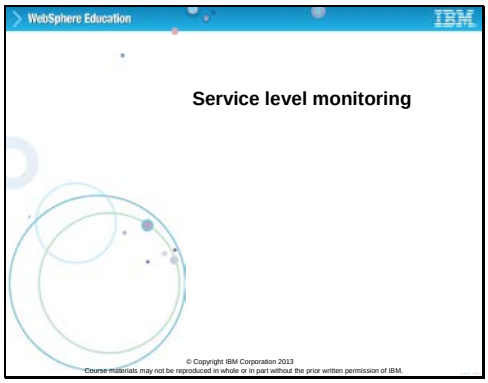
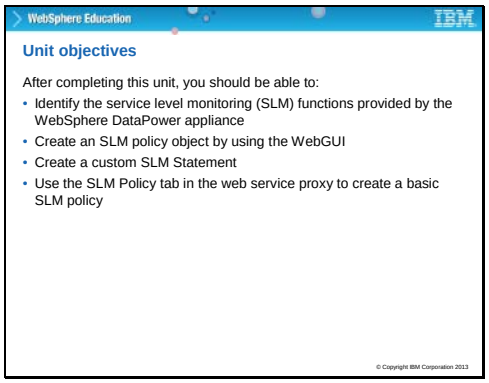
Slide 1


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

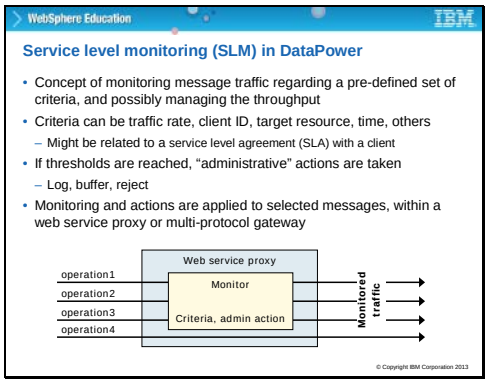
Slide 2



In this presentation, students examine how to create a service level monitoring policy. Two types of service level monitoring policies can be created: a simple statement and an advanced statement. The DataPower appliance automatically generates the simple statement. The advanced statement is constructed by creating the respective objects.

Peer URLs are not covered in this presentation, but they are relevant to SLM and might be the subject of questions that students ask. The peer URLs are used to specify a set of DataPower boxes that enforce the same service level monitoring policy. It allows one DataPower box to share traffic information with other DataPower boxes. The service level monitoring policy must also be defined on each of the boxes that are enforcing that policy.

Slide 3



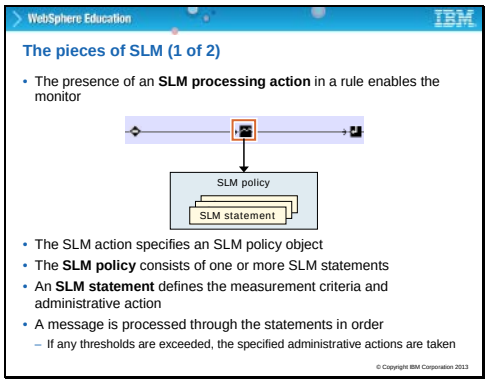
What is service level monitoring (SLM)?

So, what is Service Level Monitoring, or "SLM" as it is usually abbreviate it?

It is the process of measuring service quality. By that performance and availability are meant relative to customer expectations. One must ensure the quality stays within agreed-upon parameters that are defined by service level agreements (SLA), by reporting results and taking appropriate actions.

To implement an SLM, incoming traffic is filtered based on predefined criteria and a policy is applied to selected messages. If thresholds are reached during the measured interval, then the configured action runs.

Slide 4



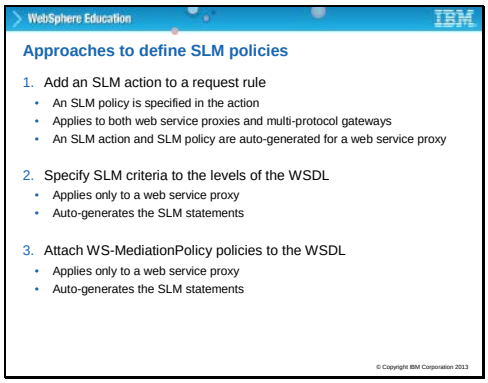
SLM in DataPower: Basic principles

First, some basic principles that apply to SLM. Service-level monitors allow administrative control over users and resource groups, and can penalize services that fail to comply with service policy.

An SLM policy consists of one or more statements that consists of restrictions, along with actions that can be taken when a restriction is violated. This restriction is implemented by an SLM policy.

An SLM Statement counts messages or measures message execution duration. You can have more than one SLM statement, and they are processed sequentially in the order they are configured. An SLM policy consists of one or more statements. Incoming traffic is monitored and controlled in accordance with the SLM policies that are defined.

Slide 5

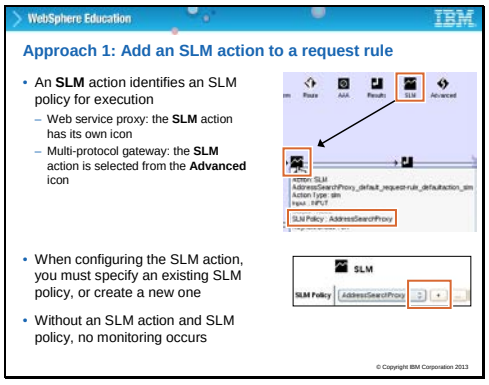


As you might expect, there are three ways to configure an SLM – top-down, and bottom-up. The first two approaches are supported for many years. The first method – top-down – typically happens during the configuration of a document processing policy.

In this approach, the SLM Rule action is configured as part of the document processing policy by adding the SLM icon to the Rule execution line. In the web service proxy, the SLM Rule action is a separate icon in the policy editor whereas in the multi-protocol gateway, the SLM Rule action is selected from the Advanced icon. The second method – bottom-up – requires you to use the left-side vertical menu, specifically, the Objects/Monitoring option. In this approach, all the basic SLM objects are first configured and then SLM policy is constructed from these basic components.

WS-MediationPolicy is an IBM proposed web service standard for quality of service (QoS) specifications. WS-MediationPolicy statements can be a policy attachment for a WSDL, and be stored in WebSphere Service Registry and Repository. WS-MediationPolicy statements auto-generate SLM-related processing rules. These rules execute before the developer-specified rules within the web service proxy. WS-MediationPolicy is not covered in any detail in this course.

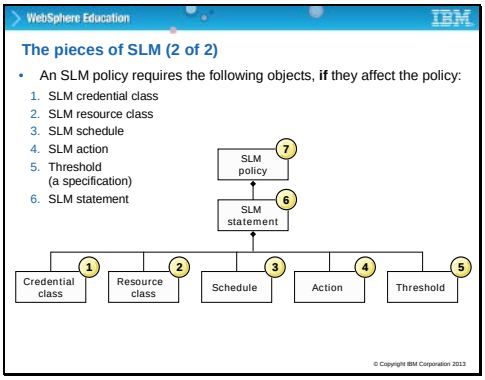
Slide 6



The **SLM** action screen capture is from a web service proxy.

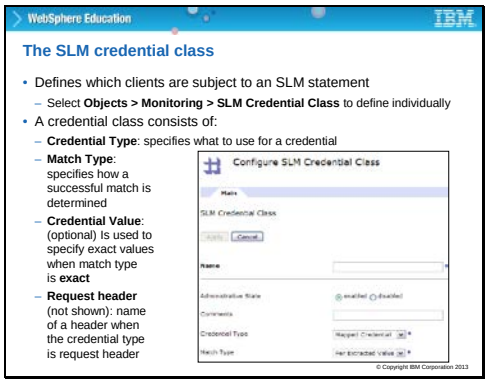
Compare this action with the SLM action object, which is covered later.

Slide 7



A threshold is not a separate object. It is a specification within an SLM statement. Depending on what criteria are needed for a specific SLM statement, only certain SLM objects are needed. For example, if you are monitoring only the target resource, then the SLM credential and SLM schedule objects are not needed. The numbered steps are used to build an SLM policy. The chart essentially shows the object dependencies. A credential class, resource class, schedule, action, and thresholds are used to define an SLM statement. The SLM policy is composed of one or more statements.

Slide 8

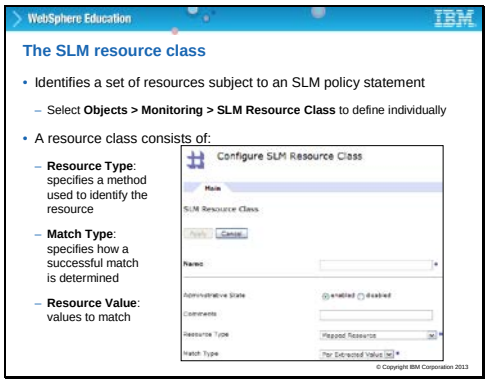


The SLM credential class

The credential class defines a user group subject to SLM statement restrictions. It consists of a Credential Type, which specifies the method that is used to obtain the credential, and a Match Type that specifies how a successful match is determined. There might be a Credential Value that is used to specify exact values for an exact match.

If the credential type is request header then you can specify the header that contains the information.

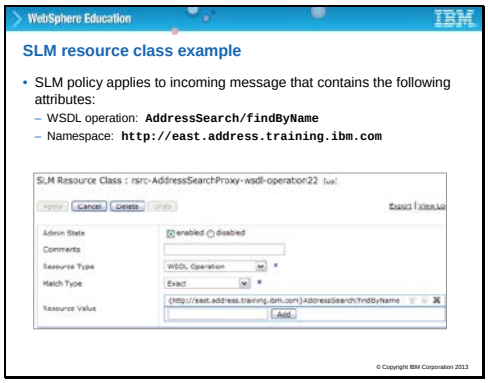
Slide 9



The SLM resource class

The SLM resource class identifies a set of resources subject to an SLM policy statement. It consists of a Resource Type, a Match Type, and a Resource Value. The Resource Type specifies a method that is used to identify the resource. Match Type specifies how a successful match is determined. Resource Value lists the values to match.

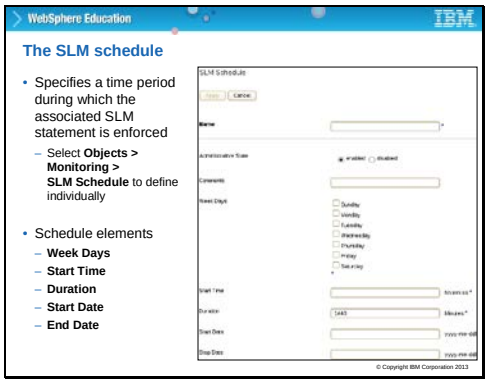
Slide 10



SLM resource class example

Here is an example of an SLM resource class. In this example, the SLM policy applies to an incoming message that contains the attributes WSDL operation, with a value of AddressSearch/findByLocation, together with a namespace with the value `http://east.address.training.ibm.com`.

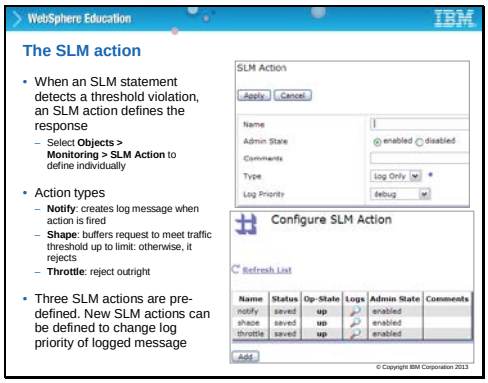
Slide 11



The SLM Schedule

Here is where the SLM definition is more sophisticated than the Message Monitor definition. It allows for selective monitoring at certain times of the day, and certain days of the week.

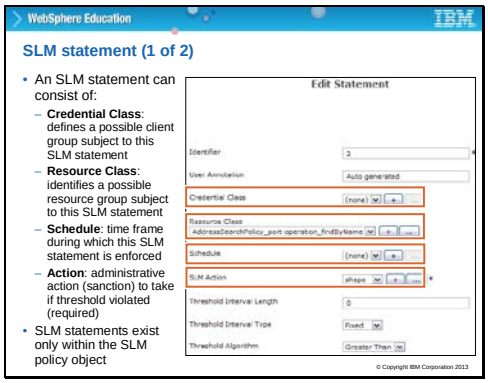
Slide 12



The SLM action

When an SLM policy statement detects a service level violation, an SLM action defines the response. The actions types can be notify, shape, or throttle.
The term “throttle” seems a little incongruous in this context. You might remember the message monitors looked at in the previous section used the term “reject” when messages are to be dropped. In this context, “throttle” means the same as “reject.”

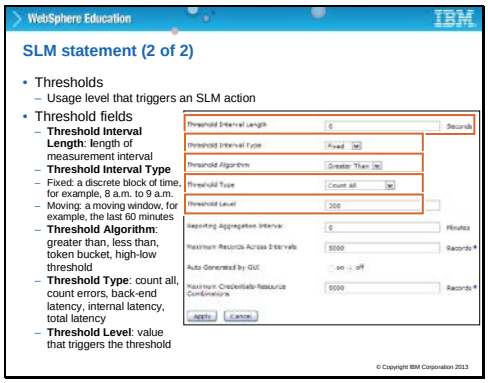
Slide 13



SLM statement (1 of 2)

This slide brings it all together. An SLM statement consists of the Credential Class, the resource class, a schedule, and an action.

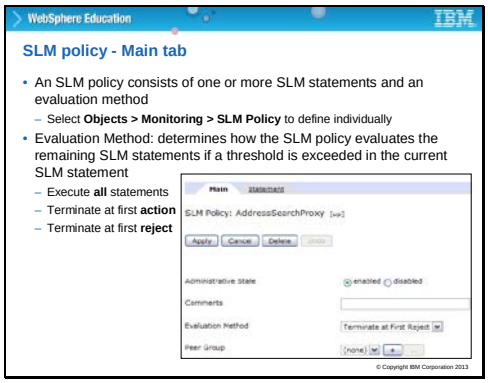
Slide 14



SLM statement (2 of 2)

Notice how the threshold parameters for SLM are more sophisticated than the message monitors. For example, the “token bucket” parameter is analogous to a “three-strikes-you-are-out” scenario. It allows you to grant some “tokens” to a particular monitor, and you take a token out of the “bucket” each time a threshold is breached. When the bucket is empty, the breach causes the defined action to take place. However, if a time period elapses during which the threshold is *not* exceeded, a token is put back in the bucket. It is like a reward for good behavior.

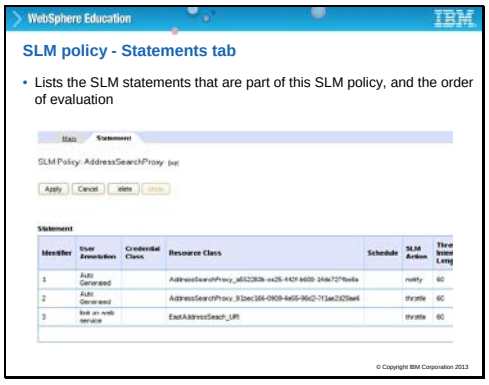
Slide 15



SLM policy

Since there can be a series of SLM statements within a single policy, it is possible that more than one might be relevant to a particular threshold breach. It is also possible that the actions taken might vary in severity from statement to statement. Within the SLM policy, there is the ability to decide whether all statements are applied. Only those statements up to the first threshold breach. Or only those statements up to the first statement that would cause a message are dropped.

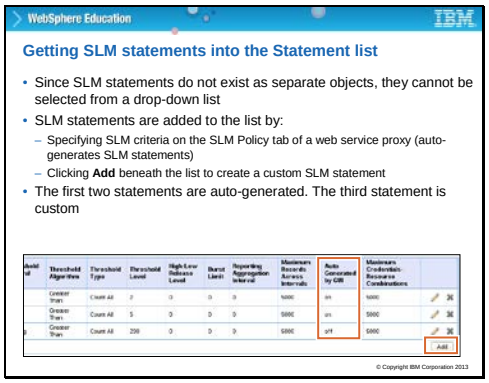
Slide 16



SLM policy – statements tab.

This slide shows the Statements tab, which lists the SLM statements that are part of this SLM policy, and the order of evaluation.

Slide 17

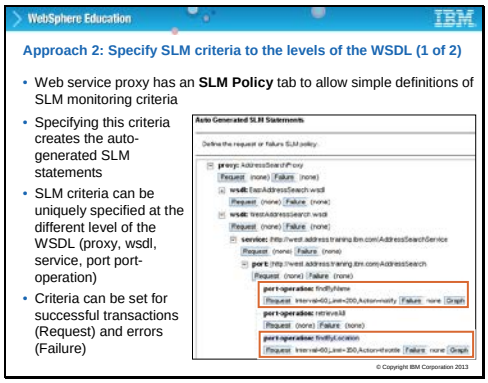


Getting SLM statements:

This graphic is the right side of the WebGUI page from the previous slide. Since SLM statements do not exist as separate objects, they cannot be selected from a drop-down list

SLM statements are added to the list by:

Slide 18



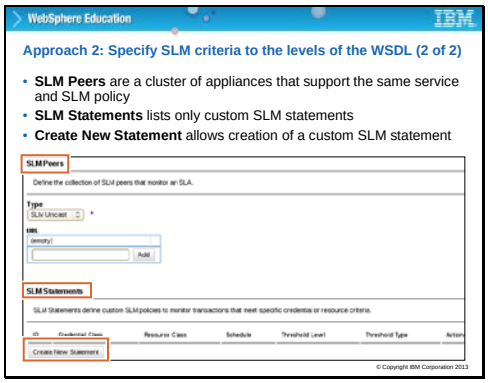
Approach 2, specify SLM criteria to the levels of the WSDL (1 of 2)

For the auto-generated SLM statements, you specify the measurement interval, the threshold value, and the SLM action to take if the threshold is exceeded.

The **Graph** button is covered in a later slide.

The screen capture shows a service-level policy for the findByName operation of 200 transactions per 60 seconds, which if exceeded results in a notify action. It also dictates that five failed transactions within 60 seconds get logged. For the findByLocation operation, a lower limit of 150 transaction per 60-seconds results in the throttle action.

Slide 19



Approach; specify SLM criteria to the levels of the WSDL (2 of 2)

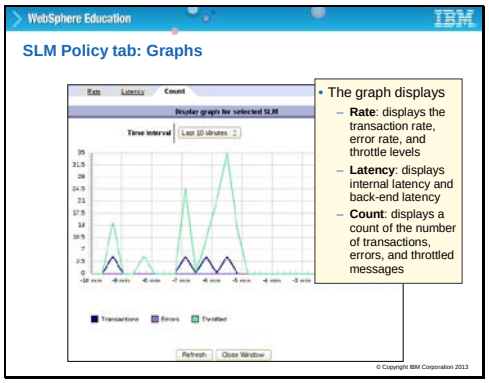
This graphic is the lower part of the SLM Policy tab for a web service proxy.

Configuring SLM peers is an administrative task.

SLM Statement lists only custom SLM statements that exist within the SLM policy that has the same name as the web service proxy. The specifications on this page define the default SLM policy object that is created for the web service proxy.

If you click **Create New Statement**, the page repaints with a section that contains the same fields as exist in an SLM statement configuration page.

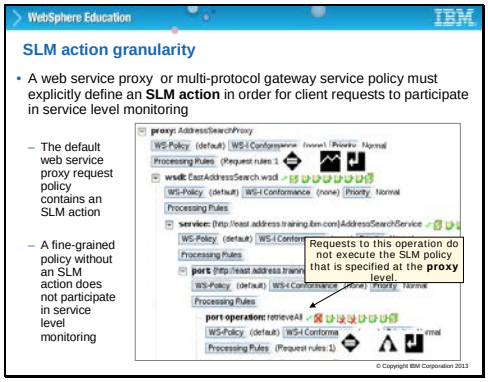
Slide 20



Service level monitor: Graphs

Here is an example of a graph that would appear if you were to click a link as described on the previous slide. You can select the duration that is represented by the graph from the pick-list at the top, and it shows three categories of message.

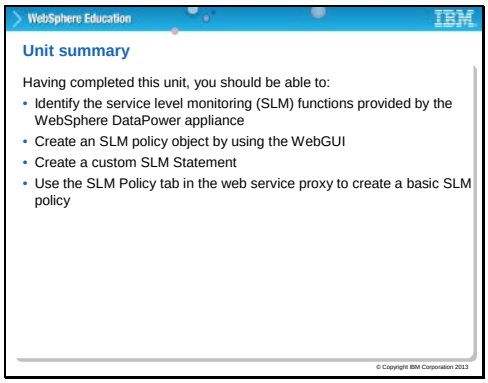
Slide 21



SLM action granularity

Default request and response rules are configured at the proxy level. The request includes a match action and a result action, together with an SLM action. You can add to or subtract from these actions if you want. You can add rules at different levels, right down to the fine-grained operation level. Remember that, if there is a rule that is defined for, say, a request at a lower level, any request rule that is defined at a higher level does not run. So for example, in the screen capture on this slide there is a request direction rule that is configured for the operation that is called findByLocation that includes a verify action but no SLM action. Therefore, any request for this operation does not run an SLM action.

Slide 22


WebSphere Education
IBM
Unit summary
Having completed this unit, you should be able to:
• Identify the service level monitoring (SLM) functions provided by the WebSphere DataPower appliance
• Create an SLM policy object by using the WebGUI
• Create a custom SLM Statement
• Use the SLM Policy tab in the web service proxy to create a basic SLM policy
© Copyright IBM Corporation 2013

Slide 23

Checkpoint questions

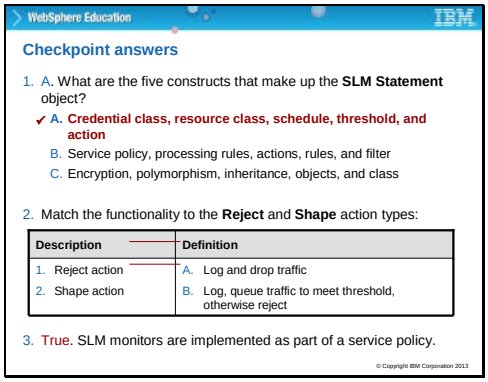
1. What are the five constructs that make up the **SLM Statement** object?
   A. Credential class, resource class, schedule, threshold, and action
   B. Service policy, processing rules, actions, rules, and filter
   C. Encryption, polymorphism, inheritance, objects, and class

2. Match the functionality to the **Reject** and **Shape** action types:

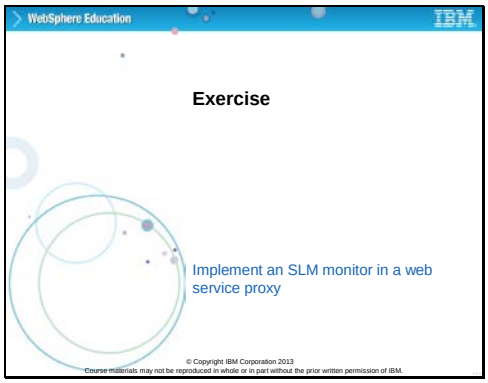
Description	Definition
1. Reject action	A. Log and drop traffic
2. Shape action	B. Log, queue traffic to meet threshold, otherwise reject

3. True or False: SLM monitors are implemented as part of a service policy.

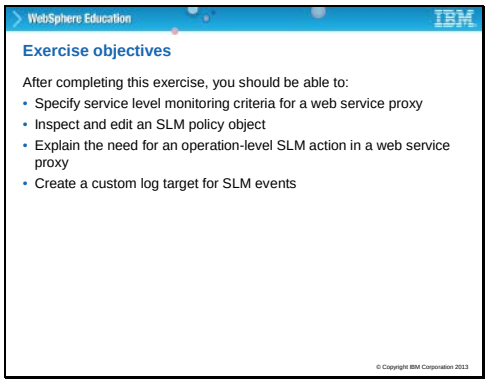
Slide 24


WebSphere Education
IBM
Checkpoint answers
1. A. What are the five constructs that make up the SLM Statement object?
✓ A. Credential class, resource class, schedule, threshold, and action
B. Service policy, processing rules, actions, rules, and filter
C. Encryption, polymorphism, inheritance, objects, and class
2. Match the functionality to the Reject and Shape action types:
Description
Definition
1. Reject action
2. Shape action
A. Log and drop traffic
B. Log, queue traffic to meet threshold, otherwise reject
3. True. SLM monitors are implemented as part of a service policy.
© Copyright IBM Corporation 2013

Slide 25


WebSphere Education
IBM
Exercise
Implement an SLM monitor in a web service proxy
© Copyright IBM Corporation 2013
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Slide 26


WebSphere Education
IBM
Exercise objectives
After completing this exercise, you should be able to:
• Specify service level monitoring criteria for a web service proxy
• Inspect and edit an SLM policy object
• Explain the need for an operation-level SLM action in a web service proxy
• Create a custom log target for SLM events
© Copyright IBM Corporation 2013