

Instrumenting Network Traffic



JP Toto

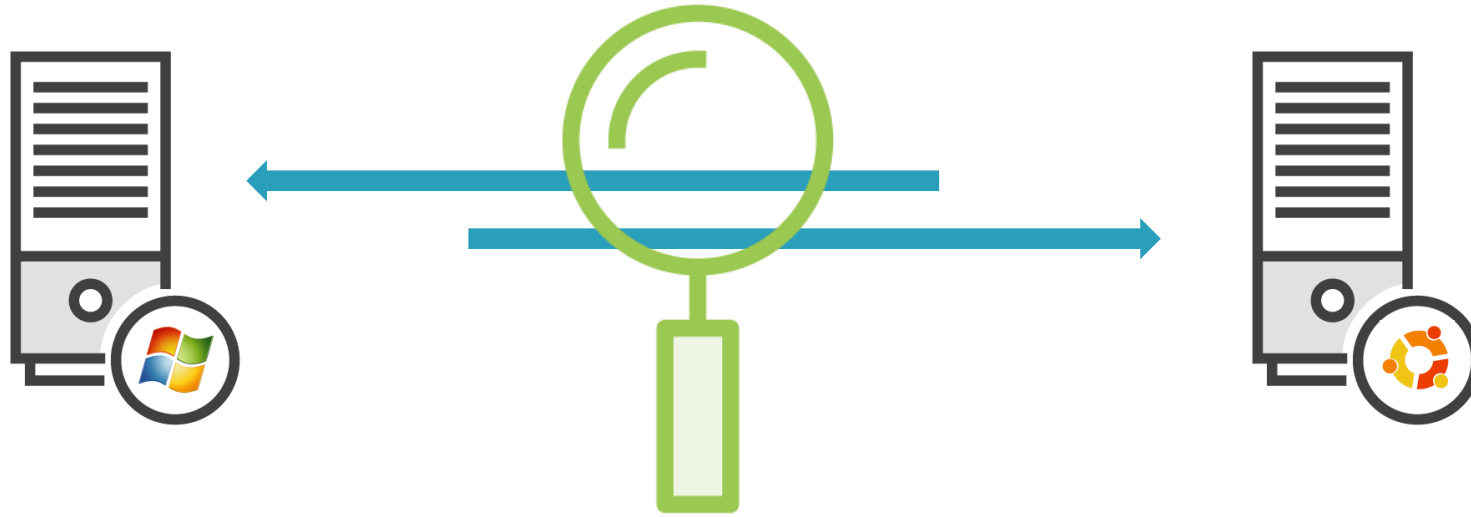
INFRASTRUCTURE DEVELOPER

@jptoto

<http://jptoto.jp>



Examining Network Traffic



Network spike?
High traffic?



Packetbeat

Realtime network packet analyzer

Bundles packets of traffic into transactions which can be charted

Can listen for ICMP, DNS, HTTP, Cassandra, MySQL, PostgreSQL, Redis, Thrift, MongoDB, and Memcache



Demo



Download, install, and configure
Packetbeat



Demo



Examine Packetbeat traffic in Kibana
Discovery screen

Create web traffic dashboard



Summary



Installed and configured Packetbeat on Windows.

Learned how to use Packetbeat to visualize network traffic and tracking load

Next: Filebeat, Logstash, and IIS

