

ISLEVER

# 1Z0-479

Oracle Access Management Suite Plus 11g  
Essentials

DEMO

<https://www.islever.com/1z0-479.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 1

What is the role of a user data store in Oracle Identity Federation (OIF) 11g when it is configured as an Identity Provider (IdP)? (Choose the best answer.)

- A. Oracle Identity Federation uses the repository to map the information in received assertions to user identities at the destination.
- B. When creating a new federation, Oracle Identity Federation uses the repository to identify a user and link the new federation to that user's account.
- C. Oracle Identity Federation uses the repository to authorize users for access to protected resources.
- D. Oracle Identity Federation uses the repository to verify user identities and to build protocol assertions.

**Answer: C**

### QUESTION 2

You have defined an application and its associated policies in Oracle Entitlements Server (OES) to protect your customer's banking application. This application is written in Java and deployed on WebLogic, using the WebLogic security module for integration. Using the policy simulator, your policy logic appears to be correct.

However, while testing, it appears that your authorization policies are not being applied and all authorization decisions are being returned as false from the security module.

Which two configuration settings in your OES admin console may be the cause of this problem? (Choose two.)

- A. The security module is configured to pull policies instead of having policies pushed to it.
- B. The application has not been associated with the security module in the OES admin console.
- C. The security module was not registered correctly when config.sh was run.
- D. You have not distributed the policies in the OES admin console.
- E. The security module has not been started.

**Answer: BD**

---

### QUESTION 3

Identify two artifacts that are present in an application domain of Oracle Access Manager 11g.

- A. Resources
- B. Authentication Scheme
- C. Authentication Policies
- D. Authentication Modules
- E. Data Sources

**Answer:** AB

### QUESTION 4

Identify two registration artifacts that are created when an 11g WebGate is registered using the Oracle Access Management console.

- A. osso.conf
- B. oaam\_cli.properties
- C. OAMRequest\_short.xml
- D. ObAccessClient.xml
- E. cwallet.sso

**Answer:** DE

### QUESTION 5

Your portfolio trading customer is using Oracle Entitlements Server (OES) to externalize authorization decisions from their share dealing application.

The trading customer has stipulated the following policy need to be implemented:

-Customers can purchase shares only if their credit limit is 20% higher than the value of the shares in their basket at checkout.

---

The value of basket and a customer's credit limit are both available in the application, and can be passed to OES as part of an authorization request if required.

You are looking to implement the most efficient policy within OES. Which three steps would you implement?

- A. Configure a Policy Information Point (PIP) to retrieve the basket value and credit limit from an internal system.
- B. Configure an authorization policy to include a condition that executes a custom function.
- C. Configure the application to include the basket value and credit limit in the authorization request.
- D. Create a custom function to calculate the difference between the basket value and the credit limit.
- E. Use a PIP to call a web service that returns the calculated difference between the basket value and the credit limit.
- F. Return an obligation that contains the difference value so that the application can decide whether to allow the transaction or not.

**Answer:** BDF

#### **QUESTION 6**

Which statement is true about a single sign-on operation initiated from a Service Provider using SAML 2.0 in Oracle Identity Federation (OIF)?

- A. Oracle Access Manager is required as a Service Provider integration module.
- B. An Oracle Access Manager WebGate is needed to protect the target web resource and redirect requests to OIF.
- C. HTTP post binding is only supported.
- D. Any HTTP request hitting the target resource is redirected to the Service Provider's OIF instance.

**Answer:** A

#### **QUESTION 7**