



Using Proactive Analytics to Better Manage Your IT Operations

Track 5 Session 2 :

Search and analyze logs to perform faster root cause analysis and avoid problems by detecting emerging problems.

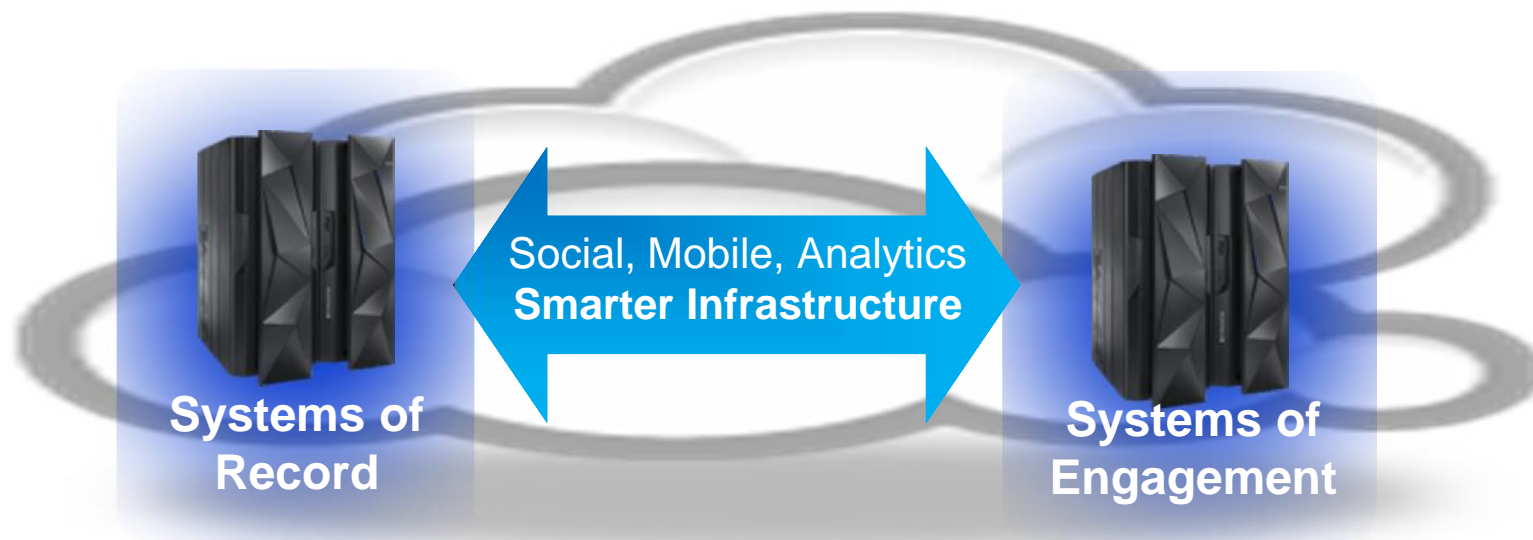
IBM z Systems Technology Summit



DC • Costa Mesa • Chicago • Cincinnati • Toronto • Atlanta • NYC • San Francisco • Dallas

Rapid growth of data from next generation technologies can be supported seamlessly on z Systems

System z scaling model and security to manage and optimize both

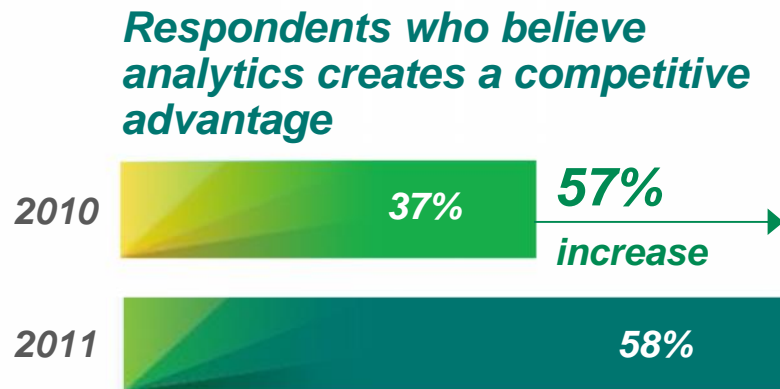


- Business Transactions
- Quality of Service
- Command & Control
- Facts and data “source of truth”
- z Systems

- Mobile and Social
- Dynamic
- Interactions and Collaboration
- Insight, trends, analytics
- Linux on z

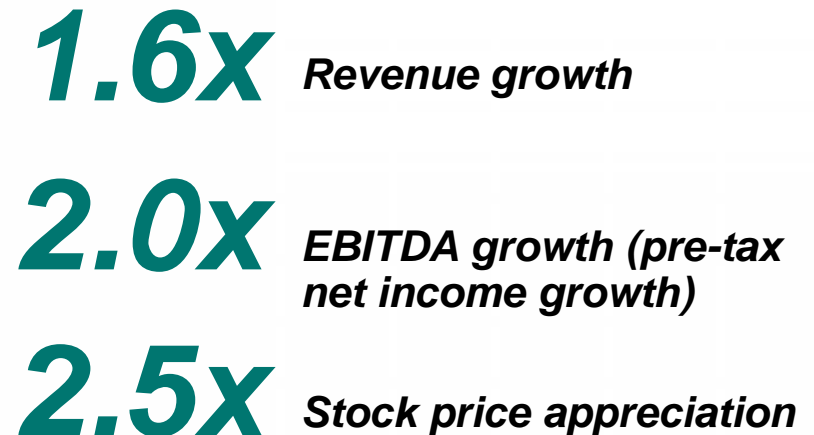
Organizations using analytics have been shown to outperform competition and improve business results

More organizations are using analytics to create a competitive advantage



Source: *The New Intelligent Enterprise*, a joint MIT Sloan Management Review and IBM Institute of Business Value analytics research partnership.
Copyright © Massachusetts Institute of Technology 2011

And leaders are outperforming their competitors in key financial measures



Source: *Outperforming in a data-rich, hyper-connected world*, IBM Center for Applied Insights study conducted in cooperation with the Economist Intelligence Unit and the IBM Institute of Business Value. 2012

Analytics strategy is now mission critical and impact bottom line results across all industries and IT



Industries

Banking

Increase account profitability

Insurance

Retain policy holders with better service & marketing

Retail

Understand sales patterns

Telecommunications

Reduce churn with custom retention offers



Operations

Industrial

Predict maintenance issues before occur

Retail

Improve store performance with P&L reports

Telecommunications

Understand & manage network traffic

Insurance

Streamline claims process

Government

Reduce fraud and waste

Analytics for z Systems addresses predict, search and optimize requirements on impact from new technology

Higher amount of IT operational data (SMF, log, journal) compared to distributed only environments.

- Focus on problem determination/time to resolution and placing a premium on availability of services and applications.

By 2016, **20% of Global 2000 enterprises will have IT operations analytics** architecture in place, up from < 1% today, looking to integrate across their enterprise to reduce outages (Gartner).

90% of the Fortune 1000 companies are running z and have System of Record dependencies for transactional processing and data serving applications .

- Regulatory requirements prevent the offloading of most data from the z platform.

IBM focused on managing end-to-end analytics for improved performance and workload management

IBM Analytics solutions for System z

Proactive Outage Avoidance

Predict

- IBM SmartCloud Analytics - Predictive Insights
- OMEGAMON & NetView w/ IBM zAware

- Pro-Active Outage Avoidance
- Predict problems before they occur

Faster Problem Resolution

Search

IBM SmartCloud Analytics - Log Analysis

- Quickly search large volumes of log data from a single search bar
- Perform log analysis while searching
- Correlate messages from multiple logs for end-to-end problem diagnosis

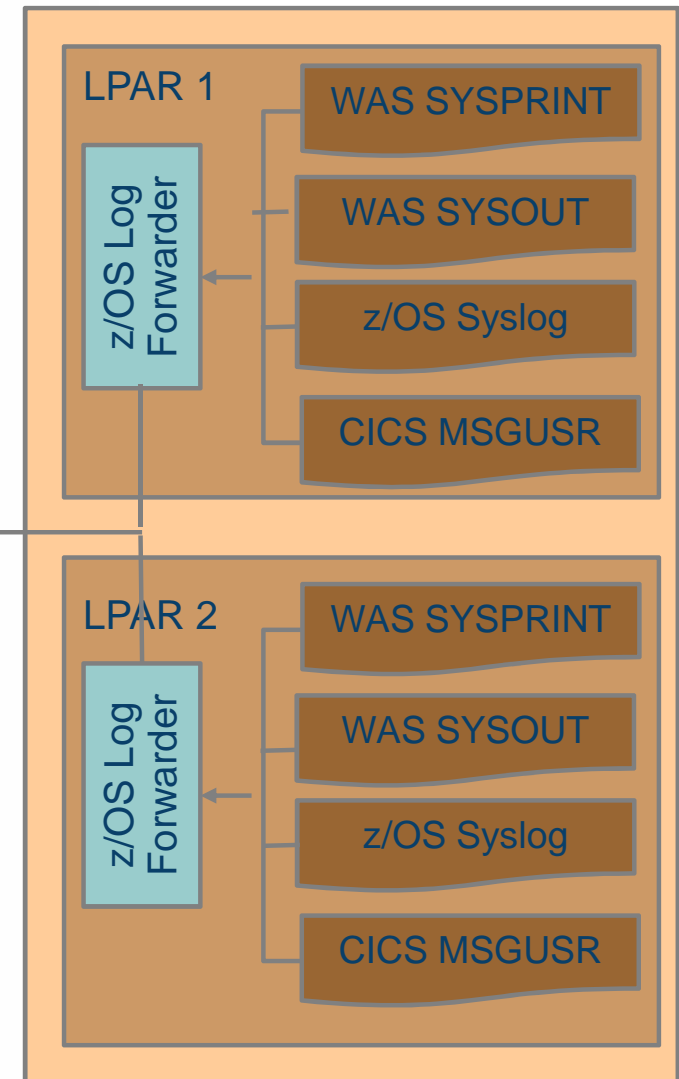
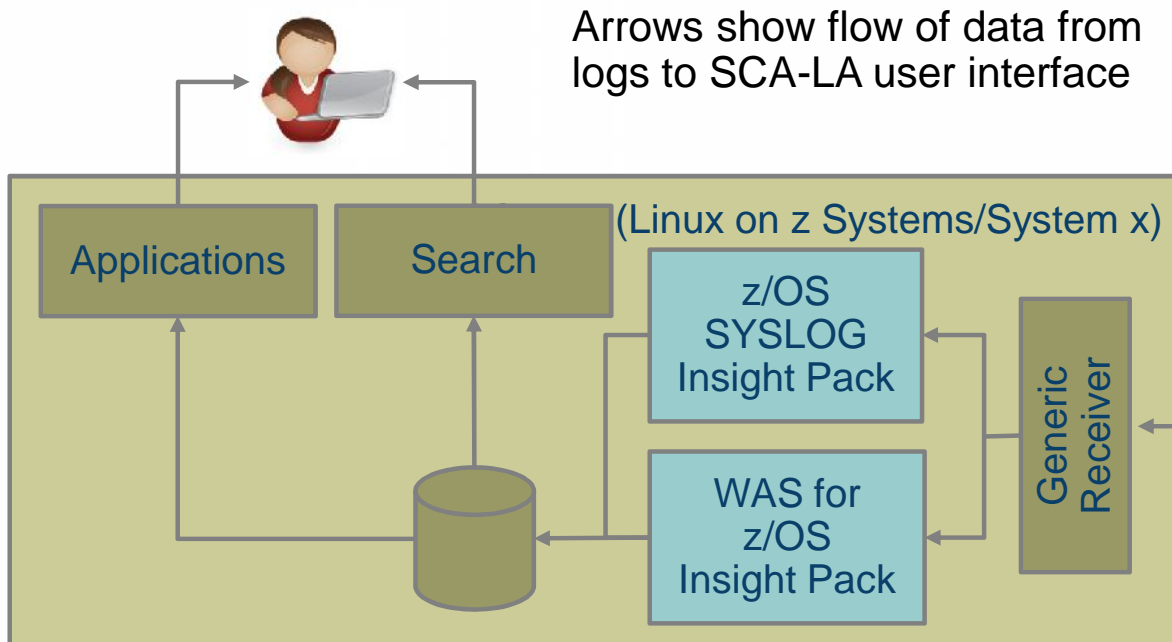
Optimized Performance

Optimize

IBM Capacity Management Analytics (CMA)

- Improve performance and forecast capacity across IT Infrastructure

IBM SmartCloud Analytics – Log Analysis z/OS Insight Packs & SCA-LA Server



- z/OS Log Forwarder is installed on each z/OS LPAR to enable Log Search
- The SCA-LA server is installed on System x or z Systems) running Linux
- z/OS Insight Packs for WebSphere and SYSLOG are installed on the SCA-LA server

Solution Components

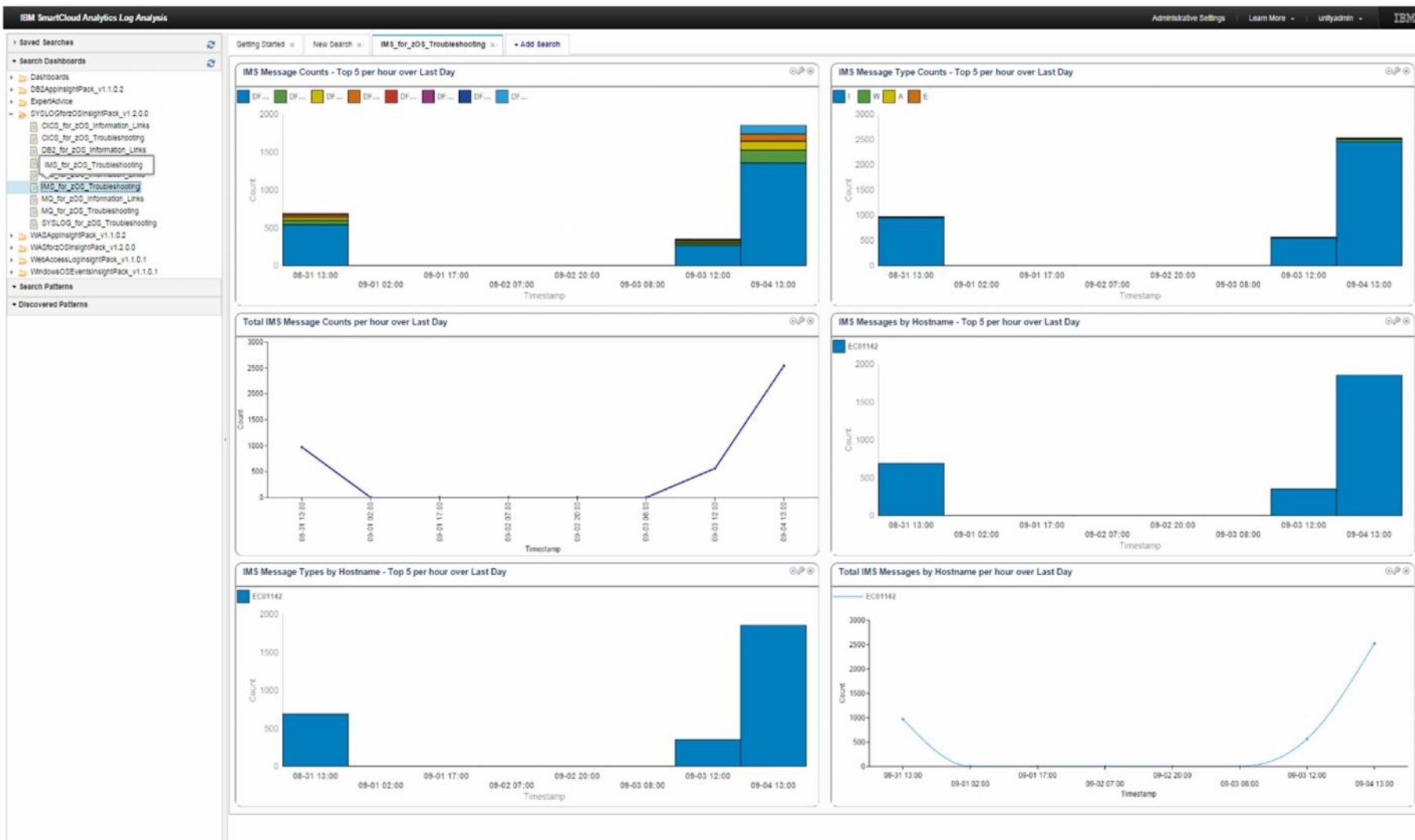
IBM SmartCloud Analytics - Log Analysis z/OS Insight Pack for SYSLOG v1.2.0

- IBM SmartCloud Analytics – Log Analysis (SCA-LA) 1.2.0.3
 - Provides data collection, analytics and storage capabilities, as well as search interface
 - Runs on Linux on z Systems and Linux on x86
- z/OS SYSLOG Insight Pack
 - An Insight Pack that extends SCA-LA so it can ingest and perform searches against DB2, CICS, MQ and IMS for z/OS log data and other log data from the SYSLOG
- z/OS Log Forwarder
 - A specialized SCA-LA data collector client that monitors and forwards z/OS SYSLOG and/or WAS for z/OS log data to SCA-LA
 - Executes independently on each z/OS LPAR that is monitored
 - Configurable to specify which WAS for z/OS jobs (if any) to monitor and whether to monitor the z/OS SYSLOG

IBM SmartCloud Analytics - Log Analysis z/OS Insight Pack for WebSphere® Application Server v1.2.0

- IBM SmartCloud Analytics – Log Analysis (SCA-LA) 1.2.0.3
 - Provides data collection, analytics and storage capabilities, as well as search interface
 - Runs on Linux on z Systems and Linux on x86
- WebSphere® Application Server for z/OS Insight Pack
 - An Insight Pack that extends SCA-LA so it can ingest and perform searches against WAS for z/OS log data
- z/OS Log Forwarder
 - A specialized SCA-LA data collector client that monitors and forwards z/OS SYSLOG and/or WAS for z/OS log data to SCA-LA
 - Executes independently on each z/OS LPAR that is monitored
 - Configurable to specify which WAS for z/OS jobs (if any) to monitor and whether to monitor the z/OS SYSLOG

Sample dashboard



Quickly and easily access IBM Support Portal based Expert Advice from Log Analysis

































Search for expert advice with the click of a button

All IBM support site documents that reference messages from search results

The screenshot displays the IBM Support Portal interface. On the left, there is a navigation pane with sections like 'Quick Searches', 'Custom Apps', 'ExpertAdvice', 'Configured Patterns', and 'Discovered Patterns'. The main content area shows search results for 'WebSphere Application Server V8: Administration and Configuration Guide'. A specific search result is highlighted: 'IZ05682: ADMINTASK RECONFIGURETAM PORT CONFLICT'. A red arrow points from this result to a detailed Technote page on the right. The Technote page is titled 'WSKeyStore CWPKI0041W warning message is found in the SystemOut.log file' and includes sections for 'Technote (troubleshooting)', 'Problem(Abstract)', 'Cause', and 'Resolving the problem'. A yellow callout box points to the search results, and a white callout box points to the Technote title.

Launch to Technote

Out of the Box Quick Searches

-  zos
 - ▾  db2
 -  DB2 Messages
 -  DB2 Action, Decision or Errors
 -  DB2 Critical Data Set Messages
 - ▾  cics
 -  CICS TS Messages
 -  CICS TS Abend or Severe
 -  CICS Action, Decision or Error
 -  CICS TS Key Messages
 - ▾  ims
 -  IMS Messages
 -  IMS Action, Decision or Error
 -  IMS Resources in Waiting Error
 -  IMS Security Violations
 -  IMS Abend Messages
 -  IMS Connect Messages
 -  IMS Common Queue Server Msgs
 -  IMS DB Recovery Control Errors
- ▾  mq
 -  MQ Messages
 -  MQ Action, Decision or Error
 -  MQ Buffer Pool Errors
 -  MQ Channel Errors
 -  MQ Channel Initiator Errors
 -  MQ Interesting Informational
 -  MQ Key Messages
 -  MQ Logs Start and Stop
 -  MQ Queue Manager Storage
- ▾  was
 -  WAS Error Messages
 -  WAS Exceptions

DB2 and WebSphere Application Server Quick Searches

- **DB2 Messages**
 - This sample searches for all DB2 messages that occurred during the last day.
- **DB2 Action, Decision or Errors**
 - This sample searches for any DB2 messages that occurred during the last day and that indicate any of the following situations:
 - Immediate action is required.
 - A decision is required.
 - An error occurred.
- **DB2 Critical Data Set Messages**
 - This sample searches for messages that indicate that DB2 log data sets are full, are becoming full, or could not be allocated during the last day.
- **WAS Error Messages**
 - This sample searches for any WebSphere Application Server for z/OS messages that occurred in the last day and that indicate an error occurred.
- **WAS Exceptions**
 - This sample searches for any occurrences of Java™ exceptions in the WebSphere Application Logs during the last day.

CICS Quick Searches

- **CICS TS Messages**
 - This sample searches for all CICS Transaction Server messages that occurred during the last day.
- **CICS TS Abend or Severe**
 - This sample searches for CICS Transaction Server messages that have all of the following characteristics:
 - The messages occurred during the last day.
 - The messages have the format `DFHccxxxx`, where `cc` represents a component identifier (such as `SM` for Storage Manager), and `xxxx` is either `0001` or `0002` (which indicates an abend or severe error in the specified component).
- **CICS Action, Decision or Error**
 - This sample searches for any CICS messages that occurred in the last day and that indicate that immediate action is required **or** that a decision is required **or** that an error occurred.
- **CICS TS Key Messages**
 - This sample searches for a set of predefined message numbers to determine whether any of the corresponding messages occurred during the last day.

- **IMS Messages**
 - This sample searches for all IMS messages during the last day.
- **IMS Action, Decision or Error**
 - This sample searches for any IMS messages that occurred in the last day and that indicate that immediate action is required **or** that a decision is required **or** that an error occurred.
- **IMS Security Violations**
 - This sample searches for error messages that indicate security violations that have been detected during the last day.
- **IMS Abend Messages**
 - This sample searches for all messages that indicate abends that have been detected during the last day.
- **IMS Common Queue Server Msgs**
 - This sample searches for all messages in the IMS Common Queue Server component during the last day.
- **IMS Resources in Waiting Error**
 - This sample searches for error messages that indicate that a resource is waiting on other resources to become available during the last day.
- **IMS DB Recovery Control Errors**
 - This sample searches for all error messages in the DB Recovery Control component during the last day.
- **IMS Connect Messages**
 - This sample searches for all messages in the IMS Connect component during the last day.

IMS search results from out-of-the-box searches

IBM SmartCloud Analytics Log Analysis

Administrative Settings | Learn More | unityadmin

Saved Searches: zos, db2, cics, **ims**, mq, was

Search Dashboards

Search Patterns: datasourceHostname (1), threadID, exceptionClassName, exceptionMethodName, exceptionPackageName, MessagePrefix (3), msgClassifier, threadAddress, javaException

Getting Started | New Search | **IMS Action, Decision or Error** | + Add Search

(MessagePrefix:DFS OR MessagePrefix:BPE OR MessagePrefix:CQS OR Mes: Search Custom

Log Events Granularity: minute Time Range: 09/04/2014, 13:00:00 - 09/04/2014, 13:45:00

1 to 75 of 75 results

N 4200000 EC01142 14247 09:38:42.11 JOB00202 00000010 DFS0062W HWSYDRU0 TMEMBER=IVP13HWS IVP1

[09/04/14 13:38:41:670 +0000] _datasource:SYSLOG-IMS, datasourceHostname:ec01142, MessagePrefix:DFS, SystemName:EC01142, MessageID:DFS3187W, Task:JOB00202, writetime:09/16/14 14:37:25:613 +0000, MessageType:W, MessageText:DFS3187W RACF NOT ACTIVE FOR RESUME TPIPE CLASS=RIMS RC=04. RACF EXIT RC=04 REASON CODE=00. IVP1

N 4200000 EC01142 14247 09:38:41.67 JOB00202 00000010 DFS3187W RACF NOT ACTIVE FOR RESUME TPIPE CLASS=RIMS RC=04. RACF EXIT RC=04 REASON CODE=00. IVP1

[09/04/14 13:38:41:670 +0000] _datasource:SYSLOG-IMS, datasourceHostname:ec01142, MessagePrefix:DFS, SystemName:EC01142, MessageID:DFS3187W, Task:JOB00202, writetime:09/16/14 14:37:25:613 +0000, MessageType:W, MessageText:DFS3187W RACF NOT ACTIVE FOR RESUME TPIPE CLASS=RIMS RC=04. RACF EXIT RC=04 REASON CODE=00. IVP1

Quick and easy search with out-of-box log analysis

WebSphere MQ Quick Searches

- **MQ Messages**
 - This sample searches for all WebSphere MQ messages during the last day.
- **MQ Action, Decision or Error**
 - This sample searches for any WebSphere MQ messages that occurred in the last day and that indicate that immediate action is required **or** that a decision is required **or** that an error occurred.
- **MQ Queue Manager Storage**
 - This sample searches for messages that indicate that Websphere MQ Queue Manager is short of storage or is no longer short of storage during the last day.
- **MQ Logs Start and Stop**
 - This sample searches for messages related to the starting, stopping and flushing of the WebSphere MQ log data sets during the last day.
- **MQ Key Messages**
 - This sample searches for a set of predefined message numbers to determine whether any of the corresponding messages occurred in the last day.
- **MQ Interesting Informational**
 - This sample searches for a set of predefined information message numbers that might warrant attention to determine whether any of the corresponding messages occurred in the last day.
- **MQ Channel Initiator Errors**
 - This sample searches for error messages that indicate Websphere MQ Channel Initiator errors during the last day.
- **MQ Channel Errors**
 - This sample searches for error messages that indicate Websphere MQ Channel errors during the last day.
- **MQ Buffer Pool Errors**
 - This sample searches for error messages that indicate Websphere MQ Buffer Pool errors during the last day.

MQ search results from out-of-the-box searches

The screenshot displays the IBM SmartCloud Analytics Log Analysis interface. The left sidebar shows a tree view of search patterns, with 'CommandPrefix (+M71L (1037))' selected. The main panel shows a search query: 'MessagePrefix:"CSQ" AND (MessageType:"A" OR MessageType:"D" OR Mess'. The search results are displayed in a table format, showing log events with timestamps and message details. A bar chart above the results shows the distribution of events over time, with a callout indicating the 'Timeframe of problem' from 8/26/14 to 8/27/14. A callout points to the search query as 'MQ log search'. Another callout points to the search results as 'Search results'.

Out-of-the-box searches for common MQ errors

MQ log search

Timeframe of problem

Search results

Quick and easy search with out-of-box log analysis

Application Views

- For each supported z/OS domain, a set of custom applications is provided that graph out incidents over time:
 - Message Counts - Top 5 over last day
 - Messages by Hostname - Top 5 over Last Day
 - Message Type Counts - Top 5 over Last Day
 - Message Types by Hostname - Top 5 over Last Day
 - Message Counts - over Last Day
 - Total Messages by Hostname - over Last Day

Installation Planning

z/OS Log Forwarder

- Supported software platforms:
 - IBM z/OS 1.13 or later
 - The z/OS Log Forwarder can run with JES2 or JES3
 - Note: If using JES3, DLOG must be disabled
- Required software components:
 - IBM Java™ Runtime Environment (JRE) V6 or later
 - Reminder: SDSF is no longer required

SmartCloud Analytics – Log Analysis (server)

- Supported software platforms:
 - RHEL 5 & 6, SLES 11 on x86 (64-bit)
 - RHEL 5 & 6, SLES 11 on z Systems (64-bit)
- Hardware requirements:
 - Depend on daily log volume to be ingested, as well as duration of log data retention
 - Detailed hardware sizing guidance to be made available
 - For sample hardware configurations, see SCA-LA v1.2.0.3 documentation ([link](#))

Send us your logs!

- Request a product demo using logs from your own test, development or production environments
- IBM will load your logs into a SCALA server, then demo the results back to you
 - A secure, dedicated drop box will be assigned to you
 - You will be sent detail upload instructions via email
 - Any file uploaded will be automatically moved to a dedicated SCALA environment within 24 hours
 - All log data will be purged from the SCALA environment within 48 hours after the demo event

To request your hosted demo, visit:

<http://services-useast.skytap.com:18280/WebDemo/>

Thank
You

The words 'Thank You' are rendered in a large, 3D-style font. Each letter is filled with a different portrait of a diverse group of people, including men and women of various ethnicities and ages. The portraits are cut out to fit the shape of the letters, creating a mosaic effect. The text is centered on the page.