ISLEVER

1Z0-478

Oracle SOA Suite 11g Essentials

DEMO

https://www.islever.com/1z0-478.html

https://www.islever.com/oracle.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

You have modeled a composite with a one-way Mediator component that is exposed via an inbound file adapter service. How do you configure the inbound file adapter to read local files in ascending order of their lastModifiedTime?

A. By setting the SingleThreadModel activationsSpec property to true and configuring the ListSorter activationSpec property to oracle.tip.adapter.file.inbound.listing.TimestampSorterAscending.
B. By not making any configuration changes because, by default, the adapter reads input files in ascending order of their lastModifiedTime.
C. By setting the ThreadCount activationSpec property to 0 and configuring the List Sorter activationSpec property to oracle.tip.adapter.file.inbound.listing.TimestampSorterDescending.
D. By setting the ThreadCount activatioSpec property to – 1 and configuring the ListSorter activationSpec property to oracle.tip.adapter.file.inbound.liting.TimestampSorterAscending.

Answer: A
Explanation: When files must be processed by Oracle File and FTP Adapters in a particular order, you must configure the sorting parameters. For example, you can configure the sorting parameters for Oracle File and FTP Adapters to process files in ascending or descending order by time stamps.

You must meet the following prerequisites for sorting scenarios of Oracle File and FTP Adapters:
Use a synchronous operation
Add the following property to the inbound JCA file:
<property name="ListSorter"
value="oracle.tip.adapter.file.inbound.listing.TimestampSorterAscending"/>
<property name="SingleThreadModel" value="true"/>

QUESTION NO: 2

Which two activities are typically performed during the service implementation and configuration phase of the SOA lifecycle?

A. Capabilities are evaluated and prioritized based on business models and ROI.
B. Oracle Enterprise Repository promotes services and harvested endpoints to the service registry.
C. Developers find and reuse services to help them complete development.
D. Developers use harvesting tools to submit their completed implementations to Oracle Enterprise Repository.

Answer: C,D
Explanation: Implementation and Configuration

As capabilities are funded, projects are established to implement the capability. SOA Suite developers working in JDeveloper can see and reuse services from the enterprise repository to complete their projects. Service Bus developers working in Eclipse can see and reuse services from the enterprise repository to complete their projects (C). Developers can also harvest their completed implementations directly to the Enterprise Repository (D). The Enterprise repository also supports VS .Net development.

QUESTION NO: 3

In your solution, a web service client needs to invoke a series of three web services in support of a single transaction. The third web service needs the identity of the original web service client.

Which statement describes how the identity is made available by Oracle Web Services Manager (OWSM)?

A. The transaction manager accesses an internal table that maintains credentials used to invoke each individual web service in the chain.
B. Each web service in the chain does its own authentication so the third web service handles its own identity checking.
C. OWSM sets the user in the Java Authentication and Authorization (JAAS) Subject when the first web service successfully authenticates, and the Java Subject is used by subsequent web services to access the identity.
D. OWSM stores a SAML token from the first web service invocation in a database table, and that table is accessed by subsequent web services in the chain to retrieve identity.

Answer: C
Explanation: Propagating Identities through a Chain of Web Services

A web service may invoke another web service which in turn may invoke yet another web service to complete a single transaction (this pattern is known as “chained web services”). Eachof the services in the chain may be protected. Instead of checking which service is calling which other service, Oracle WSM allows you to check who the original user invoking the chain of Web services is. Oracle WSM policies can be used to propagate the original user’s identity across the chained web services. Following successful authentication to the first web service in the chain, Oracle WSM sets the user as a Java Subject used throughout the transaction. When invoking another service, the Oracle WSM client policy picks up the user identity from the Java Subject, generates a SAML token based on the Subject ’s information, and inserts the SAML

token in the WS-Security header of the request message to be sent to the service provider. This allows all theweb services in a chain to track the identity of the actual user calling a web serviceendpoint instead of having the identity of the prior service in the chain calling the first web service
to get that information.

Reference: Securing Web Services and Service-Oriented Architectures with Oracle Web Services Manager 11g, Oracle White Paper

QUESTION NO: 4

Identify the best description of the recommended use of shared storage in a high-availability (HA) implementation of Oracle SOA Suite?

A. To allow access to a common installation home for all domain cluster members
B. To allow access to a shared JTA log
C. Shared storage is not recommended for Oracle SOA Suite.
D. To allow access to the default user store on the file system for all domain cluster members

Answer: A
Explanation:

QUESTION NO: 5

Composite X invokes an outbound DB adapter to write data to a database table. You have configured JCA at the binding component as follows:

<property name = “jca.retry.count” type = “xs:int” many = “false” override = “may” > 2</property>

<property name = “jca.retry.interval” type = “xs:int” many = “false” override = “may” > 2</property>

You have also modeled a modeled a fault policy to retry the invocation three times in case of remoteFault as follows:

<retryCount>3<retryCount>