



PRACA DYPLOMOWA MAGISTERSKA

System ciągłego gromadzenia, przetwarzania i wizualizacji zdarzeń z wybranego systemu informatycznego przy zastosowaniu oprogramowania ELK.

Autor: Szymon Woyda
Numer albumu: 227458

Promotor: dr inż. Łukasz Sturgulewski

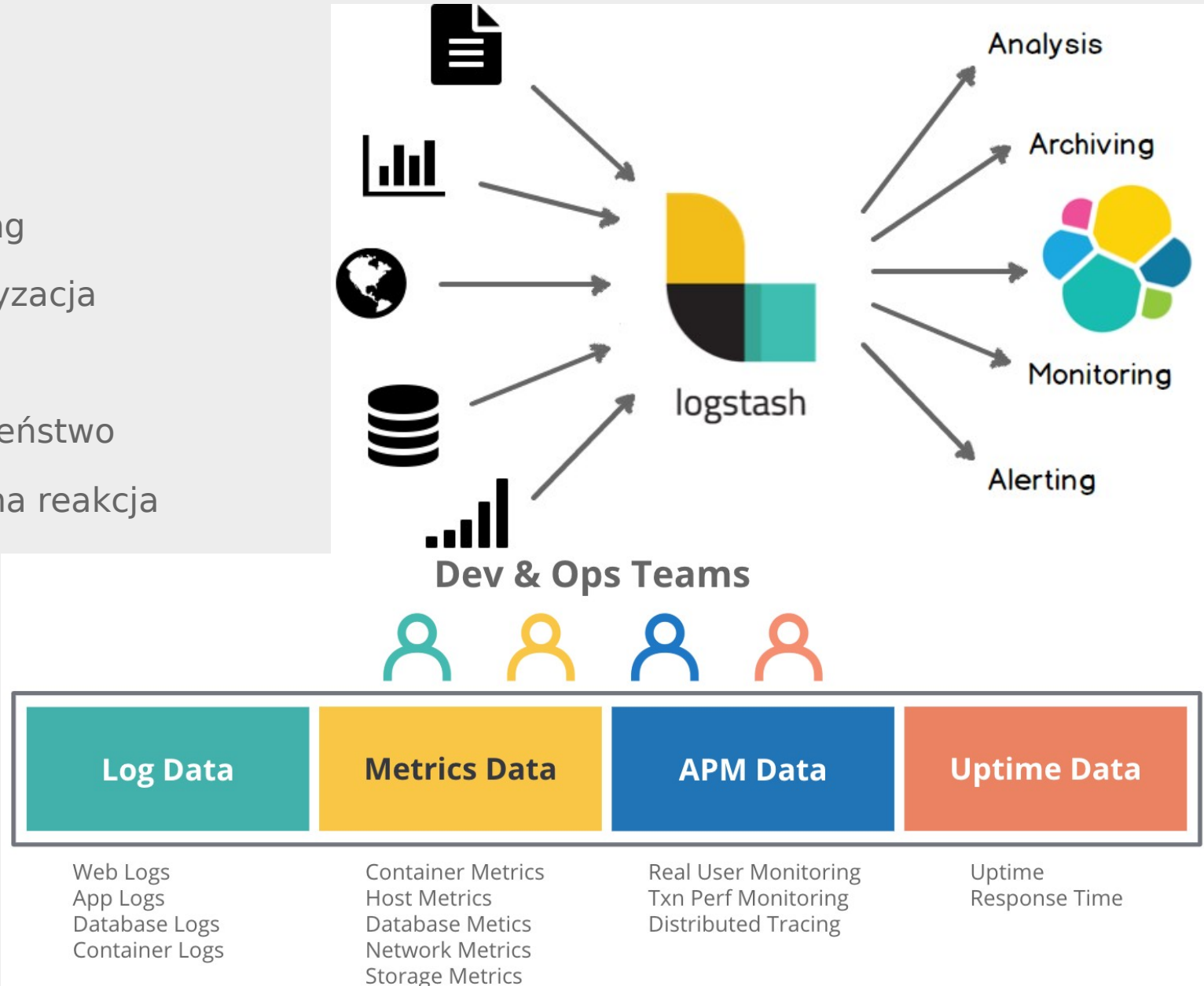
Łódź, Styczeń, 2020

Cel i zakres pracy

- Zaprojektowanie, wdrożenie i weryfikacja w środowisku wirtualnym.
- System ciągłego gromadzenia, przetwarzania i wizualizacji zdarzeń z wybranego systemu informatycznego.
- Ciągłość systemu należy rozumieć jako pracę bez przerwy.
- Wymagana niezawodność i wysoka dostępność.
- System możliwy do implementacji w średniej wielkości przedsiębiorstwie
- Zastosowanie oprogramowania ELK – Elasticsearch, LogStash, Kibana

Wprowadzenie

- Monitoring
- Automatyzacja
- Kontrola
- Bezpieczeństwo
- Precyzyjna reakcja



```

/usr/share/logstash/pipeline # cat logstash.conf
input {
  udp {
    port => 5014
    type => syslog
  }
}

filter {
  #####
  # OSPF Adjacency change section
  #####
  if "ios_parsed" in [tags] and "OSPF" in [vendor_facility] and
    grok {
      match => {
        "log_message" => "Process\s+{%NUMBER:ospf_instance}
ore_ospf_state}\s+to\s+{%DATA:after_ospf_state},\s+{%GREEDYDATA:ops
      }
      tag_on_failure => ["_grokparsefailure", "_ospfparsefail
    }
  }
}

output {
  elasticsearch {
    hosts => ["http://elasticsearch:9200"]
    index => "netlogstash-%{+YYY.MM.dd}"
  }
}

```

```

> Jan 6, 2020 @ 19:03:57.995 iosv-1 console ip domain name szymon.com
> Jan 6, 2020 @ 18:41:23.242 iosv-1 console no ip domain name
> Jan 6, 2020 @ 18:40:53.126 iosv-1 console exit
> Jan 6, 2020 @ 18:39:14.886 iosv-1 szymon lexec: enable
> Jan 6, 2020 @ 18:38:53.567 iosv-1 console transport input all
> Jan 6, 2020 @ 18:38:18.442 iosv-1 console transport input telnet
> Jan 6, 2020 @ 18:38:13.933 iosv-1 console transport input ssh

```

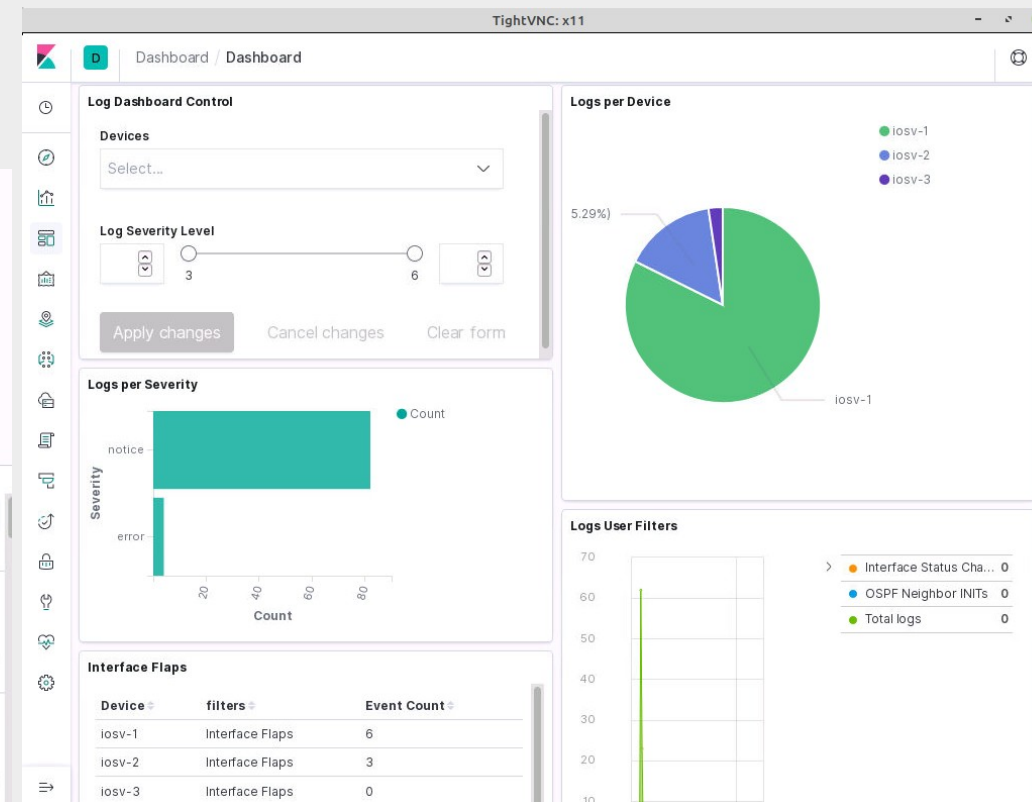
Logs

Time	device	syslog_severity	vendor_facility	vendor_facility_process	log_message
> Jan 6, 2020 @ 19:09:46.699	iosv-2	notice	OSPF	ADJCHG	Process 100, Nbr 10.10.0.11 on GigabitEthernet0/0 from LOADING to FULL, Loading Done
> Jan 6, 2020 @ 19:09:46.679	iosv-1	notice	OSPF	ADJCHG	Process 100, Nbr 10.10.0.22 on GigabitEthernet0/0 from LOADING to FULL, Loading Done
> Jan 6, 2020 @ 19:09:41.499	iosv-2	notice	LINEPROTO	UPDOWN	Line protocol on Interface GigabitEthernet0/0, changed

```

root@netautomator-1: ~
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
[root@netautomator-1:~]
# curl -X GET http://elasticsearch:9200
{
  "name" : "elasticsearch-1",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "VKdX94A0TFugJcVyQcP8lQ",
  "version" : {
    "number" : "7.4.2",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "2f90bbf7b93631e52bafb59b3b049cb44ec25e96",
    "build_date" : "2019-10-28T20:40:44.881551Z",
    "build_snapshot" : false,
    "lucene_version" : "8.2.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}

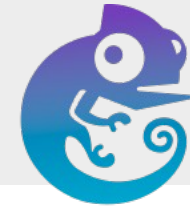
```



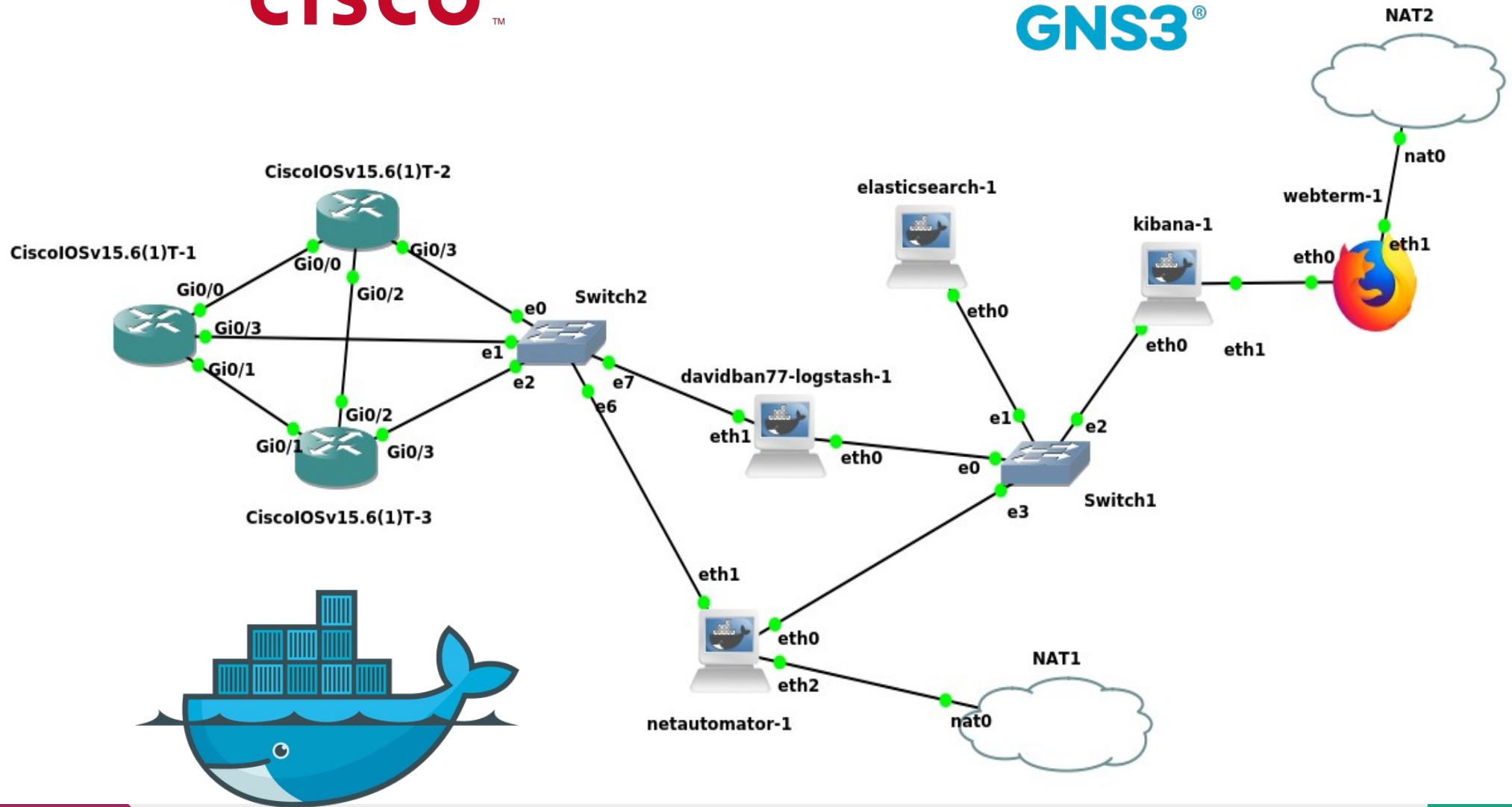


CISCO™

Topologia



GNS3®



Bibliografia

- YouTube Channel: David Flores [dostęp: 01/20]
- Github: davidban77 [dostęp: 01/20]
- Github: elastic/logstash/patterns/grok-patterns [dostęp: 01/20]
- <https://www.elastic.co/products/elastic-stack> [dostęp: 01/20]
- Vishal Sharma., Beginning Elastic Stack, wydanie I, Apress, 2016
- Clinton Gormley, Zachary Tong, Elasticsearch: The Definitive Guide, O'Reilly Media, 2015
- Adam Józefiok, GNS3. Emulowanie sieci komputerowych Cisco, Helion, 2017
- Ben Piper, Sieci Cisco w miesiąc. Podręcznik administratora, Helion, 2018
- Barrie Sosinsky, Sieci komputerowe. Biblia, Helion, 2013

Dziękuję za uwagę!