Configuring Elasticsearch

JP Toto
INFRASTRUCTURE DEVELOPER

@jptoto http://jptoto.jp

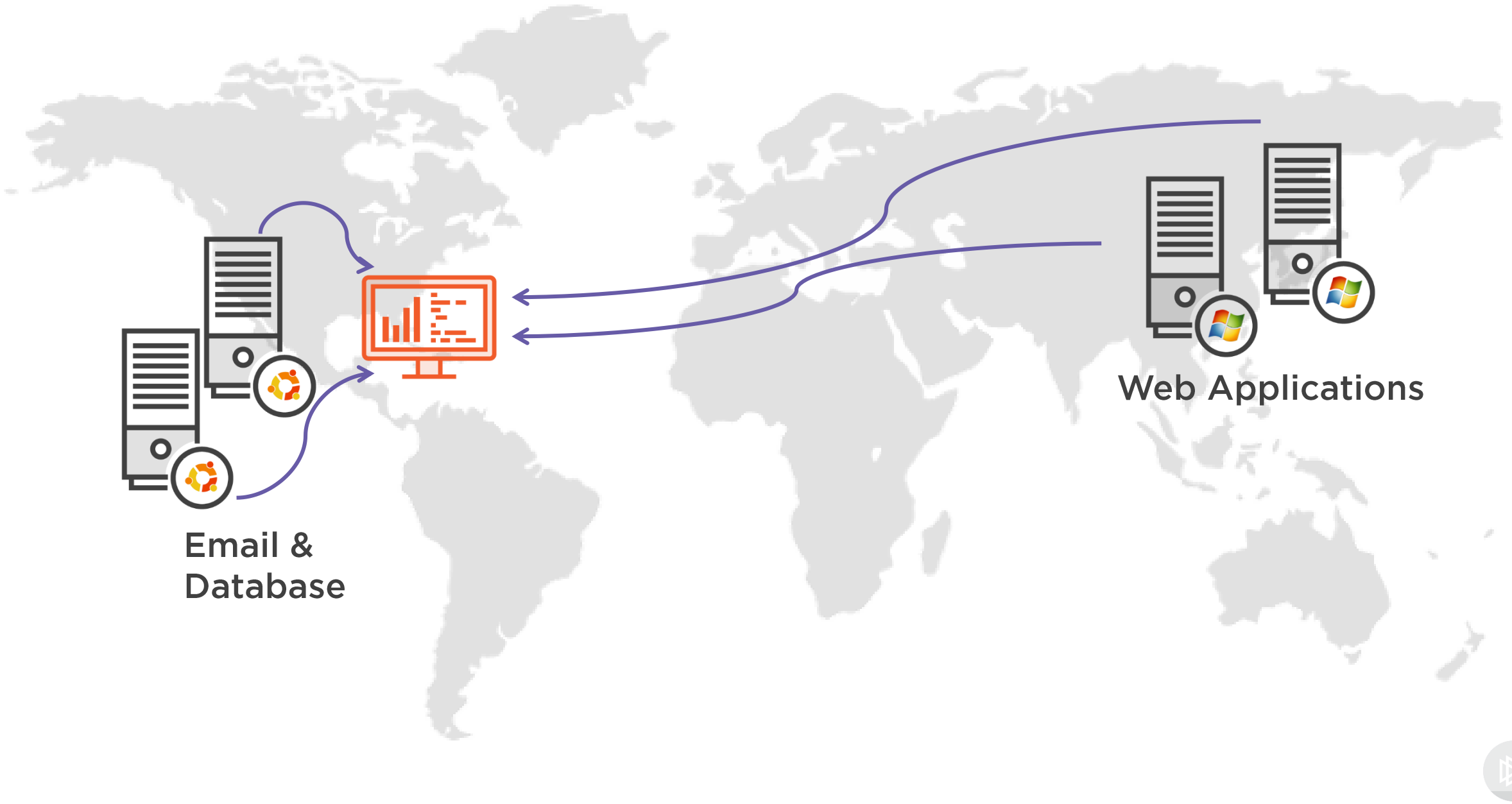
Globomantics Is Worldwide

Disk

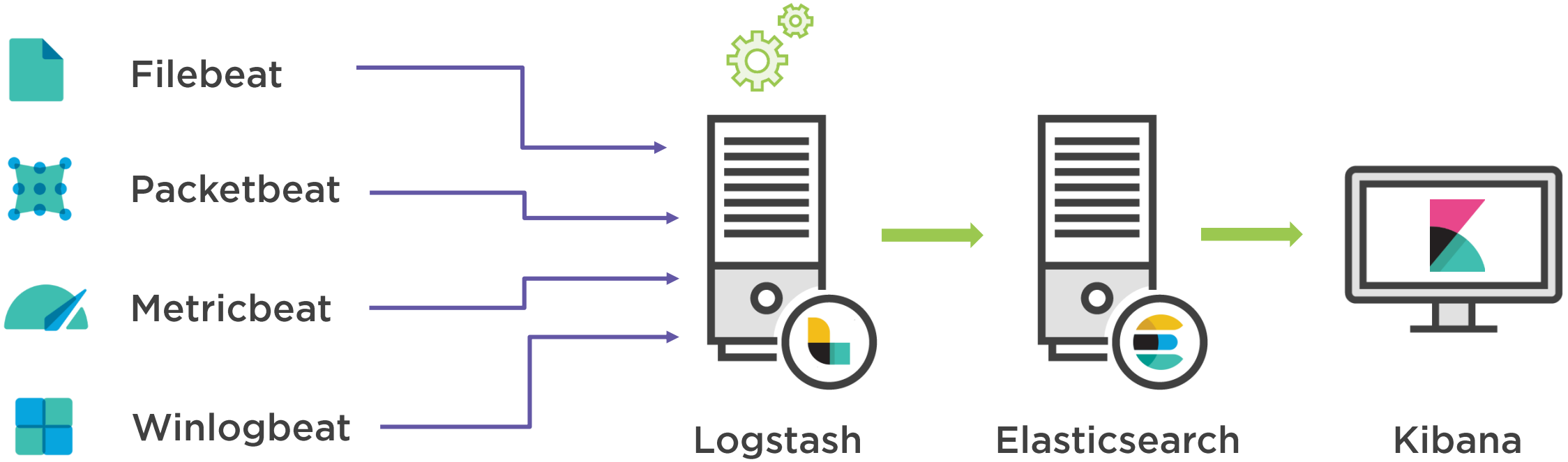
CPU & RAM

Applications

Network


Email &
Database
Web Applications

Beats


Filebeat
Packetbeat
Metricbeat
Winlogbeat
Logstash
Elasticsearch
Kibana

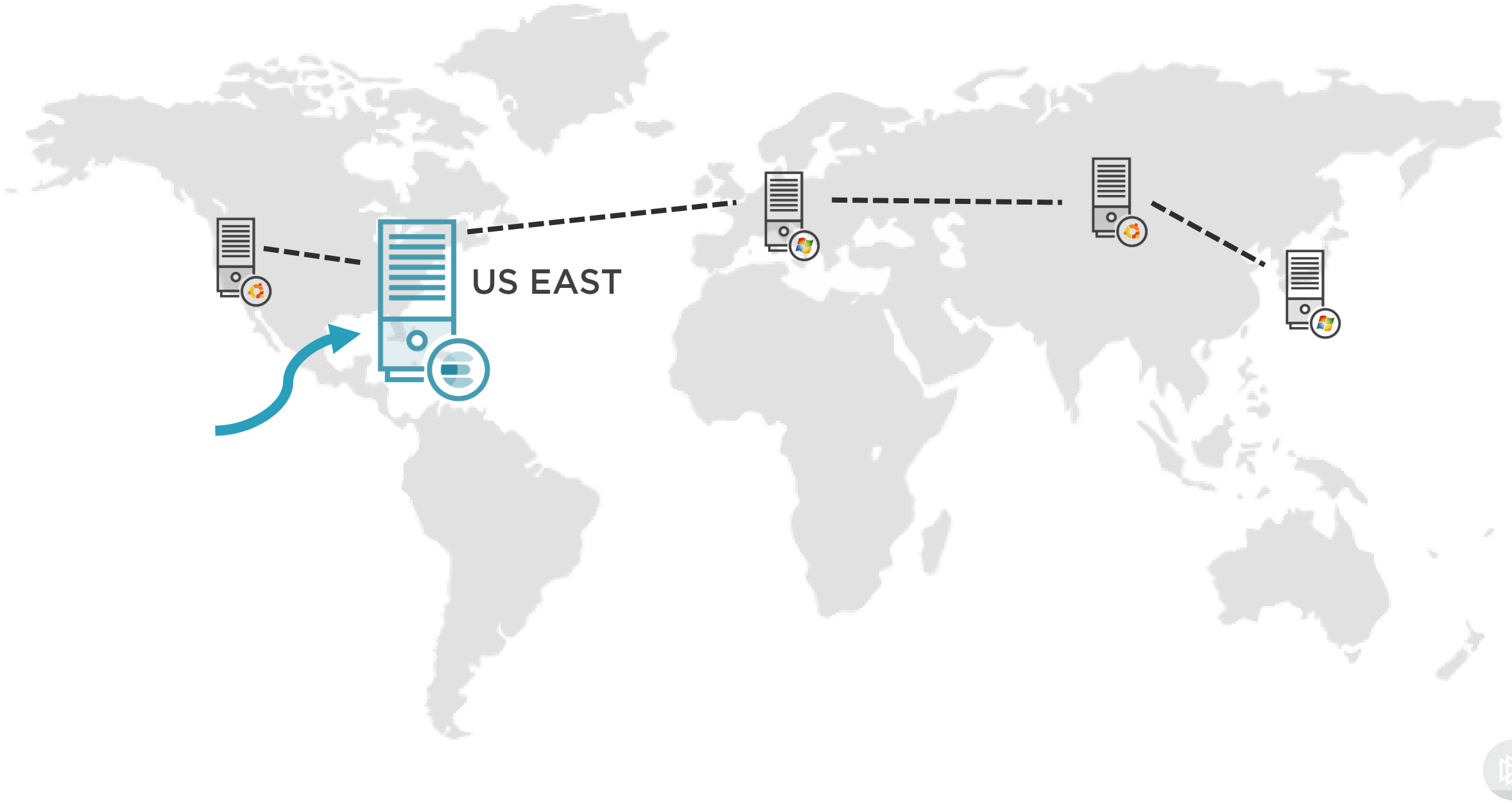
System Buildout

Start from the back, work forward

Usually Elasticsearch clusters comprise many nodes

Check out Administering an Elasticsearch Cluster

We're keeping things simple with one Elasticsearch node


US EAST

Demo

What kind of OS should we use?
Elasticsearch runs fine on Linux & Windows

We're going to choose Linux and use distribution packages

Ubuntu 16.10 Server Edition

We'll also demonstrate a Windows install

Demo

Linux install looks good, let's do a Windows install

If you're not in a mixed / heterogeneous OS environment, this section is for you

Summary

Challenges to the monitoring setup

Figured out our plan

Demonstrated how to install Elasticsearch on Linux and Windows

Next: Logstash