# 1Z0-102$^{Q\&As}$

Oracle WebLogic Server 11g: System Administration

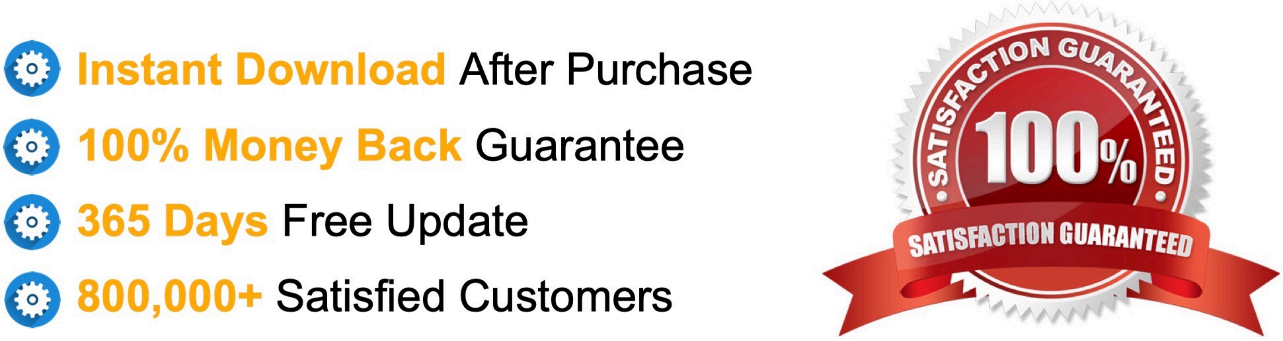
## Pass Oracle 1Z0-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.leads4pass.com/1z0-102.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Oracle Official Exam Center


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED 100%
SATISFACTION GUARANTEED

**QUESTION 1**

Which three tasks can be performed by the Node manager?

A. Start a server.

B. Define a node server.

C. Host the Node Manager console.

D. Automatically restart a failed server.

E. Kill a failed application on a server.

F. Kill the process of a server that did not shut down properly.

Correct Answer: ABD

Node Manager enables you to perform these tasks:

*

Start and stop remote Managed Servers. (A)

*

Monitor the self-reported health of Managed Servers and automatically kill server instances whose health state is "failed".

*

Automatically restart Managed Servers that have the "failed" health state, or have shut down unexpectedly due to a system crash or reboot. (D)

**QUESTION 2**

A managed server, myserver1, has a boot.properties file in the security directory. It was started with the startManageWeblogic.sh script(.cmd in windows) and his boot.properties file was used for its startup credentials.

You just used the administration console to change all administrator passwords. To continue using boot.properties, what can you do?

A. This is not possible. A boot.properties file can be used only with the Administration Server.

B. Delete boot.properties. In the administration console, under the myserver configuration, select Generate Boot Identity file.

C. You need not do anything- The password in boot .properties was automatically updated by administration console when you changed the password.

D. Edit boot.propetties. Type over the encrypted password with the new password in clear text. The next time myserver1 is started, it will encrypt the password in the file.

E. Delete boot .properties. Use the WLST encrypt () command to create a new boot.properties file containing the new password. Copy that file into the security directory of myserver1

Correct Answer: D

If you install the WebLogic Server Examples component, the default user weblogic is created that has permission to start and stop WebLogic Server. The default password is welcome1. If you change the password of the weblogic user, WebLogic Server does not automatically update this password in the boot.properties file, which is located in the DOMAIN_NAME/servers/AdminServer/security directory.

If you change the password for user weblogic, you can use either of the following workarounds so that you can continue to boot a WebLogic Server instance via that username and its new password:

*

Remove the boot.properties file. Subsequently each time you start WebLogic Server, you are prompted for the username and password. The changed password for the weblogic user will be accepted.

*

Modify the existing boot.properties file, changing the username and password as follows:

username=weblogic password=welcome1 Subsequently during the server startup process, the boot.properties file is encrypted again.

Reference: Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help 11g Release 1, Limitation Regarding User weblogic http://docs.oracle.com/cd/E15523_01/web.1111/e13708/overview.htm

**QUESTION 3**

Identify two supported methods of deploying a JMS module to a domain.

A. Create a module by using the administration console.

B. Load a module into the WebLogic database.

C. Include a module file within a web application archive.

D. Include a module file within an enterprise application archive.

E. Define a module within an existing JDBC module.

Correct Answer: AD

A: Main Steps for Creating Packaged JMS Application Modules

Follow these steps to configure a packaged JMS module:

If necessary, create a JMS server to target the JMS module to, as explained in "Configure JMS Servers" in the Administration Console Online Help.

Create a JMS system module and configure the necessary resources, such as queues or topics, as described in "Configure JMS system modules and add JMS

resources" in the Administration Console Online Help.

The system module is saved in config\jms subdirectory of the domain directory, with a "- jms.xml" suffix.

Copy the system module to a new location, and then:

Give the module a unique name within the domain namespace.

Delete the JNDI-Name attribute to make the module application-scoped to only the application. Add references to the JMS resources in the module to all

applicable J2EE application component\\'s descriptor files, as described in Referencing a Packaged JMS Application Module In Deployment Descriptor Files.

Package all application modules in an EAR, as described in Packaging an Enterprise Application With a JMS Application Module.

Deploy the EAR, as described in Deploying a Packaged JMS Application Module.

D: JMS application modules can be packaged as part of an Enterprise Application Archive (EAR), as a packaged module. Packaged modules are bundled with an

EAR or exploded EAR directory, and are referenced in the weblogic-application.xml descriptor. The packaged JMS module is deployed along with the Enterprise

Application, and the resources defined in this module can optionally be made available only to the enclosing application (i.e., as an application-scoped resource).

Such modules are particularly useful when packaged with EJBs (especially MDBs) or Web Applications that use JMS resources. Using packaged modules

ensures that an application always has required resources and simplifies the process of moving the application into new environments.

Reference: Packaging JMS Application Modules In an Enterprise Application

**QUESTION 4**

YCMJ are viewing the deployments in the administration console. A web application that is targeted to the Managed Server named server01 has a State of "Now." Which statement best explains this State?

A. Server01 is running and the application has been installed.

B. Sarver01 is shut down and the application has been installed.

C. Server01 is running and the application has not been installed.

D. Server01 is shut down and the application has not been installed.

E. Server01 is running and the application was installed for the first time.

F. Server01 is running and the application has been installed, but is not servicing requests.

Correct Answer: E

**QUESTION 5**

Which three statements are true about WebLogic users and groups?

A. A user is associated with a single security provider.

B. A user can be a member of several groups.

C. A group can contain other groups.

D. A group consists of a name and a password.

E. A group is associated with multiple security providers.

F. Both users and groups are assigned a keystore.

Correct Answer: ABC

B: For efficient security management, BEA recommends adding users to groups. A group is a collection of users who usually have something in common, such as

working in the same department in a company.

C: Example of group nesting:

Every user is a member of the everyone group.

The users group is nested within the everyone group.

Note: Security Providers - are modules that provide security service to application to protect Weblogic resource.

Types of security providers in WebLogic Server are

Authentication Provider, Authorization Provider, Auditing Providers, Credential Mapping Provider, Identity Asser- tion Provider, Principal Validation Provider,

Adjudication Providers, Role Mapping Providers, Certificate Lookup and Validation Providers, Keystore Providers and Realm Adapter providers

Incorrect answers:

D: There is no password for a group.

F: A keystore is a mechanism designed to store password-protected store private keys and trusted CA certificates. In the WebLogic Server security architecture, the WebLogic Keystore provider is used to access keystores. You cannot use a custom Keystore provider with WebLogic Server.

References: Securing WebLogic Resources, Users, Groups, And Security Roles