

*EMEA DevXchange 2017*

# Hands-On Lab: Advanced Techniques for Using the New CA Agile Operations Analytics Platform

Jeff Morris, Principal Engineering Services Architect

Rajat Mishra, Sr. Principal Architect

10 May 2017

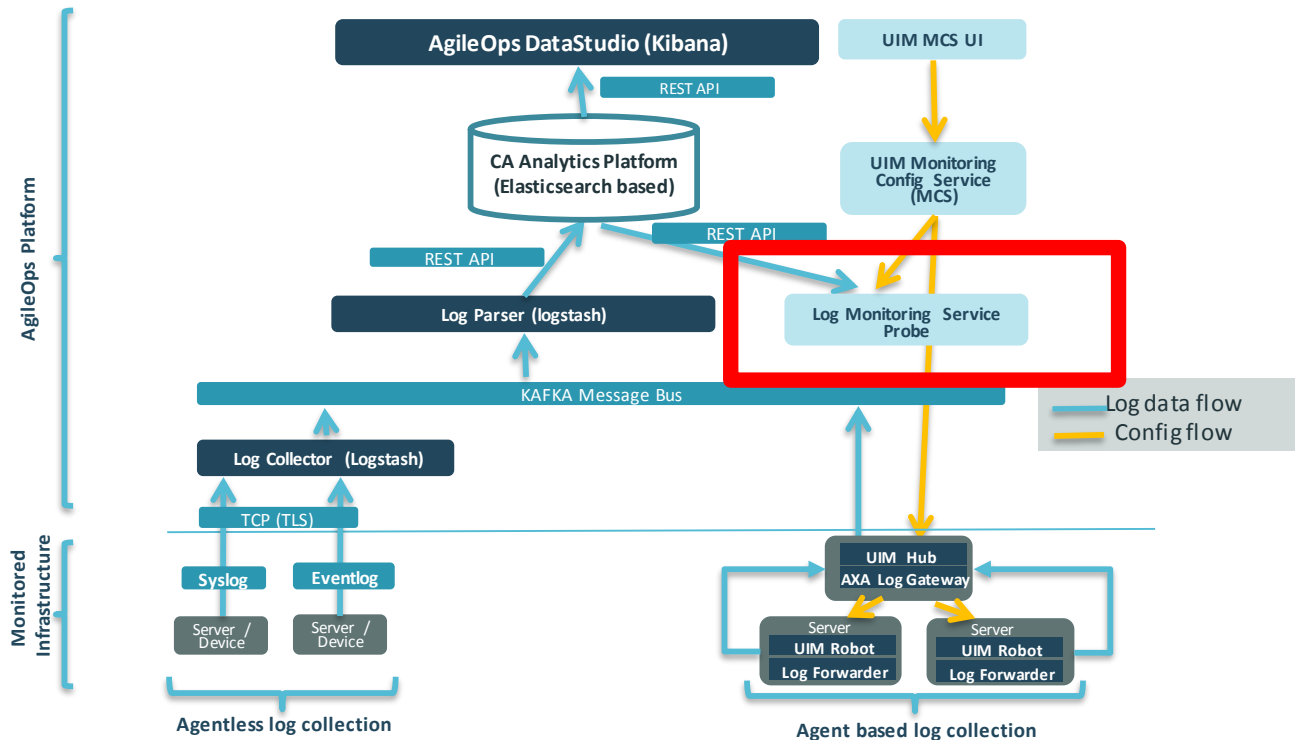


# Analytics Platform and Solution Areas



# Lab Exercise 3 – Log Monitoring Service

## *Continuation of “Introduction to Analytics” Session*



# Lab Exercise 3 – Alarming from Log Events

## *Match Errors*

- Create some errors
  - In the CA Spectrum tab in Chrome, log in (Administrator / CAdemo123)
  - Click around a few times on the tabs across the top to gen traffic
- Look in Data Studio for events matching the criteria
  - Click on Discover Tab
  - Select the “...\*\_logs\_\*...” index
  - In Query search bar enter: **response\_code:[400 TO \*]**
  - Optionally filter on **host** and/or **logtype**

# Lab Exercise 3 – Alarming from Log Events

- Configure CA Unified Infrastructure Management Log Monitoring Service
  - Config workflow
    - In Chrome go back to the CA UIM Portal tab
    - Under “Actions” select “Admin Console”
    - Select “Robots” then click “UIM”
    - Select “Probes”
    - Scroll down to “log\_monitoring\_service” probe
    - Click on the “three dots” icon and choose “Configure”
    - Now click the “three dots” and select “Add New Profile”

# CA UIM Admin Console

Search

Actions ▾ ?

Details Alarms Maintenance

Groups

	Name	Type	
✓	Application Discovery	Container	groups(2) members(0)
!	Operating Systems	Container	groups(2) members(6)
—	Spectrum	Dynamic	groups(0) members(15)

- Advanced Search
- Add Group
- Edit Group
- Delete Group
- Export Group
- Discovery Wizard
- Deploy Robots
- Admin Console**

# Navigating to the Probe in Admin Console

The first screenshot shows the 'Actions' menu with 'Admin Console' highlighted. The second screenshot shows the 'Robots' tab with 'UIM\_hub' selected. The third screenshot shows the 'Probes' tab with 'UIM' selected.

**Screenshot 1: Admin Console**

Search: [ ] Actions ▾

- Advanced Search
- Add Group
- Edit Group
- Delete Group
- Export Group
- Discovery Wizard
- Deploy Robots
- Admin Console**

groups(2) members(0)  
groups(2) members(6)  
groups(0) members(15)

**Screenshot 2: Robots**

Filter [ ] [Refresh] Info **Robots** Archive

Hub

- UIM\_hub

Robots - 6

**Screenshot 3: Probes**

Filter [ ] [Refresh] Info **Probes** Installed F

Robot

Robot	Address
UIM	/UIM_dor
devxlinux	/UIM_dor

Probes

UIM - 192.168.10

# Configuring Log Monitoring Service

The screenshot shows the UIM Admin Console interface. The breadcrumb navigation at the top indicates the path: UIM\_domain > UIM\_hub > UIM. The left sidebar shows a tree view with 'Robot' expanded, and 'UIM' selected. The main content area has tabs for 'Info', 'Probes', 'Installed Packages', and 'Environment Var'. The 'Probes' tab is active, displaying a table of probes. The 'log\_monitoring\_servi...' probe is selected, and a context menu is open with the 'Configure' option highlighted.

Filter	Probe	Port
	fault_correlation_eng..	48041
	hdb	48008
	hub	48002
	log_forwarder	48024
	log_monitoring_servi...	48040

This close-up shows the configuration page for the 'log\_monitoring\_service'. A red box highlights the '+ Add New Profile' button located at the bottom right of the configuration area.



# Lab Exercise 3 – Alarming from Log Events

- Complete the profile with these values:
  - Profile Name: **tomcat\_client\_errors**
  - Active: checked
  - Query Interval: **60 seconds**
  - Log Type: **tomcataccess**
  - Query String: **response\_code:[400 TO \*]**
  - Match Alarm Severity: **MINOR**
- Click “Submit” and then “Save”

# Adding a Log Monitoring Service Profile

Add New Profile

Submit

Profile Name \*

tomcat\_client\_errors

Active

☒

Check Interval (seconds) \*

60

Log Type \*

tomcataccess

Search String \*

response\_code:[400 TO \*]

Send Alarm On Each Match

☒

Match Alarm Message \*

Match found for \$profileName search string \$query in message: \$result

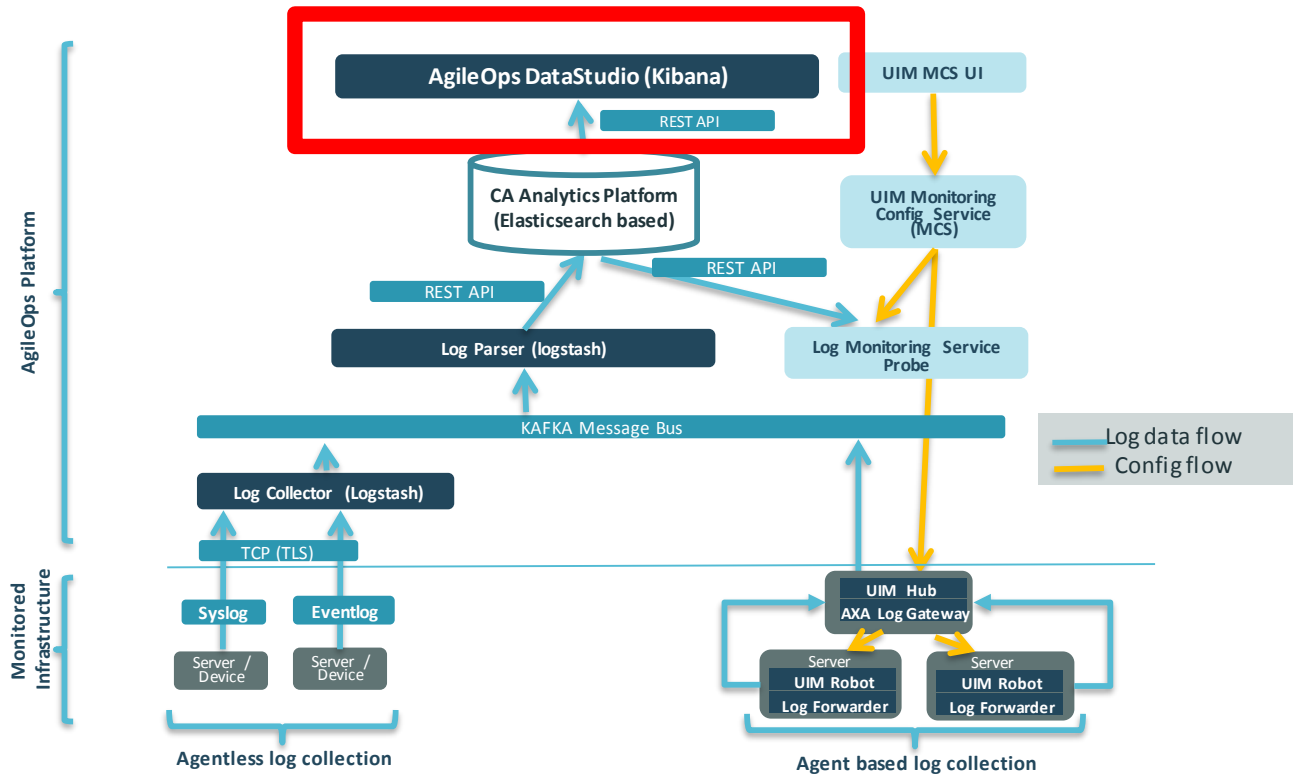
Match Alarm Severity \*

MAJOR

# Lab Exercise 3 – Alarming from Log Events

- Look in CA UIM Portal for alarm after 1-2 minutes
  - Click the Launch in Context icon of the alarm and choose “Log Analytics” to launch directly from CA UIM back to the Dashboard view
- View Alarms in CA Spectrum
  - Go to CA Spectrum tab in Chrome
  - Click “Start Console” to launch OneClick console
  - Sort descending on Date/Time to see in alarm
  - Optionally Launch in Context back to Data Studio

# Lab Exercise 4 – Custom Dashboards



# Lab Exercise 4 – Custom Dashboards

- Create a new Visualization
  - Click “Visualize” tab
  - Select “Add a Line Chart”
  - Select “..... axa\_\*\_logs\_\*
  - Y-Axis (Use down-arrow on left to expand)
    - Aggregation: Average
    - Field: Response time

# Custom Dashboards

## *Creating a Visualization*

The screenshot shows the Splunk web interface. At the top, there are three tabs: 'Discover', 'Visualize' (which is highlighted with a red box), and 'Dashboard'. Below the tabs, there's a section titled 'Create a new visualization' with a 'Step 1' indicator. This section lists three options: 'Area chart', 'Data table', and 'Line chart'. The 'Line chart' option is highlighted with a red box. To the right of these options is a large dialog box titled 'Select a search source'. Inside this dialog, there's a section 'From a new search' and a text input field 'Select an index pattern'. Below the input field, a list of index patterns is displayed. The pattern '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*logs\*' is highlighted with a blue background and a red box around the text 'axa \*logs\*'. Other patterns in the list include '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ajax\*', '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\*', '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\_alarm\_spectrum\*', '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\_inventory\_spectrum\*', '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\_metrics\_spectrum\*', '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*crashes\*', '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*error\*', '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*extension\*', and '345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*is\_func\*'.

Discover Visualize Dashboard

### Create a new visualization

Step 1

- Area chart**  
Great for stacked timelines in which the total of all series is more important than comparing any two change of unrelated data points as changes in a series lower down the stack will have a difficult to
- Data table**  
The data table provides a detailed breakdown, in tabular format, of the results of a composed aggregate charts by clicking grey bar at the bottom of the chart.
- Line chart**  
Often the best chart for high density time series. Great for comparing one series to another. Be careful can be misleading.

### Select a search source

From a new search

Select an index pattern

- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ajax\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\_alarm\_spectrum\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\_inventory\_spectrum\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*ao\_metrics\_spectrum\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*crashes\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*error\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*extension\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*is\_func\_\*
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*logs\***
- 345649d5-6e10-fb3-33c7-f13fb21787e\_axa\_\*logs\_\*

# Lab Exercise 4 – Custom Dashboards

- Create a visualization (cont.)
  - X-Axis
    - Aggregation: Date Histogram
    - Add Sub-buckets
  - Select “Split Lines”
    - Aggregation: **Terms**
    - Field: **Host**
  - Click on green “Play” button to view some results
  - Click the “Save” icon in the upper right of the search bar

# Visualization Details – Web Page Response Time

345649d5-6e10-ffb3-33c7-f13ffb21787e\_axa\_\*\_logs\_\*

DataOptions

metrics

Y-Axis

Aggregation

Average

Field

response time

CustomLabel

Web Page Average Response Time (ms)

+ Add metrics

Advanced

buckets

Select buckets type

X-Axis

Split Lines

Split Chart

buckets

X-Axis

Aggregation

Date Histogram

Field

timestamp

Interval

Auto

CustomLabel

+ Add sub-buckets

Advanced

Select buckets type

Split Lines

Split Chart

Split Lines

Sub Aggregation

Terms

Field

host

Order By

metric: Average response time

Order

Descendir

Size

5

CustomLabel



# Lab Exercise 5 – Java Log4j Logs

- Deploy log4j Log Forwarding profile from CA UIM
  - In UMP, navigate to “DXI” host and click “Monitoring” tab
  - Select “Log Forwarding log4j” Click on “+” to add profile
  - Use the following settings:
    - Profile Name: **aoap\_mdo**
    - Tags: **java,log4j,aoap**
    - File: **/opt/ca/aoap/logs/ca-mdo-server-log.txt**
    - Log Type: **log4j** (should already default)
  - Notice the OOB MCS Template settings
  - Click “Create” to create the profile

# What Questions Do You Have?

THANK YOU!