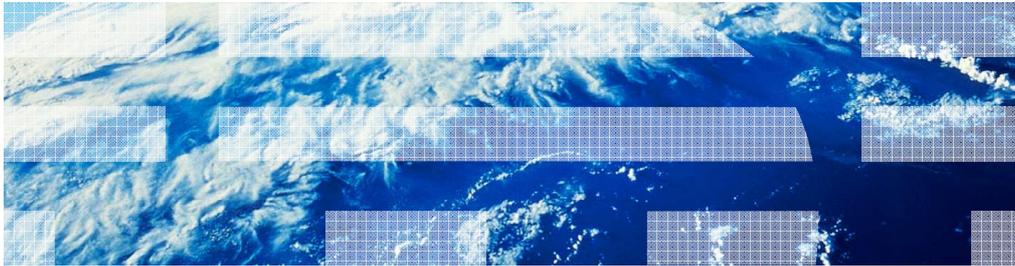


WebSphere Business Monitor

Administration



This presentation will show you the functions in the administrative console for WebSphere® Business Monitor.

Goals

- Show the administrative menus for use with WebSphere Business Monitor

This presentation will show you how to use the administrative console for managing various functions in WebSphere Business Monitor.

Agenda

- Monitor models
- Monitor data security
- Event recording
- Purge instance data
- Monitor services
- Action services
- Failed events

This is the agenda for this presentation. You will see how to manage monitor models, including configuring data security and viewing the overall security configuration. You will review the event recording capability, and you will see how to purge monitor instance data. Also, there are various services associated with your models and you will review the services management which also includes action services for business situation events. Finally, you will see where to look for failed event sequences.

Monitor menus

The screenshot displays the IBM WebSphere Business Monitor administrative console interface. It features a left-hand navigation pane and a main content area on the right. The navigation pane is divided into two main sections: 'Servers' and 'Applications'. Under 'Servers', there is a 'Server Types' sub-menu containing 'WebSphere Business Monitor configuration'. Under 'Applications', there are several sub-menus: 'New Application', 'Application Types', 'SCA modules', 'Monitor Models', 'Monitor Services', 'Monitor Action Services', 'Recorded Events Management', and 'Monitor Scheduled Services'. The 'Monitor Services' sub-menu is highlighted with a red box. The main content area on the right shows a tree view of the console's structure. It includes sections for 'Security', 'Environment', 'Integration Applications', 'System administration', 'Users and Groups', 'Monitoring and Tuning', and 'Troubleshooting'. Under 'Security', there are sub-menus for 'Business Integration Security', 'Global security', 'Security domains', 'Administrative Authorization Groups', 'SSL certificate and key management', 'Security auditing', 'Bus security', and 'Monitor Data Security'. Under 'Troubleshooting', there are sub-menus for 'Logs and trace', 'Cross-Component Trace', 'Configuration problems', 'Class loader viewer', 'Configuration Validation', 'Monitor Models', 'Diagnostic Provider', 'Runtime Messages', and 'WebSphere Business Monitor security'. The 'Monitor Models' and 'WebSphere Business Monitor security' sub-menus are highlighted with red boxes.

4 Administration © 2010 IBM Corporation

There are several monitor sub-menus in the server administrative console. In the servers section there is a menu to configure the monitor components in an installation. In the applications section you can manage your monitor model applications and monitor services. In the security section you can manage user access to your monitor models. Then in the troubleshooting section you can view failed event sequences and view the overall security configuration.

Monitor models

Monitor Models

Use this page to manage all versions of monitor models and their associated applications. To start or stop a version of a monitor model, you must start or stop the associated application. All models are initially added to the root resource group and may not be visible by its intended dashboard users. Use the Monitor data security panel to assign permission to the models.

Preferences

Start Stop Install						
Select	Model	Version	Deployment	Application	Data Security	Status
<input type="checkbox"/>	ClipsAndTasks	2007-09-11T12:07:30	OK	ClipsAndTasksApplication	Members assigned	→
<input type="checkbox"/>	GlobalHTMM	2007-06-18T09:54:38	OK	IBM_WBM_HUMAN_TASK_MONITOR_MODEL	Members assigned	→
<input type="checkbox"/>	Global_Process_Monitor	2009-11-10T20:00:00	OK	IBM_WBM_GLOBAL_PROCESS_MONITOR	Members assigned	→
<input type="checkbox"/>	MM1266614757859_1_BLM-0424adf29efb09d82ca1e7cd1e36cfa_RequestWork_DoSomethingProcesses	2010-02-19T16:26:07	OK	RequestWork_Mon_1266614757859_1App1	Members assigned	→
Total 4						

Displays warning icon if model cannot start

The monitor models page displays all versions of all models. By default, both installed and uninstalled applications are displayed, but an option under preferences allows only installed applications to be displayed. The model ID is displayed in the model column and the version timestamp is displayed in the version column. The deployment column displays an indicator of deployment status. 'OK' means the model can be started. Other indicators show you that the schema has not been created, the CEI configuration is incomplete or the model state is not active. In the application column you see the application name. In the data security column you will see an indicator to show if users are assigned to the resource group for the model. The status column shows that the application is started or stopped.

The start button starts a version in the active state so that events on its event queue can be processed.

The stop button stops a version in the active state so that events on its event queue are no longer processed. Events continue to build up on its event queue while a version is stopped.

If you click the model name for a specific model, you will see model configuration information. If you click the version number for a specific model, you will see the version information panel. If you click the application name for a model, you will see the standard enterprise application menu where you can perform additional server administrative functions for the application.

Model properties

Monitor Models

Use this page to manage all versions of monitor models and their associated applications. To start or stop a model, you must be initially added to the root resource group and may not be visible by its intended dashboard users. Use the

Preferences

Start Stop Install	
Select	Model
<input type="checkbox"/>	ClipsAndTacks
<input type="checkbox"/>	GlobalHTMM

Version
2007-09-11T12:07:30

Monitor Models > ClipsAndTacks

Use this page to view the configuration for this monitor model. Click the links to access pages for properties.

General

General Properties

Model
ClipsAndTacks

Number of versions
1

Resource group
root

[Back](#)

Model Properties

- [Change CEI configuration](#)
- [Manage Scheduled Services](#)
- [Change resource group](#)
- [Purge model](#)

If you click the model name for a model in the monitor models panel, you will see model configuration information. It shows the model name, number of versions and the resource group associated with the model. There are also links that allow you to manage CEI configuration, services, resource groups, and purging.

Purging a monitor model removes the model from the repository database. Before you can remove all versions of a model from the repository database, you must delete all versions of the schema and you must uninstall all versions of the model you are purging.

The screenshot shows the 'Model version' configuration page in the IBM BPM Monitor Administration tool. At the top, there is a table with columns 'Model' and 'Version'. The 'Version' column for the 'ClipsAndTacks' model is circled in red, showing the value '2007-09-11T12:07:30'. Below the table, the page title is 'Monitor Models > ClipsAndTacks (2007-09-11T12:07:30)'. The main content area is divided into several sections: 'General Properties' (Model, Version, Application, CEI distribution mode, Active MC instances), 'Version Properties' (Manage schema, Manage Alphablox Cubes, Change CEI distribution mode, Change runtime configuration, View model, Purge model version), and 'Manage Monitor Data' (Export Instance Data, Import Instance Data, Purge and Archive Instance Data). A 'Deployment' section at the bottom shows three checked items: 'Dashboards enabled', 'Schema created', and 'Alphablox cubes created (optional)'. The IBM logo is in the top right corner, and the page number '7' and 'Administration' are in the bottom left, and '© 2010 IBM Corporation' is in the bottom right.

If you click the version number for a model in the monitor models panel, you will see the version information panel. You can see the CEI distribution mode, and the number of active monitoring context instances. In the deployment section, you see the list of setup steps and an icon indicating the status of each step. There are additional links that you can use to manage the schema, cubes, distribution mode, runtime configuration and purging. You can also export, import and purge instance data from the monitor database.

Before you purge the model version you must delete the schema and uninstall the application. There is also a force option which doesn't check for the preconditions but you must use the administrative command to use this option.

On the manage schema page, you can run the schema script and setup the database for that version of the model. You can run a script to delete the schema for this version of the model. You can also export the scripts to your file system.

On the manage Alphablox[®] cubes page, you specify the location and security information for the Alphablox server.

On the 'Change CEI distribution mode' page, you can change the CEI distribution.

For the runtime configuration, you can set tuning fields that affect the monitor server behavior. You can define the behavior of various error handling situations and you can specify details for handling the cache for KPI value retrieval, which affect performance by caching the values for the KPIs rather than recalculating the values every time from the monitor database.

Change CEI distribution mode

[Monitor Models](#) > [ClipsAndTacks \(2007-09-11T12:07:30\)](#) > **Change CEI distribution mode**

Use this page to view and change the CEI configuration properties for a specific monitor model.

General

General Properties **Model Properties**

Distribution mode

Current
Active (monitor model queue-based)

Target
Inactive

Apply OK Reset Cancel

[Change CEI configuration](#)

- Distribution modes
 - Active
 - Inactive
 - Active (no new monitor context instances)
 - Inactive (event queue recoverable)

On the change CEI distribution mode page, you can change the CEI distribution. You can change the mode to be active, inactive or “inactive event queue recoverable”. When you install a new version then the old versions will automatically change to mode “active (no new monitor context instances)”, so that only the latest version will create new monitoring instances. The old versions are used to finish any existing monitoring instances. The mode “inactive (event queue recoverable)” can be used to handle incorrect versions of a monitor model. In this case you can deploy a newer correct version, and this new version will process the events for the incorrect versions.

You can also click to change the CEI configuration specifying location, security and group profile, but you should make sure that all versions for this model are in inactive mode before using this function.

Monitor data security - Configure

The screenshot displays the IBM administrative console interface for configuring monitor data security. On the left, a navigation tree shows various system components, with 'Monitor Data Security' highlighted. The main content area is titled 'Monitor Data Security Administration > root' and includes a 'Configure' button. Below this, there is a 'Description' section stating that the 'root' resource group is the default parent. A 'Models' list contains several entries, including 'ClipsAndTacks', 'GlobalHTMM', 'Global_Process_Monitor', and 'MM1266614757859_1_BLM-042'. A 'Roles' section provides instructions on selecting a role and lists requirements for administrative and application security. At the bottom, a dialog box allows selecting a role from a list: Business-Manager (selected), Personal-KPI-Administrator, Public-KPI-Administrator, and KPI-Administrator. The 'Users' tab is active in the dialog box.

Using the administrative console, you can configure security for your monitor models by setting data access permissions. Monitor models can be grouped into resource groups to allow easy administration of data access permissions. Permissions must be assigned to a resource group by way of a three way binding. This binding consists of a resource group, a role, and a user or group of users.

Monitor data security always has a root resource group defined. All resource groups other than root are considered children of root. All resources are visible to the root resource group. By default, all models are deployed to the root resource group unless they are added to a different resource group during model deployment. A model can be a member of only one resource group.

Monitor data security – Diagnose

- Tool for diagnosing model access problems

The screenshot shows the administrative console interface. On the left is a navigation tree with categories like Guided Activities, Servers, Applications, Services, Resources, Security, Environment, Integration Applications, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. Under the Security category, 'Monitor Data Security' is highlighted. The main content area has two tabs: 'Configure' and 'Diagnose', with 'Diagnose' selected. Below the tabs is a search section with a text input field containing an asterisk (*), a 'Search' button, and a 'Maximum results' dropdown set to '100'. A search results dropdown shows 'uid=admin,c=defaultWIMFileBasedRealm'. Below this is a table with two columns: 'Model' and 'Roles'.

Model	Roles
GlobalHTMM	Business-Manager KPI-Administrator Personal-KPI-Administrator Public-KPI-Administrator
Global_Process_Monitor	Business-Manager KPI-Administrator Personal-KPI-Administrator Public-KPI-Administrator
testModMonMM	Business-Manager KPI-Administrator Personal-KPI-Administrator Public-KPI-Administrator

10

Administration

© 2010 IBM Corporation

There is a tool for helping you diagnose monitor model access problems. In the administrative console, for monitor data security, there is a tab called diagnose. This tab displays the models assigned to a particular user, and the roles associated with it. You can also enter a search string to select the users that you want to query. This function makes it easy to determine the model access for any particular user.

Security configuration

Integrated Solutions Console: Welcome wasadmin

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
 - Logs and trace
 - Configuration problems
 - Class loader viewer
 - Configuration Validation
 - Monitor Models
 - Diagnostic Provider
 - Bugtime Messages
 - WebSphere Business Monitor security**
 - Service Integration
 - UDDI

- A single panel provides easy access to relevant security configuration information

WebSphere Business Monitor Security

Security Information

The panel below provides information about some of the security properties relevant to WebSphere Business Monitor

Component	Status
Global Security	Administrative Security is Enabled Application Security is Disabled Selected User Account Repository: Federated Repositories The user registry is searchable
WebSphere Business Monitor Data Security	There are 3 members in the root resource group The rtart resource group has no members There are 3 members in the business resource group The monitor resource group has one member The cypretgroup resource group has no members
LTPA	LTPA key regeneration is enabled The key regeneration date is: Tue Nov 10 11:00:04 EST 2009
Single Sign-on	Single Sign-on (SSO) is enabled The SSO domain has not been specified

11

Administration

© 2010 IBM Corporation

On the security page in the troubleshooting section you can view security configuration for WebSphere Business Monitor from a central location. You can access administrative and application security, Monitor data security, LTPA, and single sign-on security. This makes it easy to view security information consolidated in one place. To update the security configuration, you can click the component link and you are taken to the configuration page for that component.

Event recording and playback

- Use the administrative console to select events to playback or export
- Use toolkit server menu to manage recording during development cycle



12

Administration

© 2010 IBM Corporation

The event recording feature allows you to record an event sequence for subsequent playback. This is very useful if you want to iteratively test a monitor model as you continually change and develop the model. For a BPEL application or any other application, you can enable event recording, then manually step through the process or the application which will then generate the event sequence. The event sequence is saved to a database, so then you can replay the event sequence later to re-run the test. You can use scripts or the administrative console to manage these functions. Also, you can activate the event recording in the monitor toolkit. And you can import these events into an integrated test console script.

To enable event recording, you can use the administrative pages or you can also use the server menu in the monitor toolkit.

You can use the administrative console to manage the events. On the events management page, you can list the events that have been recorded, and you can click an event to see the details of an individual event. You can also select options to delete, import and export. The import and export functions allow you to save events to the file system. On the play back page, you can select events and model version and then you can initiate a play back.

Import, export, purge, archive instance data

- You can archive data on a one-time or scheduled periodic basis
 - This applies to instance data only, not KPI history
- Access the menu from the model version page

The screenshot displays the 'Manage Monitor Data' section of the IBM BPM Monitor Administration console. It includes three menu items: 'Export Instance Data', 'Import Instance Data', and 'Purge and Archive Instance Data'. Below these are two dialog boxes:

Purge and archive dialog: Features a 'Time Filter' section for selecting the instance termination end time (UTC) with fields for 'Purge instances before' (set to 'Not specified') and 'Time' (set to '00:00:00'). It also has an 'Archive' section with a checked checkbox 'Archive the purged instance to a directory on the server (CSV files)' and a 'Full path' field with a 'Browse...' button. At the bottom are 'Purge', 'Retrieve Instance Count', and 'Cancel' buttons.

Export dialog: Titled 'Export', it asks 'How do you want to specify which instance data to export?'. It offers two radio button options: 'Based on instance creation time' and 'Based on instance termination time'. Each option has fields for 'Export instances after' (set to 'Not specified') and 'Time' (set to '00:00:00'). Below is an 'Export Options' section with two radio button options: 'Export the monitor model instance data to your browser (zip of CSV files)' and 'Export the monitor model instance data to a directory on the server (CSV files)'. The second option includes a 'Full path' field and a 'Browse...' button. At the bottom are 'Export', 'Retrieve Instance Count', and 'Cancel' buttons.

At the bottom left of the screenshot is the number '13' and the word 'Administration'. At the bottom right is the copyright notice '© 2010 IBM Corporation'.

To help you manage your monitored instance data in the monitor database, there are functions to purge and export. You can invoke these functions using the administrative console to run them as required. If you want to setup a periodic archive, then you can do that in the monitor scheduled services menu. These functions do not operate on KPI history; they just apply to instance data.

In the administrative console, you can access a model version to get to the page to manage monitor data. On the export page you can specify the date and time information either based on instance creation time or instance termination time. You can export the data to your browser or to the server.

On the page for purge and archive, you can specify the instance termination date and time. You can also optionally select to store the data on the server.

The import page allows you to load previously exported data, but this page is only enabled for a development server.

Monitor services

Applications

- New Application
- Application Types
- SCA modules
- Monitor Models
- **Monitor Services**
- Monitor Action Services
- Recorded Events Management
- **Monitor Scheduled Services**

Model Properties

- [Change CFI configuration](#)
- **[Manage Scheduled Services](#)**
- [Change resource group](#)
- [Purge model](#)

Suspend Resume

Select	Service	Interval	Last Run	Last Duration	Last Start	Last Completion	Status
<input type="checkbox"/>	KPI History Calculation	1 hours	Success	0h 0m 2s	Nov 13, 2008 3:00:10 PM	Nov 13, 2008 3:00:13 PM	Active
<input type="checkbox"/>	KPI Prediction Calculation	1 hours	Success	0h 0m 0s	Nov 13, 2008 3:00:13 PM	Nov 13, 2008 3:00:13 PM	Active
<input type="checkbox"/>	Dynamic Alert Evaluation	1 minutes	Success	0h 0m 0s	Nov 13, 2008 3:22:10 PM	Nov 13, 2008 3:22:10 PM	Active
<input type="checkbox"/>	Alphablox Cube Refresh	1 hours	None				Suspended
<input type="checkbox"/>	Purge and Archive Instance Data	1 days	None				Suspended

14

Administration

© 2010 IBM Corporation

You can access monitor services from the applications section in the console, or from the model properties section of a monitor model. On the services page you can see the status of all the scheduled monitor services. You can see the interval, last run, last run duration, last start, last completion, and current status. If you click a specific service, then you can view the details of the selected service, and you can update the interval for the service. For purge and archive instance data, you can also select the records to purge based on the instance termination date.

You can manage monitor services which include Data Movement Service, KPI History Calculation, KPI Prediction Calculation, Dynamic Alert Evaluation, Cube Summary Table, Alphablox Cube Refresh, and Purge and Archive Instance Data.

You must enable the data movement and Alphablox cube refresh services before you can schedule them. The KPI history and KPI prediction services run once every hour and this interval is not modifiable.

Action services - Business situation events

The screenshot displays the IBM WebSphere Business Monitor Administration console. On the left is a navigation tree with the following structure:

- Applications
 - New Application
 - Application Types
 - SCA modules
 - Monitor Models
 - Monitor Services
 - Monitor Action Services
 - Configuration
 - Template Definitions
 - Notifications
 - SCA
 - Web Services
 - Installed Situation Event Bindings

The main content area is titled "Configuration" and includes the instruction: "Use this page to configure the general, federated rep...". There are three tabs: "General" (selected), "Federated repositories", and "LDAP".

General Properties

- SMTP sender name:
- SMTP host name:
- SMTP port number:

CEI action logging

- On
- Off

At the bottom of the page, the text "15 Administration" is on the left and "© 2010 IBM Corporation" is on the right.

WebSphere Business Monitor manages action services and event emissions using monitor action services. The monitor action services receives situation events emitted by applications, selects appropriate actions based on user-defined rules and policies, and invokes one or more actions in the form of alerts.

Any changes to the configuration properties that are made while Monitor action services are running are not effective until you stop and then restart the Business Monitor server.

You can also create and manage alerts in the dashboard using the alert manager widget. Using this widget you can create alert notifications from existing key performance indicators (KPIs). Creating an alert notification involves specifying a trigger condition, and creating a notification message and subscription list. You can share the alerts that you create so that other users can view and subscribe to them.

Notification template

* Template name
FeeComplianceAlert

Description

Default action service type

Dashboard Alert
 Cell phone
 Email
 Pager

To query type

Federated repositories query
 LDAP query
 Email address
 User id

To
admin

Query base

Subject
 Fee compliance: Loan
 %%cbe:CommonBaseEvents/cbe:CommonBaseEvent
 /mor:feeComplianceAlert/mor:loanNumber/text()%

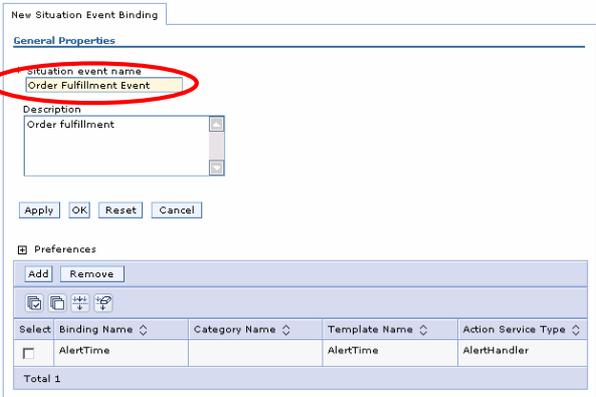
Body
 There is a fee compliance alert for loan number
 %%cbe:CommonBaseEvents/cbe:CommonBaseEvent
 /mor:feeComplianceAlert/mor:loanNumber/text()% opened
 on %%cbe:CommonBaseEvents/cbe:CommonBaseEvent
 /mor:feeComplianceAlert/mor:dateStarted/text()% by loan
 officer %%cbe:CommonBaseEvents/cbe:CommonBaseEvent

A system administrator uses the Monitor action services to notify the appropriate people about events that occur in a model. These notifications can take the form of a dashboard alert, an email, a call to a cell phone, or a call to a pager. Notifications can also be sent to web services or Service Component Architecture (SCA) services. There are three types of templates that are used to create the actions: notification, web service, and SCA.

This slide shows the notification template which is used for notifications using dashboard, email, cell phone or pager. You specify the query type and then in the 'To' field you enter a query that is used to retrieve the set of users who will receive this notification. You can enter an LDAP or a federated repositories query. You can also enter a space separated list of email addresses or user ID's.

You can enter a subject and body for the alert. Note in the body of the alert the use of a substitution variable which is marked with the percent sign. This variable is a field which was defined on the outbound event in the model, and the value of that field in the event is substituted into the body text. You can also use substitution variables in the subject of the notification.

Situation event binding



New Situation Event Binding

General Properties

Situation event name
Order Fulfillment Event

Description
Order fulfillment

Apply OK Reset Cancel

Preferences

Add Remove

Select	Binding Name	Category Name	Template Name	Action Service Type
<input type="checkbox"/>	AlertTime		AlertTime	AlertHandler
Total 1				

Outbound Event Content

Specify the triggers that cause the event to be sent. Use the Expression column to specify the value for each event attribute when the event is sent.

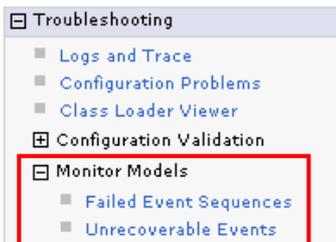
Name	Type	Expression
Average Process Duration KPI Trigger 1		
Property Data		
Extended Data		
BusinessSituationName	string	'Order Fulfillment Event'
AverageOrderProcessingTime	string	xs:string(Average_Process_Duration_KPI div xs:dayTimeDuration('P1D'))

17 Administration © 2010 IBM Corporation

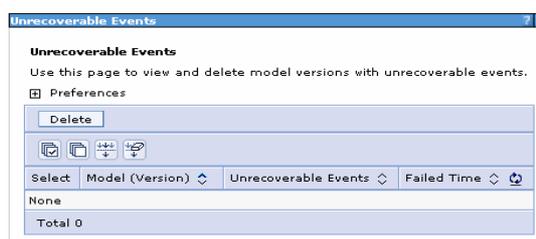
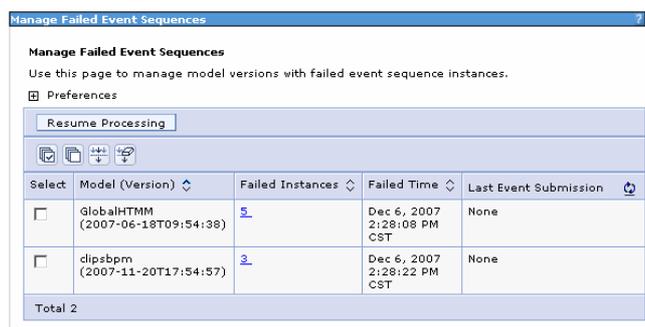
At the top is a screen capture of the situation event binding in the action services menu. You see a situation event “Order Fulfillment Event” and there is a template which has been assigned to this situation event to specify which users will receive the alert. You can have one or more service templates assigned to a situation event binding.

Business situation events can be generated by the monitor model or from any other source, as long as the event contains an extended data field with name BusinessSituationName. The value of ‘Situation event name’ on the binding should match the value of BusinessSituationName in the outbound event in the monitor model. At the bottom is a screen capture of the outbound event definition in the monitor model, and the value of BusinessSituationName is ‘Order Fulfillment Event’ which matches the situation event binding.

Monitor model failed events



- Scripting is available, see the information center topic Reference > Commands and scripts > Administrative commands > Managing failed events using scripts



You can use the administrative console to manage failed event sequences and view unrecoverable events.

If an event cannot be processed, the model stops processing all subsequent messages for the instance in which the fault occurred. Other instances for this model can continue to process incoming events. Manual intervention is therefore only required to restart processing of a particular instance. For failed events you can use the console to view, export, import, replace, delete, re-sequence and resubmit them. You can also use scripting to manage failed events. Check the information center for details.

If a model cannot parse an incoming event for example due to malformed XML, then it goes to the unrecoverable events queue. Unrecoverable events can be inspected in an attempt to establish the cause of a failure, but they cannot be resubmitted. So you can use the console to view, export and delete them.

Summary

- Covered the use of the administrative console for use with WebSphere Business Monitor

In summary, this presentation covered an overview of the administrative console menus for use with WebSphere Business Monitor.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WBPM_Monitor_Administration.ppt

This module is also available in PDF format at: [./WBPM_Monitor_Administration.pdf](#)

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Alphablox, and WebSphere 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 2010. All rights reserved.