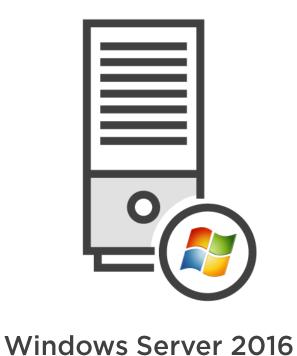
Instrumenting IIS Logs



JP Toto
INFRASTRUCTURE DEVELOPER
@jptoto http://jptoto.jp





Windows Server 2016, IIS

IIS uses the common w3c log format which is easy to read



IIS Log Example

```
#Software: Microsoft Internet Information Services 10.0
2 #Version: 1.0
  #Date: 2016-12-23 14:21:45
  #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(
  2016-12-23 14:21:45 192.168.0.13 GET / - 80 - 93.114.45.13 curl/7.51.0 - 200 0 0 67
  2016-12-23 14:22:46 192.168.0.13 GET / - 80 - 93.114.45.13 curl/7.51.0 - 200 0 0 3
  2016-12-23 14:22:46 192.168.0.13 GET / - 80 - 93.114.45.13 curl/7.51.0 - 200 0 0 3
  2016-12-23 14:22:46 192.168.0.13 GET / - 80 - 146.186.157.10 curl/7.51.0 - 200 0 0 4
  2016-12-23 14:22:46 192.168.0.13 GET / - 80 - 146.186.157.10 curl/7.51.0 - 200 0 0 3
  2016-12-23 14:31:38 192.168.0.13 GET / - 80 - 110.136.166.128 curl/7.51.0 - 200 0 0 5
  2016-12-23 14:31:38 192.168.0.13 GET / - 80 - 110.136.166.128 curl/7.51.0 - 200 0 0 4
  2016-12-23 14:31:38 192.168.0.13 GET / - 80 - 110.136.166.128 curl/7.51.0 - 200 0 0 3
  2016-12-23 14:31:39 192.168.0.13 GET / - 80 - 146.186.157.10 curl/7.51.0 - 200 0 0 6
  2016-12-23 14:31:39 192.168.0.13 GET / - 80 - 46.105.14.53 curl/7.51.0 - 200 0 0 2
```



How Should We Parse IIS Logs?



Not just good for reading syslog data

Great for reading any text log data



Demo

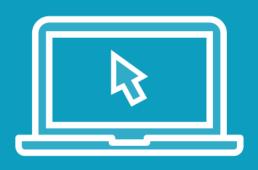


Configure Filebeat to read IIS logs

Update the Logstash configuration to parse IIS data



Demo



Examine IIS log data in Kibana

Create a geo location dashboard for requests



Summary



Configured Filebeat to read IIS log data and modified Logstash accordingly

Graphed location data of the requesting IP addresses

Next: Alerting

