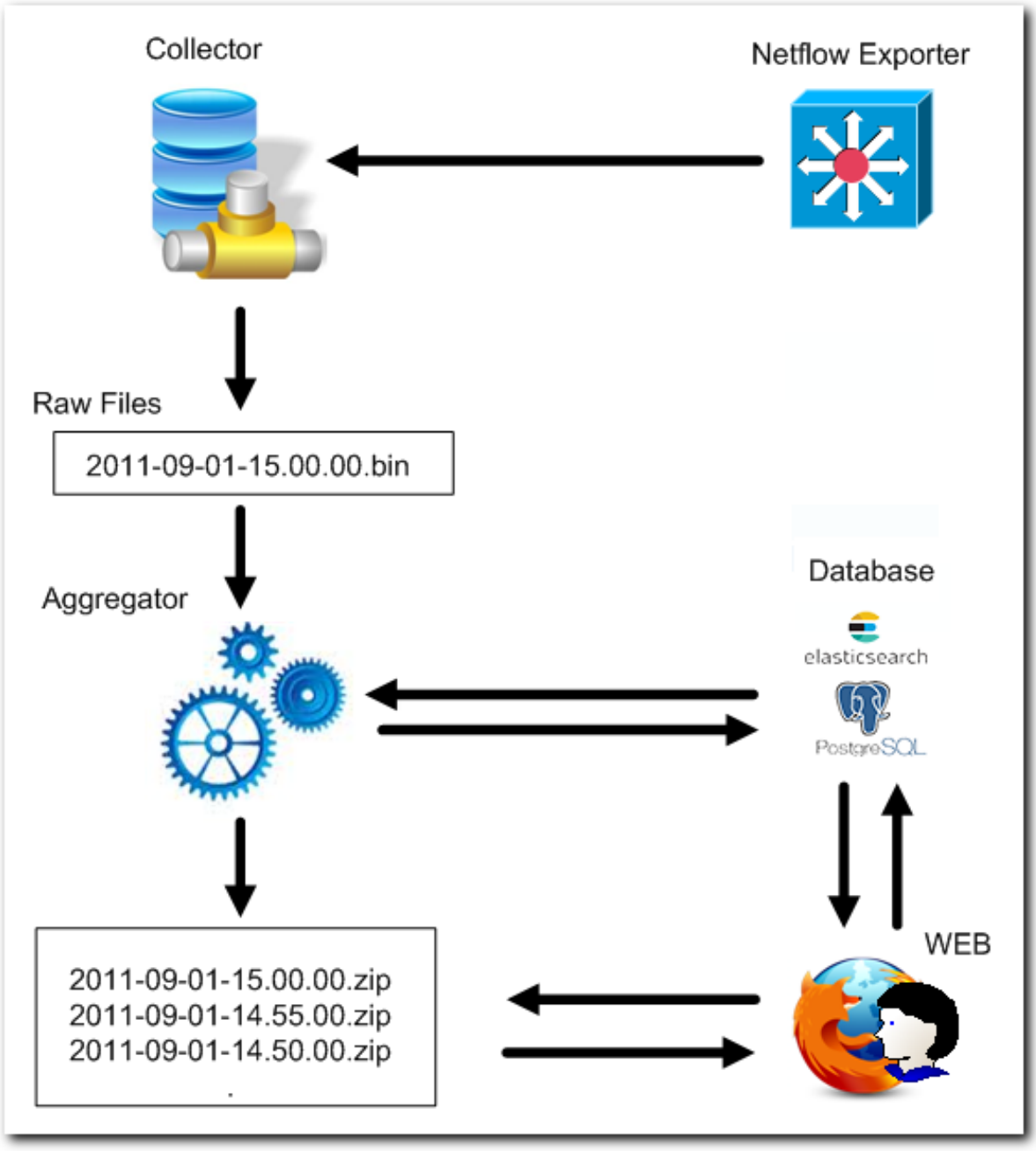
Elasticsearch Infrastructure

Elasticsearch is a noSQL database, primarily based on the text data search. In NetVizura, Elasticsearch is currently an alternative database for storing aggregated Netflow data while the primary database is still PostgreSQL.



Data in Elasticsearch is aggregated daily in a manner similar to the tables in PostgreSQL. In NetVizura, Elasticsearch currently uses around 30% of RAM, therefore don't be concerned regarding memory consumption. To learn more about NetVizura system requirements read System Requirements.

Elasticsearch RAM memory configuration

Configuration and installation of Elasticsearch database are done automatically by executing the script or, in the case of Windows, just by running the Elastcsearch exe file. NetVizura Elasticsearch installer automatically sets 30% of RAM to Elasticsearch.

Linux

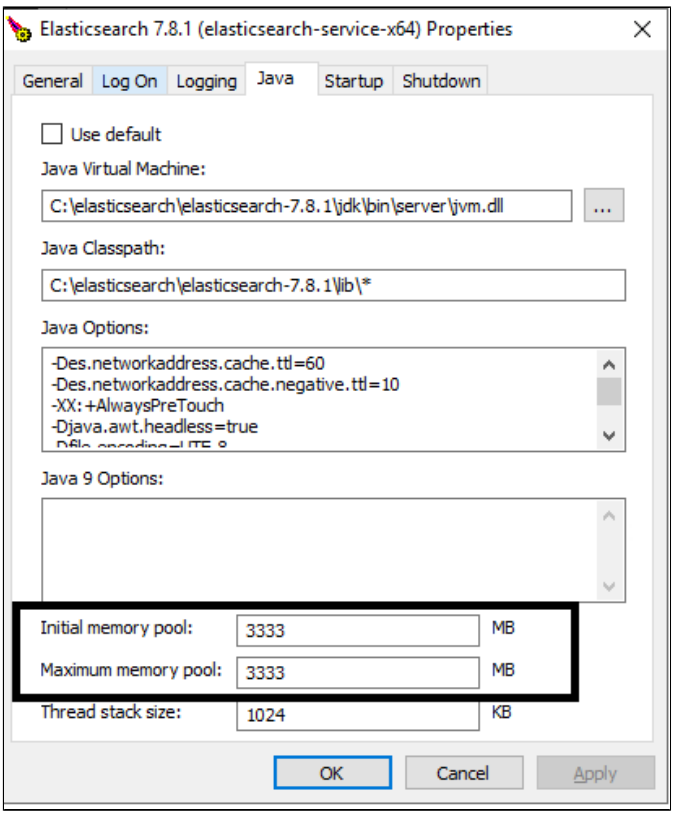
The additional configuration can be done inside jvm.conf file either in **/etc/elasticsearch** for all Linux distributions, and setting memory like this:

```
-Xms1943m
-Xmx1943m
```

Windows

There are two ways of configuring Elasticsearch RAM memory consumption on Windows host:

- Set it by running manager from command line: *C:\elasticsearch\elasticsearch-7.8.1\bin\elasticsearch-service.bat*, and by configuring in the manner similar to our example below:



- Configuring parameters `JvmMs` and `JvmMx` in the following Registry editor:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\elasticsearch-service-x64\Parameters\Java
```

Elasticsearch vs Relational DB

The table below shows the comparison between traditional relational DB and Elasticsearch:

PostgreSQL	Elasticsearch
Database	Index
Partition	Shard
Table	Type—deprecated
Column	Field
Schema	Mapping
Index	Everything is indexed
SQL	Query DSL