APNIC

Log Management

Further information | 00 Example 2020

Trainer Name

Table of Content

Logs

- Network/System logs provide organizations with records of how systems behave and interact with other systems
- Logs are generated by
  - network infrastructure devices (firewalls, switches, domain name service devices, routers, load balancers)
  - computer platforms (servers, appliances, and smartphones)
  - operating systems (Windows, apnic, IoS)
  - applications (client/server, web applications, cloud-based utilities)
- Logging allows us to monitor what happened to our network in the past
- Logs can identify issues before they become problems

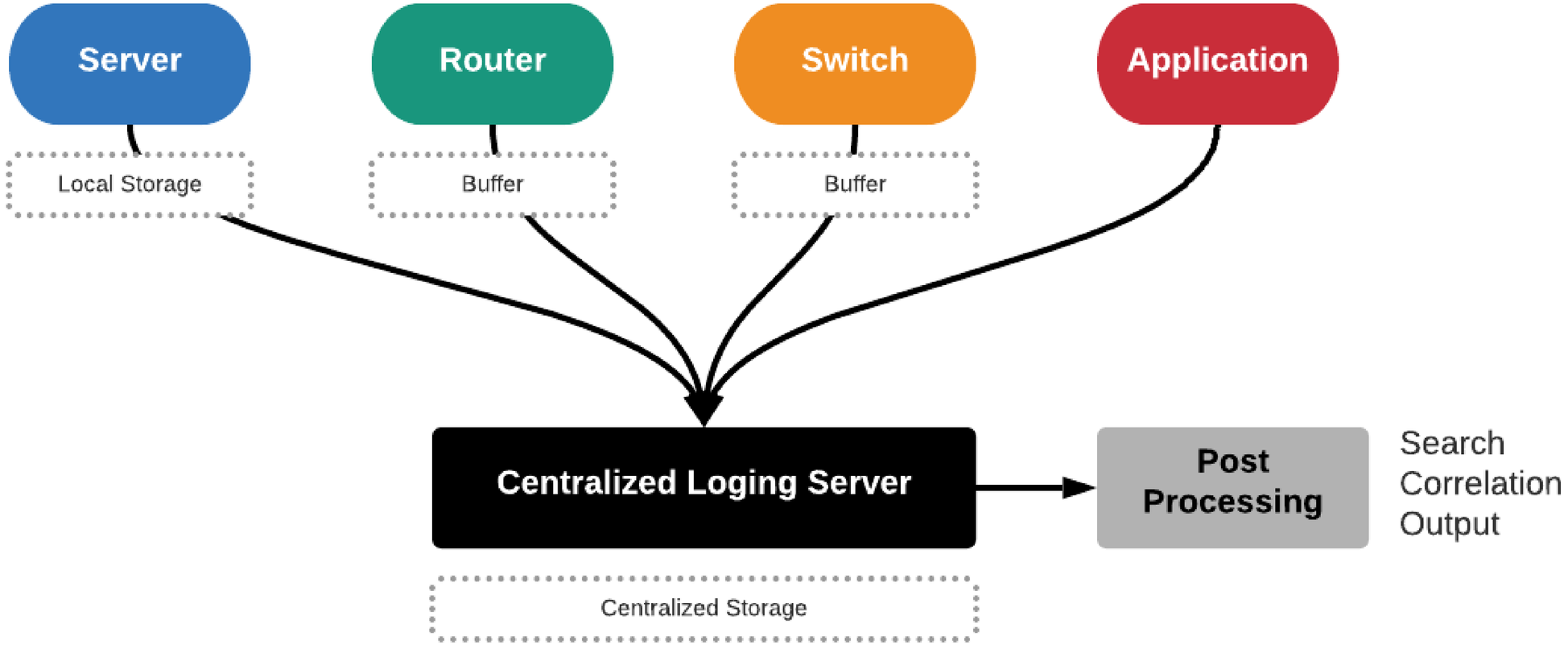
Log Management

- Systematically orchestrating the system and network logs collected by the organization
- Log management for
  - Troubleshooting or Debugging
  - Security
  - Compliance

Log Management Process

- There are five parameters to a complete log management process
  - Collection
  - Storage
  - Search
  - Correlation
  - Output

Centralized Logging



Centralized Log Management

- Comprehensive approach to network, data and security management
- All the managed devices (router, switch, server) and applications in a distributed environment configured to send their logs to a central log server
- Central log server helps normalize the differing log format
- Centralizing the logging process can also allow admins to view log data from across all network servers rather than reviewing logs from individual servers

Sample Logs

- SD-WAN Controller (vManage) log:

```
local7.info: May 22 13:15:08 vmanage VDAEMON_3[1711]: %Viptela-vmanage-vdaemon_3-6-
INFO-1400002: Notification: 5/22/2020
 13:15:8 control-connection-state-change severity-level:major host-name:"vmanage"
system-ip:167.213.228.10 personality:vmanage
peer-type:vbond peer-system-ip::: peer-vmanage-system-ip:0.0.0.0 public-
ip:192.168.100.10 public-port:12346 src-color:de
fault remote-color:default uptime:"0:00:00:00" new-state:up
```

- Server (Ubuntu) log:

```
Dec 18 21:12:36 apnic-ubuntu-server sshd[25075]: Accepted password for apnic from
192.168.100.9 port 60043 ssh2
Dec 18 21:12:36 apnic-ubuntu-server sshd[25075]: pam_unix(sshd:session): session
opened for user apnic by (uid=0)
Dec 18 21:12:36 apnic-ubuntu-server systemd: pam_unix(systemd-user:session):
session opened for user apnic by (uid=0)
```

Configure Centralized Logging

Cisco

```
core-router(config)#logging host 192.168.8.20
```

Ubuntu

```
$ sudo vi /etc/rsyslog.d/50-default.conf

*.*                 @192.168.8.20:514
```

Juniper

```
# set system syslog host 192.168.0.20 any info
```

Mikrotik

```
[admin@mt] > system logging action add remote=192.168.0.20 name=remote
target=remote
```

Syslog Ports

Service Name	Port Number	Transport Protocol	Description	Reference
syslog	514	udp		[RFC5426]
syslog-conn	601	tcp	Reliable Syslog Service	[RFC3195]
syslog-conn	601	udp	Reliable Syslog Service	[RFC3195]
syslog-tls	6514	tcp	Syslog over TLS	[RFC5425]
syslog-tls	6514	udp	syslog over DTLS	[RFC6012]

source:
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=syslog

Logging Levels

- Define detail in data logging
- Allow us to choose a block of data that we wish to have logged

Level	Title	Description
0	Emergencies	System panic or other condition that causes the router to stop functioning
1	Alerts	Conditions that require immediate correction, such as a corrupted system database
2	Critical	Critical conditions such as hard errors
3	Errors	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels
4	Warnings	Warning conditions
5	Notifications	Conditions that warrant monitoring
6	Informational	Events or nonerror conditions of interest
7	Debugging	Debugging message

Logging Facilities

- Represents the machine process that created the syslog event
- Defined in RFC5424 (https://tools.ietf.org/html/rfc5424)

Numeric Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages
5	Message generated by internally by syslogd
11	FTP daemon
12	NTP subsystem
16-23	Local use 0-9 (local0-7)

Centralized Syslog Servers

- Common centralized syslog servers:
  - syslog-ng (https://www.syslog-ng.com)
  - Rsyslog (https://www.rsyslog.com)
  - Graylog (https://www.graylog.org)
  - Logstash (https://www.elastic.co/logstash)
  - Grafana Loki (https://github.com/grafana/loki)

syslog-ng

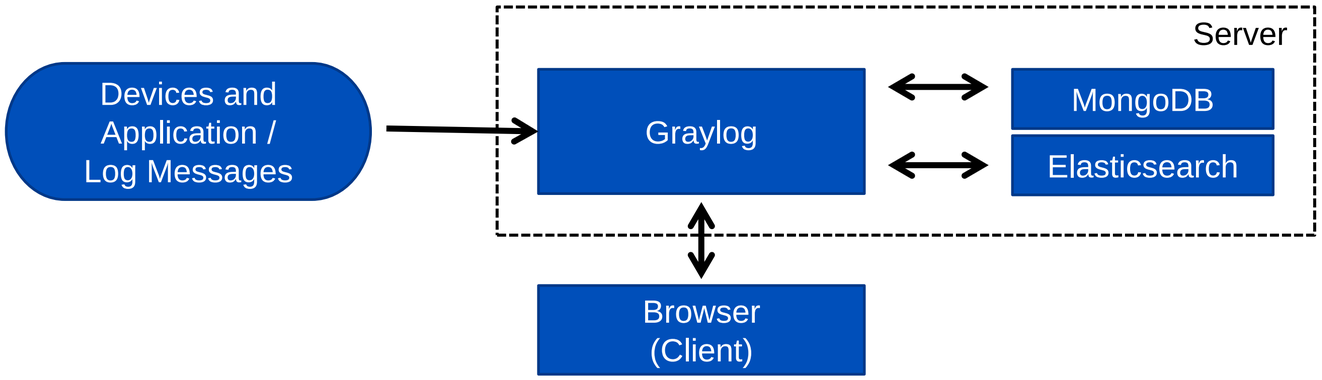
- syslog-ng is a free and open-source implementation of the syslog protocol for Unix and Unix-like systems
- Features:
  - Receive and send RFC3164 and RFC5424 style syslog messages
  - Receive and send JSON formatted messages
  - Work with any kind of unstructured data
  - Normalize, crunch, and process logs as they flow through the system
  - Hand over logs for further processing using files, message queues (like AMQP), or databases (like PostgreSQL or MongoDB)
  - Forward logs to big data tools (like Elasticsearch, Apache Kafka, or Apache Hadoop)

Rsyslog

- Rsyslog is the **r**ocket-fast **sys**tem for **log** processing
- Features:
  - Multi-threading
  - TCP, SSL, TLS, RELP
  - MySQL, PostgreSQL, Oracle and more
  - Filter any part of syslog message
  - Fully configurable output format
  - Suitable for enterprise-class relay chains

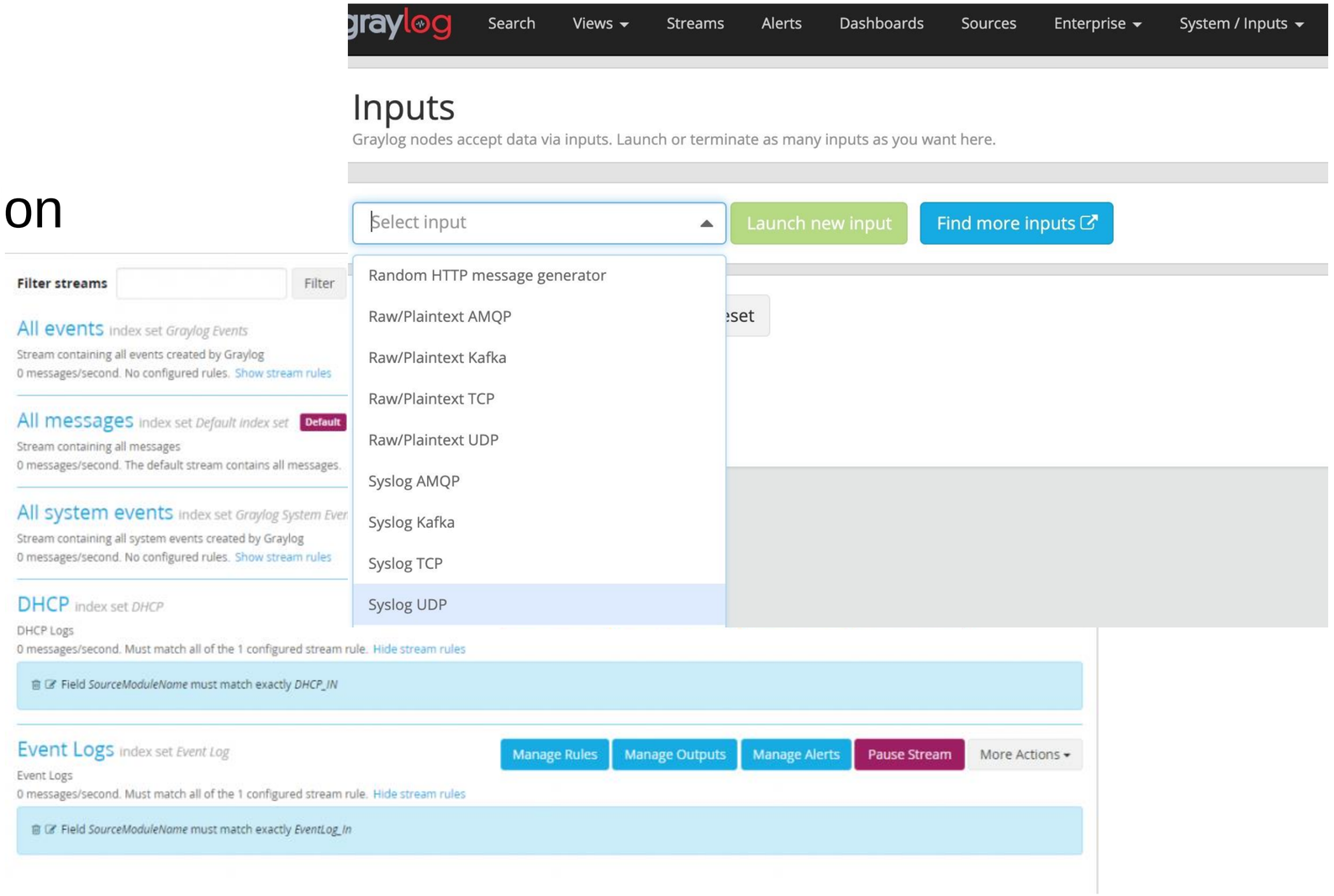
Graylog

- Graylog is a Free and open source enterprise-grade log management system which comprises of **Elasticsearch**, **MongoDB** and **Graylog** server
- The work of **Elasticsearch** is to store logs data and provide powerful search capabilities to Graylog Server
- **MongoDB** is for storing meta information and configuration data used by **Graylog** for complete Logs management



Graylog

- Graylog Features:
  - Scalable log collection
  - Simple UI for administration
  - Log enrichment data
  - Graphical log analysis
  - Alerts & Triggers
  - REST API

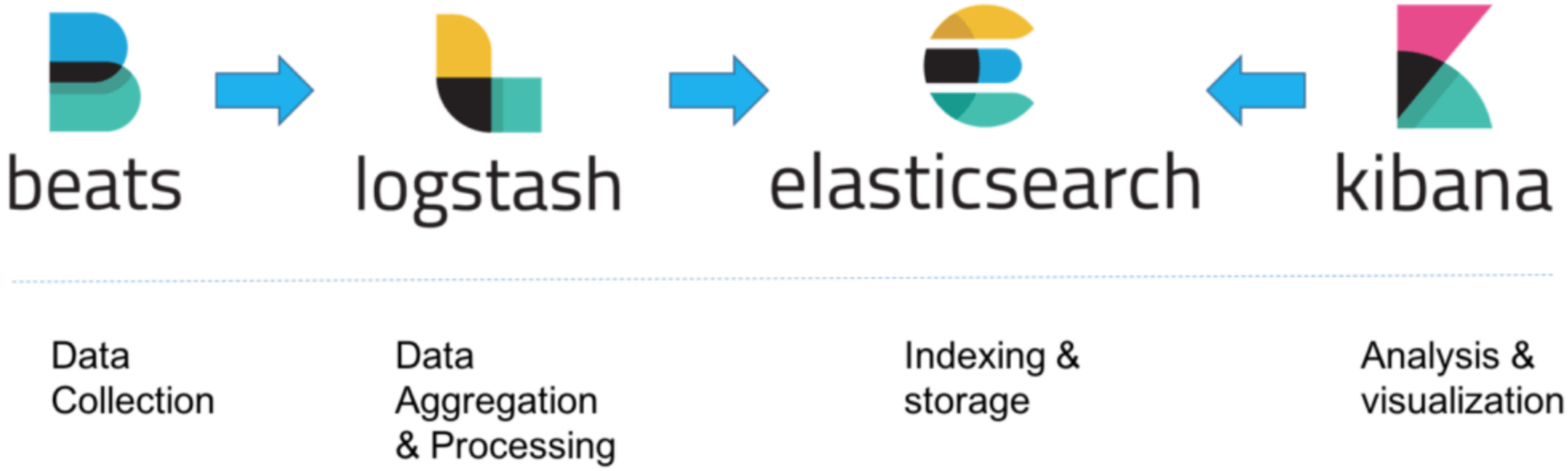


ELK Stack

- ELK Stack is a collection of open-source products:
  - **Elasticsearch**: Full-text search and analysis engine, based on the Apache Lucene search engine
  - **Logstash**: Log aggregator that collects data from various input sources, executes different transformations and enhancements and then ships the data to various supported output destinations
  - **Kibana**: Visualization layer that works on top of Elasticsearch, providing users with the ability to analyze and visualize the data
  - **Beats**: Is a single-purpose data shippers. They send data from hundreds or thousands of machines and systems to Logstash or Elasticsearch

ELK Stack

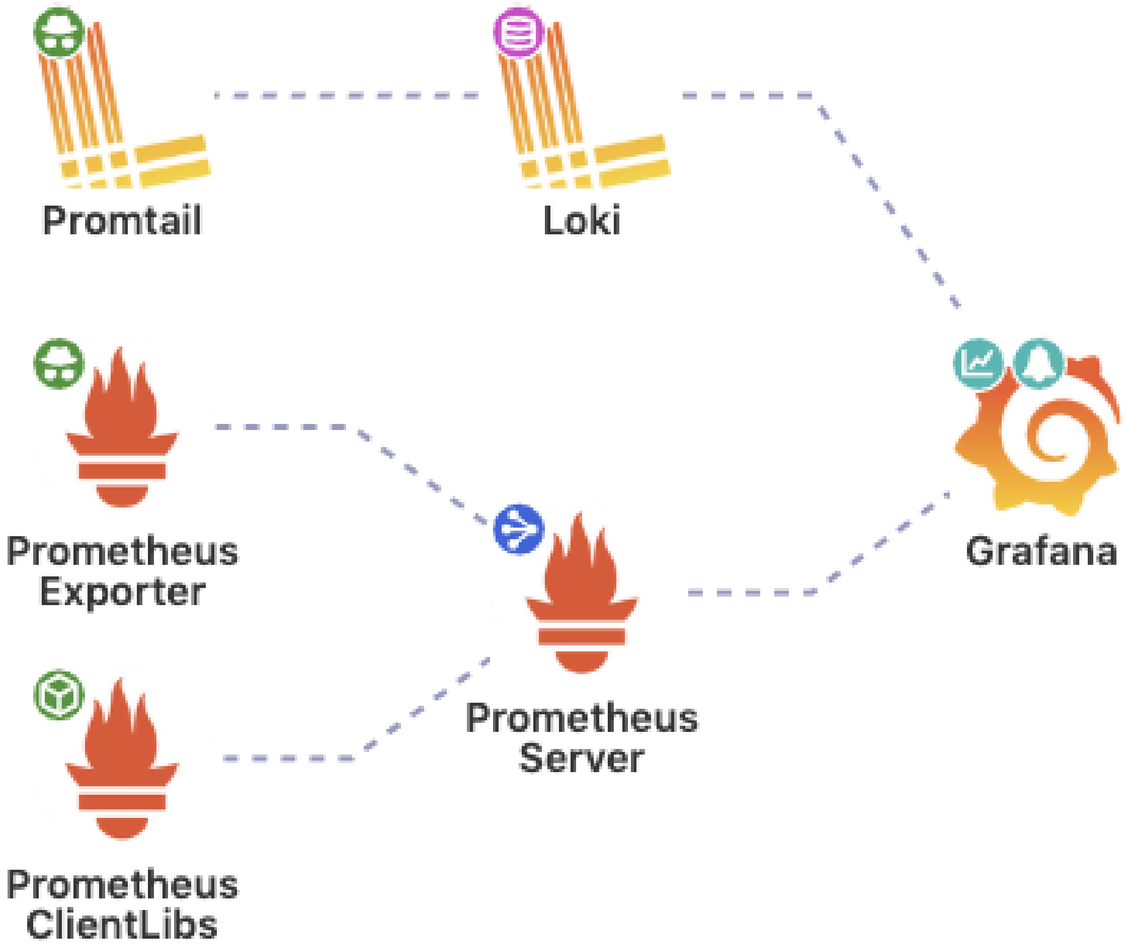
- Architecture



- Demo
  - https://www.elastic.co/demos
- Installation (Ansible ELK Playbook)
  - https://github.com/DanielBerman/ansible-elk-playbook

Grafana Loki

- Like Prometheus but for Logs!
- It is designed to be very cost effective and easy to operate.
- It does not index the contents of the logs, but rather a set of labels for each log stream
- A Loki-based logging stack consists of 3 components:
  - **Promtail** is the agent, responsible for gathering logs and sending them to Loki
  - **Loki** is the main server, responsible for storing logs and processing queries
  - **Grafana** for querying and displaying the logs



References

- Syslog-ng
  - https://github.com/syslog-ng/syslog-ng
- Rsyslog
  - https://github.com/rsyslog/rsyslog
- Graylog
  - https://docs.graylog.org/en/4.0/
- Grafana Loki
  - https://github.com/grafana/loki
- ELK Stack
  - https://github.com/elastic
- LibreNMS Syslog Integration
  - https://docs.librenms.org/Extensions/Syslog/

Log Management

Module 2: LAB

Labs

- Please follow the lab modules for
  - Lab 1: syslog-ng
  - Lab 2: rsyslog
  - Lab 3: Graylog

Thank You!