Exam Code: 000-289

Exam Name: Test289, IBM WebSphere DataPower SOA Appln. Firmware V3.6.1

Vendor: IBM

Version: DEMO

Part: A

1: You have created an XSL Proxy in Proxy Mode, with a static backend. You have a client to server StylePolicy Rule which executes an XSL Transformation on an XML Document that is submitted as part of a POST Request. The results from the static backend server will be in HTML. However when you execute an HTTP Post operation in the form of:

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

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

2: A company is using an XSL Proxy in Proxy mode to fetch and transform XML Documents from an HTTP Server. The XSL, feeValue.xsl, contains the following document function which GETs an XML Document using the HTTPS Protocol:
<xsl:variable name="feeDoc" select="document('https://192.168.1.101/fee.xml')"/>
You enter http://192.168.1.35:2063/empty.xml into a Browser to execute this Proxy Policy and see the following messages in the log:
xslproxy (myXSLProxy): document function error while executing local:///feeValue.xsl: Internal Error Connecting To https://192.168.1.101/fee.xml
Cannot establish SSL credentials
How should proper execution of the document function be enabled?
A.Use https://192.168.1.35:2063/empty.xml, not http://192.168.1.35:2063/empty.xml in Browser Request
B.Assign a Two-Way SSL Proxy Profile to XSL Proxy SSL Server Crypto Profile
C.Use 'https://192.168.1.101' as the Back End Server Address on the XSL Proxy
D.Create a Trusted Servers SSL Crypto Profile and assign it to the XSL Proxy SSL Client Crypto Profile
E.Create a Client Credentials Crypto Profile and use it in the User Agent assigned to the XSL Proxy XML Manager
Correct Answers: E

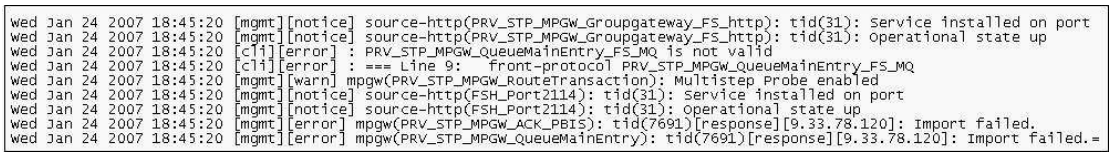
3: A company is attempting to consolidate the XML processing requirements of multiple applications. One issue is that the URLs being used to fetch the XML documents for

transformation contain an old application and servlet identifier. These must be replaced with a new consolidated application value of bc
Which technique will change a URL such as http://uri1/uri2/uri3, to http://uri1/abc ?
A.A URL-Rewrite Action with a type of eader-rewrite
B.A URL-Rewrite Action with a type of ost-body
C.A URL-Rewrite Rule with a type of bsolute-rewrite
D.A URL-Rewrite Rule with a type of ontent-type
Correct Answers: C

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

5: Which three statements are true about the product's network Packet Capture troubleshooting facility?
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 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.
D.A Packet Capture runs until the 'Maximum Duration' time has expired and keeps the last "Maximum Size" kilobytes of capture data.
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.Clicking the "Stop Packet Capture" button causes the packet capture to terminate immediately and the capture data is discarded.
Correct Answers: A B E

6: A consultant is engaged with an existing customer for a project that requires the deployment of 4 new XS40s to an existing pool of 5 XI50s. The customer is using basic security functionality, so the sales team offered the XS40s to close the deal. In order to keep all the devices in sync with the 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.
Why did this happen?



A.Configurations from XI50s are never portable to the XS40s.

B.The error report was a legacy from the original device and can be ignored.

C.The configuration provided for the XS40 is using exclusive XI50 features.

D.A Queue Manager object must be configured in the Default Domain.

Correct Answers: C

7: After configuring an XML Firewall with inbound SOAP traffic and XML outbound traffic, the system log shows the information in the exhibit. What does the log analysis show?

A.The inbound traffic is valid XML but invalid SOAP.

B.The outbound traffic is valid XML but invalid SOAP.

C.The outbound traffic is invalid XML and invalid SOAP.

D.The inbound traffic is invalid XML and invalid SOAP.

Correct Answers: C

8: A DataPower service is configured to communicate with a backend application server via HTTP on TCP Port 80. The device's System Logs indicate that the service cannot connect to the backend application server (Unable to establish backside connection). What tool should be used to verify connectivity to the backend application server?

A.MultiStep Probe

B.TCP Connection Test

C.Packet Capture

D.Ping Remote

Correct Answers: B

9: A company is having problems with their production WS-Proxy. SOAP requests are being sent to a back end Web service, where they fail schema validation. The WS-Proxy is deployed in its own domain on a shared SOA appliance, and the administrator of that domain only has access to that domain. The administrator suspects that a transparent network proxy is mangling incoming requests, but the SOA appliance is being blamed for the application behaving incorrectly. The development team has given the administrator a copy of the SOAP request which the Web service client is sending to the appliance.

How could the administrator simply demonstrate that the appliance is not at fault?

A.Submit the SOAP request using cURL from a different machine to the Web service client, connecting directly to the DataPower Appliance and bypassing the proxy.

B.Use the probe to view the incoming SOAP request and compare it to the SOAP request supplied by the development team.

C.Use the CP connection test facility to confirm that the Network Proxy is in the TCP connection path.

D.Paste the SOAP request into the end a Test Message facility to submit the Web service request locally.

E.Collect a packet capture on the SOA appliance to view the incoming SOAP request and compare it to the SOAP request supplied by the development team.

Correct Answers: D

10: A company has been testing an XML Firewall using the MultiStep Probe. What will the xport Capture feature of the Probe provide?

A.An export of Input data to the Firewall.

B.An export of the XML Firewall configuration.

C.An export of the XML Firewall configuration and an export of all transactions currently available in the probe. Input data to the Firewall will be, in most cases, extracted and stored in the local: directory.

D.An export of the XML Firewall configuration and an export of all transactions currently available in the probe. Input data to the Firewall will be, in most cases, extracted and stored in the temporary: directory.

E.An export of the XML Firewall configuration and an export of all transactions currently available in the probe. Input data to the Firewall may be, in most cases, extracted from the INPUT context of the request transactions.

Correct Answers: E

11: The MultiStep Probe allows for the display of local and global variables. Given the following StylePolicy Rule:

--- request 'setVariables_Rule_0' [up] matching matchAll ---
setvar INPUT var://local/variable A
fetch local:///fee.soap feeSOAP
setvar INPUT var://context/myContext/variable B
xform INPUT local:///getRequestResponseVariables.xsl tempvar4
xform feeSOAP local:///getRequestResponseVariables.xsl OUTPUT
--- response 'setVariables_Rule_1' [up] matching matchAll ---
xform INPUT local:///getRequestResponseVariables.xsl OUTPUT

Which statement is true regarding the two setvar commands?

A.var://local/variable is a local variable that is only available in the INPUT context of the request side rule. var://context/myContext/variable is a named context variable that is accessible from any context in the request or response side rules.

B.var://local/variable is a local variable that is only available in the INPUT context of the request side rule. var://context/myContext/variable is a named context variable that is accessible from any context and in any transaction subsequently processed by the device.

C.var://local/variable is a local variable that is only available in the INPUT context in the request or response side rules. var://context/myContext/variable is a named context variable that is accessible from any context in any transaction subsequently processed by the device.

D.var://local/variable is a local variable that is only available in the INPUT context in the request side rule. var://context/myContext/variable is a named context variable that is accessible from any context in any transaction subsequently processed by the device via a Service defined within the current domain.

E.var://local/variable is a local variable that is only available in the INPUT context in the request

side rule. var://context/myContext/variable is a named context var.
Correct Answers: A

12: How are WebGUI users authenticated and authorized when using RBM (Role Based Management)?
A.The user identity is extracted from the login request. The identity is authenticated with a local or remote source. Once authenticated, the identity is mapped to an Access Profile.
B.The user identity is extracted from the login request. The identity is authenticated with a source only local to the appliance. Once authenticated, the identity is mapped to an Access Profile.
C.The user identity is extracted from the login request. The associated AAA policy is used to authenticate and select the appropriate access policies.
D.The associated AAA policy is used to extract the user identity and authenticate the user. Once authenticated, the identity is mapped to an Access Profile.
Correct Answers: A

13: Which set of statements is true if the appliance is to act as an SSL client, client authentication is required and only a specific set of cipher suites are to be indicated in the client_hello SSL message?
A.The service is configured as an SSL client. The Crypto Profile contains a client credential and the CIPHER field is set to the supported cipher suites.
B.The service is configured as an SSL client. The Crypto Profile contains a trusted server and the CIPHER field is set to the supported cipher suites.
C.The service is configured as an SSL server. The CIPHER field is set to the supported cipher suites. The Crypto Profile contains a trusted server.
D.The service is configured as an SSL server. The Crypto Profile contains a client credential. The service object definition specifies its supported cipher suites in the CIPHER field.
Correct Answers: A

14: What is the proper format for Access Policies contained within an RBM (Role Based Management) Group definition?
A.<Application Domain>/<Resource Name> Access=<permissions>&[field=value]
B.<Device Address>/<Application Domain>/<Resource Name>?Access=<permissions>&[field=value]
C.<Address>/<Ethernet Port>/<Application Domain>/<Resource Name>?Access=<permissions>&[field=value]
D.<Device Address>/<User Account>/<Resource Name> Access=<permissions>&[field=value]
Correct Answers: B

15: A company is required to configure a DataPower Appliance to extract documents from an FTP server, then forward them on to a WebSphere MQ queue. No processing of the document is required. Some of the documents may be XML, some may be in Non-XML Formats.
Which Service and Request Type should be utilized for this process?
A.A Multi Protocol Gateway with an FTP Poller Front Side Protocol Handler a dpmq:// Backside URL and a Request Type of Pass-Thru

B.A Multi Protocol Gateway with an FTP Poller Front Side Protocol Handler a dpmq:// Backside URL and a Request Type of XML
C.A WS-Proxy with an FTP Poller Front Side Protocol Handler a dpmq:// Backside URL and a Request Type of Pass-Thru
D.A WS-Proxy with an FTP Poller Front Side Protocol Handler a dpmq:// Backside URL and a Request Type of XML
E.An XML FireWall with an FTP Poller Front Side Protocol Handler a dpmq:// Backside URL and a Request Type of Pass-Thru
Correct Answers: A

16: A customer has a DataPower device 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 DataPower Log Target configuration?
A.Specify an "Event Suppression Filter" to suppress confidential log file events on the Log Target
B.Specify a secure "Upload Method", either SSH or SCP, on the Log Target
C.Specify a "Signing Mode" on the Log Target
D.Specify a Sign Action in the processing policy
Correct Answers: C

17: A DataPower sales specialist is involved on a customer support discussion. The customer is ready to file a field device replacement because they can't connect with any of the Ethernet ports of their XA35. The customer claims their sysadmin was simply following the recommended practice to reinitialize the appliance through the SSH interface, using the command einit After that, the customer claims the device was unreachable.
What happened to the device?
A.The reinit clears the current firmware running on the appliance. A new firmware needs to be uploaded.
B.The device is behaving as designed, reinit clears the eth configs rendering it inaccessible through SSH.
C.The firmware image supplied to the reinit command was corrupt. The hardware is broken and must be returned.
D.The reinit command returns the device to factory state by removing the firmware. The firmware must be reinstalled.
Correct Answers: B

18: Which is NOT a feature of Configuration Checkpoint Management?
A.Checkpoint configurations can be deleted from file system.
B.The administrator can limit the number of Checkpoint configurations maintained.
C.Configuration objects can be imported from Checkpoint configurations.
D.Checkpoint configurations may be compared against the running configuration.
E.Checkpoint configurations may be compared against the persisted configuration.
Correct Answers: C

19: Which three external authentication systems does the DataPower device's RBM (Role Based Management) system directly support with no customization for authenticating administrative access to the product's WebGUI and SOAP Management interfaces?

A.Kerberos/SPNEGO
B.LDAP
C.Microsoft PASSPORT
D.Netegrity SiteMinder
E.RADIUS
F.TACACS/TACACS+
Correct Answers: A B E

20: An Error rule named "Error_rule" is coded as the first rule in the Configured Rules section of the Policy Editor as shown in the exhibit. Another rule, "Rule_1", in that section contains an on-error action "Error_1", followed by a processing action "Action_1", then another on-error action "Error_2". When the error occurs during action "Action_1" in Rule_1, what happens and why?
A."Error_1" action gets control since it is an on-error action that is already set for the rule.
B."Error_2" action gets control, since it is an on-error action that immediately follows the processing action that failed.
C."Error_rule" gets control since it preceded the failing rule in the Configured Rule section.
D."Error_rule" gets control since Error rules supersede any on-error actions.
Correct Answers: A