# 1Z0-102Q&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.pass2lead.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

**QUESTION 1**

Which two statements are true about Log Filters?

A. Log Filters are created at the domain level.

B. You do not have to lock the configuration to create Log Filters.

C. You can apply a Log Filter to the server log, but not to standard out.

D. The administration console assists in the creation of Log Filter expressions

Correct Answer: AD

A (not B): For any given WebLogic Server instance, you can override the default filter and create a log filter that causes a different set of messages to be written to

the domain log file.

Note:

To create and configure a log filter:

1.

If you have not already done so, in the Change Center of the Administration Console, click Lock and Edit (not B) (see Use the Change Center).

2.

In the left pane of the Console, select the name of the active domain in the Domain Structure panel.

3.

On the Configuration: Log Filters page, click New.

4.

On the Create a New Log Filter page, enter a value to identify the filter in the Name field.

5.

Click Finish.

The new log filter appears in the Log Filters table.

6.

To configure a filter expression, in the Log Filters table, click the log filter name.

7.

On the Configuration page, in the Filter Expression text box, enter criteria for qualifying messages.

A filter expression defines simple filtering rules to limit the volume of log messages written to a particular log

destination.

See D) below.

8.

Click Save.

The filter and filter expression are listed in the Log Filters table.

D: Log Filter Configuration

Use this page to define a custom log filter to restrict the set of messages that one or more servers send to a message destination, such as the domain log,

standard out, server log file, or memory buffer of recent log events.

You can click Edit to type or paste in an expression directly, using WLDF Query Language syntax (see Related Topics, below); or you can click Add Expression to

construct an expression by choosing items from lists.

Once you create a filter, you cannot change its name. Instead, you must create a new filter under a different name.

Reference: Administration Console Online Help, Log Filter Configuration Reference: Administration Console Online Help, Create log filters

**QUESTION 2**

An EJB application is targeted to a cluster. Remote EJB clients can therefore take advantage of WebLogic Server\\'s load balancing and failover capabilities.

However, a proxy server exists between the clients and the cluster, which performs IP address translation. Which cluster attribute should you modify to ensure that load balancing and failover work correctly?

A. Multicast Address

B. Persistent Store

C. Cluster Address

D. Migration Basis

E. Replication Channel

Correct Answer: C

Note:

Updating Proxy Service Configurations for an Expanded Cluster

If your AquaLogic Service Bus configuration includes one or more proxy services that use JMS endpoints with cluster addresses, then you must also perform the

following procedure using the AquaLogic Service Bus Console after adding the new managed server to the cluster:

1.

In the Change Center, click Create to create a session.

2.

Using the Project Explorer, locate and select a proxy service that uses JMS endpoints with cluster addresses.

3.

At the bottom of the View Details page, click Edit.

4.

If there is a cluster address in the endpoint URI, add the new server to the cluster address.

5.

On the Edit a Proxy Service - Summary page, click Save.

6.

Repeat step 2. through step 5. for each remaining proxy service that uses JMS endpoints with cluster addresses.

7.

In the Change Center, click Activate.

The proxy services are now configured for operation in the extended domain.

Reference: eDocs Home > BEA AquaLogic Service Bus 2.0 Documentation > Deployment Guide > Configuring a Clustered Deployment

**QUESTION 3**

You wish to restrict access to a JMS queue so that only specific accounts may receive messages from the queue. Identify two steps that, when performed together, implement this security requirement.

A. Create a policy for queue\\'s URL pattern.

B. Add a policy to the queue and associate it with a role.

C. Configure an identify assertion provider.

D. Acquire the domain configuration lock.

E. Create a global role and assign users to it.

Correct Answer: BE

B:

Security policy for a JMS Queue (Resource Level).

When you define a security policy for an individual destination on a JMS server, you can protect all operations of the

destination.

a.

Login into the Admin server console > Navigate to the Queue that needs to be secured.

b.

Click on the security tab > Policies sub tab.

You can see a small drop down list, which lists the set of the operations that can be protected.

c.

Click Add Conditions to add the policy conditions.

d.

From the predicate list, specify the policy conditions.

e.

Specify the role (the global created in E below) which needs to have the access permissions for the JMS Queue. Click Add > Finish.

E: Create a Global Role and assign the appropriate user accounts to it.

Note: There are two ways of securing the JMS resources.

1.

At the JMSModule level (Group level), where a single security policy is specified for a set of JMS resources.

2.

At the individual JMS resource level, which provides much more grained controlled over the operations that you want to secure.

Reference: SECURING WEBLOGIC JMS RESOURCES

**QUESTION 4**

Identify three attributes of a WebLogic cluster.

A. Listen Address

B. Cluster Address

C. Cluster Factory

D. Messaging Mode

E. Servers

F. Targets

Correct Answer: BDE

WebLogic Cluster Attributes includes:

B: * ClusterAddress Defines the address to be used by clients to connect to this cluster. This address may be either a DNS host name that maps to multiple IP addresses or a comma separated list of single address host names or IP addresses. If network channels are configured, it is possible to set the cluster address on a per channel basis.

D: The Message Mode of a cluster can be either Unicast or multicast.

E: Managed Servers are included in a WebLogic cluster.

Note: The config.xml file is an XML document that describes the configuration of a WebLogic Server domain. config.xml consists of a series of XML elements. The Domain element is the top- level element, and all elements in the Domain descend from the Domain element. The Domain element includes child elements, such as the Server, Cluster, and Application elements. These child elements may have children of their own. For example, the Server element includes the child elements WebServer, SSL and Log. The Application element includes the child elements EJBComponent and WebAppComponent.

Each element has one or more configurable attributes. An attribute defined in config.dtd has a corresponding attribute in the configuration API. For example, the Server element has a ListenPort attribute, and likewise, the weblogic.management.configuration.ServerMBean has a ListenPort attribute. Configurable attributes are readable and writable, that is, ServerMBean has a getListenPort and a setListenPort method.

Reference: WebLogic Server Configuration Reference, Cluster attributes
http://docs.oracle.com/cd/E13222_01/wls/docs81/config_xml/Cluster.html#447012

**QUESTION 5**

Managed Server Independence enabled is not selected in the configuration of myserver1. Which statement is true?

A. Only the Node Manager can start myserver1

B. Only a local start script can start myserver1

C. Myserver1 cannot be part of a cluster.

D. The Administration Server must be available before starting myserver1

Correct Answer: D

To prevent the Administration Server from becoming a single point of failure, Managed Servers can always function without the presence a running Administration Server. When a Managed Server starts, it contacts the Administration Server to retrieve its configuration information. If a Managed Server is unable to connect to the specified Administration Server during startup, it can retrieve its configuration directly by reading a copy of the config.xml file and other files located on the Managed Server\\'s own file system. A Managed Server that starts in this way is running in Managed Server Independence mode. In this mode, a server uses cached application files to deploy the applications that are targeted to the server.

Reference: Overview of WebLogic Server System Administration, Managed Server Indepenence
http://docs.oracle.com/cd/E13222_01/wls/docs81/adminguide/ overview.html