Oracle

1Z0-346 Exam

Oracle Mobile Cloud Service 2016 Developer Essentials Exam

Demo

Version: 8.0

Question: 1

View the Exhibit.

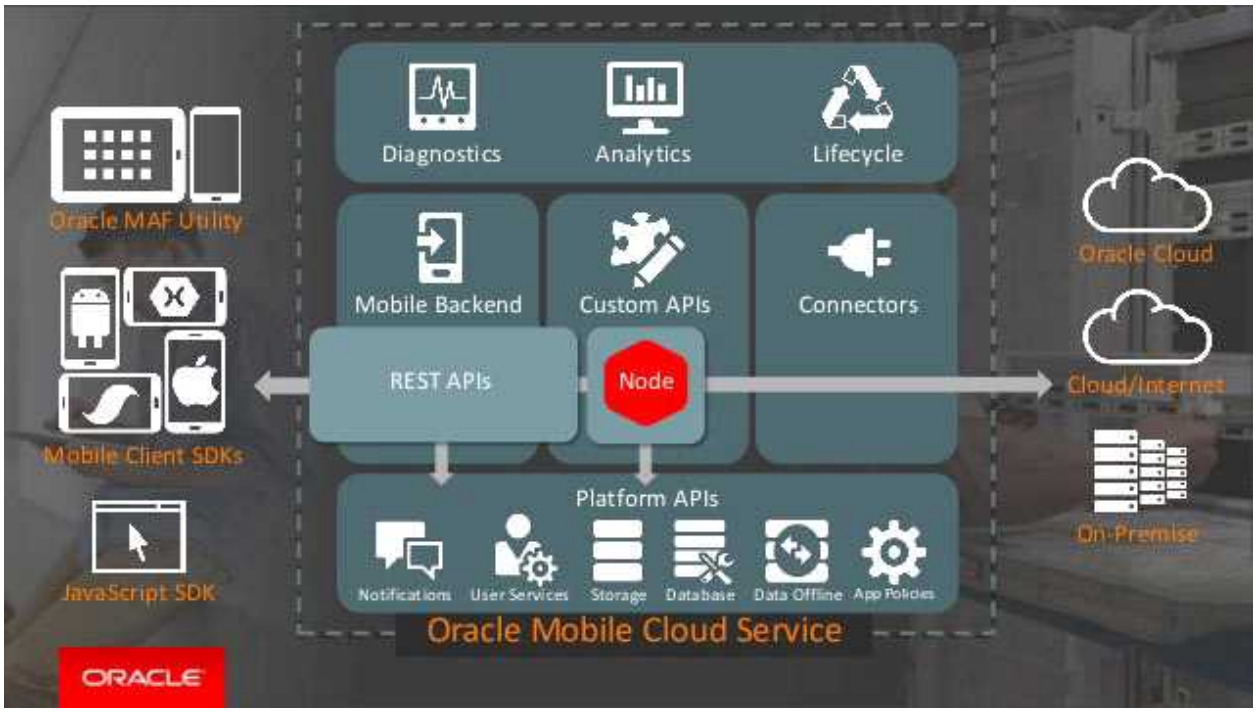
While debugging an API implementation and looking at the message logs, you see the context as shown in the exhibit. Which statement is true about the purpose of the Request Correlation Id that is shown in the exhibit? (Choose the best answer.)

A. It associates all messages that originated from the same mobile client
B. It associates all identical error messages related to a request.
C. It associates all custom code messages logged for a specific API implementation across all requests.
D. It associates all messages logged for a specific request.
E. It associates all messages for a client session.

Answer: C

Question: 2

View the Exhibit.



Which statement correctly identifies the purpose of the symbol labeled “Node”?

A. It contains the dictionary of all custom API REST resources.
B. It represents the Node.js implementation of custom APIs.
C. It references the custom APIs that are exposed to the mobile application as a Node.js library.
D. It refers to the custom APIs that are to be downloaded and executed on the mobile client by using a Node.js library.

Answer: B

Question: 3

Which statement correctly describes a functionality of the MCS client SDKs?

A. They can be used to call only the custom APIs defined in MCS.
B. They can be used to call only the MCS platform APIs.
C. The MCS SDKs for iOS and Android manage capabilities such as storing data when you work offline.
D. They provide a library of native user interface widgets for building features such as login pages.

Answer: B

Question: 4

Identify four authentication methods that can be configured for an MCS mobile backend.

A. OpenID
B. HTTP Basic
C. SAML
D. Oracle Access Manager Mobile and Social
E. OAuth Consumer
F. Enterprise Single Sign-On (SSO)
G. Facebook Login

Answer: B,E,F,G

Question: 5

Which option is a typical example of custom analytic events?

A. the screens that a user visits in the mobile application
B. user's name
C. user’s latitude and longitude
D. information about a user’s device model and operating system
E. MCS custom APIs being called from the mobile application

Answer: D

Question: 6

Which statement is true about establishing a security policy for a connector API?

A. You do not have to take a client's authentication type into account when selecting a security policy for a connector API, except when Facebook social login is used.
B. You do not have to take a client's authentication type into account when selecting a security policy for a connector API because security configuration is totally decoupled for clients and connector APIs.
C. You must take a client's authentication type into account when selecting a security policy for a connector API, but only if HTTPS connections are used.
D. You must take a client's authentication type into account when selecting a security policy for a connector API because mobile clients and connector APIs must use the same type of authentication for successful operation.
E. You must take a client's authentication type into account when selecting a security policy for a connector API, but only when using OAuth2 and Client Credential Flow.

Answer: C

Question: 7

A mobile user reports that he or she is not receiving push notifications sent from MCS for an application. All other users are successfully receiving notifications from the application. What are two correct explanations for this situation? (Choose two.)

A. The user has disabled notifications for the application by using the mobile device settings.
B. The application on the mobile device could not register to MCS.
C. An MCS team member blocked the user account from receiving push notification messages.
D. The push provider's certificate settings in the mobile backend client application configuration have expired and need to be renewed.

Answer: A,D

Question: 8

Which two capabilities are provided by the data offline and sync features? (Choose two.)

A. improved mobile application performance by caching data locally on the device rather than always making remote service calls to MCSB. mobile application access to data from any remote web service, including but not limited to, MCS
B. mobile application access to locally cached data while the device is disconnected
C. automatic caching of data from an on-premise solution to the database API within MCS

Answer: A,C

Explanation:

Reference https://blogs.oracle.com/mobile/going-offline-with-mcs-mobile-data-offline-sync