Putting your z/OS Operational Data to Work

How to apply analytics to your Operational Data

Paul Hall – IBM Z – ITSM and Security Technical Specialist
phall@ca.ibm.com
April, 2018
We are dependent on IT everyday…. and IBM Z is a big contributor

30 billion business transactions per day

$6 trillion in card payments annually

7 million people and $90B in trade crossed our Canadian boarders in Dec. 2017

27+ million personal tax returns processed by CRA

48.1 million passengers flew on Air Canada in 2017

- Insurance policies, claims and payments.
- Securities exchanges and settlement
- Retail sales
Analysis of Operational Data can help achieve Operational Excellence

1. **Cost**: Unlock your investments  
   - *Improve efficiency and reduce costs*  
     IT Operations Analytics can help you reduce your operational expense and run your IT applications more efficiently

2. **Risk**: Reduce blind spots  
   - *Proactively avoid outages and reduce blind spots*  
     Proactively identify issues before they happen and significantly improve mean time to resolution

3. **Agility**: Faster for experts, easier for beginners  
   - *Faster and easier time to market*  
     Solve problems faster using the tooling or your choice to aid experienced operators a new starters

A recent survey of Z clients showed *cost reduction* and *outage prevention* as the top 2 factors where they want to focus operational efforts.
What is z/OS Operational Data?

- **SMF**
  
  *System management facilities (SMF) collects and records system and job-related information. Useful to understand resource usage, throughput, I/O and security for applications on z/OS.*

- **Log data**
  
  *z/OS syslog, USS syslogd, and other logs are a chronological record of ‘message’ based information for the operating system, system services and active applications. Useful to understand exceptions (error and action messages) and a source for messages from different system/application components.*

- **Application Logs**
  
  *Application defined data. Can represent business state/status or any other information as defined by that application programmer.*
Format for z/OS operational data

**SMF records**
- Hundreds of different types / sub-types
- Defined and structured format
- EBCDIC formatted data

**Log data**
- Individual logs have different formats but they are mostly structured
- Usually contains time stamps and in chronological format
- EBCDIC formatted data

**Application data**
- Application defined format… could be almost anything
What needs to be done to the data?

**Data collection**
- Connect to the different data sources

**Queuing**
- Some level of queuing to make sure no data is lost

**Filtering**
- Only want to send some of the data on for analysis

**Transformation**
- Separate records (CSV)
- JSON wrapper
- EBCDIC to UTF8 format

**Transport**
- Send data to target system for analysis

IBM Common Data Provider for z Systems
IBM Common Data Provider for z Systems targets

**IBM Operations Analytics for z Systems**
- IBM program product for processing and analyzing Z operational data
- Support for z/OS and Linux on IBM Z
- Also contains the machine learning tool… ZAWARE

**ELK**
- Open Source software / commercial products
- Elasticsearch, Logstash, Kibana (data storage and analytics search engine, log collection and transformation, visualization of Elasticsearch data)

**Kafka**
- Open Source data streaming platform
- Must adopt some client technology to perform reporting

**Splunk**
- Splunk analytics product
- Widely adopted for ingestion and analysis of Windows, UNIX and Linux operational data
ELK: Art of the Possible
ELK: A simple selection list for Z data
ELK: Problem dashboard for CICS and Db2
ELK : Sample Data
ELK : Sample Data
ELK: Sample Data
ELK : Sample Data
ELK : Sample Data
ELK : Sample Data
ELK : Sample Data
ELK : IBM CDPz Ingestion kit
In Splunk you can create a dashboard based on key IBM Z performance metrics to get quick visualizations of hot spots on the system.
Within the same interface you can diving deeper into the key performance metrics gives you an at a glance view of the system over time and when key error events are hitting the system: DB service response time increased during last minutes.
Splunk: Visualizing Z log details

Deep dive in the log related to that service to quickly take down to the root cause of the problem.
Splunk – System dashboards
IBM Operations Analytics for z Systems: CICS regions hitting resource limits
IBM Operations Analytics for z Systems: Dashboard for Change Impact Analysis

Message distribution before and after system maintenance
<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Data Provider official page:</td>
<td><a href="ibm.biz/CDPzInfo">ibm.biz/CDPzInfo</a> - Product summary and contacts</td>
</tr>
<tr>
<td>ELK / CDPz Sample:</td>
<td><a href="https://ibm.co/2FaLoq7">https://ibm.co/2FaLoq7</a> - Try it out yourself…thanks to David Willoughby (I found that ELK v5.6.7 worked best for Windows 10)</td>
</tr>
<tr>
<td>ELK / CDPz Whitepaper:</td>
<td><a href="https://ibm.co/2FduvLG">https://ibm.co/2FduvLG</a> - IBM paper produced by Washington Systems Center</td>
</tr>
<tr>
<td>CDPz on Splunkbase</td>
<td><a href="https://splk.it/2qTJ69L">https://splk.it/2qTJ69L</a> - Common data provider samples on Splunkbase</td>
</tr>
<tr>
<td>CDPz and IBM Operational Analytics for z Systems</td>
<td><a href="https://ibm.co/2qVFyoq">https://ibm.co/2qVFyoq</a> - IBM Analytics solution for Operational data</td>
</tr>
<tr>
<td>ITSM News Letter</td>
<td><a href="https://ibm.biz/zITSMNewsletter">https://ibm.biz/zITSMNewsletter</a> - Subscribe to the newsletter for information, announcements, events, etc</td>
</tr>
</tbody>
</table>
Questions ?
The IBM Common Data Provider for z Systems (CDPz) collects IT operational data through a single interface, providing structured and unstructured data in near real time to a variety of analytics solutions. Data can be provided both on and off platform in a consistent, consumable format.

IBM Common Data Provider for z Systems allows you to:

- Access data with analytics tools within minutes.
- Collect data once and provide multiple different end users and products with the data they need.
- Filter the data to target specific use cases and reduce data volumes and network traffic.
- Batch data collection also available for deep dive analysis or to control CPU consumption.
- Documented protocols and formats for sending and consuming data are provided, enabling data ingestion to widely used Industry Analytics Platforms or Enterprise-specific solutions for access and analysis.

Open ecosystem: The Common Data Provider (CDP) is the standard way to gather operation analytics data for analytics engines such as Splunk, ELK and IBM products like IBM Operations Analytics for z Systems (IOAz) to enable them to prevent impact to business, optimize costs and efficiencies and reduce risk through proactive analysis of data in near real time.

Vision and Purpose

An interactive framework for combining multiple views of the same data to provide a deeper understanding of the Enterprise.