


Slide 1

WebSphere Education

IBM

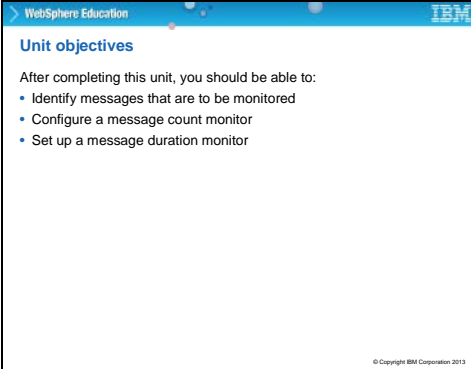
Monitoring objects



© Copyright IBM Corporation 2013
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

The diagram shows three overlapping circles in light blue. Inside and around these circles are several small dots in various colors (blue, purple, pink, yellow). The circles are arranged in a way that they overlap significantly, with one circle on the left and two on the right, creating a complex intersection pattern.

Slide 2



The slide is titled 'WebSphere Education' in the top left corner and features the IBM logo in the top right corner. The main heading is 'Unit objectives' in blue. Below it, a paragraph states: 'After completing this unit, you should be able to:'. This is followed by a bulleted list of three objectives. The bottom right corner contains a small copyright notice: '© Copyright IBM Corporation 2013'.

WebSphere Education

Unit objectives

After completing this unit, you should be able to:

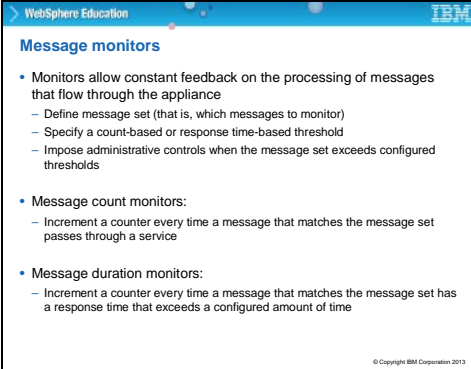
- Identify messages that are to be monitored
- Configure a message count monitor
- Set up a message duration monitor

© Copyright IBM Corporation 2013

Unit overview

This unit teaches how to track message rates and latency.

Slide 3



WebSphere Education

Message monitors

- Monitors allow constant feedback on the processing of messages that flow through the appliance
 - Define message set (that is, which messages to monitor)
 - Specify a count-based or response time-based threshold
 - Impose administrative controls when the message set exceeds configured thresholds
- Message count monitors:
 - Increment a counter every time a message that matches the message set passes through a service
- Message duration monitors:
 - Increment a counter every time a message that matches the message set has a response time that exceeds a configured amount of time

© Copyright IBM Corporation 2013

Message monitors

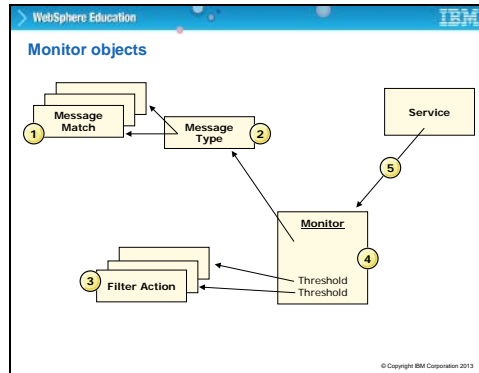
Message Monitors allow constant feedback on the processing of messages that flow through the appliance. In order to use them, first define a message set. That is, which messages are wanted to monitor. Then, specify either a count-based or response time-based threshold, and impose administrative controls when the message set exceeds those configured thresholds.

There are two basic types of message monitor – count and duration.

Message count monitors increment a counter every time a message that matches the message set passes through a service.

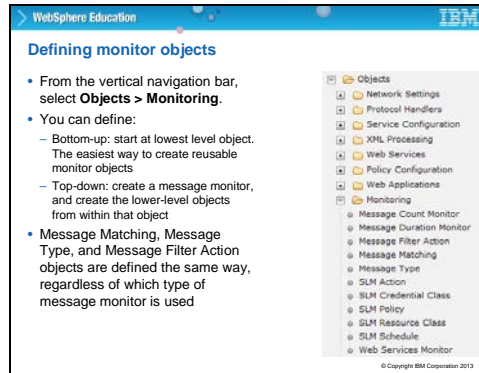
Message duration monitors increment a counter every time a message that matches the message set has a response time that exceeds a configured amount of time.

Slide 4



Monitor objects

As you know by now, DataPower services are constructed from objects that are linked together in a hierarchical fashion, and monitor objects are no exception. Number 1 shows where to begin by defining Message Match objects, which describe the criteria for identifying messages that are interested in monitoring. Next, number 2 shows how to create a Message Type object that aggregates a set of Message Match objects into a single, easily managed object. Message monitoring is all about checking for thresholds that are exceeded, and taking some action when that happens. Filter Action objects, which are shown as number 3, describe what action to take when a particular threshold is exceeded. A Monitor object, number 4, is created next that brings together the Message Type object and the Filter Action objects into a single entity. Number 5 shows that, during service definition, reference to one or more Monitor objects as needed.



WebSphere Education

Defining monitor objects

- From the vertical navigation bar, select **Objects > Monitoring**.
- You can define:
 - Bottom-up: start at lowest level object. The easiest way to create reusable monitor objects
 - Top-down: create a message monitor, and create the lower-level objects from within that object
- Message Matching, Message Type, and Message Filter Action objects are defined the same way, regardless of which type of message monitor is used

Objects

- Network Settings
- Protocol Handlers
- Service Configuration
- XML Processing
- Web Services
- Policy Configuration
- Web Applications
- Monitoring
 - Message Count Monitor
 - Message Duration Monitor
 - Message Filter Action
 - Message Matching
 - Message Type
 - SLM Action
 - SLM Credential Class
 - SLM Policy
 - SLM Resource Class
 - SLM Schedule
 - Web Services Monitor

© Copyright IBM Corporation 2013

Defining monitor objects

Here is how to define monitor objects. From the vertical navigation bar, select OBJECTS > Monitoring. You can define these objects in two ways. The Bottom-up method is where you start at lowest level object, and build upward. Bottom-up is the easiest way to create reusable monitor objects. Alternatively, you can define needed objects from the Top down. You start by creating a message monitor, and then create the lower-level objects from within that object as needed. Message Matching, Message Type, and Message Filter Action objects are defined the same, regardless of whether using them in count monitors or duration monitors.

Slide 6

The screenshot shows the 'Configure Message Matching' form in the WebSphere Education interface. The form has two tabs: 'HTTP Headers' (selected) and 'Included HTTP Cookies'. The 'Message Matching' field contains the text 'retrieveAllCounter-message-matching.xml'. Below this are buttons for 'New', 'Cancel', 'Delete', and 'Save'. The form also includes fields for 'Administrative State' (radio buttons for 'enabled' and 'disabled'), 'Comments', 'IP Addresses', 'Excluded IP Addresses', 'HTTP Method' (a dropdown menu with 'any' selected), and 'Request URL'.

WebSphere Education

Step 1: Specifying particular traffic to monitor

- From the vertical navigation bar, select **Objects > Monitoring > Message Matching > Add**
- Configure a message that matches an object to:
 - Specify an IP address range to be included or excluded in the traffic definition
 - Limit the traffic definition to a single HTTP method
 - Specify a URL set to be included in the traffic definition
 - Indicate HTTP headers and values to include or exclude (separate tabs)

Configure Message Matching

Tab: **HTTP Headers** Included HTTP Cookies

Message Matching: retrieveAllCounter-message-matching.xml

[New] [Cancel] [Delete] [Save]

Administrative State: ☒ enabled ☐ disabled

Comments:

IP Addresses:

Excluded IP Addresses:

HTTP Method: [X]

Request URL:

© Copyright IBM Corporation 2013

Step 1: Specifying particular traffic to monitor

Now go through the steps that are needed to create these monitors. First, specify the particular traffic to be monitored by defining message match objects. Assuming the bottom-up approach is used, go to the vertical navigation bar, and select OBJECTS, Monitoring, Message Matching, and click Add.

You can configure a message that matches object to look for a specific IP address range to be included or excluded in the traffic definition. Limit the traffic definition to a single HTTP method. You can specify a URL set to be included in the traffic definition, and you can indicate which HTTP headers and values are to be included or excluded. These definitions are found under separate tabs that are described on the next slide.

Slide 7

WebSphere Education

Step 1: Matching on HTTP headers

- Use the **HTTP Headers** tab to specify HTTP-based criteria for inclusion to the traffic definition
 - Specify HTTP header name-value pairs included in the traffic definition
- Use the **excluded HTTP headers** to specify exclusion from the traffic definition
 - Specify HTTP header name-value pairs to be excluded in the traffic definition

Message Matching: retrieveAllCourse

Apply Cancel Delete Undo

Name	Value Match
DataPower	X*

Add

© Copyright IBM Corporation 2013

Step 1: Matching on HTTP headers

Use the HTTP Headers tab to specify HTTP-based criteria for inclusion to the traffic definition, such as header name-value pairs. And you can also use the excluded HTTP headers to specify exclusion from the traffic definition, in this case that defines header name-value pairs to be excluded.

Slide 8

WebSphere Education

Step 2: Message type configuration

- The *message type* object is a collection of one or more *message matching* objects
- Message type objects make it possible to combine various message matching objects into one type
- Each message type can use a different combination of message matching objects

Configure Message Type

Plan

Message Type: retrieveAllCounter-message-type [v0]

Cancel Delete Update Expand | View Log | View Status | Help

Administrative State: ☒ enabled ☐ disabled

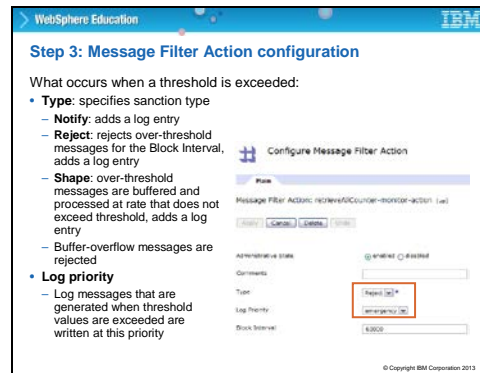
Comments:

Message Matchings: retrieveAllCounter-message-matching

© Copyright IBM Corporation 2013

Step 2: Message type configuration

Now move onto the Message Type object, which is a collection of one or more messages that matches objects. Message type objects make it possible to combine various message-matching objects into one type, and each message type can use a different combination of message-matching objects. Select the ones that you want to include from the pick list, and click Add to include them in the list of Message Matchings.



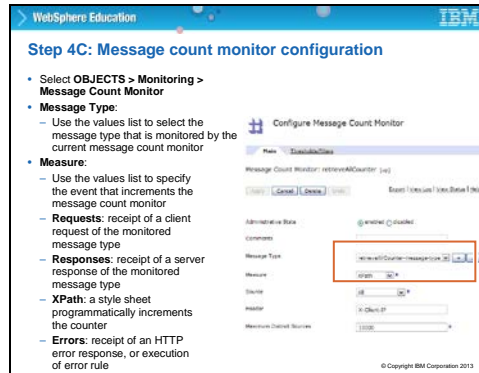
Step 3: Message Filter Action configuration

Next, define the Message Filter Actions, which describe what occurs when a threshold is exceeded. The parameters that are specified for this object are as follows:

- Type, which specifies which type of sanction to apply.
- Choose to notify that a threshold is exceeded by adding a log entry.
- Reject over-threshold messages and add a log entry. As part of this action, also specify a Block Interval, during which time, all messages from that source are blocked.

The third type of sanction is to shape the message traffic. Over-threshold messages are buffered and processed at a rate that does not exceed the threshold, and adds a log entry. Buffer-overflow messages are rejected.

Since all of these actions cause a log message to be written, specify the Log Priority that is applied to these messages.



Step 4C: Message count monitor configuration

Now look at how to configure a Message Count Monitor. From the vertical menu, select OBJECTS, Monitoring, Message Count Monitor.

Choose the Message Type you want to monitor from the pick list,

Then, choose what to measure. The choices are:

Requests, which increment the counter upon receipt of a client request of the monitored message type.

Responses, which count each receipt of a server response of the monitored message type.

XPath, allows you to have a style sheet programmatically increment the counter.

Errors, counts each receipt of an HTTP error response, or execution of error rule.

Step 4C: Thresholds/Filters for count monitor

- In the "Configure Message Count Monitor" page, select the **Thresholds/Filters** tab
 - Specify the threshold value that triggers a **Filter** action
 - Select the **Filter** action to execute upon exceeding that threshold
- Interval:** the measurement interval in milliseconds
 - Interval works with rate limit and burst limit to define the conditions that activate a **Filter** action
- Rate Limit:** threshold that is expressed in number of messages
- Burst Limit:** the allowed burst value
- Action:** select the **Filter** action to be triggered when the monitored message type exceeds threshold values
- Multiple threshold or filter settings can be specified

Edit Thresholds/Filters

Name: retire-wsCounter-count-monitor-1

Interval: 10000 messages

Rate Limit: 2 messages

Burst Limit: 3 messages

Action: retire-wsCounter-monitor-action

Apply Cancel

© Copyright IBM Corporation 2013

Step 4C: Thresholds/Filters for count monitor

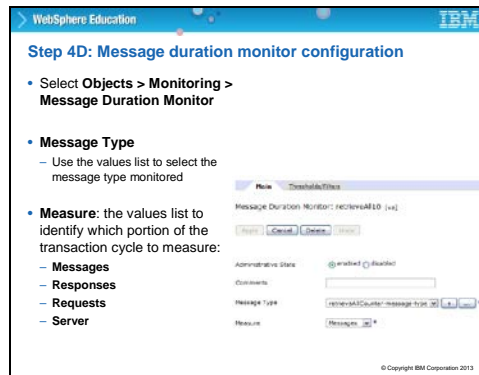
In the Configure Message Count Monitor page, you select the Thresholds/Filters tab, which allows you to specify the threshold value that triggers a previously defined Filter action object to run upon exceeding that threshold.

You also specify a measurement interval in milliseconds, which works with rate limit and burst limit to define the conditions that activate a Filter action.

The Rate Limit parameter defines the threshold that is expressed as a number of messages per interval that must not be exceeded.

Burst Limit is a parameter that allows for the occasional spike in the traffic rate that does not constitute an actionable threshold breach as such. However, if the threshold is exceeded in two successive time periods, the Burst Limit parameter has no effect.

The last pick list on this screen is where you choose the Filter action to be triggered when the monitored message type exceeds the threshold values. Specify multiple threshold/filter settings per Message Count Monitor.



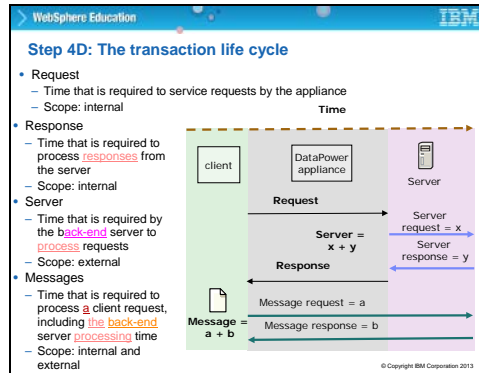
Step 4D: Message duration monitor configuration

Now turn attention to defining the message duration monitor. From the vertical menu bar, choose Objects, Monitoring, Message Duration Monitor.

Select the Message Type object to be monitored.

Use the Measure values list to identify which portion of the transaction cycle to measure.

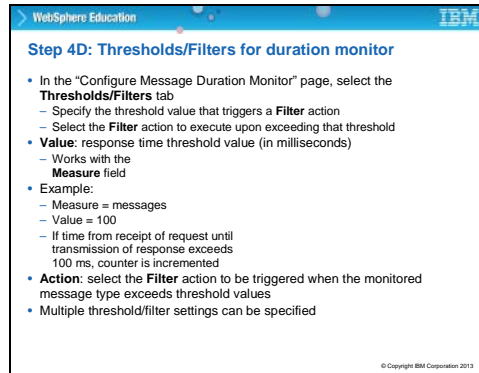
One can choose Messages, Responses, Requests, or Server.



Step 4D: The transaction lifecycle

The transaction lifecycle can be defined as one of:

- Request, being the time that is required to service requests by the appliance. That is, from the time the message arrives at the front side of the DataPower box to the time it is sent out the back end to the server. This time cycle is considered to have an internal scope, since it is all within the DataPower system.
- Response is the time that is required to process responses from the server until the message is handed back to the client. When again, the scope of this time cycle is internal.
- Server is the time that is required by the back-end server to process requests and is considered to have "external" scope.
- Messages is an aggregate of the above three time cycles. In other words, it is the total elapsed time as experienced by the client. It has a scope that is a combination of both internal and external.



WebSphere Education

Step 4D: Thresholds/Filters for duration monitor

- In the "Configure Message Duration Monitor" page, select the **Thresholds/Filters** tab
 - Specify the threshold value that triggers a **Filter** action
 - Select the **Filter** action to execute upon exceeding that threshold
- **Value:** response time threshold value (in milliseconds)
 - Works with the **Measure** field
- **Example:**
 - Measure = messages
 - Value = 100
 - If time from receipt of request until transmission of response exceeds 100 ms, counter is incremented
- **Action:** select the **Filter** action to be triggered when the monitored message type exceeds threshold values
- Multiple threshold/filter settings can be specified

© Copyright IBM Corporation 2013

Step 4D: Thresholds/Filters for duration monitor

Now configure the thresholds and filters for the duration monitor.

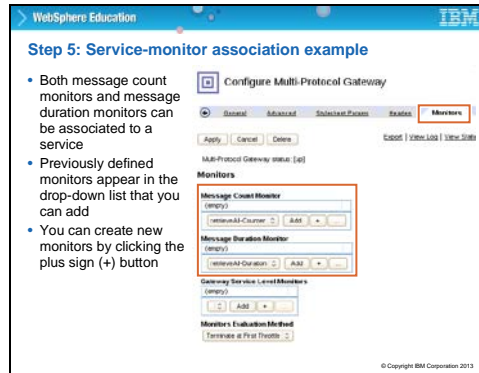
In the Configure Message Duration Monitor page, select the Thresholds/Filters tab and specify the threshold value that triggers a Filter action to be ran upon exceeding that threshold.

The Value parameter specifies the response time threshold value in milliseconds, and works with the Measure field.

For example, if one specifies the measure cycle to be "messages" and a value of 100. Asking the monitor to check whether the time from receipt of the request until transmission of the response exceeds 100 milliseconds, in which case, the counter is incremented by one.

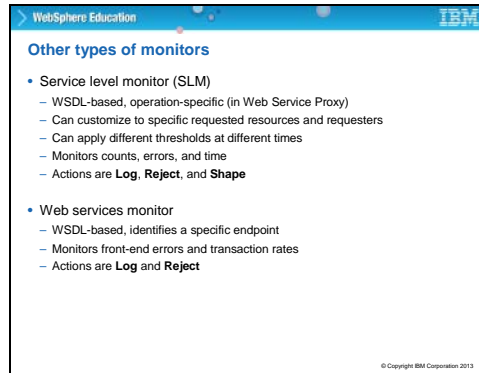
From the Action pick list, choose the previously defined Filter action to be triggered when the monitored message type exceeds threshold values.

As with the duration monitor, multiple threshold/filter settings can be specified.



Step 5: Service-monitor association example

The last step in setting up monitors within a service is choosing the ones that you want to include. Click the Monitors tab, and see two pick lists. Both message count monitors and message duration monitors can be associated to a service. Previously defined monitors appear in the drop-down list that you can Add to a list within the service configuration. If you want to do top-down creation of monitors, click the plus button.



The slide is titled "Other types of monitors" and is part of a "WebSphere Education" presentation. It lists two types of monitors: Service level monitor (SLM) and Web services monitor. The SLM is WSDL-based, operation-specific, and can be customized to specific resources and requesters. It monitors counts, errors, and time, and can apply different thresholds at different times. Its actions are Log, Reject, and Shape. The Web services monitor is also WSDL-based, identifies a specific endpoint, and monitors front-end errors and transaction rates. Its actions are Log and Reject. The slide is copyrighted by IBM Corporation in 2013.

- Service level monitor (SLM)
 - WSDL-based, operation-specific (in Web Service Proxy)
 - Can customize to specific requested resources and requesters
 - Can apply different thresholds at different times
 - Monitors counts, errors, and time
 - Actions are **Log**, **Reject**, and **Shape**
- Web services monitor
 - WSDL-based, identifies a specific endpoint
 - Monitors front-end errors and transaction rates
 - Actions are **Log** and **Reject**


© Copyright IBM Corporation 2013

Other types of monitors

There are two other types of monitor to be aware of...

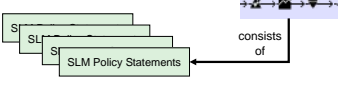
The Service level monitor, or SLM, is a WSDL-based, operation-specific monitor, usually used in the web service proxy. It can be customized to specific requested resources and requesters, and can apply different thresholds at different times. It monitors counts, errors, and time, and can apply the same three sanctions as the count and duration monitors; that is, it can Log, Reject, or Shape the message traffic. The topic SLM is discussed in more detail in a later section.

The web services monitor is also WSDL-based, and identifies a specific endpoint. It monitors front-end errors and transaction rates, and it can Log or Reject messages.

WebSphere Education 

Other types of monitors - service level monitors

- Service level monitor (SLM)
 - SLM policy actions offer the most fine-grained and sophisticated approach for setting up SLM in the DataPower device. Currently these actions can be used in the web service proxy and the multiprotocol gateway services.
 - An SLM action consists of one to many policy statements. Every statement has a numerical identifier. These identifiers define the order in which the statements are processed.



- A basic property of an SLM policy is the mode in which the contained policy statements should be handled. The following modes are available:
 - Processing of all statements of a policy
 - Processing of statements until the first action (notify, shape, reject) is taken
 - Processing of statements until a reject occurs


© Copyright IBM Corporation 2013

Other types of monitors – service level monitors.

Of the different types of monitors, service level monitors provide the finest-grained control.


Whereas, web services monitor requires that statistics be enabled on the appliance. It is called "gateway service level monitor" in a multi-protocol gateway.

In DataPower web services monitors were the original monitoring objects, and are replaced by the message monitors and the service level monitor.

WebSphere Education 

Other types of monitors - web services monitors

- Web services monitor
 - Web service monitors are configured by providing the URL of a Web Services Definition Language (WSDL). The main difference to message monitors is that a web service endpoint to be monitored can be specified. Web service monitors are also configured on the Monitor tab of the DataPower WebGUI with basic and simple configuration options.



Monitors

- Contrary to web service monitors, SLM policy actions are a more sophisticated and flexible way of monitoring web services.

© Copyright IBM Corporation 2013

Other types of monitors

There are two other types of monitor that to be aware of...

The Service level monitor, or SLM, is a WSDL-based, operation-specific monitor, usually used in the web service proxy. It can be customized to specific requested resources and requesters, and can apply different thresholds at different times. It monitors counts, errors, and time, and can apply the same three sanctions as the count and duration monitors. That is, it can Log, Reject, or Shape the message traffic. SLM is discussed in more detail in a later section.

The web services monitor is also WSDL-based, and identifies a specific endpoint. It monitors front-end errors and transaction rates, and it can Log or Reject messages.

WebSphere Education				
Monitor types supported by a service				
<ul style="list-style-type: none"> The types of monitors you can associate with a service depend on what type of service it is 				
Service type	Message monitors	Service level monitors	Web service monitors	Notes
XSL proxy	✓			
XML firewall	✓		✓	
Web Service Proxy	✓	✓		(Msg) Monitor tab in OBJECTS view
Multi-protocol gateway	✓	✓	✓	
Web application firewall	✓			Message count monitor as part of the error policy

Which monitor types are supported by a service?

The types of monitors you can associate with a service depend on what type of service it is.

The XSL Proxy supports the Message Monitors – both count and duration.

The XML Firewall supports the Message Monitors and the Web Services Monitor.

The Web Service Proxy supports the Message Monitors and the Service Level Monitor.

The Multi-Protocol Gateway supports all three.

And the Web Application Firewall supports the Message Monitors – both count and duration, and only as part of the Error Policy.

Slide 20

WebSphere Education

IBM

Unit summary

Having completed this unit, you should be able to:

- Identify messages that are to be monitored
- Configure a message count monitor
- Set up a message duration monitor

© Copyright IBM Corporation 2013

Slide 21

WebSphere Education

IBM

Checkpoint questions

- What are the two types of message monitors?
 - Message count monitor
 - Message duration monitor
 - Message size monitor
 - Message payload monitor
- Select the proper **Message Filter** action definition:
 - Message Filter** action: A **Filter** action filters the message payload to the dev/null bucket.
 - Message Filter** action: A **Filter** action specifies the administrative actions that are taken in response to the overuse of system or network resources by a monitored message type.
 - Message Filter** action: A **Message Filter** action strips off the message header as defined in the action header section. A check sum is then added to the end of the message with the specific **Message Filter** hash algorithm.

© Copyright IBM Corporation 2013

WebSphere Education

IBM

Checkpoint answers

1. A and B. What are the two types of message monitors?
 - ✓ A. Message count monitor
 - ✓ B. Message duration monitor
 - C. Message size monitor
 - D. Message payload monitor
2. B. Select the proper **Message Filter** action definition:
 - A. **Message Filter** action: A **Filter** action filters the message payload to the dev/null bucket.
 - ✓ B. **Message Filter** action: A **Filter** action specifies the administrative actions that are taken in response to the overuse of system or network resources by a monitored message type.
 - C. **Message Filter** action: A **Message Filter** action strips off the message header as defined in the action header section. A check sum is then added to the end of the message with the specific **Message Filter** hash algorithm.

© Copyright IBM Corporation 2013