

# QUESTIONS & ANSWERS

Kill your exam at first Attempt



**IBM**

**000-875**

*IBM Tivoli Federated Identity Manager V6.0 Implementation*



**Answer:** D

**QUESTION:** 135

What three actions does a WebSphere Node Agent do? (Choose three.)

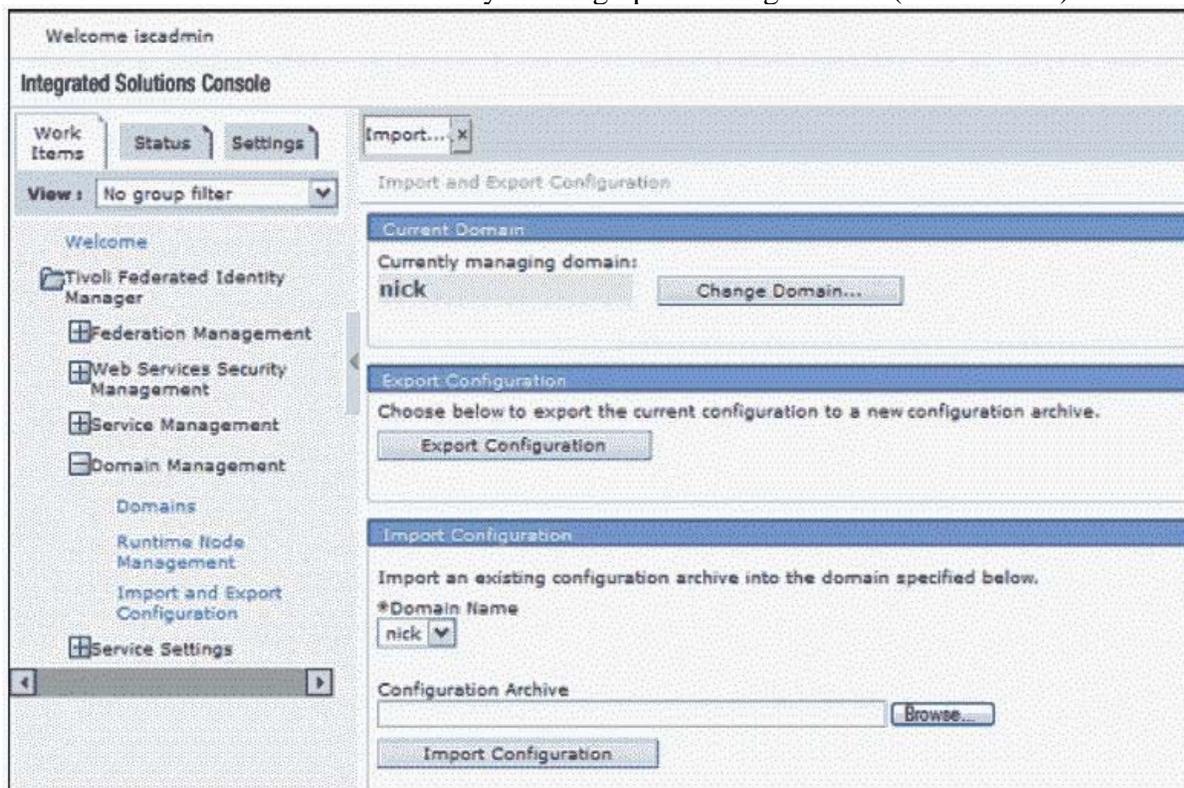
- A. monitors performance
- B. manages JVM memory
- C. serves J2EE applications
- D. manages the deployment manager
- E. manages configuration synchronization
- F. routes administrative requests to servers

**Answer:** A, E, F

**QUESTION:** 136

Click the Exhibit button.

Which two tasks would be executed by clicking xport Configuration? (Choose two.)



- A. Export an archive of the active ITFIM Domain.
- B. Initiate a file download of a configuration archive.
- C. Inform the user that WebSphere Application Server must be restarted.
- D. Duplicate the configuration of the active ITFIM Domain in a new ITFIM domain.
- E. Initiate a file download of a configuration archive and duplicate the configuration of the active ITFIM Domain in a new ITFIM domain.

**Answer:** A, B

**QUESTION:** 137

You are configuring a IBM Tivoli Federated Identity Manager (ITFIM) Web Services Security Management environment at the service provider. You need to add two partners, P1 and P2, both who whom will be accessing the application A3. A3 is deployed as a web service using RAD. Web Services requests to A3 will be required to be received over SSL and will have body-level encryption on the SOAP message. Access to A3 will require a JAAS login content based on a SAML 11 assertion defining the requestor. Partner P1 is able to issue a SAML 10 assertion with an attribute statement containing one attribute, the user's role (as previously agreed upon between P1 and the service provider). Partner P2 is able to issue a SAML 11 assertion with an attribute statement containing a list of roles that the requestor currently has. The service provider will map the partner asserted role(s) into a locally valid identity assigned to the requestor and will use this identity for the JAAS login process. Which two statements is a true statement of the configuration requirements on this overall environment? (Choose two.)

- A. Partner P2 will be deployed to ITFIM (using wsdl2tfim) and will require the parameters of the incoming token types (SAML 11 assertion type).
- B. Partner P1 will be deployed to ITFIM (using the console) and will require the parameters of the incoming token type (SAML10 assertion type).
- C. Partner P2 will be deployed to ITFIM (using the console) and will require the parameters of the incoming token types (SAML 11 assertion type).
- D. Partner P1 will be deployed to ITFIM (using wsdl2tfim) and will require the parameters of the incoming token type (SAML10 and SAML 11 assertion types).
- E. Partner P1 will be deployed to ITFIM (using the console) and will require the parameters of the incoming token type (SAML10 and SAML 11 assertion types).

**Answer:** A, B

**QUESTION:** 138

When designing a system to use WS-Federation, what browser Single Sign-On method would you use?

- A. GET
- B. POST
- C. Artifact
- D. Response

**Answer:** B

**QUESTION:** 139

In which Single Sign-On profile is one where the Security Token is passed from the Identity Provider to the Service Provider via a passive client?

- A. Browser PULL

- B. Browser PUSH
- C. Browser POST
- D. Browser Artifact

**Answer: C**

**QUESTION: 140**

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)

**Answer: C**

**QUESTION: 141**

Click the Exhibit button.

You are configuring a IBM Tivoli Federated Identity Manager (ITFIM) Federated single Sign-On (F-SSO) environment for a company acting as an Identity Provider. You have XML-based metadata files for five partners (all Service Providers (SP), all to be configured for Liberty ID-FF V1.1 functionality). Based on the metadata provided (shown below in chart form), define the grouping of these partners into the defined Identity Provider (IDP) side federations. Select the option with the minimum number of federations and partners in each federation.

| SP Partner | F-SSO Protocol Profiles | Trust Information: Signing Key Requirements | Parameter: Require Consent to Federate |
|------------|-------------------------|---|--|
| A          | SSO, SLO                | Requires messages signed with 1024 bit key  | N                                      |
| B          | SSO, SLO                | Requires messages with minimum 512 bit key  | Y                                      |
| C          | SSO, SLO, RNI, FTN      | Requires messages with 1024 bit key         | Y                                      |
| D          | SSO, SLO, RNI, FTN      | Requires messages with minimum 512 bit key  | N                                      |
| E          | SSO, SLO, RNI, FTN      | Requires messages with 1024 bit key         | Y                                      |

- A. 3 Federations, one with (A), one with (B), one with (C, D, E)
- B. 3 Federations, one with (A, B), one with (C, E) and one with (D)
- C. 4 Federations, one with (A), one with (B), one with (C, E) and one with (D)
- D. 4 Federations, one with (A, B), one with (C), one with (D) and one with (D)
- E. 5 Federations, one for each partner (no having?of federation at partner level)

**Answer:** C

**QUESTION:** 142

Where is the location of the WebSEAL trace log output configured?

- A. in pd.conf
- B. in ivmgrd.conf
- C. in the 'routing' file
- D. in the WebSEAL configuration file (webseald-default.conf)

**Answer:** C

**QUESTION:** 143

Click the Exhibit button.

When entering the WebSphere Application Server SOAP connector port during the installation of the IBM Tivoli Federated Identity Manager (ITFIM) Management Service what are you actually pointing the installer at?



- A. WebSphere cluster
- B. WebSphere installation
- C. WebSphere node agent
- D. WebSphere server instance

**Answer:** D

**QUESTION:** 144

When configured for an identity provider side Liberty V1.1 Federation, which three functionalities will require the IBM Tivoli Federated Identity Manager Alias Service? (Choose three.)

- A. Single Sign-On
- B. Single Sign-Off
- C. Attribute Management
- D. Identity Provider Proxy
- E. Register Name Identifier
- F. Identity Provider Introduction

**Answer:** A, B, E

For More exams visit <https://killexams.com/vendors-exam-list>



*Kill your exam at First Attempt....Guaranteed!*