Exam Code: 000-284

Exam Name: Test284,IBM WbS.DataPower SOA Appliances, Firmware V3.6.0

Vendor: IBM

Version: DEMO

Part: A

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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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
Correct Answers: 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.
Correct Answers: 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
Correct Answers: 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
Correct Answers: D

8: What is supported by the Front-Side Protocol Handler?
A.NFS
B.UDP

C.TNS
D.ICP
E.SNMP
Correct Answers: 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.
Correct Answers: 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
Correct Answers: E

11: You have created an XSL Proxy in Proxy Mode, with a static backend. You have a client to server StylePolicy Rule which executes an XSL Transformation on an XML Document that is

submitted as part of a POST Request. The results from the static backend server will be in HTML. However when you execute an HTTP Post operation in the form of:

POST /someURL HTTP/1.1
User-Agent: curl/7.15.4 (i586-pc-mingw32msvc) libcurl/7.15.4 OpenSSL/0.9.7e zlib/1.2.2
Host: 192.168.0.2
Accept: */*
Content-Length: 0
Content-Type: application/x-www-form-urlencoded

you see the following message in the log:
http://192.168.1.35:2063/someURL: Content type of non-xml (application/x-www-form-urlencoded) means selected stylepolicy is not executed.
What will correct this and execute the StylePolicy?
A.Add an HTTP Header of Content-Type: text/xml to the client request
B.Add an HTTP Header of Content-Type: text/html to the client request
C.Add an HTTP Header injection, Direction = Front, Header = Content-Type, Value = text/html
D.Add an HTTP Header injection, Direction = Back, Header = Content-Type, Value = text/xml
Correct Answers: A

12: A company is attempting to consolidate the XML processing requirements of multiple applications. One issue is that the URLs being used to fetch the XML documents for transformation contain an old application and servlet identifier. These must be replaced with a new consolidated application value of abc. Which technique will change a URL such as http://uri1/uri2/uri3, to http://uri1/abc ?
A.A URL-Rewrite Action with a type of header-rewrite
B.A URL-Rewrite Action with a type of host-body
C.A URL-Rewrite Rule with a type of absolute-rewrite
D.A URL-Rewrite Rule with a type of content-type
Correct Answers: C

13: An XSL Proxy is configured in loopback mode with a single request rule containing a 'validate' step followed by an 'identity transform' (xform store://identity.xsl) where the input context of the transform is set to INPUT. If a message is sent via HTTP POST to this XSL Proxy that correctly conforms to the XML Schema referenced in the 'validate' step, what will be returned to the requestor as the response document?
A.A copy of the request document
B.An empty response document
C.A W3C XML Schema conformance document
D.A schema profile document
Correct Answers: A

14: A company receives requests to their SOA applications via SOAP documents digitally signed using WS-Security. They have a requirement to perform message integrity actions on incoming requests. They have created a WS-Proxy Service using a WSDL describing the application, and have received copies of the public X.509 keys of the intended clients. How can they implement

this message integrity requirement?
A.No action required, Digital Signatures are automatically verified in a WS-Proxy
B.Create a Validation Credential Object using the Clients X.509 Private Key, and assign this to a Verify action on the Default Response Rule Policy
C.Create a Validation Credential Object using the Clients X.509 Private Key, and assign this to a Verify action on the Default Request Rule Policy
D.Create a Validation Credential Object using the Clients Public X.509 Certificate, and assign this to a Verify action on the Default Response Rule Policy
E.Create a Validation Credential Object using the Clients Public X.509 Certificate, and assign this to a Verify action on the Default Request Rule Policy
Correct Answers: E

15: For virus scanning message attachments, DataPower devices support integration with 3rd-party virus scanners using which protocol?
A.ICAP (Internet Content Adaptation Protocol)
B.MVIP (Multi-Exam Code Integration Protocol)
C.SOAP (Simple Object Access Protocol)
D.IMAP (Internet Message Access Protocol)
Correct Answers: A

16: What are three valid Resource Identification Methods for the AAA ER (Extract Resources) step?
A.URL sent to back end
B.SOAP Version Namespace
C.Client IP Address
D.Local name of request element
E.XPath expression
F.HTTP Header Value
Correct Answers: A D E

17: A company has exposed an SOA application. Requests that come from internal endpoints are sent in Plain Text over HTTP. Request documents from third party endpoints outside the DMZ must first be entirely Encrypted, by the third party, according to the WS-Security Specification. A WS-Proxy service has been created using the WSDL document describing this application. What must this company do to accommodate both the Plain Text and Encrypted requests?
A.Create a Crypto Certificate Object using the third partys client's X.509 Public Certificate
B.Provide the company's X.509 Public Certificate to the third party client for use in Encryption, and create a Crypto Key Object using the companies' X.509 Private Key
C.Provide the company's X.509 Public Certificate to the third party client for use in Encryption, add a Decrypt Action to the Default Request Rule for the WS-Proxy and create a Crypto Key Object using the companies' X.509 Private Key
D.Provide the company's X.509 Private Key to the third party client for use in Encryption, add a Decrypt Action to the Default Request Rule for the WS-Proxy and create a Crypto Key Object using the companies' X.509 Public Certificate

E.Add a Decrypt Action to the Default Request Rule, no Crypto Key or Certificate Object is required

Correct Answers: B

18: Which statement accurately describes the relationship between Authentication (AU) and Authorization (AZ) in a DataPower AAA policy?

A.Authorization (AZ) executes first in order, followed by Authentication (AU). If Authorization (AZ) fails, Authentication (AU) will not run.

B.Authorization (AZ) executes first in order, followed by Authentication (AU). Authentication (AU) will always run, even if Authorization (AZ) fails.

C.Authentication (AU) executes first in order, followed by Authorization (AZ). If Authentication (AU) fails, Authorization (AZ) will not run.

D.Authentication (AU) executes first in order, followed by Authorization (AZ). Authorization (AZ) will always run, even if Authentication (AU) fails.

Correct Answers: D

19: When authenticating inbound messages containing SAML Authentication Assertions, what is the most secure authentication mechanism?

A.SSL Mutual Authentication - Only accept SAML Assertions over SSL and force the client to authenticate with its client SSL certificate

B.Verify the digital signature on the SAML Assertion

C.Verify the digital signature on the SAML Assertion and ensure that the signer certificate matches the X.509 Distinguished Name in the SAML Assertion's 'NameIdentifier' element

D.Verify the digital signature on the SAML Assertion and verify that the signer certificate meets the criteria of the configured "SAML Signature Validation Credentials"

Correct Answers: D

20: To cause a single 'log' action to log message content to multiple destinations, which action should the policy administrator take?

A.Multiple URLs may be specified in the 'log' action's Destination URL field separated by comma (,) or semicolon (;) characters.

B.The 'log' action's Destination URL should reference a text file on the device (using the 'local:' or 'store:' protocol schemes) that contains the desired log endpoint URLs, one per line.

C.Associate the "Log Type" of the 'log' action with a user-defined log type with multiple destination URLs.

D.The Destination URL should be a DataPower variable (var://context/name) that contains a nodeset of multiple destination URLs.

Correct Answers: D