.name: server1 agent.ephemeral_id: 53359675-0a17-49dd-9034-f6e9367a02d5 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat flow.id: EAz/////AP//////CAwAAAHAqAFawKqBaSzhUABaJwAAAAAAAA flow.final: false type: flow network.transport: tcp
May 26, 2020 @ 18:01:40.012	@timestamp: May 26, 2020 @ 18:01:40.012 type: flow ecs.version: 1.5.0 host.name: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17

Type here to search

3:33 AM 5/29/2020


Kibana
[Metricbeat System] Host overvie
[Filebeat Apache] Access and err
Discover - Kibana
Not secure
192.168.1.100:5601/app/kibana#/home
D
Home / Add data / Apache metrics
Help us improve the Elastic Stack
To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.
Dismiss
Observability
APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM
Logs
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Add log data
Metrics
Collect metrics from the operating system and services running on your servers.
Add metric data
Security
SIEM
Centralize security events for interactive investigation in ready-to-go visualizations.
Add events
Add sample data
Load a data set and a Kibana dashboard
Upload data from log file
Import a CSV, NDJSON, or log file
Use Elasticsearch data
Connect to your Elasticsearch index
Visualize and Explore Data
APM
Automatically collect in-depth performance metrics and errors from inside your applications.
Canvas
Showcase your data in a pixel-perfect way.
Dashboard
Discover
Manage and Administer the Elastic Stack
Console
Skip cURL and use this JSON interface to work with your data directly.
Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.
Monitoring
Rollups
Type here to search
7:02 AM
5/28/2020

Discover - Kibana | [Metricbeat System] Host overvie | [Filebeat Apache] Access and err | Discover - Kibana

Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(_source),index:'packetbeat-*',interval:auto,query:(language:kuery,query:'NOT%20http.respon...

D Discover

Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Dismiss

New Save Open Share Inspect

NOT http.response.status_code : 500 KQL ~ 7 days ago → now Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

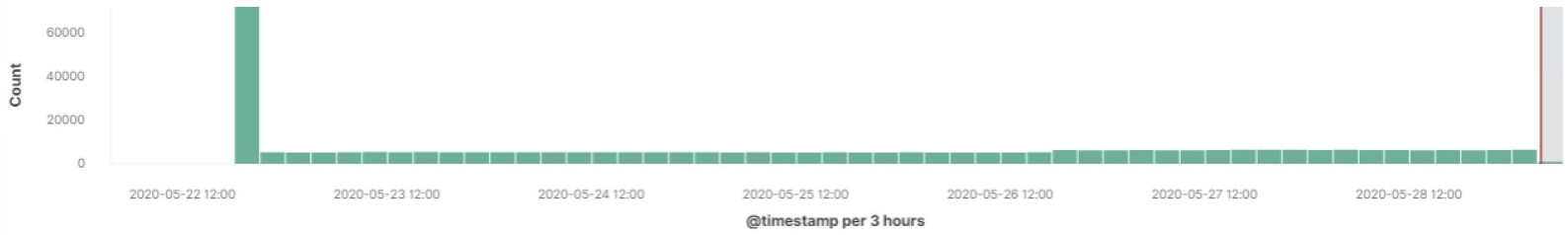
_source

Available fields

@timestamp
_id
_index
_score
_type
agent.ephemeral_id
agent.hostname add
agent.id
agent.type
agent.version
client.bytes
client.ip

352,379 hits

May 22, 2020 @ 03:24:59.734 - May 29, 2020 @ 03:24:59.734 — Auto



Time	_source
May 29, 2020 @ 03:24:50.012	@timestamp: May 29, 2020 @ 03:24:50.012 event.duration: 550512000.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: May 22, 2020 @ 18:29:29.511 event.end: May 29, 2020 @ 03:24:41.511 source.ip: 192.168.1.105 source.port: 51680 source.bytes: 308.9MB source.packets: 160,383 host.name: server1 agent.ephemeral_id: 53359675-0a17-49dd-9034-f6e9367a02d5 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat flow.final: false flow.id: EAT/////AP//////CP8AAAHAqAFkwKqBafAj4Mk type: flow network.type: ipv4 network.transport: tcp
May 29, 2020 @ 03:24:50.012	@timestamp: May 29, 2020 @ 03:24:50.012 source.packets: 330,837 source.bytes: 1.9GB source.ip: 192.168.1.105 source.port: 51682 event.end: May 29, 2020 @ 03:24:49.704 event.duration: 550519680.4 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: May 22, 2020 @ 18:29:30.023 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 53359675-0a17-49dd-9034-f6e9367a02d5 agent.hostname: server1 ecs.version: 1.5.0 host.name: server1 type: flow network.packets: 496,459 network.type: ipv4 network.transport: tcp network.community_id: 1:+xR3vH6MwZkUTt/qVzyDUDSiUM4=
May 29, 2020 @ 03:24:50.012	@timestamp: May 29, 2020 @ 03:24:50.012 flow.id: EAT/////AP//////CP8AAAHAqAFkwKgBafAjcMo flow.final: false type: flow network.type: ipv4 network.transport: tcp network.community_id: 1:qT10kKyQlhhbTkBx18ygWtL/E2U= network.bytes: 1.8MB network.packets: 27,460 source.ip: 192.168.1.105

Type here to search

3:25 AM 5/29/2020