TechLineage

Cogniyug

Case Study of

A cloud based IT Infrastructure provider

Background

Customer Name : Anonymous (Can't be disclosed)

Business of the customer : Cloud based IT Infrastructure Management company with its solution hosted in a public cloud. Manages IT infrastructure of its customers using its proprietary hosted solution in the cloud. Key solutions include Asset Discovery (both software and hardware), Real Time Monitoring of the IT infrastructure and Change Management

Cogniyug's role: A complex solution hosted in a cloud serves to many end customers. It is extremely important that this solution is up and running all the time and meets desired quality of service. The key failures in the system needs to be diagnosed and corrected quickly to minimize the downtime and reduce MTTR. Accurate and quick root cause analysis is extremely important and that's where Cogniyug plays a critical role. Application logs, database logs, syslogs and monitoring events are analyzed together to quickly pinpoint the root cause of key failures.

Cogniyug is effectively used to ascertain the effect of certain important events / sequence of events.

Cogniyug's predictive alerting capabilities are used to predict the failure events before they actually happen.

Besides, Cogniyug is used routinely to understand the normal and abnormal behaviors of the system.

It also serves as a cost effective log archival tool.

This customer intends to extend this solution as a paid service to its end customer.

Data Sources

Monitoring Events and Log files

- ✓ Monitoring Events : Customer has a basic monitoring infrastructure installed on each server that generates type of following events
  - Threshold breach events

    Static thresholds are defined on resources like CPU, Memory, Disk I/O, Network I/O etc. Events are raised when thresholds are breached indicating a resource crunch
  - Service UP/Down events

    Services and processes are monitored. UP/DOWN events are raised accordingly.
  - Configuration Change Related events

    Configuration of the OS, Applications etc are monitored and events are raised when a change in the configuration is made.
- ✓ Log files
  - Syslogs from Unix servers and Windows Event logs from Windows servers
  - Log files generated by the No-SQL Database
  - Application logs in the log4j format
  - Web logs generated by the nginix web servers

Data Collection

- Cogniyug Data collector probe is NOT installed on each server. This is because the customer sends both monitoring events and log messages to a RabbitMQ server. A single data collection probe is installed that consumes the stream of these messages continuously by directly connecting to the RabbitMQ server using a simple python client.
- Cogniyug polls per 60 seconds to read all the available messages. Reads approximately 0.1MB (1000 monitoring events + log messages) each time .
- The data gets normalized by separating the time stamp field from the message body.
- A source tag is added as the METATDATA indicating the originating server, name of the log file etc.

Root Cause Analysis (RCA)

Many critical events are being analyzed using the RCA feature of Cogniyug. Some of them are:-

- ✓ User response time degradation
- ✓ Returning of e-mails
- ✓ Compactation of the database
- ✓ Memory pressure issues on the database process
- ✓ Service down events

Customer was able to pinpoint the cause of

- ✓ Events of ‘similar’ types
- ✓ Exact ‘instances’ of the events

At a single click of mouse

Complex casual relationships were uncovered with

- ✓ Confidence
- ✓ Time relevance and
- ✓ Support measures

Effect Analysis

Cogniyug is used to identify the effects of some key events, including

- High resource utilization events
- Configuration Change related events
- Service UP/DOWN events

Cogniyug helped to understand following facts

- Events in isolation did not have critical effects
- Events, when happened in combination with certain events have serious impacts
- Consequences of configuration related changes

Customer can now

- Distinguish critical Vs non-critical events
- Understand the effects of changes better to take more informed decisions

Predictive Alerts

- ✓ Predictive Alerts were defined for key failures.
- ✓ Root Causes were analyzed using the RCA and after satisfied results were obtained, predictive alerts were defined.
- ✓ Data is continuously collected using the 'Data Collection' mechanism explained on pg 4
- ✓ The prediction model learns new causes as they are discovered every time
- ✓ Close to 'real time' predictions are made and custom actions (scripts) are executed when prediction models meet the predefined threshold.
- ✓ Latency : Data Collection happens every 1 minute and hence a maximum latency of 1 minute is theoretically possible from the point the data is made available to Cogniyug

Expected Patterns

- Cogniyug provides an amazing functionality called ‘Watch Points’
- ‘Watch Points’ watch for expected patterns and alert when expected things don’t happen in expected time.
- Exactly opposite of predictions but very handy to monitor expected patterns
- Cogniyug was used to identify the expected patterns and ‘watch points’ were defined on selected patterns
- Custom actions (scripts) are defined that get executed when certain ‘watch points’ trigger i.e. “when expected patterns don’t happen in expected time”

Complex searches

Customer uses Cogniyug

- ✓ To search through GBs of log data
- ✓ To create complex search criteria and analyze the data within customized search results for patterns, causes and exact causes
- ✓ Visualize time density of the events matching the search criteria
- ✓ Example:- Does ‘compacting of the database’ affect the ‘end user experience’?

Deployment, Scalability etc

- ✓ Deployment : In the cloud

- ✓ H/W and Software Components:

  WebServer, Application Server, Cassandra DB and the RabbitMQ client collecting streaming logs were deployed on a single Linux VM with following configuration:

  RAM 16GB, Storage 1TB, CPUs 4

  OS: Cent OS 6.4

  Pattern mining Grid was installed on a separate Linux VM with following configuration :

  RAM 8GB, Storage 100GB, CPUs 4

  OS: Cent OS 6.4

TechLineage

What next?

- Do you have complex IT logs coming from various sources?
- We would be keen to perform a free PoC (on your premise or in our cloud)
- We can work with stale data and promise to show value in 24 hours after the data is consumed inside Cogniyug.
- Write to us on info@techlineage.com to initiate a dialogue for PoC
- Your data privacy is our top priority. We comply to you data privacy standards by signing required NDAs and other agreements

TechLineage

Thank you !

Question ??

Write to us on info@techlineage.com