Corndel Digital.

in association with

Softwire

Workshop: Module 13

Logging, Monitoring & Alerting

Agenda

1000 **Welcome and Register**

Part 1: Logging & Alerts
- Recap (20 mins)
- Exercise (100 mins)

1200 **Lunch Break (1 hour)**

1300 **Part 2: Server Monitoring & Dashboarding**
- Recap (20 mins)
- Exercise (160 mins)

Objectives of this Workshop

- Install & manage logging on an existing cloud application
- Setup analytics for a web application to track logs and metrics
- Setup analytics and dashboards for your cloud infrastructure to quicky identifying the cause of issues when they occur
- Construct dashboards to visualise performance across slices of cloud infrastructure

Corndel Digital.

Softwire

Part 1

Logging & Alerts

Recap

What is Logging?

At its most simplest, logs are a record of events in a system.

Why do we log?

- To debug
- To inspect usage
- To trace performance or outcomes

What do we log to?

- Console
- Server Log File
- Log Aggregation Services

Recap

When should you log?

- Exceptions
- Calls to Other Systems
    - Internal: Databases, other servers or services in your public cloud
    - External: Calls to third party APIs, inbound requests from clients
- Execution of Scheduled Jobs
- Performance Tracing

Recap

What should you log?

- Timestamp
- Log Level: DEBUG, INFO, WARNING, ERROR, CRITICAL
- Stack Trace
- Context Information: Request/Thread Id
- Message explaining what has occurred (do not assume too much prior knowledge)

Be careful not to log personal or sensitive data!

Recap

Alerts

- Set up via alerting “rules”
- When triggered notifications are usually sent to relevant parties
- Can be used to trigger further automated actions
- Proactive rather than reactive

Exercise

Clone this repository and follow the instructions:

https://github.com/CorndelWithSoftwire/DevOps-Course-Workshop-Module-13-Learners

Corndel Digital.

Softwire

Part 2

Server Monitoring & Dashboarding

Recap

Server/Infrastructure Monitoring

Used to track the status of the (often virtual) hardware that your software is running on.

Categories of monitoring:

- OS level system logs: syslog, event viewer
- Protocol specific logs: access logs, SMTP logs
- Cloud platform specific logs: Azure Application Insights, AWS X-Ray
- User activity logs: AWS CloudTrail, Log Analytics for Azure

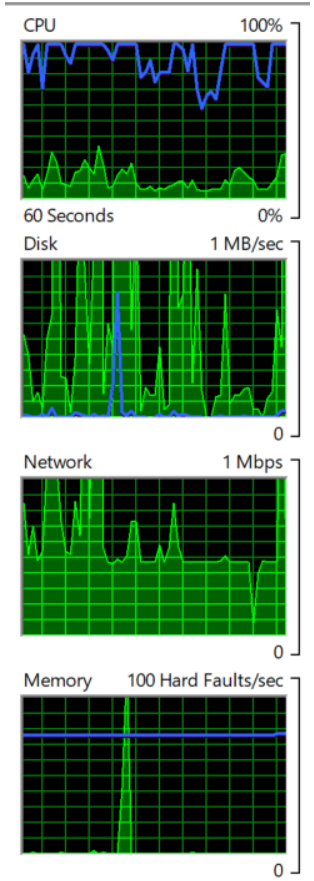
Recap

Monitoring Metrics

Monitoring often tracks the status of a system using various metrics.

Examples of metrics:

- CPU & Memory
  - CPU Core/Threading Utilisation
  - Page File Usage
- Disk Usage
  - Disk Space
  - Read/Write Rate
  - Disk Queue Length
- Network Traffic:
  - Inbound & Outbound Traffic
  - Number of Active Connections/Requests



Recap

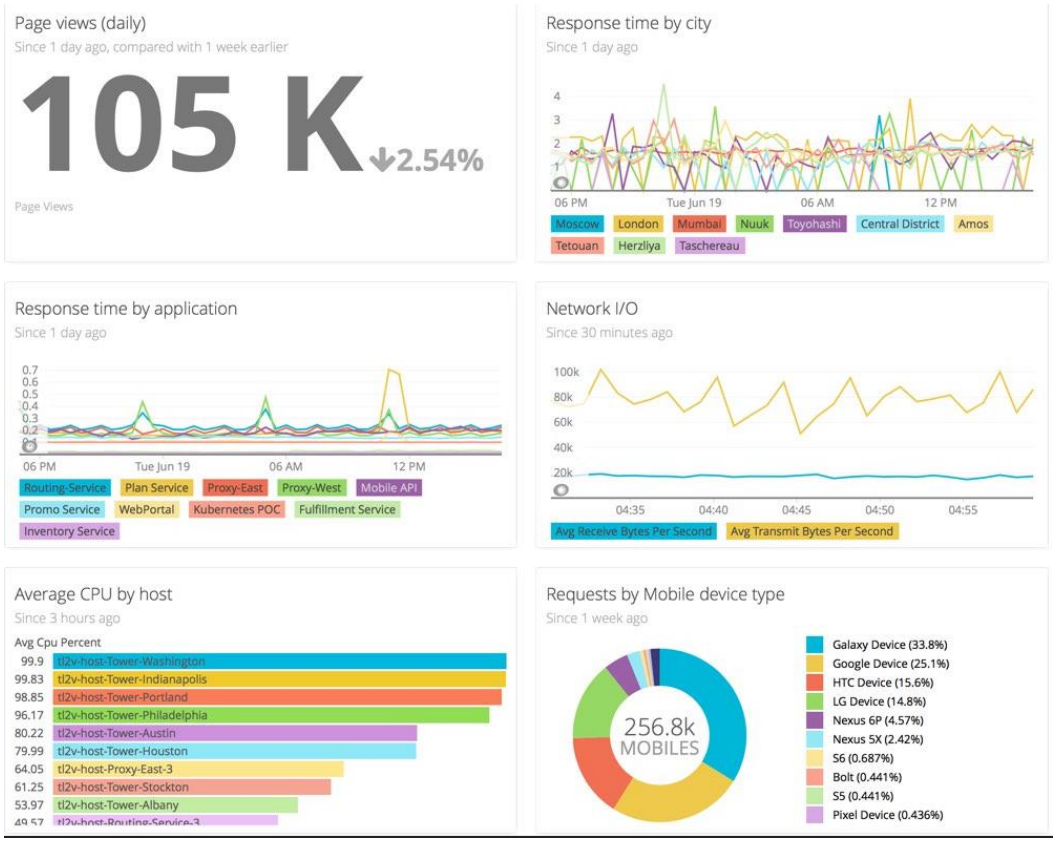
Dashboarding

Provides a concise summary of the available monitoring.

Overview dashboards should be clear and simple to read and analyse (ideally by non-technical staff as well).

Can be used as a starting point for investigations.

- Targeted dashboards focusing on specific areas could be advantageous here.



Exercise

Continue with this morning's instructions

https://github.com/CorndelWithSoftwire/DevOps-Course-Workshop-Module-13-Learners

Corndel Digital.

Softwire

Thank You!

Please Submit Your Feedback Using This Link
Or the QR Code Below: