

IBM

EXAM 000-609

**IBM WebSphere Datapower SOA Appliances Firmware V3.8.1,
Solution Implementation**

Total Questions: 136

Question: 1.

Which of the following is an advantage of using WS-Security instead of SSL?

- A. Provides assured message delivery.
- B. Provides message integrity for the entire message.
- C. Provides security in end-to-end scenarios across trust boundaries.
- D. Provides mutual authentication to authenticate both the server and client.

Answer: C

Question: 2.

A customer would like to use a WebSphere DataPower service to translate inbound XML messages into COBOL copybook messages. The translation will be performed by a predefined WebSphere Transformation Extender map file. The DataPower service should support both WebSphere MQ and HTTP on the frontside. Based on the scenario above, which of the following is the MOST appropriate DataPower service type?

- A. Web Service Proxy
- B. XML Firewall Service
- C. Multi-Protocol Gateway
- D. Web Application Firewall

Answer: C

Question: 3.

A company is planning to implement disaster recovery (DR) for their two existing WebSphere DataPower Integration Appliance XI50s which have been used for different projects.

The following conditions apply:

- 1) The two devices (source and target appliance) are located in geographically dispersed data centers.
- 2) The firmware level is V3.8.1 on the source appliance and V3.8.1 on the target appliance and their hardware is compatible
- 3) Both appliances have a different set of users that need to be merged
- 4) The source appliance has been initialized with disaster recovery mode and is to be securely backed up and restored onto the target appliance. Which of the following statements is TRUE and supports the above conditions?

- A. The target appliance must be set to disaster recovery mode for the secure restore to be successful.
- B. Merge the contents of the source appliance with the target appliance so as to merge the users on both appliances and do not use the overwrite option when prompted.
- C. The target device will be overwritten. It is not possible to automatically merge the different users on source and target appliances using secure backup and restore.
- D. After a secure restore was run, the administrator realizes that some existing data on the target appliance needs to be saved so the admin can stop the secure restore and start it later after backing up required data on the target appliance

Answer: C

Question: 4.

A customer wants to protect communication between two WebSphere DataPower appliances against a replay attack. The second DataPower appliance needs to validate that the messages received from the first appliance have spent no more than 30 seconds in transit. Which of the following configurations would meet these requirements?

- A. Set the var://service/transactiontimeout variable on the first DataPower appliance to 30 seconds.
- B. Configure mutually authenticated SSL between the two DataPower appliances with an SSL timeout configured to 30 seconds.
- C. Configure the front side handler on the second DataPower appliance with the Stale Connection Timeout field set to 30 seconds.
- D. Use a scheduled processing policy rule on the second DataPower appliance containing a Filter action and configured to run every 30 seconds.
- E. Use symmetric encryption to encrypt a token containing a timestamp on the first DataPower appliance and decrypt it on the second appliance.

Answer: E

Question: 5.

Which of the following protocols are NOT supported by Front Side Handlers?

- A. FTP
- B. NFS
- C. RSS
- D. IIOP
- E. Tibco EMS
- F. WebSphere MQ

Answer: CD

Question: 6.

A customer would like to use a Multi-Protocol Gateway (MPGW) to process an inbound XML message and use a local XSL file to map some of its data to a SOAP message. When configuring the processing policy for this MPGW, which of the following actions should be used for the data mapping?

- A. Transform (xform)
- B. Transform PI (xformpi)
- C. Transform Binary (xformbin)
- D. Transform SOAP (xformsoap)

Answer: A

Question: 7.

A solution implementer is debugging a Web Services Proxy with an HTTPS Front Side Handler listening on port 443. On the backend it communicates with a service <http://server1:9092/myserv>. The irregular performance to the backend service cannot be explained so a packet capture is run to dig deeper into the issue. The results need to be stored in a file called capture1. Also the developer does not want to have irrelevant data captured so as to focus on the problem at hand. A size limit of 30 minutes of capture time or 2.5 meg of total size of the data captured (which ever occurs first) needs to be imposed. Which of the following packet capture CLI commands is correct?

- A. packetcapture local:///capture1 30 2.5 "host server1 and src port=443"
- B. packetcapture temporary:///capture1 30 2.5 "host server1 src port=443"
- C. packetcapture temporary:///capture1 1800 2500 "host server1 and dst port=443"
- D. packetcapture temporary:///capture1 1800 2500 "host server1 and dst port=9092"

Answer: D

Question: 8.

Which of the following is the correct CIDR notation for the IP Address below?

IP Address: 192.168.1.81
Subnet Mask: 255.255.255.0

- A. 192.168.1.81/8
- B. 192.168.1.81/16
- C. 192.168.1.81/24
- D. 192.168.1.81/32

Answer: C

Question: 9.

Which of the following IPv4 address classes supports a maximum of 256 addresses per subnet?

- A. Class A
- B. Class B
- C. Class C
- D. Class D
- E. Class E

Answer: C

Question: 10.

What is the size (in bytes) of an IPv6 IP address?

- A. 4
- B. 6
- C. 8
- D. 16

Answer: D

Question: 11.

Which of the following IPv4 IP addresses is the loopback address?

- A. 0.0.0.0
- B. 0.0.0.1
- C. 127.0.0.0
- D. 127.0.0.1
- E. 255.255.255.0
- F. 255.255.255.1

Answer: D

Question: 12.

A bank wants to use PKI so that its partners can securely access financial transaction data. Certificates signed by a wellknown Certificate Authority are used to implement the solution. Which of the following solution requirements match an appropriate field in the certificate?

A.

Solution Requirement	Certificate Field
The bank and its partners need to be sure that the certificates being used are valid for exactly 1 year.	Validity notBefore notAfter

B.

Solution Requirement	Certificate Field
Compromised certificates (as declared by a trusted authority) should not be accepted by the bank or its partners.	Version

C.

Solution Requirement	Certificate Field
The partner wants to validate the hostname of the bank's SSL server using a field in the certificate.	Subject

D.

Solution Requirement	Certificate Field
The bank wants to constrain that the certificate should only be used for transport (e.g. SSL transport) purposes.	Certificate Basic constraints

E.

Solution Requirement	Certificate Field
The certificate subject of a certificate given to a partner should not be a Certification authority.	Certificate Key Usage

F.

Solution Requirement	Certificate Field
The bank wants to use X.509 V3 certificates.	Certificate Policies

Answer: AC

Question: 13.

The SAML Holder of Key (HOK) method uses PKI to establish trust between a consumer and provider in different trust domains. An Attesting Entity that is trusted by both the consumer and the provider is used. Here is an example of an HOK scenario:

- 1) A SOAP message is sent by a client to an Attesting Entity over SSL.
- 2) The Attesting Entity obtains the public key of the client and places it in the SAML token it is creating in response to the client request, and digitally signs the token.

3) The client adds that SAML token to the SOAP header and constructs the SOAP body, signs it with its own key, and calls the web service provider over SSL.

4) The web service provider verifies the SAML token was signed by the trusted Attesting Entity and processes the message.

Given this scenario, which of the following elements of PKI are used to establish trust between the consumer and provider?

A. The Attesting Entity, provider and consumer use a shared private key to establish trust between them.

B. The Attesting Entity sends its public key to the provider which the provider compares to the trusted public key in its key store to establish trust.

C. The Attesting Entity digitally signs the consumer message with its private key which the provider verifies using the trusted public key of the Attesting Entity.

D. The Attesting Entity vouches for the consumer since it authenticated the consumer first and asserts that by sending a SAML token to the provider over a secure channel.

Answer: C

Question: 14.

Which of the following is NOT a required feature of a secure SSL connection?

A. Message integrity.

B. The negotiation of a shared secret key is secure.

C. The client credentials must be sent to the server.

D. The peer's identity can be authenticated using asymmetric, or public key cryptography.

Answer: C

Question: 15.

SSL uses which encryption type to create a session between client and server?

A. Private Key encryption

B. Symmetric encryption

C. Asymmetric encryption

D. Both Symmetric and Asymmetric encryption

Answer: D

Question: 16.

Which of the following XML messages is a valid SOAP fault under the SOAP 1.1 standard?

A.

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <env:Fault>
            <faultcode>soap:Host</faultcode>
            <faultstring>Internal Error (from host)</faultstring>
        </env:Fault>
    </env:Body>
</env:Envelope>
```

B.

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <env:Fault>
            <faultname>env:Host</faultname>
            <faultstring>Internal Error (from host)</faultstring>
        </env:Fault>
    </env:Body>
</env:Envelope>
```

C.

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <env:Fault>
            <faultcode>env:Client</faultcode>
            <faultstring>Internal Error (from client)</faultstring>
        </env:Fault>
    </env:Body>
</env:Envelope>
```

D.

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <env:Fault>
            <faultname>env:Client</faultname>
            <faultstring>Internal Error (from client)</faultstring>
        </env:Fault>
    </env:Body>
</env:Envelope>
```

Answer: C

Question: 17.

Which XML document is NOT valid?

A.

```
<a xmlns="http://schemas.ibm.com/a">
  <b>
    <c xmlns="http://schemas.ibm.com/c"/>
  </b>
</a>
```

B.

```
<a:a xmlns:a="http://schemas.ibm.com/a"
      xmlns:b="http://schemas.ibm.com/b"
      xmlns:c="http://schemas.ibm.com/c">
  <b:b>
    <c:c/>
  </b:b>
</a:a>
```

C.

```
<a:a xmlns="http://schemas.ibm.com/a">
  <b:b xmlns="http://schemas.ibm.com/b">
    <c:c xmlns="http://schemas.ibm.com/c"/>
  </b:b>
</a:a>
```

D.

```
<b:a xmlns:a="http://schemas.ibm.com/a"
      xmlns:b="http://schemas.ibm.com/b"
      xmlns:c="http://schemas.ibm.com/c">
  <c:b>
    <a:c/>
  </c:b>
</b:a>
```

Answer: C

Question: 18.

Which XML document is valid?

A.

```
<a>
  <b>
    <l e="w">
      <a>
        <s>
          <i>
            <e r="e"/>
          </i>
        </s>
      </a>
    </w>
    </e>
  </l>
  </b>
</a>
```

B.

```
<m>
  <a>
    <d/>
  </a>
  <m>
    <i>
      <n>
        <e d="e"/>
      </n>
    </i>
  </m>
  </a>
  <d/>
  </a>
</m>
```

C.

```
<w>
  <a>
    <s>
      <i>
        <t>
          <a>
            <c/>
          </a>
          <r>
            <o/>
          </r>
          <a/>
          <c/>
        </a>
      </t>
    </i>
  </s>
</a>
</w>
```

D.

```
<a>
  <m>
    <a>
      <n/>
    </a>
    <p>
      <l>
        <a>
          <n/>
        </a>
        <c/>
        <a n="a"/>
      </l>
    </p>
    <a>
      <n/>
    </a>
  </m>
</a>
```

Answer: D

Question: 19.

Which of the following SOAP messages is valid according to the SOAP specification?

A.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        <a:id xmlns:id="http://www.ibm.com/identify">00230-1</id>
        <b:polling xmlns:polling="http://www.ibm.com/poll" env:role="http://www.ibm.com/logger" env:mustUnderstand="true">
    </soap:Header>
    <soap:Body>
        <getProduct>
            <Product>WebSphere DataPower</Product>
        </getProduct>
    </soap:Body>
</soap:Envelope>
```

B.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        <a:id xmlns:id="http://www.ibm.com/identify">00230-1</a:id>
    </soap:Header>
    <soap:Body>
        <items:getProduct>
            <items:Product xmlns:items="http://www.ibm.com/categories">WebSphere DataPower</items:Product>
        </items:getProduct>
    </soap:Body>
</soap:Envelope>
```

C.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        <id>00230-1</id>
    </soap:Header>
    <soap:Body>
        <items:getProduct xmlns:items="http://www.ibm.com/categories">
            <items:Product>WebSphere DataPower</items:Product>
        </items:getProduct>
    </soap:Body>
</soap:Envelope>
```

D.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header/>
    <soap:Body>
        <items:getProduct xmlns:items="http://www.ibm.com/categories">
            <items:Product>WebSphere DataPower</items:Product>
        </items:getProduct>
    </soap:Body>
</soap:Envelope>
```

Answer: D

Question: 20.

Refer to the Exhibit.

```
<?xml version="1.0" encoding="UTF-8" ?>
<msg:message xmlns:hdr="http://schemas.ibm.com/header" xmlns:msg="http://schemas.ibm.com/message" xmlns:pay="http://schemas.ibm.com/payload">
  <hdr:header>
    <sequencenum>http://esb.ibm.com/source-system:0123-4567-8901-2345</sequencenum>
    <destination>http://esb.ibm.com/dest-system</destination>
    <source>http://esb.ibm.com/source-system</source>
    <action>http://esb.ibm.com/dest-system#CustomerInfoRequest</action>
    <timestamp>2009-04-18T19:30:47.02</timestamp>
  </hdr:header>
  <pay:payload>
    <><Customer>
      <Company>Some Company</Company>
      <Name>Some Person</Name>
      <><ContactInfo>
        <Address AddressType="Business">
          <Street>123 Some Street</Street>
          <City>Some City</City>
          <State>XX</State>
          <Country>USA</Country>
          <ZipCode>12345</ZipCode>
        </Address>
        <Address AddressType="POBox">
          <Street>PO Box 123</Street>
          <City>Some City</City>
          <State>XX</State>
          <Country>USA</Country>
          <ZipCode>54321</ZipCode>
        </Address>
        <><Phone PhoneType="Business">
          <PhoneNumber>123-456-7890</PhoneNumber>
        </Phone>
        <><Phone PhoneType="Mobile">
          <PhoneNumber>987-654-3210</PhoneNumber>
        </Phone>
        <><Email EmailType="Business">
          <EmailAddress>workaddr@somecompany.com</EmailAddress>
        </Email>
        <><Email EmailType="Personal">
          <EmailAddress>homeaddr@someisp.com</EmailAddress>
        </Email>
      </ContactInfo>
    </Customer>
    <><Product>
      <ProductType>Widget</ProductType>
      <UnitPrice Currency="USD">123.45</UnitPrice>
      <Quantity>6</Quantity>
    </Product>
    <><Product>
      <ProductType>Whatsit</ProductType>
      <UnitPrice Currency="CAD">543.21</UnitPrice>
      <Quantity>7</Quantity>
    </Product>
  </pay:payload>
</msg:message>
```

Given the information in the exhibit, which XPath expression locates the element named "Company"?

- A. /*/Company
- B. /*/*/*[1]
- C. /msg:message/*/*[1]
- D. /msg:message/payload/*/*[1]

Answer: B

Question: 21.

Refer to the Exhibit.

```
<?xml version="1.0" encoding="UTF-8" ?>
<msg:message xmlns:hdr="http://schemas.ibm.com/header" xmlns:msg="http://schemas.ibm.com/message" xmlns:pay="http://schemas.ibm.com/payload">
  <hdr:header>
    <sequencenum>http://esb.ibm.com/source-system:0123-4567-8901-2345</sequencenum>
    <destination>http://esb.ibm.com/dest-system</destination>
    <source>http://esb.ibm.com/source-system</source>
    <action>http://esb.ibm.com/dest-system#CustomerInfoRequest</action>
    <timestamp>2009-04-18T19:30:47.02</timestamp>
  </hdr:header>
  <pay:payload>
    <><Customer>
      <Company>Some Company</Company>
      <Name>Some Person</Name>
      <><ContactInfo>
        <Address AddressType="Business">
          <Street>123 Some Street</Street>
          <City>Some City</City>
          <State>XX</State>
          <Country>USA</Country>
          <ZipCode>12345</ZipCode>
        </Address>
        <Address AddressType="POBox">
          <Street>PO Box 123</Street>
          <City>Some City</City>
          <State>XX</State>
          <Country>USA</Country>
          <ZipCode>54321</ZipCode>
        </Address>
        <><Phone PhoneType="Business">
          <PhoneNumber>123-456-7890</PhoneNumber>
        </Phone>
        <><Phone PhoneType="Mobile">
          <PhoneNumber>987-654-3210</PhoneNumber>
        </Phone>
        <><Email EmailType="Business">
          <EmailAddress>workaddr@somecompany.com</EmailAddress>
        </Email>
        <><Email EmailType="Personal">
          <EmailAddress>homeaddr@someisp.com</EmailAddress>
        </Email>
      </ContactInfo>
    </Customer>
    <><Product>
      <ProductType>Widget</ProductType>
      <UnitPrice Currency="USD">123.45</UnitPrice>
      <Quantity>6</Quantity>
    </Product>
    <><Product>
      <ProductType>Whatsit</ProductType>
      <UnitPrice Currency="CAD">543.21</UnitPrice>
      <Quantity>7</Quantity>
    </Product>
  </pay:payload>
</msg:message>
```

Given the information in the exhibit, which XPath expression locates the element named "pay:payload"?

- A. /pay:payload
- B. //*/Customer/..
- C. /msg:message/*
- D. /msg:message/..//*/payload

Answer: B

Question: 22.

Refer to the Exhibits.

Exhibit 1

```
<?xml version = "1.0" encoding = "UTF-8" ?>
<!DOCTYPE list SYSTEM "books.dtd">
<list>
    <book ID = "888">
        <author>John Certified</author>
        <title>I Love WebSphere DataPower</title>
        <price>$8.00</price>
    </book>
    <book ID = "999">
        <author>Alex Expert</author>
        <title>Stylesheets for Beginners</title>
        <price>$7.00</price>
    </book>
</list>
```

Exhibit 2

```
<html>
    <head>
        <title>Book List</title>
    </head>
    <body>
        <table border="1" cols="3" width="100%">
            <tbody>
                <tr>
                    <td>888</td>
                    <td>I Love WebSphere DataPower</td>
                    <td>$8.00</td>
                </tr>
                <tr>
                    <td>999</td>
                    <td>Stylesheets for Beginners</td>
                    <td>$7.00</td>
                </tr>
            </tbody>
        </table>
    </body>
</html>
```

Which of the following XSL stylesheets would transform the XML document in Exhibit 1 to the HTML result in Exhibit 2?

A.

```
<?xml version="1.0" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
    <xsl:template match="/">
        <html>
            <head>
                <title>Book List</title>
            </head>
            <body>
                <table border="1" cols="3" width="100%">
                    <tbody>
                        <xsl:apply-templates/>
                    </tbody>
                </table>
            </body>
        </html>
    </xsl:template>
    <xsl:template match="book">
        <tr>
            <td>
                <xsl:value-of select="@ID"/>
            </td>
            <td>
                <xsl:value-of select="title"/>
            </td>
            <td>
                <xsl:value-of select="price"/>
            </td>
        </tr>
    </xsl:template>
    ...
    ...(remaining templates omitted for clarity)
```

B.

```

<?xml version="1.0" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
    <xsl:template match="/">
        <html>
            <head>
                <title>Book List</title>
            </head>
            <body>
                <table border="1" cols="3" width="100%">
                    <tbody>
                        <xsl:apply-templates/>
                    </tbody>
                </table>
            </body>
        </html>
        <tr>
            <td>
                <xsl:value-of select="@ID"/>
            </td>
            <td>
                <xsl:value-of select="title"/>
            </td>
            <td>
                <xsl:value-of select="price"/>
            </td>
        </tr>
    </xsl:template>

```

... (remaining templates omitted for clarity)

C.

```

<?xml version="1.0" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
    <xsl:template match="/book">
        <html>
            <head>
                <title>Book List</title>
            </head>
            <body>
                <table border="1" cols="3" width="100%">
                    <tbody>
                        <xsl:apply-templates/>
                    </tbody>
                </table>
            </body>
        </html>
    </xsl:template>
    <xsl:template match="/">
        <tr>
            <td>
                <xsl:value-of select="@ID"/>
            </td>
            <td>
                <xsl:value-of select="title"/>
            </td>
            <td>
                <xsl:value-of select="price"/>
            </td>
        </tr>
    </xsl:template>

```

... (remaining templates omitted for clarity)

D.

```
<?xml version="1.0" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
    <xsl:template match="/">
        <html>
            <head>
                <title>Book List</title>
            </head>
            <body>
                <table border="1" cols="3" width="100%">
                    <tbody>
                        <xsl:apply-templates match="book"/>
                    </tbody>
                </table>
            </body>
        </html>
        <tr>
            <td>
                <xsl:value-of select="@ID"/>
            </td>
            <td>
                <xsl:value-of select="title"/>
            </td>
            <td>
                <xsl:value-of select="price"/>
            </td>
        </tr>
    </xsl:template>
    ...
    ... (remaining templates omitted for clarity)
```

Answer: A

Question: 23.

Refer to the Exhibit.

```
XML:
<cert>
    <topic name='Stylesheet Variables'>
        Knowledge of Stylesheet Variables
    </topic>
</cert>

XSLT:
<?xml version="1.0" encoding="utf-8"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
<xsl:output method="xml"/>

    <xsl:template match="/">
        <xsl:variable name="topic"><xsl:value-of select="//topic"/></xsl:variable>
        <html>
            <title>DataPower Certification</title>
            <xsl:element name="p">
                <xsl:choose>
                    <xsl:when test="$topic='Security'">Topic: Web Services Security</xsl:when>
                    <xsl:when test="$topic='Protocols'">Topic: Supported Protocols</xsl:when>
                    <xsl:otherwise>Topic: <xsl:value-of select="$topic"/></xsl:otherwise>
                </xsl:choose>
            </xsl:element>
        </html>
    </xsl:template>

</xsl:stylesheet>
```

Which output would be generated when the above XML is transformed by the given stylesheet?

- A. <?xml version="1.0" encoding="UTF8"?>
<html>
<title>DataPower Certification</title>
<element name="p">
Topic: Stylesheet Variables
</element>
</html>
- B. <?xml version="1.0" encoding="UTF8"?>
<html>
<title>DataPower Certification</title>
<p>
<topic>
Topic: Stylesheet Variables
</topic>
</p>
</html>
- C. <?xml version="1.0" encoding="UTF8"?>
<html>
<title>DataPower Certification</title>
<p>
Topic: Knowledge of Stylesheet Variables
</p>
</html>
- D. <?xml version="1.0" encoding="UTF8"?>
<html>
<title>DataPower Certification</title>
<p>
<topic>
Topic: Knowledge of Stylesheet Variables
</topic>
</p>
</html>

Answer: C

Question: 24.

The WS-Security BinarySecurityToken profile defines a mechanism for carrying cryptographic tokens.
Which of the following types of tokens are acceptable?

- A. Kerberos
- B. Password
- C. Username
- D. Cipher Spec
- E. X.509 Certificate

Answer: AE

Question: 25.

Where is a binary attachment packaged in a SWA (SOAP with Attachments) message?

- A. The SOAP Body
- B. The SOAP Header
- C. The root MIME part
- D. A nonroot MIME part

Answer: D

Question: 26.

The SOAP with Attachment (SWA) specification requires which of the following compression algorithms?

- A. rar compression
- B. zip compression
- C. lzw compression
- D. compression is not necessary

Answer: D

Question: 27.

Which feature of JMS and WebSphere MQ messages allows these systems to identify and handle Poisoned Messages?

- A. The automatic Virus Checking of all messages
- B. The Redelivery or Backout Count field in the message header
- C. Transactionality is optional; turning it off will avoid Poisoned Messages
- D. Message Persistence which allows logging of all messages so a Poisoned Message will not affect any other Messages

Answer: B

Question: 28.

Within which WebSphere MQ header block is the correlation ID carried on MQ response messages?

- A. MQCIH
- B. MQIIH
- C. MQMD
- D. MQRFH2

Answer: C

Question: 29.

Which of the following features ARE available on the WebSphere DataPower Integration Appliance XI50 but NOT on the WebSphere DataPower XML Security Gateway XS40?

- A. Support for WebSphere JMS as a backend protocol.
- B. Support for Reliable Multicast Messaging (RMM) as a backend protocol.
- C. Connectivity to SNMP toolkits for monitoring and alerting.
- D. The ability to transform XML to binary using a WebSphere Transformation Extender (WTX) map.
- E. A transaction viewer that can correlate Message Disposition Notification (MDN) acknowledgements with the original request message.

Answer: AD

Question: 30.

The WebSphere DataPower Low Latency Appliance XM70 supports which of the following protocols?

- A. WebSphere MQ
- B. Tibco Rendezvous
- C. AS2 (Applicability Statement 2)
- D. RUM (Reliable Unicast Messaging)
- E. RPM (Reliable Polycast Messaging)

Answer: ABD

Question: 31.

An application is sending realtime securities transactions using the FIX (Financial Information eXchange) message format. The customer wishes to route these messages to subscribers based upon a stock ticker symbol found within the FIX message. Which of the following is the appropriate WebSphere DataPower appliance for this customer?

- A. XA35
- B. XS40
- C. XI50
- D. XB60
- E. XM70

Answer: E

Question: 32.

A customer is receiving binary packed EDI using S/MIME over HTTP and S/MIME over FTP. The customer currently uses WebSphere Partner Gateway and WebSphere Transformation Extender to send functional acknowledgements, convert the message, and send a correlated response. The customer is interested in improving performance and scaling this architecture to remove some of the processing overhead. Which of the following would benefit the customer in this scenario?

- A. Add XS40 appliances in the DMZ to provide WS-Security decryption of the secure payload.
- B. Add XI50 appliances to convert the EDI to XML and send functional acknowledgements.
- C. Add XI50 appliances to parse the attachments on the request messages and deposit the result on a WebSphere MQ queue.
- D. Add XB60 appliances to move the security functionality to the DMZ and send MDN acknowledgements.
- E. Add XM70 appliances to send unicast UDP responses to the clients.

Answer: D

Question: 33.

Which of the following is NOT available as a service object on a WebSphere DataPower Appliance?

- A. XSL Proxy
- B. B2B Gateway
- C. Transformation Gateway
- D. Low Latency Messaging
- E. Web Application Firewall

Answer: C

Question: 34.

Which of the following are offered by the WebSphere DataPower Integration Blade XI50B?

- A. Support for AS1 and AS2 protocols.
- B. Support for 10 Gigabit Ethernet interfaces.
- C. Support for Tibco Rendezvous as a transport protocol.
- D. Support for the z/OS Sysplex Distributor for load balancing of client requests.
- E. Support for the z/OS Dynarouter for Intelligent Load Distribution to backend servers.

Answer: BD

Question: 35.

Which of the following are key features provided by the WebSphere DataPower Option for Application Optimization (AO)?

- A. Custom Balancing and Load Distribution
- B. Self Balancing and Round Robin Distribution
- C. Self Balancing and Intelligent Load Distribution
- D. Remote Balancing and Intelligent Self Distribution

Answer: C

Question: 36.

for firmware V3.8.1, on which of the following Websphere DataPower SOA appliances is the Application Optimization (AO) feature available?

- A. XML Accelerator (XA35)
- B. XML Security Gateway (XS40)
- C. Integration Appliance (XI50)
- D. B2B Appliance (XB60)
- E. Low Latency Appliance (XM70)

Answer: BC

Question: 37.

A company has developed an XML Firewall of type "Loopback Proxy". A 'Server to Client' Policy Rule has been implemented with a Transform action that changes the value of certain elements. When a document is submitted, the returned document appears to be unchanged. Which action should be taken to correct this?

- A. Change the Rule Direction to 'Client to Server'.
- B. Change the Front Side Request Type to PassThru.
- C. Change the Firewall Type to 'Static Backend' and provide a loopback address.
- D. Change the Firewall Type to 'Dynamic Backend' and provide a loopback Route Action.

Answer: A

Question: 38.

A company has developed a multi platform support system for wireless applications which interacts with an XML repository. Some platforms will require HTML responses, some WML, and others raw XML. The company is using a homegrown Java application to transform the responses using XSLT, but are not satisfied with performance and have chosen to use WebSphere DataPower for inline transformation. Documents will be fetched by the client via HTTP GET requests, and no security processing is required. Which service should be used to implement this architecture and optimize the XSLT transformations?

- A. WS-Proxy
- B. XSL Proxy
- C. Web Application Firewall
- D. Multi-Protocol Gateway with multiple Front Side Protocol Handlers supporting different transport protocols.

Answer: B

Question: 39.

A customer would like to make improvements to one of their existing systems. One of the improvements is to provide ebXML Messaging Service (ebMS 2.0) support for this system. Based on this information, which of the following would be the best fit WebSphere DataPower service type for this scenario?

- A. XML Firewall
- B. B2B Gateway
- C. Multi-Protocol Gateway
- D. Web Application Firewall

Answer: B

Question: 40.

A Multi-Protocol Gateway has been created to accept requests in a commaseparatedvalue format. The first action in the request rule is a binary transformation that converts the CSV to a simple XML format. The message must then be processed by further Transform actions. Which of the following is a valid option for the service Request Type?

- A. JSON
- B. SOAP
- C. NonXML
- D. PassThru

Answer: C

Question: 41.

Which of the following is TRUE regarding a rule defined to use the PassThru message type?

- A. All actions in the rule will be executed.
- B. No actions in the rule will be executed.
- C. All streamable actions in the rule will be executed.
- D. Only nonTransform actions in the rule will be executed.
- E. All actions in the rule will be executed, as long as none of them uses the input context 'INPUT'.

Answer: B

Question: 42.

In the Configured Rules section of the Policy Editor, two request rules are listed: Rule #1, followed by Rule #2. Both use the same matching rule. Which of the following will occur when a message that satisfies the matching rule is received?

- A. Only rule #1 will be executed since it is the first rule that matches the request.
- B. Rule #1 will be executed, followed by Rule #2, since all rules that satisfy the match are executed.
- C. This policy will fail during execution, since it cannot be determined which rule should be executed.
- D. This situation cannot occur, since the Policy Editor will not allow a configuration of rules that have the same match.

Answer: A

Question: 43.

A WSProxy is receiving orders from partners as SOAP messages. The service is required to reject messages if the total order cost in the message does not match the sum of the individual item costs. Which of the following describes the functionality that would support this requirement?

- A. Create an XML Schema that enforces the above business requirements and uses this schema in a Validate action.
- B. Use a Conditional Action to perform the mathematical comparison and run a Log action with 'Terminate Processing' set to On.
- C. Create a stylesheet which performs the mathematical comparison and returns either a `<dp:accept>` or `<dp:reject>` and use this in a Filter action.
- D. Define the requirement in a WSPolicy attachment for the service. The WSProxy will then automatically perform the mathematical comparison and reject any invalid messages.

Answer: C

Question: 44.

A solution implementer would like to use a set of actions in a number of processing rules in a processing policy. To speed up configuration and maintenance the implementer has used the "Create Reusable Rule" button on the Policy editor screen of the WebGUI to create a Reusable Rule. This rule has then been dragged and dropped on to several other processing rules in the policy. Later, one of the actions in the reusable rule needs to be removed.

Which of the following describes how this would be achieved?

- A. The action must be removed individually from each rule that uses it as reusable rules have no permanent link to the original rule definition.
- B. The action can be removed directly from one of the rules using the reusable rule by dragging it to the trash can icon on the Policy editor.
- C. The action can be removed from the reusable rule itself which appears as an additional named rule on the list of configured rules for the policy.
- D. The action must be removed from the reusable rule itself which only appears under the Objects menu on the Navigation Bar.

Answer: D

Question: 45.

A customer wants each SOAP request message and only the SOAP request message passing through a policy to be logged to a remote servlet via HTTP. The customer wants this logging to be done in parallel with other processing, but needs to ensure that it completes as part of their policy. Which of the following action(s) must be employed?

- A. Log Action (with Asynchronous toggle set to on)
- B. Log Action (with Asynchronous toggle set to on), Event Sink Action (with Log Action selected in the Action property)
- C. ResultsAsync Action
- D. Results Action (with Asynchronous toggle set to on)
- E. Results Action (with Asynchronous toggle set to on), Event Sink Action (with Results Action selected in the Action property)

Answer: E

Question: 46.

A customer wants to execute one of three processing rules for messages received on a given front side URL. The processing rule is to be chosen based on the result of a database query that uses content from the message in the lookup. The database query will return one of three possible values. Which of the following processing configurations is required?

- A. Three match rules, one for each possible value returned from the database.
- B. Two specific match rules, and one default match rule.
- C. Default match rule, SQL Action with XML output, Conditional Action that uses the SQL Action's output as its input.
- D. Default match rule, SQL Action with XML output, Call Action that uses the SQL Action's output as its input.

Answer: C

Question: 47.

A solution implementer is testing a simple XML Firewall which needs to be a proxy for a web application. Both request and response message types are selected as nonXML on the main configuration panel. The policy has only a matching rule and a Results action. When a URL is entered from the browser, an HTTP 405 method is received. The logs show a message of the type: xmlfirewall (TestFW): Request method (GET) without a message body is not allowed, URL: http://example.com/servlet/test Which of the following steps should the solution implementer take to correct this error?

- A. In the XML Firewall Advanced Panel, set 'Disallow GET (and HEAD)' to On.
- B. An XML Firewall cannot handle HTML traffic so a Multi-Protocol Gateway should be used.
- C. In the XML Firewall Advanced Panel, set 'Process Messages Whose Body Is Empty' to On.
- D. In the Objects Menu for the Configure Processing Rule panel, set 'NonXML Processing' to On.

Answer: C

Question: 48.

A company wants to explore the use of a URL Rewrite Policy in a Multi-Protocol Gateway. Which of the following is TRUE? A URL Rewrite Policy:

- A. can convert an MQMD header to an HTTP header.
- B. is executed before the request rule in the processing policy.
- C. cannot replace the value of the ContentType header based on a URL match.
- D. cannot replace URL encoded (for example, %2f characters) that occur in the rewritten URL.

Answer: B

Question: 49.

Which statement is NOT true about the Multi-Protocol Gateway (MPGW) service?
The MPGW:

- A. supports the use of the SLM Action.
- B. can process MQIIH and MQCIH headers.
- C. can process both DIME and MIME SOAP Attachments.
- D. can bridge between FTP Poller front end and HTTP backend protocols.
- E. supports only synchronous protocols in its Front Side Handlers when its Type is set to "Loopback Proxy".

Answer: E

Question: 50.

To perform a field trial with 'Company A', a sales engineer is provided with the following configuration for the network interface:

eth1

IP: 10.10.31.13/24

Default Gateway: 10.10.10.1

The web management service is enabled on eth1 on port 80. The sales engineer and customer then move to a conference room where they attempt to connect to the device from a workstation with the IP 10.1.1.2, but cannot reach the device's WebGUI. What is the cause of this error?

- A. eth1 has been configured with the wrong subnet mask.
- B. The customer provided the wrong network configuration.
- C. The GUI is part of the management plane and runs only on the mgmt0 interface.
- D. The WebGUI is not supported on port 80, it requires ports within range 8000-9999.

Answer: B

Question: 51.

Which of the following CLI commands should be used to enable the XML Management Interface of a WebSphere DataPower appliance?

- A. xi50# configure terminal
xi50(config xmlmgmt) # localaddress X.X.X.X
xi50(config xmlmgmt) # port XXXX
xi50(config xmlmgmt) # mode amp
xi50(config xmlmgmt) # adminstate enabled
xi50(config xmlmgmt) # exit
xi50(config) # write memory
Overwrite previously saved configuration [y/n] yes
- B. xi50# configure terminal
xi50(config) # xmlmgmt
xi50(config xmlmgmt) # localaddress X.X.X.X
xi50(config xmlmgmt) # port XXXX
xi50(config xmlmgmt) # mode amp+soma
xi50(config xmlmgmt) # adminstate enabled
xi50(config xmlmgmt) # exit
xi50(config) # write memory
Overwrite previously saved configuration [y/n] yes
- C. xi50# configure terminal
xi50(config) # xmlmgmt
xi50(config xmlmgmt) # mode amp+soma
xi50(config xmlmgmt) # adminstate enabled
xi50(config xmlmgmt) # exit
xi50(config) # write memory
Overwrite previously saved configuration [y/n] yes
- D. xi50# configure terminal
xi50(config) # xmlmgmt
xi50(config xmlmgmt) # localaddress X.X.X.X
xi50(config xmlmgmt) # adminstate enabled
xi50(config xmlmgmt) # modeamp enabled
xi50(config xmlmgmt) # exit
xi50(config) # write memory
Overwrite previously saved configuration [y/n] yes

Answer: B

Question: 52.

Which of the following is the correct syntax for Access Policies contained within an RBM (Role Based Management) Group definition?

- A. Application Domain/Resource Name?Access=permissions[&field=value]
- B. Device Address/User Account/Resource Name?Access=permissions[&field=value]
- C. Device Address/Application Domain/Resource Name?Access=permissions[&field=value]
- D. Address/Ethernet Port/Application Domain/Resource ame?Access=permissions[&field=value]

Answer: C

Question: 53.

While configuring RBM settings, which of the following are valid authentication methods?

- A. LDAP, RADIUS, SPNEGO, XML File
- B. SPNEGO, SAF, RADIUS, Client IP address
- C. LDAP, RADIUS, SSL user certificate, TACACS
- D. SAF, Local User, SSL user certificate, LTPA Token

Answer: A

Question: 54.

Which is NOT a feature of Configuration Checkpoint Management?

- A. Checkpoint configurations can be deleted from file system.
- B. Checkpoint configurations may be compared against the running configuration.
- C. Checkpoint configurations may be compared against the persisted configuration.
- D. Configuration objects can be imported from Checkpoint configurations.
- E. The administrator can limit the number of Checkpoint configurations maintained.

Answer: D

Question: 55.

Refer to the Exhibit.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
- <soapenv:Body>
- <dp:request xmlns:dp="http://www.datapower.com/schemas/management">
- <dp:do-backup format="ZIP" persisted="true">
<dp:domain name="Domain1" />
<dp:domain name="Domain2" />
<dp:domain name="Domain3" />
</dp:do-backup>
</dp:request>
</soapenv:Body>
</soapenv:Envelope>
```

The SOAP Configuration Management call above will perform which of the following actions?

- A. Return the persisted configuration of the listed domains in base64 encoded format in the SOAP response.
- B. Create a single zip file of the persisted configuration of all listed domains in the temporary directory that the users can download via the WebGUI.
- C. Create individual zip files of the running configuration of all listed domains in the temporary directory that the users can then download via the WebGUI.
- D. Persist the running configuration of the listed domains and then return the persisted configuration of listed domains in base64 encoded format in the SOAP response.

Answer: A

Question: 56.

A company is planning for disaster recovery (DR) for their WebSphere DataPower appliances and plan to use secure backup and restore.

The following conditions apply:

- 1) The two devices (source and target appliance) are located in geographically dispersed data centers.
- 2) The firmware and hardware on the source and target appliances are compatible.
- 3) The source appliance is not currently in disaster recovery mode.
- 4) The iSCSI and RAID devices on both appliances are compatible in size but need not be restored to the target appliance. Which of the following are FALSE?

- A. Backing up the iSCSI and RAID data is optional.
- B. The source appliance must be reinitialized to be able to select the disaster recovery mode option.
- C. The private keys and password type data on the source appliance are encrypted twice in the secure backup.
- D. The default log from the source device is backed up to the target device so debugging on the target can continue.
- E. Users working on the target device need not log out when the secure restore runs and can continue to complete their tasks without loss of work.

Answer: DE

Question: 57.

A solution implementer has configured two WebSphere DataPower appliances, one for testing and one for production. To simplify configuration management they have created objects on both appliances representing the different external resources that will be needed in the different environments for example a Load Balancer Group to point to the LDAP servers being used and an MQ Queue Manager to reference the specific testing or production Queue Managers.

Testers will export configurations from the testing appliance, pass these configurations to the solution implementer who will only upload the configurations to the production appliance. A process must be put in to place to guarantee that these environmentspecific objects are not overwritten when configuration changes are migrated from testing to production.

Which of the following describes a process that would meet these requirements?

- A. Institute a governance process that all testers should follow during migration to only export the objects that will be needed in production.
- B. Use the "Remove Nonshareable Device Settings" option on the WebGUI Export screen to only export the services and not the environmentspecific objects.
- C. Create a Deployment Policy which can be run when importing the configurations on to the production appliance which uses the Accepted Configuration functionality to only allow explicitly listed object types to be imported.
- D. Create two domains on the testing appliance and place all environmentspecific objects in to one domain which is visible to the second domain containing the service objects. It will then not be possible for the testers to export the environmentspecific configurations.

Answer: C

Question: 58.

A solution implementer has created a Deployment Policy to scan through configurations when they are imported and remove any references to appliance specific settings such as the ethernet addresses and the WebGUI port. Which of the following Deployment Policy settings would provide this functionality?

- A. A Filtered Configuration with a list of the objects that are to be included.
- B. A Filtered Configuration with a list of the objects that are to be excluded.
- C. A Rejected Configuration with a list of the objects that must be rejected during import.
- D. A Modified Configuration with a type of Delete Configuration and a list of the objects that must be removed during import.
- E. An Accepted Configuration with a list of the correct values for the properties for any named objects that will be updated during import.

Answer: BD

Question: 59.

As part of a system testing scenario, a customer is using the XML Management interface on WebSphere DataPower to delete a file (Testfile) from the local store on the appliance. The customer wants the change to only be applied to the default domain on the device.
Which of the following requests is a valid example for this scenario?

A.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <dp:request xmlns:dp="http://www.datapower.com/schemas/management">
            <dp:do-action>
                <DeleteFile>
                    <File>local:///Testfile</File>
                </DeleteFile>
            </dp:do-action>
        </dp:request>
    </env:Body>
</env:Envelope>
```

B.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <dp:request domain="default"
            xmlns:dp="http://www.datapower.com/schemas/management">
            <dp:do-action>
                <Delete>
                    <File>local:///Testfile</File>
                </Delete>
            </dp:do-action>
        </dp:request>
    </env:Body>
</env:Envelope>
```

C.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <dp:request xmlns:dp="http://www.datapower.com/schemas/management">
            <dp:do-action>
                <Delete>
                    <File>local:///Testfile</File>
                </Delete>
            </dp:do-action>
        </dp:request>
    </env:Body>
</env:Envelope>
```

D.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Body>
        <dp:request domain="default" xmlns:dp="http://www.datapower.com/schemas/management">
            <dp:do-action>
                <DeleteFile>
                    <Location>local:///Testfile</Location>
                </DeleteFile>
            </dp:do-action>
        </dp:request>
    </env:Body>
</env:Envelope>
```

Answer: A

Question: 60.

A solution implementer is planning to script some WebSphere DataPower configuration task, which will run against the CommandLine Interface (CLI). If the script assumes the admin user is already logged into the CLI, which sequence of commands will configure the management Ethernet interface and restrict the WebGUI to that interface?

Note that the address allocated for the management Ethernet interface is 10.0.0.1/8

- A. configure terminal
interface mgt0
ip address 10.0.0.1/8
static servicetype webgui
exit
webmgmt 10.0.0.0 9090
- B. configure terminal
interface mgt0
ip address 10.0.0.1/8
exit
webmgmt 10.0.0.1 9090
- C. configure terminal
interface mgt0
ip address 10.0.0.1/8
exit
webmgmt 0.0.0.0 9090
acl 10.0.0.1
- D. configure terminal
interface mgt0
ip address 10.0.0.1/8
exit
webmgmt 0.0.0.0 9090

Answer: B

Question: 61.

WebSphere Transformation Extender Design Studio V8.3.0.2 allows direct uploads of compiled maps for DataPower platform (DPA files) during design time. Which of the following statements is correct? Compiled transformation maps are uploaded to the appliance using the:

- A. SNMP interface.
- B. WebGUI interface.
- C. XML Management Interface.
- D. CLI using the embedded secure shell.

Answer: C

Question: 62.

A solution implementer has created a WSProxy to allow clients to access backend web services. The web services may be altered and so the WebSphere DataPower appliance has been configured to subscribe to a UDDI Registry to retrieve the WSDLs for the backend web services and update the WSProxy accordingly. Any changes to the UDDI Registry must trigger immediate updates to the WSProxy. Which of the following will provide this functionality?

- A. Enable the XML Management interface to allow UDDI Subscription and then configure the UDDI Registry to announce updates to the DataPower URL /service/uddisubscription.
- B. Configure a Scheduled Processing Policy Rule in an XML Manager object using the Command Line Interface to run a UDDI Retrieve every time the UDDI Registry has been updated.
- C. Use the WebGUI to select the Retrieve Immediate option in the UDDI Subscription object associated with the WSProxy that defines the WSDL subscription to the UDDI Registry.
- D. Use the WebGUI to configure a Document Cache Policy in the XML Manager object associated with the WSProxy to have a TimeToLive of zero which will remove the caching of the WSDLs from the UDDI Registry.s

Answer: A

Question: 63.

A company has implemented a Multi-Protocol Gateway (MPGW) service to expose HTTP and MQ Interfaces via Front Side Protocol Handlers to an SOA Application. The company would like to monitor the web service at the operation level. There is one WSDL for the service. Which of the following configuration changes can be made to accommodate this new requirement?

- A. Migrate the service to WSProxy and implement SLM.
- B. Add an SLM FrontSide Handler to the MPGW.
- C. Front the existing MPGW with an XML Firewall service using SLM.
- D. Do nothing, MPGW implements SLM by default.

Answer: A

Question: 64.

Refer to the Exhibits.

Configure SSL Proxy Profile

Main

SSL Proxy Profile

Apply **Cancel**

Name *

Admin State enabled disabled

SSL Direction *

Reverse (Server) Crypto Profile *

Server-side Session Caching on off

Server-side Session Cache Timeout seconds

Server-side Session Cache Size entries (x 1024)

Client Authentication Is Optional on off

Always Request Client Authentication on off

Configure Crypto Profile

Main

Crypto Profile

Apply **Cancel** [Help](#)

Name *

Admin State enabled disabled

Identification Credentials

Validation Credentials

Ciphers

Options

Enable default settings
 Disable SSL version 2
 Disable SSL version 3
 Disable TLS version 1
*

Send Client CA List on off

A company requires that access to its SOA Application requires Authentication and Authorization using the Client's SSL Certificate's Distinguished Name. The company has constructed a WSProxy using the WSDL provided, and added an AAA Policy which uses "Subject DN of the SSL Certificate from the Connection Peer" in the Identity Extraction phase. An AAA Info File is used in the Authentication phase. An SSL Front End Protocol Handler was created for SSL access, see the exhibit for the SSL Proxy Profile and Crypto Profile used, and the client is specifying their SSL Public Certificate on the request submission. Initial tests fail with the following message:
wsgw (demographicWSP): Policy(validateClientSSLCertDN): xmlfile authentication failed with (clientssl, serial='*Cannot decode certificate*') What is causing this problem?

- A. SSL Proxy Profile should be 'forward'.
- B. SSL Proxy Profile should be 'two way'.
- C. Crypto Profile 'Send Client CA List' should be set to 'on'.
- D. Crypto Profile does not specify a 'Validation Credentials' Object.
- E. An AAA Info file cannot be used for SSL "Subject DN" Authentication and Authorization.

Answer: D

Question: 65.

A company needs to be conformant with Web Services Interoperability (WSI) Basic Profile 1.0. In order to enforce that policy in WebSphere DataPower, the solution implementer must:

- A. check off the conformance policy flag for Basic Profile 1.0.
- B. import a new WSPPolicy into the WSProxy object and check the compatibility flag.
- C. create a new conformance policy, and check off the appropriate Profiles check box.
- D. do nothing; DataPower always checks for conformance.

Answer: C

Question: 66.

Which of the following statements depicts the correct order for interpreting policy for a request flowing through a Web Service Proxy:

- A. 1) The defined WSPPolicy
2) The defined WSI Conformance Policy
3) The defined user policy
4) The defined processing rule
- B. 1) The defined processing rule
2) The defined user policy
3) The defined WSI Conformance Policy
4) The defined WSPPolicy
- C. 1) The defined proxy policy
2) The defined processing policy
3) The defined processing rule
4) The defined processing action
- D. 1) The defined processing rule
2) The defined user policy

- 3) The defined processing action
- 4) The defined WS Policy

Answer: A

Question: 67.

A solution implementer is configuring a WebSphere DataPower appliance to receive messages from a partner, and then pass them to a backend. Responses from the backend must also be transformed before being returned to the partner. The partner is requiring that nonRepudiation must be guaranteed on the responses it receives from the DataPower appliance. Which of the following would provide this functionality?

- A. Have the DataPower appliance insert a Digital Certificate provided by the partner in the original request in the response before returning it to the partner.
- B. Have the DataPower appliance transform the response and then digitally sign the response message using a Sign action before returning it to the partner.
- C. Have the backend server digitally sign the response which can then be verified on the DataPower appliance using a Verify action before returning it to the partner.
- D. Have the DataPower appliance use an Encrypt action configured with the Public Key inside a Digital Certificate provided by the partner in the original request to encrypt the response before returning it to the partner.

Answer: B

Question: 68.

A WebSphere DataPower appliance is being used to pass requests to an external partner before returning the responses to the original requesting application. The responses from the partner must be checked to guarantee nonrepudiation. Which of the following DataPower configurations for a Verify action on a response rule will provide this functionality?

- A. Use a Validation Credential containing the Public Key matching the Private Key used by the partner to sign the response.
- B. Use a Validation Credential containing the Certificate of the Certificate Authority which has issued the partner's Certificate.
- C. Use an Identification Credential containing the Private Key matching the Certificate that was sent to the partner in the request.
- D. Use an Identification Credential containing a Digital Signature that matches the Digital Signature contained in the response from the partner.

Answer: B

Question: 69.

A company has exposed a web service to both internal and external clients. Requests from internal clients are sent in plain text and requests from external clients are encrypted in accordance with the WS-Security specification. A single WSProxy service has been created using the WSDL describing the service. Which of the following shows what this company must do to accommodate both the plain text and encrypted requests in the same WSProxy service?

- A. Add a Decrypt action to the Default Request Rule for the WSProxy, with a Certificate object associated with the external client's private key.
- B. Provide the company's public certificate to the external client for use in encryption, create a Crypto Key object using the company's private key, and set the Decrypt Key for the WSProxy.
- C. Provide the company's public certificate to the external client for use in encryption, create a Crypto Key object using the company's public certificate, and use it to add a Decrypt action to the Default Request Rule for the WSProxy.
- D. Create a Crypto Certificate object using the external client's public certificate, create a Crypto Validation Credential (valcred) using the Crypto Certificate object, and add a Decrypt action to the Default Request Rule for the WSProxy using this valcred.

Answer: B

Question: 70.

A company is integrating with a web service that verifies credit card data. The service is defined using a WSDL and the service requires that several, but not all, of the elements within the request document are to be encrypted according to the WS-Security specification. Which of the following describes how this company should configure WebSphere DataPower to encrypt the message?

- A. Use a matching rule to identify the elements to encrypt together with a Crypto Key object containing the company's public certificate in an Encrypt action on the Default Request Rule.
- B. Use a matching rule to identify the elements to encrypt together with a Crypto Certificate object containing the service's public certificate in an Encrypt action on the Default Request Rule.
- C. Create a Document Crypto Map identifying the elements to encrypt, and use it together with a Crypto Key object containing the company's private key in an Encrypt action on the Default Request Rule.
- D. Create a Document Crypto Map identifying the elements to encrypt, and use it together with a Crypto Key object containing the company's public certificate in an Encrypt action on the Default Request Rule.
- E. Create a Document Crypto Map identifying the elements to encrypt, and use it together with a Crypto Certificate object containing the service's public certificate in an Encrypt action on the Default Request Rule.

Answer: E

Question: 71.

A company is receiving digitally signed messages from a client, and responding with messages that have been encrypted using the client's signing certificate. The Encrypt action has been configured with the 'Use Dynamically Configured Recipient Certificate' parameter set to 'on'.

Which of the following statements regarding this scenario is NOT true?

- A. The certificate selected in the 'Recipient Certificate' field will take precedence over the dynamic certificate if defined.
- B. The encrypt action will use the certificate defined in the variable var://context/transaction/encryptingcert to encrypt the message.
- C. The dynamic certificate used to encrypt the outgoing message can be userdefined using the syntax 'name:CertificateObjectName'.
- D. The public certificate used to encrypt the outgoing message will be automatically extracted from the incoming signed message in a Verify action.

Answer: A

Question: 72.

Refer to the Exhibit.

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP-ENV:Envelope
    xmlns:q0="http://cert.ibm.com"
    xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc"
    xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility">
    <SOAP-ENV:Header>
        <wsse:Security
            xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/secext">
            <wsse:BinarySecurityToken
                wsu:Id="CertX509Token"
                ValueType="wsse:X509v3"
                EncodingType="wsse:Base64Binary">
                FIfb3sgwMzA9CgWaxIBASysgEmtLhrrqaQrKhi...
            </wsse:BinarySecurityToken>
        ...
    </SOAP-ENV:Header>
    <soapenv:Body>
        <q0:showAllLocations/>
    </soapenv:Body>
</soapenv:Envelope>
```

This message will be sent to the IBM Certification System using WebSphere MQ. Which of the following options should be used in a AAA Policy to specify the Identity Extraction Method?

- A. MQ User Identifier from the X.509 certificate.
- B. Contact a WSTrust Server for a WSTrust Token.
- C. BinarySecurityToken Element from the WS-Security Header.
- D. Derivedkey UsernameToken Element from the WS-Security Header.

Answer: C

Question: 73.

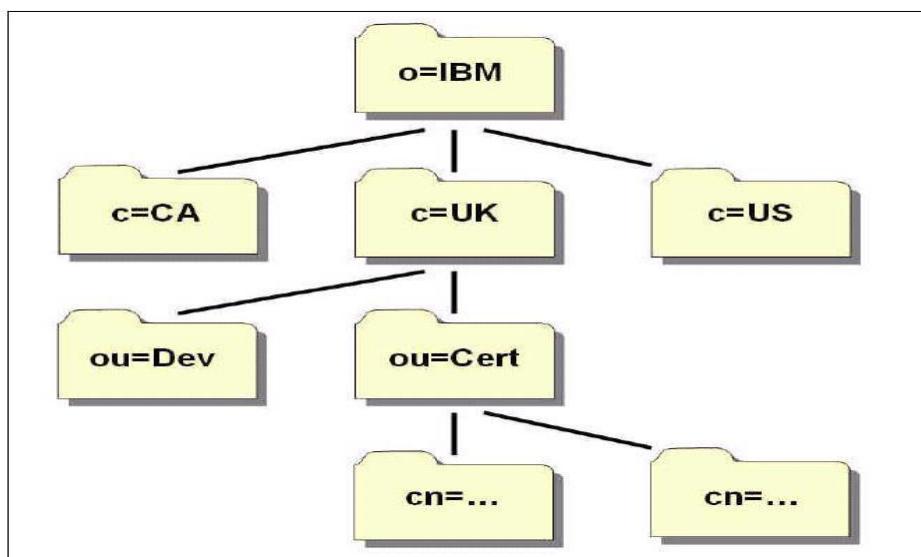
Which of the following are valid scenarios for Mapping Authentication Credentials and Mapping Requested Resources in a DataPower AAA Policy?

- A. Map the Requested Resource to Dynamically Route the Message to the correct backend.
- B. Map the Authenticated Credentials to insert an alternative Security Token in to the Message for Authorization.
- C. Map the Requested Resource from a legacy operation name to a new operation name to allow correct Authorization.
- D. Map the Authenticated Credentials from a DNformatted LDAP response to a username for Tivoli Access Manager (TAM) Authorization.
- E. Map the Authenticated Credentials to mediate the Security Headers of two different Protocols (for example from HTTP Headers to MQMD).
- F. Map the Authentication Credentials extracted from the Message before they are Authenticated to allow for Federated Identity Authentication.

Answer: CD

Question: 74.

Refer to the Exhibit.



A project needs to Authenticate IBM Certification users in the UK against the LDAP Directory described in the Exhibit.

Which of the following has the appropriate LDAP Query values?

- A. LDAP Prefix: cn= LDAP Suffix: o=IBM,c=UK,ou=Cert|Dev
- B. LDAP Prefix: cn= LDAP Suffix: ou=Cert,c=UK,o=IBM
- C. LDAP Prefix: cn= LDAP Suffix: o=IBM,c=UK,ou=Cert
- D. LDAP Prefix: o=IBM,c=UK,ou=Cert,cn= LDAP Suffix:

Answer: B

Question: 75.

A project needs to authenticate client messages which will contain either an HTTP Basic Authentication Header or a WS-Security UsernameToken and then insert an Open Standard security token into the message. Which of the following methods would achieve this?

- A. A custom stylesheet must be written to perform this functionality as it is not possible to authenticate a message unless you know which Security token is included.
- B. Add two AAA actions to a rule to authenticate each of the two Security tokens independently, one in each AAA action. Follow those actions with a Transform action to insert the Open Standard token.
- C. Add one AAA action that uses a AAA Policy to extract either of the two Security tokens by ticking both extraction mechanisms on the Extract screen and then uses Post Processing to insert the Open Standard security token.
- D. Add two AAA actions to a rule to authenticate each of the two Security tokens using "Pass Identity Token to the Authorize Step" for authentication and then "Always allow" for authorization to pass the authentication from the first AAA action to the second. Follow those actions with a Transform action to insert the Open Standard token.

Answer: C

Question: 76.

A customer wants to deploy WebSphere DataPower in the DMZ to authenticate and authorize client requests sent by an external partner company before passing these requests to a backend. The employees of the partner company change rapidly so individual partner employee credential data should not be held locally by the customer. To simplify the configuration of the DMZ, DataPower should perform authentication and authorization on the device. Which of the following configurations will allow this?

- A. Use an internal DataPower AAAInfo file to both authenticate and authorize the requests.
- B. Use the AAA authentication cache to hold an internal copy of the partner's LDAP identity server and use this to authenticate and authorize the requests.
- C. Have the partner insert a signed SAML token containing credential information into the request and configure DataPower to verify the signature of this token using an internal certificate.
- D. Configure DataPower to authenticate and authorize the requests received from the partner using Tivoli Access Manager and then insert a signed SAML token issued by Tivoli Federated Identity Manager into the requests.

Answer: C

Question: 77.

The implementation of Authentication and Authorization using WebSphere DataPower for a particular project requires a custom stylesheet. Which of the following is a valid reason for this?

- A. All DataPower functionality uses stylesheets so Authentication and Authorization always requires a stylesheet.
- B. The client message contains a custom token with security credentials in a proprietary format which is not supported by DataPower.
- C. The security data in the message has been encrypted using XML encryption and must be decrypted using a custom stylesheet so that Authentication and Authorization can be performed.
- D. The standard DataPower AAA Policy logs all rejections. This project will receive a very large number of messages which fail Authentication and therefore will generate excessive logging information. A custom stylesheet must be used to disable this logging.

Answer: B

Question: 78.

for virusscanning message attachment , WebSphere DataPower appliances use which protocol to support integration with 3rdparty virus scanners?

- A. SOAP (Simple Object Access Protocol)
- B. MVIP (MultiVendor Integration Protocol)
- C. IMAP (Internet Message Access Protocol)
- D. ICAP (Internet Content Adaptation Protocol)

Answer: D

Question: 79.

A company has an extensive list of Miscellaneous XML Threats that they require protection from. This list includes:

- XML Entity Expansion and Recursion Attacks
- XML Wellformednessbased
- Parser Attacks
- Memory Space Breach and Buffer Overflow Attacks
- Public Key DoS Attacks
- Resource Hijack Attacks
- Schema Poisoning Attacks

What must this company do to protect SOA Applications exposed via a WSDL and a WSProxy service?

- A. Enable the WSProxy's "SQL Injection Protection"
- B. Enable the WSProxy's "XML Virus (XVirus) Protection"
- C. Enable the WSProxy's "Single Message XML Denial of Service (XDoS) Protection"
- D. Enable the WSProxy's "Multiple Message XML Denial of Service (MMXDoS) Protection"
- E. Nothing is required

Answer: E

Question: 80.

A company wants to implement an XMLbased service that returns customer data. Which of the following configuration steps in an Multi-Protocol Gateway (MPGW) can be used to prevent malicious requests from returning data for multiple customers?

- A. Set Loop Detection to 'on' in the Advanced Settings tab of the MPGW.
- B. Set the XML Maximum Nodes parameter to '1' in the XML Threat Protection tab of the MPGW.
- C. Insert a Filter action on the response rule and select the SQL Injection filter from the dropdown list.
- D. Insert a Validate action on the response rule and assign a schema that restricts the response to a single record.

Answer: D

Question: 81.

A company is receiving malicious web service payloads that contain thousands of extraneous XML namespaces. What can be done in a WebSphere DataPower service to prevent this type of attack?

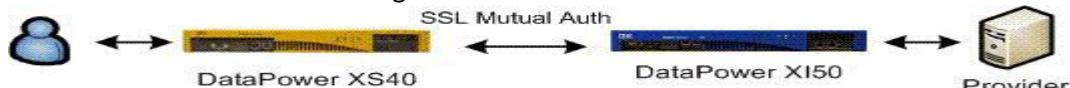
- A. No action must be taken; this attack will be automatically prevented.
- B. Set the Resolve All Namespaces parameter to 'on' in the Advanced tab.
- C. Set a reasonable limit on the XML Maximum Distinct Namespaces parameter in the service's XML Manager.
- D. Insert a Filter action in the service's request rule and select store:///namespacefilter.xsl from the dropdown list.

Answer: C

Question: 82.

Refer to the Exhibit.

A company is bridging external consumer requests to an internal service using a WebSphere DataPower XML Security Gateway XS40 as a DMZ gateway and a WebSphere DataPower Integration Appliance XI50 as an internal ESB. Each device uses a Multi-Protocol Gateway service; the two services communicate using HTTPS with SSL serverside authentication only. The company wants to ensure that requests to the XI50 are coming through the XS40, and the enterprise security architect has selected SSL mutual authentication as the appropriate technology, as shown below. Crypto Profiles consists of an Identification Credential (IDCRED) and/or a Validation Credential (VALCRED) and are defined as forward or reverse in the SSL proxy profile depending on its use as an SSL client or SSL server. See below for the target architecture.



How will the WebSphere DataPower implementer change the configuration from oneway server side authentication SSL to mutual authentication SSL, as shown above?

- A. Add an IDCRED to the XI50 crypto profile and a VALCRED to the XS40 crypto profile.
- B. Add an IDCRED to the reverse crypto profile and an VALCRED to the XI50 crypto profile.
- C. Add an IDCRED to the reverse crypto profile and an VALCRED to the forward crypto profile.
- D. Add a VALCRED to the reverse crypto profile and an IDCRED to the forward crypto profile.

Answer: D

Question: 83.

A company wants to ensure that all its backend SOAP/HTTPS services are protected from unauthorized internal access. The security architect has recommended SSL mutual authentication to be configured from WebSphere DataPower to the backend services. The SSL profile for mutual authentication is correctly configured on DataPower and the implementer wants to confirm if the backend services have configured their mutual authentication correctly. A successful transaction is run through DataPower to the backend services.

Which of the following tests could the solution implementer use to confirm that mutual authentication is working correctly end-toend?

- A. There are no warnings in the DataPower logs so mutual authentication is successfully being performed
- B. There are no errors in the DataPower logs therefore mutual authentication is successfully being performed
- C. Run a packet capture on the interface communicating with the backend and observe the SSL handshake includes the optional client authentication steps.
- D. Run a packet capture on the interface communicating with the backend and observe the SSL handshake includes the optional server authentication steps.
- E. Remove the Identification Credential from the forward crypto profile on DataPower; if the request does not succeed, the backend mutual authentication is correctly configured.

Answer: CE

Question: 84.

A company is using a DataPower Multi-Protocol Gateway (MPGW) service to dynamically choose between two thirdparty backend service providers, each using SSL for security. Which of the following would be the MOST secure option for the company to connect to either service?

- A. The MPGW cannot be used at runtime to access two backend service providers.
- B. Implementer uses an SSLProxyProfile that uses a validation credential that contains both the service certificates.
- C. Implementer uses an SSLProxyProfile that uses an identification credential that contains both the service certificates.
- D. Implementer sets var://service/routingurl and var://service/routingurlsslprofile in a custom stylesheet dynamically picking the SSLProxyProfile based on which service is requested.

Answer: D

Question: 85.

Connectivity to which of the following protocols can be directly protected with SSL mutual authentication in WebSphere DataPower using firmware V3.8.1?

- A. MQ queue manager
- B. NFS
- C. SQL Data Source
- D. IMS Connect

Answer: A

Question: 86.

Which is NOT a valid characteristic of a Front Side Handler?

- A. A single Front Side Handler can accept multiple requests from the client over multiple protocols.
- B. Each instance of an HTTP, HTTPS, FTP, or raw XML Front Side Handler listens to a specific pair of IP address and port number.
- C. Each WebSphere JMS or TIBCO EMS Front Side Handler refers to a JMS server and the associated GET and PUT queues.
- D. Each WebSphere MQ Front Side Handler refers to a WebSphere MQ queue manager and the associated PUT and GET queues used for communication.
- E. Front Side Handlers provide protocolspecific connection points to clients requesting services from a backend server.

Answer: A

Question: 87.

A customer would like to use WebSphere DataPower to process messages from 3 different systems. The protocols for each system are: HTTP, HTTPS, and MQ. In order to save time, the customer would like to have a single Multi-Protocol Gateway (MPGW) handle all of the messages. The advice to the customer should be as follows:

- A. Create 3 Front Side Handlers, one for each protocol.
- B. Create 1 shared HTTP/HTTPS Front Side Handler, and 1 MQ Front Side Handler.
- C. Only 1 Front Side Handler should be used for each MPGW.
- D. All Front Side Handlers for a MPGW should be of the same protocol type.

Answer: A

Question: 88.

A company wants to use a Multi-Protocol Gateway (MPGW) to process inbound XML messages it receives over WebSphere MQ and dynamically route these messages to specific backend systems. The MPGW will use a lookup table to determine which messages to route to which backends. In total there are 10 inbound queues and 3 queue managers. What is the minimum number of front side handlers that can be used for this MPGW?

- A. 1
- B. 3
- C. 10
- D. 30

Answer: C

Question: 89.

A solution implementer is configuring a Multi-Protocol Gateway to route messages to one of a number of backend servers. The backend servers use different protocols so the routing must include details of the protocol to be used for each particular request. Which of the following will provide this functionality?

- A. Using the extension function dp:xsettarget.
- B. Setting the variable var://service/routingurl.
- C. Selecting a Route action with an XPath Routing Map.
- D. Selecting a Route With Variables action with the variable field set to var://service/URLout.
- E. Setting the variables var://service/URI for the server address and var://service/protocolmethod for the protocol type.

Answer: B

Question: 90.

A solution implementer needs to split a request message into two and send one part to a WebSphere MQ backend and then the second part to a backend listening over HTTP. The responses from both backends must then be aggregated and returned to the requesting client. Which of the following configurations will provide this functionality?

- A. A Transform action containing a dp:urlopen tag to send the first message, followed by a Transform action and a Results action to send the second message.
- B. A Transform action containing a dp:xsettarget tag to send the first message, followed by a Transform action and a Results action to send the second message.
- C. A Transform action containing code to set the var://service/routingurl variable to send the first message, followed by a Transform action and a Results action to send the second message.
- D. A Transform action followed by a Results action with the Destination field containing the locations of the backends and the MultiWay Results Mode on the advanced tab set to Require All to send the same message to both URLs.

Answer: A

Question: 91.

A solution implementer is using a WSProxy to send requests from a client to a backend server. A dp:settarget() element in a Transform action on a request rule is being used to dynamically route the message to one of two backends dependent on XML elements within the request message. The Type of the WSProxy has been set to Dynamic Backend. A URL Rewrite Policy has been configured to replace the URI sent from the client with the format required by the backend server. When the service is tested it is found that the Client URI is being sent to the backend. Which of the following would explain this behavior?

- A. The Propagate URI property of the WSProxy must be disabled.
- B. The Force Destination URI property of the Result action must be enabled.
- C. URL Rewrite Policies are not valid for a WSProxy the remote endpoints for each WSDL used must be configured instead.
- D. It is not possible to use a dp:settarget() element with a WSProxy a Route action must be used to achieve this functionality.

Answer: A

Question: 92.

A solution implementer needs to send a request containing business data to a backend using an FTP PUT. Which of the following configurations will provide this functionality?

- A. An FTP server handler object with mode set to Transparent to send the request straight through to the backend.
- B. A Route action set to the backend server address followed by a Transform action to provide the business data in the correct form.
- C. A Transform action with a dp:urlopen tag enclosing the data to be sent and the target field set to the backend server address.
- D. An FTP poller object with the destination field set to the backend server address to send the request message to the backend and poll for a response.

Answer: C

Question: 93.

A company is using WebSphere MQ and would like to configure WebSphere DataPower to provide high availability across queue managers. Which of the following objects need to be configured on the appliance to make use of this feature?

- A. MQ Queue Manager Group should be used which includes Primary and Backup MQ Queue Manager objects that provide automatic connectivity to the active MQ instance.
- B. Multiple Front Side Handlers must be associated with the Multi Protocol Gateway service. Each Front Side Handler uses a Queue Manager object connecting to one of the instances of the Queue Manager.
- C. No specific configuration is required on the DataPower appliance. High availability across queue managers is a WebSphere MQ configuration and is transparent to DataPower.
- D. DataPower currently cannot provide high availability across queue managers.

Answer: A

Question: 94.

A company is using WebSphere MQ to mediate messages between their frontoffice and backoffice applications. WebSphere DataPower appliances, as a part of the messaging hub solution, are responsible for processing certain types of messages arriving on designated queues on the same Queue Manager. This is a high performance environment and the key requirement for DataPower is to read messages from a designated queue and place copies of the message to the designated backend queues on the same Queue Manager under a single unit of work to prevent message loss. As a solution implementer, which of the following configuration options would be MOST optimized for this environment?

- A. Create MQ RFH2 headers to create an MQ distribution list including all designated backend queues.
- B. Create MQ MQOD headers to create an MQ distribution list including all designated backend queues.
- C. Use the required number of AsyncResults actions to the designated queues and use Event Sink action to ensure all messages were written successfully.
- D. Use a context variable to create a URL nodeset and use a single AsyncResults action to send messages in a single action. No Event Sink is necessary for performance reasons.

Answer: B

Question: 95.

A Multi-Protocol Gateway (MPGW) service is bridging a message to an asynchronous backend protocol (such as WebSphere MQ, WebSphere JMS, or Tibco EMS). Which of the following properties apply to all transactions and can determine how long the MPGW will wait for a response message from the backend?

- A. The "Back Side Timeout" parameter of the MPGW.
- B. The '?QueryTimeout=' query parameter on a dynamic Backend URL.
- C. The "Back Persistent Timeout" parameter of the MPGW.
- D. The "Timeout" value associated with the MPGW's XML Manager User Agent settings.

Answer: A

Question: 96.

A company has implemented a data masking Multi-Protocol Gateway (MPGW) named Log MPGW. Log MPGW is called from another MPGW named ESB MPGW using a urlopen extension function call with option 'response=ignore' set. The service provided by Log MPGW to ESB MPGW is noncritical and should impact the performance of ESB MPGW as little as possible. Which of the following are correct?

- A. The Log MPGW should use 0.0.0.0 in its front side handler to prevent blocking of the urlopen call.
- B. The urlopen call from ESB MPGW will never block and there is no concern about impacting the performance of the core ESB flow.
- C. The backside timeout on the ESB MPGW should be changed to limit any possible blocking of the urlopen calls to the logging service.
- D. A timeout value on the urlopen call should be set reasonably to limit any possible blocking of the urlopen calls to the logging service.
- E. The transform action using the urlopen call on ESB MPGW can be made asynchronous to ensure that the performance of the core ESB flow is not impacted.

Answer: DE

Question: 97.

A customer wants to create a web service that uses SOAP over HTTP on the front end, and use WebSphere MQ on the backend so as to integrate with an existing legacy application. The customer wants to reuse an existing Web Service Proxy and just add the new WSDL to the existing proxy to leverage the existing policies in place. In order to make this work, the customer should:

- A. use the Backend URL MQ helper to build the proper Backend URL.
- B. add the new WSDL and use the endpoint referenced by the WSDL.
- C. add the new WSDL and create a new Backend URL using the dpmq:// syntax.
- D. add the new service operations to the existing WSDL and create a new MQ Backend URL.

Answer: C

Question: 98.

Using the WebSphere JMS feature, which of the following operations can the WebSphere DataPower appliance perform?

- A. Only act as a client messaging service.
- B. Only act as a sender of WebSphere JMS messages.
- C. Act as both a client and a sender of WebSphere JMS messages.
- D. Act as a WebSphere JMS server.

Answer: C

Question: 99.

A company requires that a service authenticate the user identity in a WebSphere MQ protocol header. Which of the following is correct?

- A. Use the AAA file to extract the MQ header.
- B. Use LDAP to correlate the header field with the user name.
- C. Use the Processing Metadata object to retrieve the MQ header.
- D. Define a valid identity in the MQ Queue Manager object User Name field.

Answer: C

Question: 100.

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

- A. Set syncpoint='true' on the backend HTTP URL.
- B. Set the Queue Manager object's 'Units Of Work' property to "1".
- C. The DataPower device utilizes an MQ Client, syncpoint cannot be implemented.
- D. The DataPower device utilizes an MQ Client, syncpoint is implemented by default.
- E. 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.

Answer: B

Question: 101.

A WebSphere DataPower service is receiving a message in Comma Separated Value format and needs to send it to a backend expecting a SOAP Request. Which of the following is an appropriate action that could be used to convert this message?

- A. Transform (xform)
- B. Text Transform (textform)
- C. Binary Transform (xformbin)
- D. SOAP Transform (soapform)

Answer: C

Question: 102.

Which of the following needs to take place to enable designtime testing of a WebSphere Transformation Extender map on a WebSphere DataPower appliance?

- A. Import the WTX.zip file containing WebSphere DataPower helper services onto the appliance.
- B. Install the WebSphere Transformation Extender drivers on the WebSphere DataPower appliance.
- C. Run the deployToDataPower.bat CLI command to send a WTX map from Design Studio to a WebSphere DataPower appliance.
- D. Upload the DBA file onto the WebSphere DataPower Appliance and select DBA WebSphere Transformation Extender Map Mode.

Answer: A

Question: 103.

A customer would like to use an XSL transform specified in the incoming XML request to transform that document. Which of the following would be the appropriate processing action to use in this case?

- A. Transform (xform)
- B. Transform PI (xformpi)
- C. Transform Binary (xformbin)
- D. Convert HTTP (converthttp)

Answer: B

Question: 104.

A company has defined a Multi-Protocol Gateway (MPGW) to bridge between a REST interface and a SOAP interface. The incoming GET is converted to a POST to the web service. The request must be sent as an inline external SOAP call and therefore the MPGW must be set to skip the backend server. Which of the following actions is NOT a necessary step in this process?

- A. Transform the URL parameters into a SOAP request.
- B. Use a Convert HTTP Params action to parse the URL.
- C. Set the var://service/protocolmethod variable to SOAP.
- D. Select the POST HTTP method in the Results action making the SOAP call.

Answer: C

Question: 105.

A customer has created a Multi-Protocol Gateway with a request type of JSON. Within the request rule, an action needs access to the input in JSONx format. Which of the following are methods for retrieving this data in XML?

- A. Set the Convert Input property in the Advanced tab to On.
- B. Set the action's input context to the value '__JSONASJSONX'.
- C. Insert a Fetch action, and select JSONx as the Output Type on the Advanced tab.
- D. Insert a Transform action, and select store:///jsontojsonx.xsl from the dropdown list.
- E. Insert a Convert HTTP action, and select a Default Encoding of 'JSON' in the Input Conversion Map.

Answer: BE

Question: 106.

A company converting a legacy billing application to the WebSphere DataPower implementation would like to reuse an existing Oracle database and its associated stored procedures as much as possible. The stored procedure may return multiple data sets. One of the stored procedures returns a cursor data type. The stored procedure must not return more than a maximum of 128 KB of data. The database is updated through a separate batch process and must not be modified through DataPower. The company distinguishes between nulls and empty strings returned since they have different interpretations to the business. Which of the following statements is correct?

- A. DataPower can limit the size of the data returned from queries at the Data Source level.
- B. Restricting the data source to be readonly must be done at the database level as this is not supported by DataPower.
- C. Some of the stored procedures may need to be rewritten since DataPower does not differentiate between null and empty strings.
- D. Some of the stored procedures may not be able to be reused because DataPower does not support stored procedures that return multiple data sets.

Answer: A

Question: 107.

A company wants to query a database to obtain authorization data for an authenticated user from a DB2 database. The parameterized query is of the form 'SELECT * FROM AUTH_ATTRIBUTE_TABLE WHERE REQUESTER_ID=?'.

Which of the following applies?

- A. Use a SQL Action to obtain authorization data.
- B. Use dp:sqlexecute() extension function to obtain authorization data.
- C. Use <dp:sqlexecute> extension element to obtain authorization data.
- D. The 'select * fromwhere id=?' type of parameterized query is not supported in DataPower.

Answer: C

Question: 108.

An SLM Policy has been associated with a Web Service Gateway Service to restrict access to a backend web service if one of a number of conditions has been met. The conditions are described in a series of SLM statements. What Evaluation Method must be selected in the SLM Policy to ensure that every SLM statement is checked until a throttle condition is executed?

- A. 'terminateatfirstfilter'
- B. 'terminateatfirstrefuse'
- C. 'terminateatfirstaction'
- D. 'terminateatfirstreject'

Answer: D

Question: 109.

A company wants to use the WebSphere DataPower SLM functionality with a schedule to monitor the number of messages being processed for a particular operation on week days in a Web Service Proxy. Messages should not be counted if they fail Signature Verification, but should be counted whether they pass Authentication and Authorization or not. Which of the following configurations would allow this?

- A. Define an SLM Request Count Monitor on the SLM tab of the Web Service Proxy.
- B. Define a Processing Rule for the particular operation with a Verify action, an SLM action with an appropriate SLM statement and then a AAA action.
- C. Define a AAA Policy with both Authorized Counter and Rejected Counter monitors in the Post Processing section and then attach this to the Advanced tab on the Web Service Proxy.
- D. Define a Processing Rule for the particular operation with a Verify action then a AAA action with a AAA Policy with both Authorized Counter and Rejected Counter monitors in the Post Processing section.

Answer: B

Question: 110.

A company wants to use the WebSphere DataPower SLM functionality to monitor messages from particular partners for particular backend functionality. The company needs to set up Credential and Resource Classes. Which of the following configurations would meet the requirements?

- A. Credential: front-URL (the URL the Client requested)
Resource: destination-URL (the URL sent to the Backend Server)
- B. Credential: aaa-username (the Username of the Client)
Resource: aaa-mapped-credential (the mapped Group Name of the Client)
- C. Credential: client-ip (the IP address of the Client)
Resource: wsdl-operation (the Web Service Operation the Client requested)
- D. Credential: host-name (the Ethernet interface the request was received on)
Resource: request-header (an HTTP Header present in the message)

Answer: C

Question: 111.

A company wants to use the WebSphere DataPower SLM functionality to enforce service levels for access to a backend web service. Which of the following Count and Latency monitor pairs are valid within SLM statements?

- A. count-all and latency-internal
- B. count-total and latency-errors
- C. count-reject and latency-total
- D. count-errors and latency-average

Answer: A

Question: 112.

In order to notify of policy violations for incoming web services, the solution implementer must:

- A. define a WS Policy by setting the policy's Enforcement Mode to filter, create a Policy Parameter Set, and attach a Policy Source.
- B. define a WS Policy by setting the policy's Enforcement Mode to Reject, create a Policy Parameter Set and use Policy References.
- C. select WS Conformance and create an Operation Policy Conformance policy in the service.
- D. enable all Subjects in the WS Policy and select the Log Target to use for notifying the user.

Answer: A

Question: 113.

Review the following default security profile.

```
<?xml version="1.0" encoding="UTF8"?>
<wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:sp="http://docs.oasisopen.org/wssx/
  org/wssx/
  WS-Securitypolicy/
  200512"
  xmlns:wsu="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-WS-Securityutility1.0.
  xsd">
  <dpe:summary xmlns="" xmlns:dpe="http://www.datapower.com/extensions">
    <dppolicy:domain xmlns:dppolicy="http://www.datapower.com/policy">
      http://docs.oasisopen.org/wssx/
      WS-Securitypolicy/
```

```
200512
</dppolicy:domain>
<description>
Implements WAS Web Service WS-Security Default
</description>
</dpe:summary>
<wsp:Policy wsu:Id="bindingpolicy">
<sp:AsymmetricBinding>
<wsp:Policy>
<sp:InitiatorToken>
<wsp:Policy>
<sp:X509Token
sp:IncludeToken="http://docs.oasisopen.
org/wssx/
WS-Securitypolicy/
200512/IncludeToken/AlwaysToReci
pient">
<wsp:Policy>
<sp:WssX509V3Token10/>
</wsp:Policy>
</sp:X509Token>
</wsp:Policy>
</sp:InitiatorToken>
<sp:RecipientToken>
<wsp:Policy>
<sp:X509Token
sp:IncludeToken="http://docs.oasisopen.
org/wssx/
WS-Securitypolicy/
200512/IncludeToken/AlwaysToInitiat
or">
<wsp:Policy>
<sp:WssX509V3Token10/>
</wsp:Policy>
</sp:X509Token>
</wsp:Policy>
</sp:RecipientToken>
<sp:AlgorithmSuite>
<wsp:Policy>
<sp:Basic128Rsa15/>
</wsp:Policy>
</sp:AlgorithmSuite>
<sp:Layout>
<wsp:Policy>
<sp:Strict/>
</wsp:Policy>
</sp:Layout>
<sp:IncludeTimestamp/>
```

```
<sp:EncryptSignature/>
</wsp:Policy>
</sp:AsymmetricBinding>
</wsp:Policy>
<wsp:Policy wsu:Id="request_parts">
<sp:SignedParts>
<sp:Body/>
<sp:Header Namespace="http://schemas.xmlsoap.org/ws/2004/08/addressing"/>
<sp:Header Namespace="http://www.w3.org/2005/08/addressing"/>
</sp:SignedParts>
<sp:EncryptedParts>
<sp:Body/>
</sp:EncryptedParts>
</wsp:Policy>
<wsp:Policy wsu:Id="response_parts">
<sp:SignedParts>
<sp:Body/>
<sp:Header Namespace="http://schemas.xmlsoap.org/ws/2004/08/addressing"/>
<sp:Header Namespace="http://www.w3.org/2005/08/addressing"/>
</sp:SignedParts>
<sp:EncryptedParts>
<sp:Body/>
</sp:EncryptedParts>
</wsp:Policy>
</wsp:Policy>
```

Which of the following actions would satisfy the above policy?

- A. Encrypt and sign the body of the message.
- B. Encrypt, sign and use an X.509 Token in the message.
- C. Encrypt the body, sign the Parts, and use a UsernameToken in the message.
- D. Encrypt the body and header. Sign BOTH body and header.

Answer: B

Question: 114.

A new service is being developed and WebSphere DataPower is tasked with security for the web service. The use of WS Policy is requested. In order to enforce the security requirements and communicate them to the client, the solution implementer should:

- A. document the security, document the WS Policy and send the documentation to the client.
- B. implement a Web Service Proxy that complies with the documented security guidelines.
- C. implement a Web Service Proxy, attach a WS Policy that complies with security guidelines, send WSDL to client.
- D. change the original WSDL and add the recommended security guidelines, then send the new WSDL to client.

Answer: C

Question: 115.

A customer needs message privacy and message integrity on a given transaction, and prefers the use of WS Policy. WebSphere DataPower must receive a username from each user, but no authentication is required. In order to implement this, without additional custom work, the solution implementer must:

- A. use WS Policy with UsernameToken, Encryption and Signature enforced.
- B. use WS Policy with Encryption, Signature and pass the username in the message body.
- C. use an Encrypt and Sign Action in the request, followed by a Decrypt and Verify Action in the response.
- D. use a basic authentication header, then use the default encryption and signature inherent in the WSProxy.

Answer: A

Question: 116.

What is the difference between WebSphere Service Registry and Repository (WSRR) Subscription and WSRR Saved Search Subscription?

- A. WSRR Subscription does not support automatic polling for newer versions. WSRR Saved Search supports automatic polling of the WSDL
- B. WSRR Subscription requires a direct reference to a service document such as a WSDL or Concept and namespace. WSRR Saved Search only requires users to specify a WSDL name
- C. WSRR Subscription supports WS Policy artifacts created in WSRR. WSRR Saved Search support does not support WS Policy artifacts and only supports indirect reference to WSDL or concepts.
- D. WSRR Subscription requires a direct reference to a service document such as a WSDL or Concept and namespace. WSRR Saved Search does not require a direct reference to the WSDL, concept or namespace and requires users to specify a Saved Search parameter only

Answer: D

Question: 117.

A WSProxy Service is configured with a subscription to a Concept in WebSphere Service Registry and Repository (WSRR). A new WSDL is added to the Concept from the WSRR interface.

What options are available for updating the WSProxy to include the new WSDL?

- A. Open the WSRR Server object and set the Update field to Auto.
- B. Navigate to the Advanced Proxy Settings tab and click 'Poll Now'.
- C. Navigate to the WSRR Subscription Status page and click 'Synchronize'.
- D. Set the Synchronization Method to Poll and then wait for the Refresh Interval.
- E. In the WSRR interface, open the Concept page and click 'Deploy to DataPower'.

Answer: CD

Question: 118.

A solution implementer migrated a Multi-Protocol Gateway (MPGW) from a WebSphere DataPower Integration Appliance XI50 in the development environment to a DataPower XI50 in the test environment. The MPGW uses a static backend server. The purpose of this migration was to update the version of the MPGW in the test environment, with changes made in the development environment. Prior to the migration, the version of the MPGW in the test environment was connecting to the relevant backend server successfully. Since the migration however, the MPGW is no longer able to connect to the backend server.

Which of the following is the MOST logical approach to debug this issue?

- A. Ping the address of the test environment backend.
- B. Restart the DataPower domain in the test environment.
- C. Check that the Backend URL in the MPGW holds the appropriate server address.
- D. Start again and migrate the MPGW from the development environment to the test environment.

Answer: C

Question: 119.

A customer is working through an issue where they are experiencing intermittent connection failures when connecting to a backend. The solution implementer has determined that, by network design, WebSphere DataPower must use the eth2 network to connect to the backend.

Note the Backend URL is currently set to: `http://a.example.com/userSubmissions:8221`

Which of the following would ensure that all traffic destined for this backend goes via eth2?

- A. Create a host alias.
- B. Create a static route.
- C. Change the Backend URL to `http://enginerom.company.com/userSubmissions:8221[eth2]`.
- D. Change the Backend URL to `http://enginerom.company.com/userSubmissions:8221{eth2}`.

Answer: B

Question: 120.

Which of the following statements are TRUE about the product's network packet capture troubleshooting feature?

- A. Packet capture files are stored on the device's 'temporary:' directory.
- B. Packet captures must be started from the 'default' Application Domain.
- C. Packet capture cannot be configured to capture data from particular IP addresses and ports.
- D. Clicking the 'Stop Packet Capture' button causes the packet capture to terminate immediately and the capture data is discarded.
- E. The device's packet capture files are in 'pcap' format and are readable by any 'pcap' compliant application, such as 'tcpdump' or 'Ethereal / Wireshark'.
- F. Packet capture works by placing the specified Ethernet interface in Promiscuous Mode, thereby capturing all traffic appearing on the Ethernet segment to which the interface is attached.

Answer: ABE

Question: 121.

A customer has a Log Target configured to upload log files to a remote server for analysis and correlation by the customer's centralized log correlation system. To prevent log files uploaded from the device to this central system from being tampered with once they arrive on the central log correlation system, which action should be taken in the Log Target configuration?

- A. Specify a "Signing Mode" on the Log Target.
- B. Specify a Sign Action in the processing policy.
- C. Specify a secure "Upload Method", either SSH or SCP, on the Log Target.
- D. Specify an "Event Suppression Filter" to suppress confidential log file events on the Log Target.

Answer: A

Question: 122.

A customer's WebSphere DataPower deployment has the following operational logging requirements:

Every network or systemlevel error event should generate an SNMP Trap to the customer's Tivoli Management Console. Every DataPower Management Interface (WebGUI, CLI, and SOMA) access attempt event (success *and* failure) should generate a SOAP call to the customer's IDS (Intrusion Detection System). Messagelevel Authentication/Authorization failure events should generate an SNMP Trap to the customer's Tivoli Management Console. Events generated by the device's Certificate Monitor when a digital certificate is nearing expiration need to generate 'syslog' messages to the customer's syslog host named 'sysloghost a. example.com'.

Events generated by inbound messages with invalid message encodings need to generate 'syslog' messages to the customer's syslog host named 'sysloghostb. example.com'.

What is the minimum number of Log Targets that need to be configured in the DataPower logging system to accomplish this?

- A. 3
- B. 4
- C. 5
- D. 6

Answer: B

Question: 123.

Which of the following is NOT a valid target for realtime event logs on WebSphere DataPower?

- A. JMS
- B. SOAP
- C. SNMP
- D. Console
- E. syslogng

Answer: A

Question: 124.

A customer would like to use the WebSphere DataPower WebGUI interface to view the event logs for a service that is being executed. After each refresh of the interface, the log should be updated to view only the unviewed events; there is no need for these logs to be persisted. Which of the following configurations would allow these requirements?

- A. Create a log target with a 'cache' target type.
- B. Create a log target with a 'console' target type.
- C. Choose 'realtime' from the filter dropdown on the system log page.
- D. Choose 'all' from the View Log Events section of the Troubleshooting Panel.

Answer: A

Question: 125.

A company is hosting a service exposed through WebSphere DataPower to accept transactions from its business partners. The company is facing intermittent but recurring error "0x01130006 Failed to establish a backside connection". The company wants to log a record of the errorhandling and create a DataPower error report as soon as the error occurs. Which of the following actions does the company need to perform to most effectively meet these requirements?

- A. Define a syslog log target that subscribes to 0x01130006 and a log monitor defined on syslog that runs a script to create a DataPower error report.
- B. Define a syslogng log target that subscribes to 0x01130006 and a log monitor defined on syslog that runs a script to create a DataPower error report.
- C. Define an SNMP trap that subscribes to 0x01130006 to send a message to a trap receiver program that runs a script that creates a DataPower error report.
- D. Define a log target with an event trigger that subscribes to event 0x01130006 at log level notice that runs a CLI command to create a DataPower error report.

Answer: D

Question: 126.

Refer to the Exhibit.

Event Triggers					
Message ID	Reg Exp	Only Once	Only this Trigger	CLI Command	
0x80400036		on	on	int eth0; packet-capture temporary:///mypcap	
0x80400036		on	on	int eth0; no packet-capture temporary:///mypcap	

A company would like to set event triggers to create packet captures for their intermittent errors. How many files called mypcap would be created in the temporary directory based on the event trigger defined in the exhibit above?

- A. 0
- B. 1
- C. 2
- D. unlimited

Answer: B

Question: 127.

Refer to the Exhibit.

System Log							
C Refresh Log		Target:	default-log	Filter:	(none)	notice	
time ▾	category	level	tid	dir	client	msgid	message
current time: 16:08:38 on 2009-04-18							
Sat Apr 18 2009							Show last 50 100 all
16:07:06	mgmt	notice	15408	<	9.48.32.199	0x80000001	xslproxy (web-mgmt): Configuration Import completed: 0/0 files and 11/12 objects and 0/0 data-sets successfully imported into Domain ExampleDomain
16:07:06	mgmt	error	15408	<	9.48.32.199	0x80000001	mpgw (ExampleGateway): Import failed.
16:07:06	mgmt	error	31			0x8100000b	mpgw (ExampleGateway): Event-Code (0x113002d) - Source Protocol Handler Required
16:07:06	cli	error					==== Line 8: front-protocol fsh-ExampleQueueManager
16:07:06	cli	error					fsh-ExampleQueueManager is not valid

A consultant is engaged with an existing customer for a project that requires the deployment of four new WebSphere DataPower XML Security Gateway XS40s to an existing pool of five WebSphere DataPower Integration Appliance XI50s. In order to keep all nine devices in sync with the same implementation, the customer provides a domain configuration export from one of the existing XI50s. After importing the domain to one of the new XS40s, the error log shows the information in the exhibit. Which of the following describes the reasons for this error?

- A. Configurations from XI50s are never portable to the XS40s
- B. A Queue Manager object must be configured in the Default Domain.
- C. The configuration provided for the XS40 is using XI50 exclusive features.
- D. The error message was left over from the original device and can be ignored.

Answer: C

Question: 128.

Refer to the Exhibit.

21:39:55	mpgv	error	1671442	a	0x01130006 mpgv (OpalMPGW): Failed to establish a backside connection
21:39:55	mpgv	error	1671442		0x80e00126 mpgv (OpalMPGW): Valid backside connection could not be established: Failed to establish a backside connection
21:39:40	ftp	debug	1671442		0x80e0009d mpgv (OpalMPGW): FTP Client: opening data connection to xx.xx.111.126 port 22634
21:39:40	ftp	debug	1671442		0x80e0009c mpgv (OpalMPGW): FTP Client: command 'STOR http://opalfw-test-2009-06-15T21:39:40:00.xml' sent
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: reply code 229 in state 'EPSV'. Reply text: ' Entering Extended Passive Mode(22634)'
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: command 'EPSV' sent
21:39:40	ftp	debug	1671442		0x80e00096 mpgv (OpalMPGW): FTP Client: reply code 200 in state 'MODE'. Reply text: ' MODE S ok.'
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: command 'MODE S' sent
21:39:40	ftp	debug	1671442		0x80e00096 mpgv (OpalMPGW): FTP Client: reply code 200 in state 'TYPE'. Reply text: ' Type set to 1.'
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: command 'TYPE I' sent
21:39:40	ftp	debug	1671442		0x80e00096 mpgv (OpalMPGW): FTP Client: reply code 250 in state 'CWD'. Reply text: ' CWD command successful.'
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: command 'CWD sales' sent
21:39:40	ftp	debug	1671442		0x80e00096 mpgv (OpalMPGW): FTP Client: reply code 250 in state 'CWD'. Reply text: ' CWD command successful.'
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: command 'CWD inbound' sent
21:39:40	ftp	debug	1671442		0x80e00096 mpgv (OpalMPGW): FTP Client: reply code 250 in state 'CWD'. Reply text: ' CWD command successful.'
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: command 'CWD external_interfaces' sent
21:39:40	ftp	debug	1671442		0x80e00096 mpgv (OpalMPGW): FTP Client: reply code 250 in state 'CWD'. Reply text: ' CWD command successful.'
21:39:40	ftp	debug	1671442		0x80e00098 mpgv (OpalMPGW): FTP Client: command 'CWD prod' sent
21:39:40	ftp	debug	1671442		0x80e00096 mpgv (OpalMPGW): FTP Client: reply code 250 in state 'CWD'. Reply text: ' CWD command successful.'

The WebSphere DataPower Appliance is transferring a file to a target directory via FTP.

- 1) The solution is implemented using a Multi-Protocol Gateway with a dynamic backend and an FTP URL is created dynamically.
- 2) The FTP server is listening in passive mode.
- 3) A file of 0 size is created on the target directory.
- 4) The same behavior is observed after repeated tests.

Which of the following is the most likely cause of the error?

- A. The FTP URL is incorrectly formed.
- B. DataPower does not support passive FTP mode.
- C. The target directory permissions do not allow for file transfer.
- D. A firewall is preventing a data port to be opened on the FTP server.

Answer: D

Question: 129.

Refer to the Exhibit.

```
Fri Oct 01 2010 11:38:59 [myldap][debug] xmlfirewall(map): tid(593713)[request]:  
Username and password extracted El: MyLoginID and MyPassword  
Fri Oct 01 2010 11:38:59 [/dap][warn] xmldr(map-manager): tid(593713): Binding to LDAP server xyz.bank.corp as 'CN=John Certified,  
OU=DataPower Engineers, OU=Users, DC=xyz, DC=bank, DC=corp' failed: 80090308: LdapErr: DSID-0C090334, comment:  
AcceptSecurityContext error, data 52e, vece  
Fri Oct 01 2010 11:38:59 [myldap][debug] xmlfirewall(map): tid(593713)[request]: ldap-authen Response:  
Fri Oct 01 2010 11:49:36 [/dap][debug] xmldr(map): tid(112754)[request]:  
Username and password extracted El: MyLoginID and MyPassword  
Fri Oct 01 2010 11:49:36 [myldap][debug] xmlfirewall(map): tid(112754)[request]: ldap-authen Response: <entry type="ldap">CN=John Certified,  
OU=DataPower Engineers,OU=Users,DC=xyz,DC=bank,DC=corp</entry>
```

The text in the Exhibit shows a WebSphere DataPower log:

Which of the following are TRUE for the log shown above?

- A. Shows two failed attempts at authentication.
- B. A userdefined XML Firewall called map is being used for RBM authentication.
- C. This log is a userdefined log target subscribing to both a userdefined log category and the ldap category.
- D. This log indicates that custom RBM LDAP Authentication is being used to authenticate DataPower users.
- E. This log can be obtained by switching RBM logging to On from the Troubleshooting panel in the default domain.

Answer: CD

Question: 130.

Refer to the Exhibit.

```
20100927T180155Z [conf][success] (admin:default:web-gui:192.168.0.1): (config web-mgmt)# web-mgmt  
20100927T180155Z [conf][success] (admin:default:web-gui:192.168.0.1): (config web-mgmt)# reset  
20100927T180155Z [conf][success] (admin:default:web-gui:192.168.0.1): (config web-mgmt)# admin-state enabled  
20100927T180155Z [conf][success] (admin:default:web-gui:192.168.0.1): (config web-mgmt)# local-address 192.168.0.1 9090  
20100927T180155Z [conf][success] (admin:default:web-gui:192.168.0.1): (config web-mgmt)# idle-timeout 3600  
20100927T180155Z [conf][success] (SYSTEM:default:":") web-mgmt 'WebGUI-Settings' - Configuration settings applied  
20100927T180202Z [file][success] (SYSTEM:default:":") Creating file "config:///autoconfig.cfg"  
20100927T183846Z [file][success] (SYSTEM:default:":") Creating file "image:///xi3815.odbc.tam6.tibco.script2"  
20100927T184116Z [sys][failure] (admin:default:web-gui:192.168.0.1): (config-flash)# boot image "xi3815.odbc.tam6.tibco.script2"
```

The text in the Exhibit shows a snippet of one of the logs available on a WebSphere DataPower Appliance: Which of the following is TRUE for the log above?

- A. It is the compilelog for the appliance.
- B. It is the CLI log for the default domain.
- C. It is the audit log for the appliance.
- D. It is the WebGUI log for the appliance.

Answer: C

Question: 131.

A solution implementer has enabled the Probe to determine the cause of an error in a Processing Rule. Which of the following are valid Service Error variables that would be available in the Probe?

- A. var://service/errorcode The assigned error code from the Result Code table.
var://service/errorrulename The name of the Error Rule that has been run to handle this error.
- B. var://service/errorcompletioncode A boolean field to indicate if the rule completed successfully.
var://service/formattederrormessage The formatted error message that will be written to the log file.
- C. var://service/errormessage A message showing the error condition that stopped multistep processing.
var://service/errorsubcode An additional error code that can give more specific details of the error.
- D. var://service/errorreasoncode The assigned reason code from the Result Code table.
var://service/backenderrorcode An error code passed as a result from a backend to DataPower as a response message.

Answer: C

Question: 132.

A DataPower Processing Policy has been coded to use DataPower variables. To analyze an error in one of the Rules a solution implementer has enabled the Probe. Which of the following are valid DataPower variable scopes visible in the Probe with the correct lifetimes?

- A. Context (Lifetime: Single processing rule)
Error (Lifetime: Single processing rule)
- B. Context (Lifetime: Single transaction)
Service (Lifetime: Multiple transactions)
- C. Service (Lifetime: Single transaction)
Local (Lifetime: Spans repeated transactions)
- D. Service (Lifetime: Single transaction)
System (Lifetime: Spans repeated transactions)

Answer: D

Question: 133.

Refer to the Exhibit.

Step 1: Transform Action: Input=INPUT, Transform=store:///identity.xsl, Output=dpvar_1, NamedInOutLocationType=default, OutputType=default, Transactional=off, SOAPValidation=body, SQLSourceType=static, Asynchronous=off, ResultsMode=first-available, RetryCount=0, RetryInterval=1000, MultipleOutputs=off, IteratorType=XPATH, Timeout=0, MethodRewriteType=GET, MethodType=POST, MethodType2=POST

Content Headers Attachments Local Variables Context Variables Global Variables Service Variables

Content of context 'INPUT':

```
<address:getAddressInfo
  xmlns:address="http://dpedu.ibm.com"
></address:getAddressInfo>
```

Show unformatted Send as message

A solution implementer has enabled the Probe to debug a Processing Rule. The exhibit shows the Probe results for a Request Rule when a test message has been sent to the service. Which of the following is a valid description of Probe results and a suitable action that can be taken to provide more information from the Probe?

- A. The Probe is showing successful processing of the message. The implementer could click on the yellow (righthand) magnifying glass to see the data sent to the backend.
- B. The Probe is showing successful processing of the message but that an error has been returned from the backend. The implementer could click on the yellow (righthand) magnifying glass and then on the Content tab to be shown the Error Message returned from the backend.
- C. The Probe is showing successful processing of the message but a failure to connect to the backend. The implementer could click on the yellow (righthand) magnifying glass and then on the Local Variables tab to be shown Error Codes to diagnose the connection failure.
- D. The Probe is showing a failure in the Rule to processing the message. The implementer could click on the yellow (righthand) magnifying glass and then on the Service Variables tab to be shown Error Codes to diagnose the Rule processing error.

Answer: D

Question: 134.

Refer to the Exhibit.

```
<address>getAddressInfo<br/><xmins:address>http://dpedu.ibm.com</xmins:address><br/><address>name<br/><address>title>Mr.</address>title<br/><address>firstName>John</address>firstName<br/><address>lastName>Doe</address>lastName<br/></address>name<br/></address>getAddressInfo<br/>
```

A solution implementer has enabled the Probe to debug a Processing Rule. The exhibit shows the Probe results for a Request Rule when a test message has been sent to the service. Which of the following is a valid description of Probe results?

- A. The Probe is showing the message was successfully processed by the Rule but the Service then failed to connect to the backend.
- B. The Probe is showing that the Rule created by the implementer contained only one Filter Action and that this Filter Action rejected the message.
- C. The Probe is showing that no Match Rule existed in the Processing Policy that matched the message sent in so the message was rejected using a Filter created by DataPower.
- D. The Probe is showing that no Rule has been executed for this message. This is because the service that this Rule is associated with has the Request Type set to PassThru mode.

Answer: C

Question: 135.

A solution implementer needs to write part of the information contained within a request message to a log in order to keep a record of the receipt of this message before sending the message to a backend for processing. The log message should be written to the system log. Which of the following could be used to provide this functionality?

- A. A Log Target with Target Type set to the system log and an Object Filter referencing the Service handling the request.
- B. Two Results actions defined within the request rule for the message, the first of which sets the Destination field to be the location of the log.
- C. A Transform action in the request rule for the message to pull the appropriate data from the request followed by a Log action to write the data to the log.
- D. A Transform action containing a customized XSL message extension element setting the priority, category and selected contents of the message to be written to the log.

Answer: D

Question: 136.

A solution implementer has created a Multi-Protocol Gateway to pass messages to a backend. The full contents of all request messages should be logged completely; performance is a high priority but the action should not fail if the log server is down. Which of the following logging mechanisms would satisfy both of these requirements?

- A. Add an SQL action to the start of the request rule for the message using an INSERT statement.
- B. Add a Log action to start of the request rule for the message and set the Asynchronous option to On.
- C. Create a Log Target for the request message with an Object Filter referencing the Service handling the request.
- D. Add an Extract action to the start of the request rule for the message setting the XPath field to "/" to extract the whole Request message.

Answer: B
