

Build Your Own SIEM

Kyle Donnelly – Security Engineer – Haas Automation

Zane Gittins – Security Engineer – Haas Automation

Our Backgrounds

- Kyle
 - ~4.5 Years @ Haas
 - Multiple Technical Roles
 - CSU Chico Alum
- Zane
 - ~1.5 Years @ Haas
 - First Security Engineer
 - CSU Channel Islands Alum & Working on Graduate in Computer Science

What is a SIEM?

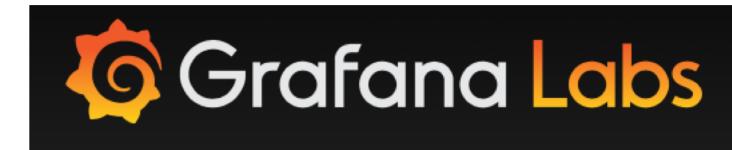
- Security Information and Event Management
- One Stop Shop

Why Build Your Own?

- Central Log Management
- Highly Configurable
- Gets Grease Under Fingernails
- Only Cost Is Man Hours + VM's
- Scalable

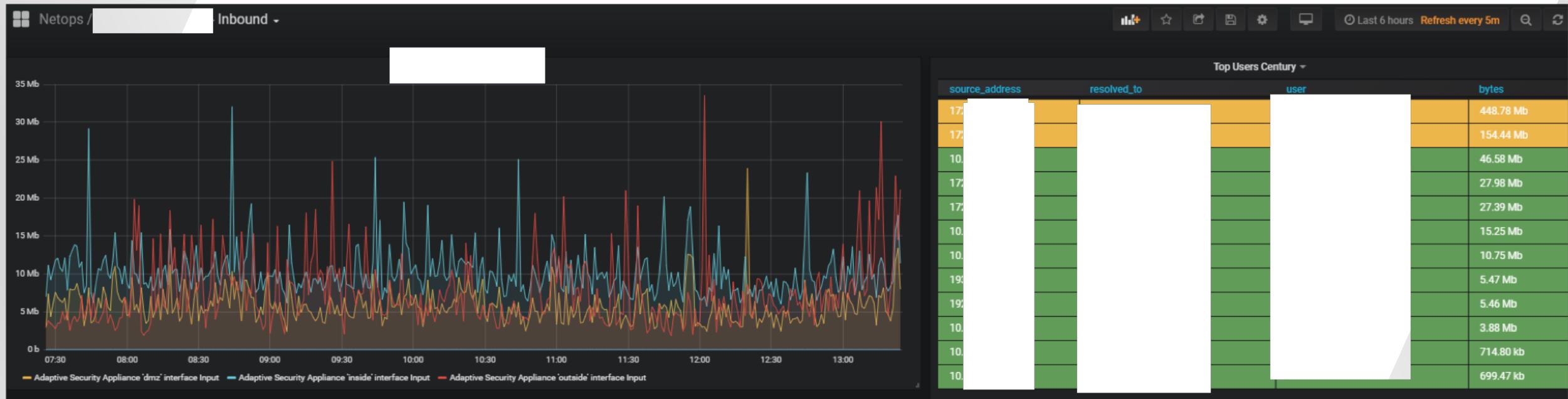
Technologies Used

- Graylog
 - ElasticSearch
 - MongoDB
- Zabbix
 - MySQL
- Grafana
- Syslog
- Winlogbeat/Filebeat
- InfluxDB
- HAProxy
- CentOS/Ubuntu



Grafana

- Monitoring/Analytics Tool
- Dashboards
- Plugins
- Many DataSources
- Alerts





Alerts

Windows Events

1246

Bash

112 commands

FireEye

36 events

HTTP Traffic

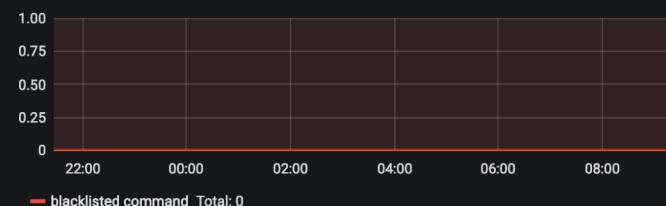
3533 requests

Attacks - Successful

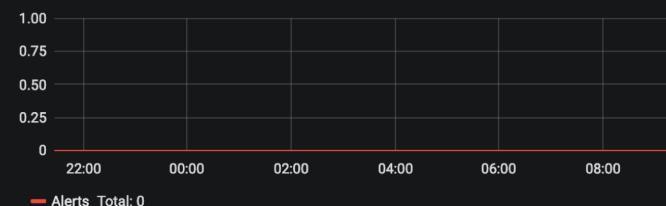


No alerts

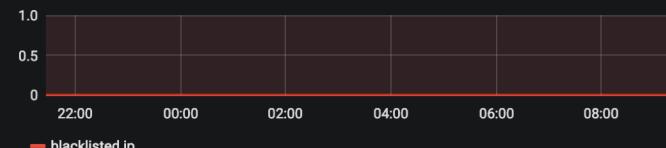
Bash History Blacklist



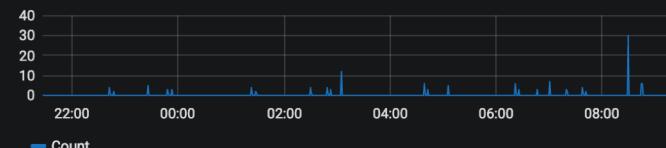
Palo Alto



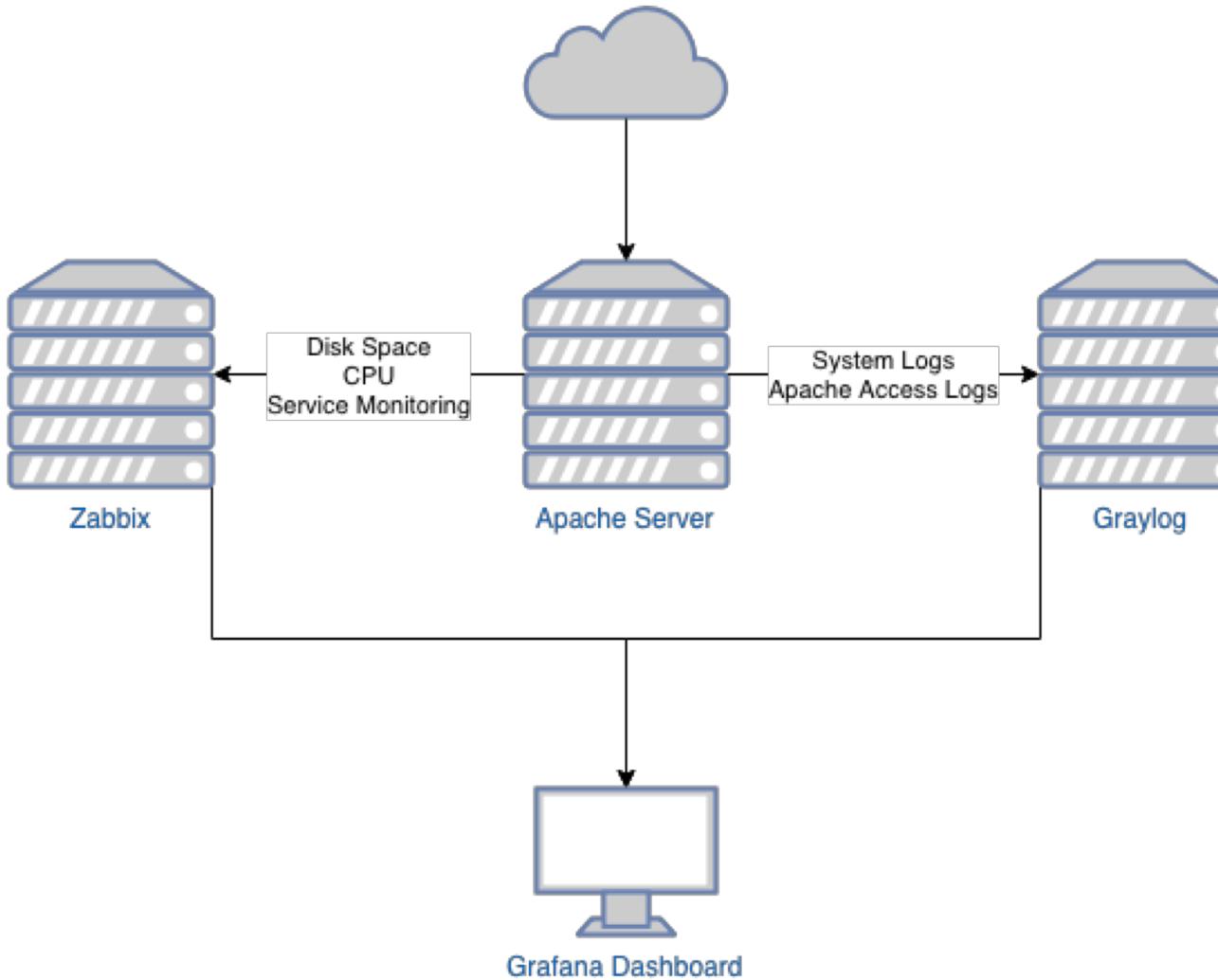
Connection Spy Blacklisted IP

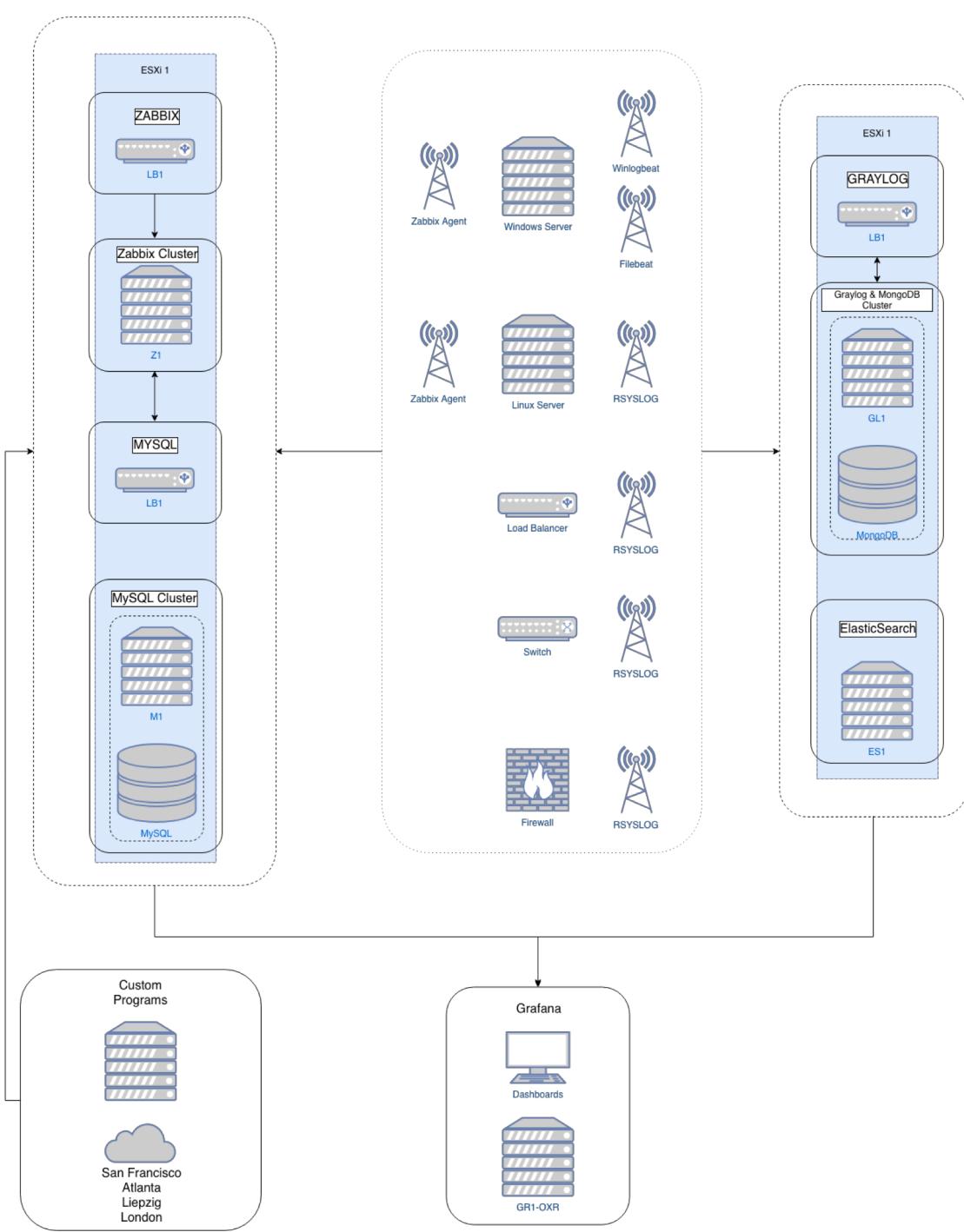


Linux Connections



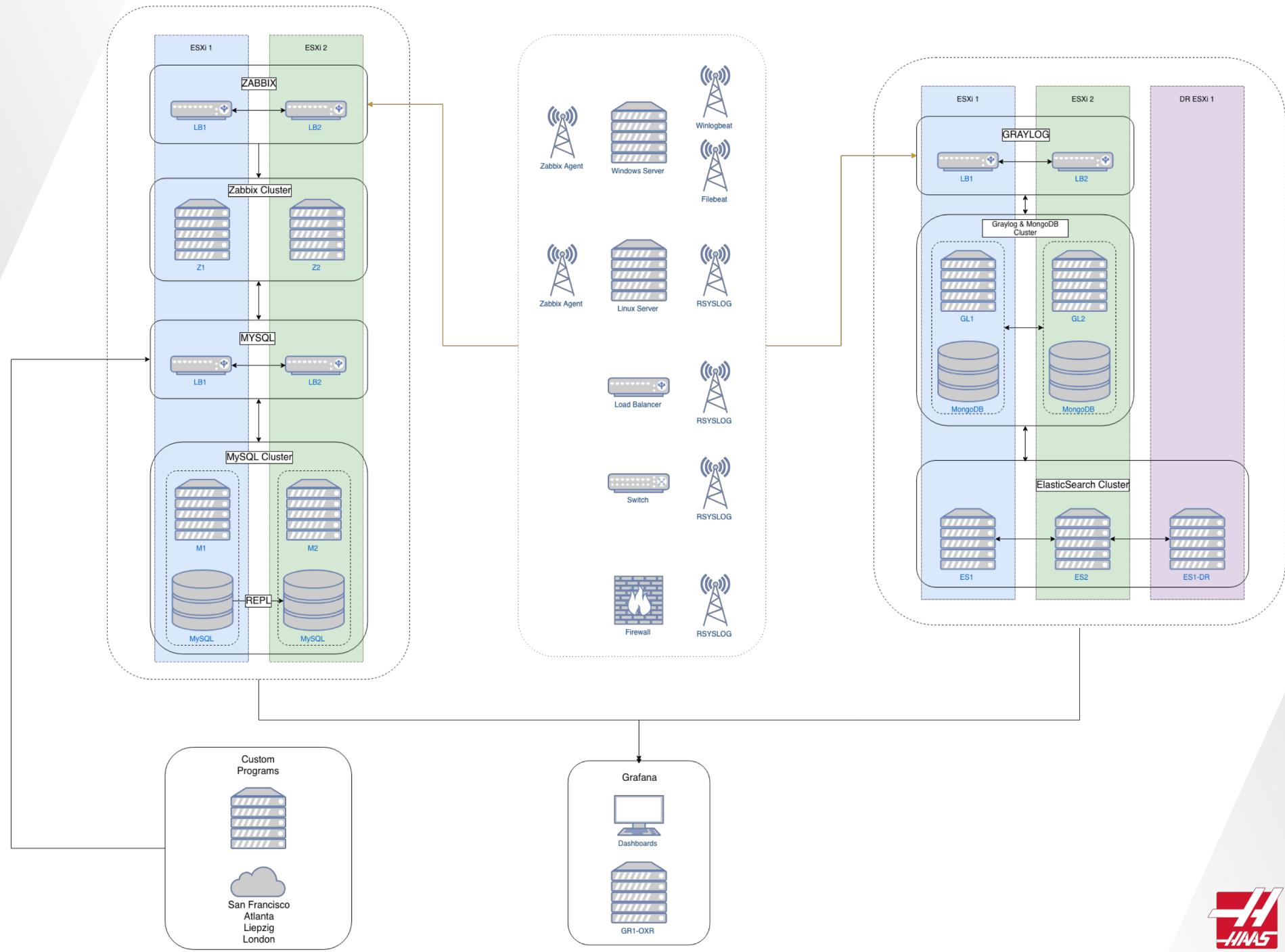
Landscape Overview



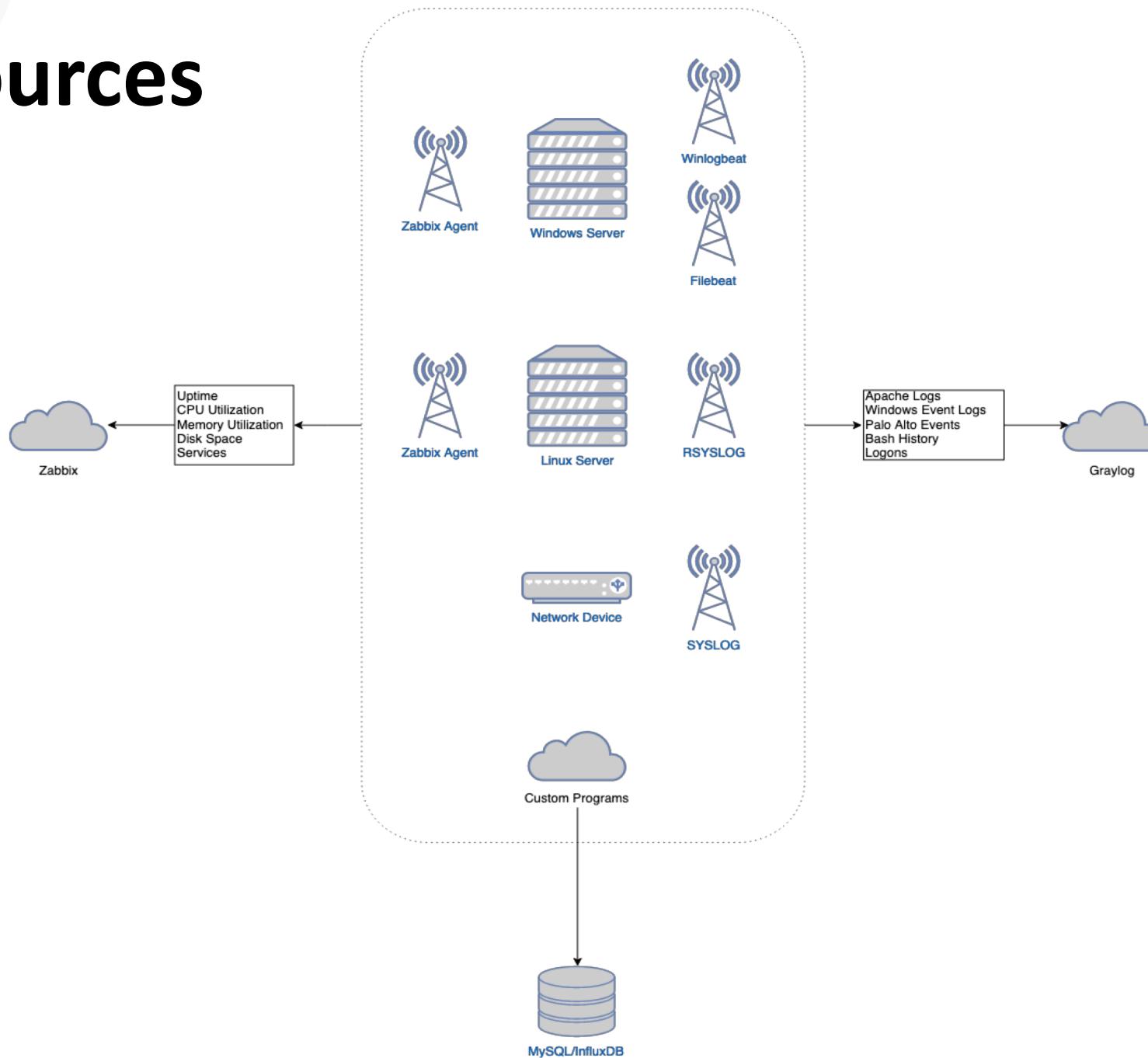


v1 Sizing

- Three VMs
- Zabbix/Grafana Server
 - 2 vCPU / 8GB RAM
 - 25 GB Disk (MySQL Database)
- Graylog Servers
 - Graylog/MongoDB
 - 4 vCPU / 4GB RAM
 - 25 GB Disk (MongoDB)
 - ElasticSearch
 - 4 vCPU / 16GB RAM
 - 100 GB Disk



Data Sources



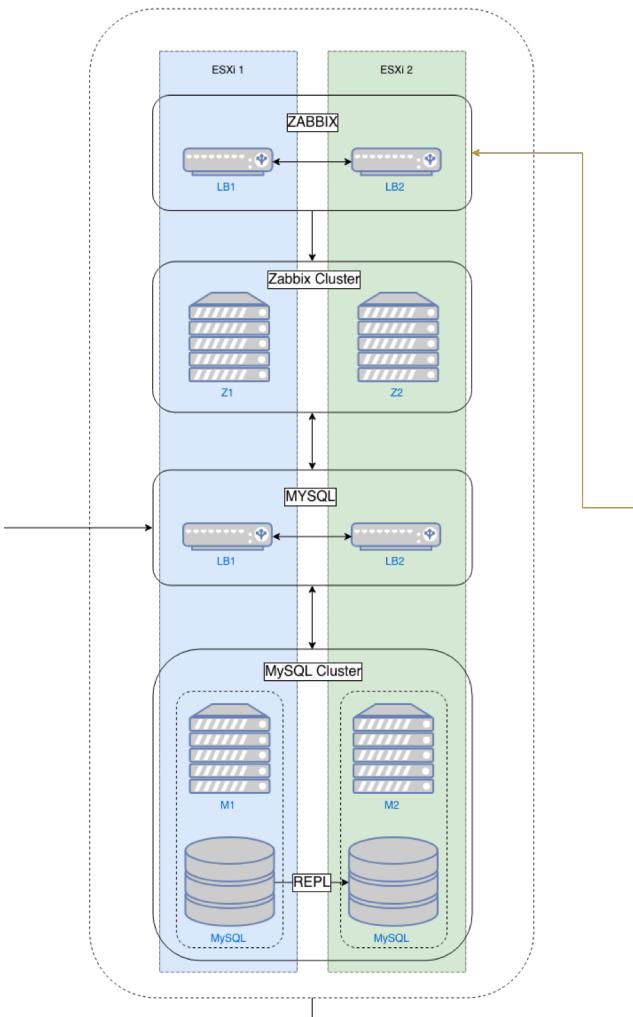
Data Sources

- Windows
 - Event Logs (Winlogbeat)
 - Flat File Logs (Filebeat)
- Linux
 - System Logs (Rsyslog)
 - Application Logs (Local Facilities -> Rsyslog)
- Network Devices
 - Cisco Devices
 - Palo Alto
 - F5
- Zabbix
- Custom Programs/Scripts
 - San Francisco

Zabbix Overview

- Open Source Monitoring Tool
- Agent & Agentless
- 3.4 -> 4.0 LTS
- Web GUI

Zabbix Landscape



Zabbix Server

- Host Monitoring
 - CPU
 - Disk
 - Memory
 - Services
- Web Monitoring
 - Unit Testing
 - Performance Testing

<input type="checkbox"/> Wizard	Name ▲	Triggers	Key
<input type="checkbox"/>	Haas - Windows: Agent ping	Triggers 1	agent.ping
<input type="checkbox"/>	Haas - Windows: Average disk read queue length		perf_counter[\234(_Total)\1402]
<input type="checkbox"/>	Haas - Windows: Average disk write queue length		perf_counter[\234(_Total)\1404]
<input type="checkbox"/>	Haas - Windows: File read bytes per second		perf_counter[\2\16]
<input type="checkbox"/>	Haas - Windows: File write bytes per second		perf_counter[\2\18]
<input type="checkbox"/>	Mounted filesystem discovery: Free disk space on C:		vfs.fs.size[C:,free]
<input type="checkbox"/>	Mounted filesystem discovery: Free disk space on E:		vfs.fs.size[E:,free]
<input type="checkbox"/>	Mounted filesystem discovery: Free disk space on C: (percentage)	Triggers 1	vfs.fs.size[C:,pfree]
<input type="checkbox"/>	Mounted filesystem discovery: Free disk space on E: (percentage)	Triggers 1	vfs.fs.size[E:,pfree]

<input type="checkbox"/>	Severity	Name ▲
<input type="checkbox"/>	Average	Mounted filesystem discovery : Free disk space is less than 10% on volume C:
<input type="checkbox"/>	Average	Mounted filesystem discovery : Free disk space is less than 10% on volume E:
<input type="checkbox"/>	Average	Haas - Windows : Host information was changed on {HOST.NAME}
<input type="checkbox"/>	Information	Haas - Windows : Host name of zabbix_agentd was changed on {HOST.NAME}
<input type="checkbox"/>	Average	Haas - Windows : Lack of available virtual memory on server {HOST.NAME}
<input type="checkbox"/>	Average	Haas - Windows : Lack of free memory on server {HOST.NAME}
<input type="checkbox"/>	Average	Haas - Windows : Processor load is too high on {HOST.NAME}
<input type="checkbox"/>	High	SQL Service Broker Status
<input type="checkbox"/>	High	TCP Tunnel Status
<input type="checkbox"/>	Average	Haas - Windows : Too many processes on {HOST.NAME}
<input type="checkbox"/>	Information	Haas - Windows : Version of zabbix_agent(d) was changed on {HOST.NAME}
<input type="checkbox"/>	Average	Haas - Windows : Zabbix agent on {HOST.NAME} is unreachable for 5 minutes
<input type="checkbox"/>	Average	Haas - Windows : {HOST.NAME} has just been restarted

Up

Landing Page (RT)

159 ms

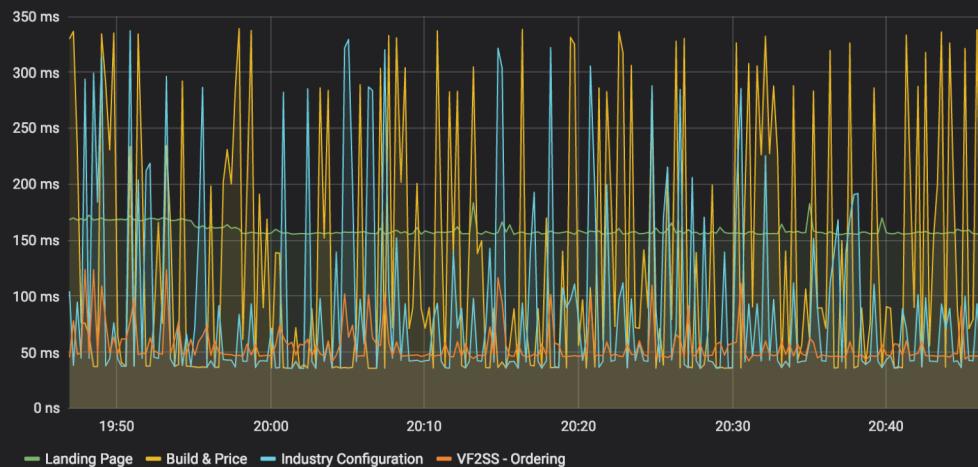
Build & Pricing (RT)

135.3 ms

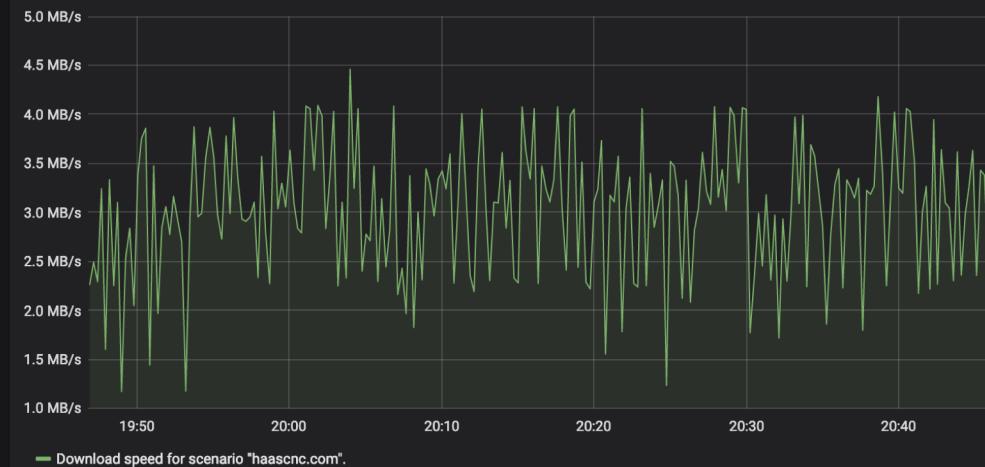
VF-2SS Customization (RT)

55.4 ms

Response Times



Download Speed



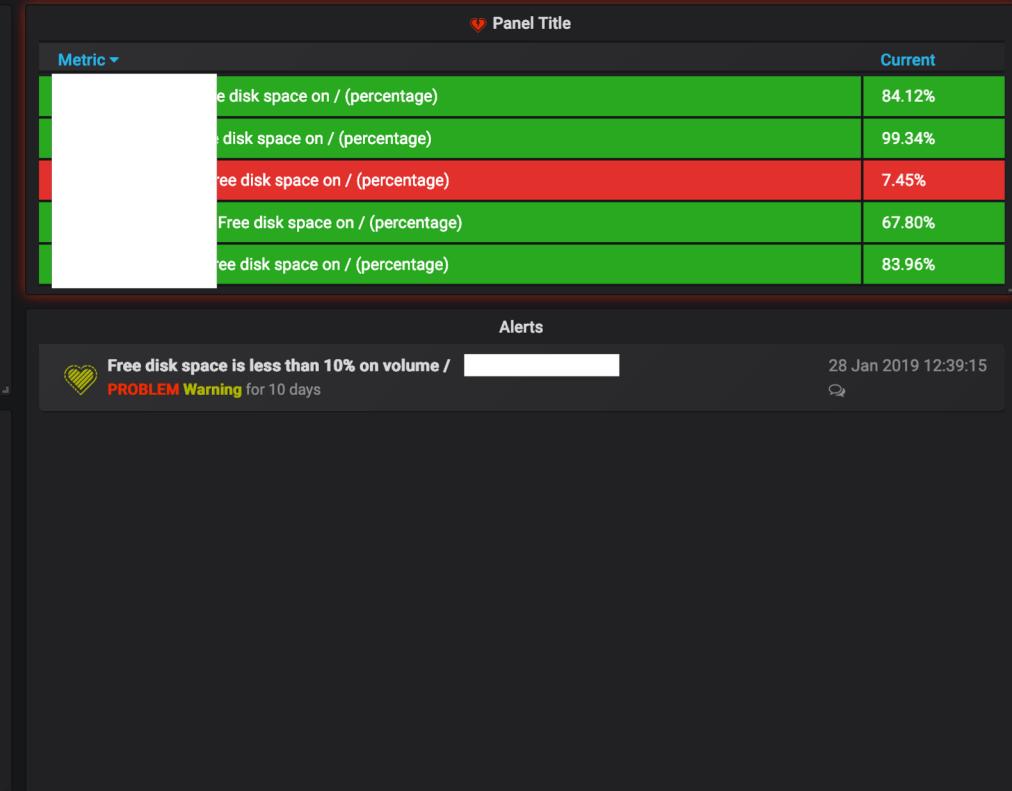
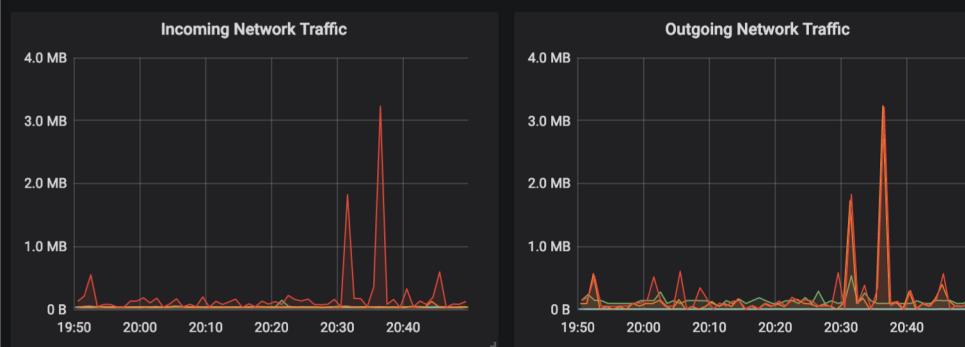
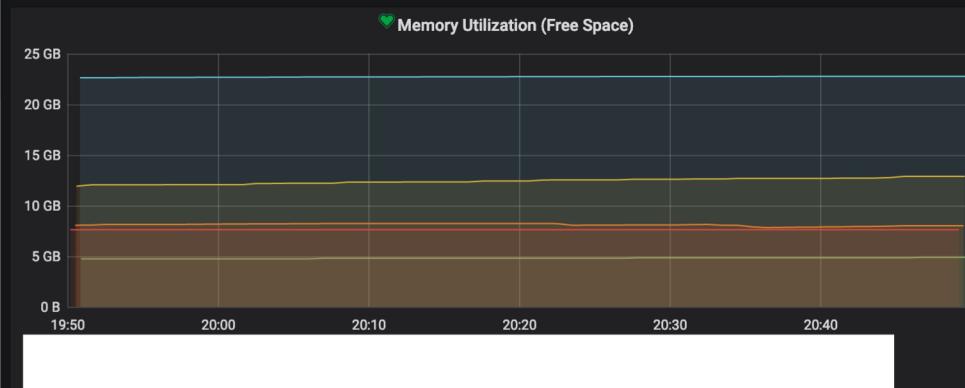
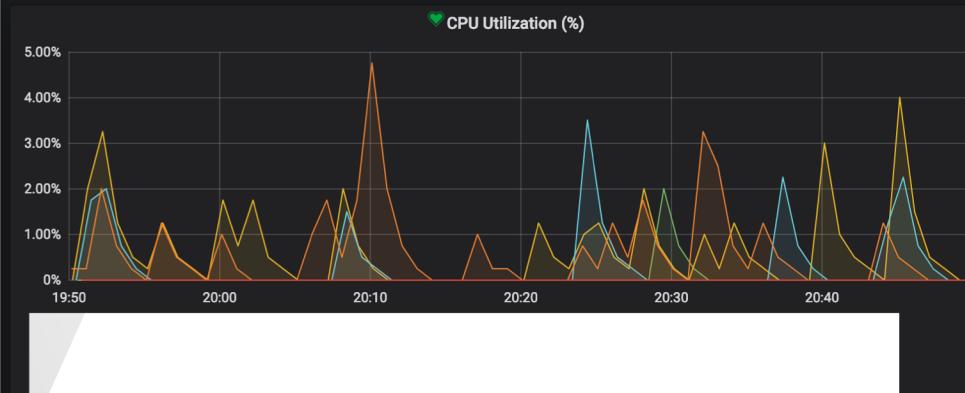
Incoming Network Utilization



Outgoing Network Utilization



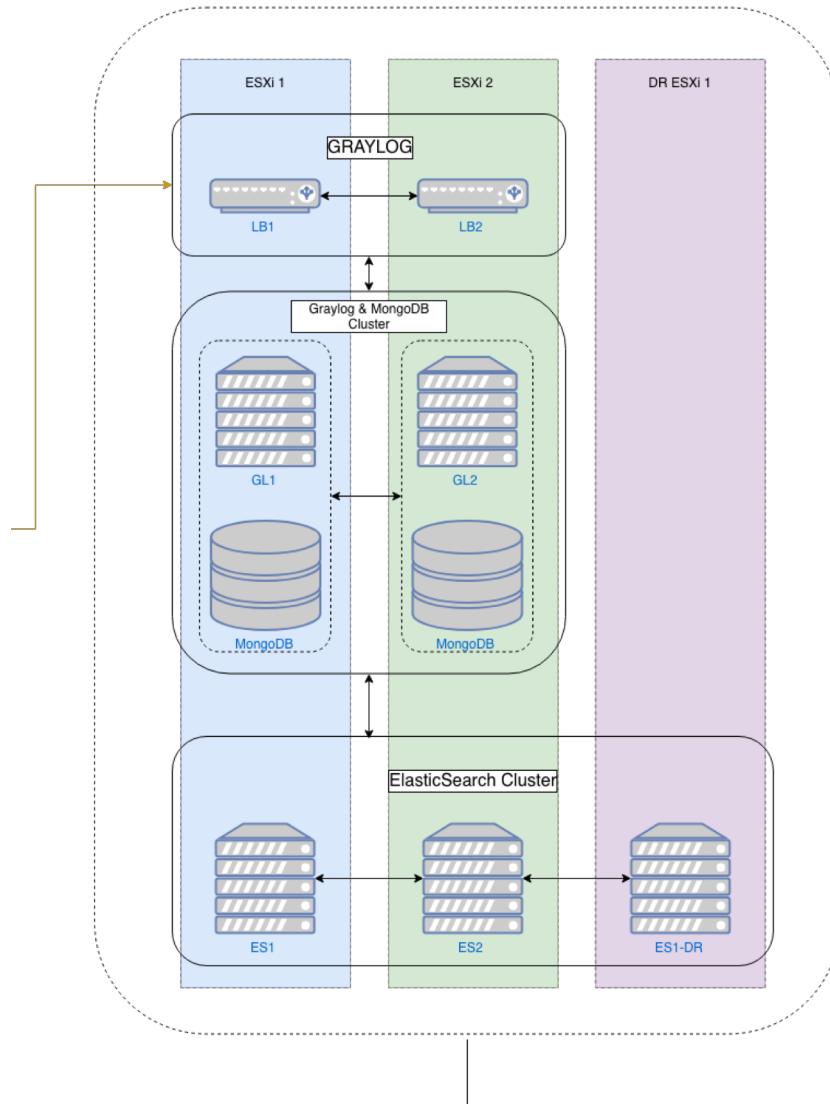
Haas
F1 Team
OFFICIAL MACHINE TOOL



GrayLog Overview

- Log Management Platform
- Intuitive Web Console
- MongoDB/ElasticSearch
- 2.5 -> 3.0 LTS

GrayLog Landscape



GrayLog Server

- Network/System/Application Logs
 - RSYSLOG – Linux
 - Application
 - SYSLOG – Appliances
 - Filebeat
 - Winlogbeat

Search in the last 5 minutes Not updating

Saved searches



Type your search query here and press enter. ("not found" AND http) OR http_response_code:[400 TO 404]



Search result

Found 17,394 messages in 5 ms, searched in 4 indices.
Results retrieved at 2019-02-07 21:24:39.

 Add count to dashboard Save search criteria More actions ▾ Fields Decorators Default All None Filter fields

- ▶ bytes_sent
- ▶ destination_ip
- ▶ destination_port
- ▶ facility
- ▶ http_status
- ▶ level
- ▶ message
- ▶ name
- ▶ proxy
- ▶ referer
- ▶ remote_user
- ▶ site
- ▶ source
- ▶ source_ip
- ▶ source_ip_city_name
- ▶ source_ip_country_code
- ▶ source_ip_geolocation
- ▶ timestamp
- ▶ type

List fields of [current page](#) or [all fields](#). Highlight results<https://graylog.haascnc.com/alerts>

Histogram

 Year, Quarter, Month, Week, Day, Hour, Minute

Messages

 Previous Next

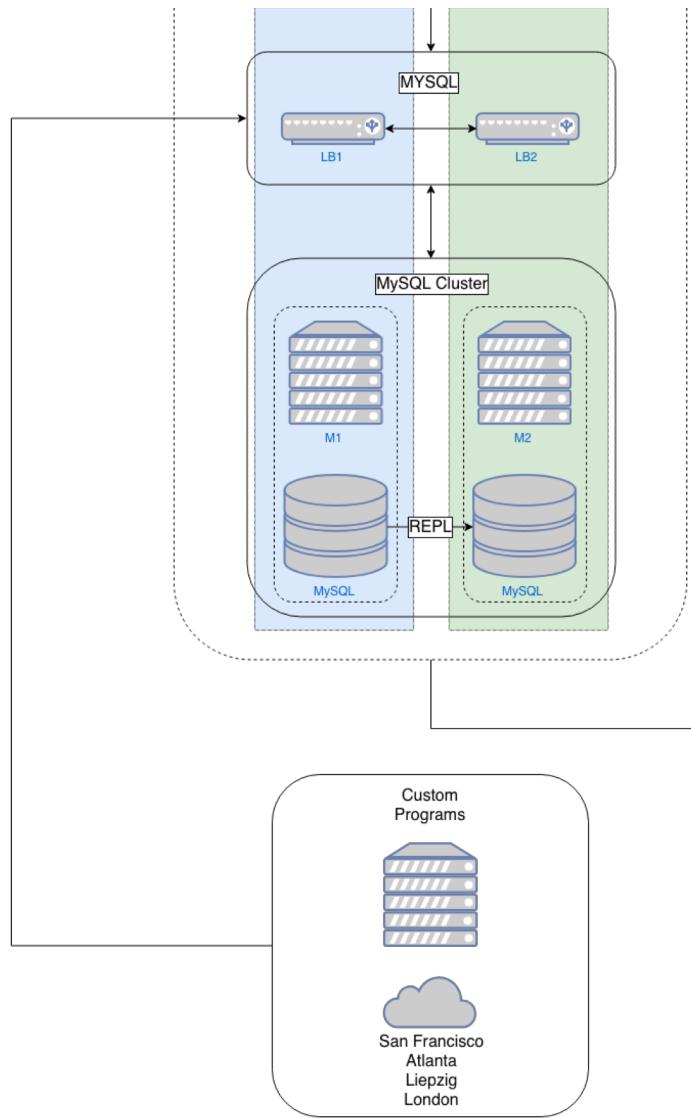
Timestamp	source
2019-02-07 21:24:35.586	10.3.4.91
2019-02-07 21:24:35.583	10.3.4.91
2019-02-07 21:24:35.106	10.3.4.91
2019-02-07 21:24:35.023	10.3.4.91
2019-02-07 21:24:35.000	linux-aempdis1
2019-02-07 21:24:35.000	linux-aempdis1
2019-02-07 21:24:35.000	linux-lb1-phx

 Haas
F1 Team
OFFICIAL MACHINE TOOL

Custom Monitoring Programs

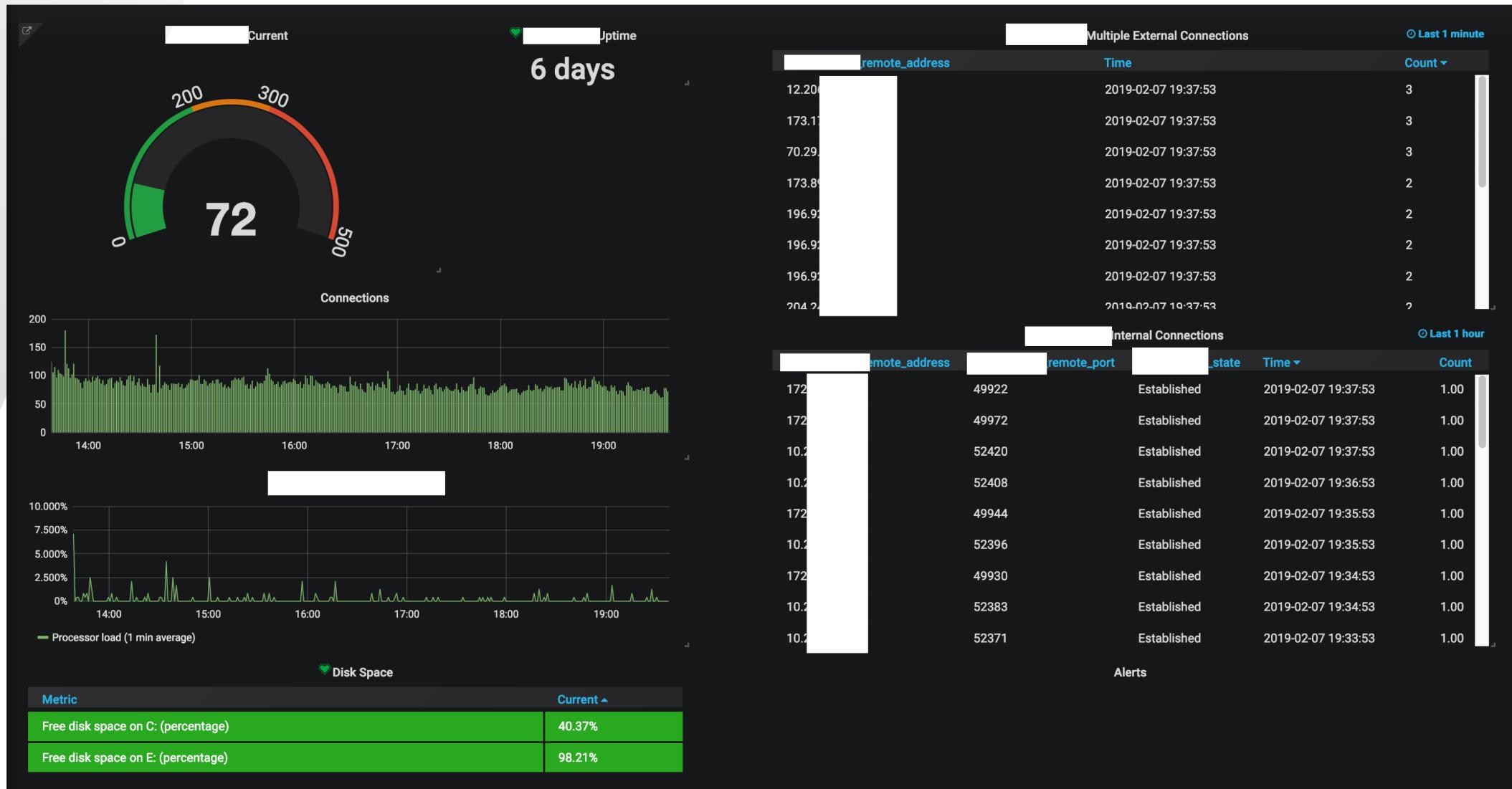
- Application Monitoring
- Custom Host Monitoring
- Database Monitoring

Custom Programs Landscape



PowerShell Example

- Get-NetTCPConnection -LocalPort 443
- Write Script to Parse Returned Values
- Put on Scheduled Task
- Script + Zabbix



Inputs

Remote Rsyslog Syslog TCP 1 RUNNING

```
allow_override_date: true
bind_address: 0.0.0.0
expand_structured_data: false
force_rdns: false
max_message_size: 2097152
override_source: <empty>
port: 5140
recv_buffer_size: 1048576
store_full_message: false
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password: *****
use_null_delimiter: false
```

[Show received messages](#)[Manage extractors](#)[Stop input](#)[More actions ▾](#)

Throughput / Metrics

1 minute average rate: 122 msg/s
Network IO: ▼22.3KB ▲0B (total: ▼21.3GB ▲0B)
Active connections: 12 (376,753 total)
Empty messages discarded: 1,121,226
[Show details](#)

Windows Beats Beats (deprecated) 1 RUNNING

```
bind_address: 0.0.0.0
override_source: <empty>
port: 5145
recv_buffer_size: 1048576
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password: *****
```

[Show received messages](#)[Manage extractors](#)[Stop input](#)[More actions ▾](#)

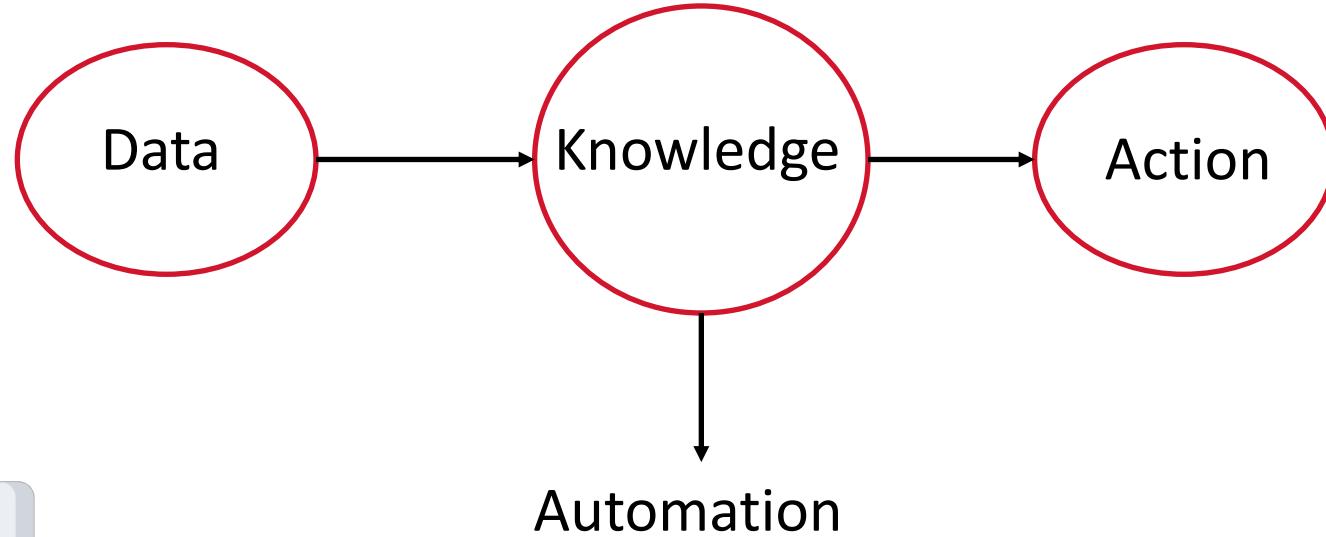
Throughput / Metrics

1 minute average rate: 8 msg/s
Network IO: ▼4.2KB ▲6.0B (total: ▼2.4GB ▲4.5MB)
Active connections: 5 (24,161 total)
Empty messages discarded: 0
[Show details](#)



Meaningful Data

- Extractors.
- Pipelines.
- Code.



Extractors

- Copy Input
- Grok Patterns
- JSON
- Regex
- Delimiters
- Substrings
- Lookup Tables

55.3.244.1 GET /index.html 15824 0.043

%{IP:client} %{WORD:method}
%{URIPATHPARAM:request} %{NUMBER:bytes}
%{NUMBER:duration}

Extractors: Use Case

- Identify malicious activity in Apache logs.

```
apache-access example.server  
<ip address>  
POST /q.php HTTP/1.1 200
```

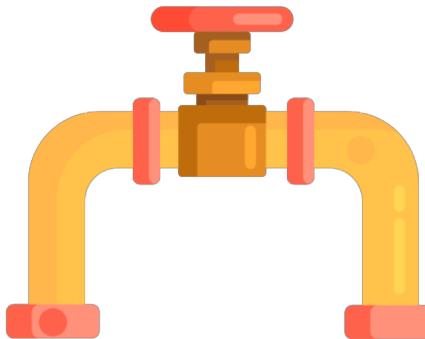


Extractors

Configured extractors		
Sort extractors		
F5_destination_ip Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>destination_ip</i> , leaving the original intact.	Delete	
F5_destination_port Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>destination_port</i> , leaving the original intact.	Delete	
F5_source_ip_extractor Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>source_ip</i> , leaving the original intact.	Delete	
F5_url Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>url</i> , leaving the original intact.	Delete	
Honeypot_source_ip Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>source_ip</i> , leaving the original intact.	Delete	
HAProxy_source_ip Regular expression	Details	Edit
Trying to extract data from <i>message</i> into <i>source_ip</i> , leaving the original intact.	Delete	
Honeypot_source_ip Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>source_ip</i> , leaving the original intact.	Delete	
Honeypot_destination_port Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>destination_port</i> , leaving the original intact.	Delete	
Honeypot_FP_source_ip Regular expression	Details	Edit
Trying to extract data from <i>message</i> into <i>source_ip</i> , leaving the original intact.	Delete	
Apache_site Split & Index	Details	Edit
Trying to extract data from <i>message</i> into <i>site</i> , leaving the original intact.	Delete	

Pipelines

- Stages
- Rules



```
rule "has firewall fields"
when
    has_field("src_ip") && has_field("dst_ip")
then
    <do action>
end
```

Pipelines

Pipeline HAProxyStats

Pipelines let you transform and process messages coming from streams. Pipelines consist of stages where rules are evaluated and applied. Messages can go through one or more stages.

[Manage pipelines](#) [Manage rules](#) [Simulator](#)

 After each stage is completed, you can decide if messages matching all or one of the rules continue to the next stage.

Details

Title: HAProxyStats
Description:
Created: 7 hours ago
Last modified: 6 hours ago
Current throughput: 0 msg/s

[Edit pipeline details](#)

Pipeline connections

This pipeline is processing messages from the stream "HAProxyStats".

[Edit connections](#)

Pipeline Stages

Stages are groups of conditions and actions which need to run in order, and provide the necessary control flow to decide whether or not to run the rest of a pipeline.

[Add new stage](#)

Stage 0

Contains 1 rule
Messages satisfying at least one rule in this stage, will continue to the next stage.
Throughput: 0 msg/s

[Delete](#) [Edit](#)

Title	Description	Throughput	Errors
function haproxy statistics fields		0 msg/s	0 errors/s (5 total)

Stage 1

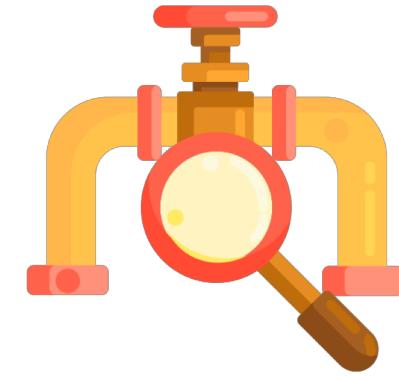
Contains 1 rule
There are no further stages in this pipeline. Once rules in this stage are applied, the pipeline will have finished processing.
Throughput: 0 msg/s

[Delete](#) [Edit](#)

Title	Description	Throughput	Errors
convert string float to numeric	Convert fields to numeric values.	0 msg/s	0 errors/s (0 total)

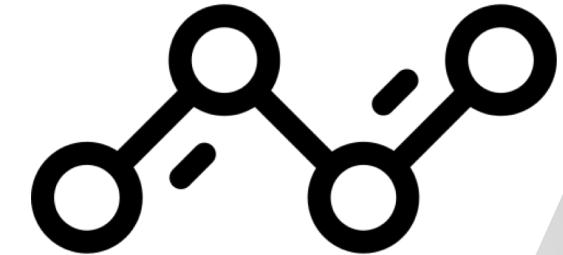
Pipelines: Use Case

- Clean “dirty” data.
- Drop noisy logs.
- Calculate hashes, match IP to CIDR, format dates, AlienVault OTX, Spamhaus, whois, and much more.



Code

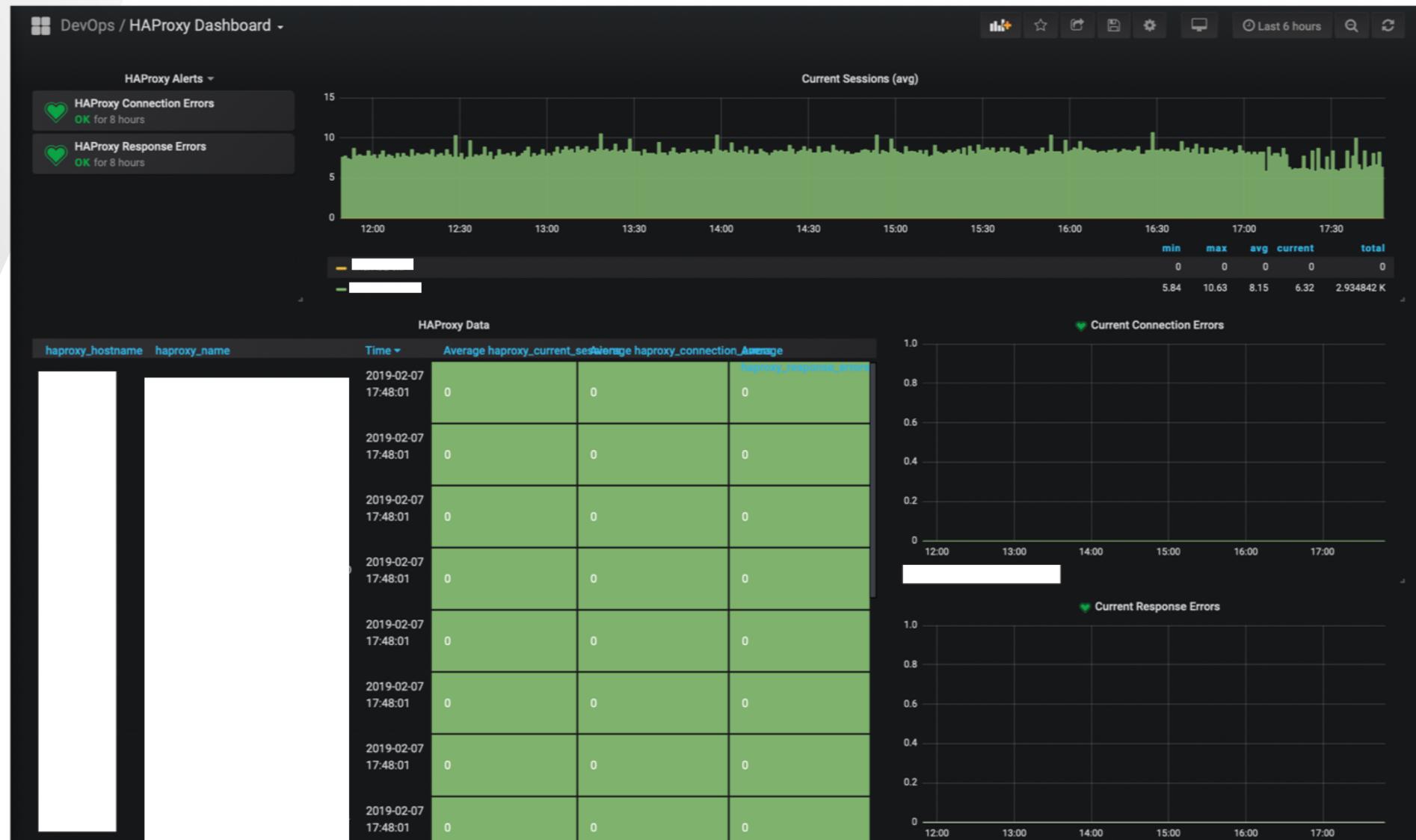
- TCP connections.
- Most powerful and time consuming.
- Language considerations.



Code: Use Case

- Connectors.
- Multiple databases.
- Environment Specific.



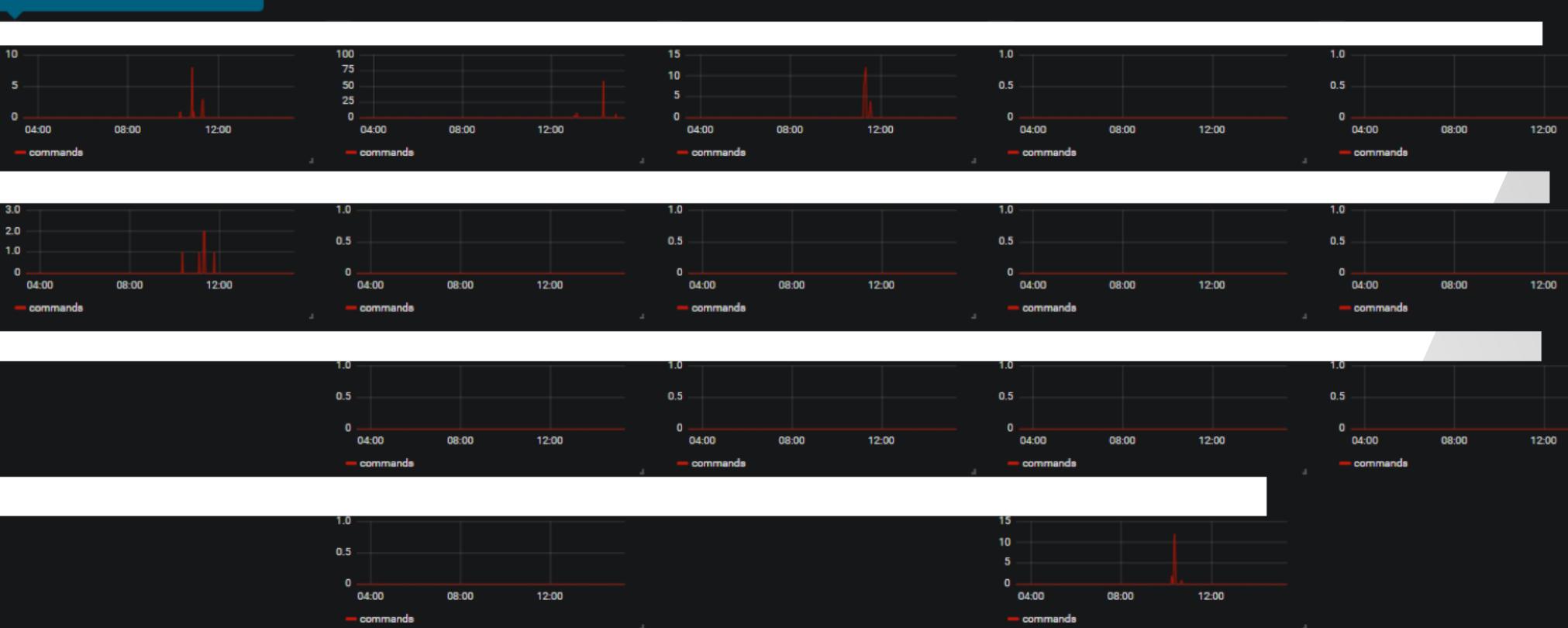


Drilldowns

GrayLog > Bash Overwatch

Bash command count for [REDACTED]

• Drilldown



Drilldowns

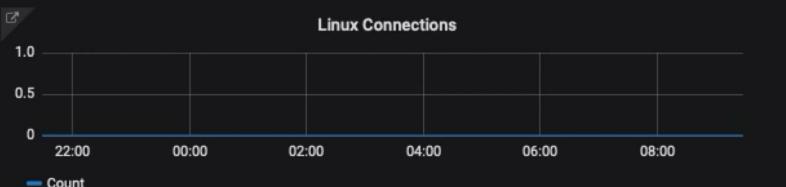
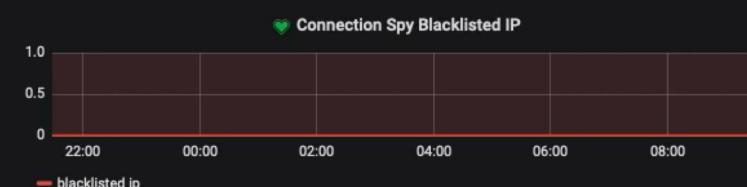
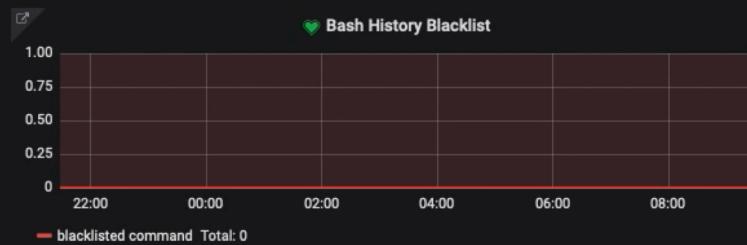
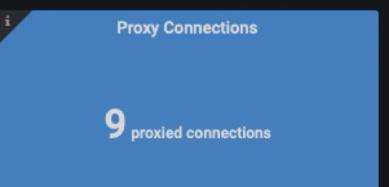
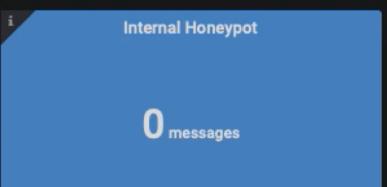
GrayLog > Bash Overwatch > Bash Commands

linux-hp1-oxr -- bash history ▾

timestamp ▾	bash_history_hostname	bash_history_user	bash_history_command	bash_history_return_code	Count
2019-02-04 16:33:05.337	linux-hp1-oxr	devops	systemctl restart rsyslog	[130]	1.00
2019-02-04 16:32:58.537	linux-hp1-oxr	devops	sudo nano graylog.conf	[0]	1.00
2019-02-04 16:32:28.965	linux-hp1-oxr	devops	ls	[0]	1.00
2019-02-04 16:32:28.669	linux-hp1-oxr	devops	clear	[0]	1.00
2019-02-04 16:32:26.641	linux-hp1-oxr	devops	ls	[0]	1.00
2019-02-04 16:32:26.221	linux-hp1-oxr	devops	cd /etc/rsyslog.d/	[0]	1.00
2019-02-04 16:32:23.932	linux-hp1-oxr	devops	cd connection_spy/	[0]	1.00

Alerts

SQLi Attacks ALERTING for 2 hours



Alerting

- Know exactly why an alert triggers.
- Many Ways to Alert:
 - Email
 - Slack
 - SMS
 - And many more.



Appendix

- Rsyslog:
 - <https://github.com/rsyslog/rsyslog>
- Graylog
 - <https://www.graylog.org/products/open-source>
- Zabbix:
 - <https://www.zabbix.com/>
- Winlogbeat:
 - <https://www.elastic.co/downloads/beats/winlogbeat-oss>
 - <https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-getting-started.html>
- Filebeat –
 - <https://www.elastic.co/downloads/beats/filebeat-oss>
 - <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-getting-started.html>
- ElasticSearch:
 - <https://www.elastic.co/downloads/elasticsearch-oss>
- Grafana:
 - <http://docs.grafana.org/installation/debian/>
- Icons:
 - www.flaticon.com