Transforming Cloud Services by Realizing Value of it’s Data

Philip Sow, CISSP | CEH, Sales Engineering Manager SEA
Broad Spectrum of Services

- Systems Integrators
- IT Outsourcing
- Managed Services

Global

- Wipro
- IBM
- Accenture
- Tata
- BDS
- CSC
- Infosys
- NTT Communications
- Sungard
- BT
- Unisys
- Dell
- AT&T
- Ciber
- Carpathia

National

- Deloitte
- GlassHouse
- Navisite
- GoGrid
- Quality

Regional

- Perimeter
- Hurricane Labs
- CompuCom
- Rackspace Hosting

Cloud Services

- IaaS
- PaaS
- SaaS

Global

- Windows Azure
- Amazon Web Services
- Salesforce
- NetSuite
- Workday
- SuccessFactors

National

- Verox
- Heroku

Regional

- Intermedia
Cloud Computing Challenges

Cloud Providers

• Need deep visibility across massive, scaled-out, distributed infrastructure to meet service levels

• Need to secure the shared environment and prove compliance

• Need to understand usage analytics (internally as well as for customers)
Many ‘Single Panes of Glass’
What It’s Like In The Trenches

Log call. The console says everything is green. **ESCALATE.**

Java monitoring tools don’t show anything either. Call the developer. **ESCALATE.**

Stop working on new code to troubleshoot. Need production logs! **ESCALATE.**

Stop current task to identify and gather production logs for developer. **ESCALATE.**

Manual investigation establishes not application problem. **RESPOND.**

DBA analyzes audit logs which points to bad query. **ESCALATE.**

NOW WHAT?
Can it be done in a easier way?

Sources

ORDER,2012-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"},
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if
you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}
### Machine Data Contains Critical Insights

#### Sources
- Order Processing
- Middleware Error
- Care IVR
- Twitter

#### Table: Machine Data Insights

<table>
<thead>
<tr>
<th>Time Waiting On Hold</th>
<th>Customer ID</th>
<th>Order ID</th>
<th>Product ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>15/04/2012 09:20</td>
<td>0569281734</td>
<td>10098213</td>
<td></td>
</tr>
<tr>
<td>05/21 16:33:11.238</td>
<td>0569281734</td>
<td>10098213</td>
<td>123456789</td>
</tr>
<tr>
<td>05/21 16:33:11.242</td>
<td>0569281734</td>
<td>10098213</td>
<td>123456789</td>
</tr>
</tbody>
</table>

#### Orders

<table>
<thead>
<tr>
<th>ORDER, 2012-05-21T14:04:12.484</th>
<th>10098213</th>
<th>569281734</th>
<th>67.17.10.12,43CD1A7B8321SA-2100</th>
</tr>
</thead>
</table>


#### Customer's Tweet

```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:"http://dallascowboys.com"},location:{displayName:"Dallas, TX"},objectType:"person",preferredUsername:"BoysFan80",statusesCount:6072},text:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}
```
Machine Data Contains Critical Insights

Sources
- Order Processing
- Middleware Error
- Care IVR
- Twitter

- Customer ID
- Order ID
- Product ID
- Time Waiting On
- Customer’s Tweet
- Customer ID
- Twitter ID
- Company’s Twitter ID

ORDER, 2012-05-21T14:04:12.784, 10098213, 569281734, 67.17.10.12, 43CD1A7B8321, SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException. Could not create pool. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type 98#1, DNIS 5555685981, ServID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk 1451.16
05/21 16:33:11.242 [SCREENPOPEVENT] ServID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] ServID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor: {displayName:"Go Boys!!", followersCount: 1366, friendsCount: 789, link: "http://dallascowboys.com/"}, location: {displayName:"Dallas, TX", objectType: "place", coordinates: [29.959081, -96.921080], objectType: "person", preferredUsername: "BaysOn80", status: "Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!", objectType: "activity", postedTime: "2012-05-21T16:39:40.647-0600"}
Cloud Computing Challenges

Cloud Providers

• Need deep visibility across massive, scaled-out, distributed infrastructure to meet service levels
• Need to secure the shared environment and prove compliance
• Need to understand usage analytics (internally as well as for customers)

Cloud Consumers

• Need visibility into service levels of cloud provider
• Need visibility into end user experience and monitoring of user activity
• Need operational analytics into consumption, costs, usage

Platform As A Service
Heroku

Software As A Service
Salesforce.com
Intuit
Genius.com
Netsmart

Infrastructure As A Service/Managed Service
Hughes Networks
Verizon Business
Voxeo
BT
Machine Data Contains Critical Insights

Sources
- Order Processing
- Middleware Error
- Care IVR
- Twitter

ORDER, 2012-05-21T14:04:12.484Z, Customer ID 10098213, Product ID 569281734

May 21 14:04:12.996 w1-01.acme.com Order 569281734 failed
May 21 11:24:48 10098213 Order 569281734 Exception follows:
weblogic.jdbc.extensions.ConnectionDeadSQLException: Could not create pool
The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

Customer ID 10098213, Order ID 569281734

Twitter ID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:"http://dallascowboys.com"},location:{displayName:"Dallas, TX"},objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}
Real-time Customer and Product Analytics

Measure customer attention to specific areas of content

Analyze click through's and how they navigate to CJ mall

Track and analyze mobile shopping customers in real time
Customer Analytics for Online Platform

- Understand and optimize customer behavior
- Improve product performance - identify and analyze bot/scraper traffic
- Measure SuperBowl Ad effectiveness
- Bring and correlate information to make faster decisions

"Splunk provided us visibility we didn’t have before."
What’s the Key Challenges?

• Trying to keep pace with the rapid influx of new customers
• Managing changes in technology
• Implementing custom and off-the-shelf applications to serve customer reporting demands
• To deliver consistent high quality services at any of its data centers worldwide
• Difficult or impossible to efficiently and effectively collect and correlate data across multiple sites and geographies.
Why do we need visibility into the data?

- Big/Complex environments: IT is “the business”:
- Managing a Service: Uptime and MTTR are critical
- Live and die by the SLA
- New source of revenue:
  - Increase ARPU
  - Reporting Capability
  - Digital Intelligence, Business analytics, etc
# Splunk Company Overview

## Company
- Global HQs:
  - San Francisco
  - London
  - Hong Kong
- 1,300 employees globally
- Annual Revenue: $302.6M (YoY +52%)

## Products
- Free trial to massive scale
- Splunk products:
  - Splunk Enterprise
  - Splunk Cloud
  - Hunk
  - Splunk MINT
  - Premium Apps

## Customers
- 8,400+ customers
- Across 100 countries
- Small to large organizations
- 75+ of the Fortune 100
- Largest license:
  - 400+ Terabytes/day

NASDAQ: SPLK
Make machine data accessible, usable and valuable to everyone.
Big Data Comes from Machines

Volume | Velocity | Variety | Variability

GPS, RFID, Hypervisor, Web Servers, Email, Messaging, Clickstreams, Mobile, Telephony, IVR, Databases, Sensors, Telematics, Storage, Servers, Security Devices, Desktops
Splunk Collects and Indexes Any Machine Data

Customer Facing Data
- Click-stream data
- Shopping cart data
- Online transaction data

Outside the Datacenter
- Manufacturing, logistics...
- CDRs & IPDRs
- Power consumption
- RFID data
- GPS data

Windows
- Registry
- Event logs
- File system
- sysinternals

Linux/Unix
- Configurations
- syslog
- File system
- ps, iostat, top

Virtualization & Cloud
- Hypervisor
- Guest OS, Apps
- Cloud

Applications
- Web logs
- Log4J, JMS, JMX
- .NET events
- Code and scripts

Databases
- Configurations
- Audit/query logs
- Tables
- Schemas

Networking
- Configurations
- syslog
- SNMP
- netflow

Logfiles
Configs
Messages
Traps
Alerts
Metrics
Scripts
Changes
Tickets

Cloud Channel Summit 2015 | @rhipecloud #RCCS15
Many ‘Single Panes of Glass’
Search, Investigate and Explore Your Data

Find and fix issues and incidents dramatically faster across your organization
Delivers Value Across IT and the Business

Application Delivery
IT Operations
Security, Compliance and Fraud
Business Analytics
Industrial Data and Internet of Things

Developer Platform (REST API, SDKs)

splunk
How Cloud Providers Use Splunk

1. Gain deep visibility and correlation across every layer of the stack.

2. Achieve flexibility in investigating and solving any kind of operational or security issue and reporting and proving compliance.

3. Provides business analytics to providers as well as customers.
Reports Across Roles & Departments

- Executive Management
- Product Managers
- Marketing Managers
- Sales Operations
- IT Mgmt & Operations
- Customer Service & Support
Users and Roles

Integrate authentication with LDAP and Active Directory.

Map LDAP & AD groups to flexible Splunk roles. Define any search as a filter.
British Telecom

The old way: Many network issues go undetected

Network monitoring and engineering teams are missing access to important event data

Errors and warnings buried in logs are ignored because of overwhelming volume

Writing scripts to analyze raw data is too slow and difficult

The new way: Splunk lets you search the network stack

✓ Search terabytes of data for network transactions across every component
✓ Index syslog, SNMP traps, configuration and netflow data
✓ Navigate from symptom to root cause quickly
✓ Find early warning signs of problems that go undetected with component monitoring
✓ Compliment existing network monitoring with scheduled searches

“Splunk gives our customer service center, NOC staff and network engineers comprehensive real time event data for incident response, chronic problem identification and monitor of monitors optimization.”

Dave McCallum, Platform Architect
Broad Adoption Across 9000 Customers
Transforming Customer Data into Values
Services Models

• Hosting/Cloud Services (Out-Sourcing)
  – MSP provides and manages infrastructure and application services including facilities, networking, storage, compute and applications.

• Remote Management (Co-Sourcing)
  – MSP manages specific parts of infrastructure and/or applications running on customer site including networking, security, compliance and applications.

• SaaS
  – MSP offers turnkey applications and services over the Internet.
Hosting/Cloud Services (Out-Sourcing)

MSP provides and manages infrastructure and application services.

Customer runs customer infrastructure and applications at MSP site

Splunk installed for a single customer or as part of MSP applications for all customers.
Delivering Cloud-based Website Testing

“We investigated many other options to aggregate and process results, but none came close to the scale or speed of Splunk”

Dan Siroker
CEO

Splunk incorporated into multi tenant, easy to use cloud based A/B and multivariate testing
Semantic logging from app used to provide tracking and results of the website testing service
Remote Management (Co-Sourcing)

MSP manages parts of infrastructure/applications running on customer site.

Customer access MSP applications locally within their own site.

Splunk installed on customer site as part of MSP solution and on MSP site for central operations.

i.e. Remote Log Management, Security Monitoring
SaaS

MSP offers turnkey applications and services over the Internet.

Splunk is integrated with MSP SaaS platform providing engine for new services.

Optionally Splunk can be installed at customer site to provide remote integration.
salesforce.com

- Offering a new service: Reporting on customer email campaigns
- Providing analytics around usage of social platform services and apps on Force.com
- Application analytics & troubleshooting

Narayan Bharadwaj
Director, Product Management
"Our high performance cloud computing offering has Splunk integrated from the ground up. It is the go-to solution for every type of question – it helps in decision making at every level, from dev/test/ops to account management, product management and pricing."

Vincent Bumgarner
Principal Systems Engineer

Splunk integrated into Riskmetrics’ high performance cloud computing effort from the ground up

Used throughout the organization for delivering deep insights to vendor pricing, CFO, account management and sales, in addition to dev/test and support.
Thank you!

enquiries.my@rhipe.com
www.rhipe.com