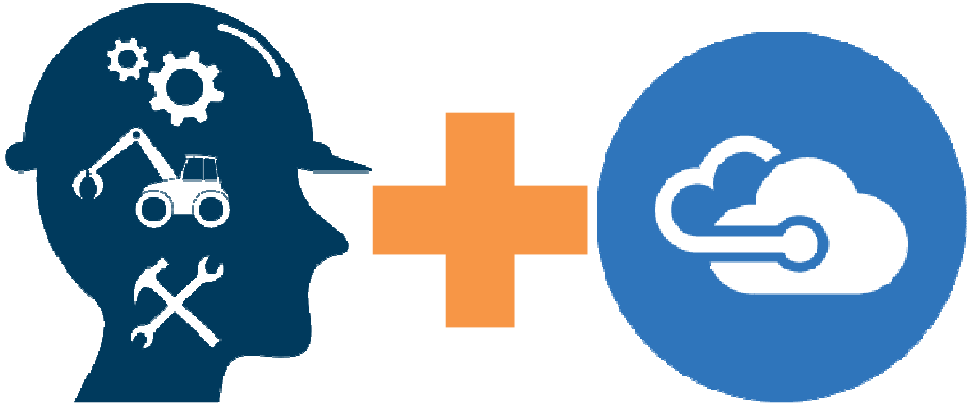
Azure LogAnalytics / OMS.

A sensible approach to observability.

Sunny Chakraborty
@sunnyc7



Context

History lesson:

- **What we know.**
  - Monitoring
    - Against known measures
  - Alerting
    - Tripwire
    - Thresholds
      - Requires knowing what normal means
    - Black-magic (Clint Huffman/PAL + WPA Team)

- **Improvements: Key milestones over the years**
  - Coda Hale - Metrics talk https://www.youtube.com/watch?v=czes-oa0yik
  - Statsd protocol by Etsy. https://github.com/etsy/statsd
  - Time-series data
    - OpenTSDB + Grafana http://opentsdb.net
    - DataDog / Sensu + few others
    - Bosun - http://bosun.org
  - Reimann** (by @aphyr) - http://riemann.io
  - Prometheus https://prometheus.io/

```
(where (or (service #"^api")
           (service #"^app"))
  (where (tagged "exception")
    (rollup 5 3600
      (email "dev@foo.com"))
    (else
      (changed-state
        (email "ops@foo.com")))))
```

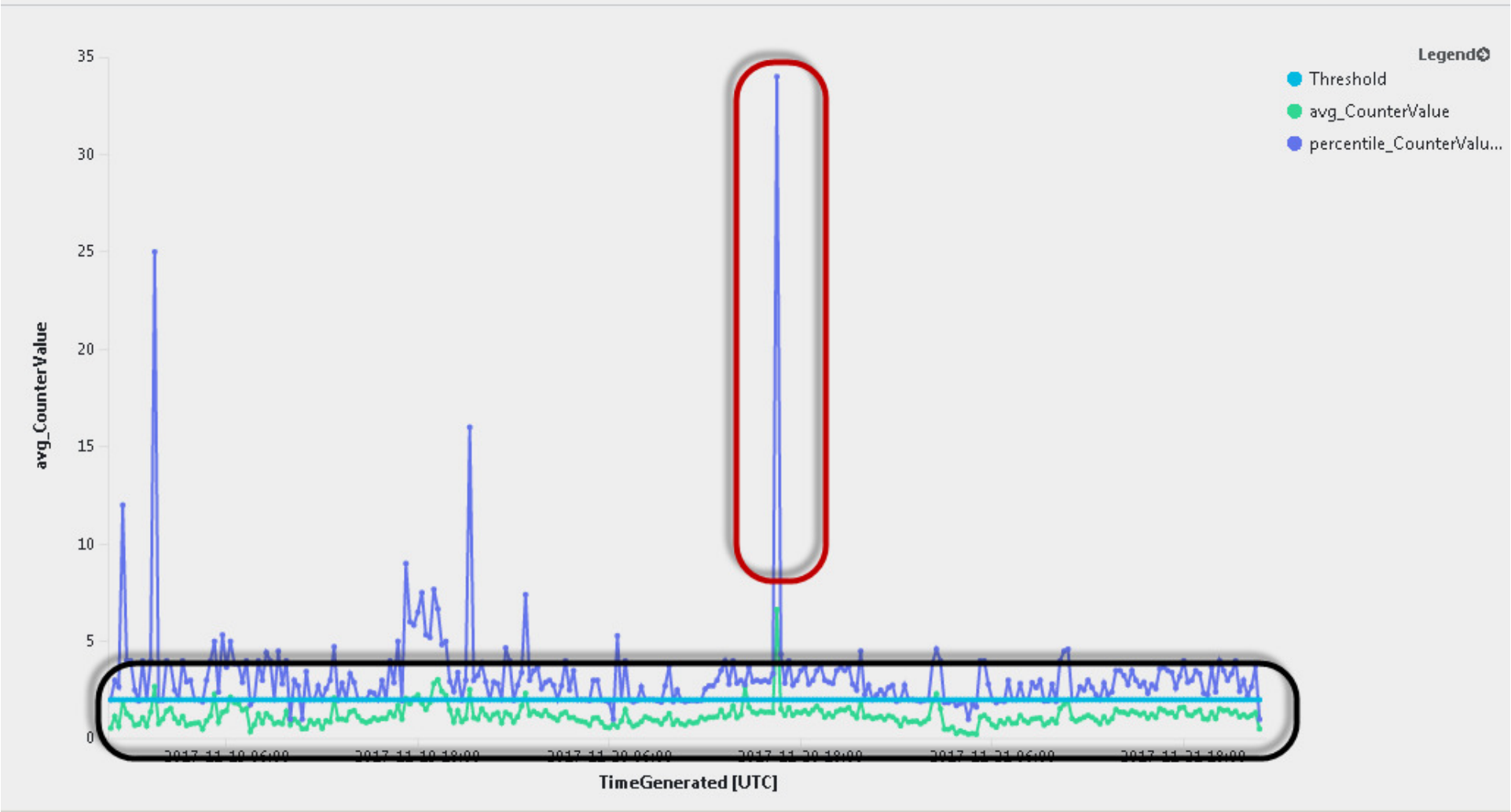
Challenges in the Windows world:

- On a 1000+ node environment:
  - **Telemetry Goals**
    - Quickly aggregate performance metrics across multiple servers.
    - Quickly visualize and derive meaningful insight from metrics.
    - Visualize performance data.
  - **Issue with available options**
    - Perfmon collects data, but cannot do statistics and P95 on 10,000+ data points per server. *
    - Visualization is challenging (try injecting perfmon data in PowerBI/Excel !!).
    - SCOM 2012/2016
      - Is limited by the physical box.
      - Customizing SCOM is challenging.
      - Dashboards– a challenging and time consuming prospect.
    - Others – absent statistical functions. Mean doesn't tell me anything.
  - **RBAC**
    - Making analytics available to rest of the team.
    - Access Logs for dashboards.
    - Enterprise requirement: RBAC based on AD Groups

The problem with SCOM:

- **Issues with SCOM:**
  - Making sense of it, is a challenge.
  - Only Alerting is email, resulting in Inboxes drowning in alert emails.
  - Concepts which no one should have to learn:
    - Alert Tuning
    - Alert Suppression
    - Overrides
  - Knowledge required to run SCOM optimally is substantially high – (Rules, OverRides, Probes, Alert Tuning.)
  - Even after investment in learning SCOM, still its hard to make sense of it.
  - SCOM Reporting - Is non-existent.
- **However, SCOM is still a far better option than the alternatives**:
  - Only solution with good product level metrics using MSFT Management Packs (Free)
  - Advantages of MSFT Product team coupling.
  - Short of custom code, SCOM is *still* one of your best bets.

Tyranny of the MEAN:



Observability

- Read
  - Charity Majors (@mipsytipsy)
  - Cindy Sridharan (@copyconstruct)
- https://medium.com/@copyconstruct/monitoring-and-observability-8417d1952e1c

> *— Why call it monitoring? That's not sexy enough anymore.*
>
> *— Observability, because rebranding Ops as DevOps wasn't bad enough, now they're devopsifying monitoring too*
>
> *— I'm an engineer that can help provide monitoring to the other engineers in the organization*
> *> Great, here's $80k.*
> *I'm an architect that can help provide observability for cloud-native, container-based applications*
> *> Awesome! Here's $300k!*
>
> *— Is that supposed to be like the second coming of DevOps? Or was it the Second Way? I can't remember. It all felt so cultish anyway.*

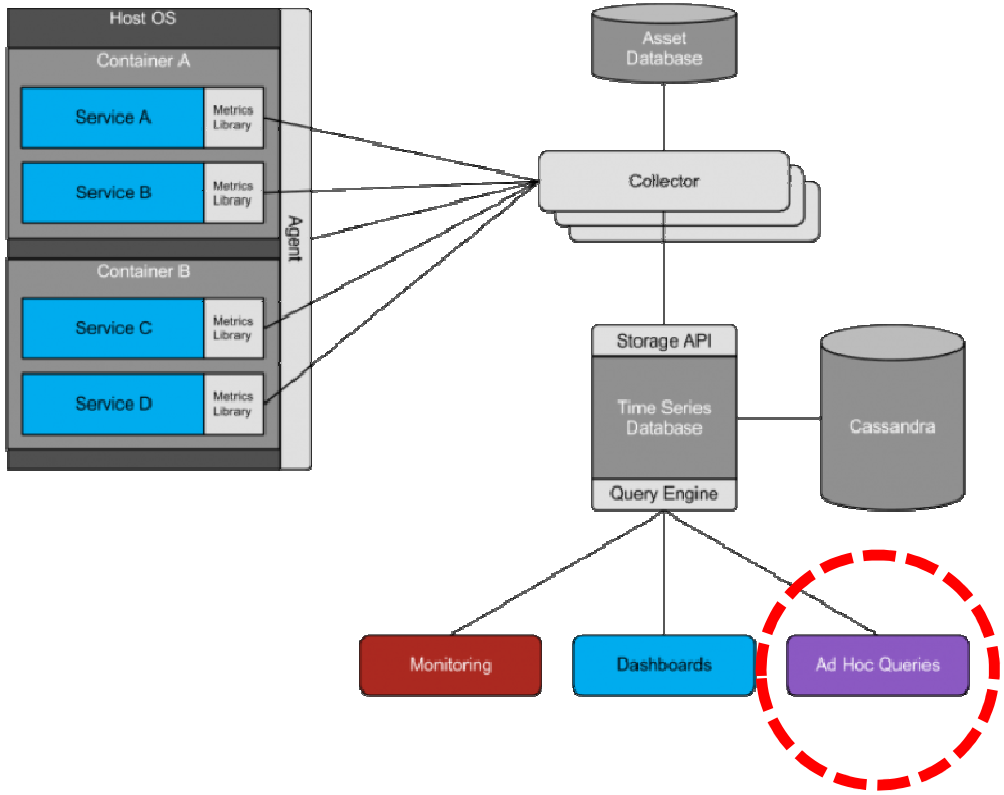
Observability /v Monitoring:

- **Monitoring**:
  - Is for Symptoms based alerting
  - Answers - What's broken, and why? (Ref SRE Book /@copyconstruct)
  - Requires knowledge of Known, hard failure modes.

- **Observability** (via Twitter / Cindy Sridharan /Charity Majors):
  - Monitoring
  - Metrics
  - Log aggregation/analytics
  - Distributed systems tracing infrastructure
  - Alerting/visualization

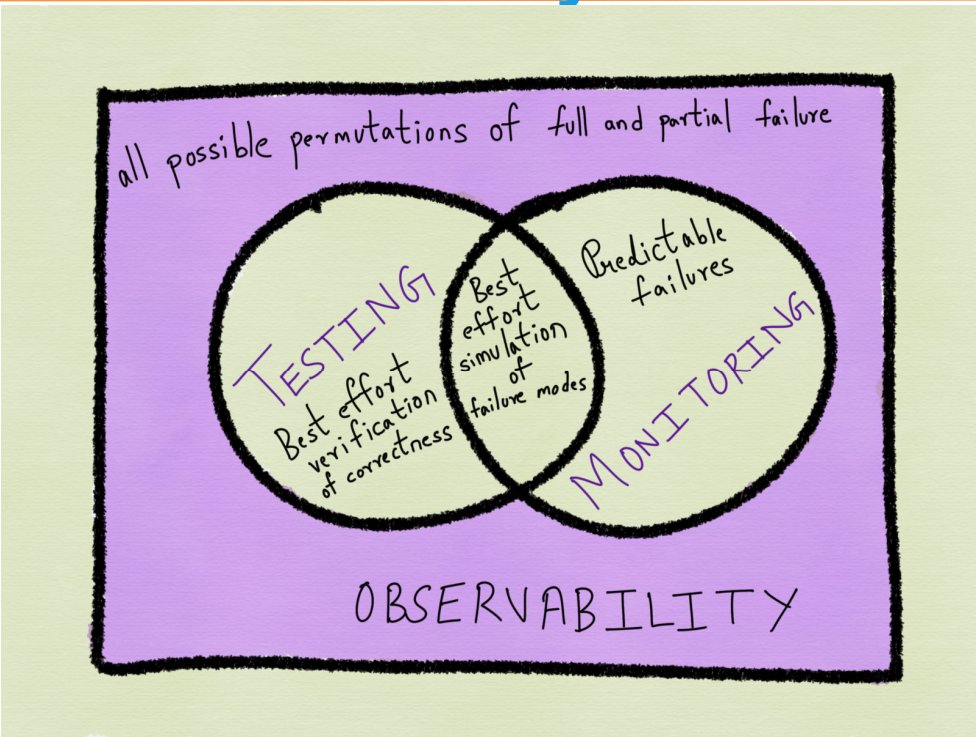
> *We have a* **ton** *of metrics, all right. We try to collect* **everything** *but the vast majority of these metrics are never looked at. It leads to a case of severe metric fatigue to the point where some of our engineers now don't see the point of adding new metrics to the mix, because why bother when only a handful are ever really used?*

Lessons from Twitter : Cloud native patterns:



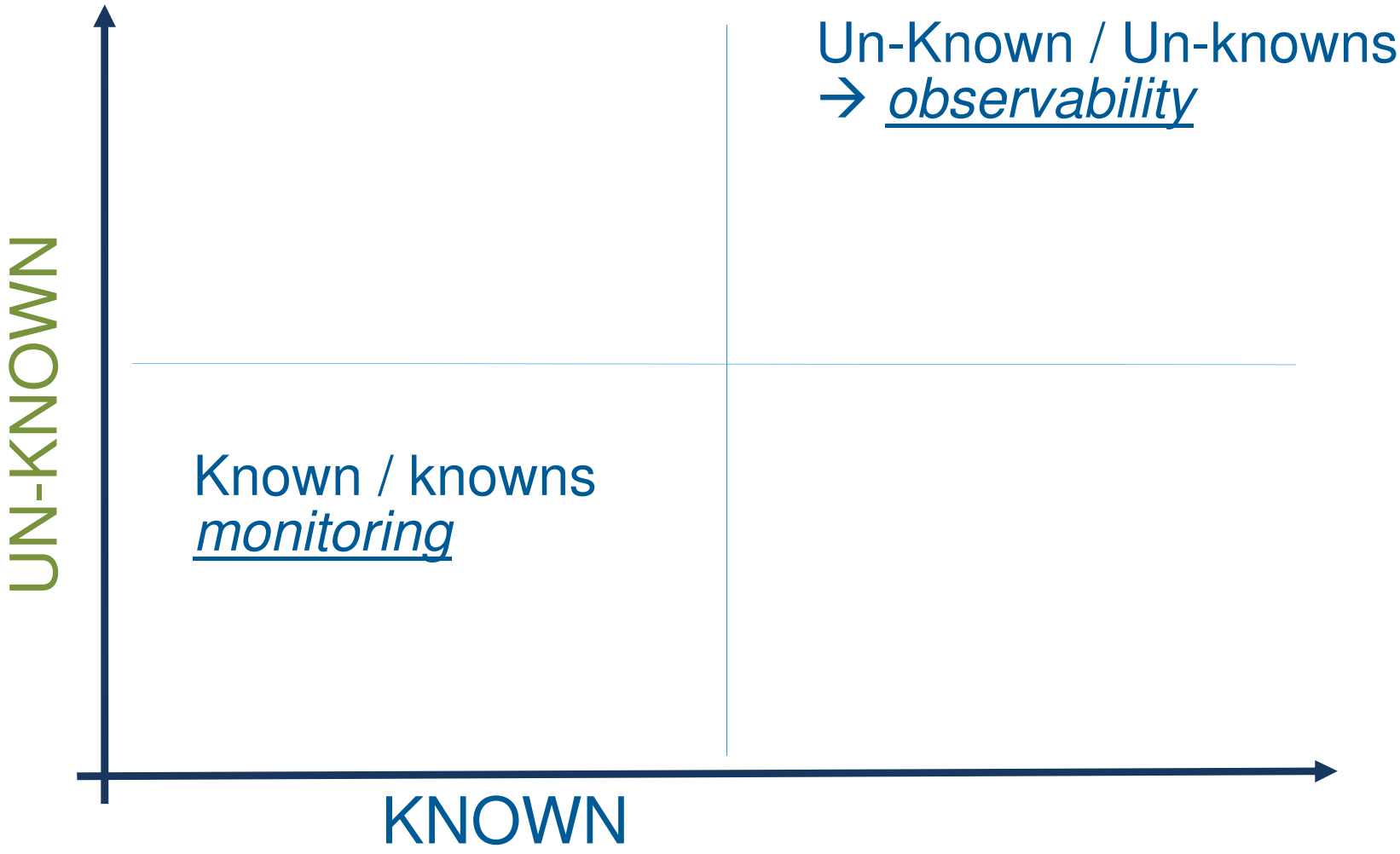
- **<u>Cloud native patterns</u>**
  - Most of these systems are for cloud-scale or for container infrastructure monitoring / observability.
  - Those 12 factor app things.
  - Pattern →
    - 1k/8k servers, depending on load/elasticity - join/unjoin
    - Add to LB.
    - Add to Monitoring - 10 mins and you are serving load.
- The red circle.

Observability /v Monitoring:

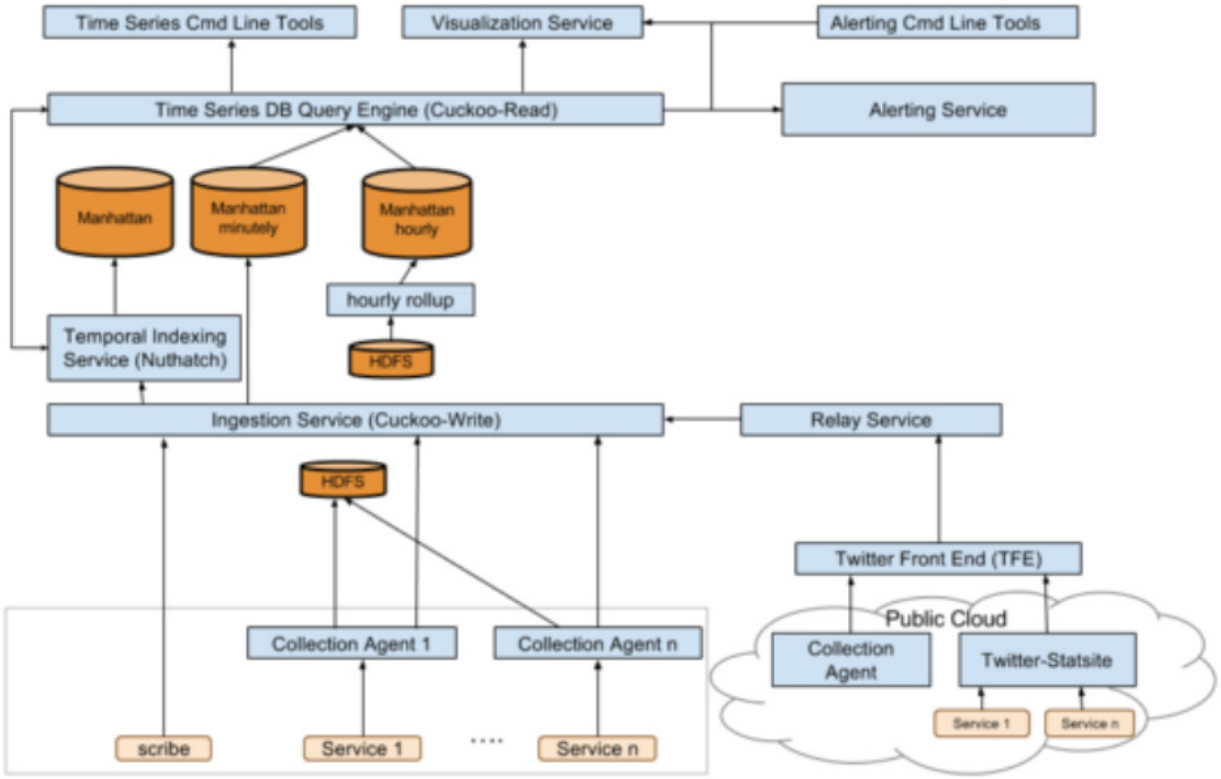


- In control theory, observability is a measure of how well internal states of a system can be inferred from knowledge of its external outputs. (@ wiki)
- Takeaway:
  - Superset of Monitoring
  - Ask any arbitrary question. https://honeycomb.io/observability/

Going full Donnie here (Rumsfeld):



Twitter Observability arch v2:



- If I have to build an observability stack, how do I go about this ? My thoughts:
  - This is really complex.
  - How do I do this in a 90% Windows environment?
  - Where do I get the budget for it to implement this in Windows ? How do I show payoffs ?
  - Looks like an expensive stack to maintain.

Framework requirements:

- **Let's take a step back and think:**
- *If you were to build an observability solution today, what are the ingredients:*
  - Backend infrastructure to process huge amounts of time-series data
    - For Performance, metrics, logs, trace data etc.
    - Handle multiple data types, formatting, file formats
  - Centralized logging
  - Event stream processing
  - Alerting
  - Built-in statistical functions
  - Visualization library
  - Really FAST.
- ++ Nice to have
  - Query based exploration/ Advanced query language (from Prometheus)
- Killer features:
  - Lambdas
  - ML Stuff
    - *** I am not sure how we can use ML, but I'd rather have a framework, which would let me explore this on my own time – easily.*

OMS / LogAnalytics

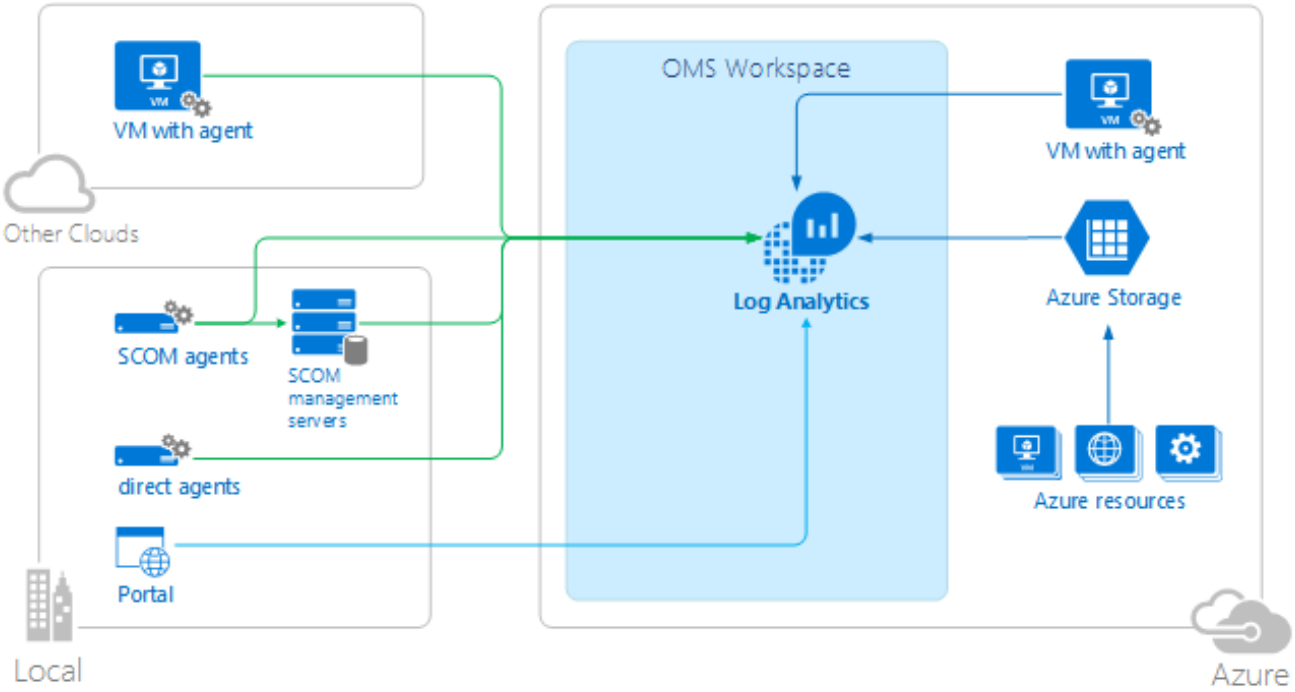
Measure / Query:

- **Server Side metrics:**
  - Calculate server side load –CPU, disk, memory, IOPS
  - Answer → "What resources are running out (resource exhaustion)?"
- **Application Side metrics:**
  - Used to calculate Service Load on components
  - Answer → "What's busy ?"
- **User metrics:**
  - User Experience
  - Answer → "How Slow ?" "Which region is affected?"

Azure LogAnalytics / OMS:

- **What is Azure Log Analytics ?**
  - Azure SaaS solution to aggregate metrics and log data.
  - Helps in solving the "unknown/unknown" problem.
- **How does it work ?**
  - Install agent on servers. Configure agent to push data to a Azure OMS Workspace.
  - Data presents itself in Azure dashboard in near real-time (less than 5 minutes)
- **Why is it better ?**
  - You can focus on the user (CXP – Customer Experience)
  - Query Language
  - Statistical functions – like P95
  - Dashboards.
  - Lambdas
- **Sweet Pricing?**
  - 500 MB /day free
  - $2.3/gb per month
  - Extended retention in Cold Store - $0.10 /GB
  - Export to other Azure properties.
- **Cons**
  - Azure only.

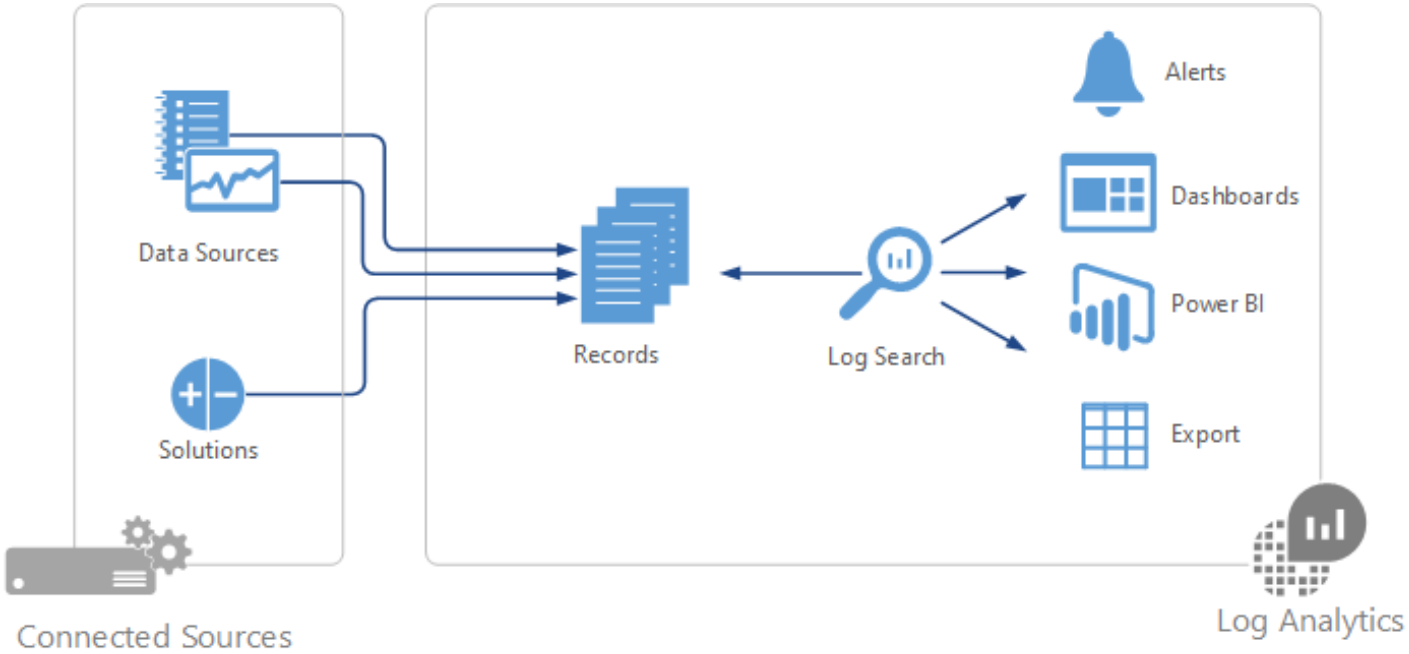
OMS/LogAnalytics Architecture:



Source: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-overview

- Agent Installation - MMA-Agentx64.msi /WORKSPACE-ID= /WORKSPACE-Key= /ACCEPTEULA
- OMS Workspace
- Query Language

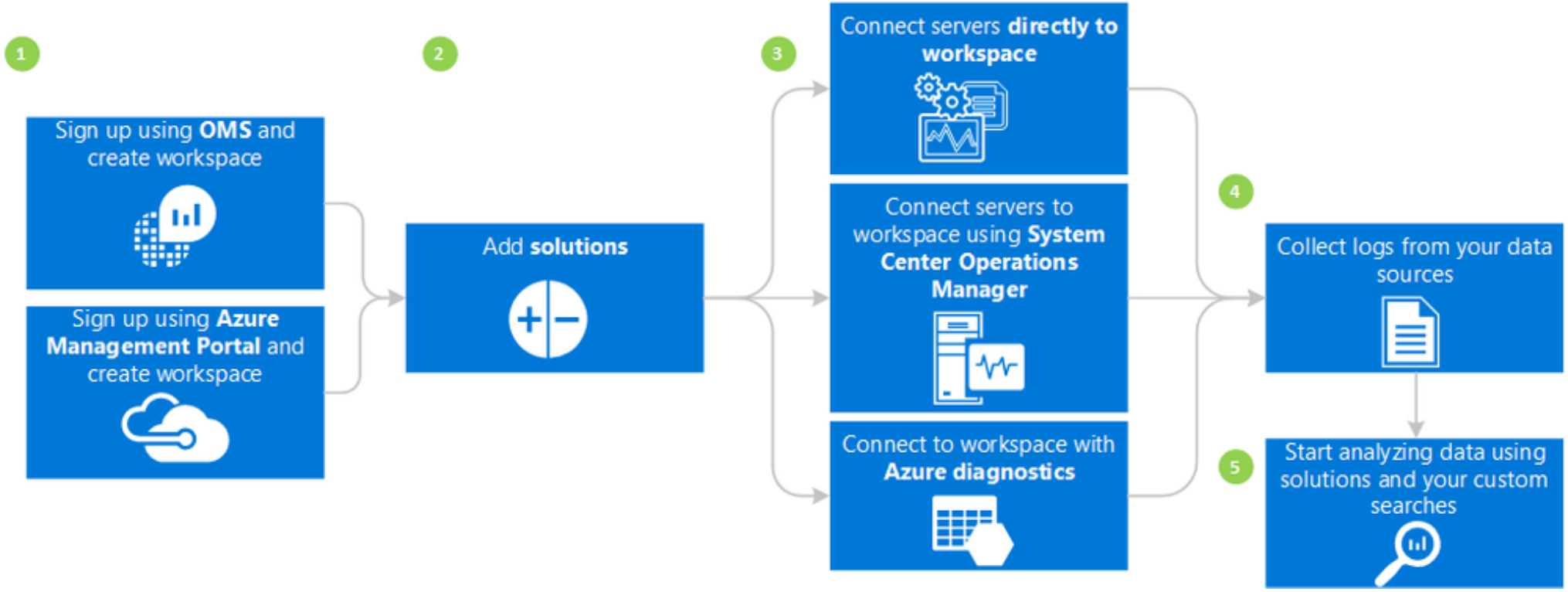
OMS/LogAnalytics components:



Source: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-overview

- **Types of data ingested:**
  - Windows Event Logs + File based logs
  - Perfmon
  - Application level metrics
  - IIS Logs, Custom Logs
  - Linux

Data Ingestion – Overview:



Source: https://techcommunity.microsoft.com/t5/Automation-and-DSC/What-is-Log-Analytics/td-p/36302

Built-in solutions:

Solutions Gallery

Security & Compliance
Antimalware Assessment
Owned
View status of antivirus and antimalware scans across your servers.

Automation Hybrid Worker
Owned
Create Hybrid Runbook Workers to run Automation runbooks on your on-premises servers.

Protection & Recovery
Backup
Owned
Manage Azure IaaS VM backup and Windows Server backup status for your backup vault.

Upgrade Analytics (Preview)
Owned
Use a data-driven approach to streamline and accelerate Windows upgrades.

Insight & Analytics
Network Performance Monitor (Preview)
Owned
Offers near real time monitoring of network performance parameters like loss and latency.

Security & Compliance
Security and Audit
Owned
Provides the ability to explore security related data and helps identify security breaches.

Insight & Analytics
Service Map
Owned
Automatically discover and map servers and their dependencies in real-time.

SQL Assessment
Owned
Assess the risk and health of SQL Server environments.

Activity Log Analytics
Owned
Track all create, update and delete activities occurring in your Azure subscriptions.

Azure Networking Analytics (Preview)
Owned
Gain insight into your Azure Network Security Group and Application Gateway logs

Automation & Control
Change Tracking
Owned
Track configuration changes across your servers

Containers
Owned
See Docker container performance metrics and logs from containers across your public or private cloud environments.

Office 365 Analytics (Preview)
Owned
Get full visibility into your Office 365 user activities, perform forensics as well as audit and compliance.

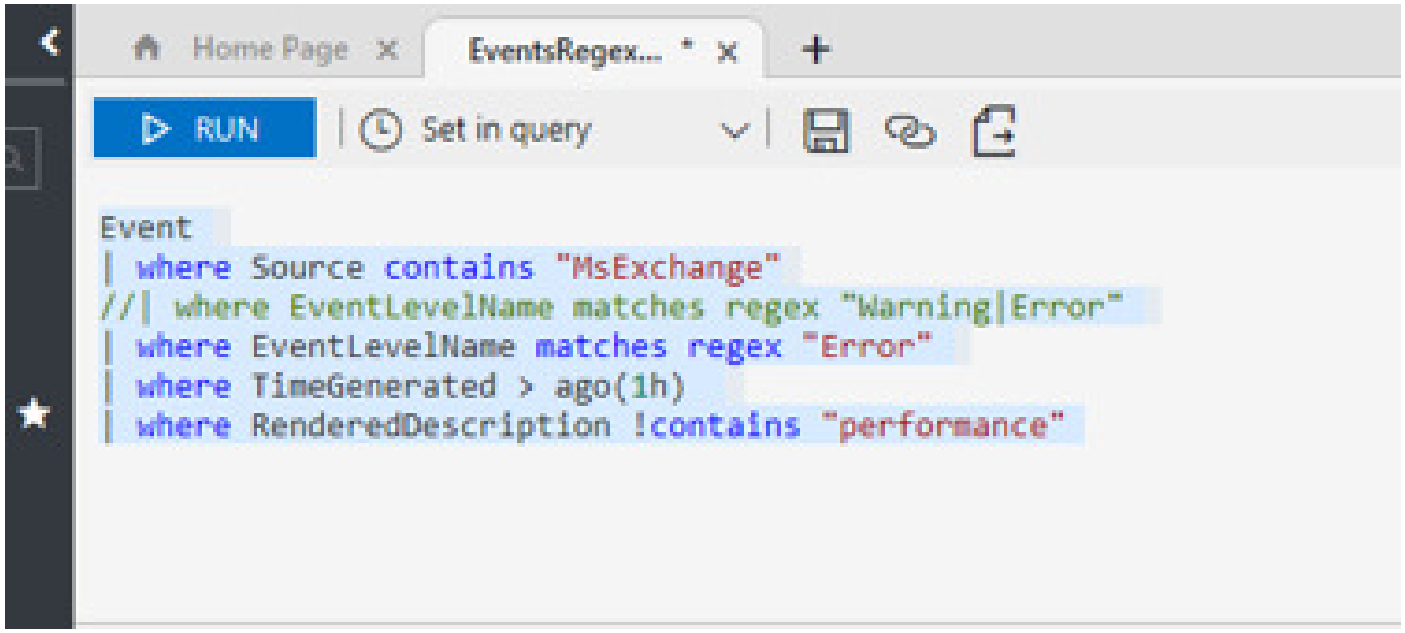
Service Fabric Analytics
Owned
Identify and troubleshoot issues across your Service Fabric cluster

Protection & Recovery
Azure Site Recovery
Owned
Monitor virtual machine replication status for your Azure Site Recovery Vault.

Surface Hub
Owned
Provides the ability to monitor Microsoft Surface Hub devices.

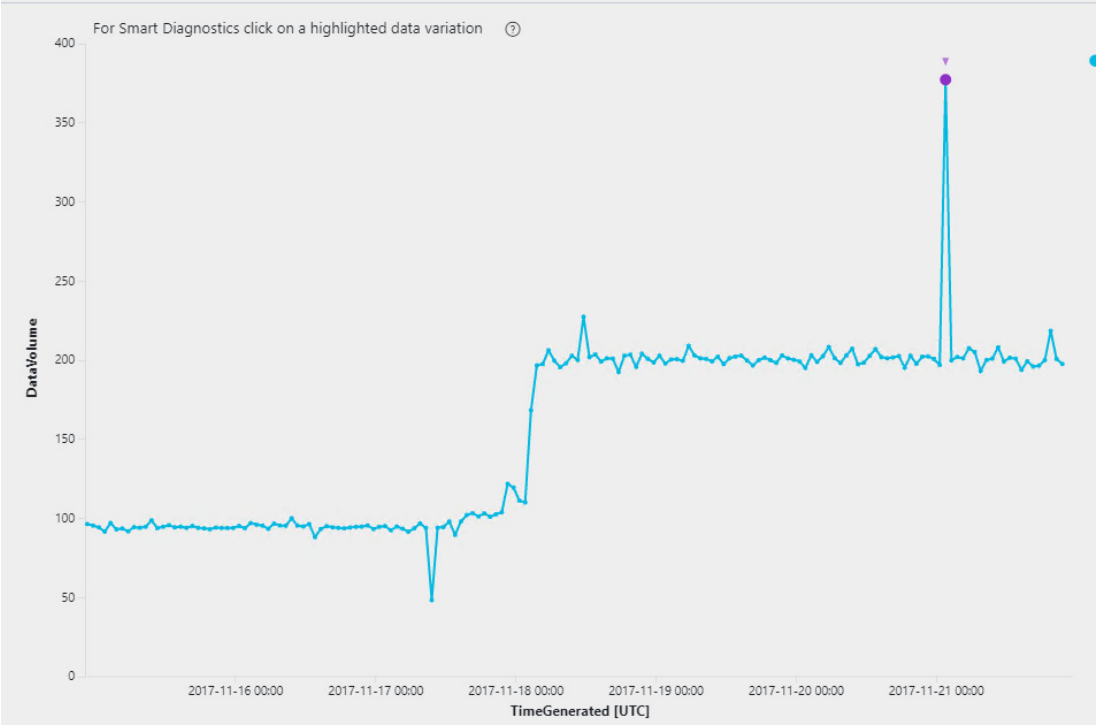
Log Analytics Features:

- **Concept of a Table**
  - Perf | Event |
  - Supports Joins – inner /outer etc.
- Language:
  - Easily understandable, if you know Powershell
- Demo WorkSpace (Playground)
- Language reference: https://docs.loganalytics.io/docs/Language-Reference
- Github Repo:
- Example query



Other cool features:

- *Functions*
- **Lambda patterns****
- Built-in ML
- Alert Manager
- Smart Diagnostics



Demos

In Conclusion:

- Pound for Pound, one of the best Observability stack readily available for Windows.
  - Not sure why many admins are falling head over heals for OMS/LogAnalytics.
  - It's really really cool.
  - Start slow. Explore. Write functions. Try ML
- Something for everybody
  - Managers / Level-1: Turn a query to a dashboard. Display on TV
  - Engineering: Exploration, triage, troubleshooting, correlations.
- Language (AIQL – formerly known as Kusto)
  - Really cool language. Very easy to learn.
  - Under active development.
  - Language reference: https://docs.loganalytics.io/docs/Language-Reference
  - Lack of articles on new query language (AIQL/OQL/Kusto). Need more details.
    - Best ref, so far: https://azure.microsoft.com/en-us/blog/root-cause-analysis-with-in-query-machine-learning-in-application-insights-analytics/
- Github Repo: https://github.com/MicrosoftDocs/LogAnalyticsExamples
- Enterprise Plan:
  - Don't ingest Security Logs.
  - Test with Application/System, IIS, Windows Updates/custom logs
  - Insights from Perfmon data is a good initial payoff.

- @sunnyc7
- github.com/sunnyc7