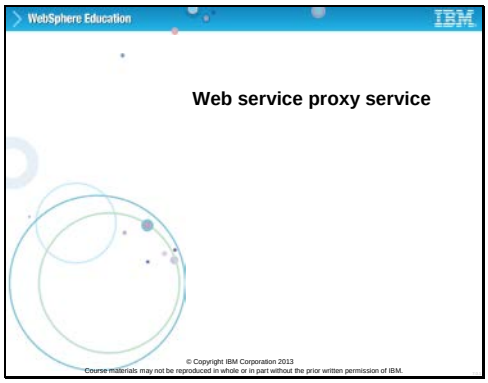
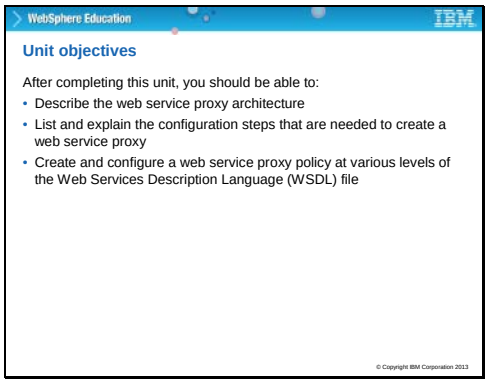
Slide 1


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

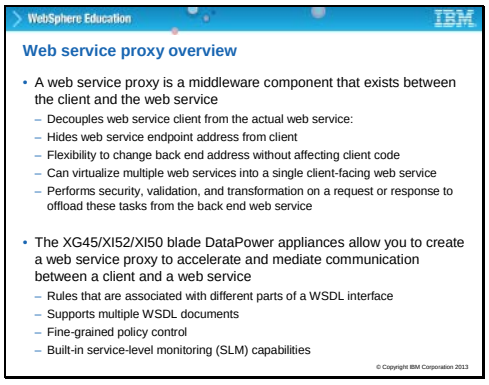
Slide 2



This presentation covers how to create a web service proxy service and associate it with multiple WSDL files. Students examine the service-wide settings and fine-grained service policy. The web service proxy service is the recommended service on the appliance. The actions that are covered in the XML firewall unit are also applicable to the web service proxy service.

Emphasize the fact that the web service proxy service supports multiple protocol handlers on the front side in a way similar to the multi-protocol gateway. The WebGUI uses only the HTTP and HTTPS as the back-end transports. However, using the dynamic back-end type allows you to use other protocol handlers, such as WebSphere MQ. The SLM support of the web service proxy service is mentioned, but it is not examined until the module and exercise on creating service level monitoring policies.

Slide 3

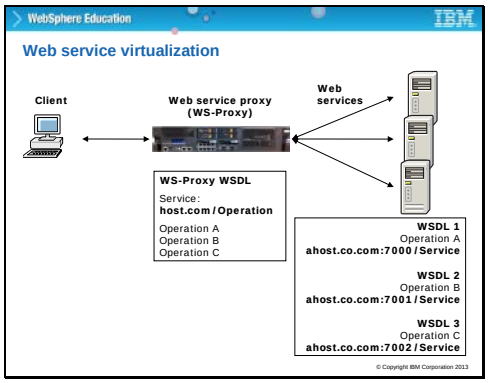


Web service proxy overview

So, what is a web service proxy? It is a middleware component that exists between the client and the web service that decouples the client from the web service. It hides web service endpoint address from the client, and has the flexibility to change the back-end address without affecting client code. It performs security, validation, and transformation on a request or response to offload these tasks from the back-end web service. It supports multiple WSDL documents that define the back-end services, and allows you to create rules that are associated with different parts of each WSDL interface, giving you fine-grained policy control with built-in service-level monitoring capabilities.

The WSP runs on the XS40, XG45, XI50, XI52, and XB62 DataPower appliances.

Slide 4

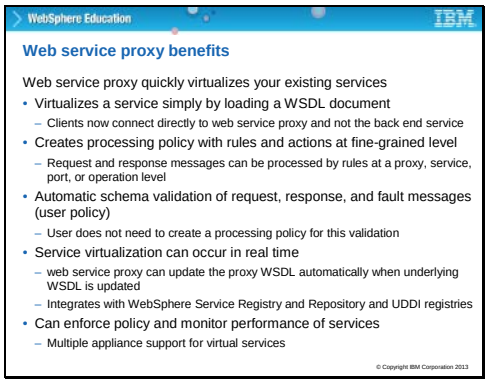


Web service proxy architecture

Notice the three back-end servers, each advertising services on different ports and expecting different operations. You can load the WSDLs that define these services into a Web Service Proxy, and create a proxy WSDL that is seen by the outside world. The client never knows the true back-end server names, addresses, ports, or services.

In addition to providing protection, this facility allows for flexibility in changing the backend servers. Since the Web Service Proxy advertises the same WSDL to the client, but maps it correctly to the new backend configuration. So system changes can be made transparent to the outside world.

Slide 5



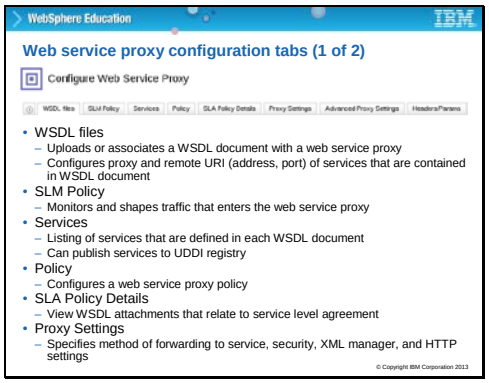
Web service proxy benefits

The web service proxy quickly virtualizes your existing services by loading a WSDL document. Clients now connect directly to the web service proxy and not the back-end service. You can create a processing policy with rules and actions at fine-grained level: request and response messages are processed by rules at a proxy, service, port, or operation level. You can also specify automatic schema validation of request, response, and fault messages (user policy), but the user does not create a processing policy. It can publish WSDL documents to a service directory, such as a UDDI repository or WebSphere Service Registry and Repository, commonly referred to as WSRR.

Service virtualization can occur in real time. A web service proxy can update the proxy WSDL automatically when underlying WSDL is updated.

You can enforce policy and monitor performance of services, even when you have multiple DataPower appliances in a cluster; it can support virtual services across the cluster.

Slide 6



Web service proxy features

When you begin to configure the Web Service Proxy, the screen displays several tabs across the top. Clicking each changes the rest of the screen to allow you to edit the appropriate parameters. Here is what they do:

WSDLs: Uploads or associates a WSDL document with a web service proxy and configures proxy and remote URI (address, port) of services that are contained in WSDL document.

SLM: Monitors and shapes traffic that enter the web service proxy.

Services: Listing of services that are defined in each WSDL document, and controls the publishing of services to a UDDI or WSRR registry.

Policy: Configures a web service proxy policy.

Proxy Settings: Specifies method of forwarding to service, security, XML manager, and HTTP settings.

Advanced Proxy Settings: Configures advance connection settings.

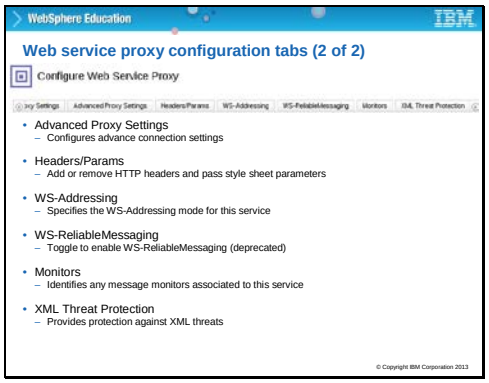
Headers/Params: Add or remove HTTP headers and pass style sheet parameters.

WS-Addressing: Specifies the WS-Addressing mode for this service.

XML Threat Protection: Provides protection against XML threats.

These last two are not shown in the screen capture, nor would they appear on a normal width screen in a browser window. But there is an arrow in a circle to the right that allows you to scroll the tabs sideways to see the extra tabs.

Slide 7



Web service proxy features

When you begin to configure the Web Service Proxy, the screen displays several tabs across the top. Clicking each changes the rest of the screen to allow you to edit the appropriate parameters. Here is what they do:

WSDLs: Uploads or associates a WSDL document with a web service proxy and configures proxy and remote URI (address, port) of services that are contained in WSDL document.

SLM: Monitors and shapes traffic that enters the web service proxy.

Services: Listing of services that are defined in each WSDL document, and controls the publishing of services to a UDDI or WSRR registry.

Policy: Configures a web service proxy policy.

Proxy Settings: Specifies method of forwarding to service, security, XML manager, and HTTP settings.

Advanced Proxy Settings: Configures advance connection settings.

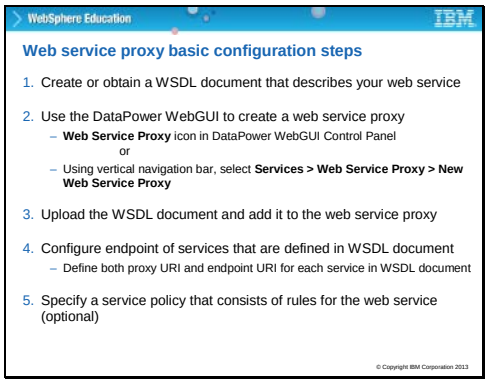
Headers/Params: Add or remove HTTP headers and pass style sheet parameters.

WS-Addressing: Specifies the WS-Addressing mode for this service.

XML Threat Protection: Provides protection against XML threats.

These last two are not shown in the screen capture, nor would they appear on a normal width screen in a browser window. But there is an arrow in a circle to the right that allows you to scroll the tabs sideways to see the extra tabs.

Slide 8

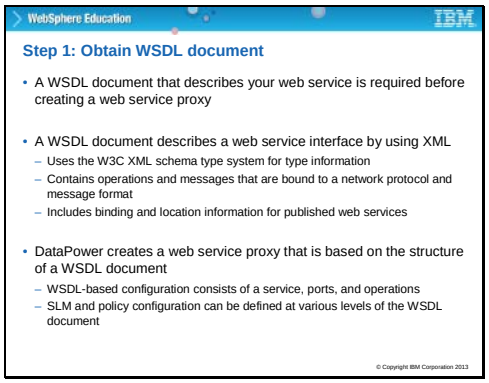


Web service proxy basic configuration steps

To configure a WSP, follow these steps:

1. Create or obtain a WSDL document that describes your web service.
2. Use the DataPower WebGUI to create a web service proxy from either the Web Service Proxy icon in the DataPower WebGUI Control Panel or by using the vertical navigation bar (**Select SERVICES > Web Service Proxy > New Web Service Proxy**).
3. Upload the WSDL document and add it to the web service proxy.
4. Configure the endpoints of services that are defined in WSDL document by defining both the proxy URI and the endpoint URI for each service in WSDL document.
5. Specify a processing policy that consists of rules for the web service (optional).

Slide 9



Step 1: Obtain WSDL document

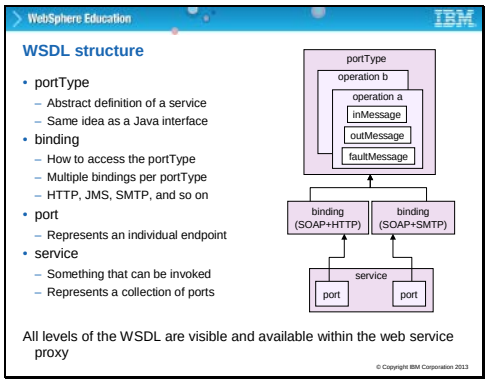
Step 1: Obtain WSDL document

A WSDL document that describes your web service is required before creating a web service proxy.

A WSDL document describes a web service interface by using the W3C XML schema type system for type information. It contains operations and messages that are bound to a network protocol and message format, and includes binding and location information for published web services.

DataPower creates a web service proxy that is based on the structure of a WSDL document that consists of a service, ports, and operations. SLM and policy configuration can be defined at various levels of the WSDL document.

Slide 10

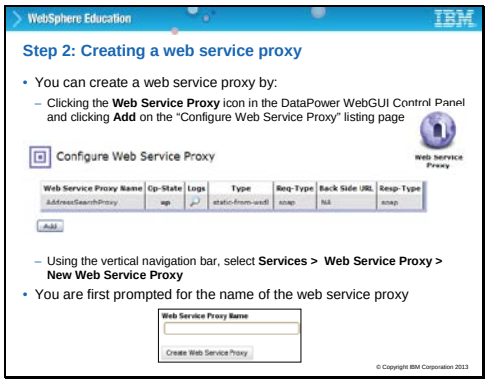


WSDL structure

The WSDL structure consists of:

- Port Type, which is an abstract definition of a service; the same idea as a Java interface.
- Binding, which describes how to access the portType. There can be multiple bindings per portType by using HTTP, JMS, SMTP, and so on.
- A port, which represents an individual endpoint.
- A Service, which is something that can be invoked; it represents a collection of ports.

Slide 11

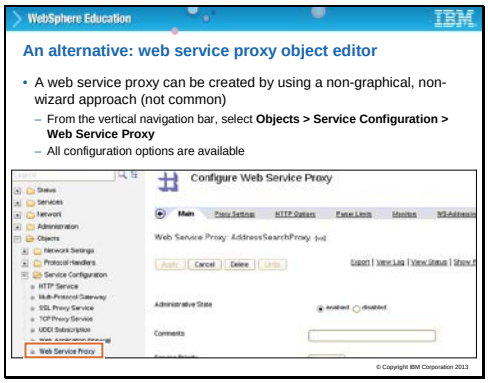


Step 2: Creating a web service proxy

A web service proxy is created by clicking the Web Service Proxy icon in the DataPower WebGUI Control Panel and clicking Add on the Configure Web Service Proxy listing page.

As is the case with most things within the DataPower system, a Web Service Proxy can also be created as just another object from the Object menu. Using the vertical navigation bar, select SERVICES > Web Service Proxy > New Web Service Proxy. However, it is usually quicker to click the icon on the Control panel.

Slide 12



Web service proxy object editor

If you do decide to create the web service proxy as an object, you can find it under Services Configuration. You then configure the objects that compose the web service proxy. The same configuration options are available as when you go through the Control Panel.

Slide 13

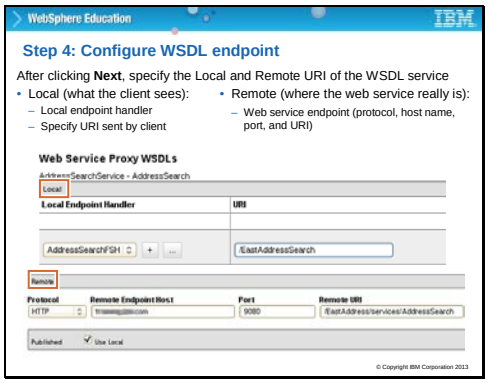
Step 3: Add WSDL document to web service proxy

When editing the WSP, select the WSDLs that reflect the backend servers to connect to. Click Add on the Configure Web Service Proxy listing page. The Configure WSP page opens with the WSDL tab already selected. Enter the Web Service Proxy Name on the creation page; then select the Add WSDL radio button. Add the WSDL file by using one of the following approaches:

- Enter WSDL File URL (remote or local URL)
- Upload WSDL file to local: or store: directory
- Select a previously uploaded WSDL document
- Browse UDDI or WSRR

When decided, click Next.

Slide 14



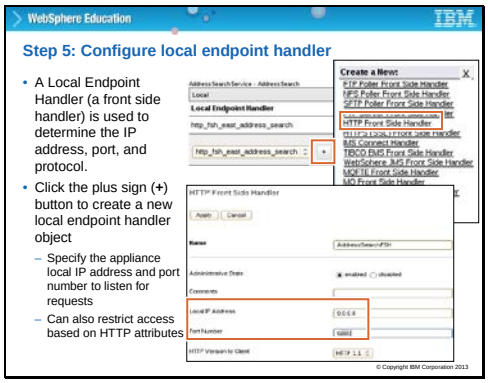
Step 4: Configure WSDL endpoint

After clicking Next, specify the Local and Remote URI of the WSDL service.

Local is what the client sees and defines a local endpoint handler and URI invoked by the client.

Remote is where the web service really is and defines the web service endpoint – its protocol, host name, port, and URI.

Slide 15

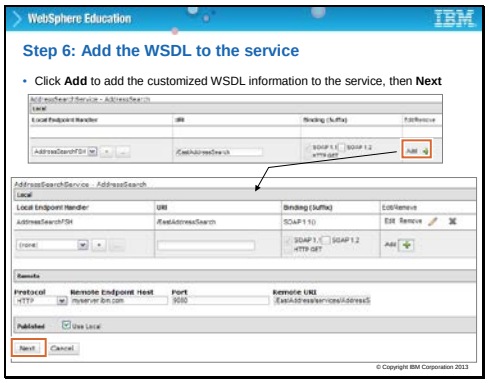


Configure local endpoint handler

Although the WSP talks HTTP to the backend servers, it lacks the ability to accept various protocols that come in from the client. Usually, its HTTP or HTTPS, but it can also be WebSphere MQ, or WebSphere Application Server JMS, or FTP, or several others. Endpoint handlers are covered in more detail when the Multi-Protocol Gateway is covered.

To create an Endpoint Handler, click the plus (+) button then specify the appliance local IP address and port number to listen for requests. You can also restrict access based on HTTP attributes.

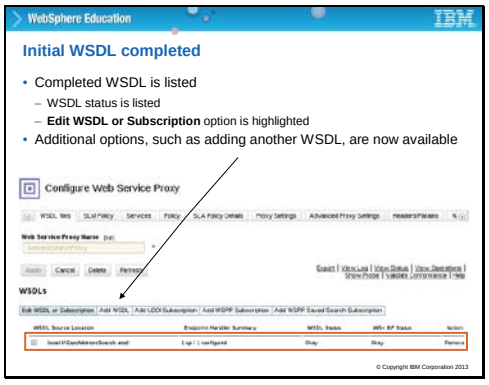
Slide 16



Add the WSDL to the service

Setting up the local endpoint handler, the URL, and the bindings is complete. Now add the information to the list of handlers that DataPower knows about. By clicking the Add button, the information appears in the list of handlers. You can edit it by choosing the appropriate action to the right of the list. You commit the handler to the service by clicking the Next button.

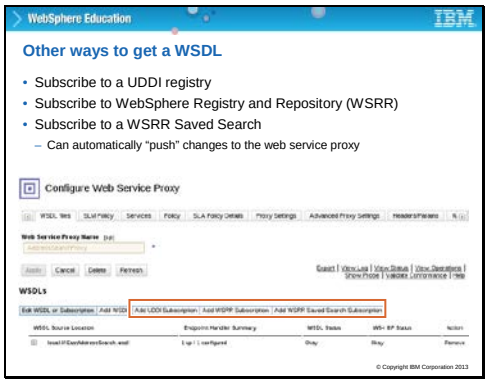
Slide 17



Initial WSDL completed

The image on the slide is what you see on the main tab. There is a list of WSDLs that are already added, and you can click the plus sign to examine the details. If you want to add another WSDL file, or another endpoint handler, you select the next tab that is called Add WSDL, and repeat the process in the same way as for the first endpoint handler.

Slide 18

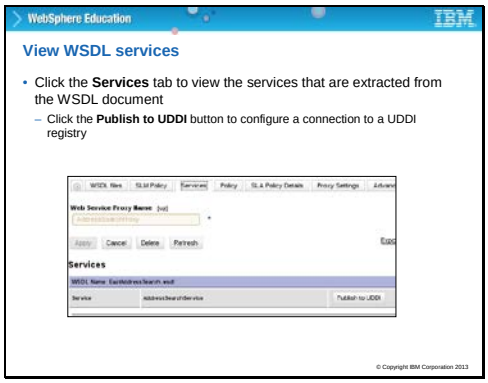


A subscription to a registry might also retrieve a WSDL file.

Generally, the registries are polled for the WSDL file on a timed basis, and can also be explicitly polled.

A WSRR Saved Search can be configured to send a WSDL file update from WSRR to the service.

Slide 19



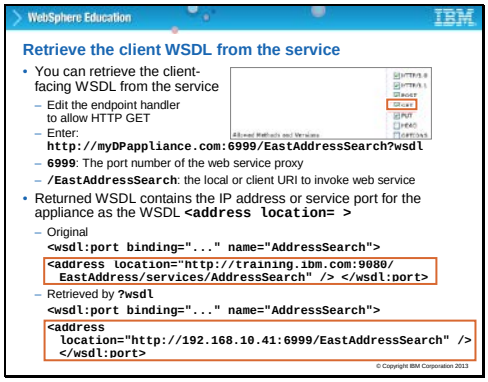
View WSDL services

Click the Services tab to view the services that are extracted from the WSDL document.

Click the Publish to UDDI button to configure a connection to a UDDI registry.

Not shown in this screen capture is another button that allows you to publish to a WSRR.

Slide 20

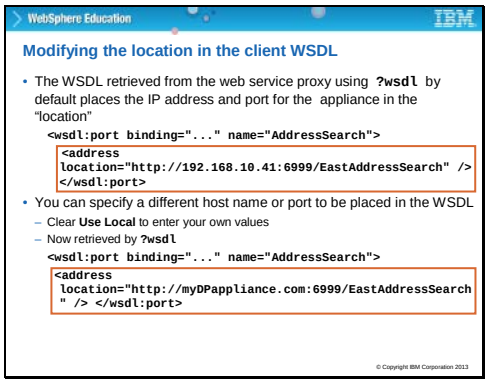


Retrieve the "client" WSDL from the service

It is a normal feature of any web service to allow the retrieval of the WSDL document by appending “question-mark-W-S-D-L” to the end of the URL. But first edit the front side handler to allow
HTTP GET.
For example, you might enter:
`http://myDPappliance.com:6999/EastAddressSearch?wsdl` to retrieve the WSDL.
In this example, *6999* is the port number of the WS-Proxy service, and *`/EastAddressSearch`* is the local or client URI to invoke web service.
The returned WSDL contains the appliances IP address or service port as the WSDL

`<address location= >` instead of the original web servers address.

Slide 21

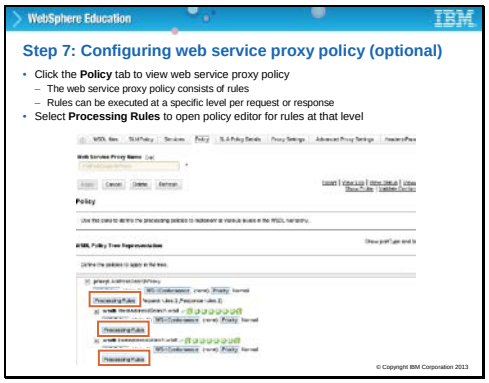


Modifying the location in the "client" WSDL

The WSDL (retrieved from the WS-Proxy service using **?wsdl** by default) places the appliances IP address and port in the "location", but you can specify a different host name or port to be placed in the WSDL. To perform this action, first clear Use Local to enter your own values.

The process provides an even greater degree of security by preventing users from seeing the true IP address and port of the DataPower device.

Slide 22



Step 7: Configuring web service proxy policy (optional)

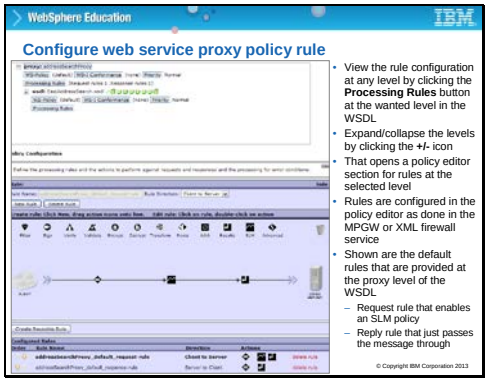
Even though the WSP is primarily driven by WSDLs and other parameters, you can also add policy rules to the service, at any level within the WSDL.

Click the Policy tab to view web service proxy policy. Rules can be ran at a specific level per request or response.

The proxy generates a default request and a default response rule – the Request rule consists of an SLM and a Results action, and the Response rule consists of a Results action.

You can arrange a hierarchy of policy rules. Click the Add Rule button to create rules at various levels of the WSDL document: proxy, wsdl, service, port, or operation.

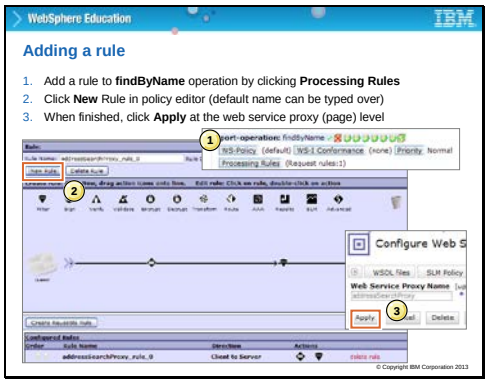
Slide 23



Configure web service proxy policy rule

View the rule configuration by clicking the Add Rule button or selecting a previously configured rule. Then, you can edit the rule just the same as in any other service.

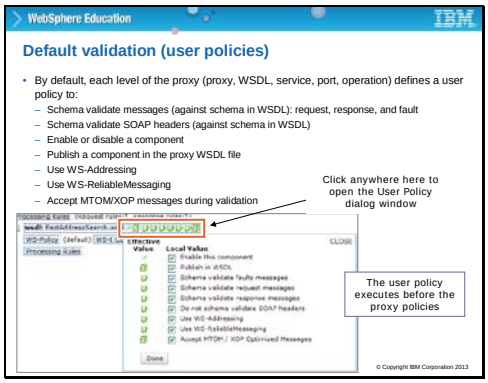
Slide 24



Adding a rule

You are already familiar with the rule editor. With a web service proxy service, you must be sure that you are adding the rule at the correct level. In the diagram on the slide, the rule is added at the operation level. You can see the list of rules that are defined at this level next to the Processing rules button. You click the button, which brings up the editor, where you can create a rule or edit an existing one.

Slide 25



Default validation (user policies)

The User Policy parameters are a little obscure – they show up as a horizontal row of small yellow folder icons, some of which might have a green check mark over them. In order to view or change the parameters, click anywhere within the row of yellow folders and a drop-down form appears. The process allows you to click check boxes to alter the degree of validation you want.

By default, each level of the proxy (proxy, wsdl, service, port, operation) defines a user policy to:

Schema validate request, response, and fault messages (against the schema in WSDL)

Schema validates SOAP headers (again, against the schema in WSDL)

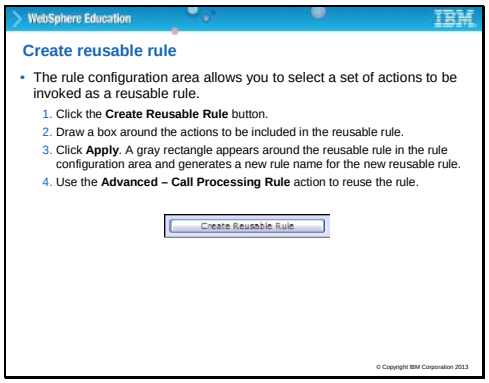
Enable or disable a component

Publish a component in the proxy WSDL file

Use WS-Addressing

Use WS-ReliableMessaging

Slide 26

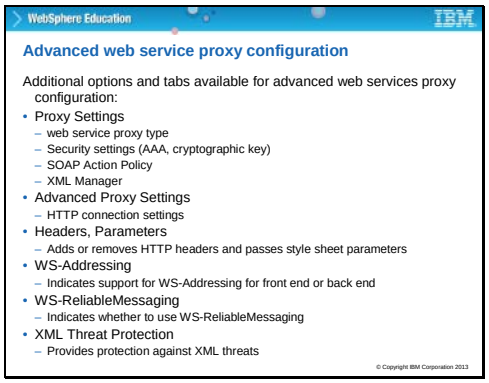


Create reusable rule

Here is a feature of the rule editor that was not covered earlier. Because you have multiple WSDLs in a WSP, and each can be broken down too many sublevels, and each of those levels can have rules, it is possible you might want to repeat certain actions many times. Since it can be tedious setting up all those actions, you can short-cut this process by creating a “reusable rule”.

Click the Create Reusable Rule button, and your mouse cursor becomes a cross. Click and drag to surround the actions you want repeated, and when you release the mouse button, you see those actions “captured” with a blue-gray rectangle around them. They can now be saved and reused in other rules. Use Advanced – Call Processing Rule action to reuse the rule.

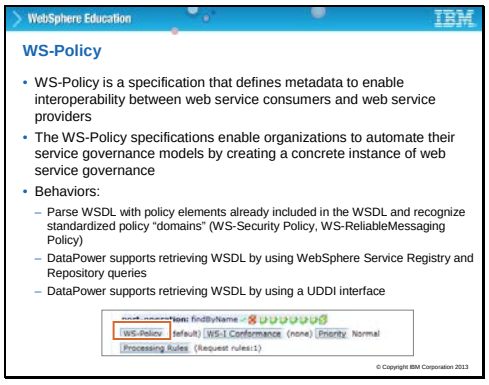
Slide 27



Advanced Web service proxy configuration

More options are available for advanced web services proxy configuration:
Proxy Settings: web service proxy type, Security settings (AAA, cryptographic key), SOAP Action Policy, XML manager.
Advanced Proxy Settings: HTTP connection settings.
Headers/Params: Adds or removes HTTP headers and passes style sheet parameters.
WS-Addressing: Indicates support for WS-Addressing for front-end or back-end.
XML Threat Protection: Provides protection against XML threats.

Slide 28



WS-Policy

WS-Policy is a specification that defines metadata to enable interoperability between web service consumers and web service providers

The WS-Policy specifications enable organizations to automate their service governance models by creating a concrete instance of web service governance

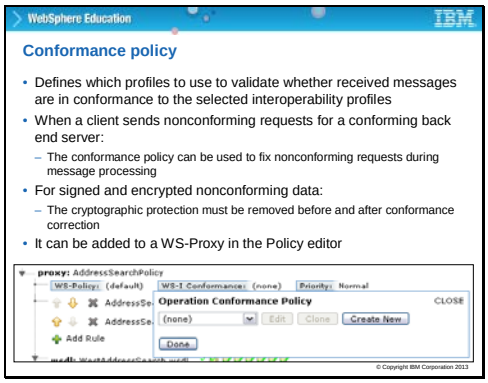
"New Behaviors" refers to features added when version 3.7 of the firmware was released. Here are three new behaviors:

Parse WSDL with policy elements already included in the WSDL and recognize standardized policy "domains". Policy domains are not related to the DataPower use of the word "domain".

Policy domains include WS-Security Policy and WS-ReliableMessaging Policy.

DataPower supports retrieving WSDL by using WebSphere Service Registry and Repository queries and by using a UDDI interface.

Slide 29

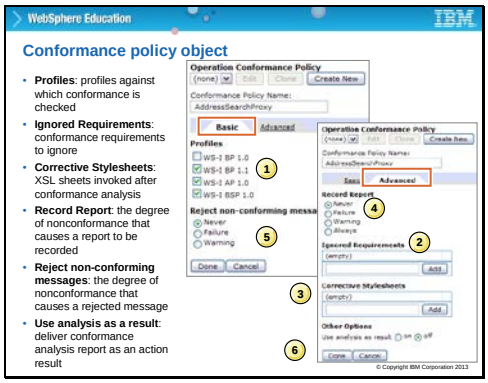


Conformance policy

The conformance policy defines which profiles are used to validate whether received messages are in conformance to the selected profiles. When a client sends non-conforming requests for a conforming back-end server, the conformance policy can be used to fix non-conforming requests during message processing. For signed and encrypted non-conforming data, the cryptographic protection must be removed before any conformance correction.

Any conformance correction must be coded in a style sheet that you create: it is not automatically provided by the appliance. It can be added to a WS-Proxy in the Policy editor.

Slide 30



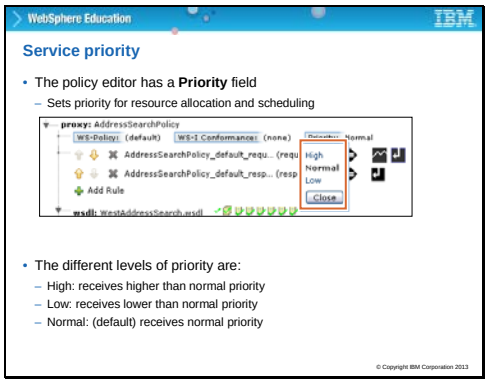
Conformance policy object

Here are some of the parameters that can be set in the Conformance Policy Object:

- Profiles against which conformance is checked.
- Conformance requirements to ignore.
- Corrective XSL Style sheets to be invoked after conformance analysis.

The degree of non-conformance that causes a report to be recorded.
The degree of non-conformance causing a rejected message.
Deliver conformance analysis report as an action result.

Slide 31

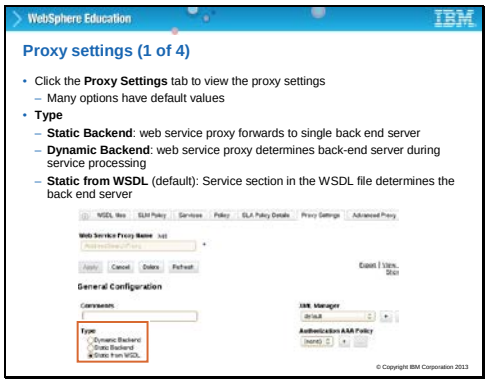


Service priority

The WS-Proxy Policy editor has a Priority field

You can set the priority for resource allocation and scheduling too High, Low, or Normal.

Slide 32



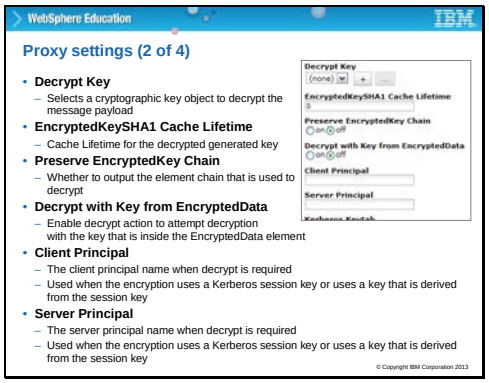
Proxy settings (1 of 4)

Click the Proxy Settings tab to view the proxy settings. Many options have default values.

Some that you might want to set are:

- Static Backend: Web service proxy forwards to single back-end server.
- Dynamic Backend: The web service proxy determines back-end server during document processing.
- Static from WSDL (default): The back-end server is determined by service section in the WSDL file.

Slide 33

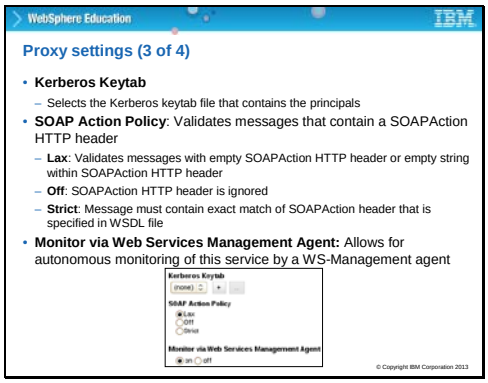


Proxy settings (2 of 4)

Continuing with Proxy settings:

- Decrypt Key: Selects a cryptographic key object to decrypt the message payload.
- Client Principal: The client principal name when decrypt is required. Used when the encryption uses a Kerberos session key or uses a key that was derived from the session key.
- Server Principal: The server principal name when decrypt is required. Used when the encryption uses a Kerberos session key or uses a key that was derived from the session key.

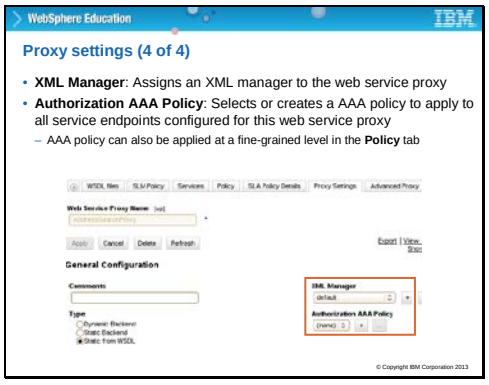
Slide 34



Proxy settings (3 of 4)

Continuing with the Proxy Settings...
Kerberos Keytab: Selects the Kerberos keytab file that contains the principals.
SOAP Action Policy: Validates messages that contain a SOAPAction HTTP header – three settings:
- Lax: Validates messages with empty SOAPAction HTTP header or empty string within SOAPAction HTTP header
- Off: SOAPAction HTTP header is ignored
- Strict: Message must contain exact match of SOAPAction header that is provided in WSDL file

Slide 35

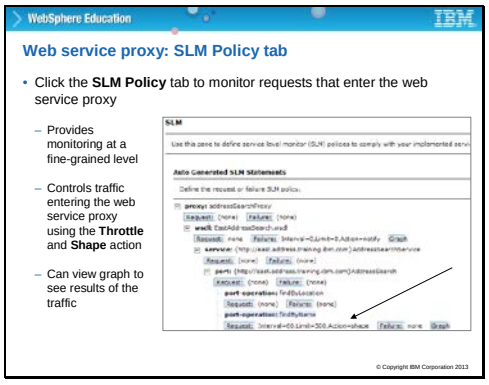


Proxy settings (4 of 4)

Final Proxy Settings:

- XML Manager: Assigns an XML manager to the web service proxy.
- AAA Policy: Selects or creates a AAA policy to apply to all service endpoints configured for this web service proxy.
- AAA policy can also be applied at a fine-grained level in the Policy tab.

Slide 36



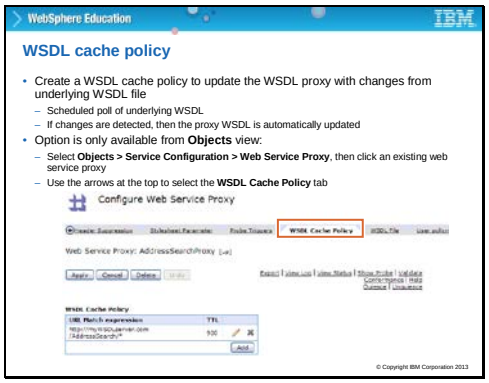
Web service proxy SLM

Service Level Monitoring allows you to control data traffic rates and take action if it exceeds certain thresholds.

Click the SLM tab to monitor requests that enter the web service proxy. It provides monitoring at a fine-grained level, and controls traffic that enter the web service proxy by using the Throttle and Shape action. You can view a graph to see results of the traffic.

Traffic shaping is covered in more detail during the Monitoring lecture later.

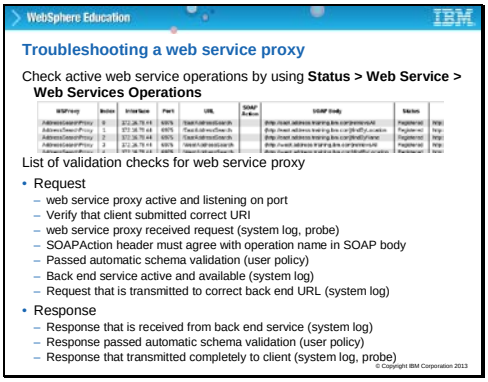
Slide 37



WSDL cache policy

WSDLs can be dynamically updated within the WSP. To configure the WSP, create a WSDL cache policy to update the WSDL proxy with changes from the underlying WSDL file. You set up a scheduled poll of the underlying WSDL, and then if changes are detected, the proxy WSDL is automatically updated. This option is only available from the vertical navigation bar: select **OBJECTS > Service Configuration > Web Service Proxy** and then click an existing web service proxy. Use the arrows at the top to select the WSDL Cache Policy tab.

Slide 38

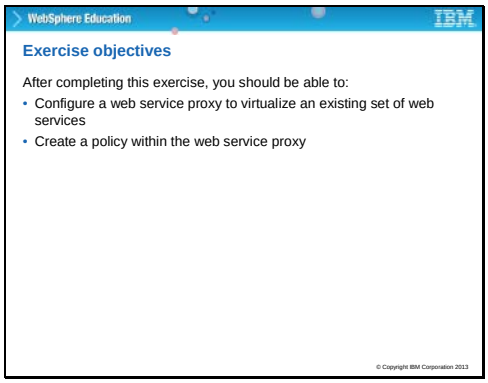


Troubleshooting web service proxy

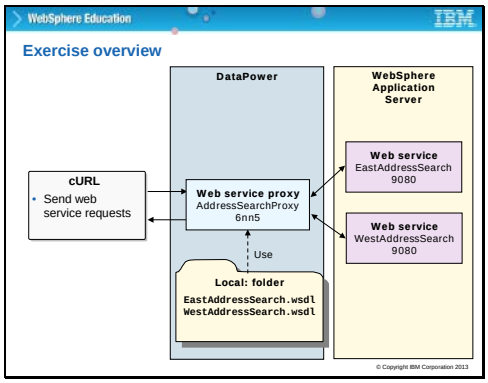
Some things to look at when troubleshooting a Web Service Proxy:
Check active web service operations by using STATUS > Web Service > Web Services Operations.
To check on a Request:
- Make sure that web service proxy is active and listening on the correct port
- Verify that the client submitted the correct URI
- Check that the web service proxy received the request
- Make sure the SOAPAction header agrees with the operation name in the SOAP body
- Make sure that the message passed automatic schema validation in the user policy
- Check that the back-end service is active and available
- Ensure that the request is being transmitted to the correct back-end URL

To check on a Response:
- Make sure that the Response was received from the back-end service
- Make sure that the Response passed automatic schema validation as defined in the user policy
- Make sure that the Response was transmitted completely to the client

Slide 43


WebSphere Education
IBM
Exercise objectives
After completing this exercise, you should be able to:
• Configure a web service proxy to virtualize an existing set of web services
• Create a policy within the web service proxy
© Copyright IBM Corporation 2013

Slide 44


WebSphere Education
IBM
Exercise overview
DataPower
WebSphere Application Server
cURL
• Send web service requests
Web service proxy
AddressSearchProxy
6nn5
Use
Local: folder
EastAddressSearch.wsdl
WestAddressSearch.wsdl
Web service
EastAddressSearch
9080
Web service
WestAddressSearch
9080
© Copyright IBM Corporation 2013