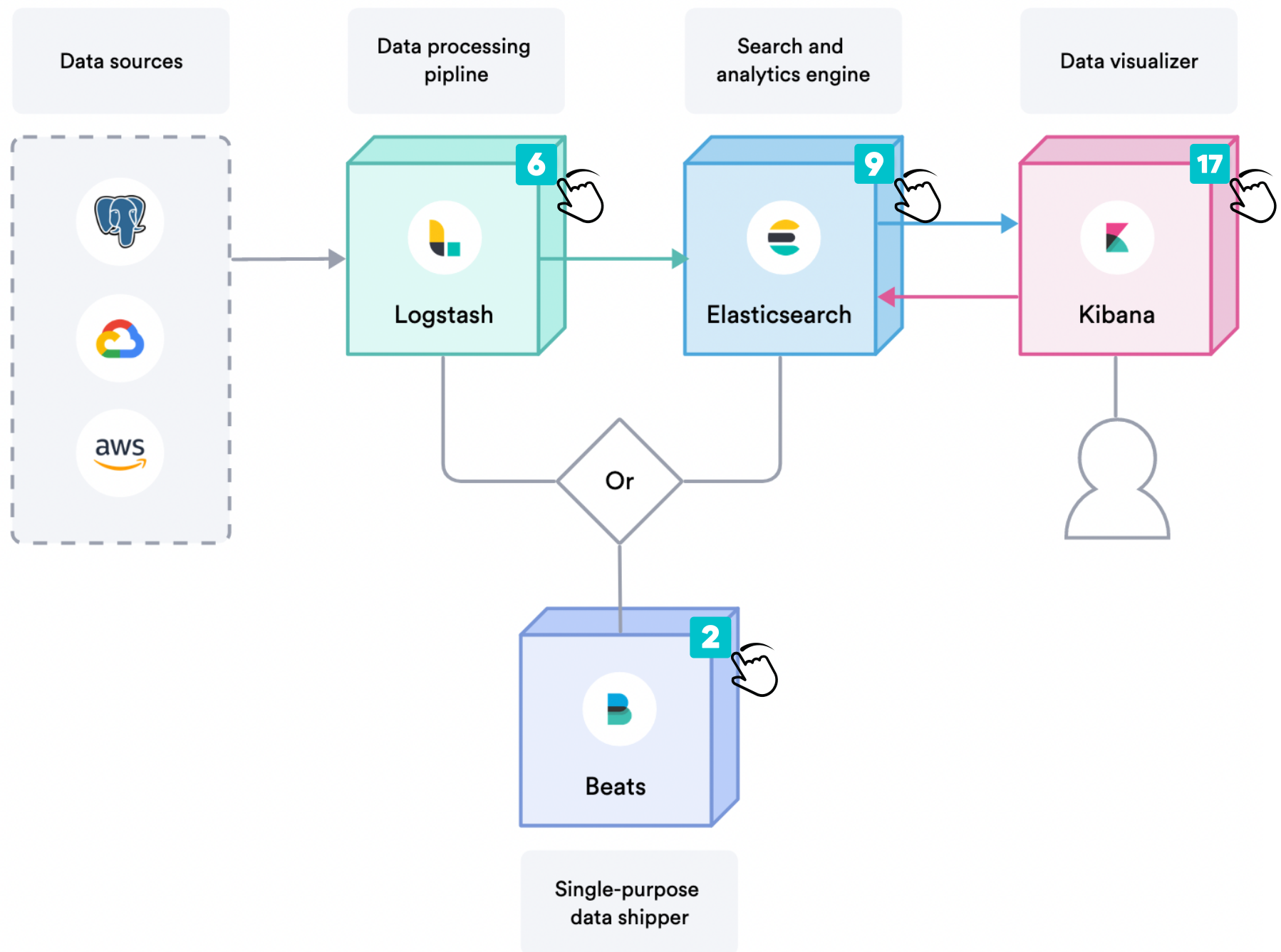


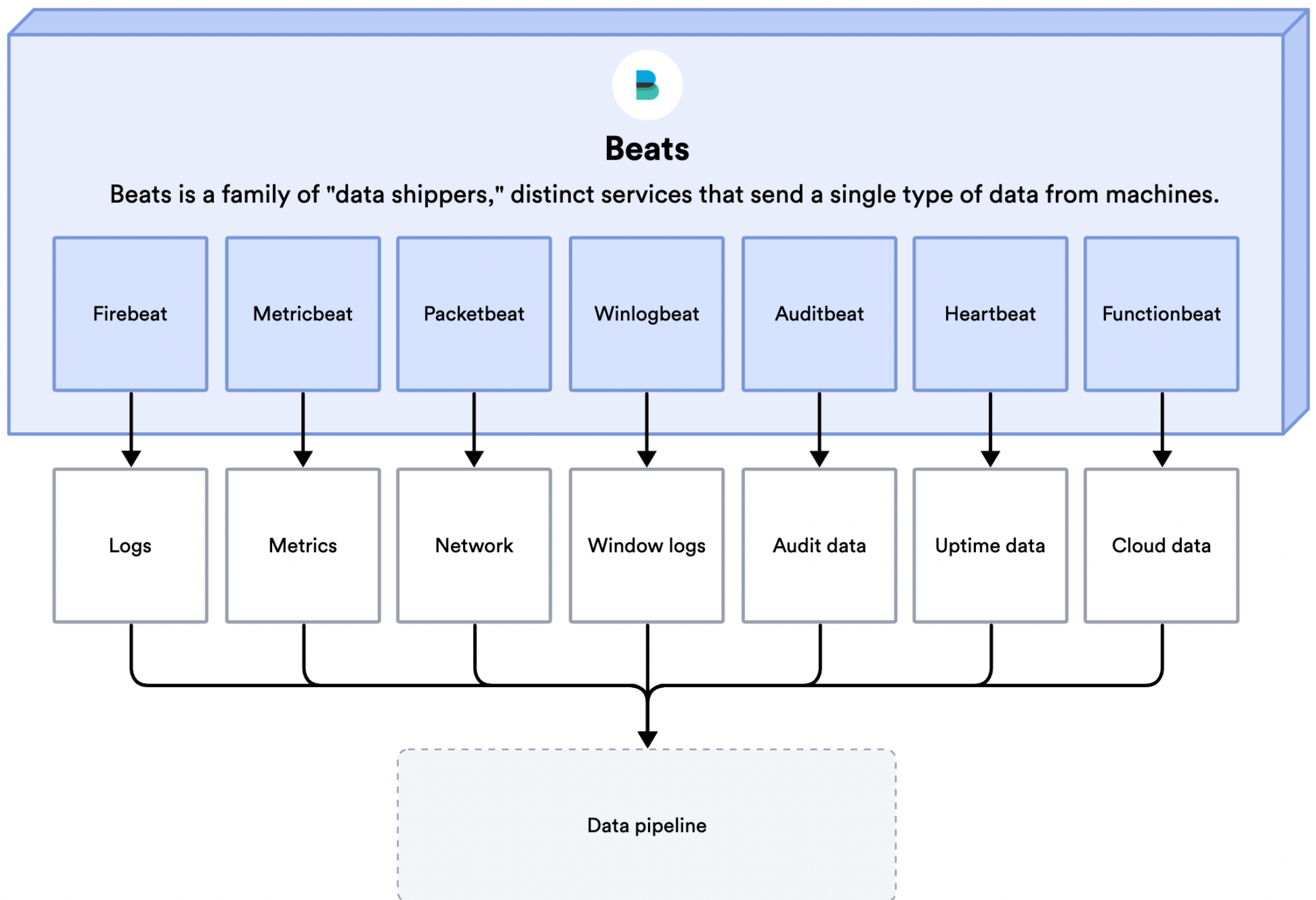


# Elastic Stack (ELK) Architecture



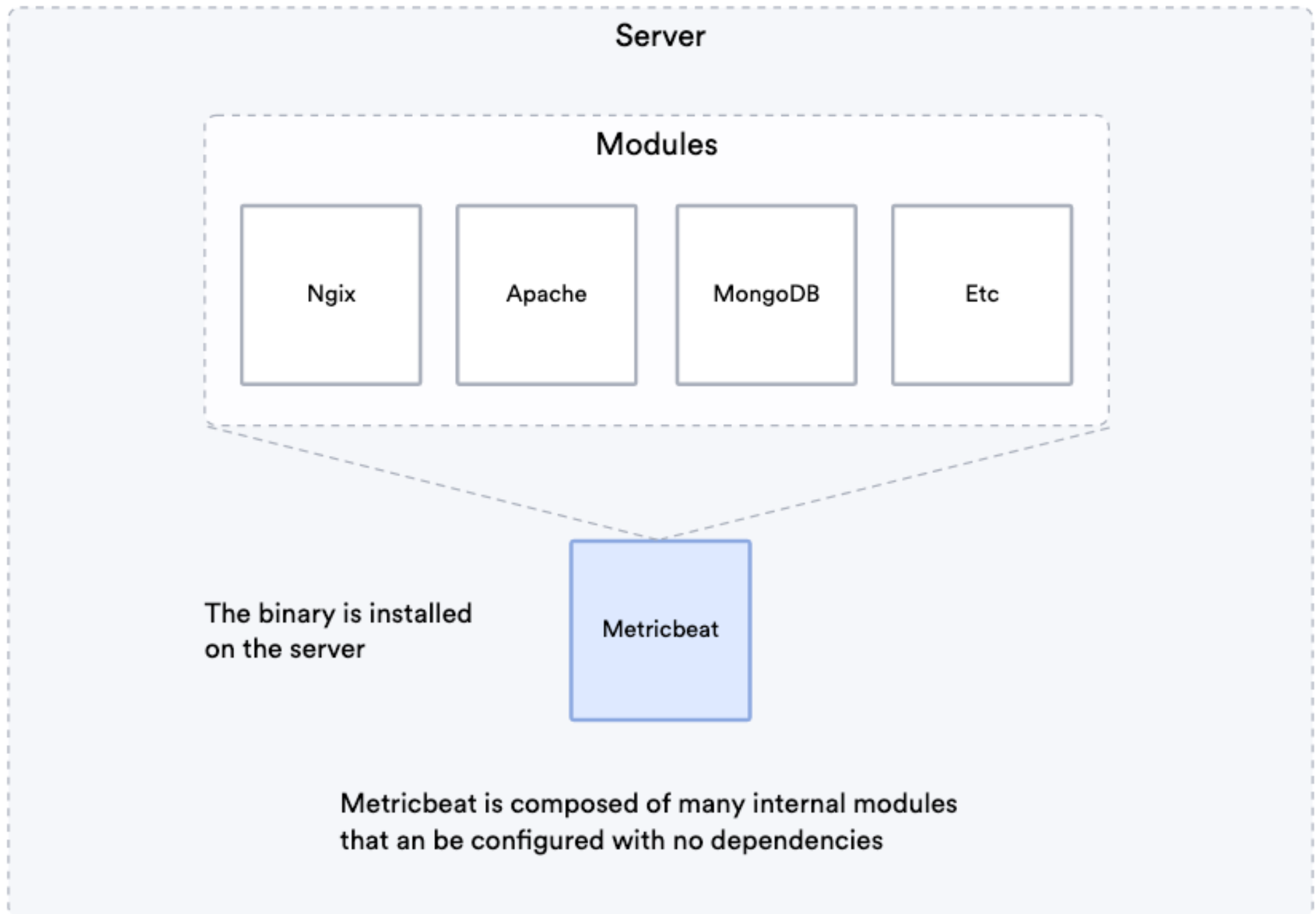
Premium Programming Courses  
[amigoscode.com](https://amigoscode.com)

# What are Beats?



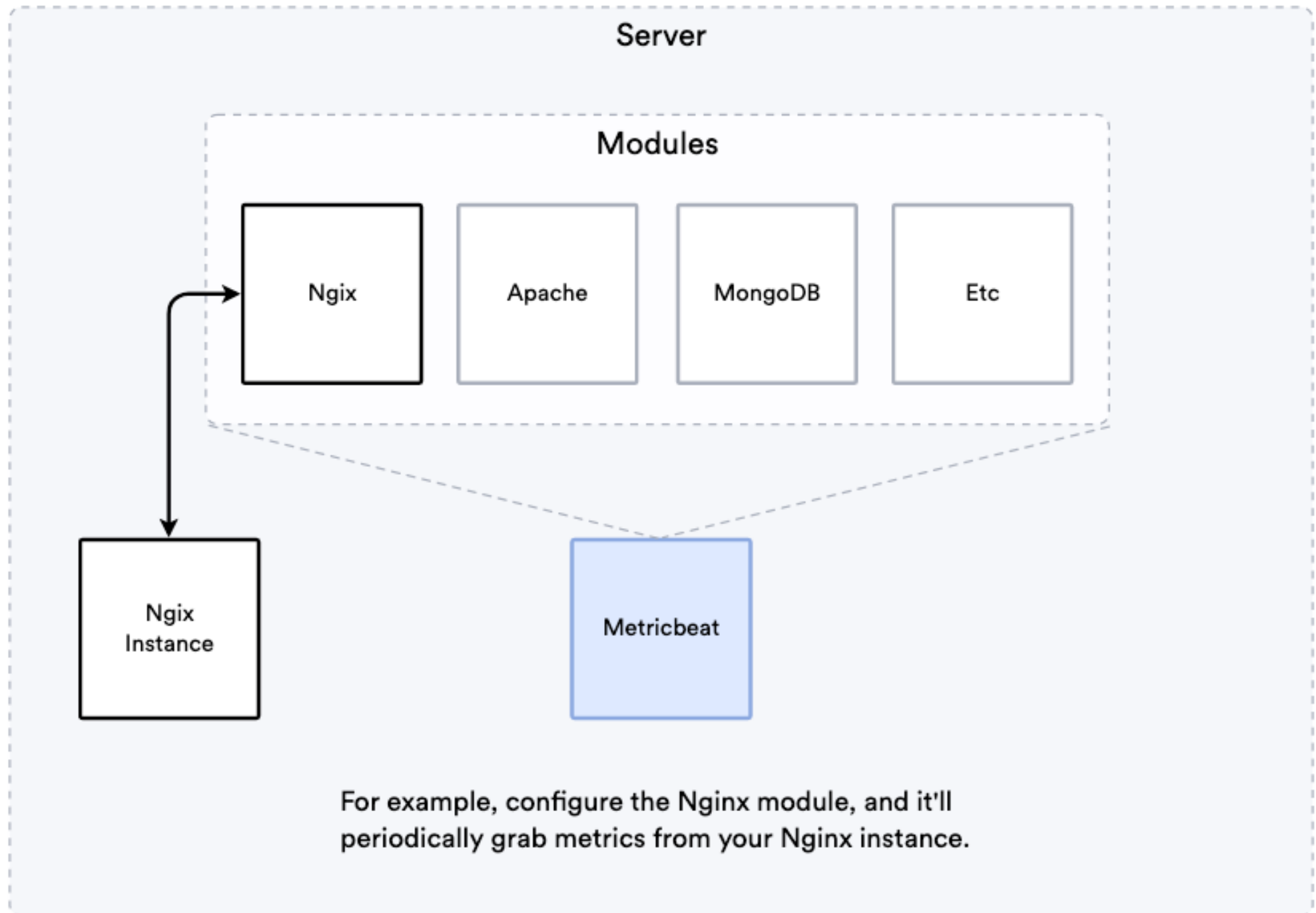


## Beats



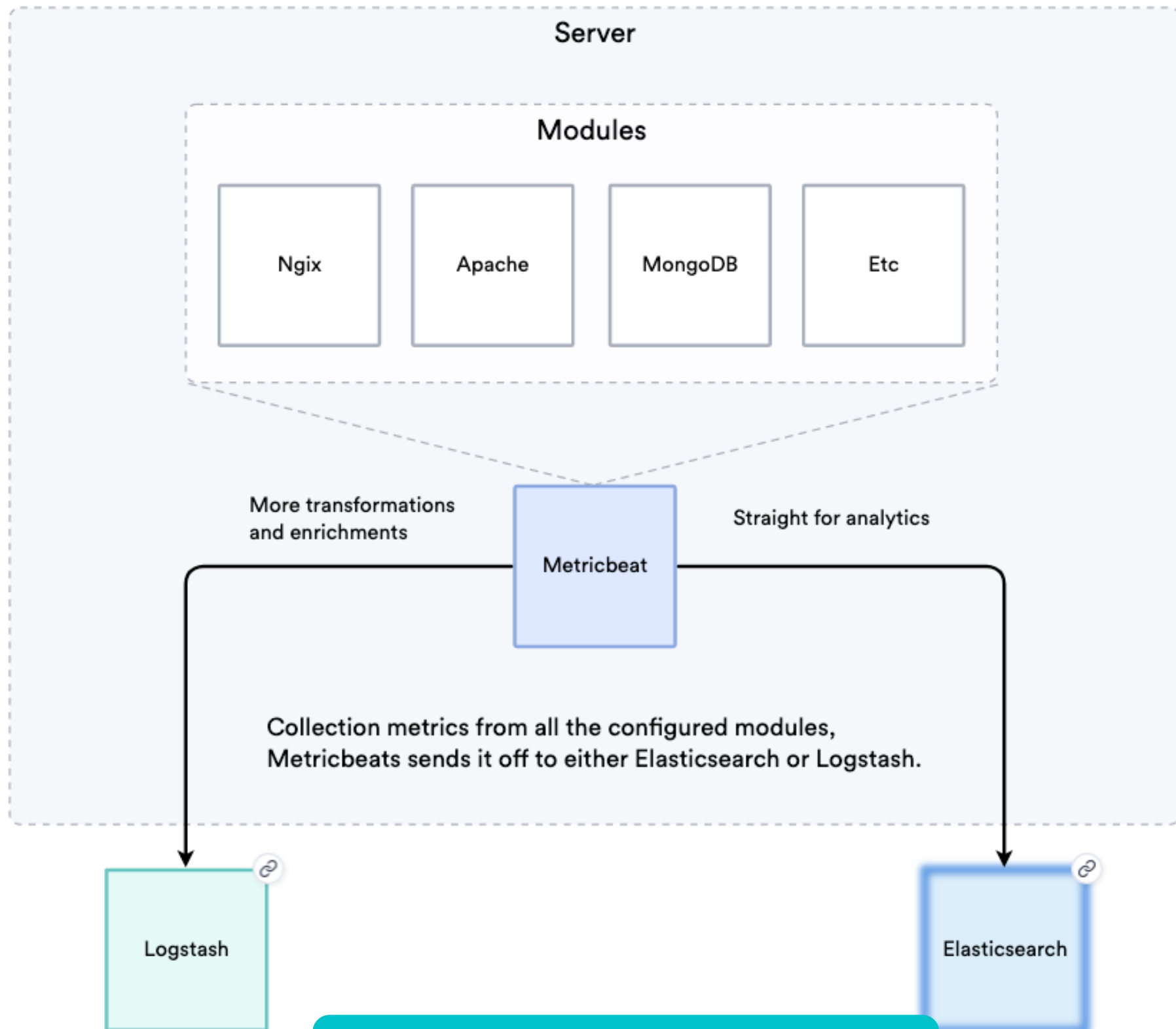


## Beats

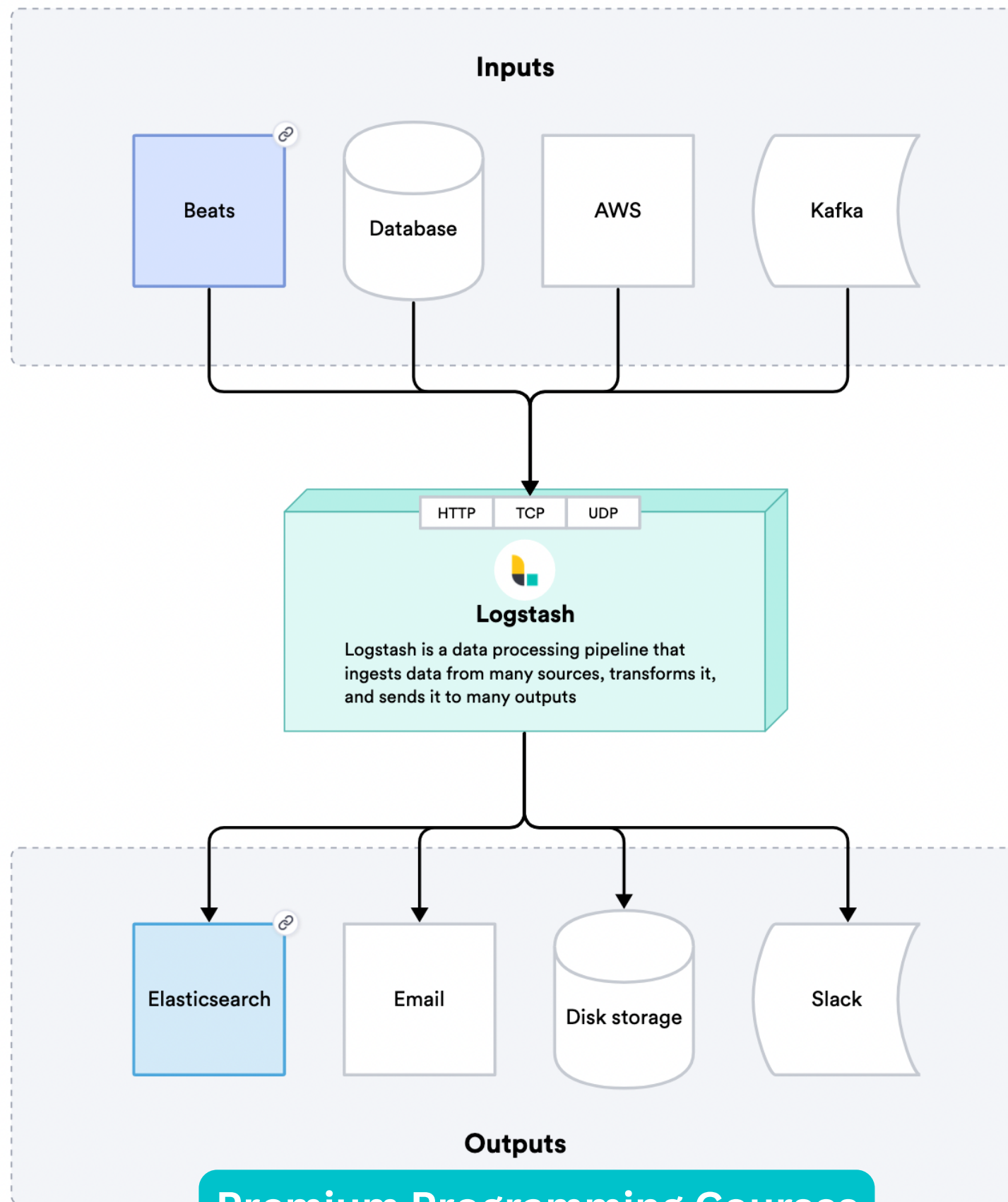




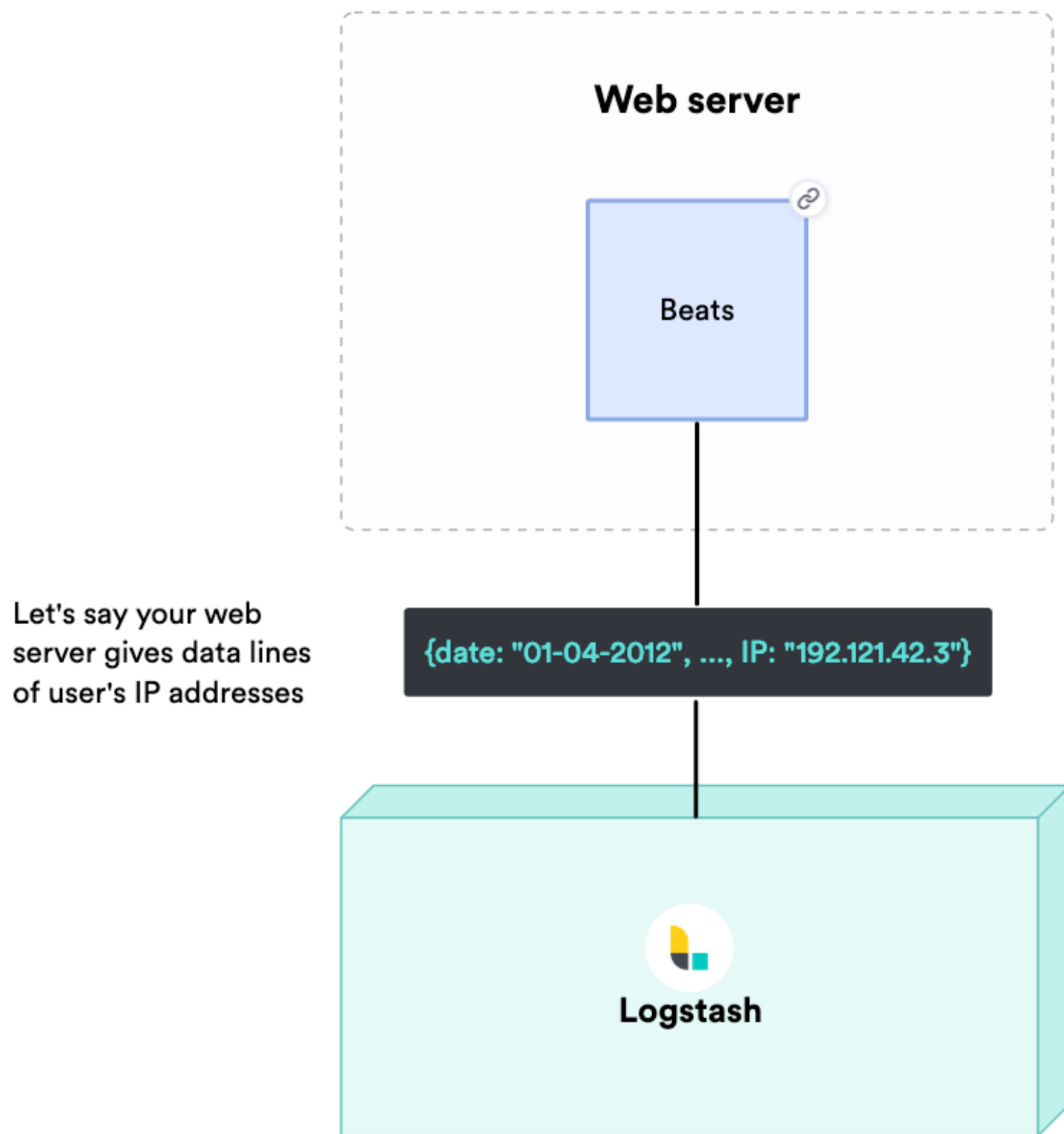
## Beats



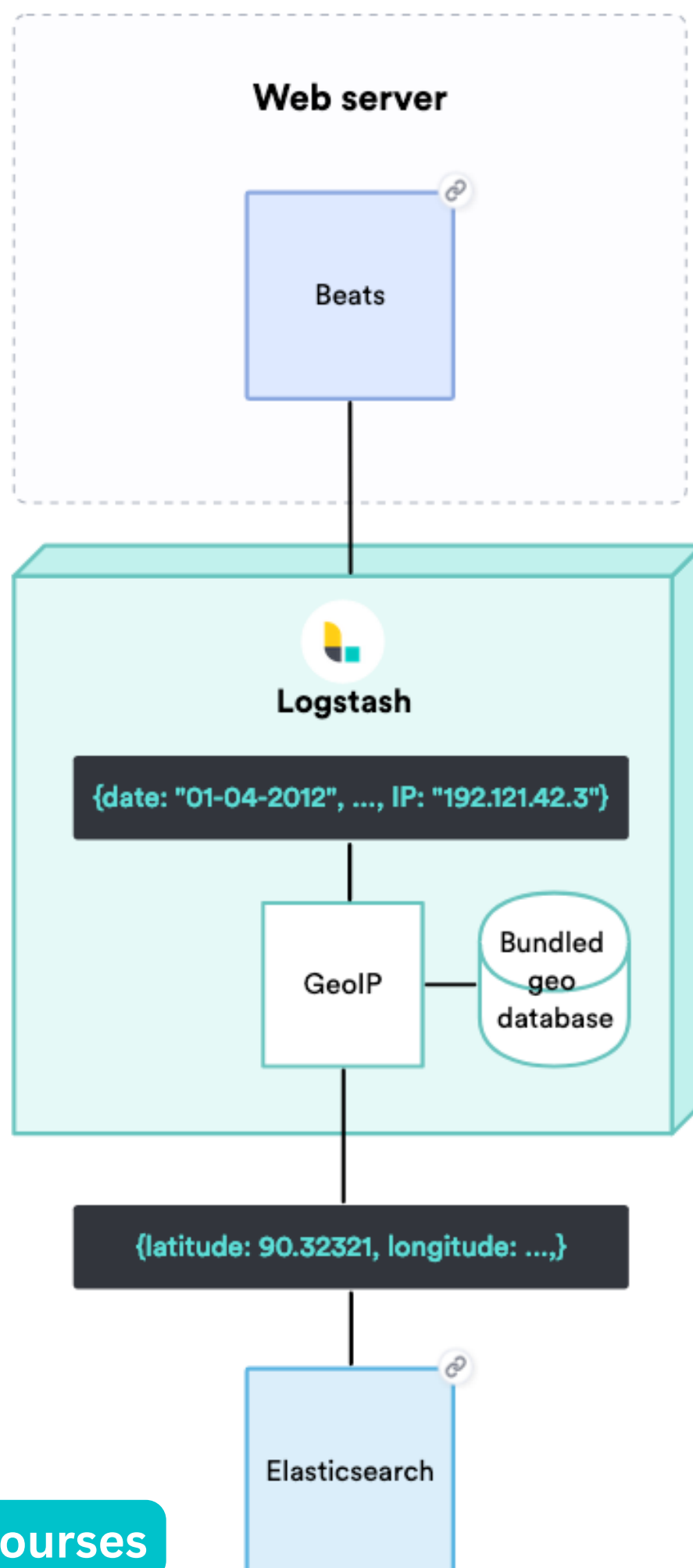
# What's Logstash?



Premium Programming Courses  
[amigoscode.com](https://amigoscode.com)



GeoIP is one of many filter plugins that help transform data in a specialized way. GeoIP takes an IP address and looks up a lat, long pair.





Data sources



## Elasticsearch

Elasticsearch is the heart of the Elastic Stack, and it's responsible for storing, querying, and analyzing data.

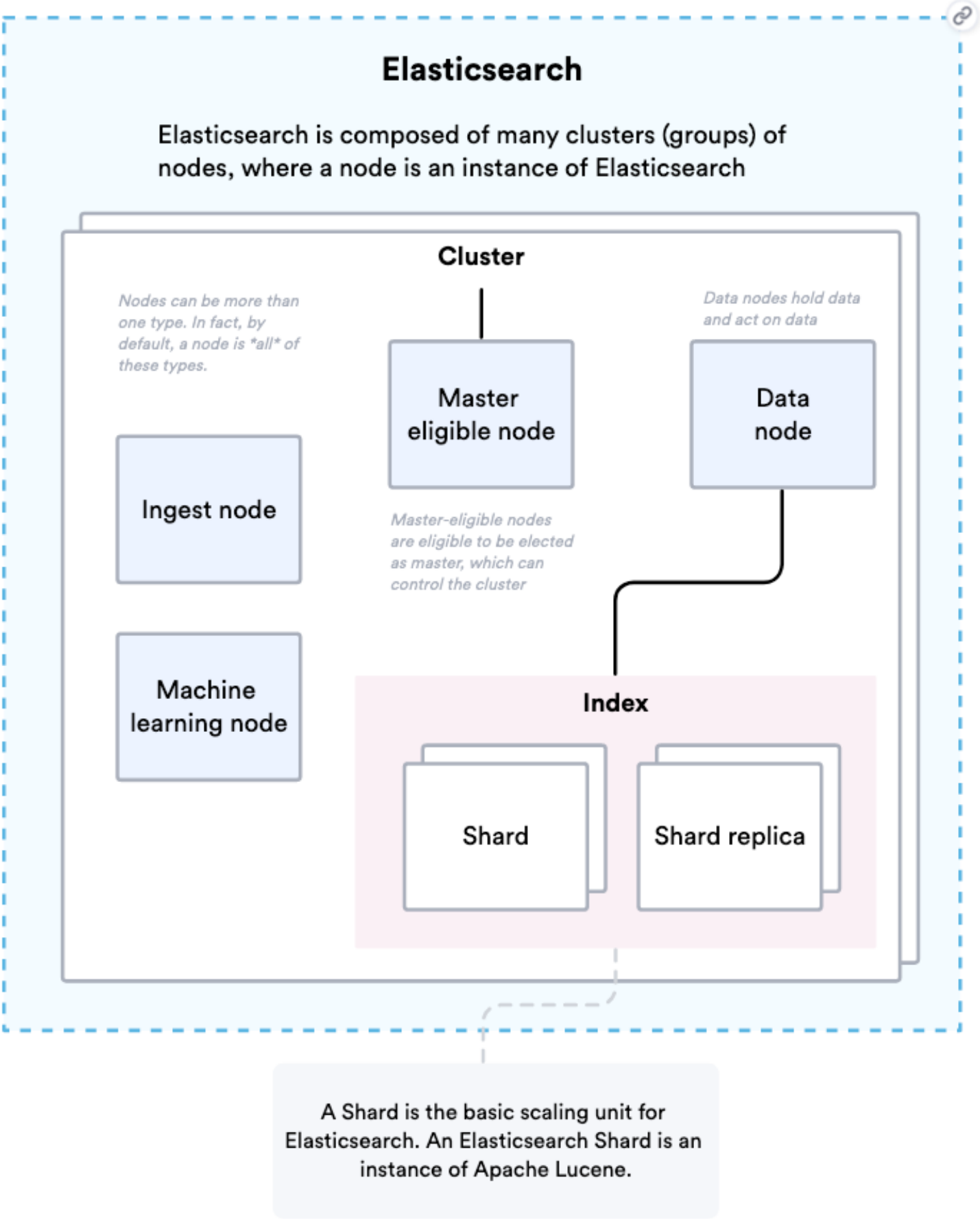
Queries

Answers

Data cluster

*The horizontal scaling of data nodes  
is what makes Elasticsearch "elastic"*

Premium Programming Courses  
[amigoscode.com](https://amigoscode.com)

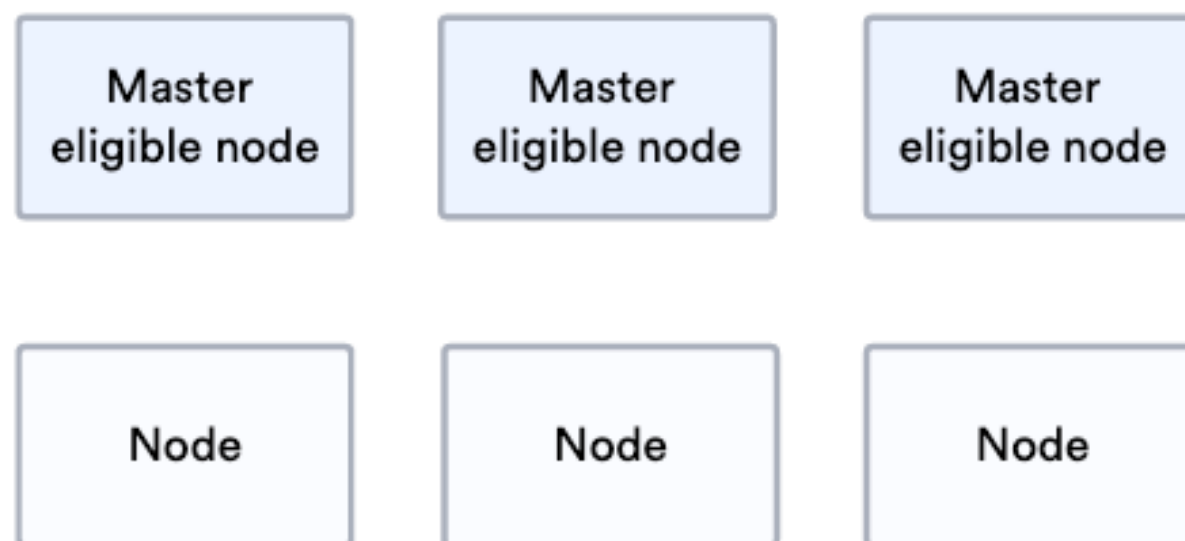




## Elasticsearch

When a node is started or when a node is without a master node, it begins "discovery"

### Clusterless nodes



"Where are the seed nodes?"

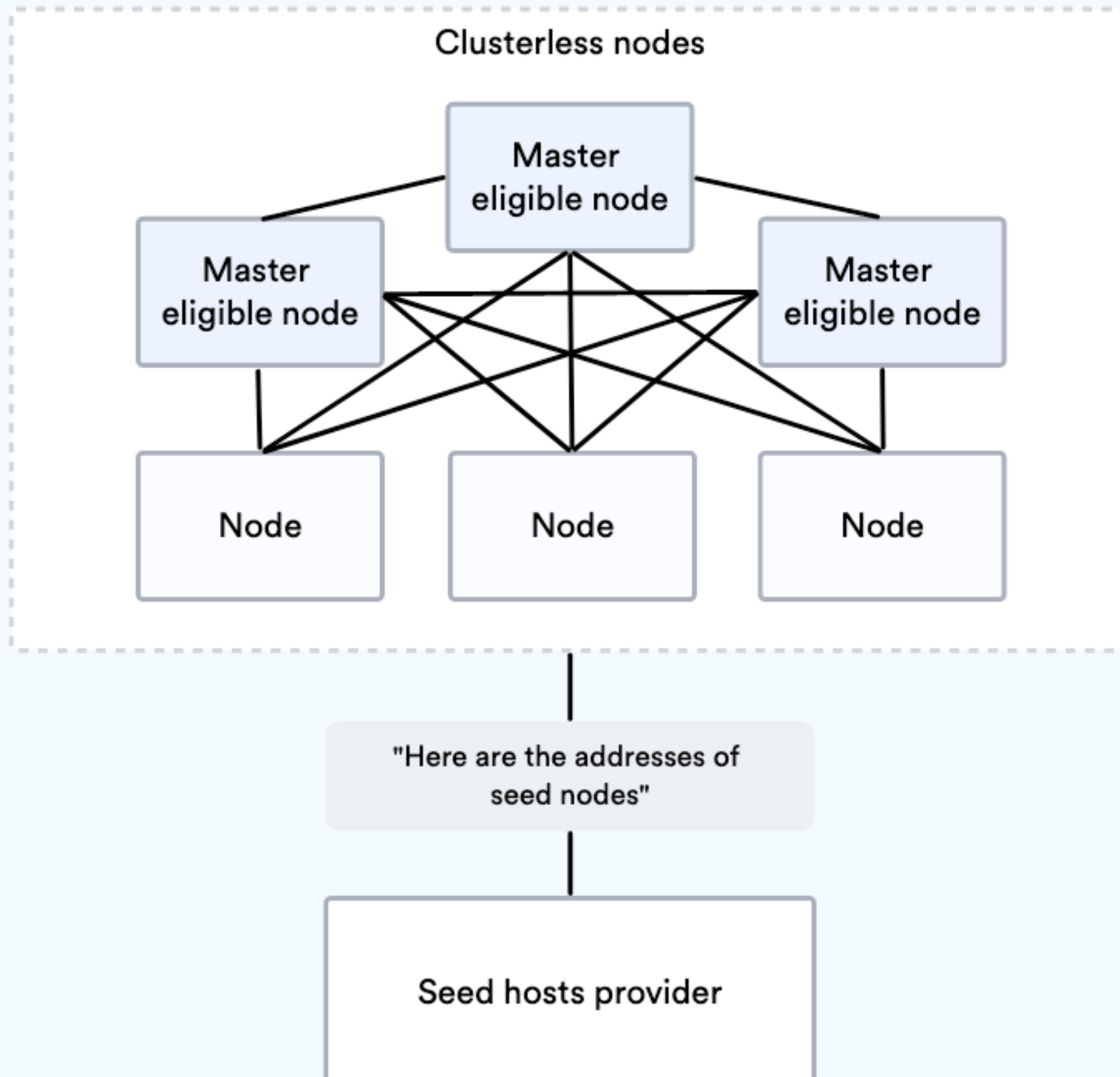
Pre-configured list  
of IP addresses or  
hostnames of  
seed nodes

Seed hosts provider



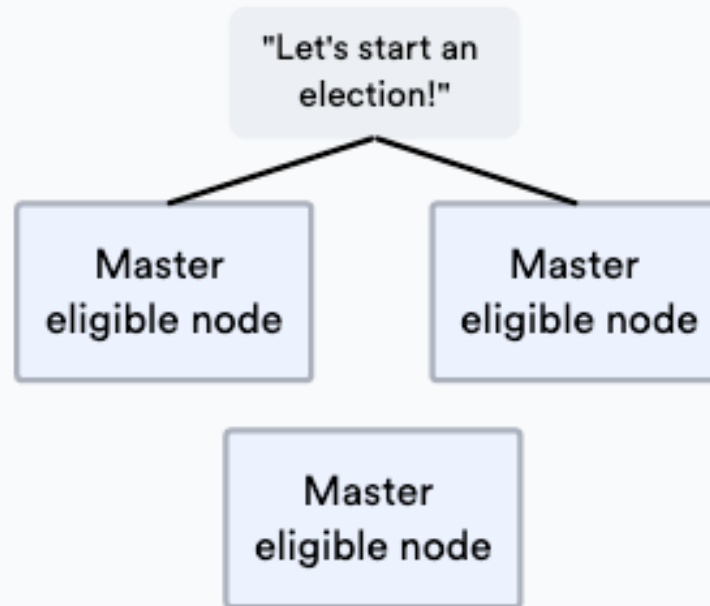
## Elasticsearch

Every node connects to every seed node, and bidirectionally share other nodes that they know. After a few iterations, every node knows the existence of every other node and which ones are master-eligible



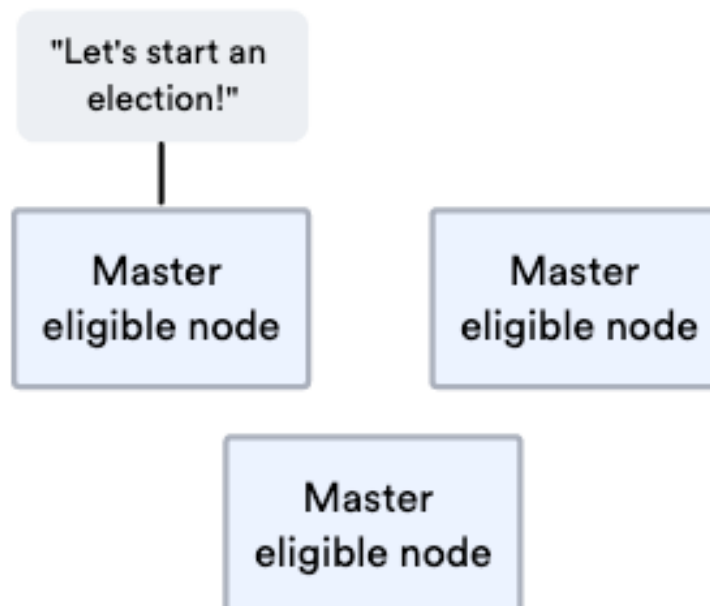
## Elasticsearch

Any master-eligible node can start an election for the new master, and each one does so with some randomness so the two elections don't happen at once.



Fails if two elections start at the same time

and it's responsible for storing, querying, and analyzing data

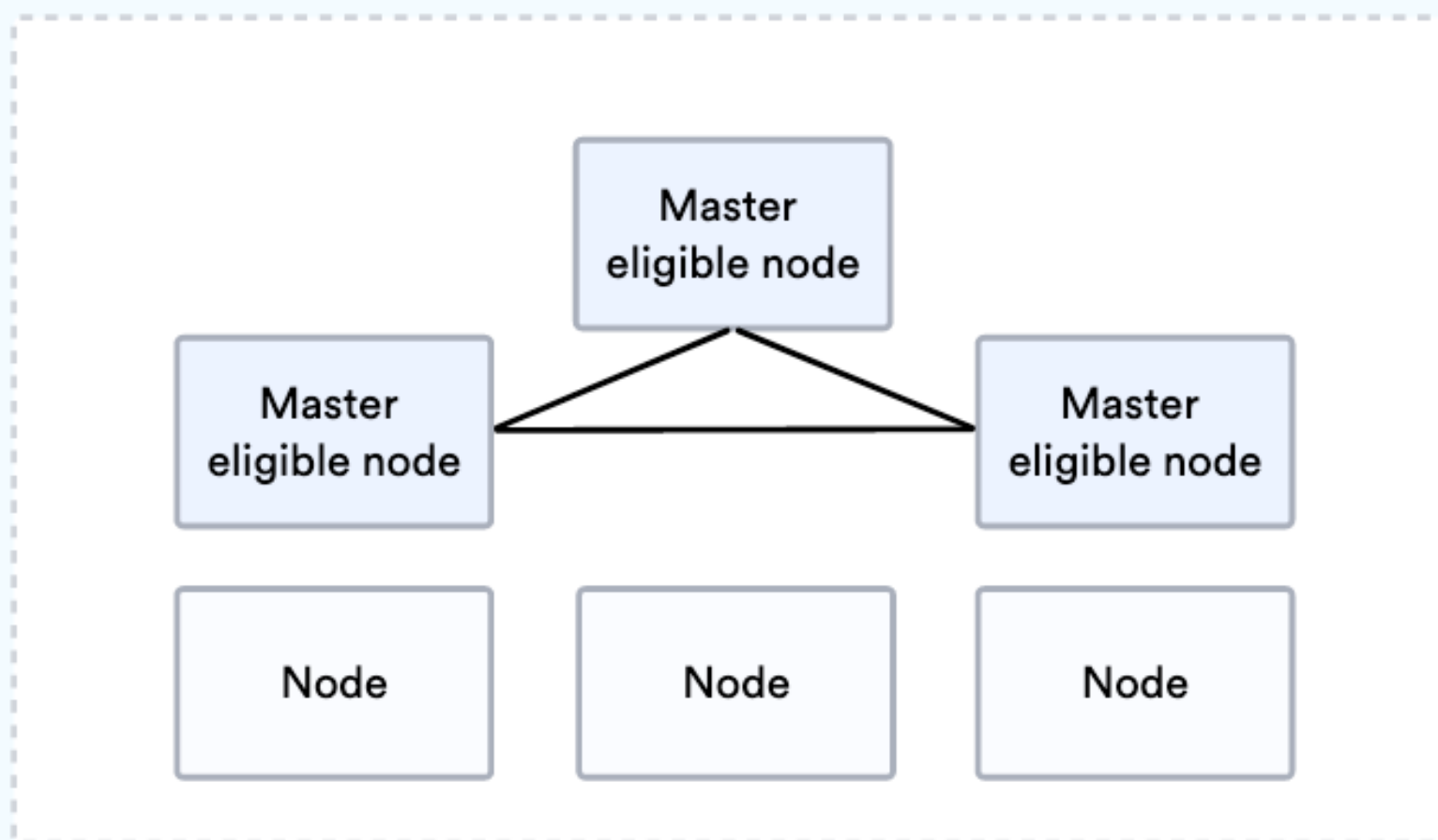


Election for a new master can start



## Elasticsearch

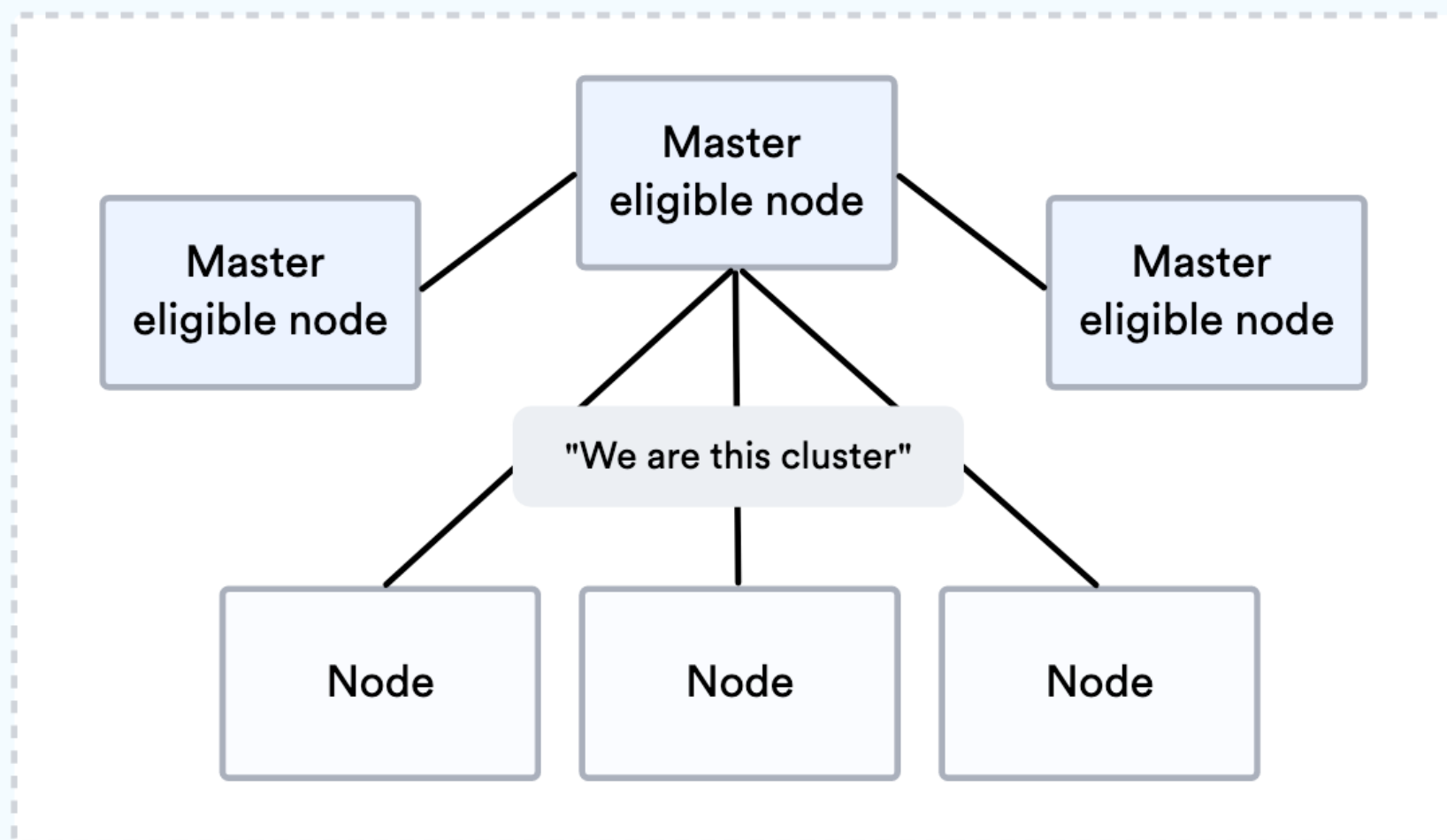
The master-eligible nodes vote amongst themselves for the new master.





## Elasticsearch

The master node is the only node that can make updates to the cluster state. It tells every other node how to behave and what their cluster is.

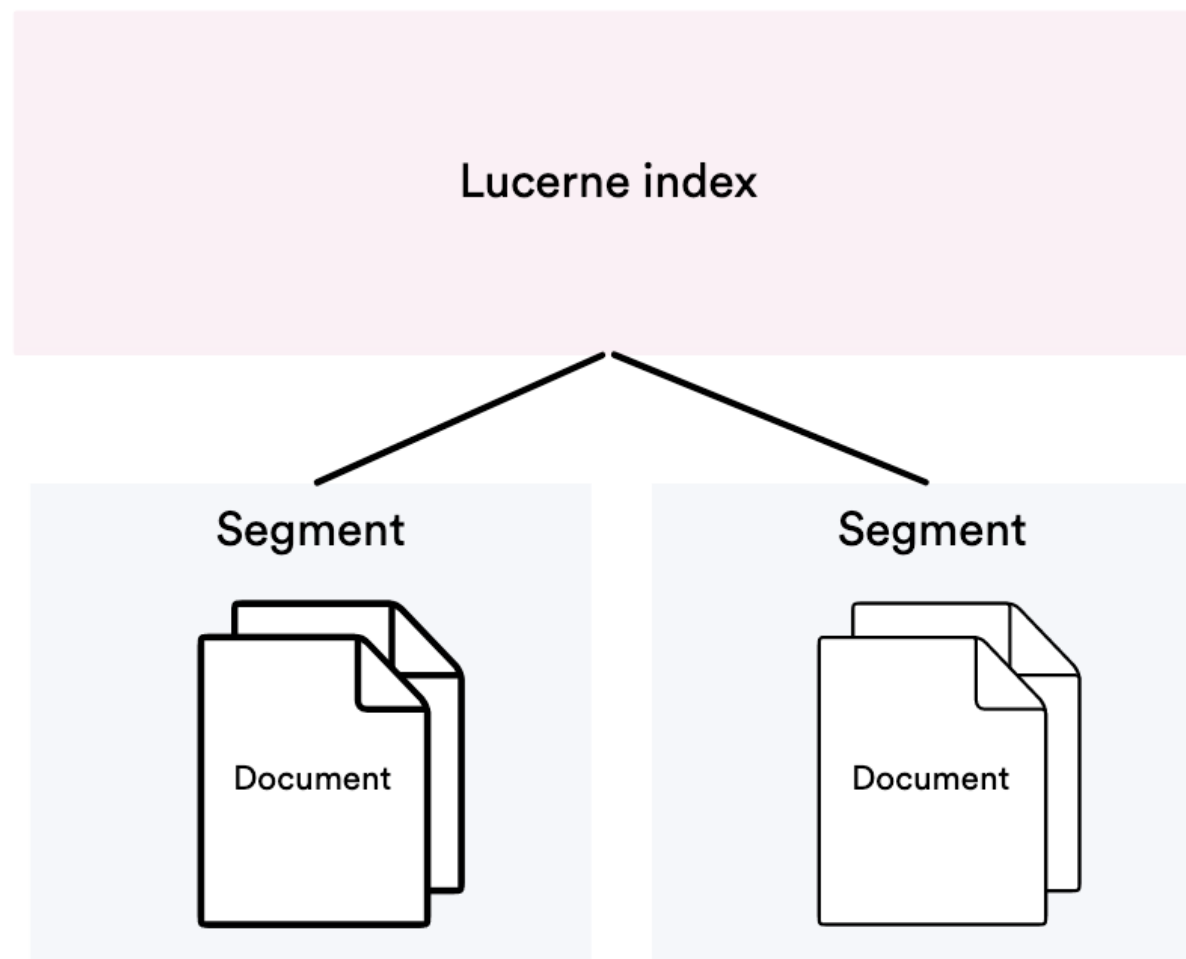


The settings for the cluster, like name, come from initial configurations of the nodes.

## Elastic shard

A Lucerne index is made of multiple Lucerne segments. It's actually an inverted index, which maps terms to documents containing the terms. when a search is performed, every shard is queried, and the Lucerne index in turn queries all its segments

### Apache Lucerne



A segment is like a mini-index on the document. A shard can only have one to thousands of segments.

Not exactly 1-1. Segments can merge with other segments.



