

SmartCloud Analytics – Log Analysis

Clyde Richardson (richardc@us.ibm.com)
Technical Sales Specialist

Anuja Deedwaniya (anujad@us.ibm.com)
IBM z Systems Enterprise Architect

Paul Smith (Smitty) (paulmsm@us.ibm.com)
IBM z Systems Service Management / zAnalytics Architect



SHARE is an independent volunteer-run information technology association
that provides **education**, professional **networking** and industry **influence**.



Agenda

- Problem Diagnosis and Resolution – Finding a needle in a haystack
- Predict, Search, Optimize
- SmartCloud Analytics – Log Analysis
 - Capabilities
 - Interface
 - Integration with your Service Management Tooling
 - Coming Soon ... Join the Beta
 - Reference Materials
 - Solution Demo



Analysis – The Problem

Find the right needle in one of many haystacks – QUICKLY!

404 ERROR

It's SLOW!!

Centralized,
Distributed, Cloud,
Resilient Architectures
Increase Data Volume

Where do I
start??

Everything is
“green”

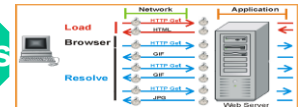
Logs,
Traces,..

[10/9/12 5:51:38:295
GMT+05:30] 0000006a
servlet E
com.ibm.ws.webcontainer.ser
vlet.IbmServletWrapper service
SRVE0068E:

Events

Node	Alert Group
10/9/12 5:51:38:295	EventAction (netcool)
10/9/12 5:51:38:295	EventAction (netcool)
10/9/12 5:51:38:295	EventAction (netcool)
10/9/12 5:51:38:295	EventAction (netcool)
10/9/12 5:51:38:295	EventAction (netcool)
10/9/12 5:51:38:295	EventAction (netcool)
10/9/12 5:51:38:295	EventAction (netcool)
10/9/12 5:51:38:295	EventAction (netcool)

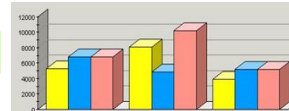
Transactions



Core files

0100011000111100001110
0110001111110000110001
111111000110011100011

Metrics



Config



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

Predict:

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

Search:

- 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

Optimize:

- Improve performance across IT Infrastructure

IBM Analytics solutions for System z

Proactive Outage Avoidance

Predict

- OMEGAMON & NetView
w/ IBM zAware

Faster Problem Resolution

Search

IBM SmartCloud Analytics -
Log Analysis

Optimized Performance

Optimize

IBM Capacity Management
Analytics (CMA)

Search for and rapidly analyze unstructured data to assist in and accelerate problem identification, isolation and repair



SmartCloud Analytics – Log Analysis



Differentiating Capabilities

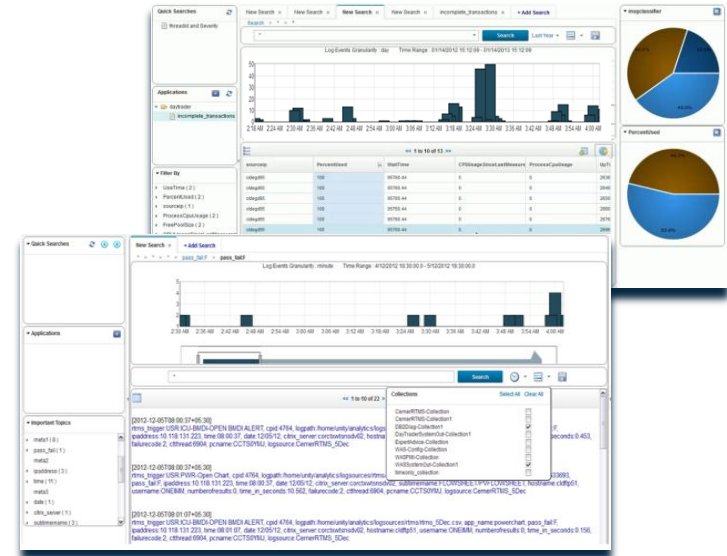
Locate **component error messages** from system, configuration, software and event logs **via rapid indexed search**

- Search logs and events across multiple platforms (distributed and mainframe), LPARs, CECs, applications, middleware, subsystems

Isolate issues and provide insights across various domains including WebSphere, DB2, CICS, IMS, MQ, OS, etc

Link support documentation and operations notes dynamically to log messages and events to resolve problems quickly

Visualize search results with analytic tools to rapidly perform root cause analysis



Search for and rapidly analyze unstructured data to assist in and accelerate problem identification, isolation and repair



SmartCloud Analytics – Log Analysis



Delivering Business

Reduce mean time to repair by identifying and isolating service impacting issues quickly

Resolve problems more efficiently with faster access to all pertinent information

Reduce effort by consolidating, analyzing information in real-time

Improve service availability by leveraging expert knowledge of applications and infrastructure

Built on IBM's leading Big Data platform

IBM expertise built-in

Download and install in minutes for quick time-to-value

Customer Experiences



Large Insurance Company

- Experienced an application outage that resulted in the team working around the clock for **29 hours** pouring through logs and traces to determine the root cause of the issue. After the issue was resolved, the logs were captured and sent to IBM lab for analysis using SCA-LA. **Within minutes**, the IBM team was able to see the scope of the issues, and find the relevant PTF to resolve the issue through the integrated expert advice.

State Agency

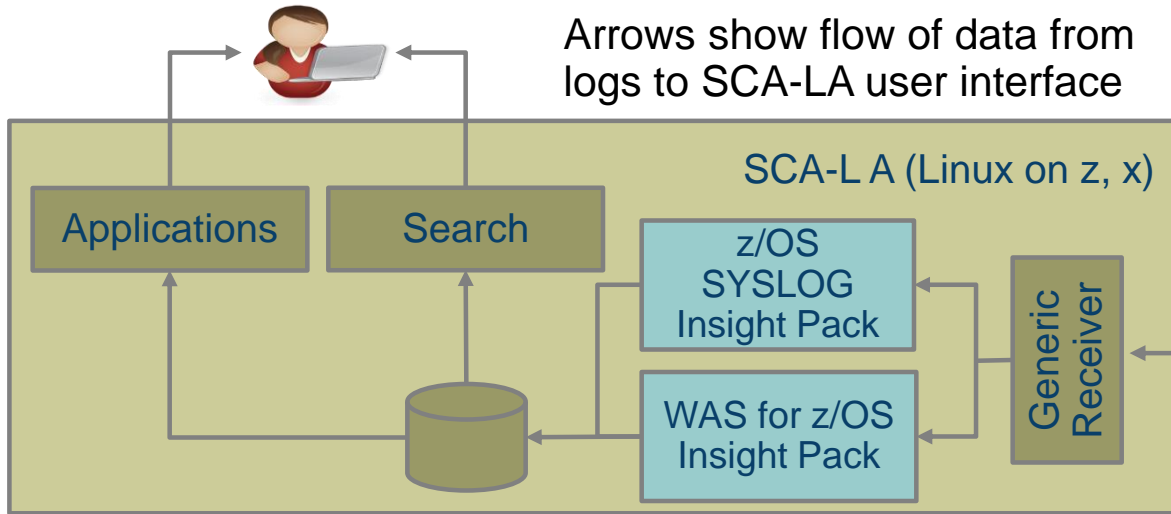
- Were able to **download, install, configure** and use SCA-LA to search their logs in **2.5 hours**.

Numerous Customers

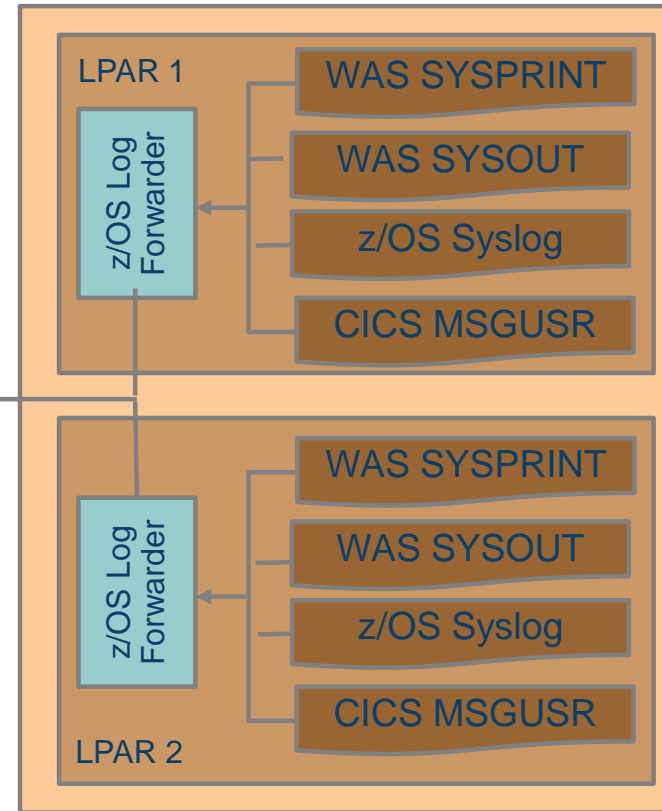
- Errors lurking in logs that are never examined because they don't necessarily cause SLA or performance problems. For example, SCA-LA found over 4,000 invalid login attempts in a three day period that had otherwise gone unnoticed.

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

z/OS Systems



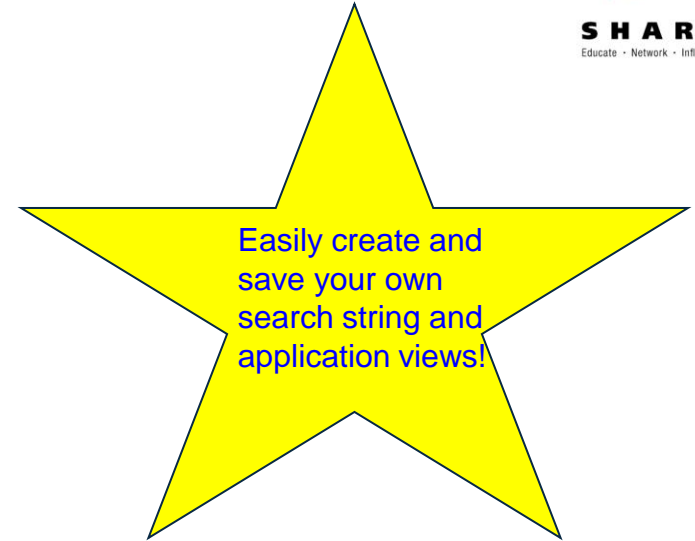
- z/OS Log Forwarder is installed on each z/OS LPAR to enable Log Search
- The SCA-LA server is installed on z Systems (or System x) running Linux (64 bit)
- z/OS Insight Packs for WebSphere and SYSLOG are installed on the SCA-LA server



SCA-LA: Search syntax – Tailor Your Queries



- Simple free form searches can be performed
 - Search for “error” for example
- **OR** is the default operator
- **AND** or **+** is the AND operator:
 - **+MessageType:"E" + MessageID:"CSQX599E"**
 - **MessageType:"E" AND MessageID:"CSQX599E"**
- Exclude terms with the **NOT** or **–** operator:
 - **+MessagePrefix:"CSQ" NOT MessageType:"I"**
 - **+MessagePrefix:"CSQ" – MessageType:"I"**
- Quotes can be used for phrases containing spaces:
 - “ended abnormally”
- Parentheses for grouping:
 - **(+MessagePrefix:"CSQ" +MessageType:"E") OR (+MessagePrefix:"CNZ"+MessageType:"E")**
- Field designator to restrict search to a particular field:
 - **MessagePrefix:"CSQ"**

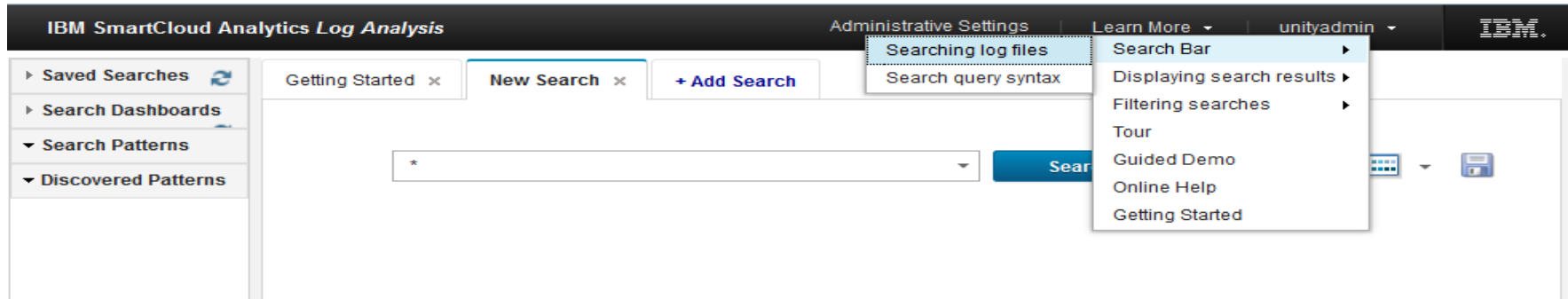


SCA-LA: Search syntax ...

- * wildcard for multiple characters:
 - **test*** might return test, tests or tester.
- ? wildcard for any single character:
 - **te?t** might return text or test

Easily create simple or advanced queries.

- Online Help available from the **Learn More** → **Search Bar** → **Search query syntax** menu:



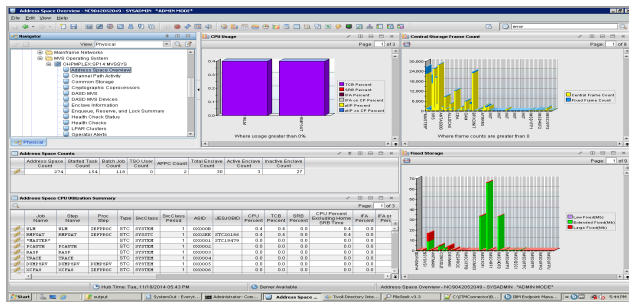
Integration with Performance Monitoring



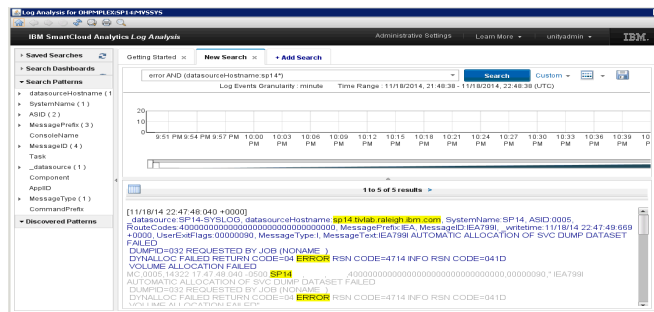
OMEGAMON + SCA-LA – Launch in Context from TEP

The **One Two – Punch**: Combine two very powerful tools to ensure performance and high availability of your enterprise.

- **Perform log analysis in context of OMEGAMON workspaces** – This approach enables OMEGAMON users to perform in-context log analysis while doing problem determination
 - From your OMEGAMON workspace, use the SCA-LA search bar to search logs (using LPAR or Sysplex as the default context)
 - Easy to implement - Configure TEP to display the SCA-LA search bar



Launch SCA-LA from OMEGAMON performance monitoring workspaces to search logs in context



Integration with Event Management

Network Operations Insight + SCA-LA – Search and Analyze Events



Event Analytics – for Seasonal Event Identification (New)

Provides opportunities for event reduction thus improving operational efficiency.



- Easily identify ‘related’ Events that may be candidates for suppression
- Identify “difficult to spot” seasonal events that often result in regular periodic problems
- Leverage visualizations that help you quickly isolate more severe and significant problems.

Also, SCA-LA can generate notifications based on data (logs messages, data, etc)



In Beta Now



- Analyze your SMF data AND your log data for a complete view of the enterprise.



- Also, Search and provide network Insights with our new Network Insights Pack



zSCA-LA v.Next Early Access and Beta Program



The **IBM SmartCloud Analytics - Log Analysis for z/OS V.next Early Access and Beta Program** was announced on January 29, 2015.

In 2015, we will build on the strong foundation established over the past months by providing insights into additional domains, as well as by enhancing existing insights through integration of performance metrics.

We are looking for customers and business partners worldwide who would like to test the new capabilities and help shape the content of the release under development.

To see the full program announcement, and to learn how to sign up, please visit us in our developerWorks community at:

<https://ibm.biz/BdEkZV>



Additional SCA-LA Reference Material



- Analytics Overview Video
 - <https://www.youtube.com/watch?v=OQJapWiQECs>
- SCA-LA z/OS Insight Packs videos:
 - http://www.youtube.com/watch?v=2oDgX_Ydr18
 - There are several YouTube videos – search for ‘SmartCloud Analytics – Log Analysis’)
- SCA-LA z/OS Insight Pack Documentation
 - Knowledge Centers
 - SYSLOG: <http://www.ibm.com/support/knowledgecenter/SS9M7K>
 - IBM WAS: <http://www.ibm.com/support/knowledgecenter/SS9MBD>
- SCA-LA Product Documentation
 - Service Management Connect
 - <http://www.ibm.com/developerworks/servicemanagement/ioa/log/index.html>
 - Knowledge Center
 - <http://www.ibm.com/support/knowledgecenter/SSPFMY>



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/>



Demo

Thank
You

Backup slides in case you can't do the demo

Launch SCA-LA (in context of LPAR) from OMEGAMON Workspace

LPAR Scenario - OMEGAMON user searches for the word 'error' in the LPAR's logs

The screenshot shows the OMEGAMON Workspace Address Space Overview window. The window is divided into several panes. The top-left pane shows a tree view of the system hierarchy. The top-right pane shows a search bar with the text 'error'. The bottom-left pane shows a table of Address Space Counts. The bottom-right pane shows a table of Address Space CPU Utilization Summary. The middle-right pane shows a bar chart of Central Storage Frame Count. The bottom-right pane shows a bar chart of Fixed Storage. The search bar is highlighted with a yellow callout box that says 'Specify search string'. The search bar is also highlighted with a yellow callout box that says 'Specify search time frame'. The search bar is also highlighted with a yellow callout box that says 'Search will be done in context of LPAR'.

Search will be done in context of LPAR

Specify search time frame

Specify search string

SCA-LA search bar now available in TEP

Address Space Overview - NC9042052049 - SYSADMIN *ADMIN MODE*

File Edit View Help

Navigator View: Physical

- Mainframe Networks
- MVS Operating System
 - OHPMPLEX:SP14:MVSSYS
 - Address Space Overview
 - Channel Path Activity
 - Common Storage
 - Cryptographic Coprocessors
 - DASD MVS
 - DASD MVS Devices
 - Enclave Information
 - Enqueue, Reserve, and Lock Summary
 - Health Check Status
 - Health Checks
 - LPAR Clusters
 - Operator Alerts

Physical

Address Space Counts

Address Space Count	Started Task Count	Batch Job Count	TSO User Count	APPC Count	Total Enclave Count	Active Enclave Count	Inactive Enclave Count
274	154	118	0	2	30	3	27

Address Space CPU Utilization Summary

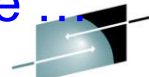
Job Name	Step Name	Proc Step	Type	SvcClass	SvcClass Period	ASID	JESJOBID	CPU Percent	TCB Percent	SRB Percent	CPU Percent Excluding Home SRB Time	IFA Percent	IFA on Perc
WLM	WLM	IEFPROC	STC	SYSTEM	1	0X000B		0.4	0.4	0.0		0.4	0.0
RMFGAT	RMFGAT	IEFPROC	STC	SYSTEM	1	0X02EE	STC20186	0.4	0.4	0.0		0.4	0.0
MASTER			STC	SYSTEM	1	0X0001	STC19479	0.0	0.0	0.0		0.0	0.0
PCAUTH	PCAUTH		STC	SYSTEM	1	0X0002		0.0	0.0	0.0		0.0	0.0
RASP	RASP		STC	SYSTEM	1	0X0003		0.0	0.0	0.0		0.0	0.0
TRACE	TRACE		STC	SYSTEM	1	0X0004		0.0	0.0	0.0		0.0	0.0
DUMPSRV	DUMPSRV	DUMPSRV	STC	SYSTEM	1	0X0005		0.0	0.0	0.0		0.0	0.0
XCFAS	XCFAS	IEFPROC	STC	SYSTEM	1	0X0006		0.0	0.0	0.0		0.0	0.0

Hub Time: Tue, 11/18/2014 05:43 PM Server Available

Address Space Overview - NC9042052049 - SYSADMIN *ADMIN MODE*

Start output SystemOut - Every... Administrator: Com... Address Space ... Tivoli Directory Inte... FileSeek v3.3 C:\ITMConnector\B... IBM Endpoint Mana... 5:44 PM

Launch SCA-LA (in context of LPAR) from OMEGAMON Workspace ...



SHARE
Educate · Network · Influence

Search results displayed in SCA-LA

The screenshot displays the IBM SmartCloud Analytics Log Analysis (SCA-LA) interface. The top navigation bar includes 'Administrative Settings', 'Learn More', and a user profile 'unityadmin'. The left sidebar shows a tree view of search patterns, with 'SystemName (1)' selected. The main panel shows a search for 'error AND (datasourceHostname:sp14*)' with a time range of '11/18/2014, 21:48:38 - 11/18/2014, 22:48:38 (UTC)'. The search results are displayed in a table with columns for time and message text. The results show an error message: 'DYNALOC FAILED RETURN CODE=04 ERROR RSN CODE=4714 INFO RSN CODE=041D VOLUME ALLOCATION FAILED'. The search string and the error message are highlighted in yellow.

Search string provided from OMEGAMON workspace

Notice there is only 1 SystemName (LPAR)

Search results with search strings highlighted

Insights surfaced during search

Simple Search Interface – Easy to Customize

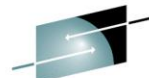


The screenshot shows the IBM SmartCloud Analytics Log Analysis web application in a Mozilla Firefox browser. The interface includes a left sidebar with navigation options: Quick Searches, Custom Apps, ExpertAdvice, Configured Patterns, and Discovered Patterns. The main content area has tabs for 'Getting Started' and 'New Search', with a '+ Add Search' button. A search input field contains an asterisk (*). To the right of the input field is a 'Search' button, a 'Last 15 Minutes' timeframe selector, and a 'Save My Search' button. Yellow callout boxes provide the following annotations:

- Enter search string**: Points to the search input field.
- Timeframe**: Points to the 'Last 15 Minutes' selector.
- Search specific logs or ALL logs**: Points to the dropdown menu next to the timeframe selector.
- Save My Search**: Points to the 'Save My Search' button.

WebSphere Application Server Search – java Exception pattern

Example of search capabilities plus insights



SHARE
Educate • Network • Influence

IBM SmartCloud Analytics Log Analysis

Administrative Settings | Learn More | unityadmin | IBM

Quick Searches: WAS_TVT7008, TVT7008_SYSLOG

Custom Apps

Configured Patterns

- exceptionPackageName (4)
- msgClassifier (32)
- _datasource (2)
- threadAddress (12)
- javaException (5)
 - org.apache.openjpa.persistence.PersistenceException (71)**
 - javax.ejb.EJBTransactionRolledbackException (18)
 - javax.servlet.ServletException (6)
 - javax.ejb.EJBException (2)
 - apache.openjpa.persistence.PersistenceException (1)
- hostname
 - exceptionClassName (4)
 - datasourceHostname (1)
 - exceptionMethodName (4)

Discovered Patterns

Getting Started | New Search | WAS_TVT7008 | + Add Search

javaException:=="org.apache.openjpa.persistence.PersistenceException" Search

Log Events Granularity : minute Time Range : 01/19/2014, 03:00:00 - 01/19/2014, 04:00:00 (UTC)

300
200
100
0
3:23 AM 3:24 AM 3:25 AM 3:26 AM

Timeframe of problem

< 1 to 100 of 638 >

exceptionPackageName	msgClassifier	_datasource	threadID
	BB000222I	TVT7008_SYSOUT	0X00000023
	BB000222I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BB000222I	TVT7008_SYSPRT	
	FFDC1003I	TVT7008_SYSOUT	0X00000015
	BB0J0011I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BB000222I	TVT7008_SYSPRT	
	BB000222I	TVT7008_SYSOUT	
	BB0J0051I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BB0J0077I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BB0J0077I	TVT7008_SYSPRT	

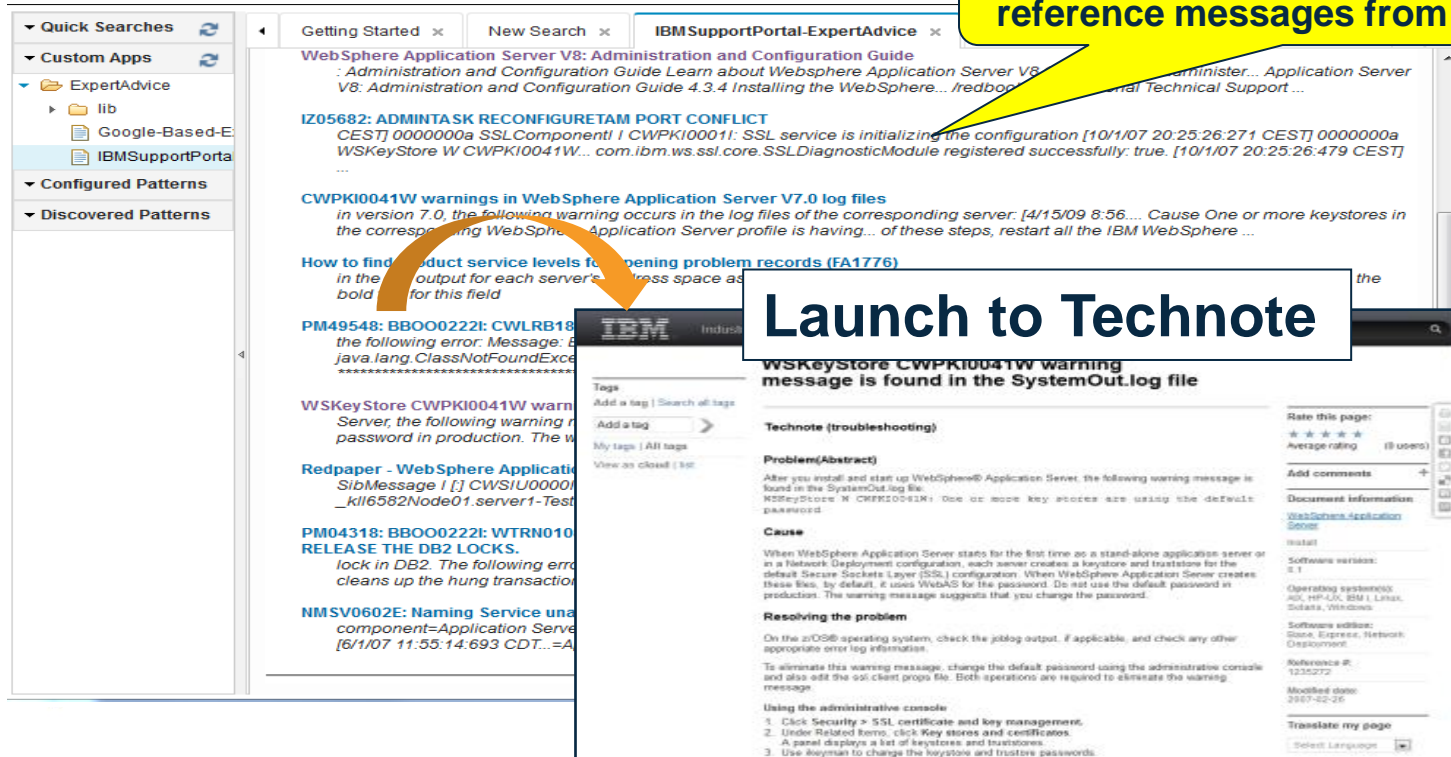
Log analysis displays number of exceptions during this timeframe

Search results

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, a sidebar contains navigation links: Quick Searches, Custom Apps, ExpertAdvice (with sub-links for lib, Google-Based-E, and IBMSupportPorta), Configured Patterns, and Discovered Patterns. The main content area shows search results for 'WebSphere Application Server V8: Administration and Configuration Guide'. A yellow callout bubble points to a search result entry: 'I205682: ADMINTASK RECONFIGURETAM PORT CONFLICT'. An orange arrow points from this entry to a detailed view of the message. The detailed view shows the message text, a 'Technote (troubleshooting)' link, and a 'Cause' section. A white box with the text 'Launch to Technote' is overlaid on the detailed view. The bottom of the detailed view shows a list of steps to resolve the problem.

Launch to Technote

WSKeyStore CWPKI0041W warning message is found in the SystemOut.log file

Technote (troubleshooting)

Problem(Abstract)

After you install and start up WebSphere® Application Server, the following warning message is found in the SystemOut.log file:

WSKeyStore W CPK0041W: One or more key stores are using the default password.

Cause

When WebSphere Application Server starts for the first time as a stand-alone application server or in a Network Deployment configuration, each server creates a keystore and truststore for the default Secure Sockets Layer (SSL) configuration. When WebSphere Application Server creates these files, by default, it uses WtbaS for the password. Do not use the default password in production. The warning message suggests that you change the password.

Resolving the problem

On the z/OS® operating system, check the joblog output. If applicable, and check any other appropriate error log information.

To eliminate this warning message, change the default password using the administrative console and also edit the ssl client props file. Both operations are required to eliminate the warning message.

Using the administrative console

1. Click Security > SSL, certificate and key management.
2. Under Related Items, click Key stores and certificates.
3. A panel displays a list of keystores and truststores.
4. Use the panel to change the keystore and truststore passwords.

Sample dashboard – Out-of-the-Box or Build your Own!

