Question 1

A recent review of the audit polices log show that a specific IP address has made a large number of failed login attempts within a few minutes you suspect that it is an internet bot attack

Select two options you can configure to prevent the bot from accessing you application

Options:

A- Enable the CAPTCHA security policy

B- Enable an authentication lockout policy

C- Enable a contect security policy

D- Enable a failed login attempts security event

Answer:

A, B

Question 2

You need to define a new LDAP authentication servlet because all of the standard LDAP servlets are

being used in authentication services

which two task do you perform to implement this requirement

Options:

A- Copy an existing LDAP servlet and rename it

B- Create a new mapping servlet and URL pattern

C- add a new URL pattern to the existing mapping servlet

D- rename an existing LDAP servlet

Answer:

A, B

Question 3

An application uses LDP authentication users have role and application attributes, but not access group attributes. select the two tasks required to configure the application to uses LDAP attributes to determine the access group for a user

Options:

A- Create a decision table that evaluate role and application properties that return access group

B- Configure the authentication mapping to evaluate the decision table

C- Create a decision table that evaluate role and application attribute value that return access group

D- Add a method to the authentication activity to evaluate the decision table

Answer:

C, D

Question 4

Question Type: MultipleChoice

which two of the following action are required to configure your application to support SSO authentication ?

A- configuring the authentication activity to identify the operator in the system

B- configure the application record to use external authentication

C- configure required mapping between LDAP attributes and operator properties

D- configure model operator records for each access group in your application

Answer:

A, C

Question 5

Question Type: **MultipleChoice**

You add database connection information to prconfig.xml and want to encrypt the password in the connection information how do you encrypt the password?

Options:

A- create an encrypted keyring password and replace the unencypted password in prconfig.xml

B- enter a password in an application ID instance and reference the external system

C- create an encrypted password with PR cipherGenerator and reference the external system

D- create an encrypted password with passGen and replace the unencrypted password in pconfig.xml

Answer:

A

Question 6

Question Type: **MultipleChoice**

How do you encrypt the storage stream of the class MyOrg-HR-Work-RFP?

Options:

A- Build a site-specific encrypting cypher and select Encrypt BLOB? on the class group for MyOrg-HRWork-RFP

B- Build a site-specific encrypting cypher and select Encrypt BLOB? on the class MyOrg-HR-Work-RFP

C- Select Encrypt BLOB? on the class MyOrg-HR-Work-RFP

D- Encrypt the pzPvStream colum of the DB table mapped to MyOrg-HR-Work-RFP class using DB tools

Answer:

B

Question 7

Question Type: MultipleChoice

An application allows users to manage Account cases. You need to configure security so that users are allowed to view and update account only if they are the primary or secondary owner

how do you implement this requirement?

Options:

A- create a when rule that validate id the current user is either a primay or secondary owner of the account configure then when rule in the required conditions section on all flow actions that allow account updates.

B- create a privilage and configure it to validate if the current user is either a primary or secondary owner of the account. Assign the privilege for read and write instances of the account class in the user's access role.

C- create an access when rule that validate if the current user is either a primary or secondary owner of the account. Assign the access when rule for read and write instances of the account class in the user's vaccess role.

D- create an access when rule that validate if the current user is either a primay or secondary owner of the ccount. Configure the access

when rule on the Accouny case type to ensure authorized access

Answer:

C

Question 8

You deplyed a pega web mashup implementation into production and are using IACAuthentication.

which two action ensure that the external authentication module, and not another source, has validated the user?

Options:

A- In the IACAuthentication service, map a passoword attribute form the LDAP server used by the external

B- In an IAC authentication activity, add a step to idenify the security token provied by the external authentication module.

C- in the IACAuthentication service, specify the appropriate bind password used by the host system

D- In an IAC authentication activity, add steps that return the security token to the external authentication module for verification.

Question 9

Question Type: **MultipleChoice**

A security requirement states that personal data should only be visible to managers in the HR

organization. All personal data is contained in a single section.

How do you restrict access to personal data ?

Options:

A- configure a visible when rule on the section

B- Create an Access control policy restricting access to the properties

C- Add an Access when to relevent properties.

D- Define a privilege for the section and add the privilege to appropriate roles

Answer:

D