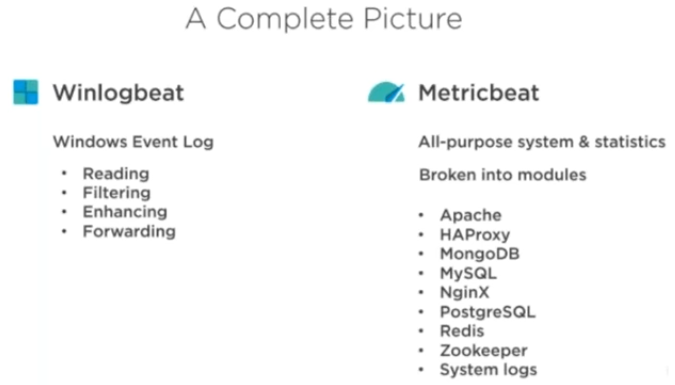
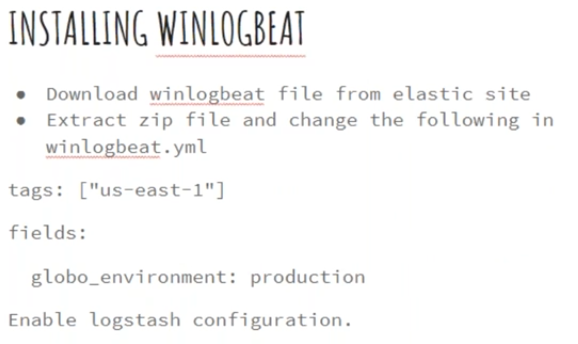


* We want to send RAM, CPU, disk and event logs from windows server to logstash
* For doing this we use two beat components called winlogbeat and metricbeat



* Generally, beat programs written in golang from google where we no need any execution, we can just download them and start
* Docker also written in golang



* We want to send the logs from windows to elastic search log
* Download winlogbeat. For any doubts we better see docs or go to github from site to see the information

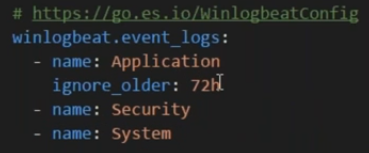


Follow the above steps

Then below also



Open configuration file

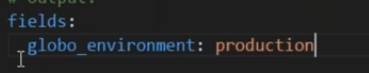


We are ignoring the logs older than 72 hrs

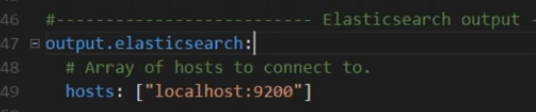


Create a tag with us-east-1. This is just to simulate that this machine is from us-east-1

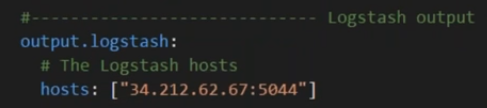
Uncomment and add global\_configuration



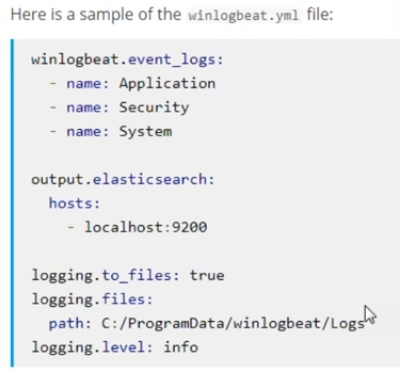
by default, it send s logs to elasticsearch

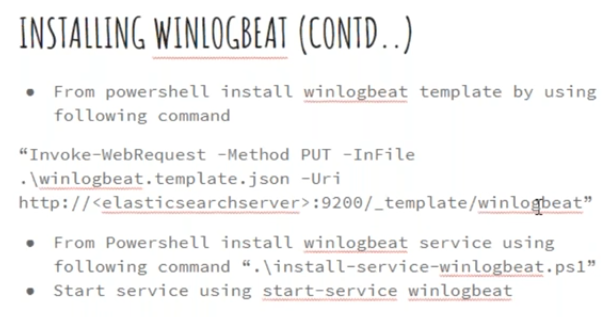


If we want, we can enable to logstash as below



This is the configuration in document from website





We have executed the above command to download the template from elastic search server

In elastic search we have index template and we have load them

If we disable automatic template loading, we need to do manually