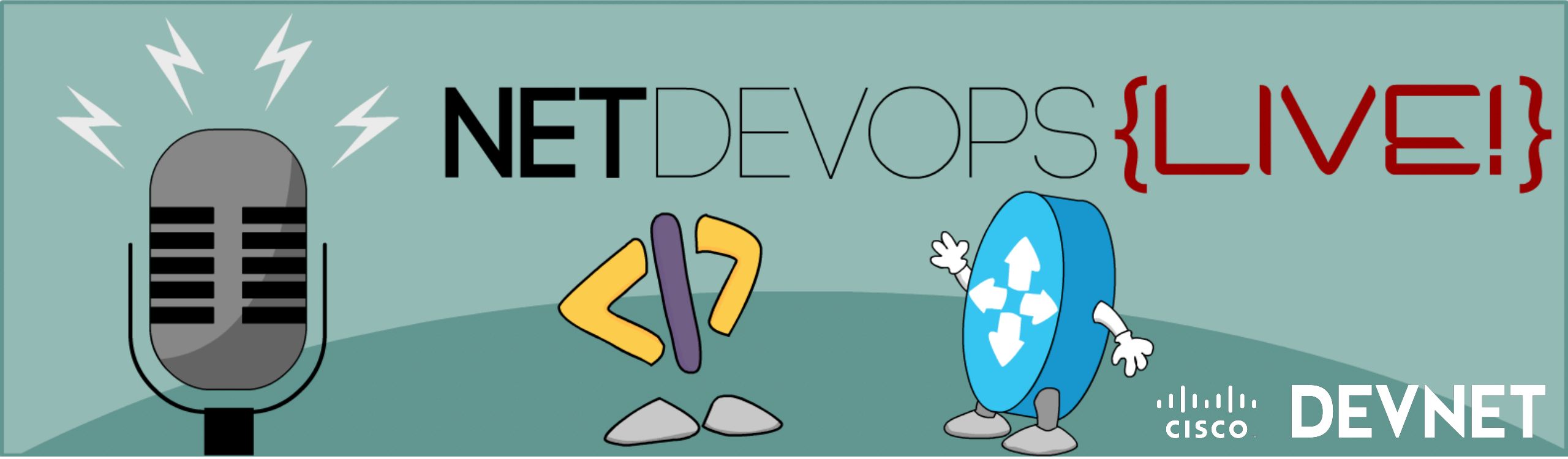


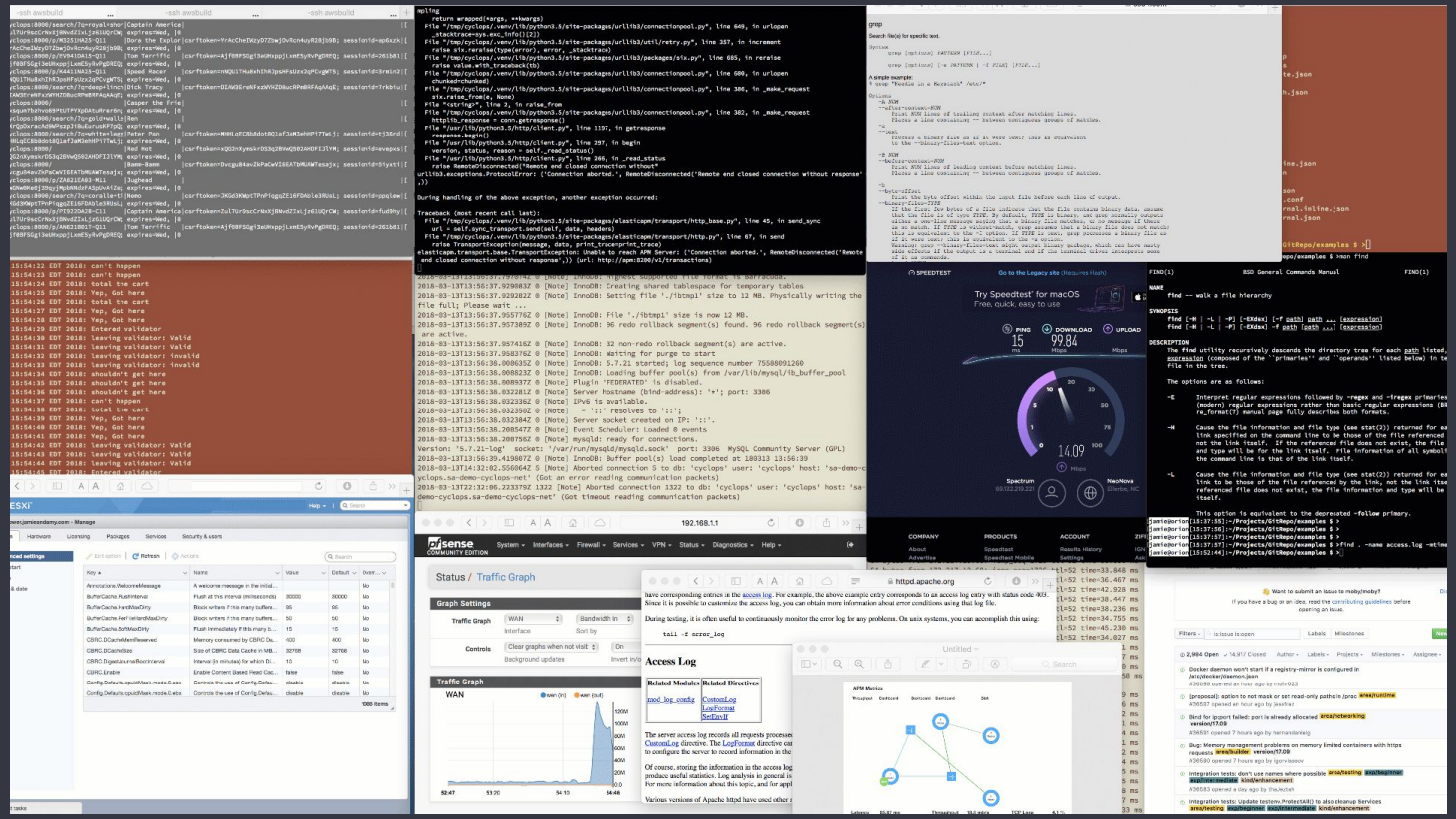
Logging and Back Again – A Network Engineers Journey with ELK

George Kobar
Elastic
Twitter: @GeorgeKobar

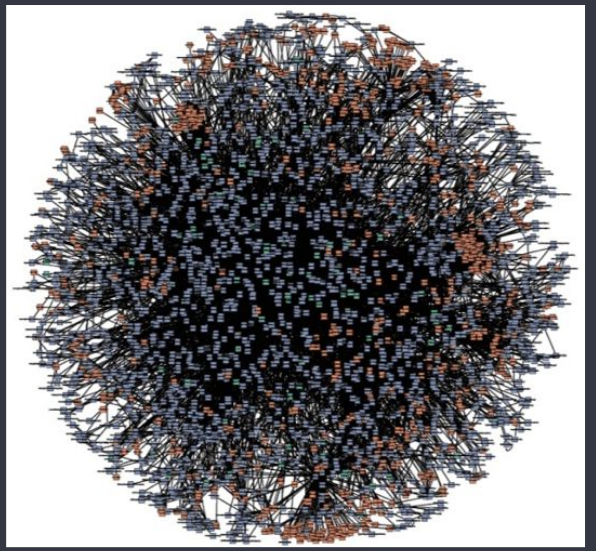
Season 3, Talk 7
Hosted by Hank Preston, NetDevOps Engineer
Twitter: @hfpreston
https://developer.cisco.com/netdevops/live

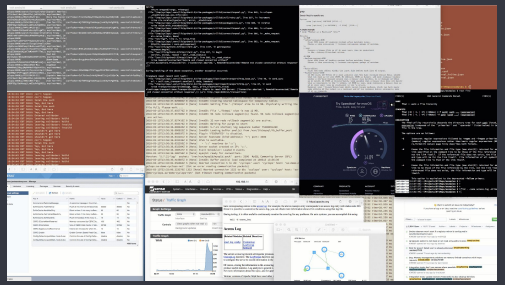

elastic
Logging and Back Again -
A Network Engineers Journey with ELK
(Elastic Stack)
George Kobar
Sr Community Advocate
@GeorgeKobar

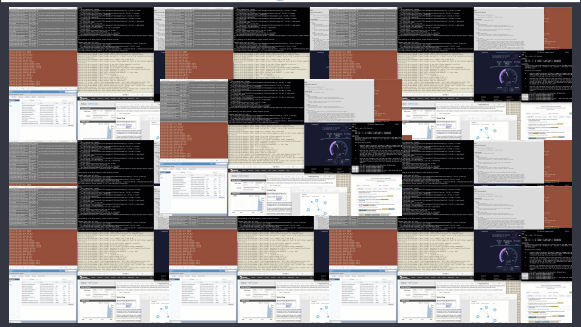
Back in My Day...



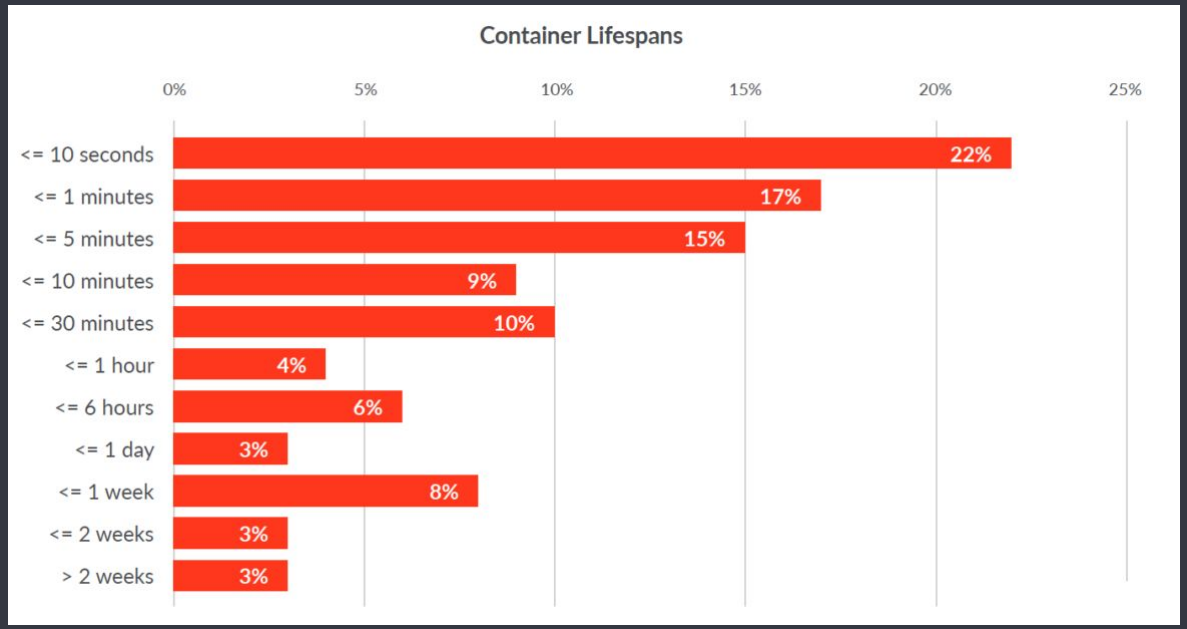
New Application Development





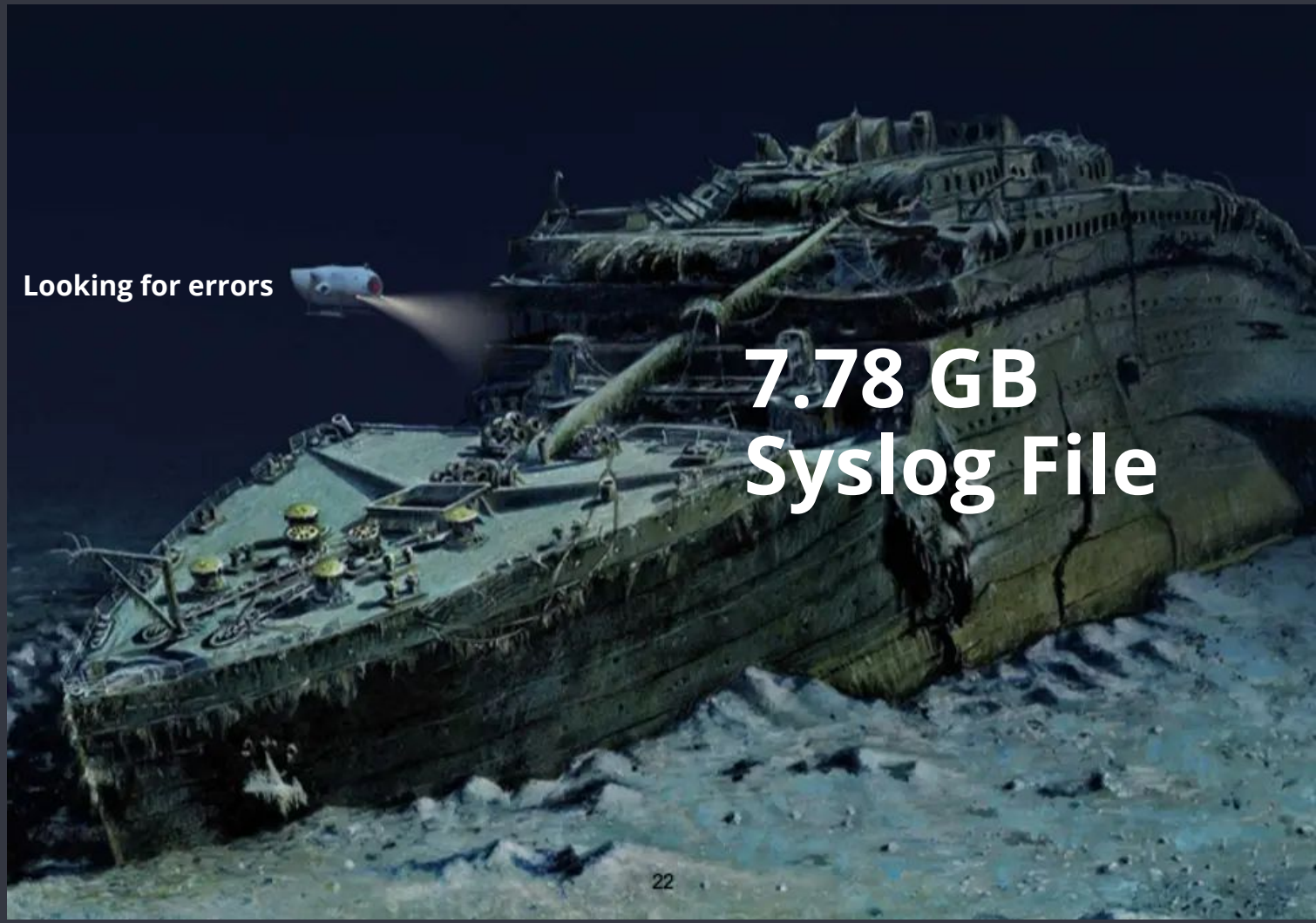


This is Fine



Source: https://sysdig.com/blog/sysdig-2019-container-usage-report/

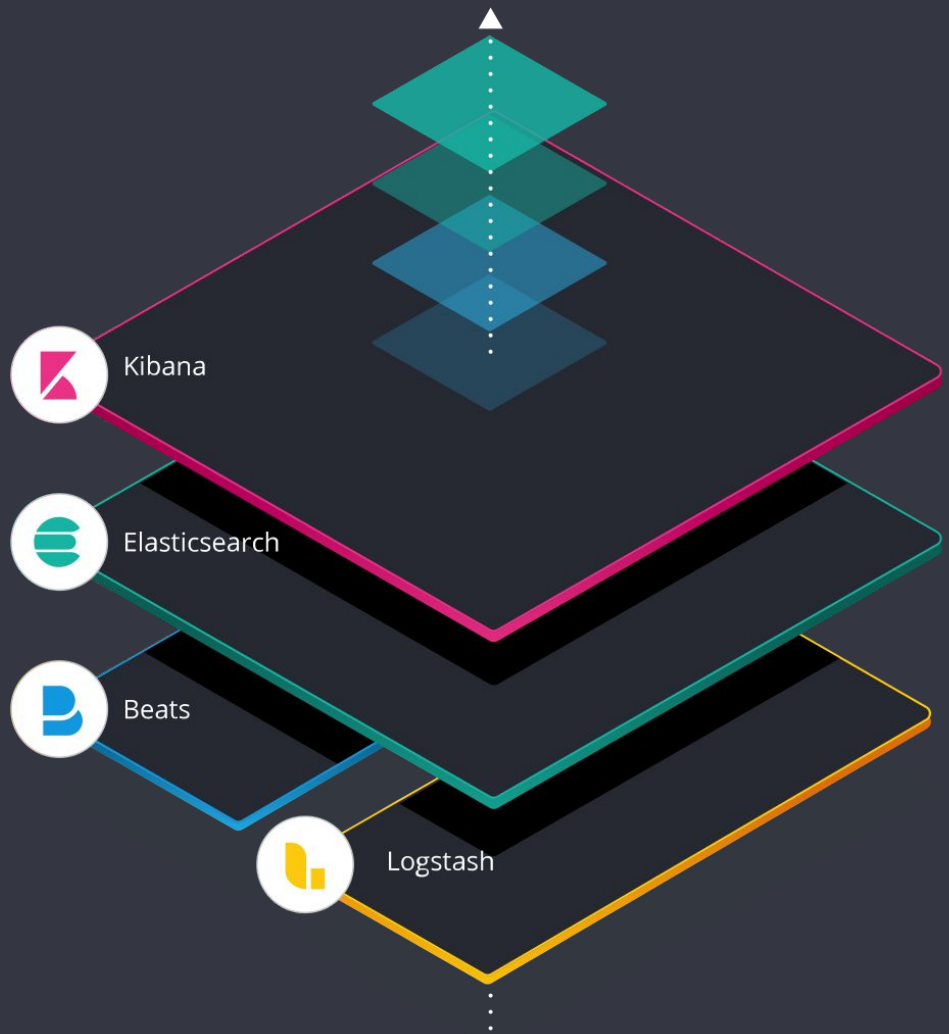
Syslog....?



This is a search problem.

Elastic is a search company.

Elastic (ELK) Stack



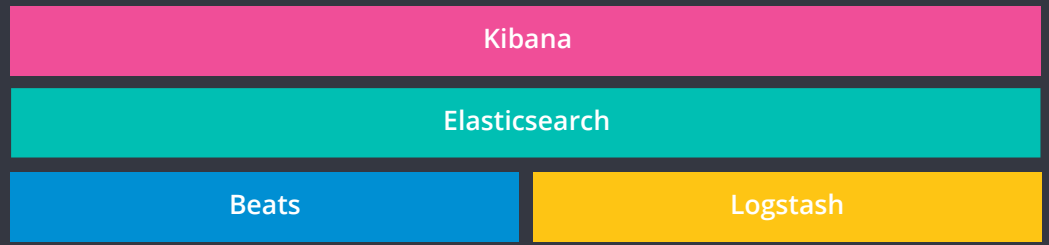
Open Source

3 Solutions Powered by 1 Stack

Elastic Enterprise Search

Elastic Observability

Elastic Security



Elastic Stack

Kibana

Elasticsearch

Beats | Logstash

Self-Managed

Elastic Cloud

Elastic Cloud Enterprise

Elastic Cloud on Kubernetes

Standalone

SaaS

Orchestration

3 Solutions Powered by 1 Stack

Elastic Enterprise Search

Elastic Observability

Elastic Security

Elastic Stack

logs

+

metrics

+

apm

=

Observability
or
O11Y

logs

+

metrics

+

apm

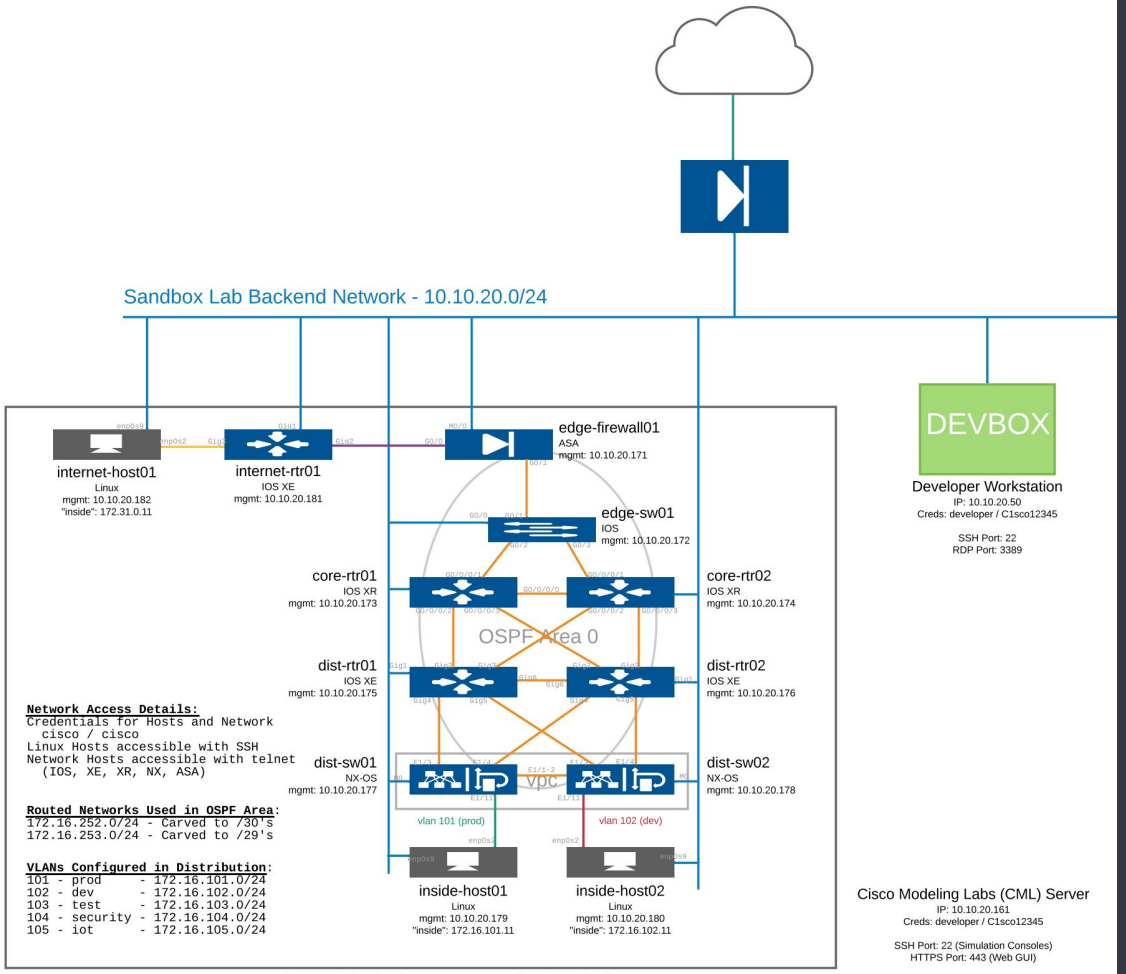
=

ObservaBLT

Observability

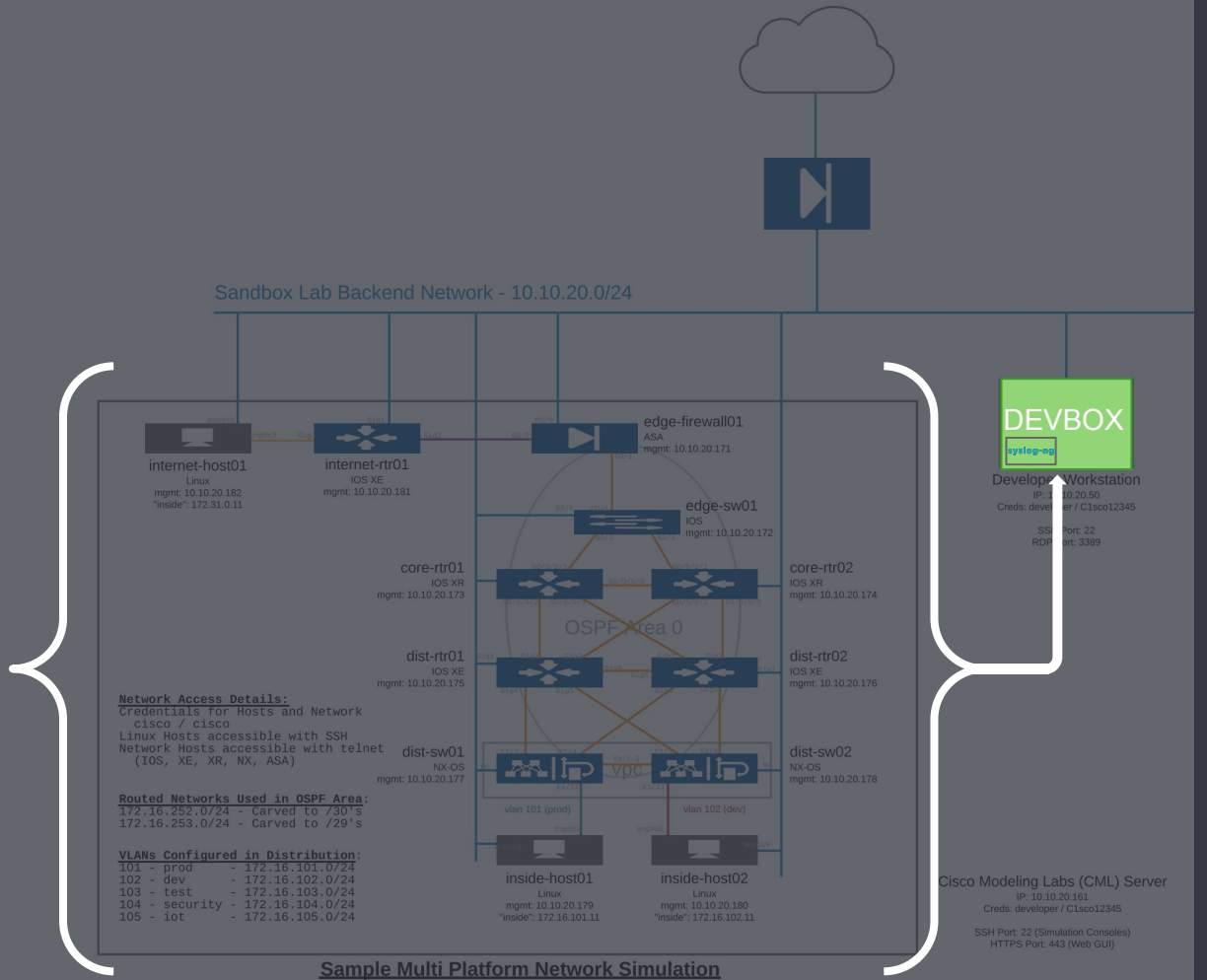
DEMO!

DevNet Sandbox Topology: Cisco Modeling Labs (CML)



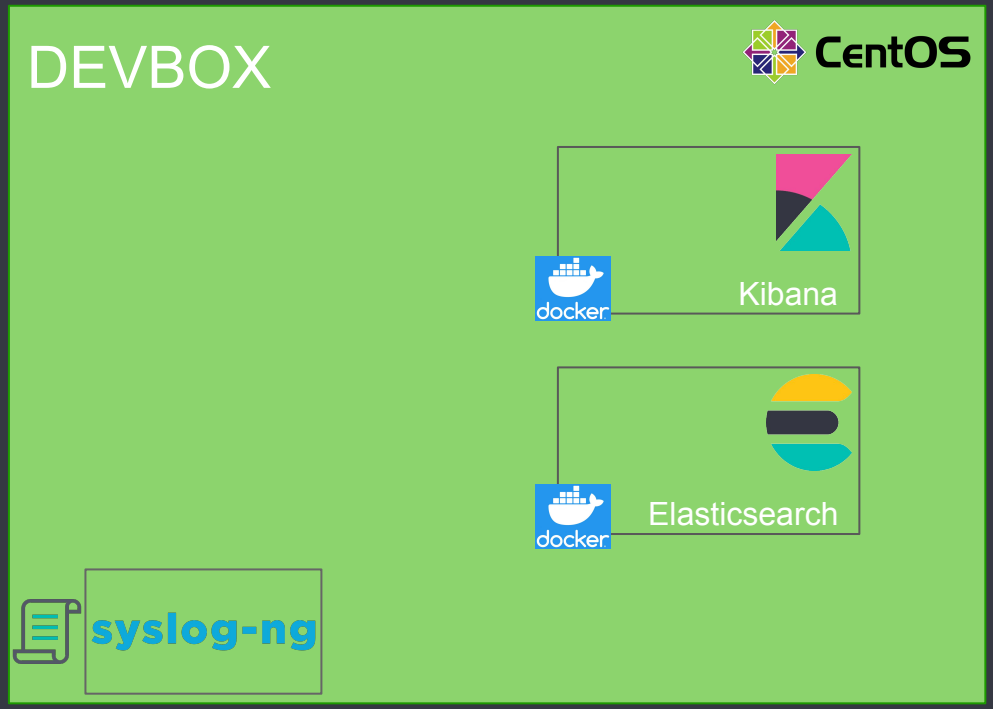
Sample Multi Platform Network Simulation

DevNet Sandbox Topology: Cisco Modeling Labs (CML)



Sample Multi Platform Network Simulation

DEVBOX


DEVBOX
CentOS
docker
Kibana
docker
Elasticsearch
syslog-ng

Elasticsearch (Enterprise Features 30 Day Trial)

```
docker pull docker.elastic.co/elasticsearch/elasticsearch:7.6.2
```

Open Source

https://www.docker.elastic.co/

Kibana (Enterprise Features 30 Day Trial)

```
docker pull docker.elastic.co/kibana/kibana:7.6.2
```

Elasticsearch Docker Startup

```
sudo docker run -d -p 9200:9200 -p 9300:9300 -e "discovery.type=single-node"
docker.elastic.co/elasticsearch/elasticsearch:7.6.2
```

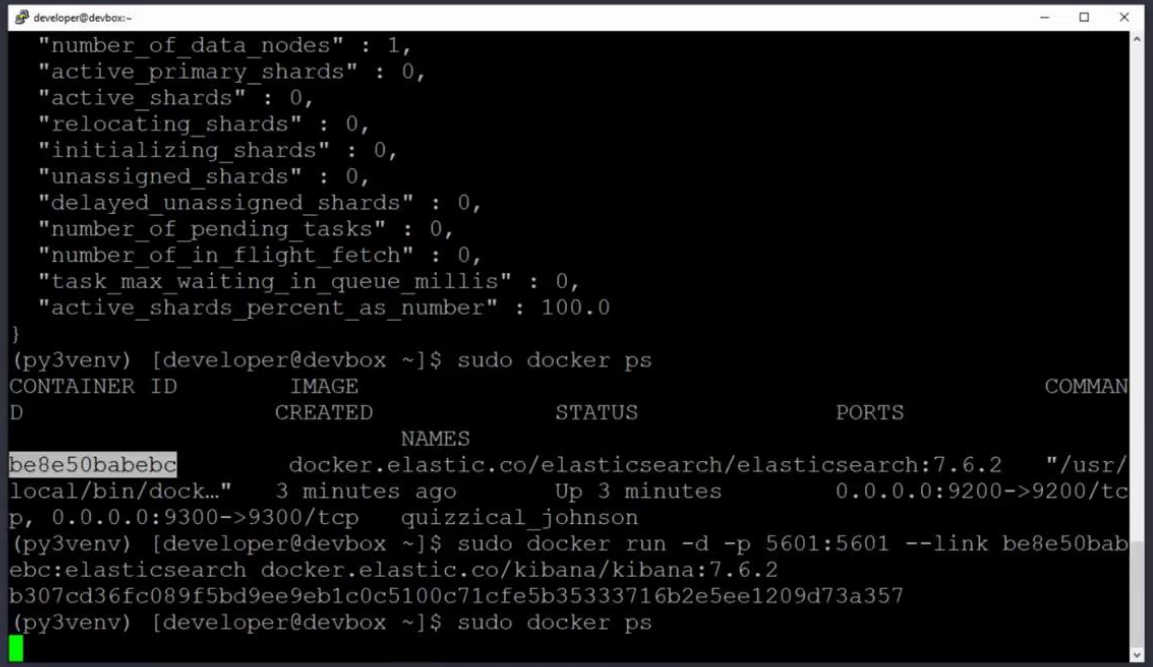
sudo docker ps

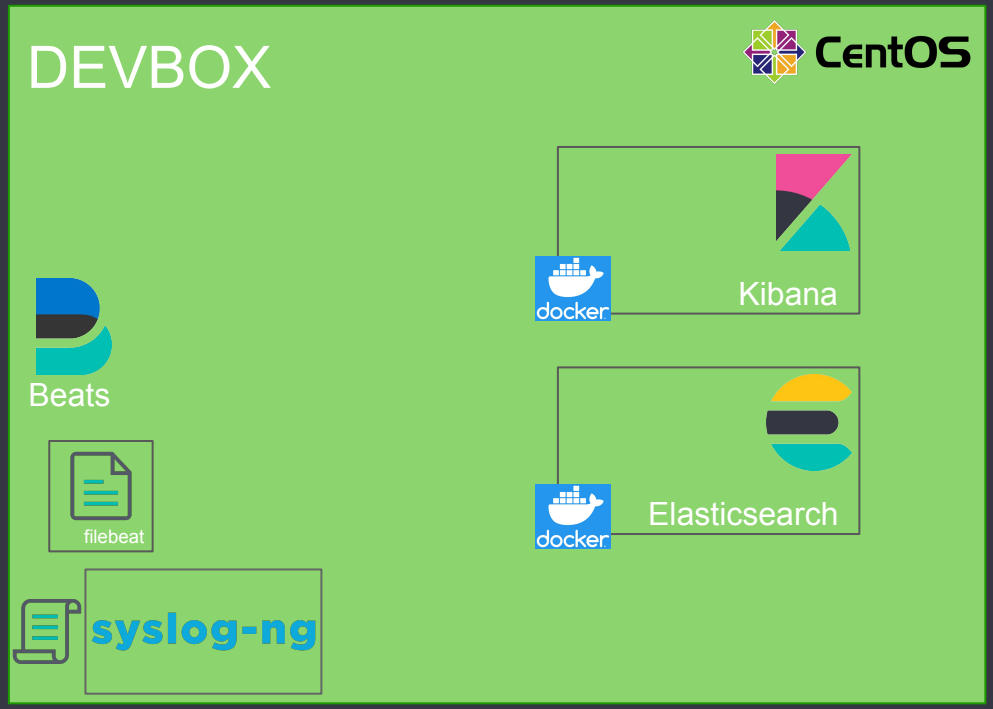
```
CONTAINER ID        IMAGE                                                  COMMAND                  CREATED
STATUS              PORTS                                                  NAMES

4d557241f188        docker.elastic.co/elasticsearch/elasticsearch:7.6.2    "/usr/local/bin/dock…"   2 minutes ago
Up 2 minutes        0.0.0.0:9200->9200/tcp, 0.0.0.0:9300->9300/tcp         reverent_poincare
```

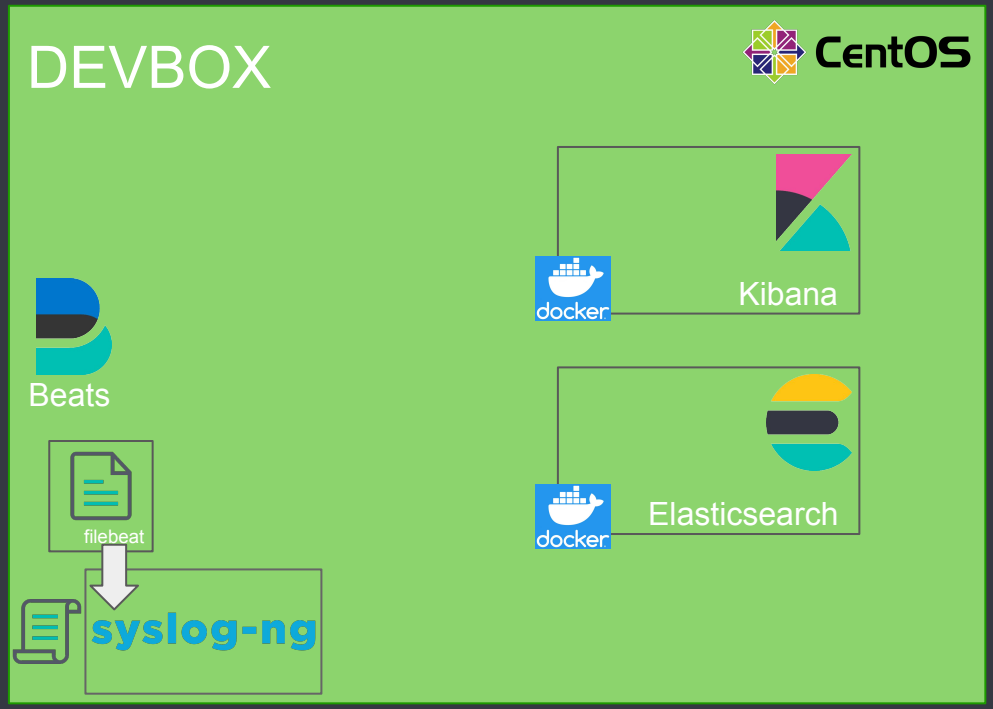
curl -X GET “10.10.20.50:9200/_cluster/health?pretty”

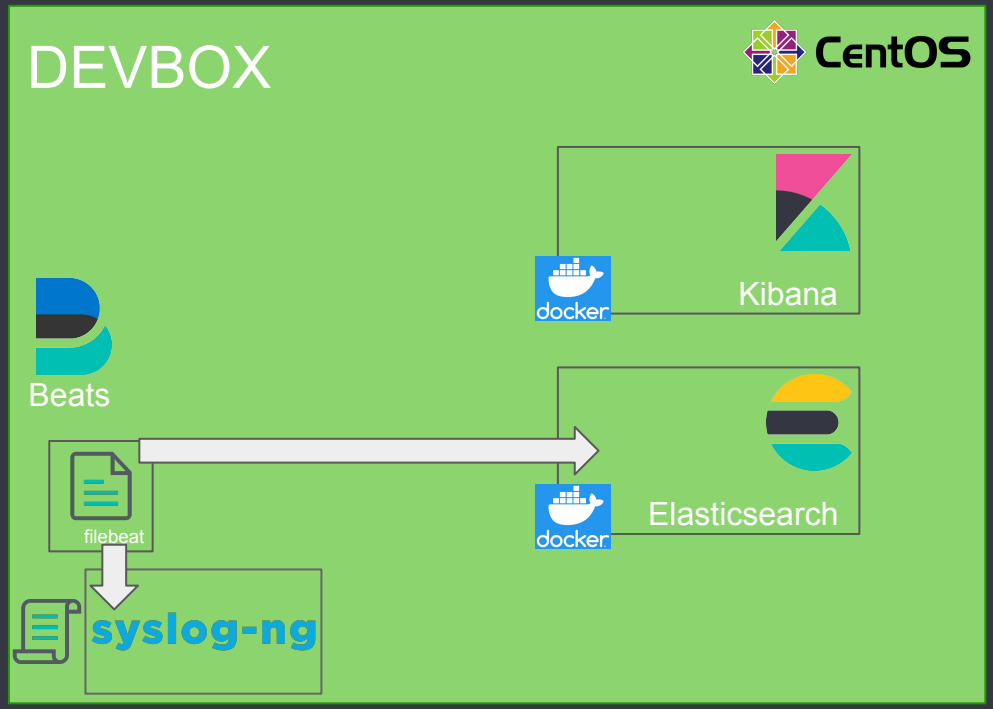
```
(py3venv) [developer@devbox ~]$ curl -X GET "10.10.20.50:9200/_cluster/health?wa
it_for_status=yellow&timeout=50s&pretty"
{
  "cluster_name" : "docker-cluster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 0,
  "active_shards" : 0,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

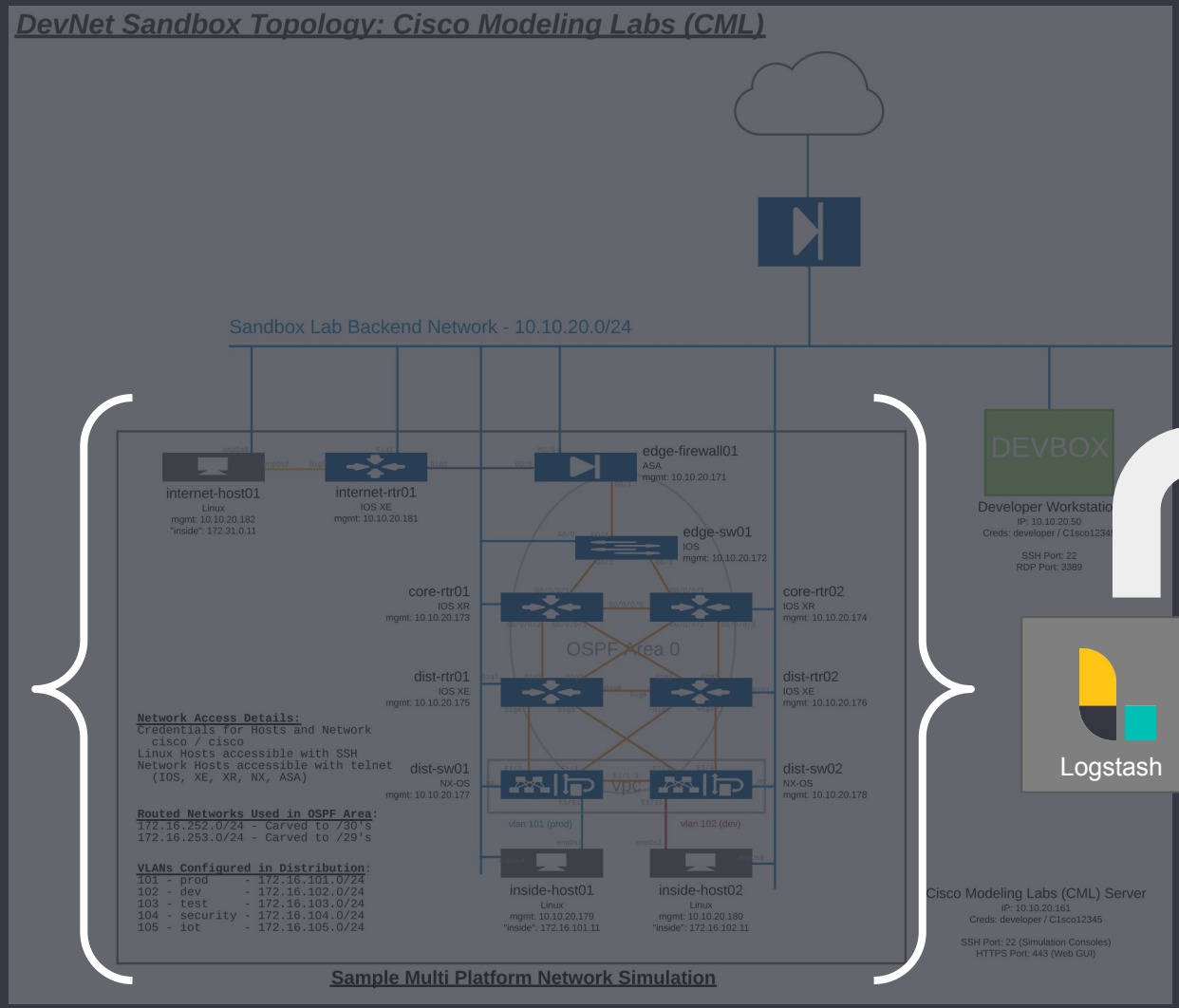
Kibana Docker Startup

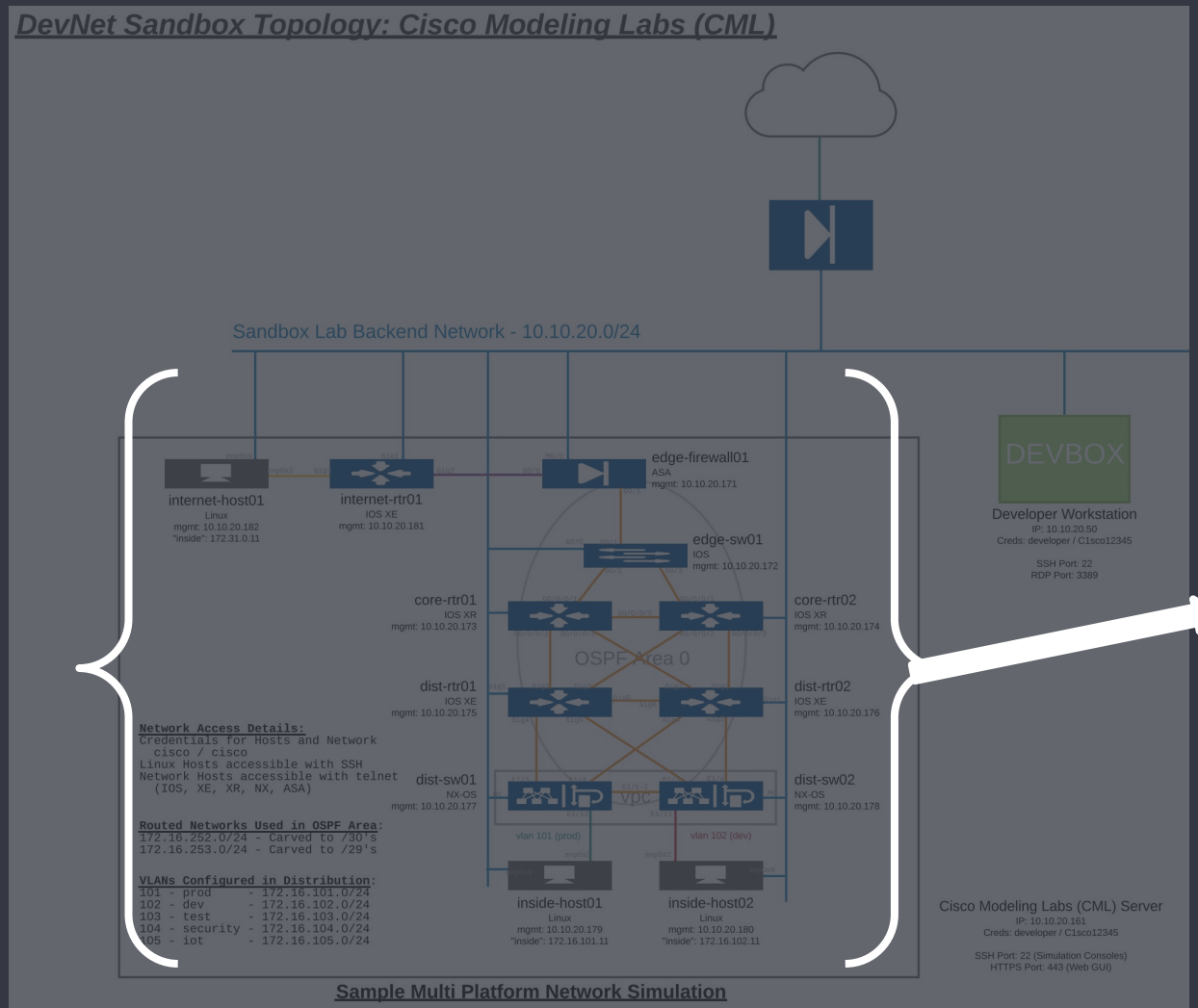


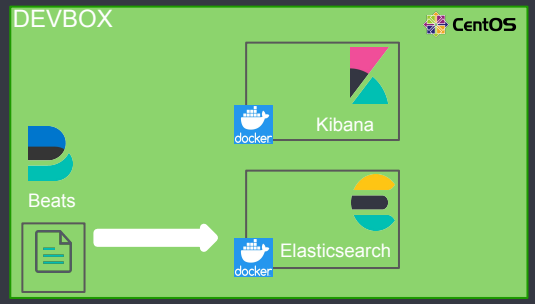

DEVBOX
CentOS
Kibana
docker
Beats
filebeat
Elasticsearch
docker
syslog-ng


DEVBOX
CentOS
Kibana
docker
Beats
filebeat
syslog-ng
Elasticsearch
docker

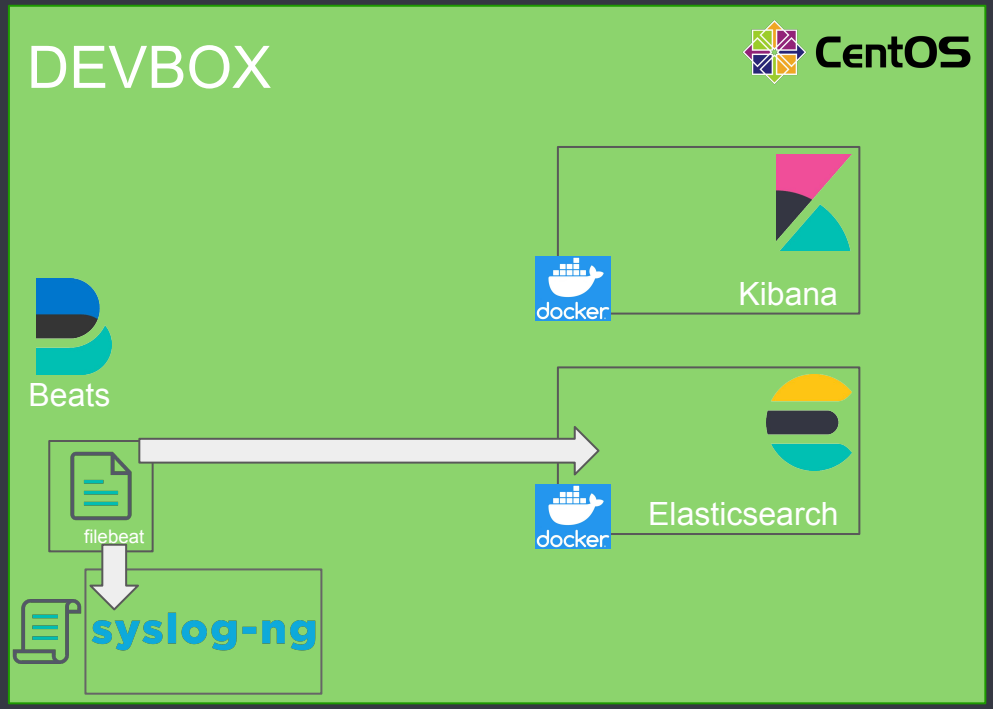

DEVBOX
CentOS
Kibana
docker
Beats
filebeat
Elasticsearch
docker
syslog-ng

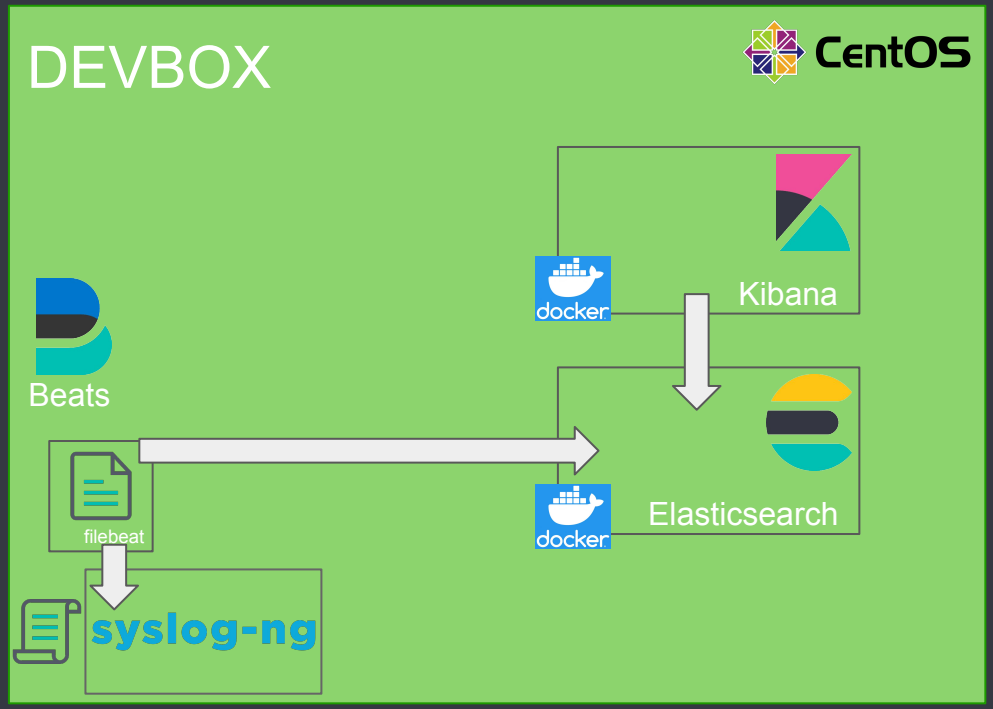

DevNet Sandbox Topology: Cisco Modeling Labs (CML)
Sandbox Lab Backend Network - 10.10.20.0/24
internet-host01
Linux
mgmt: 10.10.20.182
"inside": 172.31.0.11
internet-rtr01
IOS XE
mgmt: 10.10.20.181
edge-firewall01
ASA
mgmt: 10.10.20.171
edge-sw01
IOS
mgmt: 10.10.20.172
core-rtr01
IOS XR
mgmt: 10.10.20.173
core-rtr02
IOS XR
mgmt: 10.10.20.174
OSPF Area 0
dist-rtr01
IOS XE
mgmt: 10.10.20.175
dist-rtr02
IOS XE
mgmt: 10.10.20.176
dist-sw01
NX-OS
mgmt: 10.10.20.177
dist-sw02
NX-OS
mgmt: 10.10.20.178
vpc
vlan 101 (prod)
vlan 102 (dev)
inside-host01
Linux
mgmt: 10.10.20.179
"inside": 172.16.101.11
inside-host02
Linux
mgmt: 10.10.20.180
"inside": 172.16.102.11
Network Access Details:
Credentials for Hosts and Network
cisco / cisco
Linux Hosts accessible with SSH
Network Hosts accessible with telnet
(IOS, XE, XR, NX, ASA)
Routed Networks Used in OSPF Area:
172.16.252.0/24 - Carved to /30's
172.16.253.0/24 - Carved to /29's
VLANs Configured in Distribution:
101 - prod - 172.16.101.0/24
102 - dev - 172.16.102.0/24
103 - test - 172.16.103.0/24
104 - security - 172.16.104.0/24
105 - iot - 172.16.105.0/24
Sample Multi Platform Network Simulation
DEVBOX
Developer Workstatio
IP: 10.10.20.50
Creds: developer / C1sco1234
SSH Port: 22
RDP Port: 3389
Cisco Modeling Labs (CML) Server
IP: 10.10.20.161
Creds: developer / C1sco12345
SSH Port: 22 (Simulation Consoles)
HTTPS Port: 443 (Web GUI)
Logstash
DEVBOX
CentOS
docker
Kibana
docker
Elasticsearch
input {
udp {
port => "8514"
type => "syslog-cisco"
}
tcp {
port => "8514"
type => "syslog-cisco"
}
}

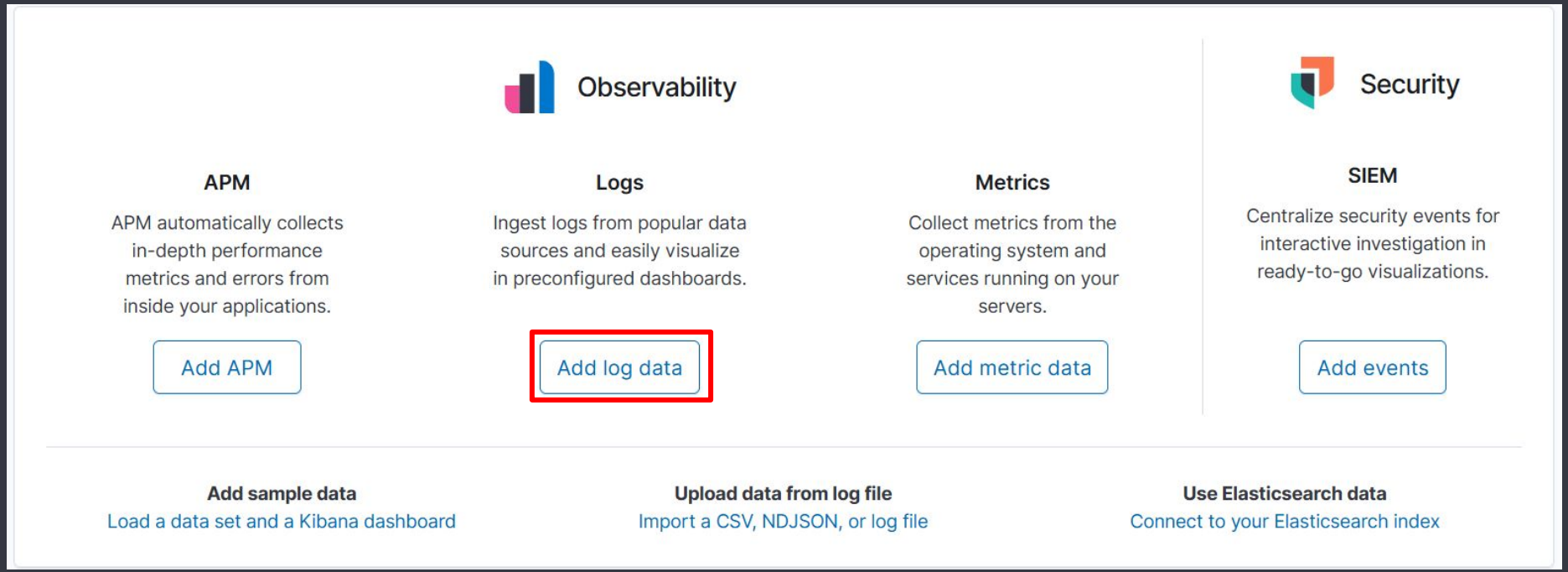





```
- module: cisco
  asa:
    enabled: true
    var.input:
"syslogfile"
    var.syslog_host:
localhost
    var.syslog_port:
9001
```


DEVBOX
CentOS
Kibana
docker
Beats
filebeat
Elasticsearch
docker
syslog-ng


DEVBOX
CentOS
Kibana
docker
Beats
filebeat
Elasticsearch
docker
syslog-ng


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

Add Data to Kibana

All | Logs | Metrics | SIEM | Sample data

ActiveMQ logs
Collect ActiveMQ logs with Filebeat.

Apache logs
Collect and parse access and error logs created by the Apache HTTP server.

AWS Cloudwatch logs
Collect Cloudwatch logs with Functionbeat.

AWS S3 based logs
Collect AWS logs from S3 bucket with Filebeat.

Elasticsearch logs
Collect and parse logs created by Elasticsearch.

IBM MQ logs
Collect IBM MQ logs with Filebeat.

IIS logs
Collect and parse access and error logs created by the IIS HTTP server.

Kafka logs
Collect and parse logs created by Kafka.

Logstash logs
Collect and parse debug and slow logs created by Logstash itself.

MySQL logs
Collect and parse error and slow logs created by MySQL.

Nats logs
Collect and parse logs created by Nats.

Nginx logs
Collect and parse access and error logs created by the Nginx HTTP server.

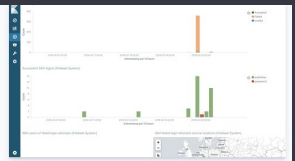
PostgreSQL logs
Collect and parse error and slow logs created by PostgreSQL.

Redis logs
Collect and parse error and slow logs created by Redis.

System logs
Collect and parse logs written by the local Syslog server.

Traefik logs
Collect and parse access logs created by the Traefik Proxy.

System logs



The `system` Filebeat module collects and parses logs created by the system logging service of common Unix/Linux based distributions. This module is not available on Windows. Learn more.

View exported fields

Self managed | Elastic Cloud

Getting Started

macOS | DEB | RPM

1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.2-x86_64.rpm
sudo rpm -vi filebeat-7.6.2-x86_64.rpm
```

Looking for the 32-bit packages? See the Download page.

2 Edit the configuration

Modify `/etc/filebeat/filebeat.yml` to set the connection information:

Copy snippet

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
setup.kibana:
  host: "<kibana_url>"
```

Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

3 Enable and configure the system module

Copy snippet

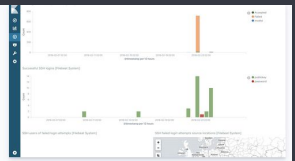
```
sudo filebeat modules enable system
```

Modify the settings in the `/etc/filebeat/modules.d/system.yml` file.

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.2-x86_64.rpm

sudo rpm -vi filebeat-7.6.2-x86_64.rpm
```

System logs

The `system` Filebeat module collects and parses logs created by the system logging service of common Unix/Linux based distributions. This module is not available on Windows. Learn more.



View exported fields

Self managed | Elastic Cloud

Getting Started

macOS | DEB | RPM

1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.2-x86_64.rpm
sudo rpm -vi filebeat-7.6.2-x86_64.rpm
```

Looking for the 32-bit packages? See the Download page.

2 Edit the configuration

Modify `/etc/filebeat/filebeat.yml` to set the connection information:

Copy snippet

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
setup.kibana:
  host: "<kibana_url>"
```

Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

3 Enable and configure the system module

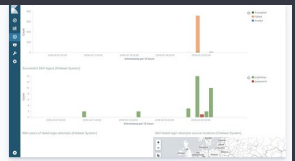
Copy snippet

```
sudo filebeat modules enable system
```

Modify the settings in the `/etc/filebeat/modules.d/system.yml` file.

```
filebeat.inputs:
- type: log
  enabled: false
  paths:
filebeat.autodiscover:
  providers:
    - type: docker
      templates:
        - condition:
            contains:
              docker.container.image: centos
          config:
            - type: container
              paths:
                -
/var/lib/docker/containers/${data.docker.container.id}/*.log
              exclude_lines: ["^\\s+[\\-`('.|_]"]
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: true
  reload.period: 10s
setup.template.settings:
  index.number_of_shards: 1
  _source.enabled: true
name: log_repo
tags: ["syslog", "network"]
fields:
  env: prod
setup.kibana:
  host: "localhost:5601"
output.elasticsearch:
  hosts: ["localhost:9200"]
  username: "elastic"
  password: "changeme"
processors:
  - add_host_metadata: ~
  - add_cloud_metadata: ~
  - add_docker_metadata: ~
  - add_kubernetes_metadata: ~
```

System logs



The `system` Filebeat module collects and parses logs created by the system logging service of common Unix/Linux based distributions. This module is not available on Windows. Learn more.

View exported fields

Self managed | Elastic Cloud

Getting Started

macOS | DEB | RPM

1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.2-x86_64.rpm
sudo rpm -vi filebeat-7.6.2-x86_64.rpm
```

Looking for the 32-bit packages? See the Download page.

2 Edit the configuration

Modify `/etc/filebeat/filebeat.yml` to set the connection information:

Copy snippet

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
setup.kibana:
  host: "<kibana_url>"
```

Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

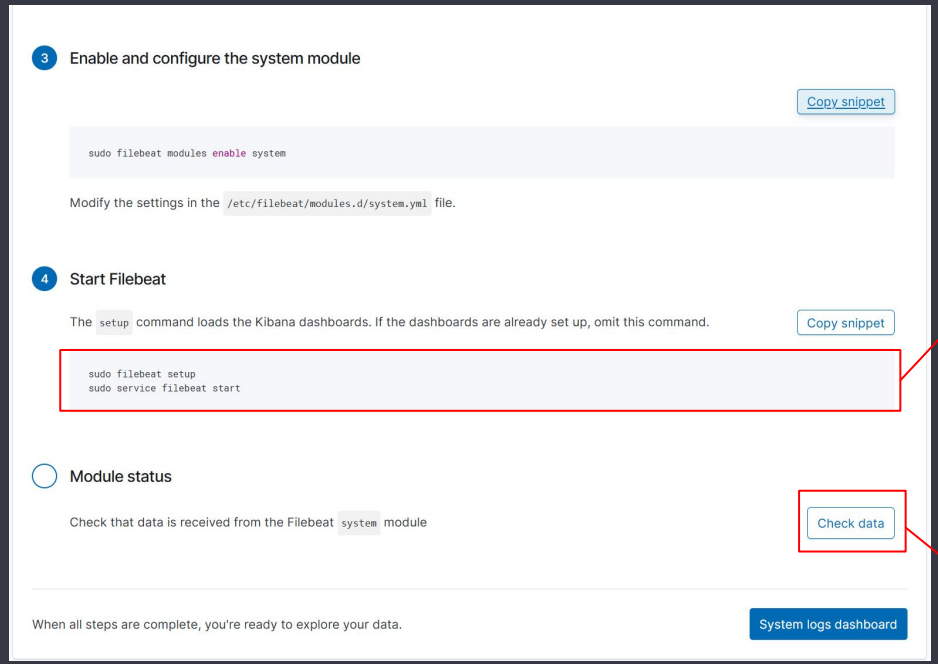
3 Enable and configure the system module

Copy snippet

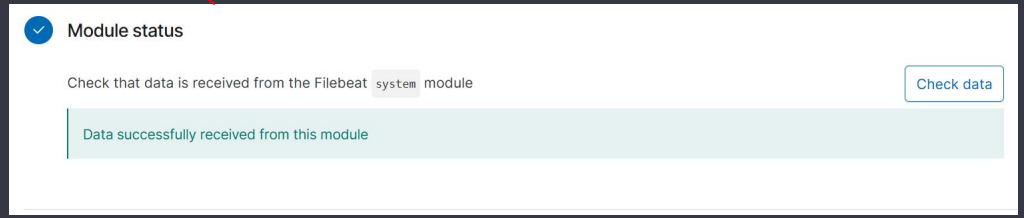
```
sudo filebeat modules enable system
```

Modify the settings in the `/etc/filebeat/modules.d/system.yml` file.

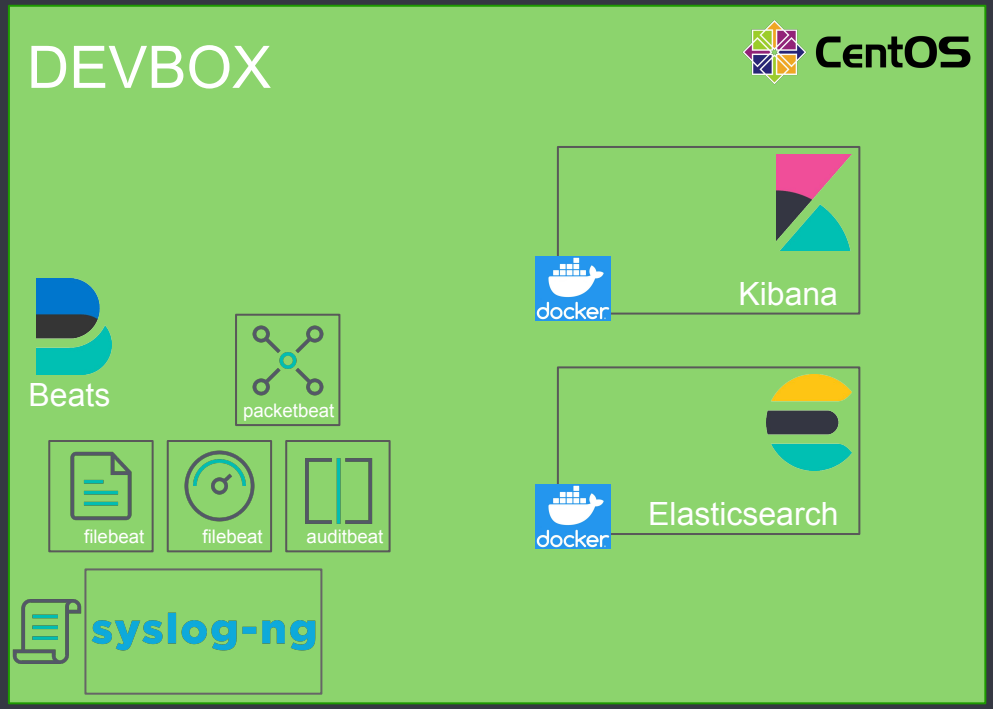
```
sudo filebeat modules enable system

sudo filebeat modules enable cisco
```




```
sudo filebeat setup

sudo service filebeat start
```



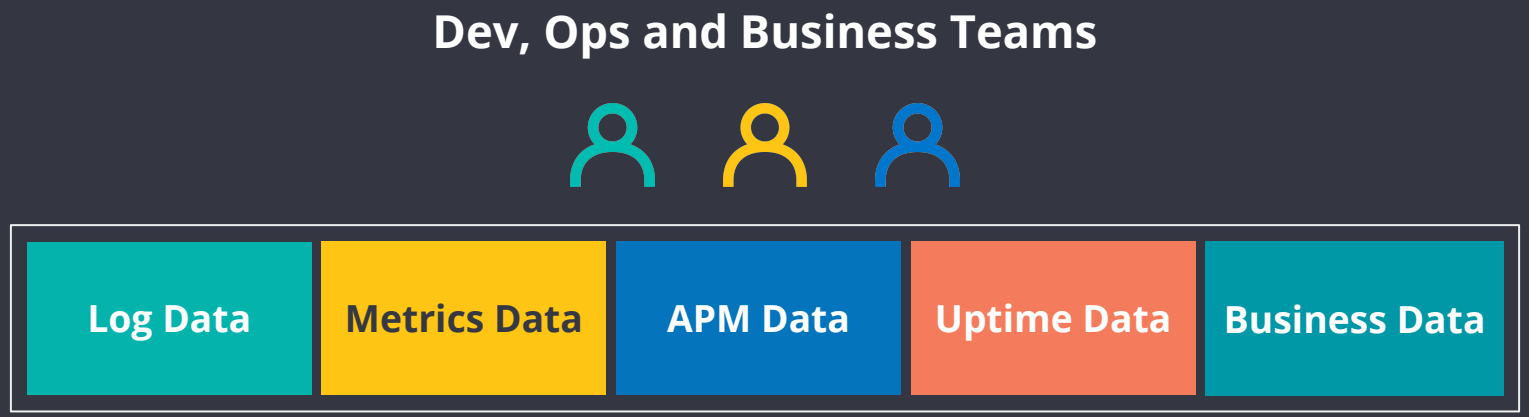
Live Demo


DEVBOX
CentOS
Kibana
docker
Beats
packetbeat
filebeat
filebeat
auditbeat
Elasticsearch
docker
syslog-ng

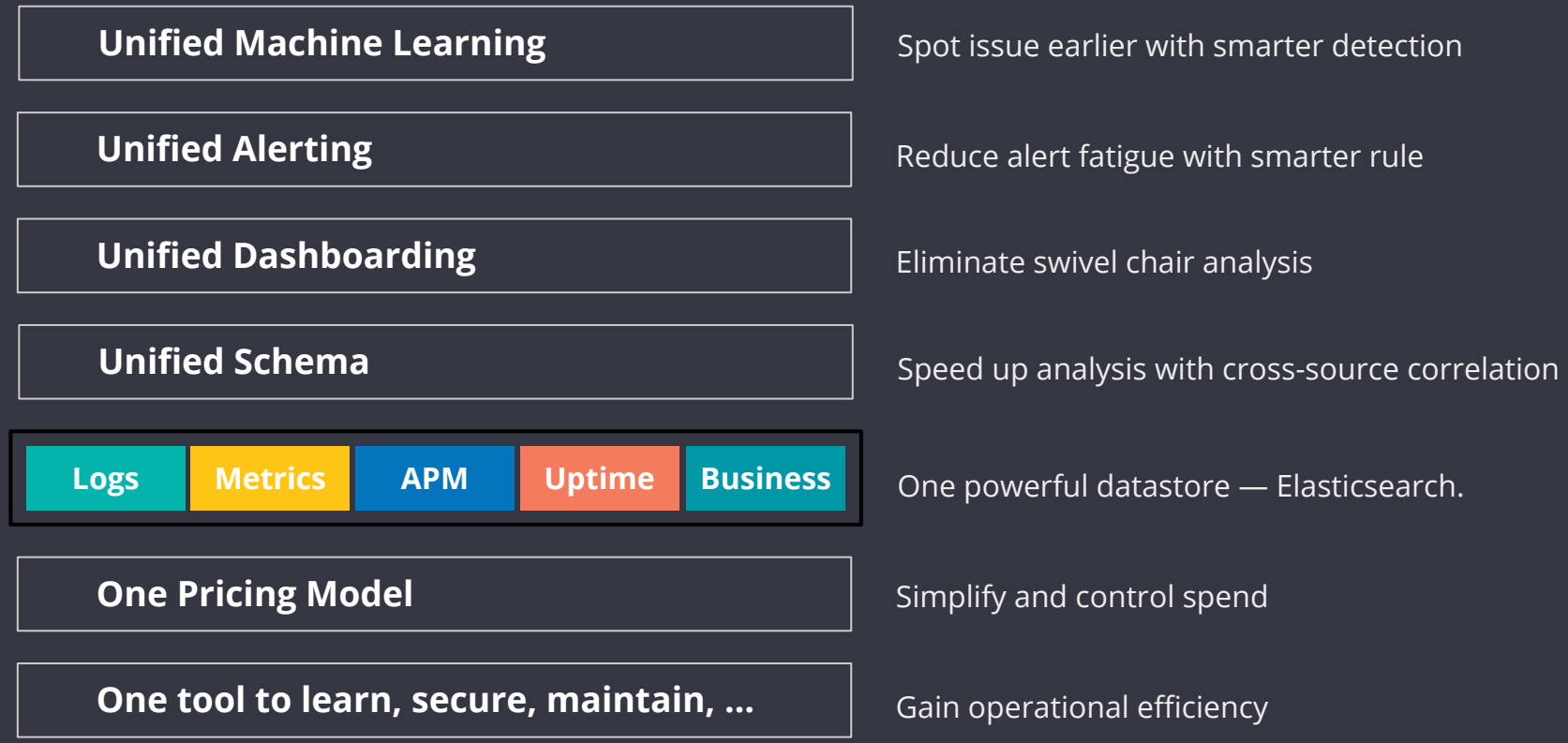
Typical observability stack

Ops: Log Monitoring	Ops: Infra Monitoring	Development Team	Ops: Service Monitoring	Business Team
				
Log Tool	**Metrics Tool**	**APM Tool**	**Uptime Tool**	**Business Tool**
Web Logs App Logs Database Logs Container Logs	Container Metrics Host Metrics Database Metics Network Metrics Storage Metrics	Real User Mon. Txn Perf Mon. Dist. Tracing	Availability Response Time	Business KPIs

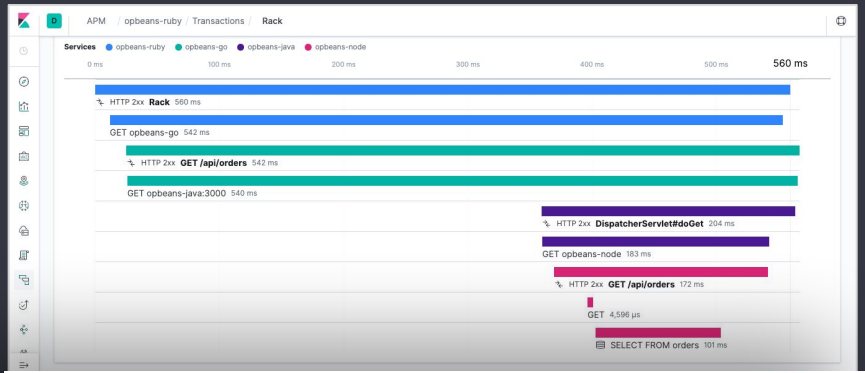
Elastic approach to observability

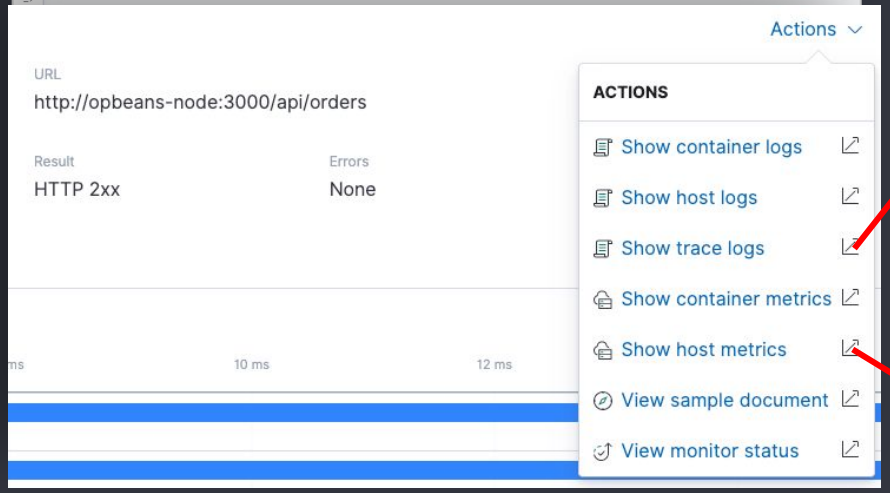


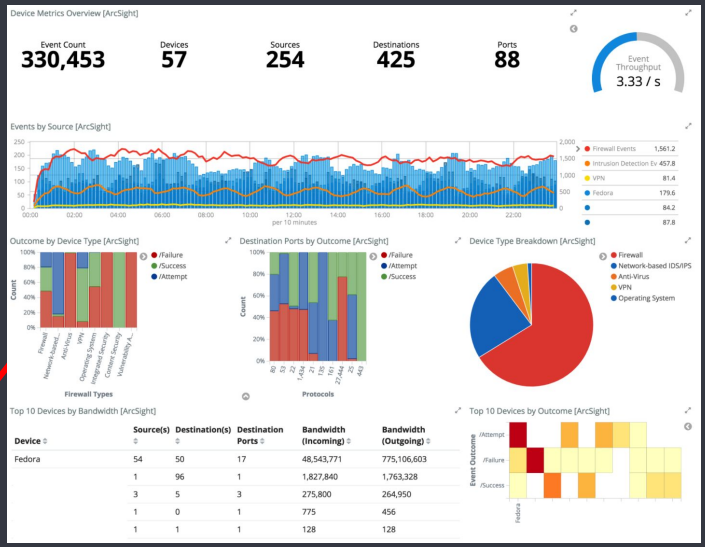
No more silos, unification at every layer

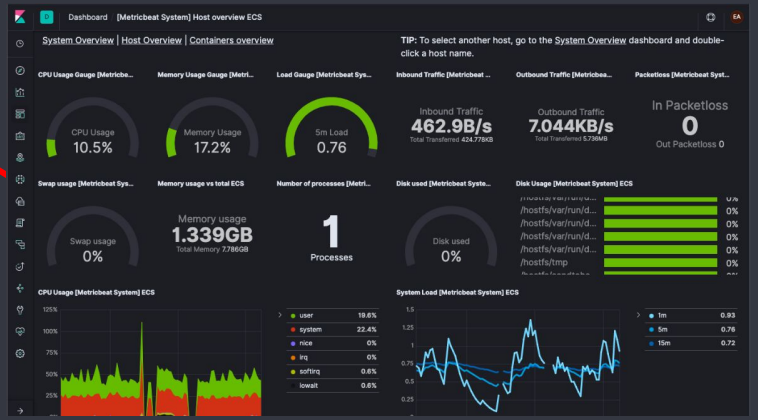


Elastic approach to observability


APM / opbeans-ruby / Transactions / Rack
Services opbeans-ruby opbeans-go opbeans-java opbeans-node
0 ms 100 ms 200 ms 300 ms 400 ms 500 ms
560 ms
HTTP 2xx Rack 560 ms
GET opbeans-go 542 ms
HTTP 2xx GET /api/orders 542 ms
GET opbeans-java:3000 540 ms
HTTP 2xx DispatcherServlet#doGet 204 ms
GET opbeans-node 183 ms
HTTP 2xx GET /api/orders 172 ms
GET 4,596 µs
SELECT FROM orders 101 ms


Actions
URL
http://opbeans-node:3000/api/orders
Result
HTTP 2xx
Errors
None
ACTIONS
Show container logs
Show host logs
Show trace logs
Show container metrics
Show host metrics
View sample document
View monitor status
10 ms
12 ms


Device Metrics Overview [ArcSight]
Event Count 330,453
Devices 57
Sources 254
Destinations 425
Ports 88
Event Throughput 3.33 / s
Events by Source [ArcSight]
Outcome by Device Type [ArcSight]
Destination Ports by Outcome [ArcSight]
Device Type Breakdown [ArcSight]
Top 10 Devices by Bandwidth [ArcSight]
Device Source(s) Destination(s) Destination Ports Bandwidth (Incoming) Bandwidth (Outgoing)
Fedora 54 50 17 48,543,771 775,106,603
1 96 1 1,827,840 1,763,328
3 5 3 275,800 264,950
1 0 1 775 456
1 1 1 128 128
Top 10 Devices by Outcome [ArcSight]


Dashboard [Metricbeat System] Host overview ECS
System Overview | Host Overview | Containers overview
TIP: To select another host, go to the System Overview dashboard and double-click a host name.
CPU Usage 10.5%
Memory Usage 17.2%
5m Load 0.76
Inbound Traffic 462.9B/s
Outbound Traffic 7.044KB/s
In Packetloss 0
Out Packetloss 0
Swap usage 0%
Memory usage 1.339GB
Processes 1
Disk used 0%
CPU Usage [Metricbeat System] ECS
System Load [Metricbeat System] ECS

elastic

Elastic Cloud

Connect with Elastic Stack experts and fellow users at an Elastic{ON} event near you

Login

Email

Password

Log in

Forgot password?

Don't have an account? Sign up.

https://www.elastic.co/cloud/elasticsearch-service/signup

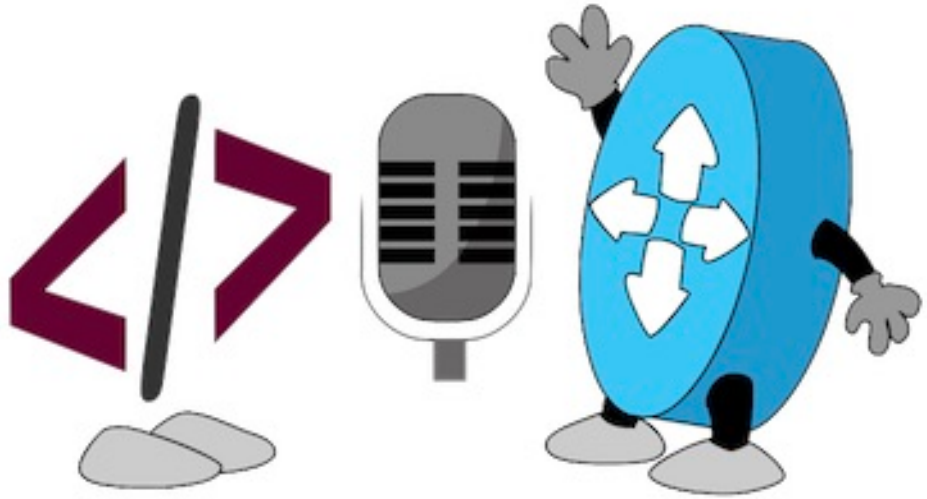
Terms of service Privacy Contact us

Thank you!

Q & A

@GeorgeKobar

NetDevOps Tech Chat

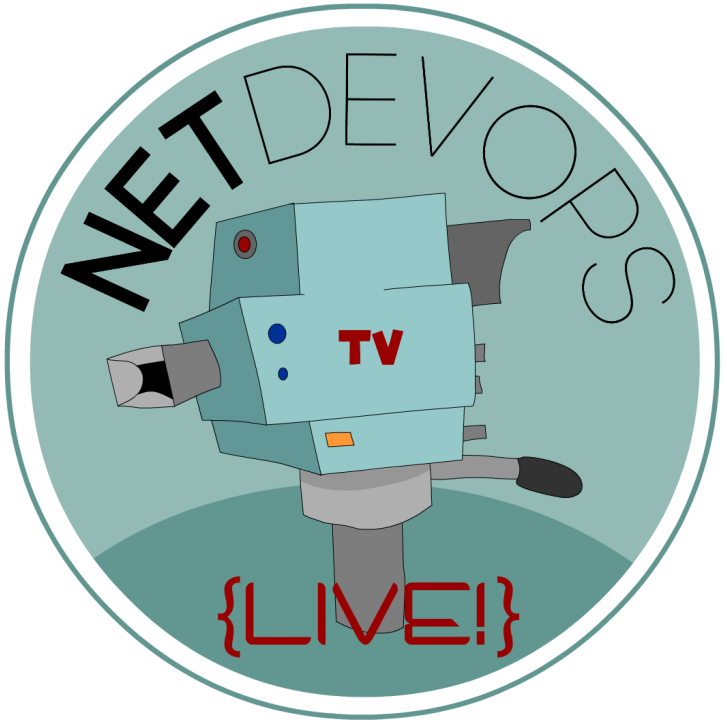


DEVNET
developer.cisco.com

</finish>

Webinar Resources on DevNet!

- Docs and Links
- Learning Labs
- DevNet Sandboxes
- Code Samples

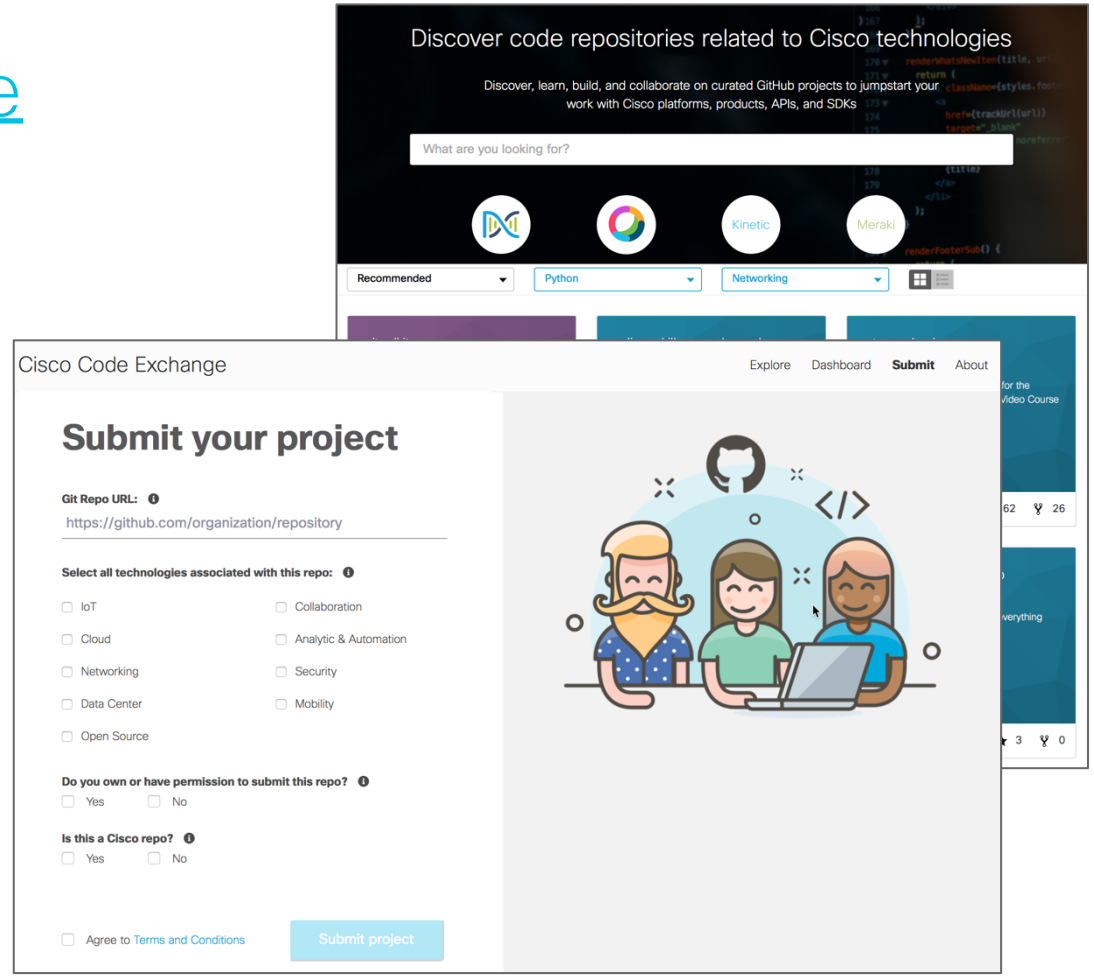


developer.cisco.com/netdevops/live/#s03t07

NetDevOps Live! Code Exchange Challenge

developer.cisco.com/codeexchange

Event driven something! Monitor syslog for some key message and take an action based on it.



Example: Every time the configuration changes on a device send yourself a chat message!

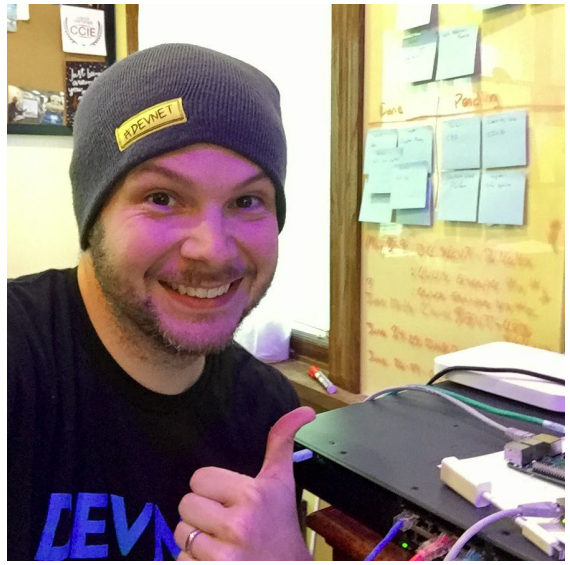
Looking for more about NetDevOps?

- NetDevOps on DevNet
  developer.cisco.com/netdevops
- NetDevOps Live!
  developer.cisco.com/netdevops/live
- NetDevOps Blogs
  blogs.cisco.com/tag/netdevops
- Network Programmability Basics Video Course
  developer.cisco.com/video/net-prog-basics/

Thanks for Joining Season 3

https://developer.cisco.com/netdevops/live/#s03

Got more questions? Stay in touch!



Hank Preston

hapresto@cisco.com
@hfpreston
http://github.com/hpreston

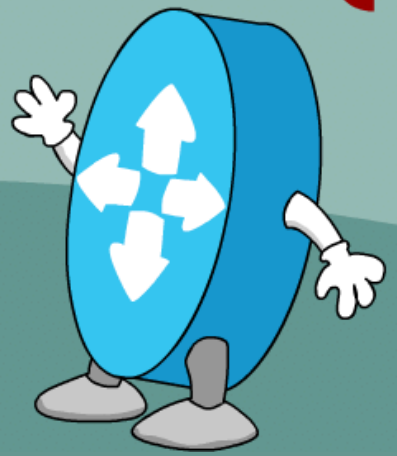
CISCO DEVNET
LEARN CODE INSPIRE CONNECT

developer.cisco.com

@CiscoDevNet
facebook.com/ciscodevnet/
http://github.com/CiscoDevNet

NETDEVOPS {LIVE!}

CISCO DEVNET



https://developer.cisco.com/netdevops/live

@netdevopslive