Elasticsearch Best Practice Architecture

The webinar will start soon...
whoami

Eric Westberg
Solutions Architect
Stockholm, Sweden
Joined Elastic last year
Webinar Housekeeping & Logistics

• **Slides and recording** will be available following the webinar
• Please ask questions via “Q&A”
Inside an Elasticsearch Cluster
Elasticsearch Node Types

Nodes can play one or more roles, for workload isolation and scaling

- **Master Nodes**
  - Control the cluster, requires a minimum of 3, one is active at any given time
- **Data Nodes**
  - Hold indexed data and perform data related operations
  - Differentiated Hot and Warm Data nodes can be used
- **Ingest Nodes**
  - Use ingest pipelines to transform and enrich before indexing
- **Coordinating Nodes**
  - Route requests, handle search reduce phase, distribute bulk indexing
  - All nodes function as coordinating nodes
- **Alerting Nodes**
  - Run alerting jobs
- **Machine Learning Nodes**
  - Run machine learning jobs
Split Brain

- Cluster with 3 master eligible nodes
- Concern if network becomes partitioned
- The cluster would inadvertently elect two masters, which is referred to “split brain”
Avoiding Split Brain

- A master eligible node needs at least minimum_master_nodes votes to win an election
  - Setting it to a quorum prevents the split brain scenario
- Recommendation for production clusters is to have 3 dedicated master eligible nodes
  - with the setting `minimum_master_nodes = 2`
Inside a Large Elasticsearch Logging Cluster

Reduce infrastructure costs, isolate workloads, and manage data lifecycle
Logging Architectures
Quick Start

Beats, Elasticsearch and Kibana

- Beats
  - FILEBEAT
  - WINLOGBEAT
  - HEARTBEAT
  - METRICBEAT
  - PACKETBEAT
  - AUDITBEAT
  - File Spool Queue

- Elasticsearch
  - Uniform Nodes (3+)

- Kibana
Advanced Processing and Resiliency

Adding Logstash processing, differentiated Elasticsearch node types

Beats
- FILEBEAT
- WINLOGBEAT
- HEARTBEAT
- METRICBEAT
- PACKETBEAT
- AUDITBEAT

Logstash
- Workers (1+)
- Persistent Queues

Elasticsearch
- Master Nodes (3)
- Data Nodes (2+)
- ML Nodes (2+)

Kibana

File Spool Queue
Flexible ingestion and input sources

Beats
- FILEBEAT
- WINGLOGBEAT
- HEARTBEAT
- METRICBEAT
- PACKETBEAT
- AUDITBEAT

Data store
- Kafka
- Redis

Web APIs
- Messaging Queue

Social

Sensors

Elasticsearch
- Master (3)
- Ingest (X)
- Coordinating (X)
- Data – Hot (X)
- Data – Warm (X)
- Alerting (X)
- Machine Learning (2+)

Kibana

All product names, logos, and brands are property of their respective owners and are used only for identification purposes. This is not an endorsement.
Application Metric Collection with Elastic APM

Beats

Logstash

Elasticsearch

Kibana

apm-agents

apm-server

Real User Monitoring (RUM)

Datastore

JMX

NodeJS

Python
Deployment Best Practices
Centralized Monitoring Cluster

Maintain isolated monitoring cluster for monitoring workload isolation
Cloud Monitoring Cluster

Opt-in Elastic Cloud cluster for monitoring on-premise stack
Isolated Audit Logging Cluster

Maintain isolated audit logging cluster for increased security and compliance
Multi Data Center
Multiple Data Centers, Duplicate Data

Kafka
Redis
Messaging Queue

Replication

Logstash
Elasticsearch
Kibana

ACTIVE

Logstash
Elasticsearch
Kibana

ACTIVE

Load Balancer

Kafka
Redis
Messaging Queue

All product names, logos, and brands are property of their respective owners and are used only for identification purposes. This is not an endorsement.
Multi Data Centers with a Queue at Each DC

DC1
- Beats
- Datastore
- Web APIs
- Logstash
- Kafka
- Messaging Queue
- Logstash
- Elasticsearch

DC2
- Beats
- Datastore
- Web APIs
- Logstash
- Kafka
- Messaging Queue
- Logstash
- Elasticsearch
Multi Data Center, Distinct Data and Cross-Cluster Search
Scaling Kibana
High Availability

Pair two coordinating nodes with two independent Kibana nodes
Separating Dashboards by Groups

Isolate user content by group in different Kibana instances
Questions?
Thank You

- **Web**: www.elastic.co
- **Products**: https://www.elastic.co/products
- **Forums**: https://discuss.elastic.co/
- **Community**: https://www.elastic.co/community/meetups
- **Twitter**: @elastic
- **Contact us**: www.elastic.co/contact