DUMPSARENA

SAP Certified Associate - SAP Mobile Platform Native and Hybrid Application Administration (SMP 3.0)

SAP C_SMPADM_30

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, SAP Mobile Platform 3.0 Overview	9
Topic 2, SAP Mobile Platform 3.0 Architecture	14
Topic 3, SAP Mobile Platform 3.0 Installation	8
Topic 4, SAP Mobile Platform 3.0 Administration	24
Topic 5, SAP Mobile Platform 3.0 Security	21
Topic 6, SAP Mobile Platform 3.0 Monitoring and Troubleshooting	24
Total	100

QUESTION NO: 1

Which authentication providers can be used for basic authentication when configuring an application definition in SMP 3.0? Note: There are 3 correct answers to this question.

A. HTTP/HTTPS Authentication

B. System Login (Admin Only)

C. Security Assertion Markup Language (SAML) 2.0

D. Kerberos

E. Directory Service - Lightweight Directory Access Protocol (LDAP)/ Active Directory (AD)

ANSWER: A B E

Explanation:

In SMP 3.0, basic authentication is based on a user ID and password supplied to the platform, with the configured authentication provider responsible for validating those credentials. **HTTP/HTTPS Authentication** supports this model by delegating credential validation to an HTTP or HTTPS endpoint. This is useful when an existing Web-based authentication service or infrastructure is responsible for authenticating users.

Directory Service - Lightweight Directory Access Protocol (LDAP)/ Active Directory (AD) is also suitable because SMP can validate the supplied user name and password against a corporate LDAP directory or Microsoft Active Directory. This enables applications to use centrally managed enterprise identities without maintaining a separate user store in SMP.

System Login (Admin Only) uses the SMP server's internal system-login credentials and supports basic user-name-and-password authentication for administrative access scenarios. It is intended for the administrative scope identified in its name, rather than general enterprise identity federation.

SAP's Mobile Platform documentation describes authentication-provider configuration as part of application and server security administration. See the SAP Mobile Platform documentation on SAP Help Portal and the SAP Mobile Platform product support page for product documentation and lifecycle resources.

QUESTION NO: 2

Which values can be set to increase the detail of information written to the server log?

Note: There are 2 correct answers to this questions.

A. Console

B. Debug

C. Error

D. Trace

ANSWER: B D

Explanation:

Debug and Trace are the logging values that increase the amount of diagnostic detail written by SAP Mobile Platform Server. Debug logging provides detailed information useful for investigating application and server processing, such as execution flow and internal component activity. Trace provides an even finer-grained level of diagnostic output, allowing administrators to follow low-level processing when troubleshooting complex or intermittent issues. These levels are normally enabled temporarily and for the relevant logger or component, because the additional messages can increase log-file volume and may affect performance or storage consumption on a busy production server.

Using Debug first is generally appropriate when standard operational logging does not provide sufficient evidence. Trace is appropriate when Debug output still does not expose the required processing details. SAP Mobile Platform administration

guidance treats server logging as a configurable diagnostic facility, while the underlying logging-level model places Debug and Trace above normal operational severity levels in verbosity. For related SAP Mobile Platform documentation, see the SAP Mobile Platform documentation on SAP Help Portal. For the standard logging-level behavior and the relative verbosity of Debug and Trace, see the Apache Log4j logging-level documentation.

QUESTION NO: 3

Which operations are part of the OSGi bundle lifecycle in SAP Mobile Platform? Note: There are 3 correct answers to this question.

A. Install a bundle

B. Start a bundle

C. Update a bundle

D. Replicate a database

E. Register a mobile client

ANSWER: A B C

Explanation:

OSGi provides a modular runtime in which bundles can be installed, started, updated, stopped, and uninstalled. **Install** adds a bundle to the OSGi framework. **Start** activates the bundle so that its services and runtime behavior become available. **Update** replaces an installed bundle with a newer bundle version.

Database replication and mobile-client registration are SAP Mobile Platform functions, but they are not OSGi bundle-lifecycle operations. For background on the modular runtime model, see the OSGi specifications.

QUESTION NO: 4

Which datasource type satisfies these requirements?

* Mapping is controlled by the OData model

* Entity property names match table/column names

A. JDBC

B. ODC

C. SOAP

D. JPA

ANSWER: A

Explanation:

JDBC is the appropriate datasource type when the OData model itself controls the mapping to a relational database and the OData entity property names correspond directly to database table and column names. In SAP Mobile Platform, a JDBC-based data source is intended for direct access to relational data through SQL/JDBC connectivity. The service's OData model defines the entity sets, entity types, and properties exposed to mobile clients, while the simple naming convention enables those properties to be mapped directly to the underlying relational structures. This is especially suitable where the database schema is already available and no separate persistence-object mapping layer is intended.

The OData model provides the metadata contract consumed by clients: entity types describe structured business data and properties describe their fields. With JDBC, aligning those property names to the table and column names lets the server use the model-defined mapping convention for relational operations. This supports a straightforward database-to-OData

exposure pattern for native and hybrid mobile applications. SAP Mobile Platform documentation is available through the SAP Mobile Platform Help Portal; the OData metadata model is specified by the OASIS OData Common Schema Definition Language specification.

QUESTION NO: 5

Which statements are correct for an SAP Mobile Platform clustered deployment? Note: There are 2 correct answers to this question.

A. A load balancer can distribute client requests across available server nodes

B. Nodes must use a consistent shared configuration for deployed applications and services

C. Individual nodes no longer require monitoring

D. Adding a node automatically corrects backend connection errors

ANSWER: A B

Explanation:

A load balancer can distribute client requests across available server nodes is correct. A load balancer provides a common entry point and directs traffic to operational nodes, helping distribute processing demand.

Nodes must use a consistent shared configuration for deployed applications and services is also correct. Clustered nodes must be configured consistently so that a request handled by any available node receives the expected application, security, and service behavior.

A cluster does not eliminate the need to monitor every node, and adding a node does not automatically correct an invalid backend connection or security configuration. SAP Mobile Platform clustered deployment concepts are available through the SAP Mobile Platform documentation.

QUESTION NO: 6

Solution Manager can monitor system changes, such as OS-level changes and database changes. What is the name of this functionality?

A. Technical Available Monitoring

B. End-to-End Change Analysis

C. Workload Analysis

D. End-to-End Tracing

ANSWER: B

Explanation:

End-to-End Change Analysis is the SAP Solution Manager functionality used to identify and analyze changes across the technical landscape, including operating-system-level and database-related changes. It relies on configuration data collected for managed systems and enables administrators to compare configuration information over time. This provides a structured way to determine what changed in a system or landscape during a selected period, which is especially useful when investigating incidents, performance degradation, or unexpected behavior after a change.

In SAP Solution Manager, this capability is associated with Root Cause Analysis and uses the Configuration and Change Database data collected from managed systems. The analysis presents change history and comparison results for technical components, allowing operations teams to correlate a problem's timing with configuration modifications. This broad, end-to-end visibility is the key purpose captured by the term End-to-End Change Analysis. SAP describes its Solution Manager application lifecycle and operations capabilities at SAP Support Portal: SAP Solution Manager; further SAP documentation is available through the SAP Help Portal: SAP Solution Manager.

QUESTION NO: 7

Which of the following are advantages of using HTTPS between a mobile client and SAP Mobile Platform Server? Note: There are 3 correct answers to this question.

A. Encryption of data in transit

B. Server identity validation

C. Integrity protection for transmitted data

D. Automatic authorization to all backend resources

E. Elimination of the need for application authentication

ANSWER: A B C

Explanation:

Encryption of data in transit is an advantage because HTTPS uses TLS to protect application requests and responses from disclosure while they travel across untrusted networks. **Server identity validation** is also provided when the client validates the certificate presented by the server, helping the client confirm that it is communicating with the intended server. **Integrity protection for transmitted data** is another benefit because TLS detects modification of protected traffic in transit.

HTTPS does not replace application authentication or authorization. Those controls still determine who can use an application and which resources that identity may access. See the HTTP Semantics specification and the SAP Mobile Platform documentation.

QUESTION NO: 8

You are configuring a Security Profile with Kerberos as the authentication provider. How do you use Kerberos to ensure successful authentication?

A. Kerberos must be used with another authentication provider and placed anywhere other than first in the stack of providers in the profile.

B. Kerberos must be the only authentication provider configured.

C. Kerberos must be used with another authentication provider and placed last in the stack of providers in the profile.

D. Kerberos must be used with another authentication provider and placed first in the stack of providers in the profile.

ANSWER: D

Explanation:

Kerberos must be used with another authentication provider and placed first in the stack of providers in the profile. In SAP Mobile Platform, a security profile can chain authentication providers, and their order controls the authentication flow. Placing the Kerberos provider first allows SMP to process the client's Kerberos credentials and establish the authenticated Kerberos context before the subsequent provider is invoked. The additional provider is required to complete the profile's authentication configuration and to supply the identity processing needed by the application's security setup.

This ordering is particularly important for integrated enterprise authentication, where a user may already have a Kerberos ticket issued by the corporate domain. The Kerberos provider must receive and validate that ticket at the beginning of the chain, so downstream authentication processing can use the resulting principal consistently. Administrators should also ensure that the SMP host, service principal name, keytab, KDC connectivity, and time synchronization are configured correctly; these are essential operational prerequisites for Kerberos ticket validation. SAP Mobile Platform documentation is available through the SAP Mobile Platform Help Portal, and SAP's general product documentation entry point is the SAP Help Portal.

QUESTION NO: 9

Which HTTP status code indicates that a request requires user authentication?

A. HTTP 200

B. HTTP 401

C. HTTP 404

D. HTTP 500

ANSWER: B

Explanation:

HTTP 401 is correct. The 401 Unauthorized status code indicates that the request has not been applied because valid authentication credentials are required for the target resource. A server commonly includes an authentication challenge in the response so that the client can supply appropriate credentials.

This status is distinct from HTTP 403, which indicates that the server understood the request but refuses to authorize it. See RFC 9110, HTTP 401 Unauthorized.

QUESTION NO: 10

What are WebSockets?

A. They are a standard for allowing bidirectional real-time communication between clients and servers. encapsulated within another transport protocol. like HTTPS.

B. They define the necessary socket communication layer to allow encrypted ideal-time data communication between clients and servers.

C. They provide a real-time bi-directional communication protocol to use in place of HTTPS lo provide secure and encrypt data between clients and servers.

D. they are another standard method for encrypting communication data between clients and servers like HttPS.

E. They are a standard protocol for persistent, full-duplex, bidirectional real-time communication between clients and servers.

ANSWER: E

Explanation:

WebSockets are a standardized communications protocol that provides full-duplex, bidirectional communication between a client and a server over a single, persistent connection. A client initially establishes the connection through an HTTP-based handshake and requests an upgrade to the WebSocket protocol. Once the upgrade succeeds, either endpoint can send messages at any time without the client repeatedly issuing HTTP requests or the server relying on polling. This makes WebSockets well suited to real-time scenarios, such as application notifications, live status updates, messaging, and synchronization events.

WebSocket itself is not an encryption mechanism. Secure WebSocket connections use the `wss://` scheme, which protects the connection with TLS, analogous to the relationship between HTTPS and HTTP. The protocol is defined by the IETF in RFC 6455, including its opening handshake, framing, and full-duplex message exchange model. See RFC 6455: The WebSocket Protocol and the MDN WebSocket API overview.