

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

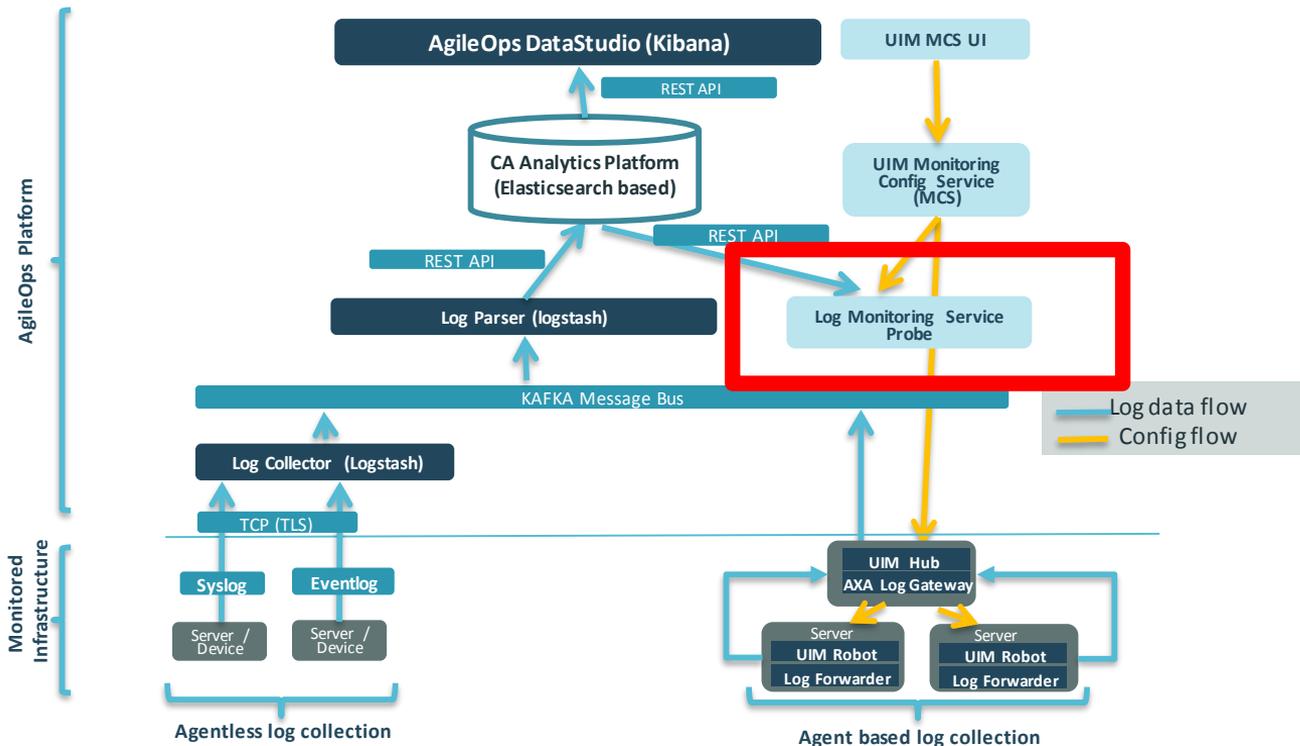


Analytics Platform and Solution Areas



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 image illustrates the navigation process in the CA Admin Console through three sequential screenshots:

- First Screenshot:** Shows the 'Actions' dropdown menu. The 'Admin Console' option is highlighted with a red box. The background shows a 'Hub' view with 'UIM_hub' selected and a 'Robots' tab highlighted in the top right.
- Second Screenshot:** Shows the 'Robots' page. A table lists robots with columns for 'Robot' and 'Address'. The 'UIM' robot is highlighted with a red box. A mouse cursor is pointing at the 'UIM' entry.
- Third Screenshot:** Shows the 'Probes' page. The 'UIM' robot is selected, and the 'Probes' tab is highlighted in the top right. A green progress indicator is visible at the bottom right.

Configuring Log Monitoring Service

The screenshot shows the UIM Admin Console interface. The browser address bar displays `uim/adminconsoleapp/`. The breadcrumb navigation shows `UIM_domain > UIM_hub > UIM`. The main content area is divided into a left sidebar and a main table.

Left Sidebar: A list of robots is shown under the heading "Robot". The "UIM" robot is selected and highlighted with a red box. Other robots listed include `devxlinux`, `dxi`, `jump`, `sag-tixinabox-prod`, and `spectrum`.

Main Table: A table with columns "Probe" and "Port" is displayed. The "log_monitoring_servi..." entry is highlighted with a red box. A context menu is open over this entry, with the "Configure" option selected and highlighted with a red box. Other options in the menu include "Activate", "Deactivate", "Restart", "Delete", and "Raw Configure".

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

The screenshot shows the configuration page for the `log_monitoring_service`. The "UIM" robot is selected. 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 *

Active

Check Interval (seconds) *

Log Type *

Search String *

Send Alarm On Each Match

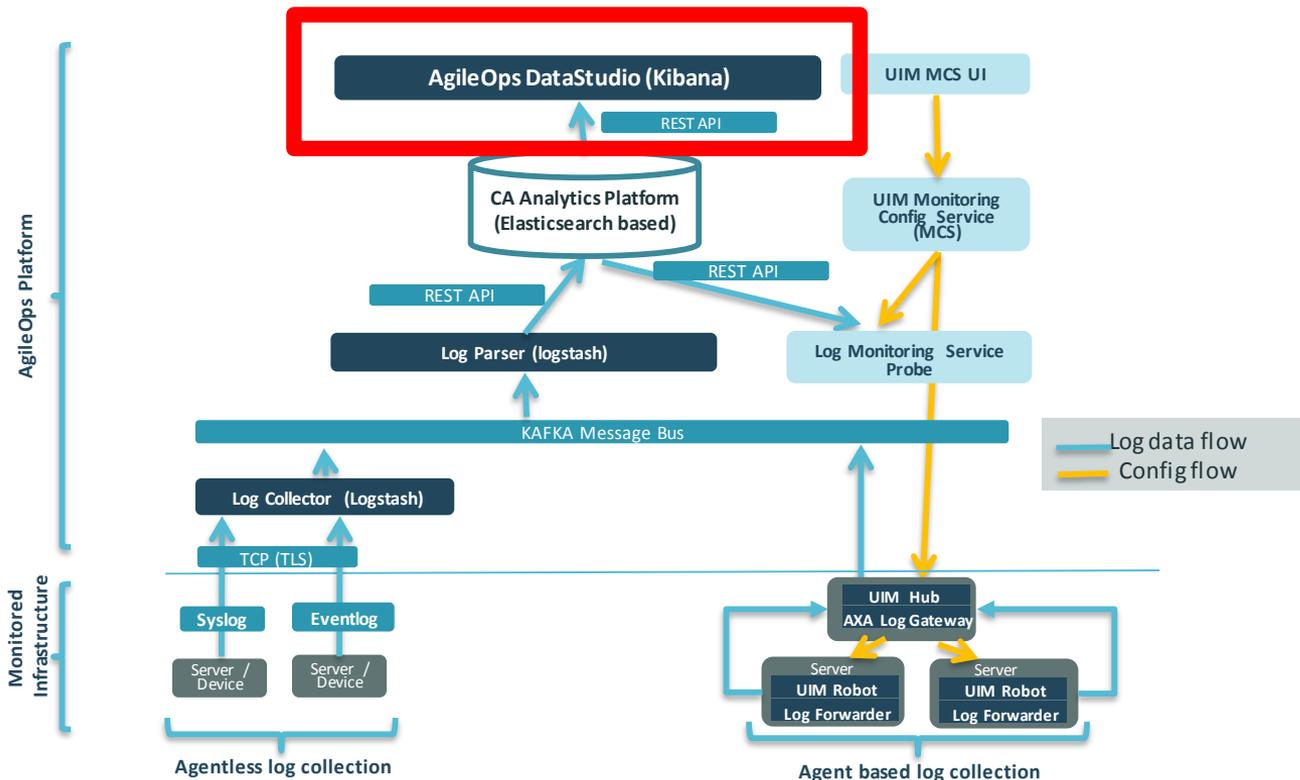
Match Alarm Message *

Match Alarm Severity *

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 interface with the 'Visualize' tab selected. On the left, there are three visualization options: 'Area chart', 'Data table', and 'Line chart'. The 'Line chart' option is highlighted with a red border. On the right, the 'Select a search source' dialog is open, showing a list of index patterns. The pattern '345649d5-6e10-fb3-33c7-f13fb21787e_axa_* logs_*' is highlighted with a blue background and a red border.

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

The image shows a configuration interface for a visualization titled "345649d5-6e10-ffb3-33c7-f13ffb21787e_axa*_logs_*". The interface is divided into several sections:

- metrics**:
 - Y-Axis**: Aggregation is set to "Average".
 - Field**: Set to "response time".
 - CustomLabel**: Set to "Web Page Average Response Time (ms)".
- buckets** (Main):
 - X-Axis**: Aggregation is set to "Date Histogram".
 - Field**: Set to "timestamp".
 - Interval**: Set to "Auto".
 - CustomLabel**: Empty.
- buckets** (Sub):
 - Select buckets type**: "X-Axis" is selected.
 - Sub Aggregation**: Set to "Terms".
 - Field**: Set to "host".
 - Order By**: Set to "metric: Average response time".
 - Order**: Set to "Descendir".
 - Size**: Set to "5".
 - CustomLabel**: Empty.

Red boxes highlight the following elements in the image:

- Y-Axis Aggregation: Average
- Y-Axis Field: response time
- Y-Axis CustomLabel: Web Page Average Response Time (ms)
- X-Axis Aggregation: Date Histogram
- Select buckets type: X-Axis
- Sub Aggregation: Terms
- Field: host
- Order By: metric: Average response time
- Order: Descendir
- Size: 5
- Add sub-buckets button

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!