



IBM Software Group

# Automating problem identification using IBM Autonomic Computing technology

Denilson Nastacio



WebSphere® Support Technical Exchange



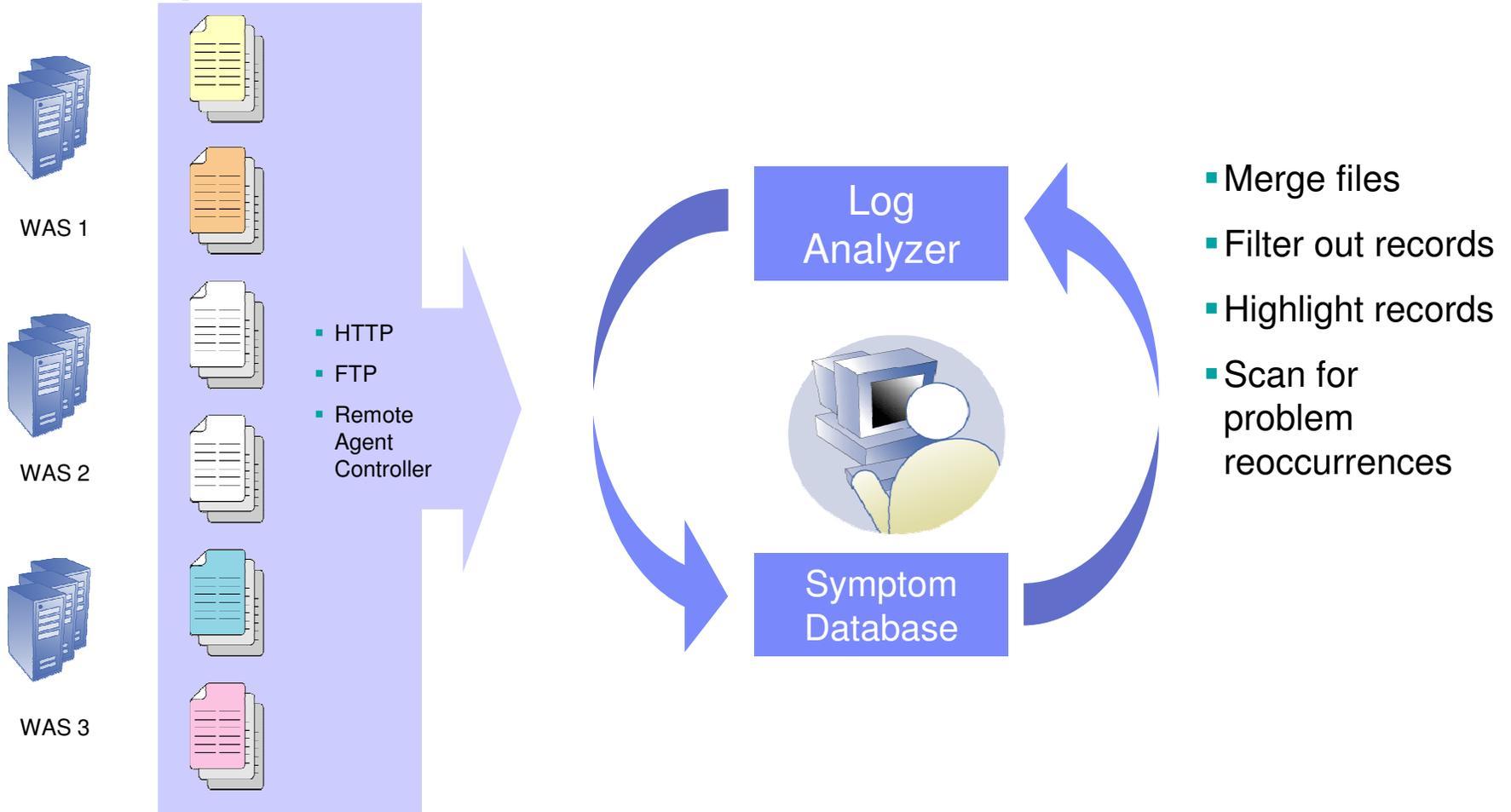
# Agenda

- The business cases for Log Analysis
- Tool overview
  - ▶ IBM Support Assistant
  - ▶ Log Analyzer
  - ▶ Symptom Editor
- Case study
  - ▶ A recurring security error in a WAS installation

## When customers call...

- Recreate the problem
- Run a diagnosis tool
- Google...Google again
- Ask a coworker...wait for him to Google...again
- When all else fails, read the logs entries, all thousands...Google them

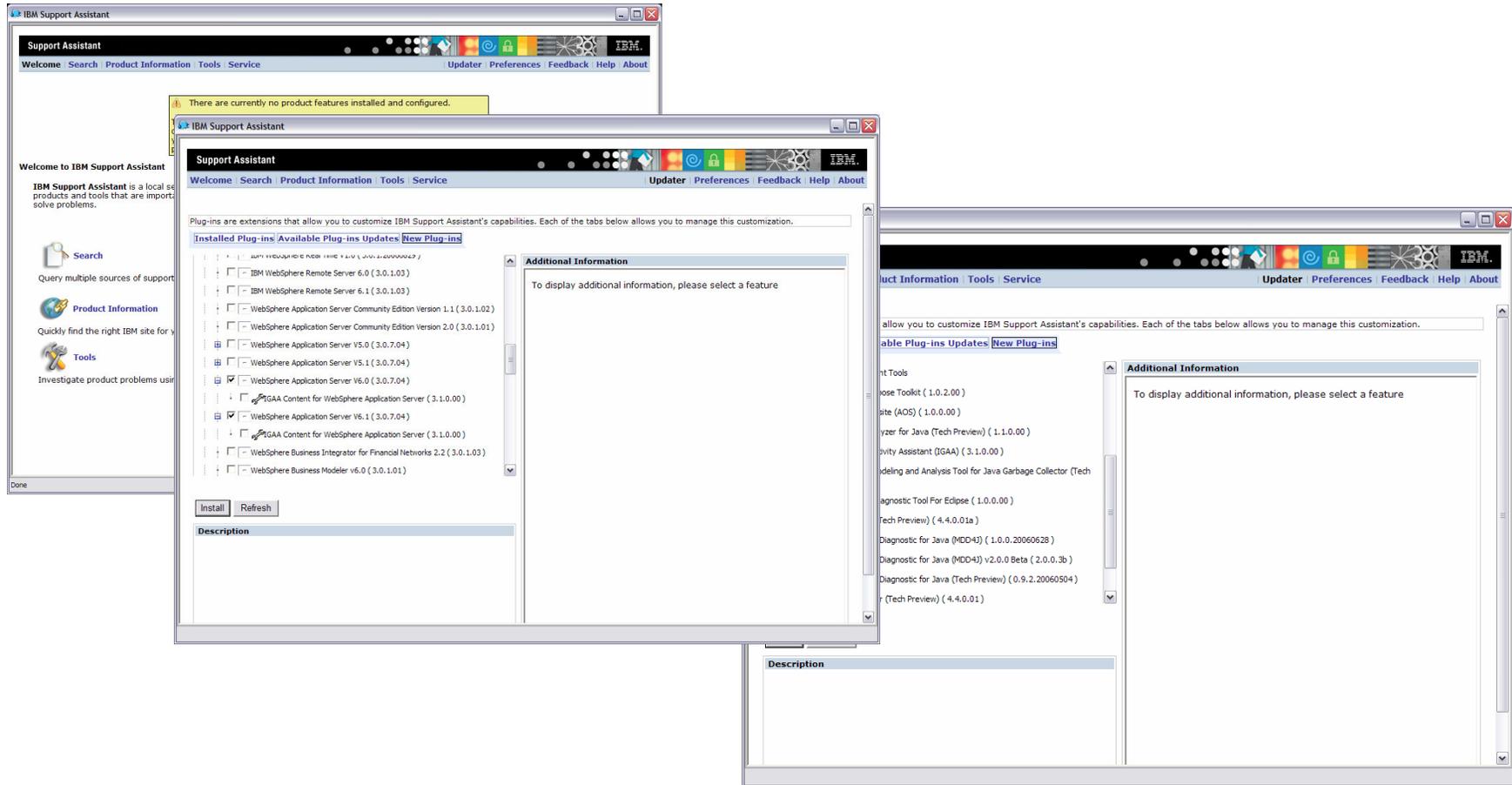
# When problem hits



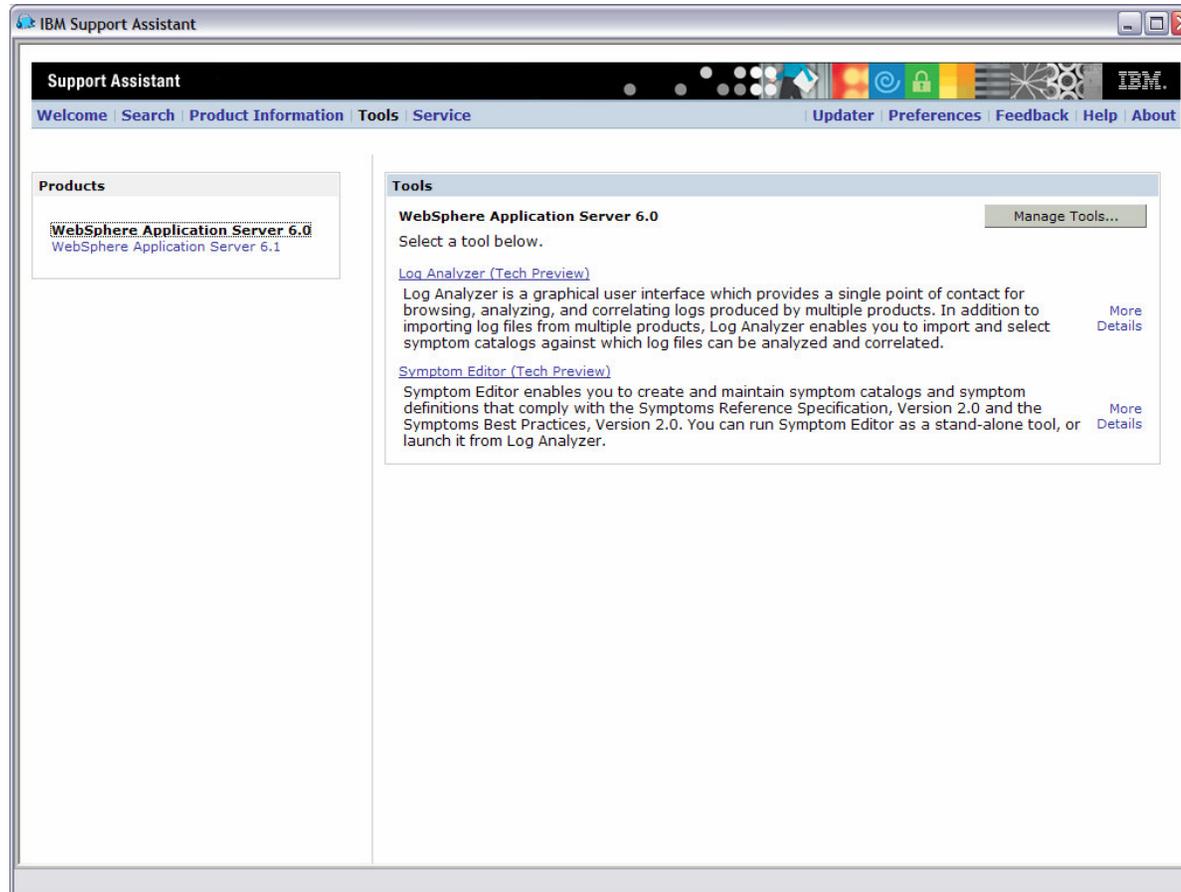
# IBM Support Assistant

- Download
- Install product plug ins
  - ▶ WebSphere Application Server
  - ▶ Other IBM products
- Install tool plug ins
  - ▶ Log Analyzer
  - ▶ Symptom Editor
- <http://www.ibm.com/software/support/isa/>

# Product specific and common plug ins

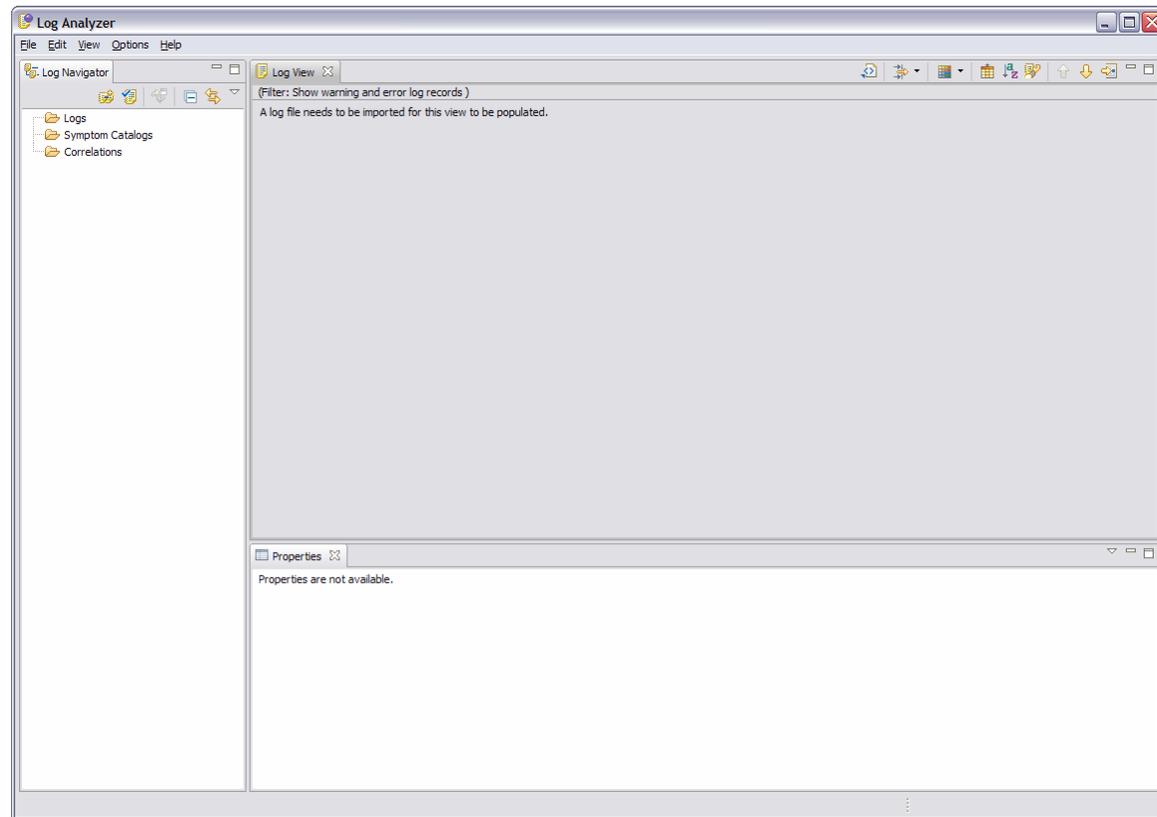


# Select a product...and...launch a tool



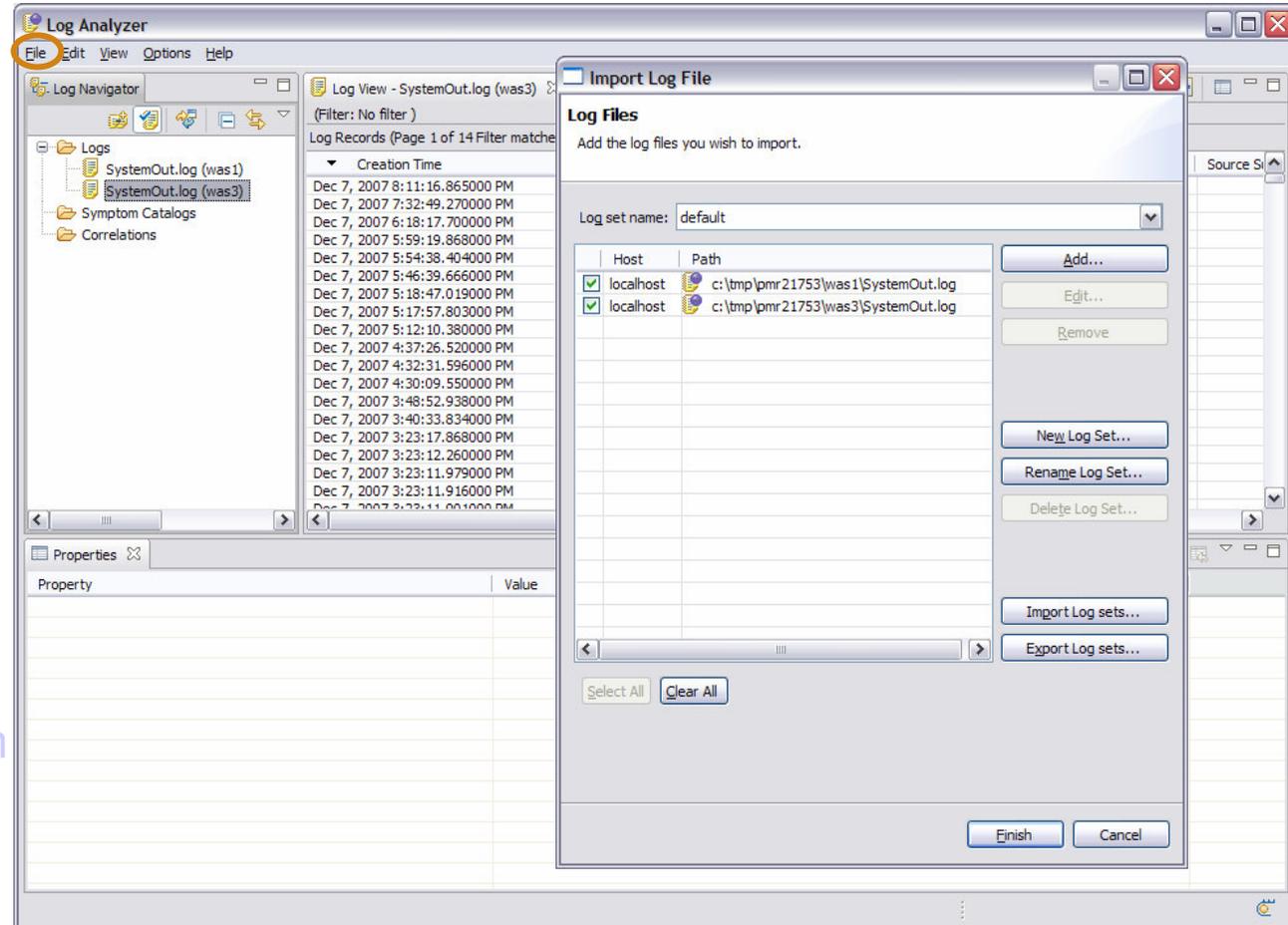
# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches



# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches



# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches

The screenshot shows the Log Analyzer application window. The main display area contains a table of log records. The table has the following columns: Creation Time, Severity, Message Text, Situation Type, Source Component, and Source Stack. The records are filtered to show 14 records on page 1 of 14, with a total of 135527 records matching the filter. The messages include various system logs and error reports, such as '2 user.CanAccess(APPROVAL\_MNG...', 'APACHE LOG:/en/search/images/sp...', 'GMWB MAV: Match at Pos = 27', and 'From CVQ screenOWNERDOB&&&&...'.

# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches

The screenshot displays the IBM Log Analyzer main screen. The interface includes a 'Log Navigator' on the left, a central 'Log View' table, and a 'Filters' dialog box in the foreground. The 'Log View' table shows log records with columns for Creation Time, Severity, Message Text, Situation Type, Source Component, and Source Sub-component. The 'Filters' dialog box is open, showing an 'Edit filter' window with a filter name 'No socket exceptions' and an advanced filtering table. The advanced filtering table has columns for Attribute, Operator, and Value, with one entry: 'Message Text' with operator '<>' and value '\*java.net.Socket\*'. The dialog also shows a group expression set to 'AND'.

Creation Time	Severity	Message Text	Situation Type	Source Component...	Source Sub-compon...
Dec 6, 2007 7:43:01.048000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 6, 2007 7:45:11.609000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 6, 2007 7:45:14.656000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 6, 2007 7:47:37.046000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 6, 2007 7:47:38.749000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 6, 2007 7:59:42.369000 PM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 6, 2007 9:42:14.400000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 6, 2007 9:59:52.680000 PM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 6, 2007 9:59:56.737000 PM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 6, 2007 10:41:57.237000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 6, 2007 10:50:39.358000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup
Dec 7, 2007 7:57:32.424000 AM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 7, 2007 7:57:38.073000 AM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 7, 2007 9:57:48.877000 AM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 7, 2007 11:58:02.269000 AM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 7, 2007 1:57:23.005000 PM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 7, 2007 1:58:16.660000 PM	50	SECJ0306E: No received or invocation credential e...	ReportSituation	IBM WebSphere Ap...	RoleBasedAuth
Dec 7, 2007 2:57:23.247000 PM	50	SRVE0026E: [Servlet Error]-]: java.lang.NullPointe...	ReportSituation	IBM WebSphere Ap...	WebGroup

# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches

The screenshot shows the Log Analyzer application window. The 'Log Navigator' on the left shows a tree structure with 'Logs' (containing SystemOut.log files) and 'Symptom Catalogs'. The main 'Log View' pane displays a table of log records. The table has columns: Creation Time, Severity, Message Text, Situation Type, Source Component, and Source Sub-component. The records are filtered to show 18 of 224721 records. The bottom pane shows 'Event Details' for a selected record, including a stack trace and fields for Creation Time, Severity, Version, and Priority.

Creation Time	Severity	Message Text	Situation Type	Source Component	Source Sub-component
Dec 7, 2007 2:57:23.247000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 7, 2007 1:58:16.660000 PM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 7, 2007 1:57:23.005000 PM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 7, 2007 11:58:02.269000 AM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 7, 2007 9:57:48.877000 AM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 7, 2007 7:57:38.073000 AM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 7, 2007 7:57:32.424000 AM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 6, 2007 10:50:39.358000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 6, 2007 10:41:57.237000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 6, 2007 9:59:56.737000 PM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 6, 2007 9:59:52.680000 PM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 6, 2007 9:42:14.400000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 6, 2007 7:59:42.369000 PM	50	SECJ0306E: No received or invocati...	ReportSituation	IBM WebSphere Ap...	Rolef
Dec 6, 2007 7:47:38.749000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 6, 2007 7:47:37.046000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 6, 2007 7:45:14.656000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 6, 2007 7:45:11.609000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	
Dec 6, 2007 7:43:01.048000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM WebSphere Ap...	

**Event Details**

Additional Data Attributes

Correlation Data Attributes

Situation

Message Information

Source Component

Reporting Component

Associated Event

Message Text

```
SRVE0026E: [Servlet Error]-[]: java.lang.NullPointerException at java.lang.Floatin...
```

Creation Time: Dec 6, 2007 9:42:14.400000 PM

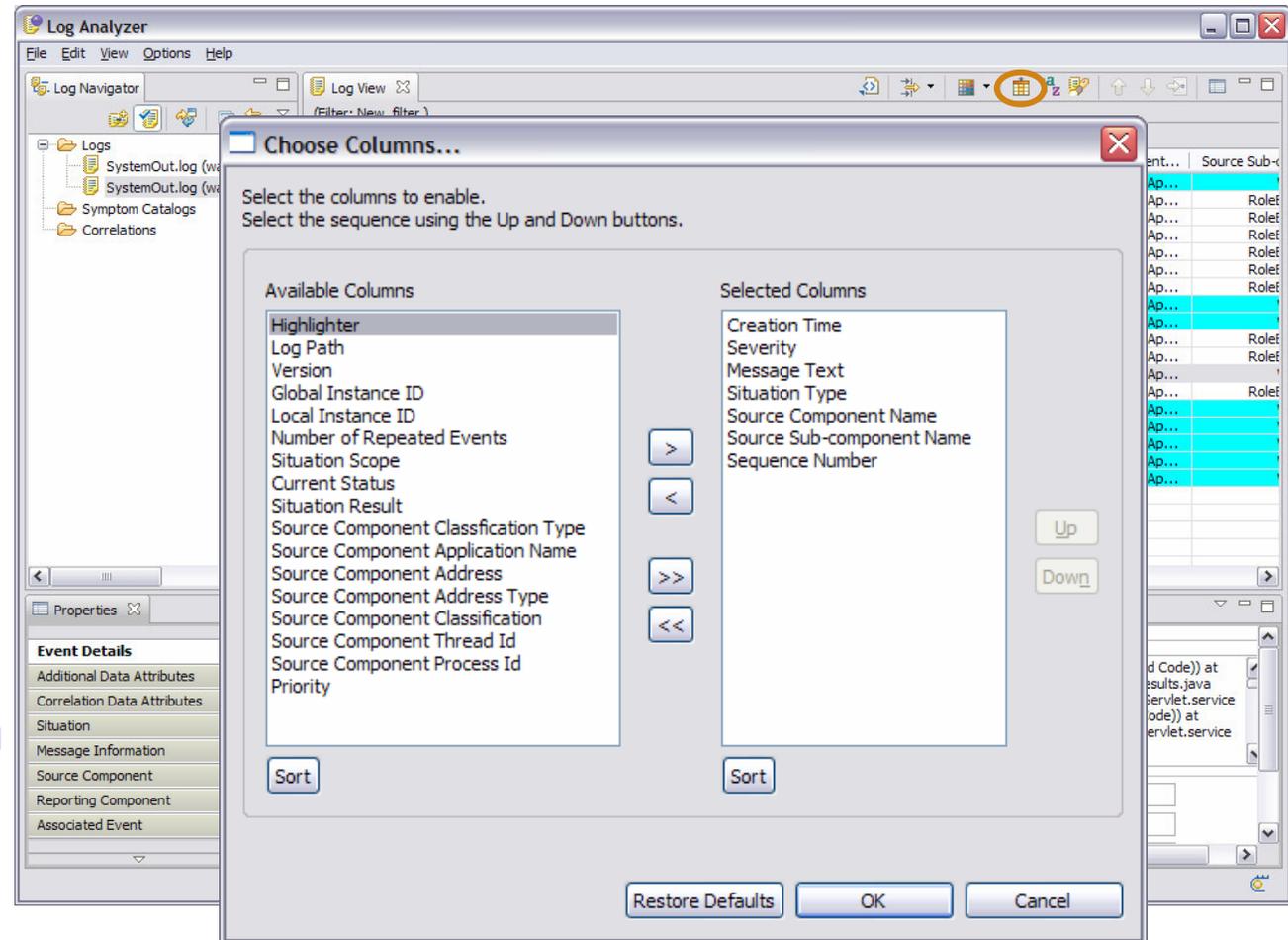
Severity: 50

Version: 1.0.1

Priority: 0

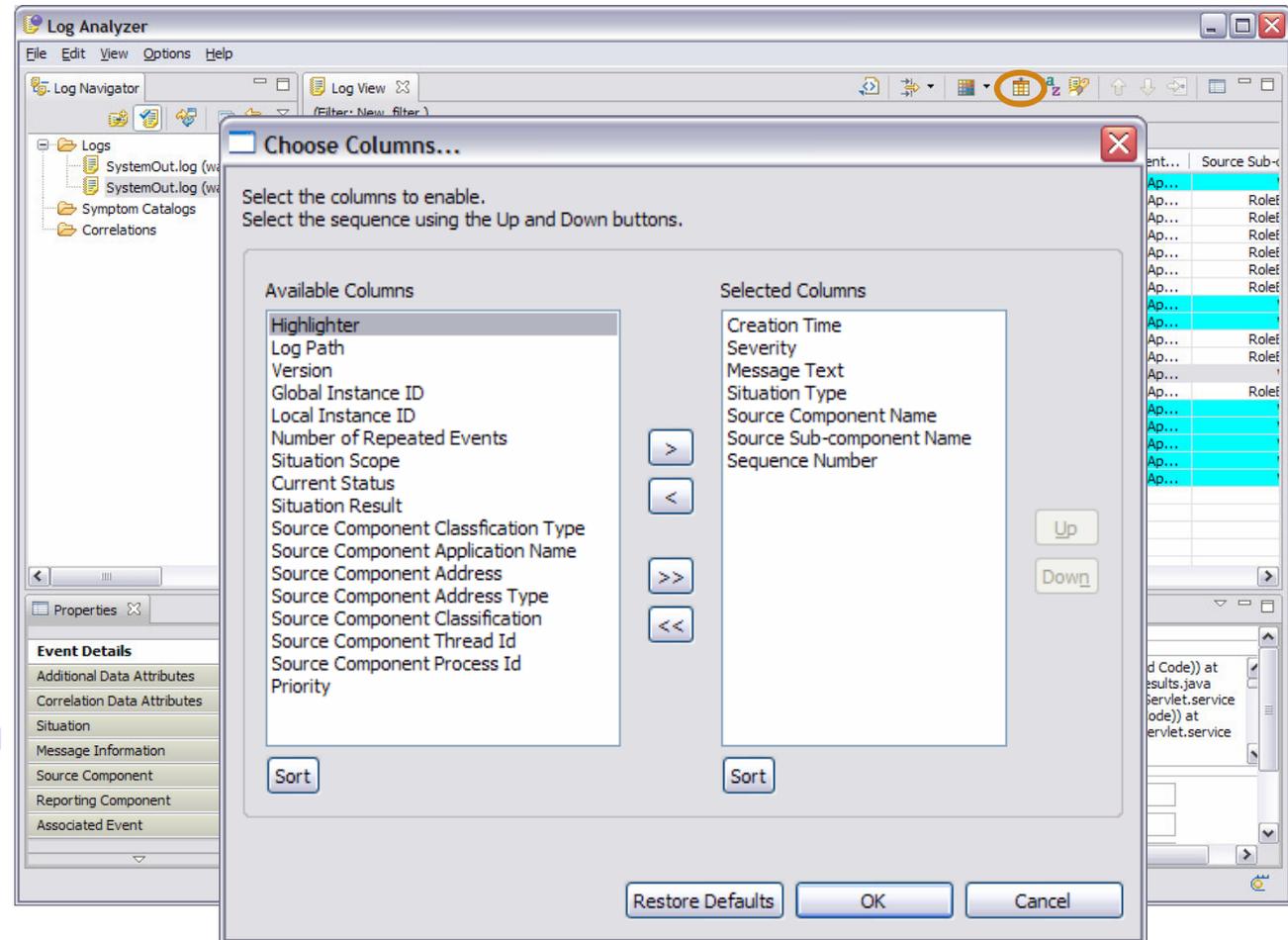
# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches



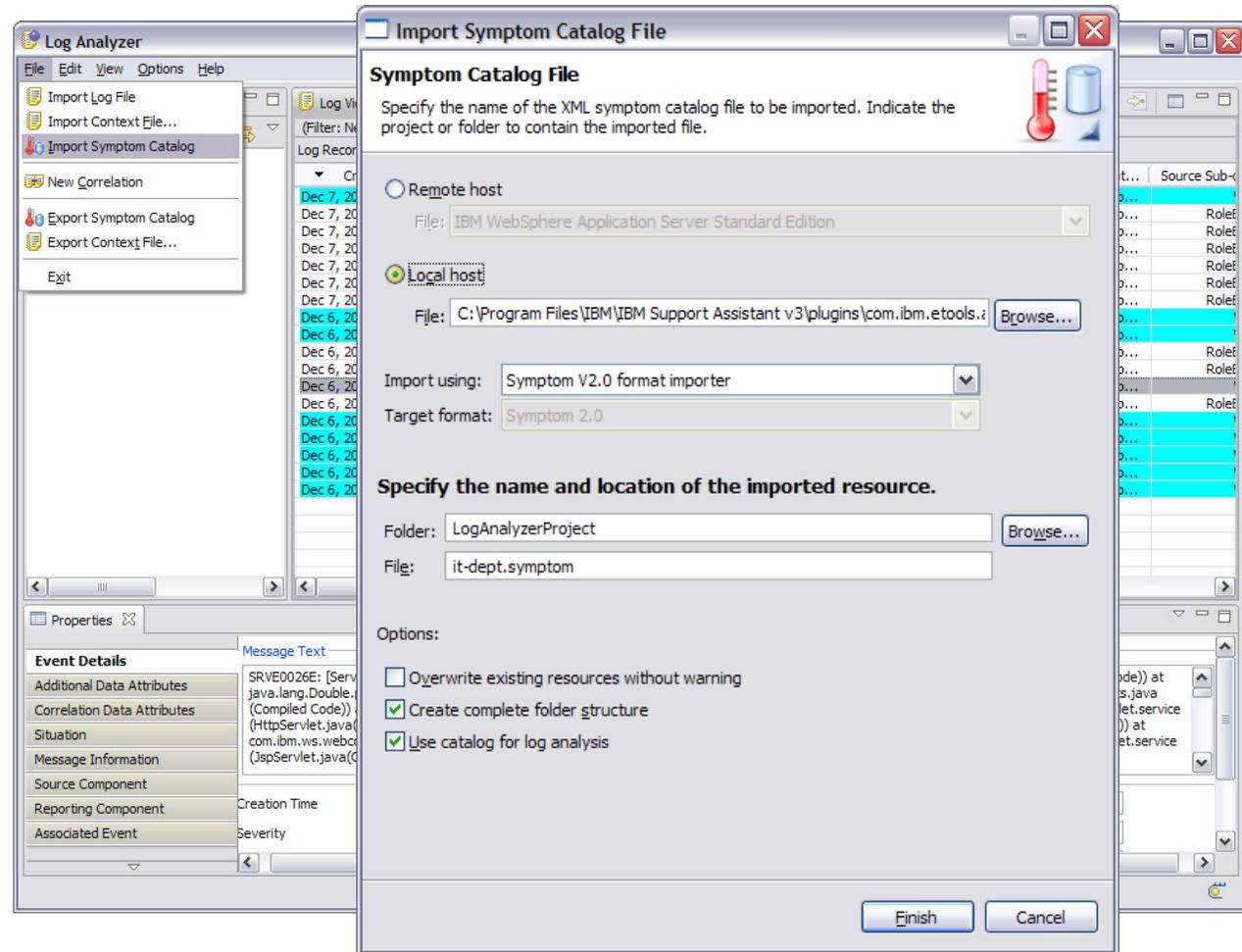
# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches



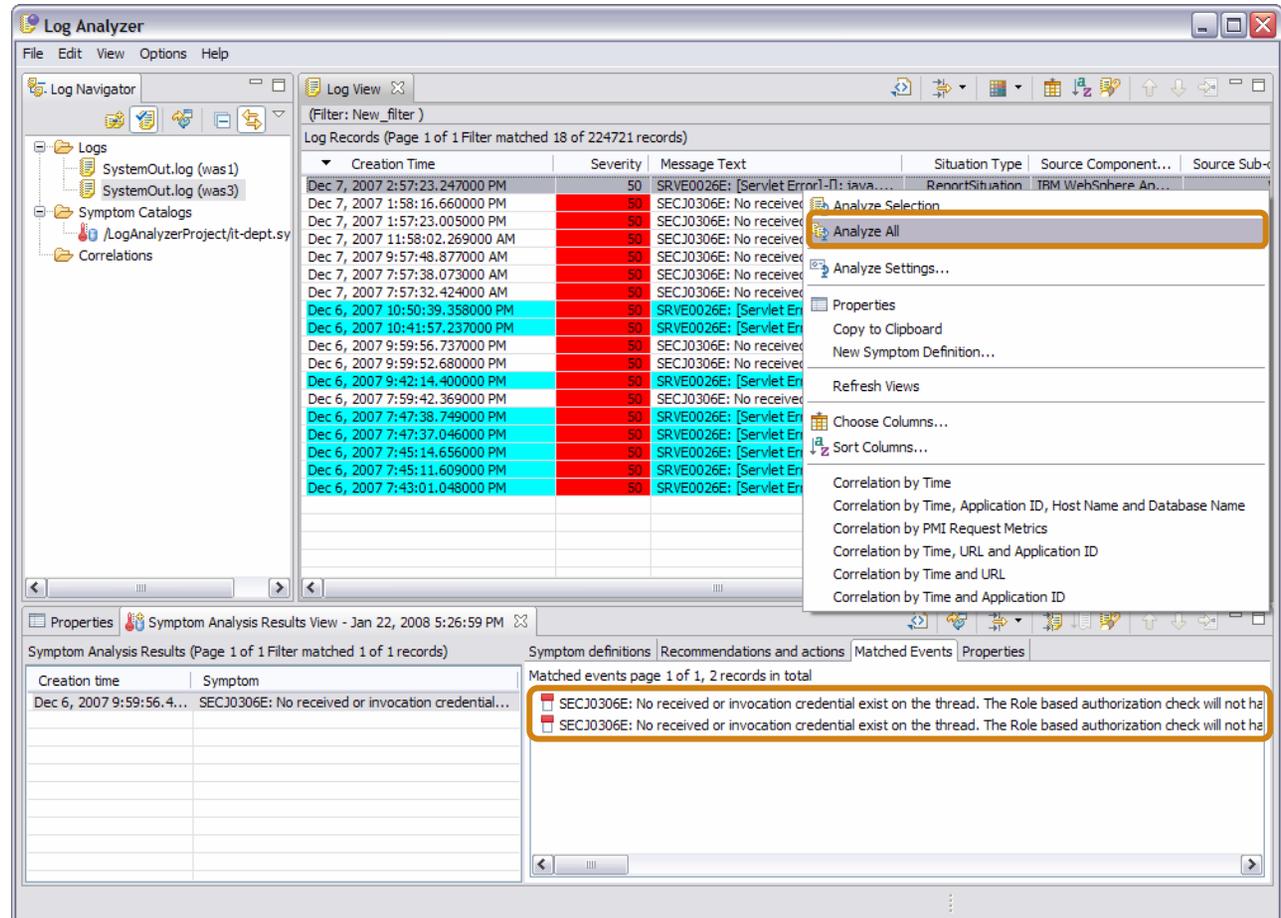
# Log Analyzer Main Screen

- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches



# Log Analyzer Main Screen

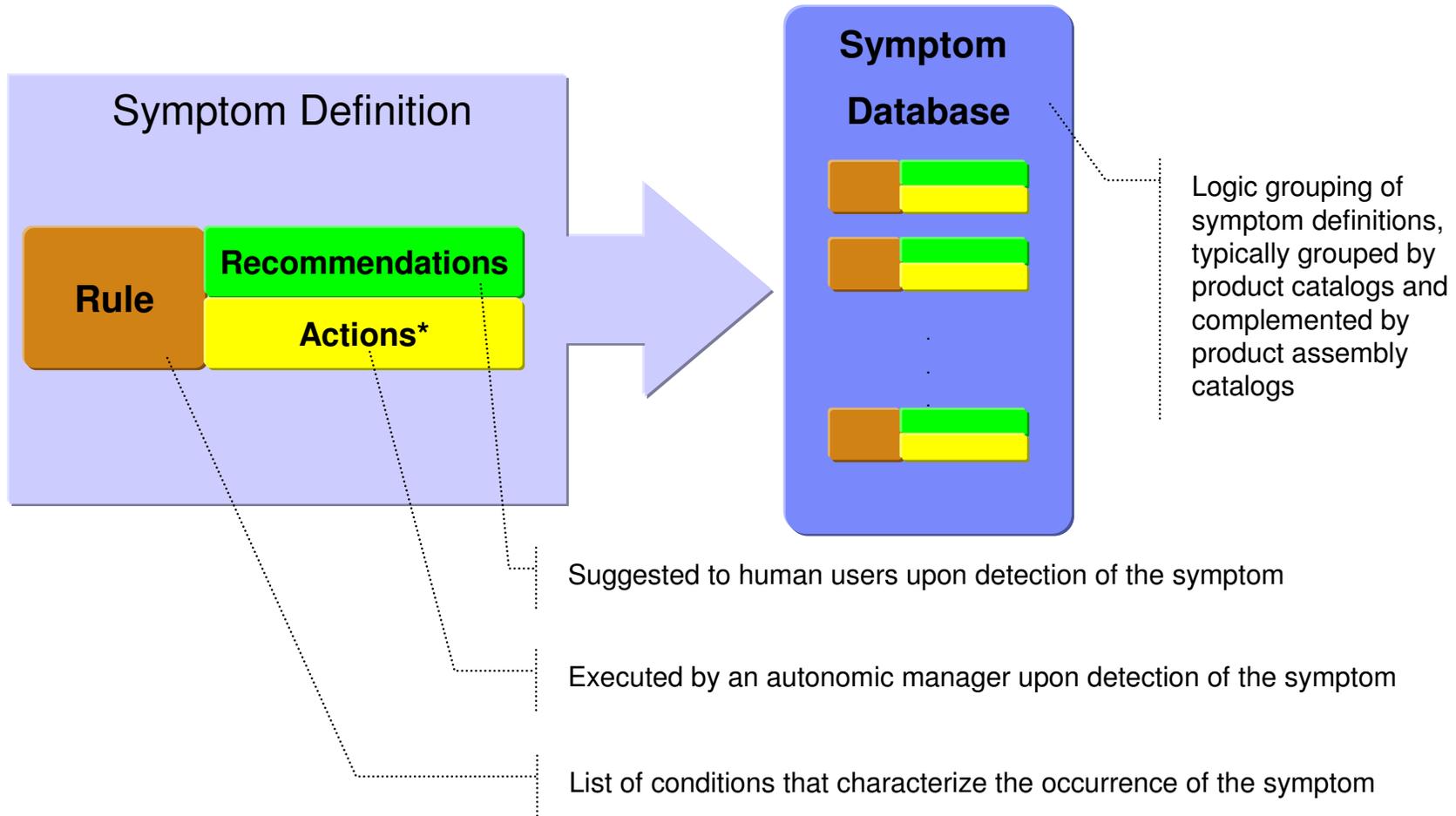
- Import log files
- Merge log files
- Apply filters
- Apply highlighters
- Choose and reorder columns
- Import symptom databases
- Scan for symptom matches



Symptom matches, you say?



# Symptom Definitions and Symptom Databases



# Symptom examples

event .msgid=CEI0011E and  
situation.category=connect

“...verify that the JMS message provider used by the Common Event Infrastructure is up and running, you can find the provider hostname by...”

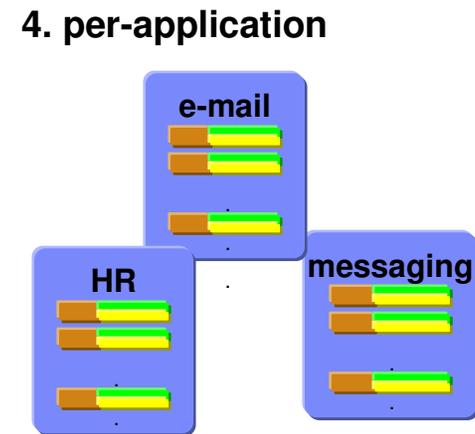
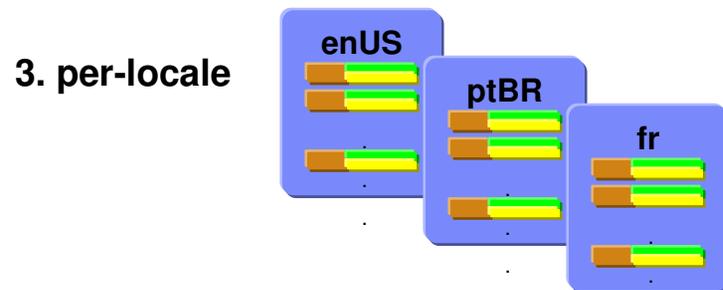
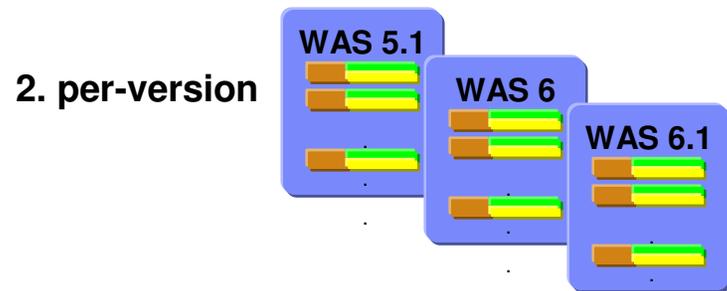
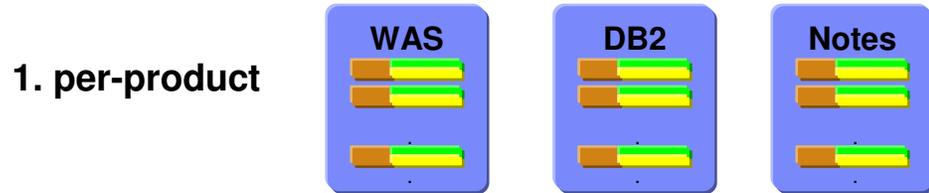
No Actions

event .msgid=CEI0011E and  
situation.category=connect  
AND  
previously.observed.event.msg  
id=JMS0089I

“The JMS server used by the Common Event Infrastructure is stopped”

wsadmin -hostname {0} -f startjms.jacl

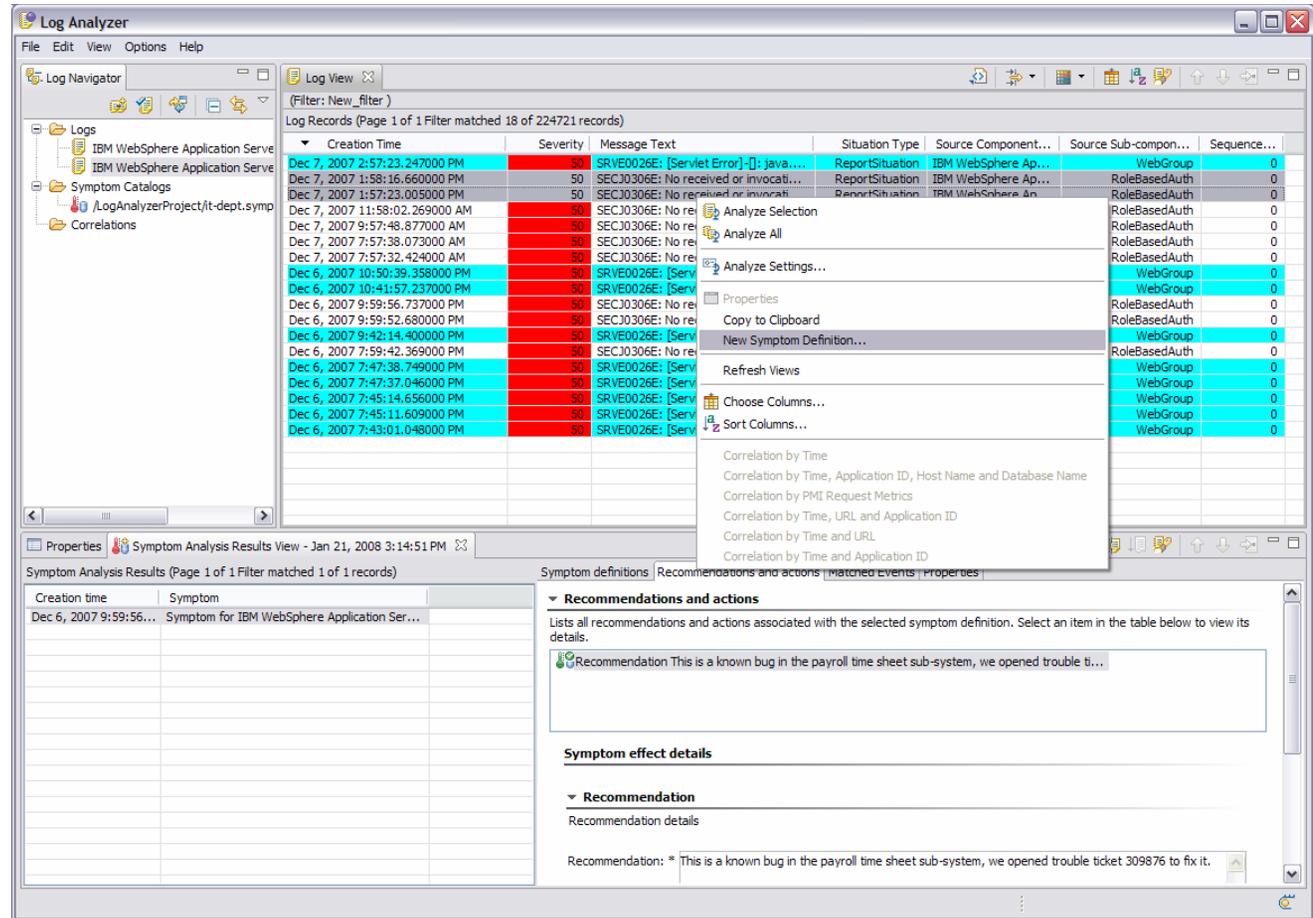
# Symptom Databases (suggestions)



... etc ...

# Creating new symptom definitions

1. Select events
2. Select pattern
3. Add recommendation
4. Share the symptom definitions



# Creating new symptom definitions

**Log Analyzer**

Log View (Filter: New\_filter)

Log Records (Page 1 of 1 Filter matched 18 of 224721 records)

Creation Time	Severity	Message Text	Situation Type	Source
Dec 7, 2007 2:57:23.247000 PM	50	SRVE0026E: [Servlet Error]-[]: java....	ReportSituation	IBM W
Dec 7, 2007 1:58:16.660000 PM	50	SECJ0306E: No received or invocab...	ReportSituation	IBM W
Dec 7, 2007 1:57:23.005000 PM	50	SECJ0306E: No received or invocab...	ReportSituation	IBM W
Dec 7, 2007 11:58:02.269000 AM	50	SECJ0306E: No rel		
Dec 7, 2007 9:57:48.877000 AM	50	SECJ0306E: No rel		
Dec 7, 2007 7:57:38.073000 AM	50	SECJ0306E: No rel		
Dec 7, 2007 7:57:32.424000 AM	50	SECJ0306E: No rel		
Dec 6, 2007 10:50:39.358000 PM	50	SRVE0026E: [Serv		
Dec 6, 2007 10:41:57.237000 PM	50	SRVE0026E: [Serv		
Dec 6, 2007 9:59:56.737000 PM	50	SECJ0306E: No rel		
Dec 6, 2007 9:59:52.680000 PM	50	SECJ0306E: No rel		
Dec 6, 2007 9:42:14.400000 PM	50	SRVE0026E: [Serv		
Dec 6, 2007 7:59:42.369000 PM	50	SECJ0306E: No rel		
Dec 6, 2007 7:47:38.749000 PM	50	SRVE0026E: [Serv		
Dec 6, 2007 7:47:37.046000 PM	50	SRVE0026E: [Serv		
Dec 6, 2007 7:45:14.656000 PM	50	SRVE0026E: [Serv		
Dec 6, 2007 7:45:11.609000 PM	50	SRVE0026E: [Serv		
Dec 6, 2007 7:43:01.048000 PM	50	SRVE0026E: [Serv		

**New Symptom Definition**

Symptom Rule

Rules for identifying the symptom

Rule type: Sequence Pattern

Version: 1.0

Description: SECJ0306E: No received or invocation credential exist on the thread. The Role based authorization check will not have an accessId of the caller to check. The parameters are: access check method getState on resource Server and module Server. The stack trace is java.lang.Exception: dump thread stack for debugging com.ibm.ws.security.role.RoleBasedAuthorizerImpl.checkAccess

Event selector: Symptom for IBM WebSphere Application Server - Express\_ProductName\_20080121034018

- Event Selector
  - If ANY of the following are true:
  - Event Selector
    - If ANY of the following are true:

Rule qualified by each value of:

Attribute:

Sequence rule options:  Ordered sequence

Time window: 5 Seconds

**Symptom Recommendation and Action**

Recommendations and actions for the symptom

Name: Symptom Effect for Symptom for IBM WebSphere Application Server - Express\_ProductName\_20080121034018

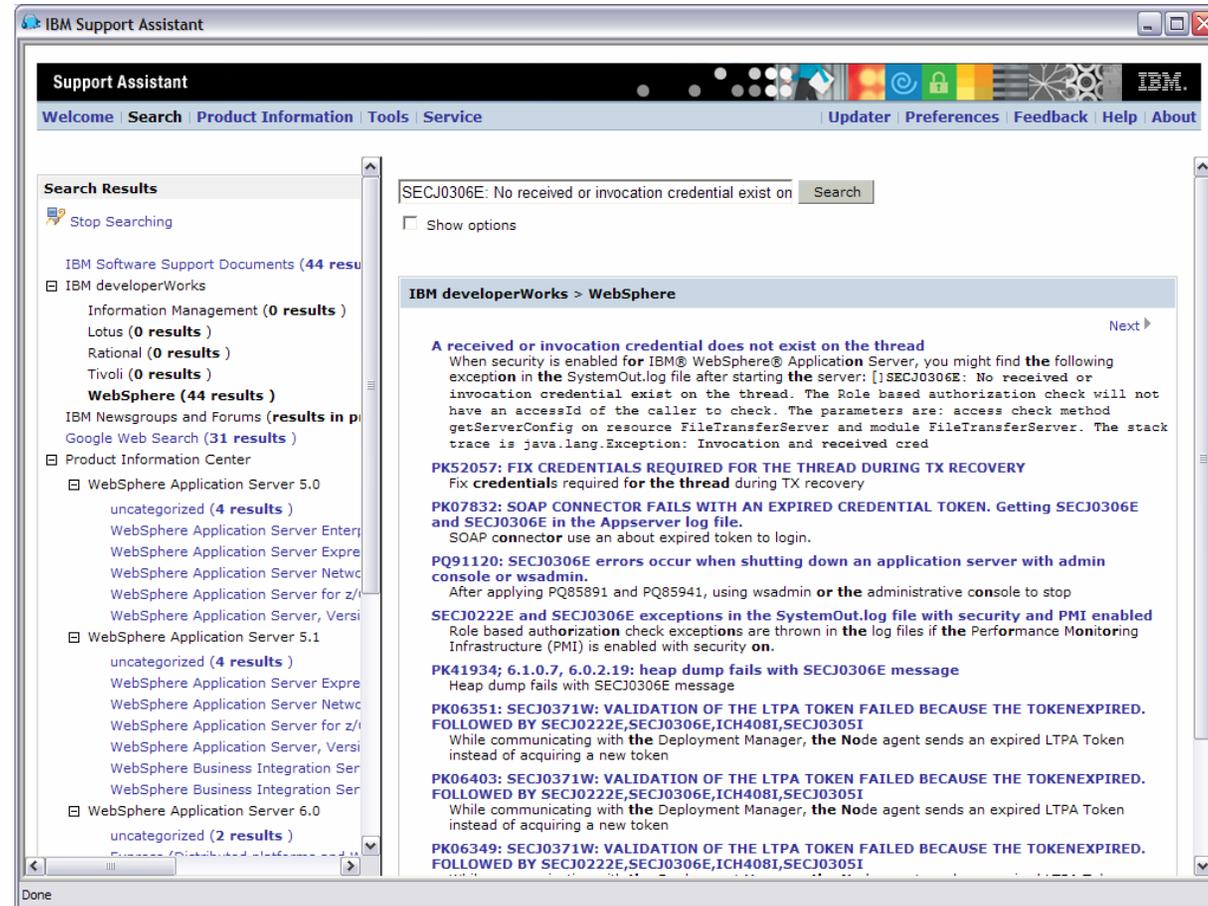
Version: 1.0

Description: SECJ0306E: No received or invocation credential exist on the thread. The Role based authorization check will not have an accessId of the caller to check. The parameters are: access check method getState on resource Server and module Server. The stack trace is java.lang.Exception: dump thread stack for debugging com.ibm.ws.security.role.RoleBasedAuthorizerImpl.checkAccess (RoleBasedAuthorizerImpl.java:292) at com.ibm.ws.management.AdminServiceImpl.preInvoke(AdminServiceImpl.java:1347) at com.ibm.ws.management.AdminServiceImpl.invoke(AdminServiceImpl.java:637) at

Recommendation: Multiple instances of the service are running on different services, contact application administrator and ask that he kills one of them.

# Where do you get your recommendations?

- Colleagues
- “Oh, you knew about it...”
- ISA Federated Search

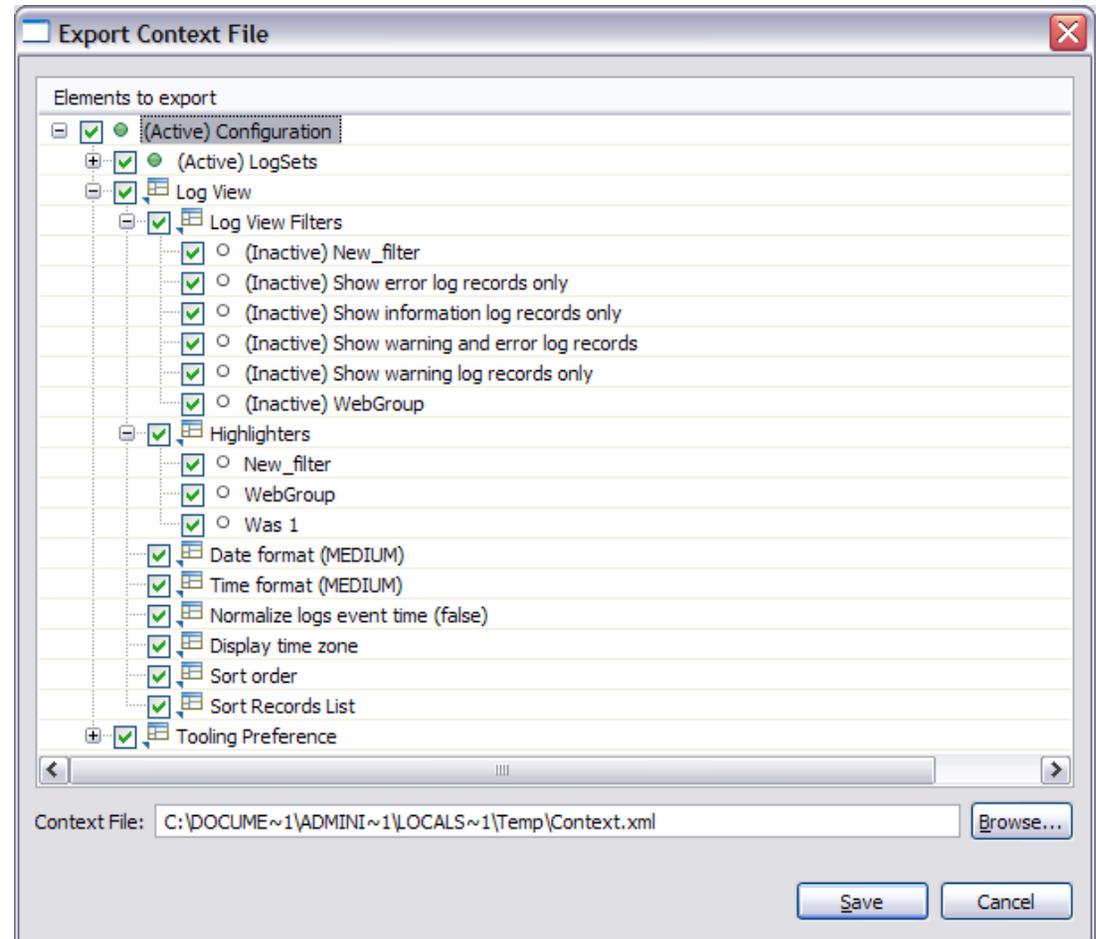


# Sharing your settings and findings



# Collaboration with other specialists

- Export and import configuration
- Filters
- Highlighters
- Sorting
- Column choices
- Data formats



# Share the results...

**Symptom Analysis Results (1 matches exported)**

Creation time	Priority	Probability	Properties
Dec 6, 2007 9:59:56.400000 PM	50	100	<p><b>Resource</b> IBM WebSphere Application Server - Express</p> <p><b>Descriptions</b> SECJ0306E: No received or invocation credential exist on the thread. The Role based authorization check will not have an accessId of the caller to check. The parameters are: access check method getState on resource Server and module Server. The stack trace is java.lang.Exception: dump thread stack for debuggingat com.ibm.ws.security.role.RoleBasedAuthorizerImpl.checkAccess(RoleBasedAuthorizerImpl.java:292) at com.ibm.ws.management.AdminServiceImpl.preInvoke(AdminServiceImpl.java:1347) at com.ibm.ws.management.AdminServiceImpl.invoke(AdminServiceImpl.java:657) at com.ibm.ws.management.connector.AdminServiceDelegator.invoke(AdminServiceDelegator.java:130) at sun.reflect.GeneratedMethodAccessor14.invoke(Unknown Source) at java.lang.reflect.Method.invoke(Method.java:Compiled Code)) at com.ibm.ws.management.connector.soap.SOAPConnector.invoke(SOAPConnector.java:Compiled Code) at com.ibm.ws.management.connector.soa</p> <p><b>Recommendations</b> Multiple instances of the service are running on different services, contact application administrator and kill one of them.</p> <p><b>Matched Events</b> Dec 6, 2007 9:59:52.680000 PM SECJ0306E: No received or invocation credential exist on the thread. The Role based authorization check will not have an accessId of the caller to check. The parameters are: access check method getState on resource Server and module Server. The stack trace is java.lang.Exception: dump thread stack for debuggingat com.ibm.ws.security.role.RoleBasedAuthorizerImpl.checkAccess(RoleBasedAuthorizerImpl.java:292) at com.ibm.ws.management.AdminServiceImpl.preInvoke(AdminServiceImpl.java:1347) at com.ibm.ws.management.AdminServiceImpl.invoke(AdminServiceImpl.java:657) at com.ibm.ws.management.connector.AdminServiceDelegator.invoke(AdminServiceDelegator.java:130) at sun.reflect.GeneratedMethodAccessor14.invoke(Unknown Source) at java.lang.reflect.Method.invoke(Method.java:Compiled Code)) at com.ibm.ws.management.connector.soap.SOAPConnector.invoke(SOAPConnector.java:Compiled Code) at com.ibm.ws.management.connector.soa</p>

Situation Type	Source Component Name
ReportSituation	IBM WebSphere Application Server - Express
ReportSituation	IBM WebSphere Application Server - Express
	IBM

## Summary

- Log Analyzer as a triage tool
- Filter what you do not want to see
- Highlight what it is important
- Record new found knowledge in a symptom definition
- Save your time...and others' too

## Resources

- IBM Support Assistant
  - ▶ <http://www.ibm.com/software/support/isa/>
  
- Apache Derby (for large log support)
  - ▶ <http://db.apache.org/derby/>
  
- DB2® Express (for large log support)
  - ▶ <http://www.ibm.com/software/data/db2/udb/support/downloadv8.html>

## Resources (symptoms databases)

- Symptoms deep-dive series
  - ▶ <http://www.ibm.com/developerworks/autonomic/library/ac-symptom1/>
- Eclipse Test & Performance Tools Platform
  - ▶ <http://www.eclipse.org/tptp/>
- Symptoms best-practice
  - ▶ [http://download.boulder.ibm.com/ibmdl/pub/software/dw/opensource/btm/SymptomBestPractices\\_v2.0.pdf](http://download.boulder.ibm.com/ibmdl/pub/software/dw/opensource/btm/SymptomBestPractices_v2.0.pdf)
- Symptom Catalog 2.0 specification
  - ▶ [http://download.boulder.ibm.com/ibmdl/pub/software/dw/opensource/btm/SymptomSpec\\_v2.0.pdf](http://download.boulder.ibm.com/ibmdl/pub/software/dw/opensource/btm/SymptomSpec_v2.0.pdf)

# Additional WebSphere Product Resources

- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:  
<http://www.ibm.com/developerworks/websphere/community/>
- Learn about other upcoming webcasts, conferences and events:  
[http://www.ibm.com/software/websphere/events\\_1.html](http://www.ibm.com/software/websphere/events_1.html)
- Join the Global WebSphere User Group Community: <http://www.websphere.org>
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:  
<http://www.ibm.com/software/info/education/assistant>
- View a Flash replay with step-by-step instructions for using the Electronic Service Request (ESR) tool for submitting problems electronically:  
<http://www.ibm.com/software/websphere/support/d2w.html>
- Sign up to receive weekly technical My support emails:  
<http://www.ibm.com/software/support/einfo.html>

# Questions and Answers

