NOLSATU

Elastic Stack Administration (EL-ADM)

Keywords

Elasticsearch, Logstash, Kibana, Beat, Elastic Stack, Log Data, Log Management

References

- https://www.elastic.co/guide/index.html
- Learning Elastic Stack 6.0 - Pranav Shukla & Sharath Kumar 2017

Log Data and Log Management

What is Log Data?

Log data is the intrinsic meaning that a log message has. Or put another way, log data is the information pulled out of a log message to tell you why the log message generated

What is Log Management?

Log management (LM) comprises an approach to dealing with large volumes of computer-generated log messages (also known as audit records, audit trails, event-logs, etc.)

What does LM cover?

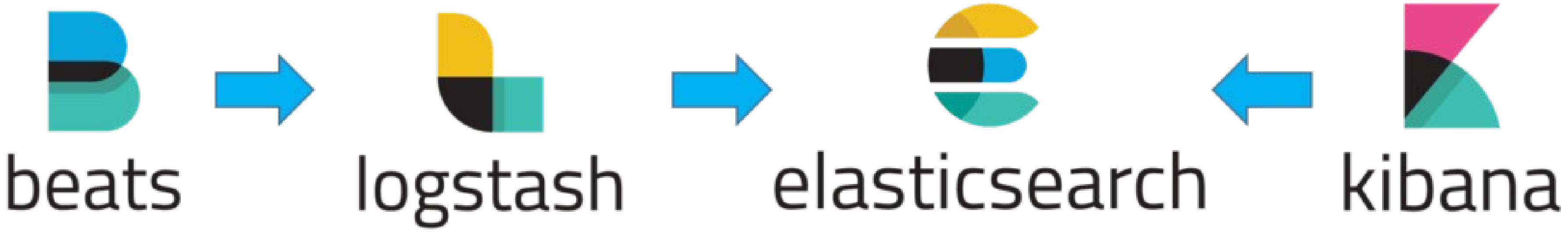
- Log collection
- Centralized log aggregation
- Long-term log storage and retention
- Log rotation
- Log analysis (in real-time and in bulk after storage)
- Log search and reporting.

elastic stack

What is Elastic Stack?

- Consist of Elasticsearch, Logstash, Kibana, and Beat
- Built on an open source foundation
- The Elastic Stack lets you reliably and securely take data from any source, in any format, and search, analyze, and visualize it in real time.

Elastic Stack Architecture



Data Collection

Data Aggregation & Processing

Indexing & storage

Analysis & visualization

Elasticsearch (1)

Elasticsearch is a distributed, RESTful search and analytics engine capable of solving a growing number of use cases. As the heart of the Elastic Stack, it centrally stores your data so you can discover the expected and uncover the unexpected.

Elasticsearch (2)

- Elasticsearch lets you perform and combine many types of searches — structured, unstructured, geo, metric — any way you want.
- Elasticsearch aggregations let you zoom out to explore trends and patterns in your data.
- It scales horizontally to handle kajillions of events per second, while automatically managing how indices and queries are distributed across the cluster for oh-so smooth operations.

Logstash (1)

Logstash is a dynamic data collection pipeline with an extensible plugin ecosystem and strong Elasticsearch synergy.

Logstash (2)

- Logstash supports a variety of inputs that pull in events from a multitude of common sources, all at the same time.
- As data travels from source to store, Logstash filters parse each event, identify named fields to build structure, and transform them to converge on a common format for easier, accelerated analysis and business value.
- Logstash has a variety of outputs that let you route data where you want, giving you the flexibility to unlock a slew of downstream use cases.

Logstash (3)

- **Input plugin**: beats, exec, file, github, stdin syslog, twitter, tcp, udp, websocket, http.
- **Filter plugin**: cidr, csv, date, dns, geoip, grok, json, mutate, useragent, urldecode.
- **Output plugin**: elasticsearch, datadog, email, file, influxdb, stdout.

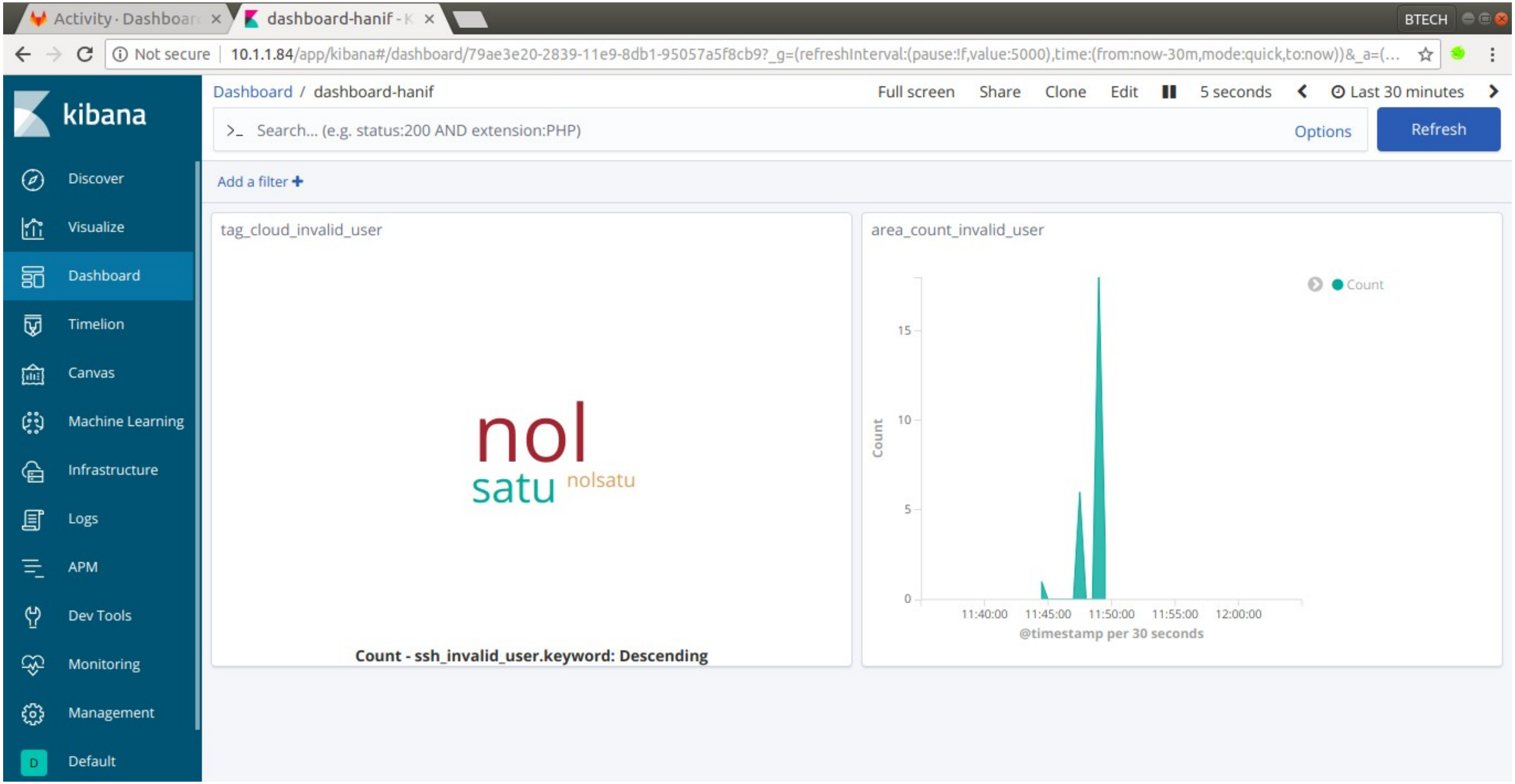
Check:

- https://www.elastic.co/guide/en/logstash/current/input-plugins.html
- https://www.elastic.co/guide/en/logstash/current/filter-plugins.html
- https://www.elastic.co/guide/en/logstash/current/output-plugins.html

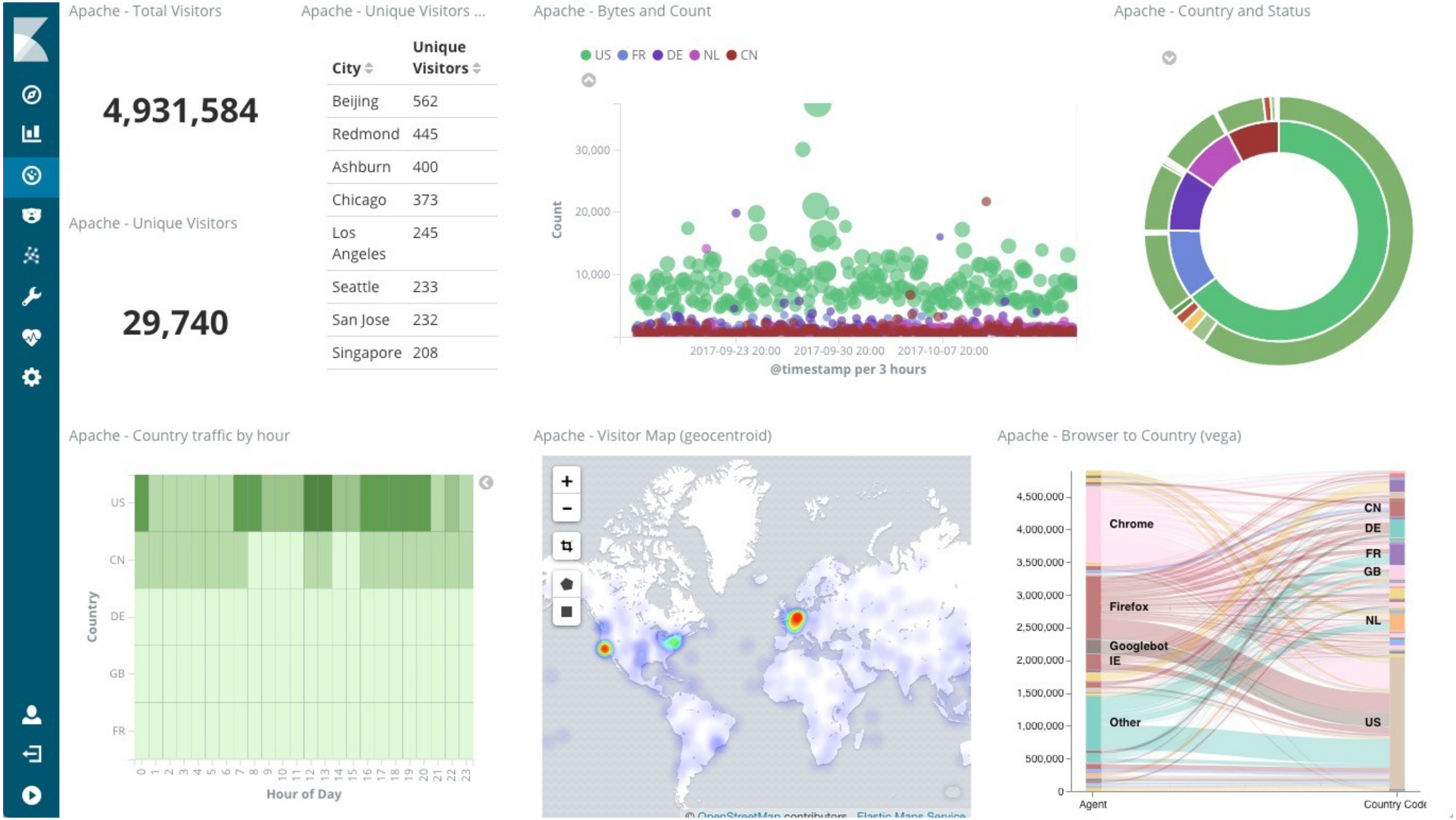
Kibana (1)

Kibana gives shape to your data and is the extensible user interface for configuring and managing all aspects of the Elastic Stack.

Kibana (2)


Activity · Dashboard
dashboard-hanif - K
BTECH
Not secure
10.1.1.84/app/kibana#/dashboard/79ae3e20-2839-11e9-8db1-95057a5f8cb9?_g=(refreshInterval:(pause:!f,value:5000),time:(from:now-30m,mode:quick,to:now))&_a=(…
kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
D Default
Dashboard / dashboard-hanif
Full screen
Share
Clone
Edit
5 seconds
Last 30 minutes
>_ Search... (e.g. status:200 AND extension:PHP)
Options
Refresh
Add a filter +
tag_cloud_invalid_user
nol
satu
nolsatu
Count - ssh_invalid_user.keyword: Descending
area_count_invalid_user
● Count
Count
15
10
5
0
11:40:00
11:45:00
11:50:00
11:55:00
12:00:00
@timestamp per 30 seconds

Kibana (3)



Apache - Total Visitors

4,931,584

Apache - Unique Visitors

29,740

Apache - Unique Visitors ...

City	Unique Visitors
Beijing	562
Redmond	445
Ashburn	400
Chicago	373
Los Angeles	245
Seattle	233
San Jose	232
Singapore	208

Apache - Bytes and Count

Apache - Country and Status

Apache - Country traffic by hour

Apache - Visitor Map (geocentroid)

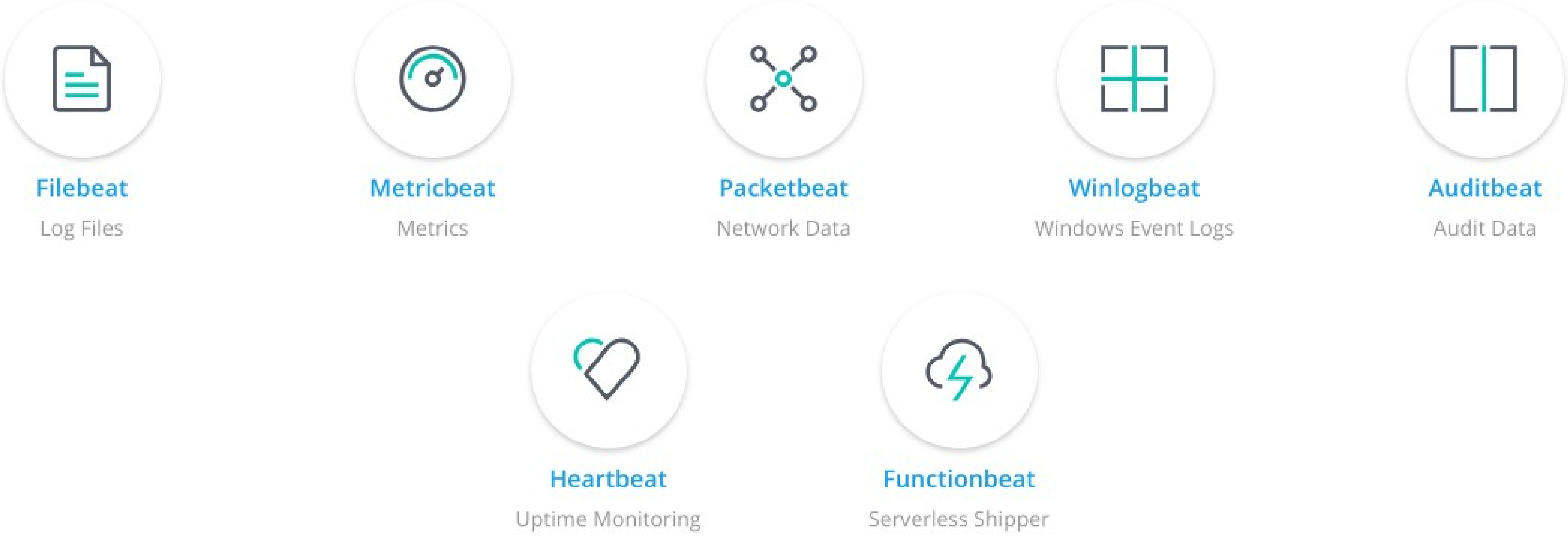
Apache - Browser to Country (vega)

Beat

Beats is a platform for lightweight shippers that send data from edge machines to Logstash and Elasticsearch.

The Beats Family

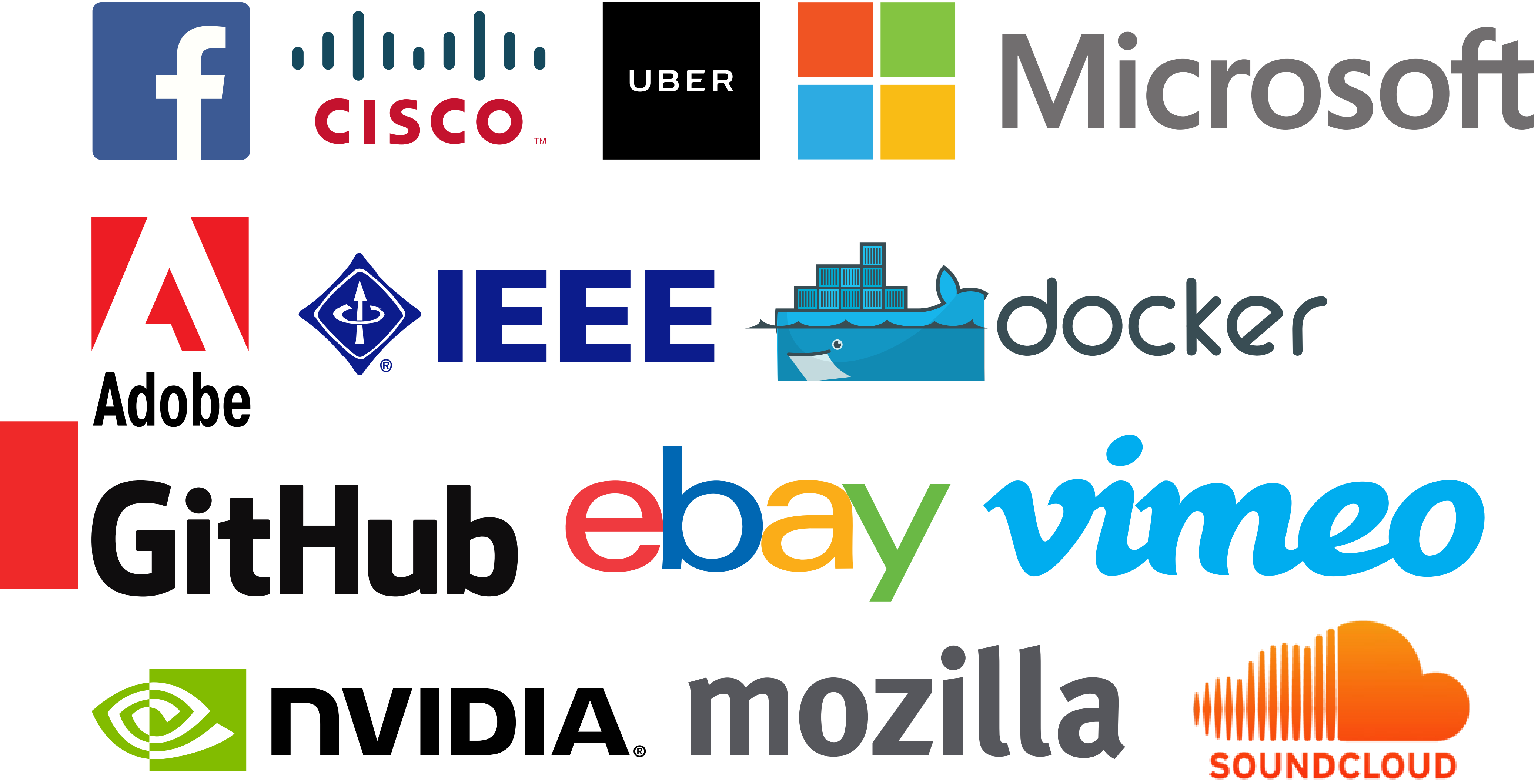
- Filebeat
- Metricbeat
- Packetbeat
- Winlogbeat
- Auditbeat
- Heartbeat
- Functionbeat



Use Cases

- Log and security analytics
- Product search
- Metrics analytics
- Web search and website search

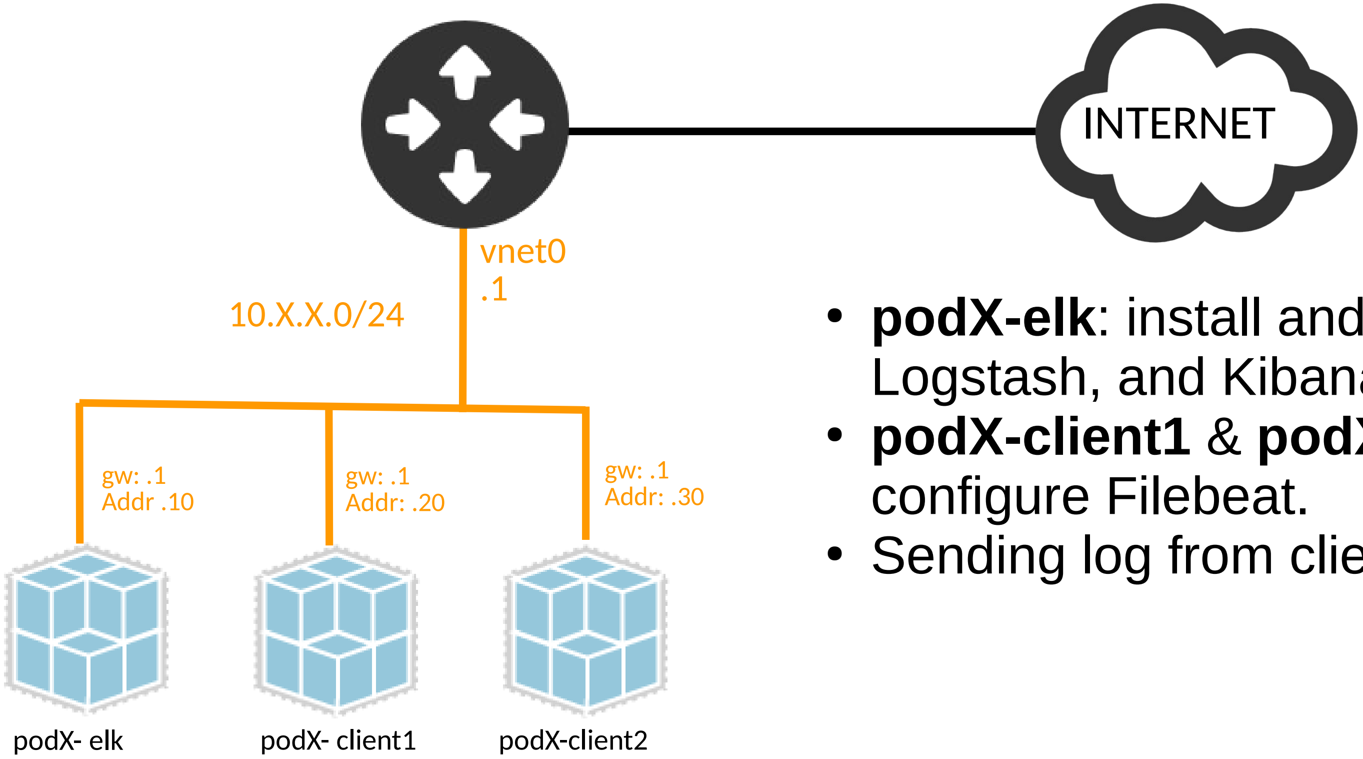
Elastic Stack Users



Lab 1

Elasticsearch, Logstash, and Kibana Administration

Lab 1 Topology

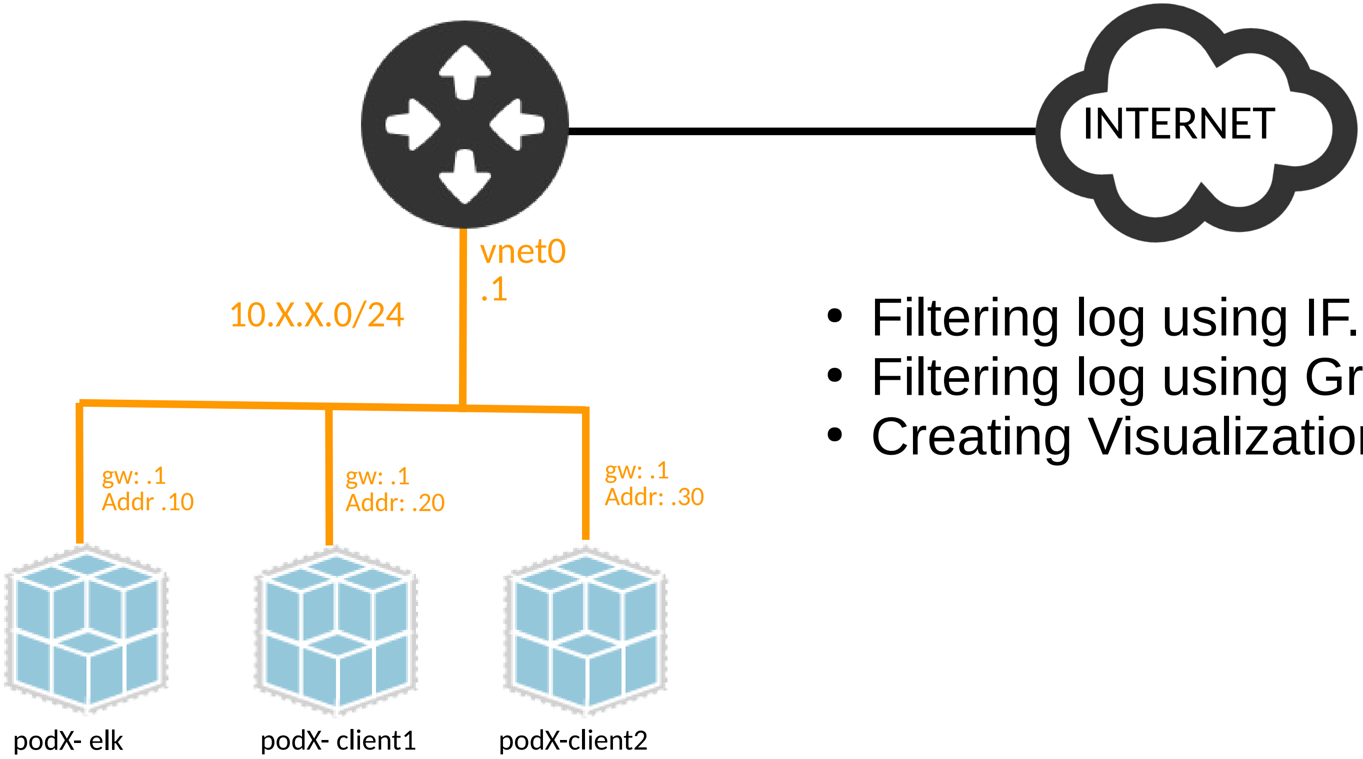


- **podX-elk**: install and configure Elasticsearch, Logstash, and Kibana.
- **podX-client1** & **podX-client2**: install and configure Filebeat.
- Sending log from client to elk server.

Lab 2

Elasticsearch, Logstash, and Kibana Administration

Lab 2 Topology



- Filtering log using IF.
- Filtering log using Grok.
- Creating Visualization and Dashboard.

NolSatu.id