



The bridge to possible

How Cisco TAC solves your infrastructure and application problems faster using Machine Learning

Gavin Cohen, VP Product Management, ScienceLogic
@gcohen222

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



The Cisco TAC

- 191 countries served
- 11,000+ engineers
- 60,000+ partners worldwide

- 2.2 million cases handled annually
- \$18.5 billion+ in spare parts inventory
- 11 global CX centers

Goal—resolve and figure out root cause



Majority of SRs (cases) solved in < 24 hours

But... Toughest cases require laborious log analysis



Thousands of hours
spent each month

Hunting through logs is really hard

- Customer uploads log bundle
- Find/guess the right logs within bundle
- Start searching for errors or known key words (often symptoms)
- Hunt around for new/rare/unexpected log lines
- Leverage intuition and experience...
- Iterate until root cause is found

```
2021-12-04 18:28:32,221 INFO org.springframework.boot.StartupInfoLogger [main] Starting LoggingDemoApplication using
Java 1.8.0_212 on VMAL12819 with PID 3568
2021-12-04 18:28:32,223 DEBUG org.springframework.boot.StartupInfoLogger [main] Running with Spring Boot v2.6.0, Spring
v5.3.13
2021-12-04 18:28:32,224 INFO org.springframework.boot.SpringApplication [main] No active profile set, falling back to
default profiles: default
2021-12-04 18:28:33,789 INFO org.springframework.boot.web.embedded.tomcat.TomcatWebServer [main] Tomcat initialized
with port(s): 8080 (http)
2021-12-04 18:28:33,798 INFO org.apache.juli.logging.DirectJDKLog [main] Initializing ProtocolHandler [http-nio-8080]
2021-12-04 18:28:33,799 INFO org.apache.juli.logging.DirectJDKLog [main] Starting service [Tomcat]
2021-12-04 18:28:33,799 INFO org.apache.juli.logging.DirectJDKLog [main] Starting Servlet engine: [Apache
Tomcat/9.0.55]
2021-12-04 18:28:33,875 INFO org.apache.juli.logging.DirectJDKLog [main] Initializing Spring embedded
WebApplicationContext
2021-12-04 18:28:33,875 INFO org.springframework.boot.web.servlet.context.ServletWebServerApplicationContext [main]
Root WebApplicationContext: initialization completed in 1588 ms
2021-12-04 18:28:34,212 INFO org.apache.juli.logging.DirectJDKLog [main] Starting ProtocolHandler [http-nio-8080]
2021-12-04 18:28:34,230 INFO org.springframework.boot.web.embedded.tomcat.TomcatWebServer [main] Tomcat started on
port(s): 8080 (http)
```

```
03/22 08:52:50 INFO .....init_policyAPI: RegisterWithPolicyAPI: Writing to socket = 22
03/22 08:52:50 INFO .....init_policyAPI: ReadBuffer: Entering
03/22 08:52:51 INFO .....init_policyAPI: ReadBuffer: Exiting
03/22 08:52:51 INFO .....init_policyAPI: RegisterWithPolicyAPI: Exiting
03/22 08:52:51 INFO .....init_policyAPI: Policy API initialized
03/22 08:52:51 INFO .....rpapi_getPolicyData: RSVPIndActionName: Entering
03/22 08:52:51 INFO .....rpapi_getPolicyData: ReadBuffer: Entering
03/22 08:52:51 INFO .....rpapi_getPolicyData: ReadBuffer: Exiting
03/22 08:52:51 INFO .....rpapi_getPolicyData: RSVPIndActionName: Result = 0
03/22 08:52:51 INFO .....rpapi_getPolicyData: RSVPIndServiceDetailsOnActionName: Entering
03/22 08:52:51 INFO .....rpapi_getPolicyData: RSVPIndServiceDetailsOnActionName: Result = 0
03/22 08:52:51 INFO .....api_reader: appl chose service type 1
03/22 08:52:51 INFO .....rpapi_getSpecData: RSVPGetSpec: Entering
03/22 08:52:51 INFO .....rpapi_getSpecData: RSVPGetSpec: Result = 0
03/22 08:52:51 INFO
[Sun Dec 04 05:12:26 2005] [notice] jk2_init() Found child 25803 in scoreboard slot 8
[Sun Dec 04 05:12:28 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 05:12:28 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 05:12:28 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 05:12:28 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 05:12:30 2005] [notice] jk2_init() Found child 25805 in scoreboard slot 9
[Sun Dec 04 05:12:30 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 05:12:30 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 05:15:09 2005] [error] [client 222.166.160.184] Directory index forbidden by rule:
/var/www/html/
[Sun Dec 04 05:15:13 2005] [notice] jk2_init() Found child 1900 in scoreboard slot 10
[Sun Dec 04 05:15:16 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 05:15:16 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 06:01:00 2005] [notice] jk2_init() Found child 32347 in scoreboard slot 6
[Sun Dec 04 06:01:00 2005] [notice] jk2_init() Found child 32348 in scoreboard slot 7
[Sun Dec 04 06:01:21 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 06:01:21 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 06:01:30 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 06:01:42 2005] [notice] jk2_init() Found child 32352 in scoreboard slot 9
[Sun Dec 04 06:01:42 2005] [notice] jk2_init() Found child 32353 in scoreboard slot 10
[Sun Dec 04 06:01:42 2005] [notice] jk2_init() Found child 32354 in scoreboard slot 6
[Sun Dec 04 06:02:01 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 06:02:02 2005] [error] mod_jk child workerEnv in error state 7
[Sun Dec 04 06:02:05 2005] [notice] jk2_init() Found child 32359 in scoreboard slot 9
[Sun Dec 04 06:02:05 2005] [notice] jk2_init() Found child 32360 in scoreboard slot 11
[Sun Dec 04 06:02:05 2005] [notice] jk2_init() Found child 32358 in scoreboard slot 8
```

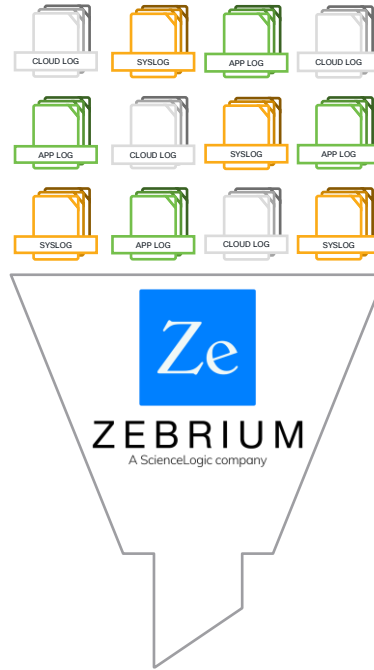
There has to be a better way!



ZEBRIUM

A ScienceLogic company

ScienceLogic Zebrium



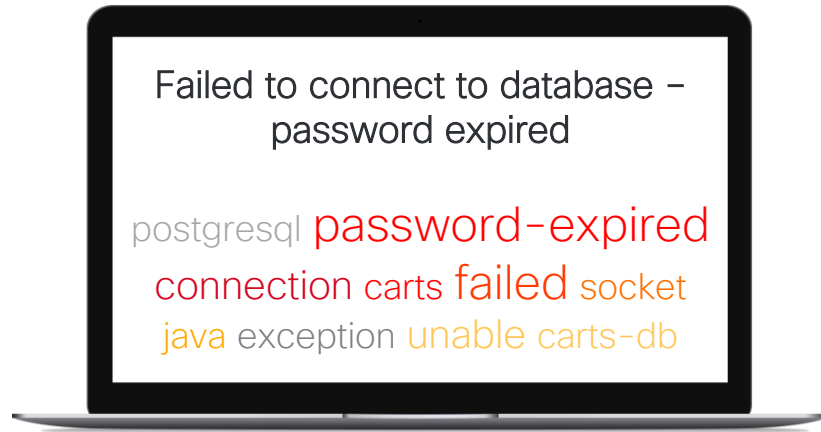
Logs go in

Root cause comes out!

Instead of this...



See root cause without hunting or digging through logs



Automated root cause analysis



Accuracy in < 24 hours



No rules or manual training

Man vs. Machine



Can ML analyze logs faster than human experts?



UCS

4



DNAC

Product lines



Webex Client



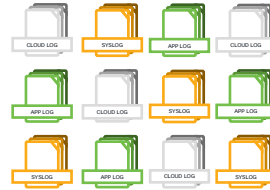
ISE

192

Complex customer cases

Man

Expert engineers



Many hours to days spent:

- Analyzing each log bundle
- Often escalating

Machine

ScienceLogic Zebrium



Minutes (automatic):

- No manual rules
- No pre-training

95.8% – Zebrium correctly found root cause

Some color from the Zebrium users

“Didn’t just highlight the connection error but also the reason.”

“Caught errors I would have normally missed among millions of logs and led me to the root cause.”

“This is amazing. It wasn’t an easy issue to troubleshoot, and it pointed us at exactly the right root cause.”

Demo



How does
it work?





LOG_1.... LOG_N

Log streams or files are sent to Zebrium in native format. No need for structuring or parsing rules.

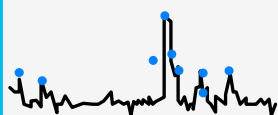
```
11652 2016-08-09
00:15:34.977532
INFO regmgr:axr_startsd:Mismatch
corrected at coff 278095203957
```

	Mismatch corrected at coff
Pid	11652
ttz	2016-08-09
Event Type	00:15:34.977532
Severity	INFO
Module	regmgr
Function	axr_startsd
coff	278095203957

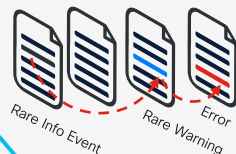
- 01 **Structuring and categorization**
Unsupervised machine learning automatically structures and categorizes log events.

Event_1.....
Event_2
Event_N

- 02 **Pattern learning**
The patterns are learnt for each type of log event.



- 03 **Anomaly Detection**
Each new incoming event is scored based on how anomalous it is.



- 04 **Identification of correlated anomalies**
The ML looks for correlated clusters of anomalies across logs.

NLP summary and word cloud



- 05 **Summarization**
Relevant key words are extracted and GPT-3 is used to produce a plain language summary.

Root Cause Report

Summary

Shopping cart crashed: out of memory

Root cause indicators & symptoms

Oct 9 13:38:29
Oct 9 13:38:29
Oct 9 13:38:30
...



RCA fingerprinted for future occurrences

Interactive root cause report generated and sent as a "suggested alert"

Connects with existing tools and workflows

AIOps

ScienceLogic

APM and observability

APPDYNAMICS
part of Cisco

Elastic Stack

new relic

DATADOG

dynatrace

Incident response and collaboration*

slack

ATLASSIAN
Opsgenie

VictorOps

OpsRamp

PagerDuty

Webex Teams

Microsoft Teams

Works with logs from any infrastructure or application

*additional tools supported through ScienceLogic integration

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Logs go in, root cause comes out

- No training or rules
- Works with any logs
- Sign-up for a free trial:
sciencelogic.com/request-a-free-trial

ScienceLogic



Visit us at booth C05



The bridge to possible

Thank you

CISCO *Live!*

