Alerting with Watcher

JP Toto
INFRASTRUCTURE DEVELOPER

@jptoto http://jptoto.jp

Alerting with Watcher

Watcher

Security

Monitoring

Graph

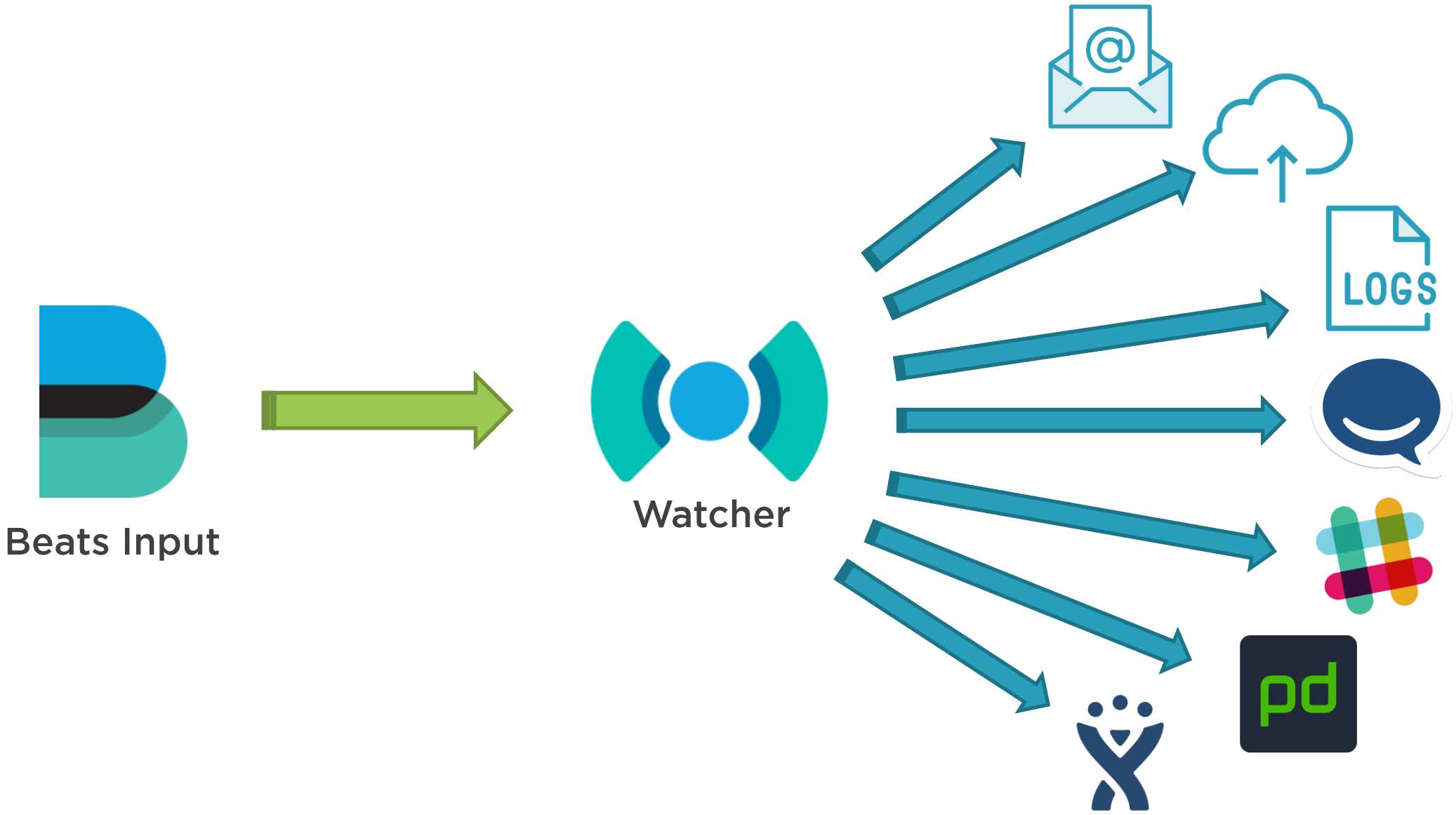
Reporting

Alerting

* Not free, commercial plugin

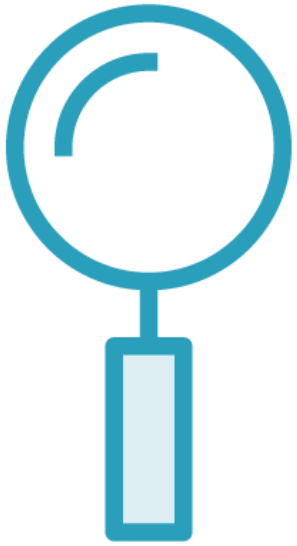
Free 30 day trial

Watcher is a Plugin for Elasticsearch

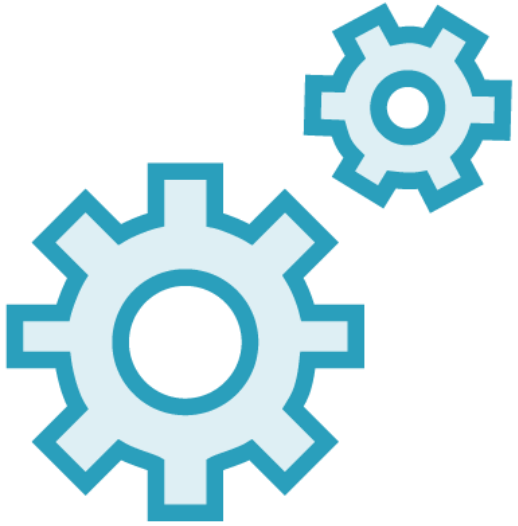


Watcher Workflow

Schedule / Trigger



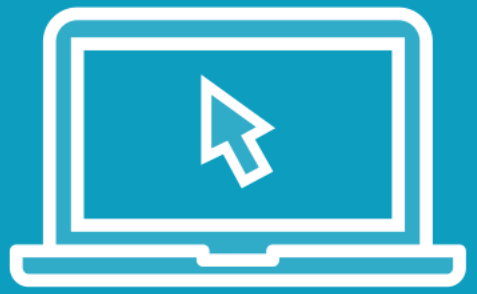
Input / Query



Condition

Action

Demo

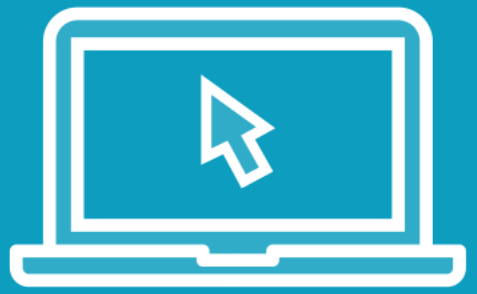


Install X-Pack onto Elasticsearch

X-Pack must be installed on each Elasticsearch Node

Configure SMTP settings

Demo



Setup a Watch inside Elasticsearch using Postman

Scan winlogbeat indices for Windows Eventlog Errors

Summary

Setup a basic query Watch for winlogbeat errors

Added an email alert

Course Summary

Congratulations, we're done!

https://www.elastic.co/guide/index.html

Always keep Elastic Stack versions in sync

https://www.pluralsight.com/courses/administering-elasticsearch-cluster

Good luck!

Contact me by email or @jptoto