examunion

Certified IT Exam Material Authority

Accurate study guides, High passing rate!
We offer free update service for one year!
http://www.examunion.com

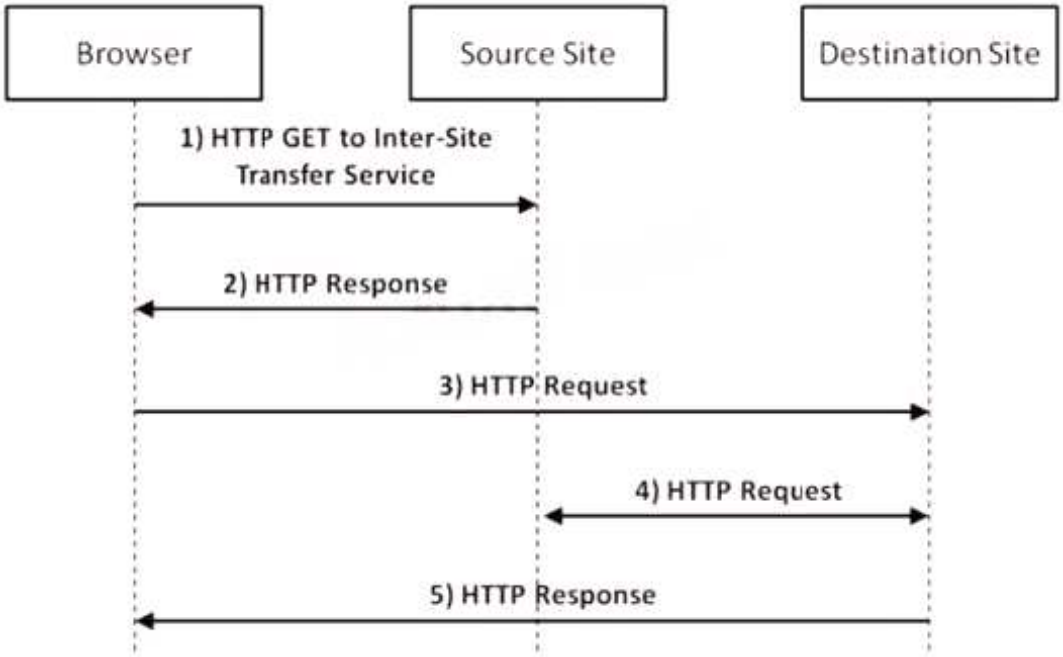
Exam : **C2150-575**

Title : IBM Tivoli Federated Identity Manager V6.2.2 Implementation

Version : Demo

1.What is the default file name of the IBM Tivoli Directory Integrator log?
A. tdi.log
B. ibmdi.log
C. ibmdisrv.log
D. ibmdirectoryintegrator.log
Answer: B

2.Click the Exhibit button.



Which three statements are true regarding this SAML 1.1 flow diagram.? (Choose three.)
A. The HTTP request in Step 3 is a GET.
B. The assertion is sent with an HTTP 200 response in Step 2.
C. An artifact value is sent with an HTTP 302 response in Step 2.
D. This is a Browser/POST profile, so in Step 3 the assertion is sent to the Assertion Consumer Service endpoint through an HTTP POST of an HTML form.
E. The HTTP response in Step 5 must be a 302 redirect based upon the resource requested and the user's authorized access which is determined by the response in Step 4.
F. This is a Browser/Artifact profile, so the artifact received in Step 2 must be sent to the Artifact Resolution Service in Step 3, and the assertion must be retrieved through a SOAP backchannel in Step 4.
Answer: A,C,F

3.What is XSLT?
A. A concatenative language for transforming input XML documents into new documents, which typically takes an XML source document and applies template rules to subexpressions, producing a new output document.
B. A declarative language for transforming input XML documents into new documents, which typically takes an XML source document and applies template rules in an XSLT stylesheet to it, producing a new output document.
C. An imperative language for transforming input XML documents into new documents, which typically

takes an XML source document and applies template rules in an XSLT stylesheet to it, producing a new output document.
D. A automata-based language for transforming input XML documents into new documents, which typically takes an XML source document and applies template rules to transition element states, producing a new output document.
Answer: B

4.What is always required when creating an IBM Tivoli Federated Identity Manager V6.2.2 (TFIM) Single Sign-On federation partner?
A. A signer certificate
B. A login protocol endpoint
C. A metadata file containing the partner definitions
D. A federation default or partner-specific mapping rule or function
Answer: D

5.Which HTTP status code is always issued by an identity provider using SAML 1.1 Browser/POST when communicating with the Assertion Consumer Service?
A. 101
B. 200
C. 206
D. 302
Answer: B

6.Custom Java mapping functions must be deployed into which IBM Tivoli Federated Identity Manager V6.2.2 directory?
A. Plug-ins
B. Add-ins
C. Mappings
D. Extensions
Answer: A

7.What is always required when deploying the IBM Tivoli Federated Identity Manager V6.2.2 runtime and management service?
A. WebSEAL
B. IBM HTTP Server
C. IBM Tivoli Identity Manager
D. IBM WebSphere Application Server
Answer: D

8.What does this XSL code do?
```
<xsl:template match-'@* | node()">
<xsl:copy>
<xsl:apply-templates select="@* | node()"/>
</xsl:copy>
```

</xsl:template>
A. It makes a copy of the template transforms on the input document.
B. It performs a series of transforms on a copy of the input document.
C. It creates a new copy of the input document, copying all attributes, but not elements.
D. It creates a new copy of the input document, copying all elements, but not attributes.
Answer: B

9.Given IBM Tivoli Federated Identity Manager V6.2.2 configured as an OpenID provider, what is a correct statement regarding processing of attributes when using an IBM Tivoli Directory Integrator AssemblyLine as a mapping function?
A. Only requested attributes can be returned.
B. All attributes requested must be BASE64 encoded to ensure proper handling.
C. The AssemblyLine must assure that values for non-optional attributes are returned.
D. Requested attributes that have an empty value (not an empty string) must be removed and cannot be returned.
Answer: C

10.Which statement is true regarding event pages when creating a federation in IBM Tivoli Federated Identity Manager V6.2.2 (TFIM)?
A. Event pages are tied to a protocol and not to a specific federation.
B. Event pages must be created (or copied from the defaults) and stored in the federation event directory.
C. Event pages can use the @FEDSTATUS@ macro to provide detailed Single Sign-On status information to the user.
D. When creating event pages for a federation, it is important to append the federation name to the event page filename so the TFIM runtime will use that instead of the default protocol event page.
Answer: A

11.A customer uses WebSEAL as the point of contact for IBM Tivoli Federated Identity Manager V6.2.2 (TFIM) where IBM Tivoli Access Manager (TAM) is configured to support Federal Information Processing Standards (FIPS). When running the tfimcfg.jar tool this error is received:
FBTTAC1161 The SSL handshake failed. Retrying connection with certificate validation disabled
What must be done?
A. TFIM must be configured for SSL communication.
B. FIPS must be enabled on all TFIM WebSphere servers.
C. The TAM public certificates must be imported to the WebSphere trust store.
D. The tfimcfg.jar tool needs to run with the-sslfactory TLS argument.
Answer: D

12.What is a trust service chain in IBM Tivoli Federated Identity Manager V6.2.2 (TFIM)?
A. It is a defined set of WS-Trust security tokens, which together form a proof of trust and are organized sequentially in their correct order of precedence.
B. It is a defined set of WS-Security trust tokens, which together form a proof of claim and are organized sequentially in their correct order of precedence.
C. It is a defined set of individual processing module instances, collectively executed in a specific order,

with the interface to and roles for each module conforming to the WS-Trust model.
D. It is a defined set of individual processing module instances which are always executed in the specific order required by the authentication flow, with the interface to and roles for each module conforming to the WS-Trust model.
Answer: C

13.Which partner vouches for the identity of a user in a Single Sign-On federation?
A. Relying party
B. Attribute party
C. Service provider
D. Identity provider
Answer: D

14.When configuring WebSEAL as the point of contact for IBM Tivoli Federated Identity Manager V6.2.2 using the WebSEAL No ACLD profile, which configuration requirement(s) are relevant?
A. This option must be set: Disable Access Manager (IVCred) credential issuing (requires EAI to be configured).
B. This option must be cleared: Enable Access Manager (IVCred) credential issuing (requires PDJRTE to be configured).
C. This option must be set: Disable Access Manager (IVCred) credential issuing (requires EAI to be configured); and the no-acid tag value attribute must be defined in the WebSEAL configuration.
D. This option must be cleared: Enable Access Manager (IVCred) credential issuing (requires PDJRTE to be configured); and the no-acid tag value attribute must be defined in the WebSEAL configuration.
Answer: B

15.Which statement is true about the IBM Tivoli Federated Identity Manager V6.2.2 Business Gateway?
A. Users can use several gateway protocols.
B. Users can access external Web services.
C. Users can create Federated Single Sign-On partnerships with multiple providers.
D. Users cannot create Federated Single Sign-On partnerships with multiple providers.
Answer: C

16.What does SAML stand for?
A. System Access Markup Language
B. Security Assertion Markup Language
C. Server Authenticated Markup Language
D. Secure Authentication Markup Language
Answer: B

17.A company wants to establish a Federated Single Sign-On (FSSO) relationship with a partner identity provider to allow partner administrator access. This company provides services for credit card processing. What is the most secure choice for the FSSO protocol?
A. OpenID using Associate Mode
B. SAML 2.0 using HTTP Redirect/POST bindings, signed response, and signed assertion

C. SAML 1.1 using a Browser/POST profile, signed response and assertion, and a narrow assertion validity window of only a few seconds
D. SAML 2.0 using an HTTP-Artifact binding, signed response and assertion, an encrypted assertion, and a narrow assertion validity window of only a few seconds
Answer: D

18.Which roles are typically defined in an IBM Tivoli Federated Identity Manager V6.2.2 Single Sign-On federation configuration?
A. Relying Party or Service Provider
B. Asserting Party or Service Provider
C. Identity Provider or Asserting Party
D. Identity Provider or Service Provider
Answer: D

19.When is IBM WebSphere Application Server required for IBM Tivoli Federated Identity Manager V6.2.2 (TFIM)?
A. It is always required for TFIM.
B. When it is used as the point of contact.
C. When the Management Console GUI is used.
D. When Web Services Security Management is used
Answer: A

20.A client has installed IBM Tivoli Federated Identity Manager V6.2.2 (TFIM) and is establishing a SAML 1.1 Single Sign-On (SSO) configuration with a service provider (SP). The client wants to provide SP-initiated Federated SSO. How can this be accomplished?
A. A link or redirect to the SP login endpoint with the parameters SP_PROVIDER_ID and target can be used to initiate the protocol at the SP. The SP will then redirect the user to the corresponding identity provider (IdP) login endpoint.
B. A link or redirect to the SP login endpoint with the parameters IDP_PROVIDER_ID and target can be used to initiate the protocol at the SP. The SP will then redirect the user to the corresponding IdP login endpoint.
C. Because a SP-initiated sign-on is not supported in SAML 1.1, this can be simulated by using a link or an HTTP 302 redirect to the IdP login endpoint with the query string parameters SP_PROVIDER_ID and TARGET to initiate the protocol.
D. Because a SP-initiated sign-on is not supported in SAML 1.1, and only an HTTP POST to the IdP can be used to initiate the protocol, the SP must generate an HTTP 200 response containing a form with the SP_PROVIDER_ID and target values which is self-posted to the IdP login endpoint.
Answer: C