

InfoSphere Information Server

How to use logging components



© 2011 IBM Corporation

This presentation explains how to use InfoSphere® Information Server version 8 logging components to capture trace information.

Objectives

- What are logging components
- How to configure logging components
- How to use log views

The objectives of this presentation are to explain what the Information Server logging components are, how to use them to generate debugging information and how to use log views to view this information.

What are logging components?

- Information Server stores event messages with information about its processes
- Messages are organized by components and severity levels
- Logging components control what components and severities will store messages
- Most used components are: CAS, ISD, ISF

Information Server can save event messages with information about the processes that run in the suite. These messages are organized by components and severity levels. A component represents a specific area of the suite. A severity level indicates how critical the message is. The logging components are used to define what components and what severities are stored in the metadata repository. Some of the most used components are the connector Access, referred to as CAS, the Information Services Director, referred to as WISD in version 8.1 and ISD in version 8.5, and the Information Server Framework, referred to as ISF. The CAS component can be used to troubleshoot connectivity problems in Information Analyzer, node agents exceptions, or common connector problems in DataStage®. The ISD and ISF components can be used to troubleshoot problems involving ISD jobs. For this presentation you will configure and retrieve information using the CAS Component.

How to configure logging components (1 of 5)

- Open Information Server web console
 - Example: Logging components for connector access

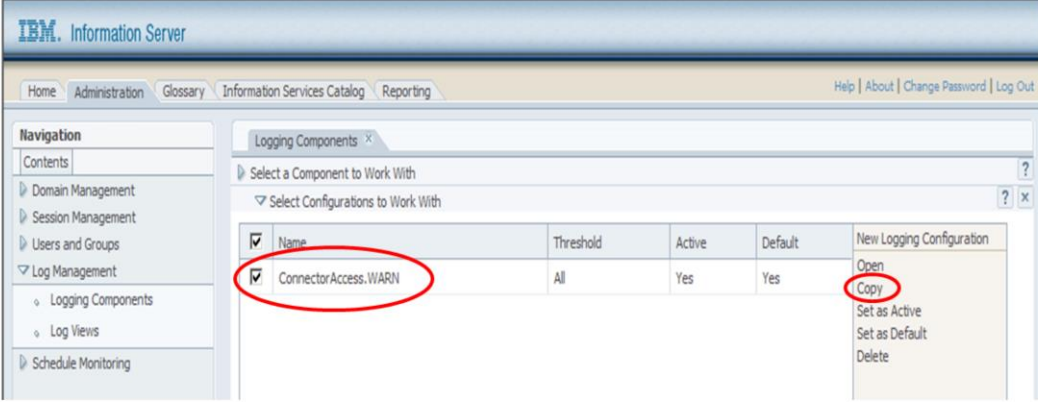
The screenshot shows the IBM Information Server web console interface. The top navigation bar includes 'Home', 'Administration', 'Glossary', 'Information Services Catalog', and 'Reporting'. The 'Administration' tab is active. On the left, the 'Navigation' pane shows 'Log Management' expanded to 'Logging Components'. The main content area displays a table of logging components with columns for Name, Active Configuration, and Default Configuration. The 'Connector Access' component is selected, and the 'Manage Configurations' link is highlighted. A table with the following data is shown:

Name	Active Configuration	Default Configuration	Manage Configurations
BrowseService	Glossary	Glossary	
Connector Access	ConnectorAccess.WARN	ConnectorAccess.WARN	
DataStage	DataStage.ALL	DataStage.ALL	
Information Analyzer	InformationAnalyzer.WARN	InformationAnalyzer.WARN	
ISF	ISF.WARN	ISF.WARN	
ISF Agent	ISFAgent.WARN	ISFAgent.WARN	
ISTools	ISTools.INFO	ISTools.INFO	
Mapping Services	FastTrack	FastTrack	

The logging components are configured using the Information Server web console. First, open the web console and click the “Administration” tab. Next, click “Log Management” and then click “Logging Components”. You will see the list of all available logging components. For this example, click “Connector Access” to work with this component. Click “Manage Configurations”.

How to configure logging components (2 of 5)

- Select Configuration
- Create copy



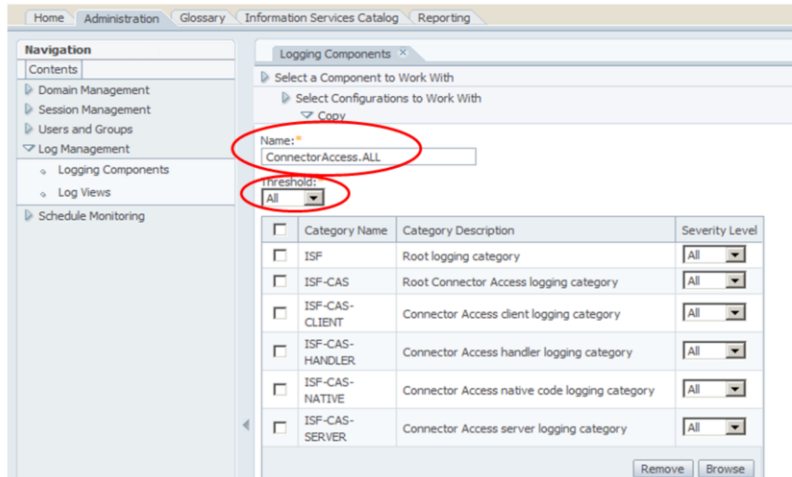
The screenshot shows the IBM Information Server Administration console. The main content area displays a table of logging configurations for a selected component. The table has columns for Name, Threshold, Active, Default, and New Logging Configuration. The configuration 'ConnectorAccess.WARN' is selected, and the 'Copy' option is highlighted in the context menu.

<input checked="" type="checkbox"/>	Name	Threshold	Active	Default	New Logging Configuration
<input checked="" type="checkbox"/>	ConnectorAccess.WARN	All	Yes	Yes	Open Copy Set as Active Set as Default Delete

This slide displays all the existing configurations for a particular component. You can have multiple saved configurations for a logging component but only one can be active at a time. By default, all components start with a configuration set to save messages with a “Warning” severity or higher. It is good practice not to modify this default configuration and instead create a copy that you can modify when you want to troubleshoot issues. Click “Copy” to create a copy.

How to configure logging components (3 of 5)

- Provide name for configuration
- Select threshold



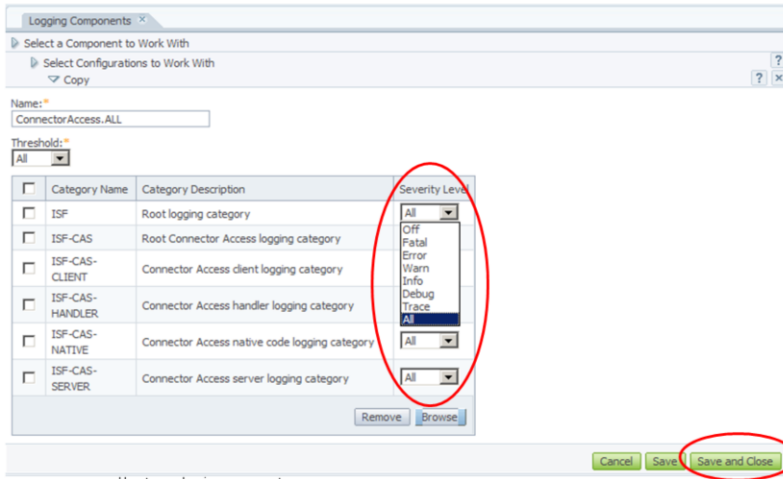
The screenshot shows the 'Logging Components' configuration page in the IBM WebSphere Administration Console. The 'Name' field is set to 'ConnectorAccess.ALL' and the 'Threshold' dropdown is set to 'All'. A table lists logging categories with their descriptions and severity levels.

<input type="checkbox"/>	Category Name	Category Description	Severity Level
<input type="checkbox"/>	ISF	Root logging category	All
<input type="checkbox"/>	ISF-CAS	Root Connector Access logging category	All
<input type="checkbox"/>	ISF-CAS-CLIENT	Connector Access client logging category	All
<input type="checkbox"/>	ISF-CAS-HANDLER	Connector Access handler logging category	All
<input type="checkbox"/>	ISF-CAS-NATIVE	Connector Access native code logging category	All
<input type="checkbox"/>	ISF-CAS-SERVER	Connector Access server logging category	All

When on the screen displayed on this slide, you will define your new configuration. Name this configuration: "ConnectorAccess.ALL". Then select a threshold. The threshold defines the lowest level of severity for a configuration and is used to control how much information you want to generate. The severities available are, from highest to lowest: Fatal, Error, Warning, Information, Debug, and Trace. The lower the threshold, the more information you will generate and store. For example, if you select as threshold "Warning", then you will capture "Warning" messages, and "Error" and "Fatal" messages since these have a higher severity. For this example, you want to capture as much information as possible so select All.

How to configure logging components (4 of 5)

- Select severity level for each category
- Threshold level of configuration takes precedence over severity level of category



7

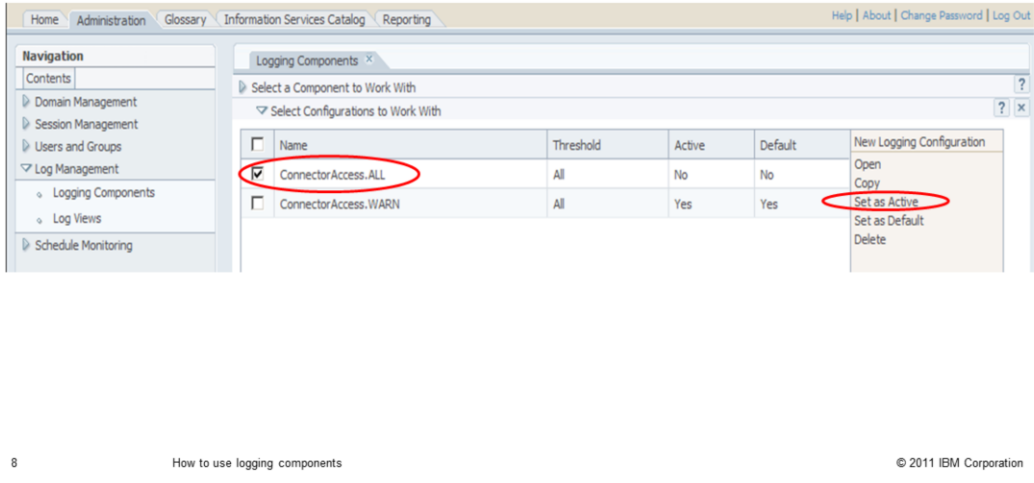
How to use logging components

© 2011 IBM Corporation

Each logging component contains categories that are associated with more specific parts of the suite. Click “Browse” to see all the categories available for this logging component. In addition to the threshold, you can also define severity levels for each category within a component. Keep in mind that the threshold level of the configuration takes precedence over the severity level of the category. For example, if the severity level of the category is “Warning” but the threshold of the configuration is “Error”, only “Error” messages and “Fatal” messages will be written to the metadata repository. This is because “Warning” has a lower priority than the threshold. For this example, use “All” for all Categories. Click “Save and Close” when you are done setting the levels.

How to configure logging components (5 of 5)

- Select new configuration and click “Set as Active”
- Set ConnectorAccess.WARN back to “Active” when finished



The screenshot shows the IBM Administration console interface. The main content area is titled "Logging Components" and contains a table with the following data:

<input type="checkbox"/>	Name	Threshold	Active	Default	New Logging Configuration
<input checked="" type="checkbox"/>	ConnectorAccess.ALL	All	No	No	Open Copy Set as Active Set as Default Delete
<input type="checkbox"/>	ConnectorAccess.WARN	All	Yes	Yes	

The "Set as Active" button in the "New Logging Configuration" column for the "ConnectorAccess.ALL" row is circled in red. The "ConnectorAccess.ALL" row is also circled in red.

Navigation menu items: Home, Administration, Glossary, Information Services Catalog, Reporting, Help, About, Change Password, Log Out.

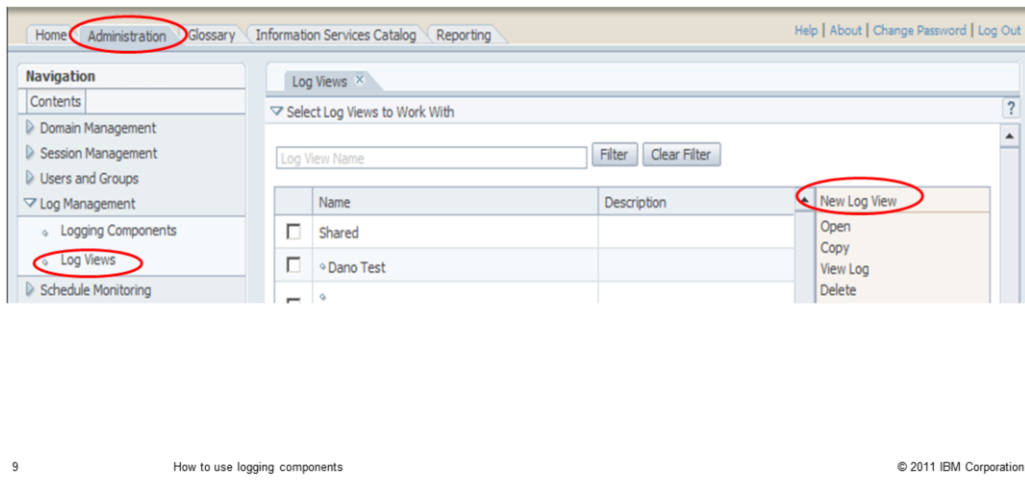
Navigation sidebar items: Contents, Domain Management, Session Management, Users and Groups, Log Management, Logging Components, Log Views, Schedule Monitoring.

Page number: 8. Page title: How to use logging components. Copyright: © 2011 IBM Corporation.

Next you will see a new configuration saved. Click the check box of the new logging configuration and then click “Set as Active” to activate this configuration. After you activate the configuration, the metadata will start saving the event messages according to your new definition. Once you are done collecting the information, go back to this screen and activate the default configuration. This is a recommended practice because configurations that increase the amount of information, for example configuration with low thresholds, can cause the metadata repository to grow too rapidly and this should be avoided.

How to use log views (1 of 5)

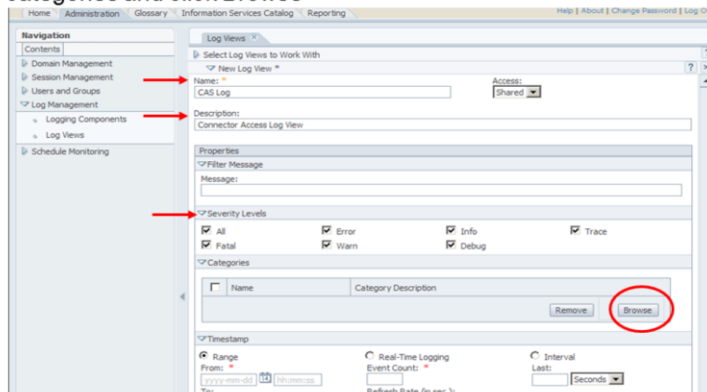
- Create log view
 - Displays event messages stored in repository



Now that you have configured the logging components, you need to create a log view. A log view is a report that will display the event messages stored in the repository. To do this, click “Administration” and under Log Management, click “Log Views”. Next, click “New Log View” to create a new one.

How to use log views (2 of 5)

- Provide name and description for log view
- Expand severity levels
- Click all to include all levels
- Expand categories and click Browse



10

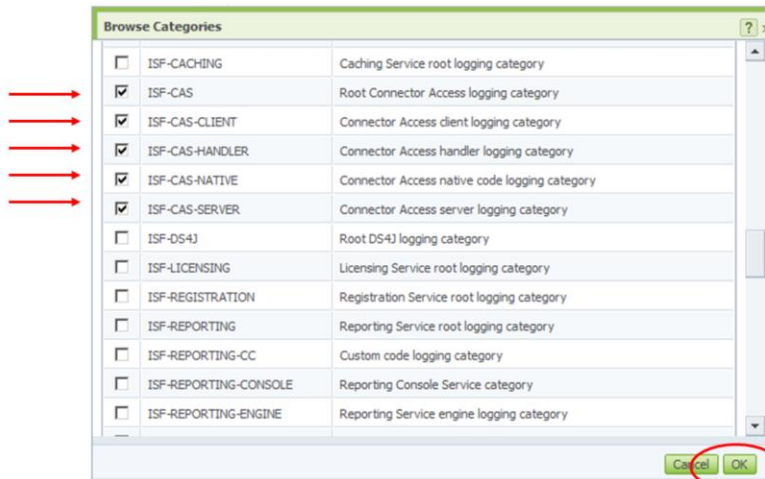
How to use logging components

© 2011 IBM Corporation

Provide a name and a description for the report. For this example, use “CAS Log” as Name. Then, expand the severity levels and select the same severity levels you included in the logging component configuration. For this example use “All” and then expand the categories and click “Browse”.

How to use log views (3 of 5)

- Find categories included in configured logging component



11

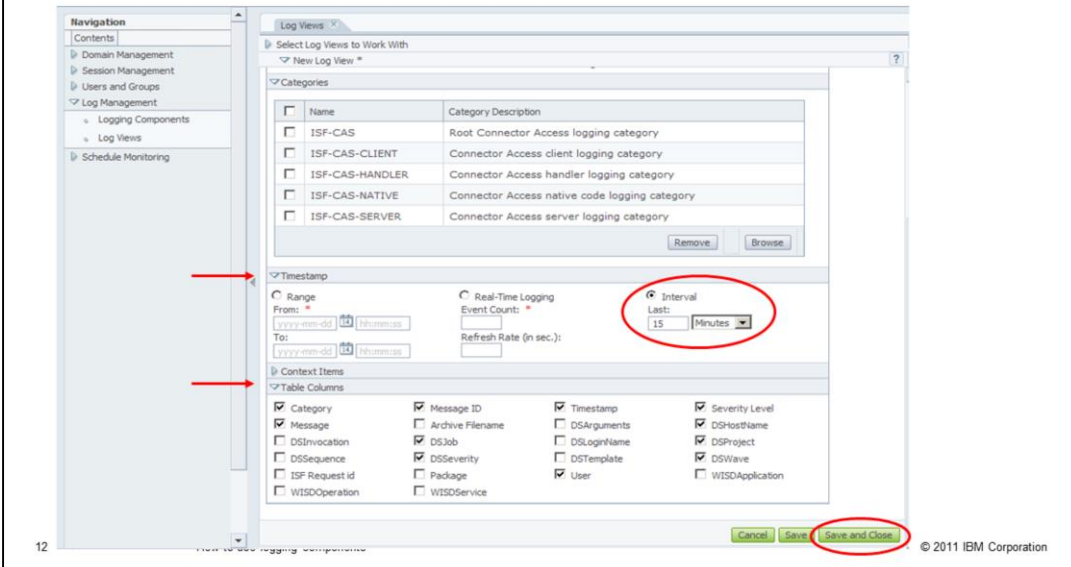
How to use logging components

© 2011 IBM Corporation

When on the screen displayed on this slide, select the same categories you included in the logging component configuration. For this example, pick all the categories with prefix ISF-CAS. Click Ok.

How to use log views (4 of 5)

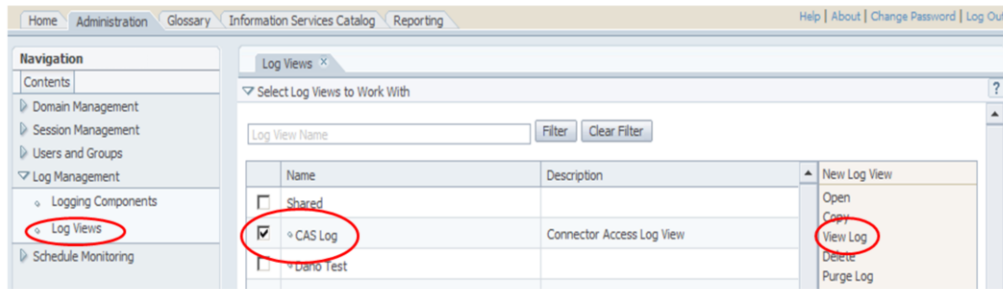
- Expand timestamp and choose one option to filter events
- Expand table columns and select columns



Next, click Timestamp. Choose one of the options to filter events by time. If you can reproduce the problem at will, then it is easier to choose a small interval, such as 15 minutes. For random problems that do not happen frequently, use a range filter. Starting at Information Server version 8.1, you can change this time filter at run-time. Finally, expand the Table Columns section and select the columns you need. The most important are Category and Message. If you are not sure what to include, select All. Click Save and Close.

How to use log views (5 of 5)

- Reproduce problem
- Wait few minutes
- Select log view



13

How to use logging components

© 2011 IBM Corporation

If you can reproduce the problem you want to troubleshoot, do it now. If the problem is random, wait until it happens again to use the log view. Once you are ready to see the messages, go to Log Management and click “Log Views”. Select your new log and click “View Log” on the right side of the screen. This will open a screen with the messages available. Keep in mind that it might take a couple of minutes before the messages are available in a log view.

Export and purge

- From log view
 - Export logs to file
 - Purge logs

The screenshot displays the IBM Log Management interface. On the left is a navigation pane with categories like 'Domain Management', 'Session Management', 'Users and Groups', 'Log Management', 'Logging Components', 'Log Views', and 'Schedule Monitoring'. The main area shows a 'Log Views' window with a search filter for 'View Log' and a date range from 2011-03-02 00:00:00 to 2011-03-09 00:00:00. Below the filter is a table of log entries with columns for Category, Message ID, Timestamp, Level, and Message. At the bottom right of the log view, there are four buttons: 'Close', 'Export Log', 'Purge Log', and 'Refresh'. The 'Export Log' button is circled in red.

Category	Message ID	Timestamp	Level	Message
ISF-CAS-HANDLER	100011	2011-03-02 10:00:27	Trace	A request of type class com.ascential.asb.cas.shared.utb.....
ISF-CAS-HANDLER	100010	2011-03-02 10:00:27	Trace	A response of type class com.ascential.asb.cas.sha.....
ISF-CAS-HANDLER	100011	2011-03-02 10:00:27	Trace	A request of type class com.ascential.asb.cas.shared.utb.....
ISF-CAS-HANDLER	100010	2011-03-02 10:00:27	Trace	A response of type class com.ascential.asb.cas.sha.....
ISF-CAS-HANDLER	100011	2011-03-02 10:00:27	Trace	A request of type class com.ascential.asb.cas.shared.utb.....
ISF-CAS-HANDLER	100010	2011-03-02 10:00:27	Trace	A response of type class com.ascential.asb.cas.sha.....
ISF-CAS-HANDLER	100011	2011-03-02 10:00:28	Trace	A request of type class com.ascential.asb.cas.shared.utb.....
ISF-CAS-HANDLER	100010	2011-03-02 10:00:28	Trace	A response of type class com.ascential.asb.cas.sha.....
ISF-CAS-SERVER	000004	2011-03-02 12:16:09	Trace	Enter method ConnectorAccessServiceBean.getConnection.....
ISF-CAS-SERVER	010002	2011-03-02 12:16:09	Debug	Executing XMeta query 'select x from x in Connecto.....
ISF-CAS-SERVER	010005	2011-03-02 12:16:09	Debug	1 agents were found for router 5874305.92408369.18.....

14

How to use logging components

© 2011 IBM Corporation

You can use the log view page to export your logs to a file by clicking the Export Log button. You can also use a log view to purge the event messages from the database. Be aware that purged messages are deleted permanently so you have to be careful when doing this. Once you have captured the information you need, remember to go back to logging component, select Connector Access and activate the default configuration to prevent the metadata from storing unnecessary information. See slide 8 for more details.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, DataStage, and InfoSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2011. All rights reserved.