Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **000-284**

Title : IBM Wbs. DataPower SOA Appliances, Fimware v3.6.0

Version : DEMO

1. A company requires the transformation of a CSV (comma-separated values) file into an XML Format. They have provided an FFD (Flat File Descriptor) file and an XSL File that references the FFD for this capability. An XML Firewall, in Loopback mode, has been created for this process. How should this FFD be used to perform the CSV to XML Transformation?

A. Add a Transformation Action of type XFORMBIN to the Client to Server Rule, and specify the FFD file

B. Add a Transformation Action of type XFORMBIN to the Client to Server Rule, and specify the XSL file

C. Add a Transformation Action of type XFORM to the Server to Client Rule, and specify the FFD file

D. Add a Transformation Action of type XFORM to the Server to Client Rule, and specify the XSL file

E. Add a Transformation Action of type XFORMBIN to the Both Directions Rule, and specify the FFD file

Answer: B

2. A company has developed an XML Firewall to respond to HTTP requests with a binary document, stock.csv, contained in the local: directory of an application domain. The Request Type of the Firewall has been set to Pass-Thru and the Response Type has been set to Non-XML.

The following Style Policy Rule has been configured:

--- request 'returnBinary_Rule_0' [up] matching matchAll --- results INPUT

--- response 'returnBinary_Rule_1' [up] matching matchAll --- fetch local:///stock.csv OUTPUT

Requests are failing with the following messages in the log:

xmlfirewall (returnBinary): response returnBinary_Rule_1 #1 fetch: 'from local:///stock.csv stored in OUTPUT' failed: illegal character 'S' at offset 0 of local:///stock.csv

What must be done to correctly return the binary document?

A. Change the Firewall Response Type to Pass Thru

B. Change the Firewall Request Type to Non-XML

C. Change the Fetch Action Output Type to xml

D. Change the Fetch Action Output Type to binary

E. Move the Fetch Action to the Request Rule and the Results Action to the Response Rule

Answer: D

3. Which DataPower object is required to be configured and active to perform a PUT on a queue using the backend of a Multi Protocol Gateway service on an XI50 using the dpmq:// url syntax?

A. DataPower MQ Host

B. DataPower MQ Queue Manager and DataPower MQ queues

C. DataPower MQ Queue Manager

D. DataPower MQ Gateway

Answer: C

4. A company requires syncpoint on each message extracted from a Request Queue. The Message is processed via HTTP by a backend system. If the DataPower device does not successfully process the message, it should not be removed from the Request Queue. They have created a Multi-Protocol Gateway Service which uses an MQ Front Side Handler and a MQ Queue Manager to facilitate this. How can they implement syncpoint?

A. The DataPower device utilizes an MQ Client, syncpoint cannot be implemented

B. The DataPower device utilizes an MQ Client, syncpoint is implemented by default

C. Set the Queue Manager objects Units Of Work property to 1

D. Create two Queue Manager objects, assign the Request Queue to one Queue Manager and the Reply Queue to the other then add them both to a single MQ Queue Manager Group

E. Set the Queue Manager objects Total Connection Limit property to 1

Answer: C

5. Which statement is NOT true about the Multi-Protocol Gateway service?

A. The Multi-Protocol Gateway can process both DIME and MIME SOAP Attachments.

B. The SLM Action can be used in a Multi-Protocol Gateway Policy.

C. The Multi-Protocol Gateway supports "Synchronous to WS-Addressing" bridging in both directions ("Synchronous to WS-Addressing" and "WS-Addressing to Synchronous").

D. The Multi-Protocol Gateway's "Loopback Mode" can be used with both synchronous and asynchronous protocols.

Answer: D

6. What is the correct configuration to perform FTP PUT into an FTP server using the backend of a Multi Protocol Gateway service?

A. Create and configure the FTP front side handler

B. Configure the backend URL using the FTP protocol

C. Create and configure an NFS object

D. Protocol negotiation is automatic, only a valid host:port is necessary

Answer: B

7. When a Multi-Protocol Gateway service is bridging a message to any asynchronous Backside protocol (such as WebSphere MQ, WebSphere JMS, or Tibco EMS), which Multi-Protocol Gateway property that applies to all transactions can determine how long the Multi-Protocol Gateway will wait for a response message from the Backside Protocol before the Multi-Protocol Gateway gives up and fails the transaction?

A. The "Timeout" value associated with the Multi-Protocol Gateway's XML Manager User Agent settings

B. The 'QueryTimeout=' query parameter on a dynamic Backend URL

C. The "Front Side Timeout" parameter of the Multi-Protocol Gateway

D. The "Back Side Timeout" parameter of the Multi-Protocol Gateway

Answer: D

8. What is supported by the Front-Side Protocol Handler?

A. NFS

B. UDP

C. TNS

D. ICP

E. SNMP

Answer: A

9. A company is supporting an SOA application which receives SOAP Messages over HTTPS. They are required to enrich these messages with data contained within a DB2 Database Table. How can they access this data to provide this capability?

A. Create a service which uses an SQL Front End Protocol Handler to identity the Database, Username, Password, Source ID, Host, Port, and SQL required to extract the necessary data. Specify an Output

Context that can be used in a subsequent StylePolicy Action.

B. Create a service which uses an SQL Backend URL in the form sql:// /static/SELECT%20*%20FROM%20TableName. Specify an Output Context that can be used in a subsequent StylePolicy Action.

C. Create a service which uses a DB2 Data Source; specify the Database, Username, Password, Source ID, Host, Port, and SQL required to extract the necessary data. Specify an Output Context that can be used in a subsequent StylePolicy Action.

D. Use an SQL Data Source and an SQL Action in a StylePolicy Rule which specifies the SQL Data Source. An SQL statement is required to extract the necessary data. Specify an output context that can be used in a subsequent StylePolicy Action.

Answer: D

10. A company is using an XSL Proxy in Proxy mode to fetch and transform XML Documents from an HTTP Server. The XSL, feeValue.xsl, contains the following document function which GETs an XML Document using the HTTPS Protocol:

<xsl:variable name="feeDoc" select="document('https://192.168.1.101/fee.xml')"/>

You enter http://192.168.1.35:2063/empty.xml into a Browser to execute this Proxy Policy and see the following messages in the log:

xslproxy (myXSLProxy): document function error while executing local:///feeValue.xsl: Internal Error Connecting To https://192.168.1.101/fee.xml

Cannot establish SSL credentials

How should proper execution of the document function be enabled?

A. Use https://192.168.1.35:2063/empty.xml, not http://192.168.1.35:2063/empty.xml in Browser Request

B. Assign a Two-Way SSL Proxy Profile to XSL Proxys SSL Server Crypto Profile

C. Use 'https://192.168.1.101' as the Back End Server Address on the XSL Proxy

D. Create a Trusted Servers SSL Crypto Profile and assign it to the XSL Proxys SSL Client Crypto Profile

E. Create a Client Credentials Crypto Profile and use it in the User Agent assigned to the XSL Proxys XML Manager

Answer: E