Introduction to Logging
with the ELK Stack

Amy Ghate
Solutions Architect
logs + metrics + apm = ObservaBLT
Observability
Elastic Approach to Observability

Dev & Ops Teams

Log Data
- Web Logs
- App Logs
- Database Logs
- Container Logs

Metrics Data
- Container Metrics
- Host Metrics
- Database Metrics
- Network Metrics
- Storage Metrics

APM Data
- Real User Monitoring
- Txn Perf Monitoring
- Distributed Tracing

Uptime Data
- Uptime
- Response Time

Kibana

Elasticsearch
Agenda
Things we're going to cover

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security
Agenda

Challenges with log analytics

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security
Logs for one host or app
This is fairly straightforward

```bash
$ > tail -f /var/log/messages
Dec 10 14:05:30 justa-build kernel: type=1326 audit(1575986730.517:383998660): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17069 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7efe9c254889 code=0x50000
Dec 10 14:05:30 justa-build kernel: type=1326 audit(1575986730.551:383998661): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17069 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7efe9c269171 code=0x50000
Dec 10 14:05:33 justa-build kernel: type=1326 audit(1575986733.110:383998662): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17179 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7fee1cf0f889 code=0x50000
Dec 10 14:05:33 justa-build kernel: type=1326 audit(1575986733.150:383998663): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17179 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7fee1cf24171 code=0x50000
Dec 10 14:05:35 justa-build kernel: type=1326 audit(1575986735.155:383998664): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17367 comm="node" sig=0 arch=c000003e syscall=324 compat=0 ip=0x7ffb3b7bf889 code=0x50000
Dec 10 14:05:35 justa-build kernel: type=1326 audit(1575986735.194:383998665): auid=4294967295 uid=0 gid=0 ses=4294967295 subj=system_u:system_r:container_runtime_t:s0 pid=17367 comm="node" sig=0 arch=c000003e syscall=332 compat=0 ip=0x7ffb3b7d4171 code=0x50000
```
Interacting with logs
Built-in tools for log viewing

• grep
• tail
• cat / less / more / type
• sed / awk / perl
• vim / notepad / event viewer
• clever combinations of the above
Immediate needs for log analytics

What's missing from the previous desktop

- Easy setup for a variety of sources
- Correlating and cross referencing
- Searching, filtering, and highlighting
- Visualize
- Anomaly detection and alerting
- Flexible retention
Agenda
Things we're going to cover

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security
We're running in Elastic Cloud
Works the same in the cloud or running the default distribution
Click on the Logging Button
Works the same in the cloud or running the default distribution
Many choices
We're going to ingest the **System logs**

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apache logs</strong></td>
<td>Collect and parse access and error logs created by the Apache HTTP server.</td>
</tr>
<tr>
<td><strong>Cloudwatch Logs</strong></td>
<td>Collect Cloudwatch logs with Functionbeat</td>
</tr>
<tr>
<td><strong>Elasticsearch logs</strong></td>
<td>Collect and parse logs created by Elasticsearch.</td>
</tr>
<tr>
<td><strong>IIS logs</strong></td>
<td>Collect and parse access and error logs created by the IIS HTTP server.</td>
</tr>
<tr>
<td><strong>Kafka logs</strong></td>
<td>Collect and parse logs created by Kafka.</td>
</tr>
<tr>
<td><strong>Logstash logs</strong></td>
<td>Collect and parse debug and slow logs created by Logstash itself.</td>
</tr>
<tr>
<td><strong>MySQL logs</strong></td>
<td>Collect and parse error and slow logs created by MySQL.</td>
</tr>
<tr>
<td><strong>Nats logs</strong></td>
<td>Collect and parse logs created by Nats.</td>
</tr>
<tr>
<td><strong>Nginx logs</strong></td>
<td>Collect and parse access and error logs created by the Nginx HTTP server.</td>
</tr>
<tr>
<td><strong>PostgreSQL logs</strong></td>
<td>Collect and parse error and slow logs created by PostgreSQL.</td>
</tr>
<tr>
<td><strong>Redis logs</strong></td>
<td>Collect and parse error and slow logs created by Redis.</td>
</tr>
<tr>
<td><strong>System logs</strong></td>
<td>Collect and parse logs written by the local Syslog server.</td>
</tr>
</tbody>
</table>
Detailed instructions
Context-aware instructions for cloud or on-prem installs

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

Getting Started
macOS DEB RPM

1. Download and install Filebeat
   First time using Filebeat? See the Getting Started Guide.
   ```bash
   curl -L -o https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-darwin-x86_64.tar.gz
tar xvf filebeat-7.5.0-darwin-x86_64.tar.gz
cd filebeat-7.5.0-darwin-x86_64/
   ```

2. Edit the configuration
   Modify `filebeat.yml` to set the connection information:
Getting Started

Cloud or on-prem installs

• Download and install Filebeat
• Edit the configuration
• Enable and configure the system module
• Start Filebeat
• Check out the dashboard!
Steps
Download and install Filebeat

$ >curl -LO --silent \\nhttps://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-darwin-x86_64.tar.gz

$ >tar xzvf filebeat-7.5.0-darwin-x86_64.tar.gz

$ >cd filebeat-7.5.0-darwin-x86_64

$ >ls -l
LICENSE.txt
NOTICE.txt
README.md
fields.yml
filebeat*
filebeat.reference.yml
filebeat.yml
kibana/
module/
modules.d/
Steps
Edit the configuration

• Download and install Filebeat
• Edit the configuration
• Enable and configure the system module
• Start Filebeat
• Check out the dashboard!
Configuration
Cloud aware - using superuser

Modify `filebeat.yml` to set the connection information for Elastic Cloud:

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

- `cloud.id` = "Sandbox:dXMyV2VudHJ..."
- `cloud.auth` = "elastic:<password>"

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

Copy the snippet, paste in the password

```yaml
#================================= Elastic Cloud ==================================
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.

cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "elastic:long-random-password" # because we are using Elastic Cloud

output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"] ← If we were not using Elastic Cloud
  #username: "elastic" ←
  #password: "long-random-password" ←
```

- UU-:----F1  `filebeat.yml`  (YAML)
Steps
Set up the system module

- Download and install Filebeat
- Edit the configuration
- **Enable and configure the system module**
- Start Filebeat
- Check out the dashboard!
Enable the system module

Again, just copy and paste the snippet

$ >./filebeat modules enable system
Enable the system module

Again, just copy and paste the snippet

```bash
$ ./filebeat modules enable system
Enabled system
```
Enable the system module

Check your work

$ >./filebeat modules enable system
Enabled system

# Can also verify
Enable the system module
Check your work

$ >./filebeat modules enable system
Enabled system

# Can also verify

$ >./filebeat modules list
Enable the system module
All good

$ >./filebeat modules enable system
Enabled system

# Can also verify

$ >./filebeat modules list
Enabled:
system

Disabled:
apache
auditd
aws
azure
(...)
Steps
Start Filebeat

• Download and install Filebeat
• Edit the configuration
• Enable and configure the system module
• Start Filebeat
• Check out the dashboard!
And start it up!

Startup steps

4 Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
./filebeat setup
./filebeat -e
```
First run the setup process

Setup preps dashboards and indices

$ >./filebeat setup
First run the setup process

Setup preps dashboards and indices

$ >./filebeat setup
Index setup finished.
First run the setup process
Setup preps dashboards and indices

$ >./filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
First run the setup process
Setup preps dashboards and indices

$ >./filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded Ingest pipelines
Finally, start it!

-e tells it to send messages to console

$ >./filebeat -e
Finally, start it!
-e tells it to send messages to console

$ >./filebeat -e

2019-12-09T18:02:42.500Z INFO instance/beat.go:610 Home path: /home/user/logs-demo/filebeat-7.5.0-linux-x86_64  Config path: /home/user/logs-demo/filebeat-7.5.0-linux-x86_64  Data path: /home/user/logs-demo/filebeat-7.5.0-linux-x86_64/data  Logs path: /home/user/logs-demo/filebeat-7.5.0-linux-x86_64/logs

2019-12-09T18:02:42.501Z INFO instance/beat.go:618 Beat ID: 04e276d0-79bd-40e3-9c83-3cdc4a64f791

2019-12-09T18:02:42.513Z INFO add_cloud_metadata/add_cloud_metadata.go:93 add_cloud_metadata: hosting provider type detected as gcp, metadata="availability_zone":"us-east1-b","instance":{"id":"8271592631829869565","name":"user-smith-build"},"machine":{"type":"n1-standard-8"},"project":{"id":"elastic-product-marketing"},"provider":"gcp"

2019-12-09T18:02:42.564Z INFO [seccomp] seccomp/seccomp.go:124 Syscall filter successfully installed

(....)
Essential needs for log analytics

Recall the earlier list

• Easy setup for a variety of sources
• Correlating and cross referencing
• Searching, filtering, and highlighting
• Visualize
• Anomaly detection and alerting
• Flexible retention
Needs for log analytics

Easy setup for variety of log sources
Needs for log analytics
Correlating and cross referencing

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>@timestamp</td>
<td>2020-01-14T13:37:08.838Z</td>
</tr>
<tr>
<td>_id</td>
<td>1xVFpGB8YbYXi60tEL1</td>
</tr>
<tr>
<td>_index</td>
<td>filebeat-7.5.1-2020.01.14-000048</td>
</tr>
<tr>
<td>agent.ephemeral_id</td>
<td>4b0464e0-cf97-498c-a2bb-61cdbaba36b6</td>
</tr>
<tr>
<td>agent.hostname</td>
<td>filebeat-6xktz</td>
</tr>
<tr>
<td>agent.id</td>
<td>520ddfa4-1182-44c9-b919-2f344cd00ca5</td>
</tr>
<tr>
<td>agent.type</td>
<td>filebeat</td>
</tr>
<tr>
<td>agent.version</td>
<td>7.5.1</td>
</tr>
<tr>
<td>cloud.availability_zone</td>
<td>us-central1-a</td>
</tr>
<tr>
<td>cloud.instance.id</td>
<td>25672863551-04662140</td>
</tr>
<tr>
<td>cloud.instance.name</td>
<td>gke-eden-prod-default-pool-ef9bba0b-5bpx</td>
</tr>
<tr>
<td>cloud.machine.type</td>
<td>n1-standard-8</td>
</tr>
<tr>
<td>cloud.project.id</td>
<td>elastic-product</td>
</tr>
<tr>
<td>cloud.provider</td>
<td>gcp</td>
</tr>
<tr>
<td>container.id</td>
<td>fba2b833ce0b9d39f95b77f65e0cf43ac8001e6eacaeae45ee3742</td>
</tr>
</tbody>
</table>
# Needs for log analytics

## Searching, filtering, and highlighting

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Message</th>
<th>kubernetes.container.name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 14, 2020 @ 16:37:08.790</td>
<td>[INFO] received ad request (context.words=[Cookware])</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.790</td>
<td>[INFO] Cache miss for category: Cookware</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.792</td>
<td>[redis.log][verbose] Accepted 19.48.4.11:36768</td>
<td>redis-master</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.800</td>
<td>[redis.log][verbose] Client closed connection</td>
<td>redis-master</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.811</td>
<td>[INFO] Adding 2 items to cache</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.811</td>
<td>[INFO] Items 9801 now in cache</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.811</td>
<td>[INFO] Returning 2 ads</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.820</td>
<td>[INFO] received conversion request</td>
<td>currency-service</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.823</td>
<td>[INFO] conversion request successful</td>
<td>currency-service</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.832</td>
<td>[INFO] Getting supported currencies...</td>
<td>currency-service</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.836</td>
<td>[DEBUG] request complete</td>
<td>frontend</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.838</td>
<td>[INFO] Adding 1 items to cache</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.838</td>
<td>[INFO] Items 9802 now in cache</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.838</td>
<td>[INFO] Returning 1 ads</td>
<td>adservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.844</td>
<td>[DEBUG] request complete</td>
<td>frontend</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.938</td>
<td>[DEBUG] request started</td>
<td>frontend</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.946</td>
<td>[DEBUG] view user cart</td>
<td>frontend</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:08.948</td>
<td>[INFO] GetCartAsync called with userId=&quot;59aee2be-5279-4a9f-86d8-a4d733b47bcb1&quot;</td>
<td>cartservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:09.280</td>
<td>[INFO] received conversion request</td>
<td>currency-service</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:09.364</td>
<td>[INFO] conversion request successful</td>
<td>currency-service</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:09.390</td>
<td>[INFO] Getting supported currencies...</td>
<td>currency-service</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:09.394</td>
<td>[INFO] listing products</td>
<td>productetaillogservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:09.452</td>
<td>[INFO] [Rec] ListRecommendations product_ids=&quot;16922MYYFZ&quot;, &quot;8PK6V6W0&quot;, &quot;ZFYJ3G4MN&quot;, &quot;9SO8TO0J&quot;, &quot;DLJC8EPC7&quot;]</td>
<td>recommendationservice</td>
</tr>
<tr>
<td>Jan 14, 2020 @ 16:37:09.520</td>
<td>[INFO] Getting product with ID 6E922MYYFZ</td>
<td>productetaillogservice</td>
</tr>
</tbody>
</table>
Needs for log analytics

Visualize
Needs for log analytics

Visualize
Needs for log analytics

Visualize
Anomaly detection and alerting
Can't stare at the screen all day
Needs for log analytics

Flexible retention
Needs for log analytics

Anomaly detection and alerting
Essential needs for log analytics

From the earlier list

✓ Easy setup for a variety of sources
✓ Correlating and cross referencing
✓ Searching, filtering, and highlighting
✓ Visualize
✓ Anomaly detection and alerting
✓ Flexible retention
Agenda

Beyond logging: Observability

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security
Many integrations
For example, system metrics

System metrics
Collect CPU, memory, network, and disk statistics from the host.
Metrics

Visualizing metrics
Metrics

Inventory view with multiple perspectives
Integrated Experience

Observability with one datastore
Setting up APM
Instructions in Kibana

APM
APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Observability
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

Visualize and Explore Data
APM
Automatically collect in-depth performance metrics

Canvas
Showcase your data in a visual, perfect way

Manage and Administer the Elastic Stack
Console
Skip cURL and use this JSON interface to work

Index Patterns
Manage the index patterns that help optimize your
Application Performance Monitoring

Distributed Tracing

Transactions duration distribution

Trace sample

3 minutes ago 2,613 ms (100.0% of trace) Safari (5.0)

Timeline Metadata

Services

placeOrderHandler 2,613 ms
PlaceOrderRequest 1,872 ms

/hipstershop/CheckoutService/PlaceOrder 1,871 ms

OK /hipstershop/CheckoutService/PlaceOrder 1,785 ms

prepareOrderItemsAndShippingQuoteFromCart 1,428 ms

getUserCart 259 ms
Uptime Monitoring

Service availability

Overview

1/22 monitors are down

Monitor status

- **Up**
  - 8 minutes ago
  - adservice-7bcd956677-7ftmb
    - URL: tcp://10.48.6.48:10000
  - a few seconds ago
  - unnamed-auto-http-0X4FA94B0D313EE0BC4-c7eca219068B820
    - URL: https://www.bbc.com
  - a few seconds ago
  - unnamed-auto-http-0X4FA94B0D313EE0BC4-debdf0c562e9997
    - URL: https://demo.elastic.co/status
  - a few seconds ago
  - unnamed-auto-http-0X4FA94B0D313EE0BC4-f2bd09f715add916
    - URL: https://www.elastic.co

- **Down**
  - a few seconds ago
  - apm-server-969d845bc-sjc2d
    - URL: http://10.48.3.115:8200
  - a few seconds ago
  - unnamed-auto-http-0X4FA94B0D313EE0BC4-c7eca219068B820
## Uptime Monitoring

### Service availability

7/33 monitors are down

### Monitor status

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>URL</th>
<th>Downtime History</th>
<th>Integrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Unnamed - auto-http-0X14D5C52E77FA69FF</td>
<td><a href="https://www.elastic.co/">https://www.elastic.co/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>Unnamed - auto-http-0X1BEDFCSAB874F394</td>
<td><a href="http://192.168.64.11:3000">http://192.168.64.11:3000</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Down</td>
<td>Website Monitor - Infra Error</td>
<td><a href="https://www.elastic.co/products/infrastructure-monitoring">https://www.elastic.co/products/infrastructure-monitoring</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>NodeJS</td>
<td><a href="http://opbeans-node:3000/api/customers">http://opbeans-node:3000/api/customers</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>NodeJS</td>
<td><a href="http://opbeans-node:3000/api/stats">http://opbeans-node:3000/api/stats</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>NodeJS</td>
<td><a href="http://opbeans-node:3000/api/orders">http://opbeans-node:3000/api/orders</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Down</td>
<td>SecurityContents</td>
<td><a href="https://www.elastic.co/products/siem">https://www.elastic.co/products/siem</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Uptime Monitoring

**Integrated experience**

#### Monitor status

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>URL</th>
<th>Downtime History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up a few seconds ago</td>
<td>Unnamed - auto-http-0X14D5CS2E77F4E9FF</td>
<td><a href="https://www.elastic.co/">https://www.elastic.co/</a></td>
<td></td>
</tr>
<tr>
<td>Up a few seconds ago</td>
<td>Unnamed - auto-http-0X1BEDFCSAB57F394</td>
<td><a href="http://192.168.64.11:3000">http://192.168.64.11:3000</a></td>
<td></td>
</tr>
<tr>
<td>Down a few seconds ago</td>
<td>Website Monitor - Infra Error</td>
<td><a href="https://www.elastic.co/products/infrastructure-monitoring">https://www.elastic.co/products/infrastructure-monitoring</a></td>
<td></td>
</tr>
<tr>
<td>Up a few seconds ago</td>
<td>NodeJS</td>
<td><a href="http://opbeans-node:3000/api/customers">http://opbeans-node:3000/api/customers</a></td>
<td></td>
</tr>
<tr>
<td>Up a few seconds ago</td>
<td>NodeJS</td>
<td><a href="http://opbeans-node:3000/api/stats">http://opbeans-node:3000/api/stats</a></td>
<td></td>
</tr>
<tr>
<td>Up a few seconds ago</td>
<td>NodeJS</td>
<td><a href="http://opbeans-node:3000/api/orders">http://opbeans-node:3000/api/orders</a></td>
<td></td>
</tr>
<tr>
<td>Down a few seconds ago</td>
<td>SecurityContents</td>
<td><a href="https://www.elastic.co/products/isen">https://www.elastic.co/products/isen</a></td>
<td></td>
</tr>
</tbody>
</table>
Integrated Experience
Observability with one datastore
Agenda

Securing your Beats

1. Challenges with log analytics
2. Sending logs to Elasticsearch
3. Beyond logging: Observability
4. Leveraging Elastic security
Recall the Filebeat steps
Use parameterized credentials

• Download and install Filebeat
• Edit the configuration
• Enable and configure the system module
• Start Filebeat
beats_writer Role
Required permissions

• Cluster Permissions:
  – monitor
  – read_ilm
  – manage_indexTemplates
  – manage_pipeline
• Index Privileges (*beat-*):
  – create_index
  – index
  – view_index_metadata

Corresponding User
Tying roles to users

• Give the user the corresponding roles
• Create a secure password
• beats-writer gets the writer role we created, plus the shipped beats_system role

Set up the keystore
Hiding credentials for beats-writer

Usage:
  filebeat keystore [command]

Available Commands:
  add      Add secret
  create   Create keystore
  list     List keystore
  remove   Remove secret

• Command: filebeat keystore
• Create the keystore
• filebeat keystore add:
  – BEATS_WRITER_USER
  – BEATS_WRITER_PASSWORD
• Access keys via ${KEY_NAME}
Previous Configuration
Had the user & password hardcoded

# elastic-cloud

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The `cloud.id` setting overwrites the `output.elasticsearch.hosts` and `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.

cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "elastic:long-random-password" # because we are using Elastic Cloud

-UU-:----F1 filebeat.yml (YAML)
Parameterize the user
Had the user & password hardcoded

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.

```
cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "${BEATS_WRITER_USER}:long-random-password"  # because we are using Elastic Cloud
```
And the password

No more plain text!

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.

cloud.id: "Sandbox:dXMtY2VudHJ..."
cloud.auth: "${BEATS_WRITER_USER}:${BEATS_WRITER_PASSWORD}"  # because we are using Elastic Cloud
Starts the same way
Automatically picks up the keystore

$ >./filebeat -e
Finally, start it!
assumes that you've run setup

$ >./filebeat -e

2019-12-09T18:02:42.500Z INFO instance/beat.go:610 Home path: [/home/user/logs-demo/filebeat-7.5.0-linux-x86_64] Config path: [/home/user/logs-demo/filebeat-7.5.0-linux-x86_64] Data path: [/home/user/logs-demo/filebeat-7.5.0-linux-x86_64/data] Logs path: [/home/user/logs-demo/filebeat-7.5.0-linux-x86_64/logs]

2019-12-09T18:02:42.501Z INFO instance/beat.go:618 Beat ID: 04e276d0-79bd-40e3-9c83-3cdc4a64f791

2019-12-09T18:02:42.513Z INFO add_cloud_metadata/add_cloud_metadata.go:93 add_cloud_metadata: hosting provider type detected as gcp, metadata={"availability_zone":"us-east1-b","instance":{"id":"8271592631829869565","name":"user-smith-build"},"machine":{"type":"n1-standard-8"},"project":{"id":"elastic-product-marketing"},"provider":"gcp"}

2019-12-09T18:02:42.564Z INFO [seccomp] seccomp/seccomp.go:124 Syscall filter successfully installed (...)
Continuing your Journey
Where to find more information

• Spin up a cluster
  – Hosted: cloud.elastic.co
  – Self managed - elastic.co/downloads
• Explore live examples @ elastic.co/demos
• Watch webinars @ elastic.co/videos
• Chat with us @ Forums: https://discuss.elastic.co/
• Go deeper with documentation @ elastic.co/guide
• Sign up for training @ elastic.co/training
• Attend a local meetup or Elastic{ON}