TRALIOS
Linux Server Management

Intern: Graylog

Large-scale Log Management

Luca Bilke ▪ 11.08.2022

Übersicht

TRALIOS
Linux Server Management

- Allgemeines
- Queries
- Input Extractors
- Alerts
- Dashboards

Allgemeines

TRALIOS
Linux Server Management

- Graylog, ehemals Torch, wurde in 2009 als Open Source Projekt von Lennart Koopmann in Hamburg gegründet.
- Der Hauptsitz befindet sich heute in Houston, Texas.
- Graylog veröffentlichte 2016 sein erstes kommerzielles Angebot.
- Im Jahr 2018 ist Graylog auf über 35.000 Installationen weltweit angewachsen.

Architektur

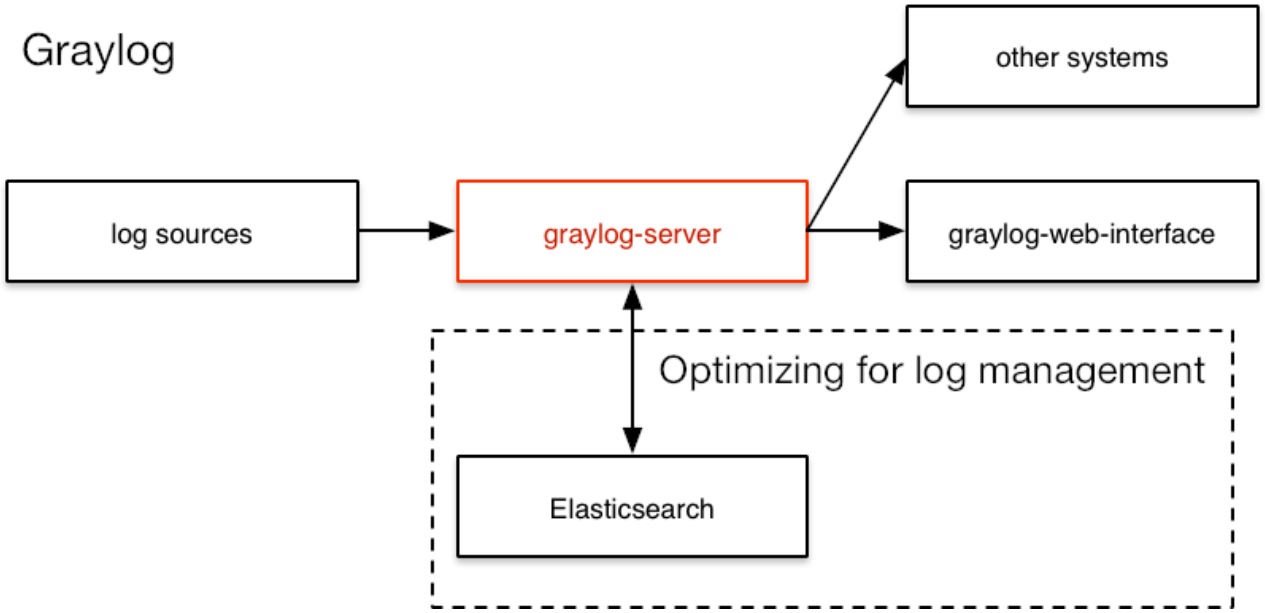

Abbildung: https://docs.graylog.org/docs/ideas-explained

Query Syntax

TRALIOS
Linux Server Management

ssh	*“ssh” kommt vor*
ssh login	*“ssh” oder “login” kommt vor*
“ssh login”	*der “ssh login” kommt vor*
type:ssh	*Feld “type” ist als “ssh” gesetzt*
type:(ssh OR login)	*Feld “type” hat den Wert “ssh” oder “login”*
type:“ssh login”	*Feld “type” ist als “ssh login” gesetzt*
exists:type	*Feld “type” existiert*

Mehr Query Syntax

TRALIOS
Linux Server Management

/ethernet[0-9]+/	*Regex Suche für “ethernet[0-9]+”*
*.sh	*Wildcard für mehrere Buchstaben*
exam?le	*Wildcard für einen einzelnen Buchstaben*
exmaple˜	*Fuzzy Match mit Levenshtein Distanz von 2*
exmplae˜5	*Fuzzy Match mit Levenshtein Distanz von 5*
“foo bar”˜	*Proximity search (Fuzzy Distance/Order)*

Noch mehr Query Syntax!

TRALIOS
Linux Server Management

http_code:[500 TO 504]	*500 <= Nummer <= 504*
http_code:{400 TO 404}	*400 < Nummer < 404*
bytes:{0 TO 64]	*0 < Nummer <= 64*
<, >, <=, >=	*Nur in eine Richtung beschränkt*
“2019-07-23 09:53:08.175”	*Datum (YYYY-MM-DD HH:MM:SS.sss)*
[now-5d TO now-4d]	*Relative Daten*

Weitere Syntax Kleinigkeiten

TRALIOS
Linux Server Management

& — : \ / + - ! ( ) { } [ ] ^ ~ * ?

Müssen mit einem Backslash escaped werden

Streams

TRALIOS
Linux Server Management

Streams werden ähnlich wie Searches definiert

Streams teilen Nachrichten in Kategorien, ein sobald sie ankommen

Dies ermöglicht Echzeitprozesse wie

- Alerting
- Forwarding an andere Prozesse

Text Extractors

TRALIOS
Linux Server Management

Extractors parsen Daten aus Messages und fügen diese Daten dann in Felder ein. Die gibt es in verschiedenen Varianten:

- Können vom Graylog Marketplace installiert werden
- Regex Patterns
- Grok Patterns
- JSON Parser
- Key=Value Pair Parser

Regex Extractors

TRALIOS
Linux Server Management

Regex Extractors funktionieren mit Capture Groups.

Um z.B: IP Addressen von SSH Logs auszulesen:

```
error: PAM: Permission denied for \w+ from ([\d.]+)
```

Lookup Tables

TRALIOS
Linux Server Management

Lookup Tables können Felder auf andere Values übersetzen/mappen

Das Lookup System besteht aus vier Komponenten:

- Data Adapter (Macht den Lookup)
- Caches (Cacht den Lookup)
- Table (Datenbank, CSV oder HTTP Endpoint mit Werten)

Alerts

TRALIOS
Linux Server Management

Konfigurierte Condition wird erfüllt → Alert wird getriggert

Condition Beispiele

- Search “program:traliosserverd AND POST AND NOT 200” returns a result
- Geolocation of “denied_ssh_ip” is in Russia
- Count of firewall event messages is over 100

Alerts können dann:

- E-Mail schicken
- Script ausführen
- HTTP request Durchführen

Widgets

TRALIOS
Linux Server Management

Widgets visualisieren konfigurierte Metriken, z.B:

1. Durchschnittliche Werte
2. Anzahl von Messages mit bestimmten Wert
3. Heatmap aus mehreren Werten erstellt

Dashboards

TRALIOS
Linux Server Management

Dashboards bestehen aus mehreren Widgets

Dashboards haben ein paar Vorteile:

- Widgets können verschiedene Queries/Time Ranges benützen
- Man kann für ein Dashboard global die Time Ranges ändern
- Ein Dashboard kann mehrere Tabs haben
- Ein Dashboard kann mehrere Searches anzeigen

Dashboard Beispiel

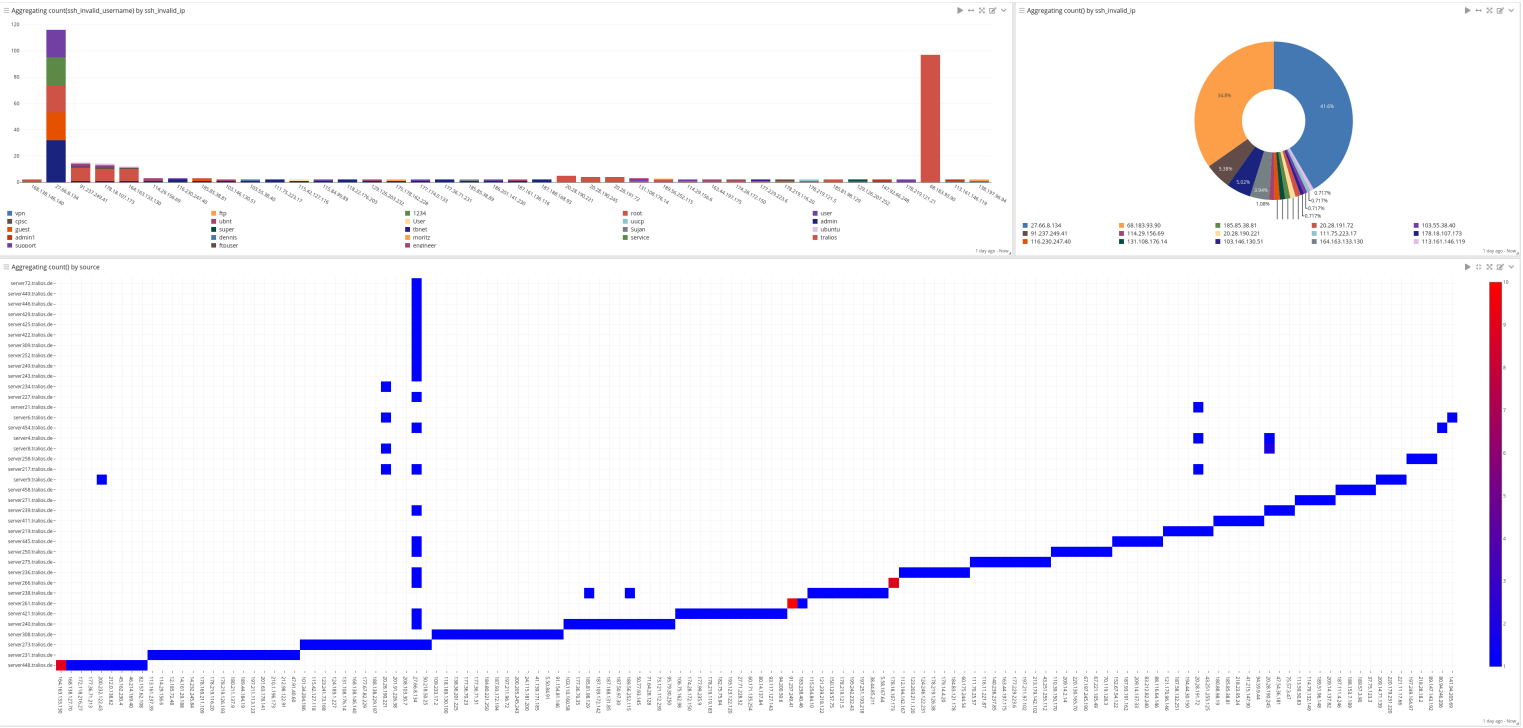

Abbildung: https://docs.graylog.org/docs/dashboards

Fazit

- Sachen, die man sich merken sollte
- Aktueller Stand und Ausblick

Danke

TRALIOS
Linux Server Management

Danke für Ihre Aufmerksamkeit!