Instrumenting Windows Servers

JP Toto
INFRASTRUCTURE DEVELOPER

@jptoto http://jptoto.jp

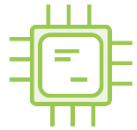
Instrumenting Windows Servers

File Hosting

Web Server

Email Server

RAM



CPU

Disk

Event Log

A Complete Picture

Winlogbeat

Windows Event Log

- Reading
- Filtering
- Enhancing
- Forwarding

Metricbeat

All-purpose system & statistics

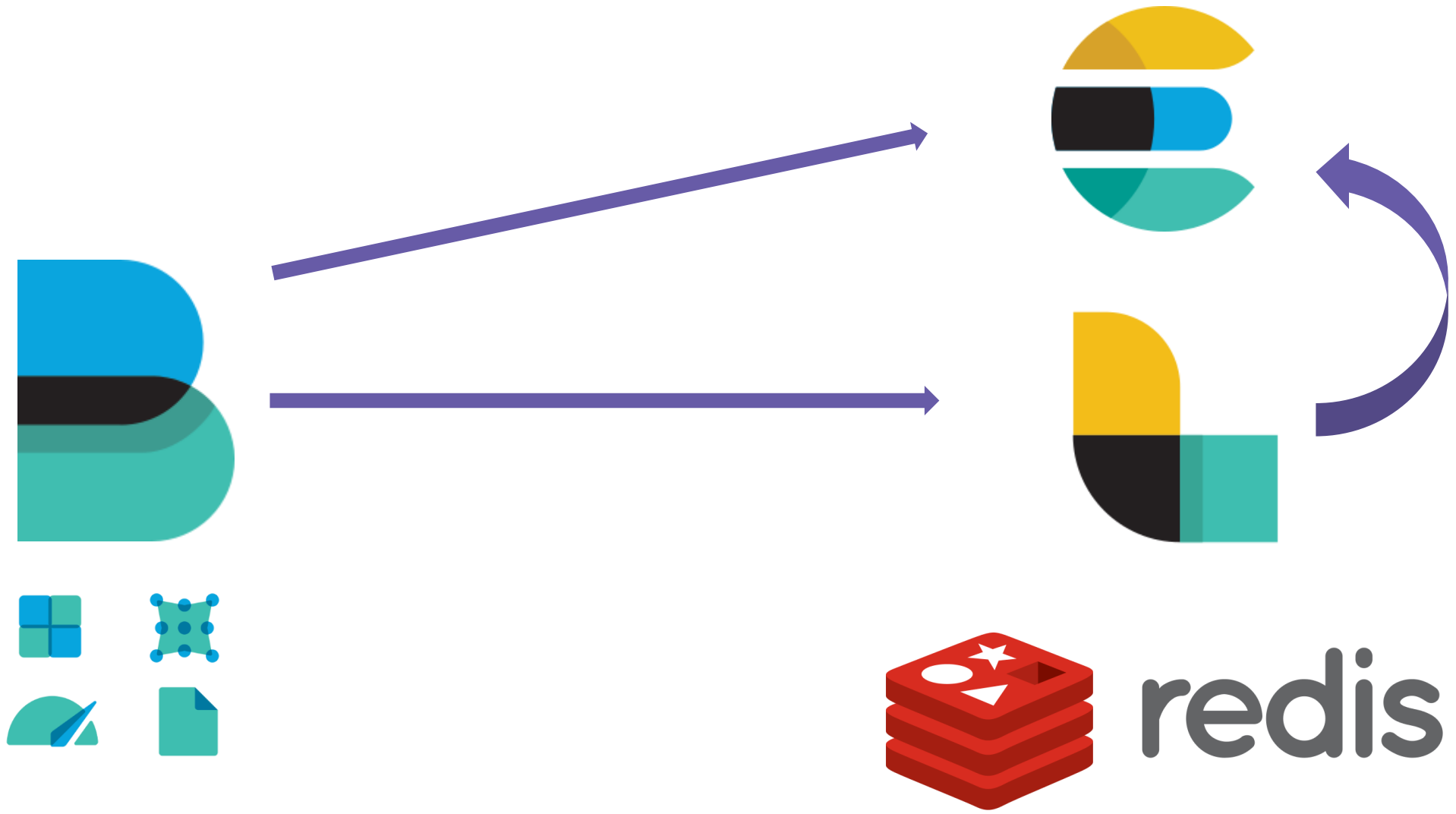
Broken into modules

- Apache
- HAProxy
- MongoDB
- MySQL
- NginX
- PostgreSQL
- Redis
- Zookeeper
- System logs

Go programs are static binaries, no need for JVM or other runtimes

Can be “cross-compiled” to work on Windows, Linux, macOS, and BSD

Usually pretty small and lightweight – great for system utilities


redis

Usually large companies have dozens, hundreds, or even thousands of servers

For our purposes, we're going to use two Windows web servers and one Windows file server

Will keep the data diverse enough for our demonstrations

Demo

Download and unpack Winlogbeat

Configure it to use logstash and add some custom fields and data

Set it up to run as a Windows service

Demo

Configure Logstash to read Beats data and forward it to Elasticsearch

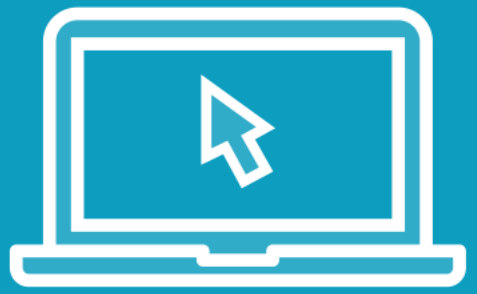
Demo

Learn how basic Kibana configuration works

General querying

Visualizations and dashboards

Demo



Configure Metricbeat it to use logstash and add some custom fields and data

Set it up to run as a Windows service

Build a new dashboard in Kibana

Summary

- Installed and configured Winlogbeat and Metricbeat
- Built our first Logstash configuration
- Created dashboards in Kibana
- Next: Instrumenting Linux