



IBM Support Technical Exchange

Ask the Experts

DataPower® Topics on Appliance Reloads, MQ Integration points, Networking/SSL, FTP, and HTTP Content-Type Manipulation.

10 August 2016



WebSphere® Support Technical Exchange



Agenda

- Introduce the panel of experts
- Introduce DataPower Topics on Appliance Reloads, MQ Integration points, Networking/SSL, FTP, and HTTP Content-Type Manipulation Topics
- Answer questions submitted by email
- Open telephone lines for questions
- Summarize highlights

Panel of Experts

Panelist	Role at IBM and Contact Information
Clarissa Washington	IBM DataPower Level 2 Support Engineer clarisab@us.ibm.com dwAnswer id: clarissab
Dominic Micale	IBM DataPower Level 2 Support Engineer dmmicale@us.ibm.com dwAnswer id: dmmicale
Chin Sahoo	IBM DataPower Level 2 Support Engineer chintam3@us.ibm.com dwAnswer id: chintam3
James Barrett	IBM DataPower Level 2 Support Engineer jtbarret@us.ibm.com dwAnswer id: jim
Trey Williamson	IBM DataPower Level 2 Support Engineer alfredq@us.ibm.com dwAnswer id: trey
Paul Megani	AVL/AVS DataPower megani@us.ibm.com

Introduction

- We will be covering a number of questions that cover various **IBM DataPower** Topics :
 - SSL
 - FTP
 - MQ
 - Reload
 - WebGUI and SSH Access
 - Manipulating the Content-Type header for request and responses
- Platforms covered will include 7.0, 7.1, 7.2 and 7.5

Question 1

How can I quickly assess and gather the key information from an appliance reload?



Quickly handle appliance reload

- Before the reload occurs be sure to have enabled Failure Notification to capture an error report and enable “always on startup”

<https://developer.ibm.com/answers/questions/204407/datapower-best-practices-most-detailed-error-repor.html>

- Check the failure status provider:



Failure Notification

Refresh Status

Date Created	Reason	Upload Status	
20160708154257360EDT	on-shutdown	success	temporary:///ern
20160722092220357EDT	user-requested	success	temporary:///ern
20160727170344793EDT	user-requested	success	temporary:///ern

Quick elimination on reload

- If the Failure Notification reason reports “Throttle” then we know that we need to go back and look over the metrics to see what happened.
- If the reason code is “crash” then IBM support will need to decode the backtraces and piece together a time line of events.
- Be prepared to include latency logs and error level logs leading up to the time of the reload. Support may also request metrics, snmp/csv, some format.
- More importantly did you check the fix release list?

Question 2

How to inject MQ PMO options for response message in DataPower?

MQ PMO option for Response Message

- The MQ Front Side Handler (FSH) does not have Put Message Option (PMO) attribute in its configuration
- In order to add PMO, one has to configure “Result” Action in the response rule and specify the “PMO” tag in the MQ URL configured in the destination box
- Example: `dpmq://DP1-QM/?RequestQueue=QUEUE2;PMO=2052`
- Note: DP1-QM is the mq-qm object configured in the domain, PMO=2052 is used to set MQPMO_SET_IDENTITY_CONTEXT

MQ PMO option for Response Message (continued)

- To inject MQMD header fields related to origin context, one must set the MQPMO_SET_ALL_CONTEXT option.
- For DataPower MQ URL, use PMO=2052, if mq-qm object is not using units-of-work (sync point flow), use PMO=2050 if mq-qm is using units-of-work.
- To inject MQMD header fields related to identity context, one must set the MQPMO_SET_IDENTITY_CONTEXT
- For DataPower MQ URL, use PMO=1028, if mq-qm object is not using units-of-work, use PMO=1026 if mq-qm object is using units-of-work

Question 3

How to inject MQOD headers using Gateway scripts?

MQOD Headers

- Use the following gateway script code snippet in Request Rule to save MQMD.ReplyToQ and MQMD.ReplyToQMgr values

```
var hm = require('header-metadata');  
var requestMQMD = hm.current.get({type: 'mq'}, 'MQMD');  
var ctx1 = session.name('myMQMD') ||  
    session.createContext('myMQMD');  
ctx1.setVariable('RQ', requestMQMD.MQMD.ReplyToQ['$']);  
ctx1.setVariable('RQM', requestMQMD.MQMD.ReplyToQMgr['$']);  
console.debug("Request.MQMD.ReplyToQ   : %s",  
    ctx1.getVariable('RQ'));  
console.debug("Request.MQMD.ReplyToQMgr : %s",  
    ctx1.getVariable('RQM'));
```

MQOD Headers (Continued)

- Define XML MQOD structure and inject in the Response rule to route the message to the destination queue

```
var hm = require('header-metadata');
var ctx1 = session.name('myMQMD') || session.createContext('myMQMD');
console.debug("Response.MQMD.ReplyToQ : %s", ctx1.getVariable('RQ'));
console.debug("Response.MQMD.ReplyToQMgr : %s", ctx1.getVariable('RQM'));

//define the MQOD structure
var xmlMQOD = '<MQOD>' + '<Version>2</Version>' + '<ObjectName>' + ctx1.getVariable('RQ') +
  '</ObjectName>' + '<ObjectQMgrName>' + ctx1.getVariable('RQM') + '</ObjectQMgrName>' +
  '</MQOD>';

//inject MQOD
hm.current.set('MQOD', xmlMQOD);
console.debug("The Response MQOD : %s", xmlMQOD);
```

Question 4

How to inject MQMD headers using Gateway scripts?

MQMD Headers

- Define MQMD structure using Gateway scripts

```
var hm = require('header-metadata');
```

```
var mqmd =
```

```
  '<MQMD>' +
```

```
    '<StructId>MD</StructId>' +
```

```
    '<Format>MQHRF2</Format>' +
```

```
    '<MsgType>1</MsgType>' +
```

```
    '<Persistence>1</Persistence>' +
```

```
    '<ReplyToQ>QUEUE3</ReplyToQ>' +
```

```
  '</MQMD>';
```

MQMD Headers (Continued)

- Define MQRFH2 header and inject MQMD first and then MQRFH2 header second in sequence

```
var mqrh2 =  
  '<MQRFH2>' +  
  '<Version>2</Version>' + '<Format>MQSTR</Format>' +  
  '<NameValueData>' + '<NameValue>' +  
  '<usr>' + '<From>Business Partner1</From>' + '<To>Business Partner2</To>' +  
  '<ChargeBackType>credit</ChargeBackType>' +  
  '</usr>' + '</NameValue>' + '</NameValueData>' +  
  '</MQRFH2>';  
  
//Inject MQMD and MQRFH2 headers  
hm.current.set('MQMD', mqmd);  
hm.current.set('MQRFH2', mqrh2);  
  
//Print MQMD and MQRFH2 headers to system log  
console.debug("The MQMD : %s", mqmd);  
console.debug("The MQRFH2 : %s", mqrh2);
```


Question 5

Why do logins fail to DataPower when WebGUI/SSH is accessible and credentials are valid?

Login Failures

- RBM Settings controls accessibility through SSH, WebGUI, XML-Mgmt, Rest-Mgmt interfaces.
- Should RBM Settings go into a [DOWN] state due to any other referenced object, valid login credentials including the 'admin' user will fail against SSH/WebGUI/XML-Mgmt/Rest-Mgmt
- fallback-login local does not stop this issue.
- When RBM Settings is down the only fallback is to use the admin user in the serial / virtual console.

Login Failures (continued)

- RBM Settings Authentication tab supports LDAP, when using SSL with LDAP you need to assure:
 - ▶ The certificate in the SSL Proxy Profile will not expire (always replace before expiration)
 - ▶ SSL Proxy Profile remains in a valid UP state, if it should be modified and forced into a DOWN state, RBM Settings will also remain DOWN.
 - ▶ SSL Client Profile remains in a valid UP state..

Login Failures (continued)

- To recover SSH/WebGUI access to 'admin' you must use the 'admin' user in the serial / virtual console (after each CLI set try webgui/ssh login).
- Removing a expired ldap certificate/down sslproxy
 - ▶ top; co; rbm; no ldap-sslproxy; exit
- Removing a down ssl client profile
 - ▶ top; co; rbm; no ssl-client; exit
- Resetting RBM settings
 - ▶ top; co; rbm; reset; exit
- Reminder: write-mem to save changes!

Question 6

How can I manipulate the content-type header for requests/responses on DataPower?

Content-type Headers

- Sometimes in processing requests and responses on DataPower, the content-type changes during the course of processing.
- Users may also have a need for manipulating the content-type header and forcing it to be a certain value.
- This can be achieved by using a set variable action, an XSL stylesheet, or gatewayscript.

Content-type Headers (continued)

- In version 7.2 there was a new variable added:
var://service/mpgw/proxy-content-type
- The variable controls whether the Content-Type header is preserved and under what conditions it can be modified, based on its value for each processing action and at the end of the processing rule.
- Using version 7.2 and later you may need to set this variable to manipulate the content-type header:
http://www.ibm.com/support/knowledgecenter/en/SS9H2Y_7.2.0/com.ibm.dp.doc/var-service-mpgw-proxy-content-type.html

Content-type Headers (continued)

- Sample Set variable action:

The screenshot shows the 'Configure Set Variable Action' dialog box in the DataPower XI52 interface. The dialog is titled 'Configure Set Variable Action' and has a 'Help' button. It is divided into 'Basic' and 'Advanced' tabs, with 'Basic' selected. The 'Input' section shows 'Context' set to 'INPUT'. The 'Options' section is expanded to show 'Set Variable' settings. The 'Variable Name' is 'var://service/set-request-header/content' with a 'Var Builder' button. The 'Variable Assignment' is 'var://service/original-content-type' with a 'Var Builder' button. The 'Asynchronous' option is set to 'off'. At the bottom are 'Delete', 'Done', and 'Cancel' buttons.

DataPower XI52

Configure Set Variable Action [Help](#)

Basic Advanced

Input

Context INPUT INPUT *

Options

Set Variable

Variable Name var://
service/set-request-header/content Var Builder

Variable Assignment var://service/original-content-type Var Builder

Asynchronous on off

Delete Done Cancel

Content-type Headers (continued)

- Sample XSLT:

```
<xsl:stylesheet version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  extension-element-prefixes="dp"
  xmlns:dp="http://www.datapower.com/extensions"
  exclude-result-prefixes="dp">
  <xsl:output method="xml"/>
  <xsl:template match="/">
<xsl:copy-of select="."/>
    <xsl:variable name="content_type"
select="dp:variable('var://context/INPUT/content-type')" />
    <dp:set-http-request-header name="Content-Type" value="$content_type" />
    <!-- Substitute response for request to manipulate response -->
  </xsl:template>
```

Content-type Headers (continued)

- Sample Gatewayscript:

```
var hm = require('header-metadata');
```

```
//Setting the content-type
```

```
hm.current.set('content-type', 'application/xml');
```

```
//retrieve and log the content-type in the logs to verify change
```

```
var contentType = hm.current.get('content-type');
```

```
console.log(contentType)
```

- Additional Gatewayscript examples can be found in store:// directory on appliance or in knowledge center

Question 7

What are the common reasons for SSL handshake failures?

SSL Handshake Failures

- The SSL/TLS handshake protocol allows the server and client to authenticate each other, negotiate an encryption algorithm and create symmetric keys to transmit encrypted application data.
- There are three main phases to the SSL handshake:
 - ▶ Hello Exchange
 - ▶ Certificate Exchange
 - ▶ Key Exchange
- Most handshake failures occur during the Hello Exchange or Certificate Exchange if the client and server do not support the same:
 - ▶ protocol version
 - ▶ cipher suite
 - ▶ TLS extension

 - ▶ or if the server's certificate cannot be validated by the client.
(or the client's certificate cannot be validated by the server, if requiring client authentication)

SSL Handshake Failures (continued)

- In order to avoid common causes of handshake failures:
 - ▶ With DataPower SSL client:
 - Make sure to understand the remote SSL server's requirements and enable the same in the DataPower Crypto profile or SSL Client Profile:

 - ▶ With DataPower SSL server:
 - Make sure to understand the remote SSL client's requirements/capabilities and enable the same in the DataPower Crypto profile or SSL Server Profile:

SSL Handshake Failures (continued)

Examples:

- If the remote server only supports TLSv1, ensure that the DataPower SSL client has TLSv1 enabled
- If the remote client only supports RC4 ciphers, ensure that the DataPower SSL server has RC4 ciphers enabled
- If the remote server requires Server Name Indication (SNI), ensure that the DataPower client is configured to send the SNI TLS extension in the client hello message (enabled by default).
- If the remote client is not capable of supporting client authentication, set "Request client authentication" to OFF in the DataPower SSL Server Profile
 - If yes, set "Request client authentication" to ON and ensure that the validation credential of the DataPower server contains a certificate of the Certificate Authority (CA) that signed the client's certificate or a copy of the exact client's certificate

Question 8

What are the DataPower FTP and SFTP supported Commands?

FTP/SFTP Supported Commands

- There have been PMRs that ask this question.
- The following technotes answer these questions.

SFTP:

- <http://www.ibm.com/support/docview.wss?uid=swg21396290>

FTP

- <http://www.ibm.com/support/docview.wss?uid=swg21460152>
- SFTP technote link describes the series of commands that would be needed in doing a get request.
- For SFTP, at a high level and from an FTP user perspective, the commands **list**, **get**, **mget**, **put**, and **mput** are supported. However, the commands to do these functions use a different set of commands.
- For FTP, there is a list of the raw FTP commands that are supported.

Question 9

How to determine if there is allowance for anonymous FTP logins?



Anonymous FTP logins

- By default, the FTP server front side handler will allow anonymous logins.
- To force authentication you will need to define some form of AAA policy which controls who can and can't authenticate.
- You will want to navigate to the "control connection authorization" tab.
- To define a standard authentication where the ftp client provides a username and password you would define a username-password AAA policy.
- This AAA Policy will perform authentication of user names and passwords provided to the DataPower FTP server by the client with the USER and PASS commands.

Anonymous FTP logins (continued)

- If the authentication succeeds, the FTP client may use all the features of the DataPower FTP server Front Side Handler.
- If the authentication fails, a 530 error is returned, and the user can attempt to authenticate again.
- Without this AAA Policy configured, any user name and password will be accepted.
- If you are using a firmware lower than 7.2 this will not be in a separate tab. It will be called "Password AAA Policy" and it will be in the main tab.

Question 10

How can DataPower support multi-instance QMGRS as High Availability (HA)?



Multi-instance QMGRS as High Availability

- DataPower uses Active/Active mode for mq-qm objects. However, multi-instance qmgrs uses active/standby mode in the MQ server runtime environment.
- Due to this mis-match, DataPower will generate many errors of 2009/2059 when the mq-qm object can't connect to the standby qmgr instance. For this reason, there is no true support of multi-instance qmgrs in DataPower.
- However, the retry parameters of the mq-qm object can be tuned to minimize the reporting of the MQ errors of 2009/2059 by using longer reporting interval.
- The critical MQ errors can't be suppressed in DataPower. For further details, see the following WSTE presentation.

<http://www.ibm.com/support/docview.wss?uid=swg27043344>

DataPower integration with Multi-instance MQ Queue Managers

Open Lines for Questions



Connect with us!

1. Get notified on upcoming webcasts

Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe

2. Tell us what you want to learn

Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com

Summary



Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
<http://www.ibm.com/developerworks/websphere/community/>
- Join the Global WebSphere Community:
<http://www.websphereusergroup.org>
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
<http://www.ibm.com/software/info/education/assistant>
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
<http://www.ibm.com/software/websphere/support/d2w.html>
- Sign up to receive weekly technical My Notifications emails:
<http://www.ibm.com/software/support/einfo.html>