

**Exam Code:** 000-875

**Exam Name:** ibm tivoli federated identity manager v6.0  
implementation

**Vendor:** IBM

**Version:** DEMO

## Part: A

1: Under which IBM Tivoli Federated Identity Manager Console main menu option would you find the settings for logging and tracing?

- A. Service Settings
- B. Logging and Auditing
- C. Service Management
- D. Monitoring and Logging

**Correct Answers: A**

2: Consider the following scenario involving customers of companies RBTelco and RBBenefits. RBTelco is a large multinational company that outsources health care benefit management to RBBenefits. RBTelco employees access RBBenefits resources through an authenticate-able account at each company.

RBTelco employees are being moved to a federated environment. Employees will access RBBenefits's resources using Single Sign-On. When Single Sign-On is enabled, all RBTelco employees will be migrated to the federated Single Sign-On implementation. RBTelco employees will have access to RBBenefits's resources based on his or her RBTelco authentication. After the migration, ALL access to RBBenefits's resources will be by Single Sign-On from RBTelco direct authentication to RBBenefits by a RBTelco employee will not be possible.

RBBenefits requires that RBTelco identify each employee with an alias that is based on a mathematical function using the employee number, social insurance number, and several other variables (shared between RBTelco and RBBenefits only). They will use a Liberty ID-FF 1.2 Browser/POST approach for Single Sign-On between companies. The number of machines required to support this environment when each machine is an Intel-based processor with 1GB RAM, 10 GB hard drive, and RHEL 30 is:

A.2 = (TAMeB WebSEAL on one machine) + (remainder TAMeB and all ITFIM components on one machine)

B.3 = (TAMeB WebSEAL on one machine) + (remainder TAMeB on one machine) + (all ITFIM components on one machine)

C.3 = (TAMeB WebSEAL on one machine) + (remainder TAMeB and ITFIM runtime/management on one machine) + (remainder ITFIM on one machine)

D.2 = (TAMeB WebSEAL and IBM Tivoli Federated Identity Manager (ITFIM) runtime/management on one machine) + (remainder TAMeB and ITFIM on one machine)

**Correct Answers: C**

3: What would result in this error message?

com.tivoli.am.fim.trustserver.sts.STSEException: FBTSTM015E The given TokenType or AppliesTo({{https://sp.benefitsx.com/demo/FIMDemo/Benefits/protected/accountinfo.jsp};{ };{ }}) in the request is not supported by this server's configuration for http://schemas.xmlsoap.org/ws/2004/04/security/trust/Validate RequestType and Issuer ({{https://idp.myemployerx.com/FIM/sps/wsfed/wsf};{ };{ }}).

- A. An incorrect certificate has been configured at the Service Provider.
- B. The resource being requested by the Identity Provider is not recognised.

- C.The clocks on the Identity Provider and Service Provider are out of sync.
- D.The partner realm name at the Service Provider has been configured incorrectly.

**Correct Answers: D**

4: Which two security tokens may carry user attribute information as part of the defined token format? (Choose two.)

- A.Kerberos
- B.X.509 Token
- C.SAML Assertion
- D.Liberty Assertion
- E.Username Token

**Correct Answers: C D**

5: Which two commands can be used to query the status of WebSEAL servers on the local machine? (Choose two.)

- A.iv status
- B.amstatus
- C.pdweb status
- D.pd\_start status
- E.webseald –status

**Correct Answers: C D**

6: Company-A has created a web service application for use by both its trading partners. The application requires a web services security request that includes a SAML token identifying both the end-user and attributes of that user.

The trading partners have agreed to submit a web service request with a signed SAML token that includes both the user's identity and attributes of the user. The SAML attributes will vary by partner but the application requires a consistent set of attributes for example, the same set of attributes are required for all client requests.

SAML Assertions must be authenticated via validation of the token's <ds:Signature> element.

Which scenario satisfies the requirements of the application?

A.A WSSM Partner is configured for each trading partner. Each WSSM Partner configuration specifies the mapping rules required to transform the identity & attributes received from the partner into those required by the application. The signed SAML token of each WSSM partner will be validated with a key that is unique to that trading partner.

B.A WSSM Partner is configured for each trading partner that is not already part of a SAML federation for SSO. The mapping rules for all partners must transform the identity and attributes received from the partner into those required by the application. The signed SAML token of each partner will be validated with a key that is unique to that trading partner.

C.The SAML token submitted by the trading partner is known to be trustworthy because its <ds:Signature> element will be validated by WebSphere. A WSSM Partner is configured for each trading partner and each configuration specifies the mapping rules required to transform the attributes received from the partner into those required by the application.

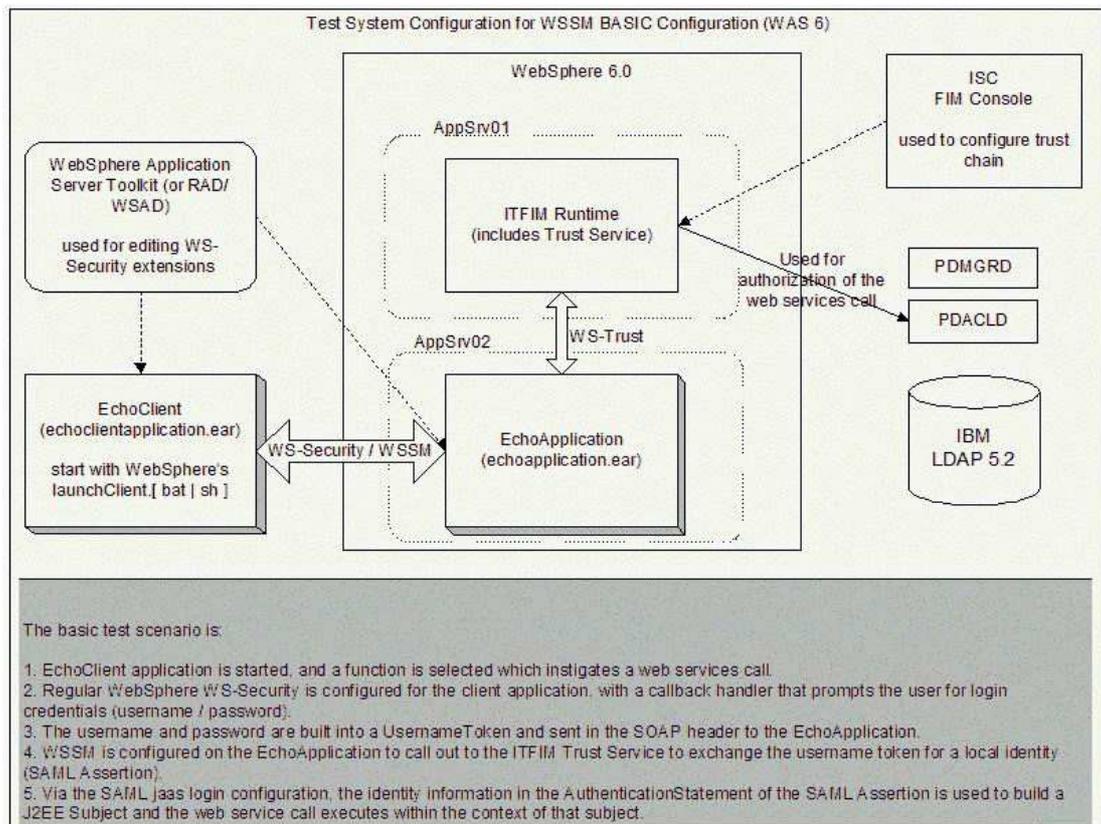
D.A Web Services Security Management (WSSM) Partner is configured for each trading partner.

The signed SAML token of each WSSM partner is validated with a key that is unique to that trading partner. Because all partners submit a SAML token, mapping rules are not required. SAML is a standard and all elements of a SAML token must comply with that standard.

**Correct Answers: A**

7: Click the Exhibit button.

You have started with an EchoApplication.ear that has no WS-Security configured. When configuring WS-Security on the EchoApplication.ear, which piece of the configuration indicates that a UsernameToken will be required for Java Authentication and Authorization Service (JAAS) login?



A. Caller Part

B. Token Consumer

C. Required Confidentiality

D. Required Security Token

**Correct Answers: A**

8: What error condition would cause the error message below to appear in the logs?

FBTLIB204E No federation exists for this principal

A. Consent to federate was not granted.

B. IBM Tivoli Access Manager user account is invalid.

C. The federation being requested by the user has not been enabled.

D. The federation being requested has not been defined for this user.

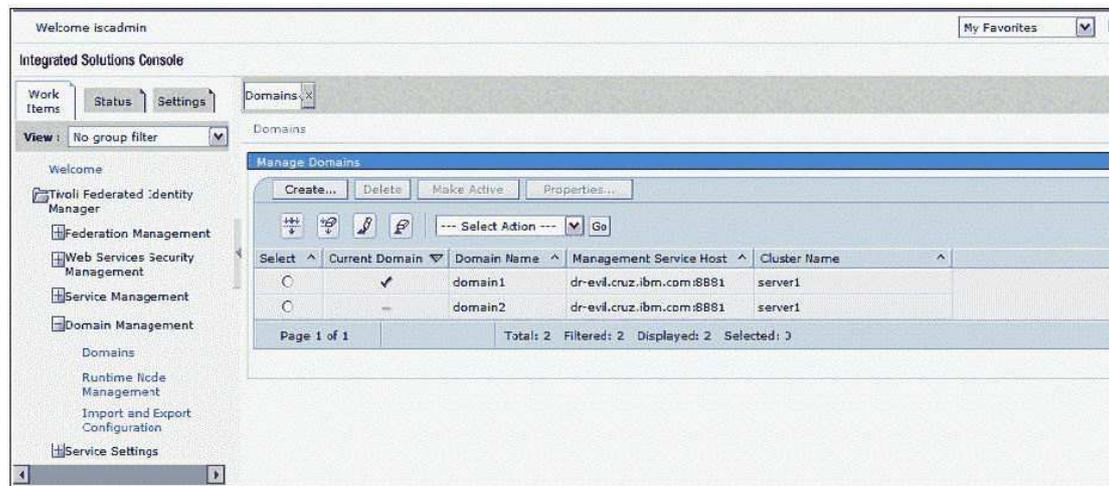
**Correct Answers: A**

- 9: What triggers the consent to Federate page to be displayed?
- A. The Consent flag is set in an incoming federate request.
  - B. The Consent flag is set in an incoming authentication request.
  - C. The Identity Provider configuration requires the page to be displayed.
  - D. The Service Provider configuration requires the page to be displayed.

**Correct Answers: C**

10: Click the Exhibit button.

In the IBM Tivoli Federated Identity Manager (ITFIM) Console, you have two different domains: domain1 and domain2. Which steps would back up domain2 if the domains currently appear as in the exhibit?



- A. Click the import and Export Configuration link, click the export Configuration button, and save the archive.
- B. Backup files included in /opt/IBM/WebSphere/AppServer/profiles/<WAS\_PROFILE\_NAME>/config/itfim/domain2.
- C. Click the delete button to remove domain1, then click the import and Export Configuration link, click the export Configuration button, and save the archive.
- D. Select domain2, click the take Active button, then click the import and Export Configuration link, click the export Configuration button, and save the archive.

**Correct Answers: D**

11: Once you have successfully placed your custom alias service plug-in in the correct location, what are the three Runtime custom properties required to enable your plug-in? (Choose three.)

- A. com.tivoli.am.fim.alias.factory.moduleId
- B. com.tivoli.am.fim.alias.service.factory.id
- C. com.tivoli.am.fim.alias.service.moduleName
- D. com.tivoli.am.fim.alias.factory.moduleVersion
- E. com.tivoli.am.fim.alias.service.moduleVersion
- F. com.tivoli.am.fim.alias.factory.exposedClassId

**Correct Answers: A D F**

12: Which IBM Tivoli Directory Server utility is used to perform LDAP tracing?

- A.ldtrc
- B.trace
- C.slaptc
- D.ldapmodify

**Correct Answers: A**

13: A financial planning company would like to enter into a Federation with an online business partner who provides financial forecasting and modeling for customers. The expected user flow would have the customer authenticating to their account with the financial planner and selecting a special link for forecasting and Modeling. This would re-direct the user to the business partner who would obtain the customer's portfolio information and balances via a real-time back channel communication initiated by a Liberty ID-FF V1.1 Browser/Artifact SSO flow. This information will be used by the business partner to establish and update the user's local business partner side information.

What can you determine about the type of provisioning solution that has been agreed upon?

- A.a priori
- B.runtime
- C.no account linking
- D.unable to determine

**Correct Answers: B**

14: What do the IBM Extensions to the SAML Single Sign-On (SSO) protocol enable?

- A.the SSO profile to be specified in the SSO Trigger
- B.an SSO exchange to be initiated from the Service Provider
- C.signed messages to be passed over the SOAP backchannel
- D.additional identity mapping information to be passed in the SAML message

**Correct Answers: A**

15: In order to write a plug-in that implements a custom Alias service, what are the two required public interfaces that need to be implemented? (Choose two.)

- A.com.tivoli.am.fim.service.CustomService
- B.com.tivoli.am.fim.alias.service.AliasServiceClient
- C.com.tivoli.am.fim.identity.service.client.IdServiceClient
- D.com.tivoli.am.fim.alias.service.AliasServiceClientFactory
- E.com.tivoli.am.fim.identity.service.client.IdServiceClientFactory

**Correct Answers: C E**

16: What must be unique across all federations?

- A.Provider ID
- B.SSO Protocol
- C.Point of Contact
- D.Identity Mapping Rules

**Correct Answers: A**

17: What are two locations to turn on per process tracing of WebSEAL? (Choose two.)

- A.in the pd.conf file
- B.with the pdconfig utility
- C.using pdadmin trace functions
- D.routing file for the WebSEAL instance
- E.in the WebSEAL configuration file (webseald-default.conf)

**Correct Answers: C D**

18: What is the most likely cause of this failure?

=====

```
<Trace Level="MIN">
  <Time Millis="1111369746437"> 2005-03-20 19:49:06.437-06:00</Time>
  <Server Format="IP">ip1</Server>
  <ProductId></ProductId>
  <Component>trustservice</Component>
  <ProductInstance></ProductInstance>
  <LogText><![CDATA[]]></LogText>
  <Source          FileName="com.tivoli.am.fim.trustserver.service.SecurityTokenService"
Method="requestSecurityToken(MessageContext)"/>
  <Thread>WebContainer : 0</Thread>
  <Exception><![CDATA[com.tivoli.am.fim.trustserver.sts.STSException:          FBTSTS008E
Assertion issuer is not configured.
```

```
atcom.tivoli.am.fim.trustserver.sts.STSModuleChainManager.makeNoMapSTSException(STSMo
duleChainManager.java:185)
atcom.tivoli.am.fim.trustserver.sts.STSModuleChainManager.processthroughChains(STSModule
ChainManager.java:101)
atcom.tivoli.am.fim.trustserver.sts.STSModuleChainManager.process(STSModuleChainManager.j
ava:66) at com.tivoli.am.fim.trustserver.sts.STSManager.process(STSManager.java:57)
atcom.tivoli.am.fim.trustserver.service.SecurityTokenProcessor.process(SecurityTokenProce
ssor.java:63)
atcom.tivoli.am.fim.trustserver.service.SecurityTokenService.requestSecurityToken(SecurityToke
nService.java:79)
atcom.tivoli.am.fim.trustserver.service.SecurityTokenService.requestSecurityToken(SecurityToke
nService.java:112)
atcom.tivoli.am.fim.trustserver.ws.was.RequestSecurityTokenPortBindingImpl.requestSecurityTo
ken(RequestSecurityTokenPortBindingImpl .java:29)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:58)
atsun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java(Compi
led Code)) at java.lang.reflect.Method.invoke(Method.java(Compiled Code))
atcom.ibm.ws.webservices.engine.dispatchers.java.JavaDispatcher.invokeMethod(JavaDispatcher.
java:178)
```

atcom.ibm.ws.webservices.engine.dispatchers.java.JavaDispatcher.invokeOperation(JavaDispatcher.java:141)  
atcom.ibm.ws.webservices.engine.dispatchers.SoapRPCProcessor.processRequestResponse(SoapRPCProcessor.java:393)  
atcom.ibm.ws.webservices.engine.dispatchers.SoapRPCProcessor.processMessage(SoapRPCProcessor.java:356)  
atcom.ibm.ws.webservices.engine.dispatchers.BasicDispatcher.processMessage(BasicDispatcher.java:134)  
atcom.ibm.ws.webservices.engine.dispatchers.java.SessionDispatcher.invoke(SessionDispatcher.java:203)  
at com.ibm.ws.webservices.engine.PivotHandlerWrapper.invoke(PivotHandlerWrapper.java:218)  
at  
com.ibm.ws.webservices.engine.handlers.jaxrpc.JAXRPCHandler.invoke(JAXRPCHandler.java:144)  
at com.ibm.ws.webservices.engine.handlers.WrappedHandler.invoke(WrappedHandler.java:64)  
at com.ibm.ws.webservices.engine.PivotHandlerWrapper.invoke(PivotHandlerWrapper.java:218)  
at com.ibm.ws.webservices.engine.WebServicesEngine.invoke(WebServicesEngine.java:274)  
atcom.ibm.ws.webservices.engine.transport.http.WebServicesServlet.doPost(WebServicesServlet.java:688)  
at javax.servlet.http.HttpServlet.service(HttpServlet.java:763)  
atcom.ibm.ws.webservices.engine.transport.http.WebServicesServletBase.service(WebServicesServletBase.java:341)  
at javax.servlet.http.HttpServlet.service(HttpServlet.java:856)  
at com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java:1212)  
at com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest(ServletWrapper.java:629)  
at com.ibm.ws.webcontainer.webapp.WebApp.handleRequest(WebApp.java:2837)  
at com.ibm.ws.webcontainer.webapp.WebGroup.handleRequest(WebGroup.java:220)  
at com.ibm.ws.webcontainer.VirtualHost.handleRequest(VirtualHost.java:204)  
at com.ibm.ws.webcontainer.WebContainer.handleRequest(WebContainer.java:1681)  
at com.ibm.ws.webcontainer.channel.WCChannelLink.ready(WCChannelLink.java:77)  
atcom.ibm.ws.http.channel.inbound.impl.HttpInboundLink.handleDiscrimination(HttpInboundLink.java:421)  
atcom.ibm.ws.http.channel.inbound.impl.HttpInboundLink.handleNewInformation(HttpInboundLink.java:367) at  
com.ibm.ws.http.channel.inbound.impl.HttpInboundLink.ready(HttpInboundLink.java:292)  
atcom.ibm.ws.tcp.channel.impl.NewConnectionInitialReadCallback.sendToDiscriminators(NewConnectionInitialReadCallback.java:201)  
atcom.ibm.ws.tcp.channel.impl.NewConnectionInitialReadCallback.complete(NewConnectionInitialReadCallback.java:103)  
at  
com.ibm.ws.tcp.channel.impl.WorkQueueManager.requestComplete(WorkQueueManager.java:548)  
at com.ibm.ws.tcp.channel.impl.WorkQueueManager.attemptIO(WorkQueueManager.java:601)  
at com.ibm.ws.tcp.channel.impl.WorkQueueManager.workerRun(WorkQueueManager.java:934)

at com.ibm.ws.tcp.channel.impl.WorkQueueManager\$Worker.run(WorkQueueManager.java:1021)

at com.ibm.ws.util.ThreadPool\$Worker.run(ThreadPool.java:1332)

]]></Exception>

</Trace>

=====

- A.The module chain does not exist.
- B.The module chain is incorrectly configured.
- C.The IBM Tivoli Federated Identity Manager Trust Server cannot map the request to a module chain.
- D.The IBM Tivoli Federated Identity Manager Trust Server is stopped and cannot process the request.

**Correct Answers: B**

19: When configured for a Service Provider side Liberty V1.2 Federation, which functionality will require the IBM Tivoli Federated Identity Manager Alias Service? (Choose three.)

- A.Single Sign-On
- B.Single Sign-Off
- C.One Time Identifiers
- D.Consent to Federate
- E.Identity Provider Proxy
- F.Register Name Identifier

**Correct Answers: A B F**

20: Assuming /FIM is the junction defined with defaults for the Federated Single Sign-On using WS-Federation and IBM Tivoli Federated Identity Management, what policy is required at the Identity Provider so that only the SSL connection is allowed to the Single Sign-On Protocol Service?

- A.Attach a POP with qop set to ssl.
- B.Attach a POP with qop set to none.
- C.Attach a POP with qop set to privacy.
- D.Attach a POP with qop set to integrity.

**Correct Answers: C**