PassQueen
a.k.a dumpsqueen.com

D Application Server Network Deployment V8.5.5 and Liberty Profile System Administration

IBM C9510-401

Version Demo

Total Demo Questions: 10

Total Premium Questions: 103

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Installation and Configuration	19
Topic 2, Application Deployment	14
Topic 3, Security	20
Topic 4, Administration	23
Topic 5, Monitoring and Tuning	13
Topic 6, Problem Determination	14
Total	103

QUESTION NO: 1

A new cell contains a cluster with members defined in two managed nodes running on two different machines. The cell also contains two unmanaged nodes running on HTTP servers with HTTP plug-in. Session persistence has been enabled.

Which additional component(s) can the system administrator configure to make this environment highly available?

A. Enable administrative security.

B. Configure a DMZ secure proxy.

C. Configure High Performance Extensible Logging.

D. Configure primary and backup load balancers for the HTTP servers.

ANSWER: D

Explanation:

Configuring primary and backup load balancers for the HTTP servers completes high availability at the web-server entry tier. The application cluster already provides redundancy for application processing because its members run on separate managed nodes and machines. Session persistence ensures that session state can be recovered or accessed when a request is routed to another available cluster member. However, clients still need a resilient way to reach the HTTP servers themselves. A load balancer distributes incoming client traffic across the available HTTP servers, allowing requests to continue through a surviving web server when one becomes unavailable. Providing a backup load balancer also removes the load balancer as a single point of failure. The HTTP Server plug-in then routes requests from the selected web server to available cluster members, using its generated configuration and server health information. This layered design provides availability from the client-facing web tier through the application-server cluster. IBM documents the use of load balancers as part of highly available WebSphere topologies and describes the web-server plug-in's role in routing requests to application servers. See WebSphere Application Server high-availability topologies and Web server plug-ins.

QUESTION NO: 2

A system administrator is asked by a development team to monitor the performance of a newly deployed EJB application. The administrator noticed that the heap size of the application server is growing.

What should the administrator do to fix the problem using ORB settings?

A. Use J2EE managed object MBeans.

B. Enable the pass by reference option.

C. Disable the application scoped resources in the application deployment descriptor.

D. Ensure that Process embedded configurations is not selected when exporting the EAR.

ANSWER: B

Explanation:

Enable the pass by reference option. In WebSphere Application Server, the ORB normally uses pass-by-value behavior for EJB parameter objects, including when an EJB client and its target EJB are in the same server JVM. Pass-by-value requires the runtime to create copies of parameter objects, which increases object allocation activity and consequently adds pressure to the Java heap and garbage collector. For an application with frequent local EJB invocations or substantial parameter graphs, those temporary copies can materially contribute to observed heap growth and reduced performance.

When pass by reference is enabled, eligible local EJB calls use references to the existing objects rather than serializing or copying the parameter objects. This reduces transient allocations and heap consumption, directly addressing the ORB-related overhead described in the scenario. The setting is available from the application server's Object Request Broker configuration in the administrative console. Before enabling it, the development team should confirm that the application does not rely on remote-style copy isolation, because a callee can observe or modify the same object instance supplied by the caller. IBM documents the ORB configuration and the pass-by-reference behavior in its ORB settings documentation and EJB pass-by-reference documentation.

QUESTION NO: 3

An application deployed to a multi-node cluster is reported to have slowness and hung threads. A system administrator is asked to review the logs on each node and identify if the hung threads are a false alarm.

How can the administrator determine that the hung threads are a false alarm?

Analyze the:

A. ffdc logs

B. SystemErr.log

C. SystemOut.log

D. native_stderr.log

E. javacore files (thread dumps)

ANSWER: E

Explanation:

The correct item to analyze is the javacore files (thread dumps). A potentially hung-thread message means that a server thread has exceeded the configured hung-thread threshold; it does not, by itself, establish that the thread is truly deadlocked or unable to make progress. A javacore captures the Java threads in the JVM, including each thread's name, state, stack trace, owned monitors, and waiting or blocking relationships. The administrator should match the thread name reported by the hung-thread warning to that thread in javacores collected from the affected cluster members.

To establish that the warning is a false alarm, collect multiple javacores at short, regular intervals and compare the target thread's stack. If its stack location changes, or it is progressing through expected application or I/O processing, the thread is active despite having exceeded the threshold. The dumps also provide the evidence needed to distinguish expected long-running work from an actual wait, lock contention, deadlock, or blocked external dependency. IBM documents that hung-thread detection reports *potentially* hung threads and recommends using javacore data for diagnosis. See IBM's hung thread detection documentation and its javacore reference.

QUESTION NO: 4

A system administrator has started a Liberty profile server using the default values. Later, the administrator modified the server.xml file for the server to include

dropins="${server.config.dir}/applications" dropinsEnabled="true"/>

The administrator placed the application ServletApp.war in the apps directory under ${server.config.dir}. While accessing the correct URL for the home page of the application, the error "Context Root Not Found" occurs in the browser.

How can the administrator resolve this error?

A. Restart the Liberty profile server.

B. Install the ServletApp.war file using the Integrated Solutions Console (ISC).

C. Place the ServletApp.war file in the directory named dropins under ${server.config.dir}.

D. Place the ServletApp.war file in the directory named applications under ${server.config.dir}.

ANSWER: D

Explanation:

The configured `applicationMonitor` setting enables drop-in application deployment and explicitly sets the monitored drop-ins location to `${server.config.dir}/applications`. Liberty therefore polls that configured directory for deployable application archives, such as a WAR file. Since `ServletApp.war` was instead copied to an `apps` directory, it is

outside the location that Liberty is monitoring and is not deployed. Consequently, no web application is available at the requested context root.

Placing `ServletApp.war` in the directory named `applications` under `${server.config.dir}` aligns the archive location with the configured `dropins` attribute. With the update trigger set to polling, Liberty detects the archive during its polling cycle and deploys it. After deployment completes, the application's context root becomes available without requiring installation through an administrative console. Liberty documentation describes the `applicationMonitor` configuration, including its drop-ins directory and polling behavior, at IBM: applicationMonitor configuration. IBM also documents application deployment methods for Liberty at IBM: Deploying applications in Liberty.

QUESTION NO: 5

A system administrator has deployed an application. The development team has updated a new version of this application. The administrator needs to immediately deploy this updated application and guarantee that only this new edition is used by clients and that any service requests for the application are queued during the deployment of the new application.

How can the administrator achieve this task without any downtime to the application?

A. Perform a soft rollout.

B. Perform a hard rollout.

C. Perform an atomic rollout.

D. Perform a concurrent activation rollout.

ANSWER: C

Explanation:

Perform an atomic rollout. An atomic rollout is the application-edition rollout method designed for a switch that must be consistent for every client. WebSphere activates the new application edition across the deployment target as a single coordinated change. During the activation interval, incoming requests are held in the request queue rather than being dispatched to an instance running either the previous edition or a partially activated set of members. After activation completes, those queued requests are processed by the new edition. This behavior provides the required guarantee that clients use only the new edition once the rollout takes effect, while preserving service availability from the client perspective because requests are queued instead of rejected. The administrator should ensure that the deployment environment has sufficient queue capacity and that the new edition has been fully installed and validated before initiating the rollout. IBM documents application edition management and its rollout behavior for Network Deployment environments in its WebSphere Application Server documentation: Application edition management and Application edition rollout options.

QUESTION NO: 6

A system administrator has been asked to uninstall an application from a cluster running in a WebSphere Application Server Network Deployment cell. This application was installed from the Integrated Solutions Console (ISC). The monitored directory for the cluster is .

What step(s) can the administrator perform to uninstall the application?

A. Delete the application file from .

B. Stop the running cluster.Delete the application file from .

C. Stop the running cluster.Copy the application file to .Delete the application file from .

D. Create a properties file to describe the deletion of the application file.Copy the properties file to .

ANSWER: D

Explanation:

Create a properties file to describe the deletion of the application file.Copy the properties file to .

is correct because WebSphere Application Server Network Deployment supports application administration through monitored directories and application properties files. A properties file placed in the monitored directory is detected by the deployment manager and processed as an administrative deployment request. To remove an existing deployed application, the file describes an uninstall action and identifies the target application. Once the properties file is copied or dragged into the cluster's monitored directory, WebSphere processes that request and uninstalls the application from the configured cluster scope. This mechanism is useful for repeatable, scripted, and unattended administration; it does not require the administrator to use the Integrated Solutions Console for every deployment operation. The application's having originally been installed through the console does not prevent it from being uninstalled with a monitored-directory properties file, because both methods manage the same cell configuration. IBM documents that properties files can be used to install, update, and uninstall deployed applications and modules by placing the file in a monitored directory. See IBM WebSphere Application Server: monitored-directory application deployment and IBM Knowledge Center: application properties files.

QUESTION NO: 7

A system administrator has created a Jython script called globalScript.py.

What should the administrator do to ensure globalScript.py is loaded when the wsadmin shell is used?

A. Compile globalScript.py to a Java class in the bin directory.

B. Invoke wsadmin with the argument –profileName globalScript.py.

C. Modify the configureCustomProperty script to import globalScript.py.

D. Set the script profiles in the wsadmin.properties file to load globalScript.py.

ANSWER: D

Explanation:

Set the script profiles in the wsadmin.properties file to load globalScript.py. WebSphere Application Server uses the wsadmin.properties configuration file to control wsadmin scripting behavior, including scripts that are automatically loaded when an interactive wsadmin session starts. The `com.ibm.ws.scripting.profiles` property identifies one or more script-profile files to load. A script profile can contain Jython statements, such as importing a shared Jython module, making its functions and variables available for subsequent commands entered in the wsadmin shell. This is the supported mechanism for establishing reusable global scripting definitions rather than requiring an administrator to manually import the script in every session. The relevant wsadmin.properties file is associated with the profile from which wsadmin is run, so the administrator should update the appropriate profile's properties file and specify the script profile that loads `globalScript.py`. IBM documents the scripting properties, including the script-profiles setting, in its wsadmin properties reference. See wsadmin.properties file and Starting the wsadmin scripting tool.

QUESTION NO: 8

The installation of WebSphere Application Server did not complete successfully, and a system administrator needs to troubleshoot the installation.

What can the administrator do to identify the cause of the installation failure?

A. Run the installver command with the appropriate command line options.

B. Check the files under the Agent data location of IBM Installation Manager.

C. Check the files under the logs directory in the IBM Installation Manager agent data location.

D. Check the log.txt under .

ANSWER: C

Explanation:

Check the files under the logs directory in the IBM Installation Manager agent data location. IBM Installation Manager records installation activity, progress, warnings, errors, and exception details in its log files. These records are the primary diagnostic source when a WebSphere Application Server installation does not complete, because they capture the specific package operation being performed and the underlying failure reported by Installation Manager.

The administrator should review the installation logs, especially the most recent entries around the time the failure occurred, for error messages, return codes, prerequisite or repository-access issues, permission failures, and details about the affected package. The agent data location is particularly important because it contains Installation Manager operational data and logs; its default location varies by operating system and can also be configured during Installation Manager setup. Reviewing these files provides the evidence needed to determine the cause before retrying the installation or collecting data for IBM Support.

IBM documents Installation Manager troubleshooting and diagnostic logging in the Installation Manager troubleshooting documentation. WebSphere installation guidance is also available in the WebSphere Application Server Network Deployment installation documentation.

QUESTION NO: 9

A newly deployed application has authorization errors when invoking EJB methods from a servlet. An additional review indicates that users are authenticated, but do not have the correct authorization.

How can a system administrator fix the issue ensuring only authorized access?

A. Using the Integrated Solutions Console (ISC), map all security roles to the special subject Everyone.

B. Using the Integrated Solutions Console (ISC), map the security roles that are still not mapped to groups in the correct user registry.

C. Edit the application using an assembly tool to add a security constraint for the servlet and reinstall the application.

D. Edit the application using an assembly tool to remove the security constraint defined for the servlet and reinstall the application.

ANSWER: B

Explanation:

Using the Integrated Solutions Console (ISC), map the security roles that are still not mapped to groups in the correct user registry. is correct because authentication and authorization are distinct steps in WebSphere Application Server security. The successful authentication described in the scenario establishes the caller's identity, but access to protected servlet resources and EJB methods also requires that the caller be granted an application security role. Application deployment descriptors define those roles, while the administrator maps each role to the appropriate users or, more commonly, groups in the configured user registry.

In the ISC, the administrator can open the deployed enterprise application's security-role mapping configuration and associate each required role with the registry group that contains the intended users. After saving the configuration and synchronizing nodes where applicable, WebSphere can evaluate the caller's group membership and authorize invocation of the EJB method only when the caller belongs to a group mapped to the required role. This preserves least-privilege access: authorization is granted specifically to the appropriate registry groups rather than broadly to all authenticated identities. IBM documents this deployment-time administrative task under mapping users and groups to roles.

QUESTION NO: 10

There are many applications deployed in a large WebSphere Application Server cluster. A system administrator is required to give Configurator role access to a developer for a single application deployed in that cluster.

How should the administrator meet this requirement and restrict Configurator role access for a single application?

A. Create a J2C authentication alias for that developer.

B. Create an Administrative user role and provide Configurator access to the developer.

C. Create an Administrative group role and provide Configurator access to the developer.

D. Create an administrative authorization group, scope it only for that application and create an Administrative user or group role to give Configurator access to the developer.

ANSWER: D

Explanation:

Create an administrative authorization group, scope it only for that application and create an Administrative user or group role to give Configurator access to the developer. WebSphere Application Server fine-grained administrative security supports authorization at the level of an individual resource rather than granting a cell-wide administrative role. An administrative authorization group is the mechanism used to collect the resource or resources that require the same administrative privileges. In this case, the target application is assigned to its own authorization group, which establishes the required administrative scope.

The administrator then maps the developer, either directly as an administrative user or through an administrative group, to the Configurator role for that authorization group. The Configurator role permits configuration changes for resources within the assigned authorization group, allowing the developer to administer the intended application while maintaining the required resource-specific boundary. This configuration is appropriate for a shared, large cluster because the authorization is associated with the selected application resource, not with every application deployed in the cell or cluster.

IBM documents this capability as fine-grained administrative security and describes using administrative authorization groups to assign administrative roles for specific resources. See Fine-grained administrative security and Administrative authorization groups.