Free Questions for C9510-401 by actualtestdumps

Shared by Arnold on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A system administrator needs to view the list of certificates for unmanaged web server located on a remote system.

How should the administrator do this?

Options:

A- View the plugin-cfg.xml

B- Look at the SSL configuration in the httpd.conf

C- Use iKeyman to view the keyring.

D- Use the administrative console to check the content of the cell default keystore.

Answer:

C

Explanation:

You do not have a secure network connection until you have created a key for secure network communications and received a certificate from a certificate authority (CA) who is designated as a trusted CA on your server. Use IKEYMAN to create the key database file, public-private key pair, and certificate request. After you receive the CA-signed certificate, use IKEYMAN to receive the certificate into the key database where you created the original certificate request.

References: http://www-01.ibm.com/software/webservers/httpservers/doc/v10/ibm/9atikeyu.htm

Question 2

Question Type: MultipleChoice

A system administrator needs to deploy a new enterprise application which requires that application security be enabled, but, the existing applications in the cell cannot be executed with application security enabled. The cell has the global security and Java 2 security disabled.

How can the administrator handle this requirement?

Options:

A- Enable Java 2 security for the cell.Create a security domain with application security enabled.Associate the security domain to the new application.

B- Enable Java 2 security for the cell.Create a security domain with application security enabled.Associate the security domain to a new cluster to be used to deploy the new application.

C- Enable administrative security for the cell.Create a security domain with application security enabled.Associate the security domain at the application level for the new application.

D- Enable administrative security for the cell.Create a security domain with application security enabled.Associate the security domain to the new cluster where the new application is deployed.

Answer:

C

Explanation:

When Java 2 security is enabled for a WebSphere Application Server, all the applications that run on WebSphere Application Server undergo a security check before accessing system resources. An application might need a was.policy file if it accesses resources that require more permissions than those granted in the default app.policy file

References: https://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/tsec_waspolicy.html

Question 3

Question Type: MultipleChoice

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?

Options:

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

Question 4

Question Type: **MultipleChoice**

A web application has a configured session timeout of eight hours and a default LTPA token timeout of two hours. After every two hours, the users have to log in again from their HTTP browser. The system administrator is required to make configuration changed so users only have to log in once, while keeping the above mentioned timeouts the same. The authentication mechanism available is Kerberos.

How should the administrator do this?

Options:

A- Configure the SIP digest authentication.

B- Configure the SPNEGO Web or SPNEGO TAI.

C- Enable Session Management Security Integration.

D- Ensure Web Inbound security attribute propagation is enabled.

Answer:

B

Explanation:

In WebSphere Application Server Version 6.1, a trust association interceptor (TAI) that uses the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) to securely negotiate and authenticate HTTP requests for secured resources was introduced. This function was deprecated In WebSphere Application Server 7.0. SPNEGO web authentication has taken its place to provide dynamic reload of the SPNEGO filters and to enable fallback to the application login method.

References: https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/csec_ssovo.html

Question 5

Question Type: MultipleChoice

A system administrator is configuring the security of a new environment. The administrator has been asked to configure one LDAP server that has different sub-trees for business users and administration users.

What should the administrator do to implement the required security configuration?

Options:

A- Install and configure a TAI (Trust Association Interceptor)

B- Configure a security domain for the stand-alone LDAP server.

C- Use Federated repositories and configure the supported entity types.

D- Use Stand-alone custom registry and configure the flat file implementation.

Answer:

C

Explanation:

select the type of user registry that you need for your environment:

References: WebSphere Application Server V8.5 Administration and Configuration Guide for the Full Profile (July 2013), page 212

Question 6

Question Type: MultipleChoice

How can a system administrator secure a WebSphere Application Server environment to ensure that an application code will not be allowed to access any files in the server's file system?

Options:

A- Configure the CSIv2 outbound communications under RMI/IIOP security.

B- Configure the file-based repository and create the fileRegistry.xml file.

C- Enable Java 2 security and configure the app.policy and was.policy files.

D- Use the AdminTask deleteAuthorizationGroup to remove application access.

Answer:

C

Explanation:

When Java 2 security is enabled for a WebSphere Application Server, all the applications that run on WebSphere Application Server undergo a security check before accessing system resources. An application might need a was.policy file if it accesses resources that require more permissions than those granted in the default app.policy file

References: http://www.aiotestking.com/ibm/how-can-a-system-administrator-secure-a-websphere-application-server-environment-to-ensure-that-an-application-code-will-not-be-allowed-to-access-any-files-in-the-servers-file-system/

Question 7

Question Type: MultipleChoice

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?

Options:

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:

Fine-grained administrative security

In releases prior to WebSphere Application Server version 6.1, users granted administrative roles could administer all of the resources under the cell. WebSphere Application Server is now more fine-grained, meaning that access can be granted to each user per resource.

For example, users can be granted configurator access to a specific instance of a resource only (an application, an application server or a node).

To achieve this instance-based security or fine-grained security, resources that require the same privileges are placed in a group called the administrative authorization group or authorization group. Users can be granted access to the authorization group by assigning to them the required administrative role.

References: http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/csec_fineg_admsec.html?cp=SSEQTP_8.5.5%2F1-8-1-30-3-3

Question 8

Question Type: MultipleChoice

A customer has enabled LTPA as their authentication mechanism and has web resources that are not secured by proper security constraints. A system administrator is required to ensure that all web resources are secured.

How should the administrator accomplish this?

Options:

A- Enable "Authenticate when any URI is accessed".

B- Enable "Authenticate only when the URI is protected".Disable "Use available authentication data when an unprotected URI is

accessed".

C- Enable "Authenticate only when the URI is protected".Enable "Use available authentication data when an unprotected URI is accessed".

D- Map the application security roles to the configured user registry's groups.

Answer:

A

Explanation:

Authenticate only when the URI is protected

The application server challenges the web client to provide authentication data when the web client accesses a Uniform Resource Identifier (URI) that is protected by a Java Platform, Enterprise Edition (Java EE) role. The authenticated identity is available only when the web client accesses a protected URI.

This option is the default Java EE web authentication behavior that is also available in previous releases of WebSphere Application Server.

References: https://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.base.doc/ae/usec_webauth.html

Question 9

Question Type: MultipleChoice

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?

Options:

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:

The Object Request Broker (ORB) pass by reference option determines if pass by reference or pass by value semantics should be used when handling parameter objects involved in an EJB request. This option can be found in the administrative console by navigating toServers => Application Servers =>server_name=> Object Request Broker (ORB). By default, this option is disabled and a copy of each parameter object is made and passed to the invoked EJB method. This is considerably more expensive than passing a simple reference to the existing parameter object.

References: https://www.ibm.com/developerworks/websphere/techjournal/0909_blythe/0909_blythe.html#sec3e