Logstash :

Logstash is typically used for collecting, parsing, and storing logs for future use as part of a log management solution.

Logstash is a plugin-based component, meaning it is highly extensible in what sorts of source/destination systems it supports and transformations it can do.

Logstash has a larger footprint, but provides a broad array of input, filter, and output plugins for collecting, enriching, and transforming data from a variety of sources.

Logstash's biggest con or "Achille's heel" has always been performance and resource consumption (the default heap size is 1GB).

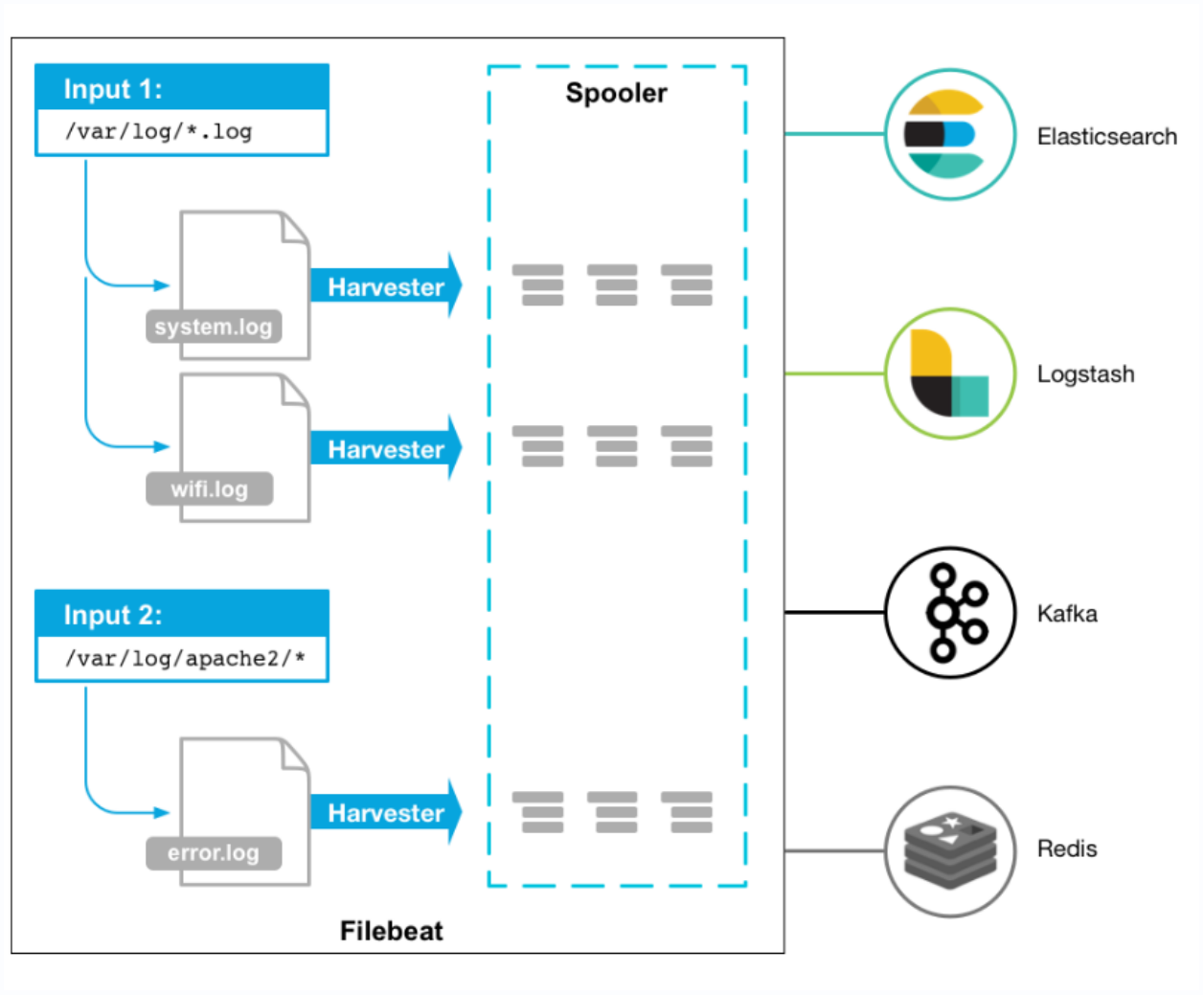
If we want to do any sort of data processing or want to capture any complex data, which isn't possible using Beats, we must use Logstash. If we just want to read log data, system metrics data, or any data that's easily available using Beats, we should go for Beats in that case.

FileBeats:

lightweight log shipper that you install as agents on your servers that pushes to Logstash, Kafka or Elasticsearch. Filebeat takes less resources.

Filebeat consists of two main components: *inputs* and *harvesters*. These components work together to tail files and send event data to the output that you specify.

A harvester is responsible for reading the content of a single file. The harvester reads each file, line by line, and sends the content to the output.
An input is responsible for managing the harvesters and finding all sources to read from.



If the input type is log, the input finds all files on the drive that match the defined glob paths and starts a harvester for each file. Each input runs in its own Go routine.

Filebeat guarantees that events will be delivered to the configured output at least once and with no data loss. Filebeat is able to achieve this behavior because it stores the delivery state of each event in the registry file.

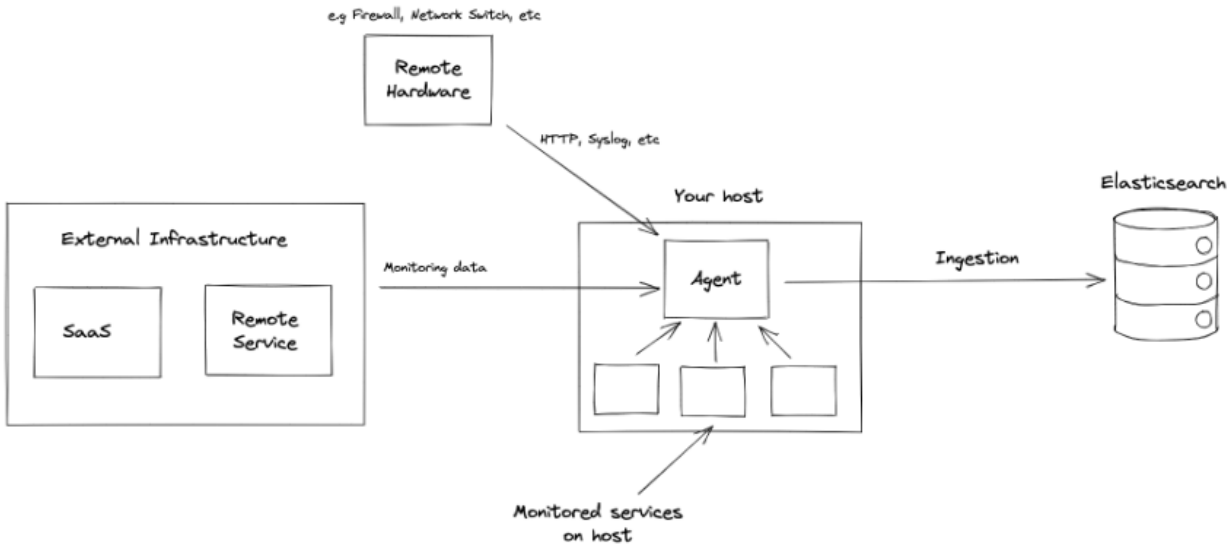
Filebeat comes with modules for specific log types. For example, the Apache module will point Filebeat to default access.log and error.log paths, configure Elasticsearch's Ingest node to parse them, configure Elasticsearch's mappings and settings as well as deploy Kibana dashboards for analyzing things like response time and response code breakdown.

Filebeat to Elasticsearch's Ingest

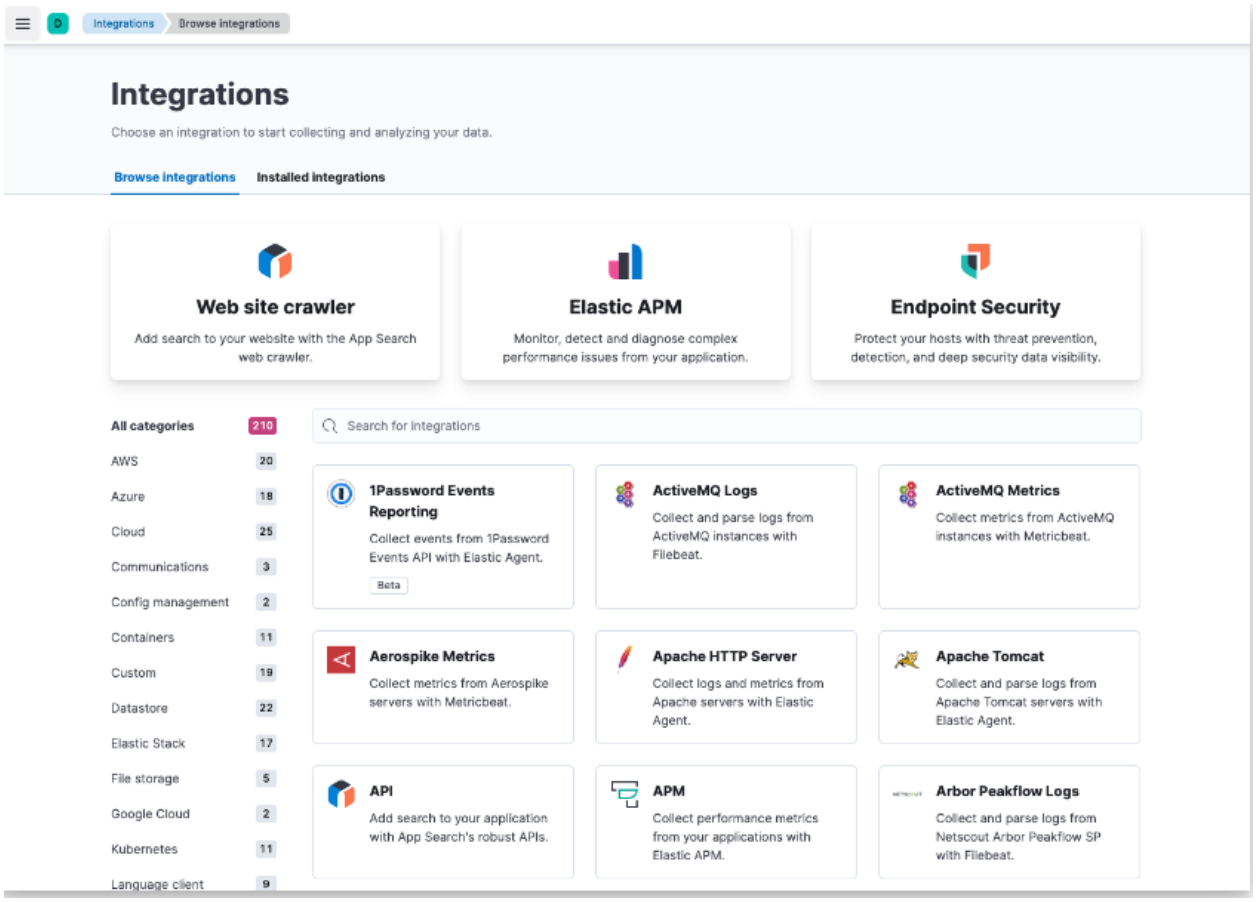
Elasticsearch comes with its own parsing capabilities (like Logstash's filters) called Ingest. This means you can push directly from Filebeat to Elasticsearch, and have Elasticsearch do both parsing and storing.
You shouldn't need a buffer when tailing files because, just as Logstash, Filebeat remembers where it left off:

Elastic Agent & Fleet:

Elastic Agent is a single, unified way to add monitoring for logs, metrics, and other types of data to each host. You no longer need to install multiple Beats and other agents. This will make it easier and faster to deploy across your infrastructure. Additionally, Elastic Agent has a single, unified configuration. Thus, there is no need to edit multiple configuration files for Filebeat, Metricbeat, and others. This will make it easier to add integrations for new data sources.

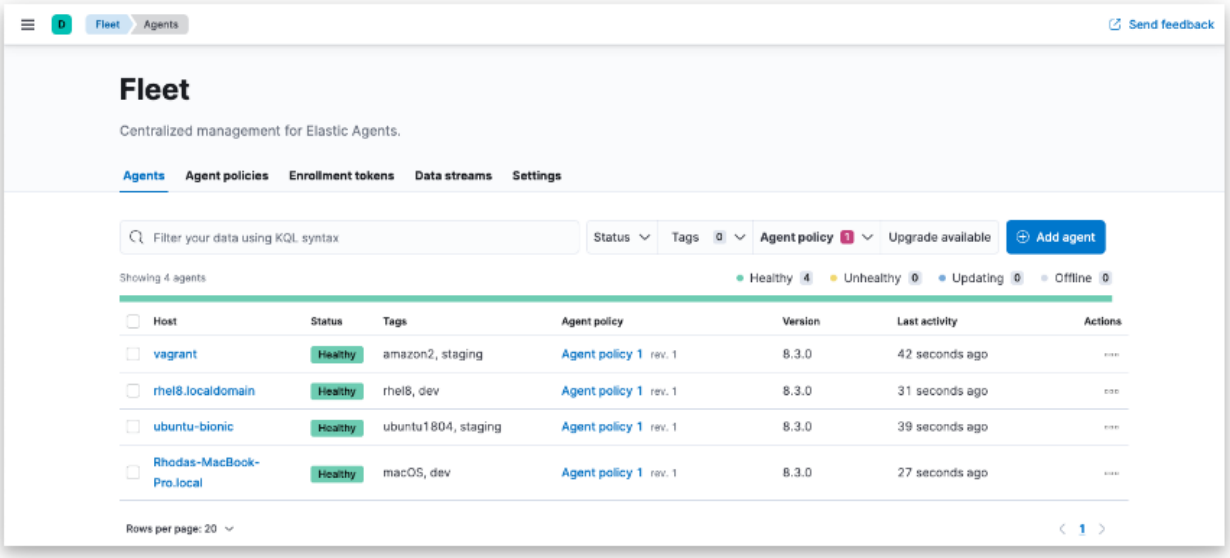


Elastic Agent runs Beats under the covers. Elastic Agent is a lightweight interface on top that allows for easier deployment and central management.
Listed below is the integrations supported by Agent.



Agent policies specify which integrations you want to run and on which hosts. You can apply an Elastic Agent policy to multiple agents, making it even easier to manage configuration at scale.

Fleet provides a web-based UI in Kibana for centrally managing Elastic Agents and their policies.



Fleet Server is the mechanism to connect Elastic Agents to Fleet.
Beats and Elastic Agent can both send data directly to Elasticsearch or via Logstash, where you can further process and enhance the data, before visualizing it in Kibana.

Outputs supported by Agent and beats:

Output	Beats	Fleet-managed Elastic Agent	Standalone Elastic Agent
Elasticsearch Service	✔	✔ only to the same cluster where Fleet runs	✔
Elasticsearch	✔	✔ only to the same cluster where Fleet runs	✔
Logstash	✔	✔	✔
Kafka	✔	Under consideration	Under consideration
Redis	✔	✘	✘
File	✔	✘	✘
Console	✔	✘	✘