


Slide 1

WebSphere Education

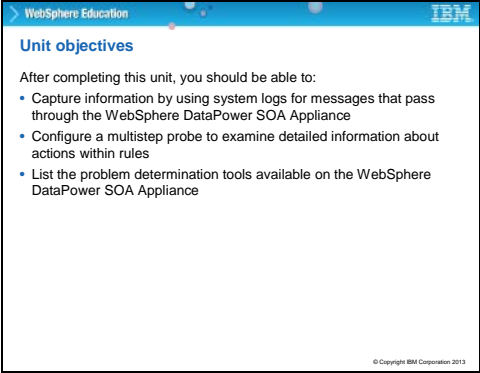
IBM

**Problem determination
tools**



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

Slide 2



WebSphere Education

Unit objectives

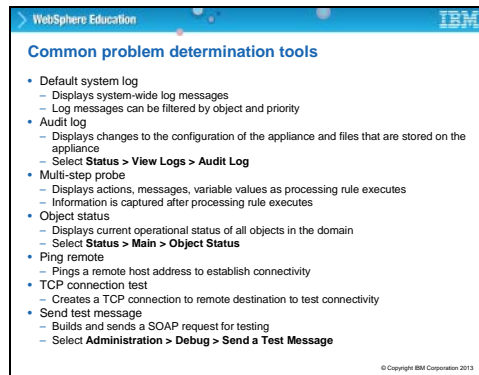
After completing this unit, you should be able to:

- Capture information by using system logs for messages that pass through the WebSphere DataPower SOA Appliance
- Configure a multistep probe to examine detailed information about actions within rules
- List the problem determination tools available on the WebSphere DataPower SOA Appliance

© Copyright IBM Corporation 2013

Unit overview

This unit teaches how to use the troubleshooting tools available for debugging problems on the DataPower appliance.



Common problem determination tools

Here is a general list of the tools available. Some that were already covered, others are reviewed in this unit.

The default system log was covered in the previous unit. You can look either at the log for the entire system (the default system log), or you can filter the information by type of object and priority of the logged message. The audit log holds information about changes to the configuration of DataPower and its on-board files. Both of these logs are useful for seeing general information about the system and its services. The multi-step probe is much more specific. You enable it for a specific service, or, more precisely, for a process on a service. It records information from the execution of the rules of the process. As you can imagine, a processor-intensive activity, and so it is suggested that you enable it only when you need it, and you disable it as soon as you have the information you require.

Object status can be viewed for all objects that are created in a domain. You can open this view from the left navigation bar and searching for Object Status from the Main subcategory of the Status option.

The last three options are aimed at testing connectivity between DataPower and a remote system. You can ping the system, create a TCP connection to it, or even send a SOAP message and check the reply.

Slide 5

WebSphere Education

Appliance status information

- File system information
 - Displays available encrypted, unencrypted, and temporary space for file storage
 - Status > System > Filesystem information
- CPU usage
 - Displays percentage of CPU usage
 - Status > System > CPU Usage
- System usage
 - Displays load and work queue status
 - Status > System > System Usage

Free Encrypted Space	8	Mbytes
Total Encrypted Space	233	Mbytes
Free Temporary Space	223	Mbytes
Total Temporary Space	242	Mbytes
Free Internal Space	241	Mbytes
Total Internal Space	242	Mbytes

10 sec	4	%
1 min	25	%
10 min	25	%
1 hour	25	%
1 day	25	%

Task ID	Task Name	Load (%)	Work List	CPU (%)	Memory (%)	File Count
1	FWT	1	0	2	1	25

© Copyright IBM Corporation 2013

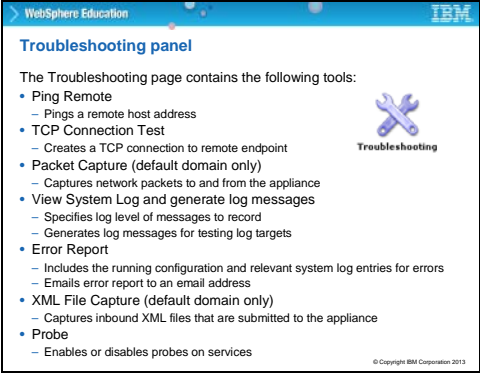
Appliance status information

Take a closer look at some of the options available for getting information about an appliance. Remember that the first drawer of the navigation panel is the status bar. You can open up and get these different options.

The first on this slide gives the information about the space available in the on-board file system. The three types of space that are listed are for encrypted information, unencrypted, or just 'internal' information or space. And temporary space, the space that is reserved for information that are deleted if the appliance is rebooted.

CPU usage is straightforward; you can see average loads over five different intervals, from a minimum 10 seconds up to the full day. Finally, there is a percentage indication of the load on the box during the specified time period, which is typically one second.

Slide 6



WebSphere Education

Troubleshooting panel

The Troubleshooting page contains the following tools:

- Ping Remote
 - Pings a remote host address
- TCP Connection Test
 - Creates a TCP connection to remote endpoint
- Packet Capture (default domain only)
 - Captures network packets to and from the appliance
- View System Log and generate log messages
 - Specifies log level of messages to record
 - Generates log messages for testing log targets
- Error Report
 - Includes the running configuration and relevant system log entries for errors
 - Emails error report to an email address
- XML File Capture (default domain only)
 - Captures inbound XML files that are submitted to the appliance
- Probe
 - Enables or disables probes on services

Troubleshooting

© Copyright IBM Corporation 2013

Troubleshooting panel

From the control panel page, you can see the troubleshooting icon, which is shown on this slide. The panel gives access to a number of tools, ranging from a simple ping of a remote system to a full-scale probe on a service. Each of the tools that is shown on this page is covered in more detail on the following slides.

Slide 7


WebSphere Education

IBM

Troubleshooting panel

The Troubleshooting page contains the following tools:

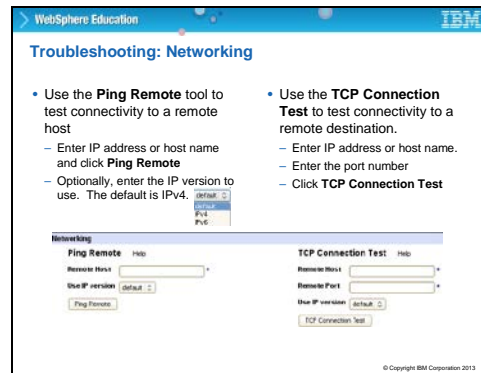
- Networking
 - Ping Remote
 - TCP Connection Test
- Packet Capture (default domain only)
 - Start Packet Capture
 - Stop Packet Capture
- Logging
 - Set Log Level
 - Generate Log Event
- Reporting
 - Generate Error Report
 - Send Error Report
- Advanced
 - XML File Capture (default domain only)
 - View Running Config



Troubleshooting

© Copyright IBM Corporation 2013

Slide 8



Troubleshooting: Network connectivity

Here is a look at the "Ping Remote" troubleshooting utility. Ping is for network connectivity. You can put an IP address in here, or even a server name or an alias. You can ping remote servers, but you cannot ping the DataPower appliance from a desktop on a local computer. The inability to ping is implemented for the simple reason that the Aventail firewall that you are going through to get the connectivity blocks pings!

There is a TCP connection test panel to the right of the ping tool. Like with the ping tool, you can put in an IP address or a server name, but also you can specify the port that you want to connect to. When you click TCP Connection Test, you get a dialog that tells you whether the connection was successfully created or not. This one is not blocked because it is not a simple ping but an actual connection request that is sent. The process is a common thing to use to make sure that you can get from the DataPower appliance to the back-end servers, and that a particular port is active and responding. You can try the process in the exercise environment. You give the remote host alias of "WSserver" and the port 9080, and you should see that the back-end server responds correctly. Network connectivity tools are handy that get used often!

Slide 9

WebSphere Education

IBM

Troubleshooting: Packet capture

- Available in default domain only
- Captures the IP packets sent to and from the appliance
 - Captures full network-level exchange between the appliance and other endpoints
 - Captured in **pcap** format
 - Tools such as **Wireshark** can be used to view the traffic in detail
- Useful when troubleshooting network connectivity, TCP sequencing, or other network-level problems
- The packet capture file is available from the **temporary:** directory

Packet Capture

Start Packet Capture

Stop Packet Capture

Interface Type

Interface

Start

Stop

Maximum Duration

Maximum Size

Maximum Packet Size

Filter Expression

Start Packet Capture

Interface Type

Interface

Start

Stop

Maximum Duration

Maximum Size

Maximum Packet Size

Filter Expression

Stop Packet Capture

© Copyright IBM Corporation 2013

Troubleshooting: Packet capture

Packet capture is only available in the default domain. One does not see packet capture if logged in to a domain other than default. It captures IP packets, working at network level, looking at the exchange of packet information between the appliance and whatever is at the other end. A packet is composed of a small portion of your data. This portion of data is included with the address you are sending to, your own address, the total number of packets that are involved in this message, and the number of this particular packet. The capture is in pcap format, which is a packet capture data format that is used by Ethereal, or Wireshark. You can define a specific interface on the appliance. Define timing for the capture or a maximum size, and capture the information to a file on the temporary directory.

WebSphere Education

Troubleshooting: Logging

- Use **Set Log Level** to set the log level for the current domain.
- The **Generate Log Event** to verify that log targets are active and able to capture events.

Logging

Set Log Level Help

[View System Logs](#)

Log Level: debug

Enable Internal Logging: ☒ on ☐ off

Enable IBM Debug Logging: ☒ on ☐ off

Global IP Address Log Filter:

[Set Log Level](#)

Generate Log Event Help

Log Category: java

Log Level: notice

Log Message:

Event Code: Default Code

[Generate Log Event](#)

© Copyright IBM Corporation 2013


Troubleshooting: Enable Internal Logging:

Enable internal logging to troubleshoot failing requests through the XML management interface. Internal logging provides detailed error messages for requests that are submitted to the XML management interface. When enabled, the system log in the default domain contains debug-level messages in the WebGUIi category. The system log is available only in the default domain.

WebSphere Education
IBM

Troubleshooting: System log

- Displays system-wide log messages that are generated by the appliance
 - Click the **View Logs** icon in the Control Panel
 - In the Troubleshooting panel, scroll down to the Logging section
 - Click **View System Logs**
- By default, log messages are only captured with severity of notice or greater
 - Log levels are hierarchical
 - Highest severity (emergency) is at the top of the list
 - Each level captures messages at or above the current level
 - To enhance troubleshooting, set the log level to debug
 - Lowest severity (debug) captures the most information


View Logs

debug
emergency
alert
critical
error
warning
notice
info
debug

Debug-Level Logging is enabled, which impacts performance. [Manage debug settings](#)

Troubleshooting Panel

© Copyright IBM Corporation 2013

Troubleshooting: System log

The system log shows the different message that is generated by the different objects that are running on the appliance. Log targets are covered in the second half of this presentation. Review the different logging levels that are available.

The image at the lower left of the slide shows these different levels of logging. The most detailed level is *debug*, and the most severe is *emergency* (which, hopefully, you never see in a production environment). Each level records the messages that are generated at that level, plus any that had a higher severity level. The default level is *notice*, which captures warning information, and error information, continuing up to emergency. Logging data is already a fair bit of information to be processing, but if necessary you can increase the detail by specifying *info* or even *debug*. With this quantity of logging going on, performance starts to suffer. So if you enable the lowest level, you get a warning that debug level that logs is being used and that it impacts performance. Obviously, debug is a good level for detailed debugging of problems, but you would not want to leave the appliance set to this level for long!

Slide 12

WebSphere Education

Filtering system log

- In the default domain, the system log shows all log entries
 - In non-default domains, log entries are only shown for the objects in that domain
- Filter the system log by:
 - Log target
 - Domain (shown only in the default domain)
 - DataPower objects (xmlfirewall, ws-proxy, and more)
 - Log level type (debug, info, and more)

The screenshot shows the 'System Log' window with a filter bar at the top. The filter bar includes a 'Target' dropdown set to 'defaultlog', a 'Filter' dropdown set to '(none)', and a 'Log level' dropdown set to 'error'. Below the filter bar, there is a table of log entries. The table has columns for 'Time', 'Category', 'Level', 'Direction', 'Status', 'Target', and 'Message'. The log entries are displayed in reverse chronological order, with the most recent at the top.

Time	Category	Level	Direction	Status	Target	Message
03/30/07 10:02	System Log	error	out	error	defaultlog	...
03/30/07 10:02	System Log	error	out	error	defaultlog	...
03/30/07 10:02	System Log	error	out	error	defaultlog	...
03/30/07 10:02	System Log	error	out	error	defaultlog	...
03/30/07 10:02	System Log	error	out	error	defaultlog	...


Filtering system log

Log entries can be extensive, so they can be filtered in a few different ways. First, in any domain that is not the default, you get the message generated for the objects of that domain. Default domain logging is what you would want because you would have no interest in or use for the messages that are created for another domains objects. In fact, if you are in the default domain, you might still desire to see entries for one specific domain. You can therefore filter the system log messages by domain from the default domain. In any domain, you can filter message in two other ways also. You can choose which object you want to examine, or ask to see message of a certain level and above. You can mix and match these two filters, and define a view of error messages for an XML firewall, for example. Messages are displayed in reverse chronological order, the most recent being at the top of the list.

WebSphere Education

Troubleshooting: Generate Log Event

- Use the **Generate Log Event** tool to test whether:
 - Log messages are generated in appropriate log target on the appliance (default system log captures all log messages)
 - Log messages are sent to remote host when off-box logging is used
- Configure log messages with:
 - Log Type: object class or category
 - Log Level: debug, info, and more
 - Log Message: string inside log message
 - Event Code: for generating an event code-based message



© Copyright IBM Corporation 2013

Troubleshooting: Generate Log Event

This interesting little option can be found just to the right of the view system log. You can say what type of object is attached to this message. For example, an XML firewall object – you can decide on what minimum severity level you are interested in addressing. You can add a text message to the event log, and you can add an event code to identify what event occurred. You then click Generate Log Event and go to look in the log file to see whether the message actually arrives. The point is to create logs that capture specific information about specific events.

Slide 14

WebSphere Education

Troubleshooting: Reporting

- Generate Error Report
 - Error report is required when engaging with IBM DataPower support
 - Error report file is created in the temporary directory
- Error Report contains:
 - Current configuration
 - Current contents of the system log
 - Contents of CLI log
- Send Error Report:
 - DataPower uses an external mail server (SMTP) to email the error report to a specific email recipient.

Reporting

Generate Error Report Help

No Error Report Available for Viewing

[Generate Error Report](#)

Send Error Report Help

SMTP Server

Location

Email Address

Email Sender Address

[Send Error Report](#)

© Copyright IBM Corporation 2013

Click **Generate Error Report**. A dialog window asks for confirmation and indicates the location of the resulting file.

If an error report is available, an icon is shown that allows immediate access to the file.

Slide 15

The screenshot shows the 'WebSphere Education' interface with the title 'Troubleshooting: Advanced'. It contains two bullet points: 'Use XML File Capture to allow the configuration of system-wide file-capture mode. - The file capture facilitates the visibility of erroneous XML and XSLT content.' and 'Use View Running Config to view the configuration of all the objects that are currently in memory.' Below the text is a screenshot of the 'Advanced' section of the WebSphere Administration Console. It features two tabs: 'XML File Capture' and 'View Running Config'. The 'XML File Capture' tab is active, showing a 'View File Capture' link, a 'Mode' dropdown set to 'Ignore', and an 'XML File Capture' button. The 'View Running Config' tab is also visible with a 'View Running Config' link. The IBM logo is in the top right corner, and the copyright notice '© Copyright IBM Corporation 2013' is at the bottom right.

WebSphere Education

Troubleshooting: Advanced

- Use XML File Capture to allow the configuration of system-wide file-capture mode.
 - The file capture facilitates the visibility of erroneous XML and XSLT content.
- Use **View Running Config** to view the configuration of all the objects that are currently in memory.

Advanced

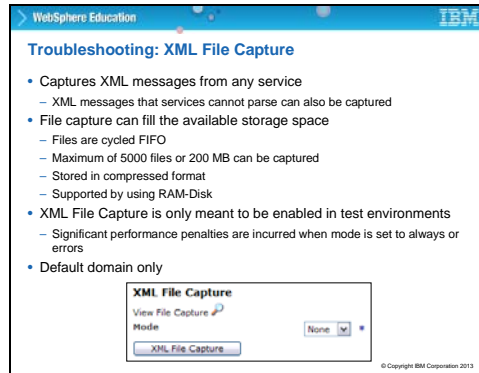
XML File Capture View File Capture Mode: Ignore XML File Capture

View Running Config View Running Config

© Copyright IBM Corporation 2013

Troubleshooting: Advanced

The advanced section of troubleshooting includes activation for XML file capture and view that runs config.



The slide is titled "WebSphere Education" and "Troubleshooting: XML File Capture". It contains a bulleted list of information about XML File Capture:

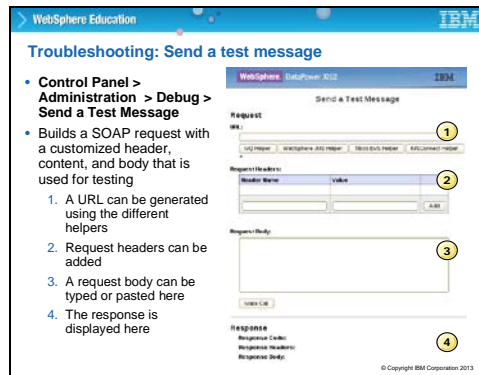
- Captures XML messages from any service
 - XML messages that services cannot parse can also be captured
- File capture can fill the available storage space
 - Files are cycled FIFO
 - Maximum of 5000 files or 200 MB can be captured
 - Stored in compressed format
 - Supported by using RAM-Disk
- XML File Capture is only meant to be enabled in test environments
 - Significant performance penalties are incurred when mode is set to always or errors
- Default domain only

Below the list is a small screenshot of the "XML File Capture" configuration window. It shows a "View File Capture" link, a "Mode" dropdown menu currently set to "None", and an "XML File Capture" button. The IBM logo is in the top right corner, and the copyright notice "© Copyright IBM Corporation 2013" is in the bottom right corner.

Troubleshooting: XML File Capture

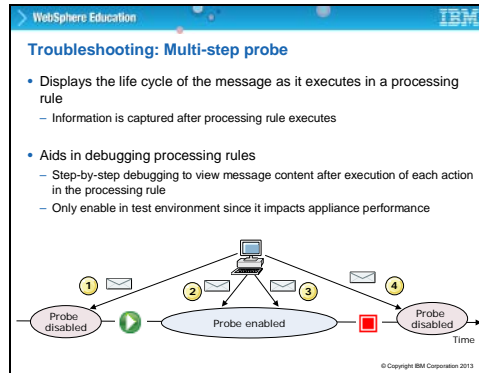
The XML file capture option captures entire messages, rather packets of information. It captures messages that have formatting problems and that cannot therefore be parsed by a service. You would use this tool if you were sending in an XML file that you thought is well-formed, but it never gets to the policy; it gets rejected. With XML file capture, you can examine the actual form of the message that comes in to the service.

One thing to note with this tool is that it can fill the available memory for XML file storage. If so, then the first file that is captured is the first to be deleted. In other words, your latest files always are captured, potentially at the expense of earlier captured files. In fact, you might not reach this limit. You have 200 megabytes of space to fill up, or you can capture 5,000 files, whichever comes first! One must be in the default domain to use this tool.



Troubleshooting: Send a test message

"Send a test message" is similar to a curl command. You can type the destination URL, or if you require help on setting it up you can click the appropriate button just under the URL field. You do not see these buttons unless you have a license for WebSphere MQ, or Tibco, and the others. You might want to add some header information, and you can add the request body. When you click "Make Call" the SOAP message is fired off to the destination URL designated, and the response is eventually displayed at the bottom of the test message dialog. The only drawback with this test message is that you cannot recall the setup in the same way you can with a curl command prompt message. So your request body information is typed in each time, as opposed to pointing to a file for the information.



Troubleshooting: Multistep probe

The multistep probe, often called 'probe', is probably one of the most useful tools in the troubleshooting area, and also one of the most costly in terms of processing power. This one captures state at each step of the execution of a rule. You cannot see state at the moment it is generated, but you can examine the probe results for every stage of the policy rule after execution. Typically, enable the probe. Next, run a process. Then, disable the probe. And finally, examine the information.

Slide 19

WebSphere Education

Troubleshooting: Enabling the multi-step probe

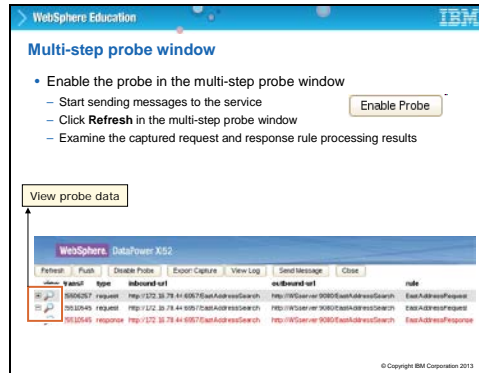
Two ways to enable a probe for a service:

- Select the **Debug Probe** tab in the Troubleshooting panel
 - Use the **Add Probe** button to add a multi-step probe for that service
- On the service configuration page, click the **Show Probe** button
 - Enable the probe inside the multi-step probe window

The screenshot shows the WebSphere Education interface. At the top, there's a blue header with 'WebSphere Education' and the IBM logo. Below the header, the title 'Troubleshooting: Enabling the multi-step probe' is displayed. The main content area is divided into two sections. The top section, 'Multi-Protocol Gateway', has a 'Debug Probe' tab selected. It contains a table with columns 'Name', 'Op State', 'Probe', and 'Disable Probe'. Below the table is an 'Add Probe' button. The bottom section, 'Web Service Proxy', also has a similar table and an 'Add Probe' button. On the right side of the interface, there's a 'Configure Multi-Protocol Gateway' window. It has tabs for 'General', 'Advanced', 'Troubleshooting', 'Status', 'Monitor', 'WS-Addressing', 'WS-ReliableMessaging', and 'WS-Security'. The 'Troubleshooting' tab is selected, and it shows a 'Show Probe' button. The 'Show Probe' button is highlighted with a red box. At the bottom right, there's a copyright notice: '© Copyright IBM Corporation 2013'.

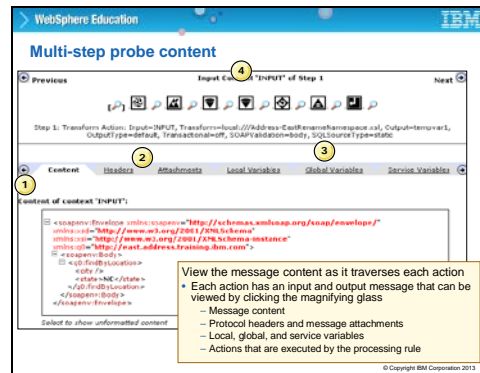
Troubleshooting: Enabling the multistep probe

The 'Show Probe' link is on the main page of a service (on the lower screen capture on the slide). You can also open the troubleshooting icon from the control panel, and switch to the 'Debug Probe' page. A complete list of services is shown, and you can activate a probe for whichever service you want to debug.



Multistep probe window

When you click the 'Show Probe' link, you get a dialog where you can enable the probe. When enabled, the button name changes to 'Disable Probe'. After running a service you click the Refresh button to update the list of messages. If you see a message in red, you know that there was an error in the execution. To view the data, you click the magnifying glass icon. You might notice that the second line of probe data says 'error', but it is not in red. The rule is not red because the rule ran perfectly correctly; it was an error rule. The first line was a request direction rule, and something went wrong during its execution.

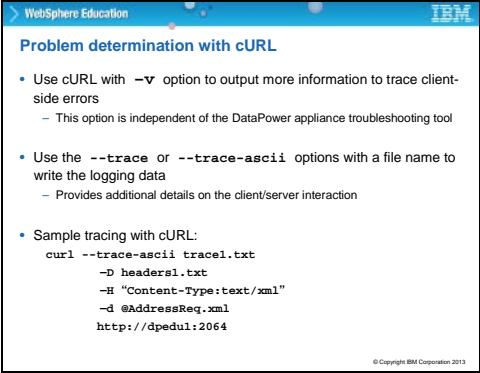


Multistep probe content

The screen capture is what you see when you view the probe data. The content tab shows the input context; in other words, the data that is passed into the rule by the match action. You can switch tabs to view the header information, or any attachments to the file, or the state of different variables. 'Service Variables' is probably one of the more important ones here; service variables show that you debug information and routing information, and other information.

The section at the top of the view shows the different actions that comprise the rule. The square braces around the first magnifying glass show that what you are examining in the lower portion of the screen. You can step through either by clicking the magnifying glass next to the action you are interested in, or by clicking the next and previous buttons at the top of the screen. You can see that this rule is composed of a transform action, a validate action, two filters, a header rewrite, a set variable action and a results action.

Notice that the one action that is not shown in the list of actions is the match action, the first one in the rule. Why would this action not be shown? Because, you would not get into the rule if there were no match! The fact that you are looking at the sequence of actions shows that the match was successful.



WebSphere Education

Problem determination with cURL

- Use cURL with `-v` option to output more information to trace client-side errors
 - This option is independent of the DataPower appliance troubleshooting tool
- Use the `--trace` or `--trace-ascii` options with a file name to write the logging data
 - Provides additional details on the client/server interaction
- Sample tracing with cURL:

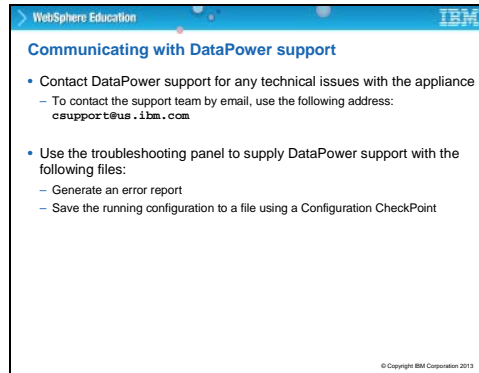
```
curl --trace-ascii trace1.txt
-D headers1.txt
-H "Content-Type:text/xml"
-d @AddressReq.xml
http://dpdul:2064
```

© Copyright IBM Corporation 2013

Problem determination with cURL

The dash-v option on cURL means 'verbose'. It does not do anything on the appliance, but it provides more information as to what is happening between the command prompt and DataPower. You might find that the `-v` option is useful if you are doing, for example, SSL communication and something is not working correctly. Another option is to capture trace information to a file. For tracing, you would use dash-dash trace dash ASCII followed by the name of the file where you want the information written. Note the initial double trace! You often see this method with cURL commands. Do not forget to put dash-dash.

The example at the bottom of the screen shows the trace that is directed to a file called trace1.txt. Uppercase 'D' is used to indicate that you want to write the protocol headers to the file headers.txt. The lowercase 'd' indicates the source data that should be posted to this particular destination.

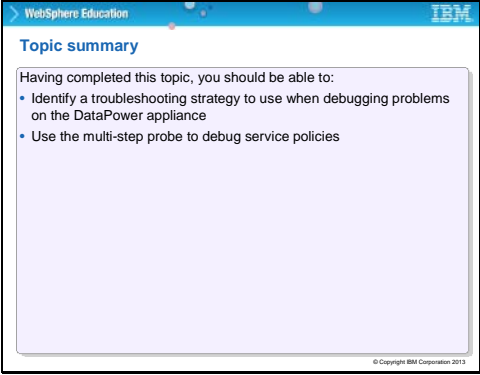


Communicating with DataPower support

You need at least a file to send to DataPower support if things go wrong! In fact, the process that changed somewhat since this slide was written. Now, you can click the control panel link to the display of icons for the services. At the bottom of the screen, you see a small section called "Having trouble?" There are several links available here, and you can start by clicking the link to the WebSphere DataPower Support Site.

You already covered the options on the troubleshooting panel. Remember that there is an option here to generate an error report, and even to send it directly from DataPower without having to copy it out from the temporary storage area.

Slide 24



WebSphere Education

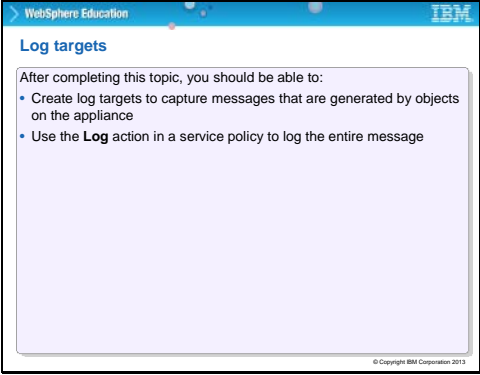
Topic summary

Having completed this topic, you should be able to:

- Identify a troubleshooting strategy to use when debugging problems on the DataPower appliance
- Use the multi-step probe to debug service policies

© Copyright IBM Corporation 2015

This section covers log targets.



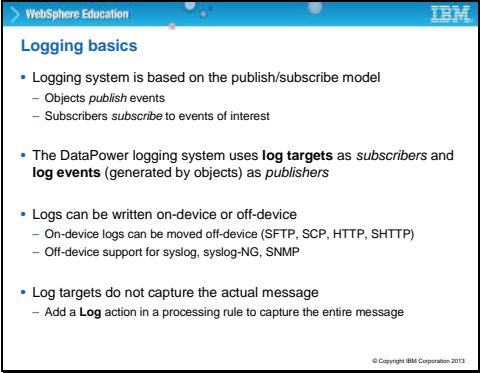
WebSphere Education

Log targets

After completing this topic, you should be able to:

- Create log targets to capture messages that are generated by objects on the appliance
- Use the **Log** action in a service policy to log the entire message

© Copyright IBM Corporation 2015



WebSphere Education

Logging basics

- Logging system is based on the publish/subscribe model
 - Objects *publish* events
 - Subscribers *subscribe* to events of interest
- The DataPower logging system uses **log targets** as *subscribers* and **log events** (generated by objects) as *publishers*
- Logs can be written on-device or off-device
 - On-device logs can be moved off-device (SFTP, SCP, HTTP, SHTTP)
 - Off-device support for syslog, syslog-NG, SNMP
- Log targets do not capture the actual message
 - Add a **Log** action in a processing rule to capture the entire message

© Copyright IBM Corporation 2013

Logging basics

Logging is based on the so-called pub-sub model. As objects ran on the appliance execute, they publish events that detail their state and their execution. A subscriber then indicates an interest in the event by subscribing to that event on that object. Log targets are the subscribers. They are the files that the logging system uses to record the events. Typically, the actual message is not written out to a log target. To record the message, you should use an action on the rule that is called a log action.

WebSphere Education

Available log levels

List of log levels for the system log:

- Emergency: system is unusable
- Alert: take immediate action
- Critical: critical condition
- Error: an error occurred
 - The error code is included
- Warning: a warning condition occurred
 - Nothing might be wrong, but conditions indicate that a problem might occur soon if nothing changes
- Notice: a normal but significant condition applies
- Info: an informational message only
- Debug: debug-level messages
 - This level generates numerous messages

Set Log Level

View System Logs

Log Level: debug +

Enable Internal Logging: off

Enable RSH Debug: off

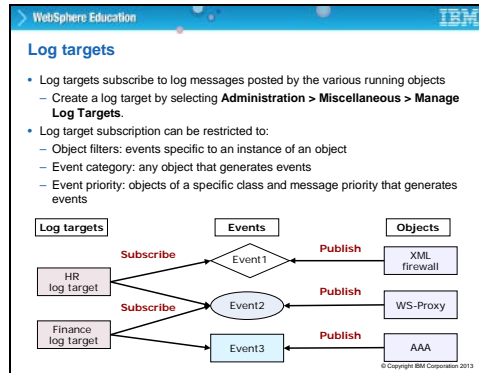
Set Log Level

Log Levels: emergency, alert, critical, error, warning, notice, information, debug

© Copyright IBM Corporation 2013

Available log levels

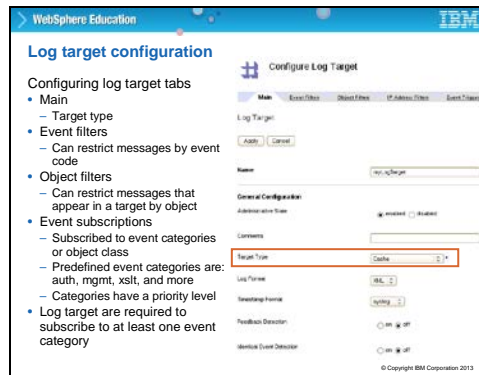
Now is a good moment to review the log levels that are available. You set the level in the troubleshooting panel. The most severe is 'emergency', where a message gets written out just before the box dies. After an emergency message, the system cannot be used. Alert informs you that if you do not take immediate action, an emergency follows fast! As you go down the list, the urgency of the log diminishes. Notice says that there is some condition that has significance, but that is anyway normal and so does not require any particular action taken. Below that point, the number of messages increases significantly, with information that tells you that everything is going well, and debug telling you the low-level details about how well everything is going. You should use debug to do exactly that: to debug some rule. It entails a considerable performance hit, and DataPower even gives you warnings that the log level is set to debug and that you should raise it as soon as possible.



Log targets

Here is an opportunity to revisit log targets and see the relationship between targets, events, and objects with a diagram.

You can create your own log target and provide it with the information about which events it should listen to, and also what log level you want it to react to. As seen, the log target then becomes the subscriber, listening for an event is published. The objects that run on DataPower generate these events whether a target subscribed or not.



Log target configuration

Here is how the log target is configured. Each of the tabs (event filters, object filters, and event subscriptions) is described on the following slides.

On the Main tab, you give the log a name and decide what target type you want (covered on the next slide). What the format of the log is going to be, how large you want the file to be, and so on. Depending on what target type you chose, the rest of the page repaints to add different options.

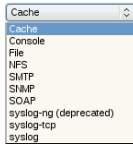
Archive mode allows you to back up the file. When the first file reaches the maximum size is indicated (in this case, half a megabyte) it is archived and a new file is started. When that one reaches the maximum size it also is archived, and so on, until the number of files reaches the number of 'rotations' specified. The first file is dropped, then the second, and so on.

If you set 'Identical Event Detection' to 'on', the repeat events are not logged for a specified amount of time (by default, 10 seconds). The time delay avoids having the log filled with hundreds of repeated identical messages.

WebSphere Education

Ten-log target types

- A **Target Type** field of a log target supports the following values
 - **Cache**: writes log entries to system memory
 - **Console**: writes log entries to a Telnet, SSH, or CLI screen
 - **File**: writes log entries to a file on the device flash
 - **NFS**: writes log entries to a file on a remote NFS server
 - **SMTP**: forwards log entries as email to configured addresses
 - **SNMP**: forwards log entries as SNMP traps
 - **SOAP**: forwards log entries as SOAP messages
 - **Syslog**: forwards log entries to a remote syslog daemon
 - **syslog-ng**: depreciated. Use syslog-tcp.
 - **syslog-tcp**: forwards log entries by using TCP to a remote syslog daemon. The local address, remote address, remote port, syslog facility can be set. An SSL connection to the syslog host can be created. The processing rate can be limited.



© Copyright IBM Corporation 2013

10-log target types

There are 10 options for the log target type. You can cache the login system memory. Write the cache directly to a screen for viewing, or create a log. The other six options write the log to some remote point, such as an NFS server. Or create a SOAP message with the log information, or even create an email and forward it to a configured address.

WebSphere Education

Event filters

- In the "Configure Log Target" web page, select the **Event Filters** tab
- Event filters create filters for a log target that is based on **event codes**
 - Use the **Event Subscription Filter** to subscribe to specific event codes

Event Code	Category	Severity	Message
SWI100001	about	error	Time zone config mismatch
SWI100001	crypto	alert	Cryptic accelerator not supported by this node
SWI100002	crypto	critical	node is unbalanced
SWI100003	crypto	critical	node PID log-in failed
SWI100004	crypto	critical	node PID log-out failed
SWI100005	crypto	alert	Microcode file not found
SWI100006	crypto	alert	Microcode load failed
SWI100007	crypto	alert	VMIO controller not found

Event Filters

Log Target

Apply Cancel

Event Subscription Filter (empty) Add Filter Select Code

Event Suppression Filter (empty) Add Filter Select Code

- Use the **Event Subscription Filter** to exclude certain event codes from being written to the log target
- Click the **Select Code** buttons to add event codes to **Event Code** value list

© Copyright IBM Corporation 2013

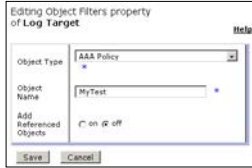
Event filters

The event filters tab allows you to restrict event that logs to specific event types. If you leave the fields blank, you get every event that is generated. There are two ways to process. Either you subscribe to events, or you suppress the recording of events. You can mix and match these two options. There is a select code button that allows you to pick the event codes you are interested in; you do not have to remember the event codes.

WebSphere Education

Object filters

- In the "Configure Log Target" web page, select the **Object Filters** tab
- Object filters allow only those messages that are generated by selected objects to be written to a log target
- It is possible to create a log target that collects log messages for a particular class of objects
 - Example: AAA policy object called MyTest



© Copyright IBM Corporation 2013

Object filters

The objects filter works in a similar way to the event filter. This time, you are restricting messages either to a specific type of object, or even to one object of a specific type. If you want all objects of a certain type, you must put an asterisk into the object name field. You might want to have messages from objects that the one you specified is referencing; you can add those objects by selecting the radio button at the bottom of the dialog.

WebSphere Education

IBM

Event subscriptions

- In the "Configure Log Target" web page, select the **Event Subscriptions** tab
- Log targets subscribe to particular event categories.
- Example event categories:
 - **xmlfirewall**: for XML firewall objects
 - **auth**: authorization
 - **mgmt**: for configuration management events
- A priority level can be specified for each event category that is chosen
 - Additional level of filtering

Adding new Event Subscriptions property of Log Target

Help

Event Category

xmlfirewall

Minimum Event Priority

debug

Save

Cancel

© Copyright IBM Corporation 2013

Event subscriptions

You must subscribe to at least one event for a log target. You choose your category, and also specify the priority that you are interested in. The minimum priority indication, in other words, gets events at this level and all superior levels. With the setting indicated on the screen capture, you would get every event, since debug is the lowest level of event.

Log action

The **Log** action sends the contents of the **Input** context to a destination URL.

- Is used to log entire message instead of creating a log entry
- Configure:
 - **Destination**: must be a valid URL to either a local file or remote destination
 - **Log Type**: log priority
 - **Log Level**: event category

Configure Log Action

Basic | **Advanced**

Input

Input: (auto) (auto)

Options

Log

Destination: (http://) (Var Builder)

Log Level: (notice) *

Log Type: (major) *

Asynchronous: ☐ on ☒ off

Method: (POST) *

Output

Output: (OUTPUT) *

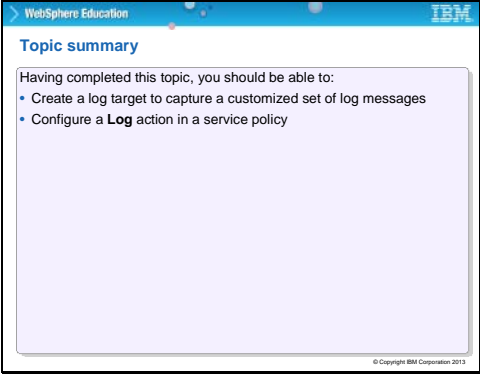
OK Cancel Cancel

© Copyright IBM Corporation 2013

Log action

Remember that you do not get the actual contents of a message when capturing to log targets: just the information about what is happening to the message. If you want the message itself to be logged, you add a log action to a rule on a processing policy. You configure the log action to give it a destination URL, a specific minimum log level and the log type. You would use this action when you needed to have an audit log for some messages.

The log action is one of the advanced actions available for a rule.



WebSphere Education

IBM

Topic summary

Having completed this topic, you should be able to:

- Create a log target to capture a customized set of log messages
- Configure a **Log** action in a service policy

© Copyright IBM Corporation 2013

Slide 36

WebSphere Education

IBM

Unit summary

Having completed this unit, you should be able to:

- Capture information by using system logs for messages that pass through the WebSphere DataPower SOA Appliance
- Configure a multistep probe to examine detailed information about actions within rules
- List the problem determination tools available on the WebSphere DataPower SOA Appliance

© Copyright IBM Corporation 2013

Slide 37

WebSphere Education

IBM

Checkpoint questions

1. True or False: To test a Log Event, one would use the Generate Log Event option in the troubleshooting panel to generate a log message, and verify that it is included or excluded in a log target.
2. A client cannot connect to the XML firewall service. Select the best steps to troubleshoot this problem.
 - A. Check the client URL and Object status (and possibly TCP connection test)
 - B. Ping the DNS to validate the proper XML firewall service. Check the backside connection.
3. Logs can be stored off-device by using (select five):
 - A. SMTP
 - B. SOAP
 - C. NFS
 - D. syslog-ng
 - E. daemon
 - F. syslog
 - G. POP

© Copyright IBM Corporation 2013

WebSphere Education

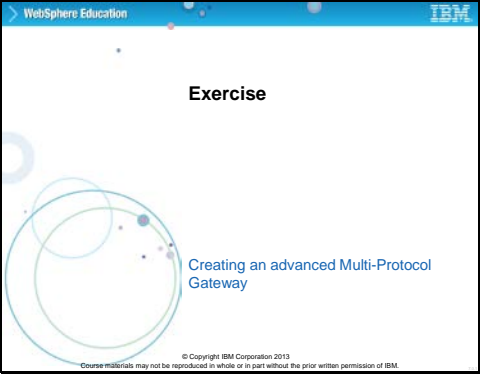
IBM

Checkpoint answers

1. **True.** To test a Log Event, one would use the Generate Log Event option in the troubleshooting panel to generate a log message, and verify that it is included or excluded in a log target.
2. **A.** A client cannot connect to the XML firewall service. Select the best steps to troubleshoot this problem.
 - ✓ **A. Check the client URL and Object status (and possibly TCP connection test)**
 - B.** Ping the DNS to validate the proper XML firewall service. Check the backside connection.
3. **A, B, C, D, and F.** Logs can be stored off-device by using (select five):
 - ✓ **A. SMTP**
 - ✓ **B. SOAP**
 - ✓ **C. NFS**
 - ✓ **D. syslog-ng**
 - E. daemon**
 - ✓ **F. syslog**
 - G. POP**

© Copyright IBM Corporation 2013

Slide 39



WebSphere Education

IBM

Exercise

Creating an advanced Multi-Protocol Gateway

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

WebSphere Education

IBM

Exercise objectives

After completing this exercise, you should be able to:

- Create a multi-protocol gateway from a WSDL definition
- Configure a document processing policy with more actions
- Configure content-based routing by using a Route action
- Test the multi-protocol gateway policy that uses the command-line tool cURL
- Perform basic debugging by using the system log and multistep probe

© Copyright IBM Corporation 2013

Slide 41

