Question 1

In the event of a failover of the Vault server from the primary to the DR, which configuration option ensures that a CP will continue being able to refresh its cache?

Options:

A- Add the DR Vault IP address to the "Address" parameter in the file main_appprovider.conf. .<version> found in the AppProviderConf safe.

B- Add the IP address of the DR vault to the "Address" parameter in the file Vault.ini.file on the machine on which the CP is installed.

C- In the Password Vault Web Access UI, add the IP address of the DR Vault in the Disaster Recovery section under Applications > Options.

D- In the Conjur UI, add the IP address of the DR Vault in the Disaster Recovery section under Cluster Config > Credential Provider > Options.

Answer:

B

Question 2

Followers are replications of the Leader configured for which purpose?

Options:

A- synchronous replication to ensure that there is always an up-to-date database

B- asynchronous replication from the Leader which allows secret reads at scale

C- asynchronous replication from the Leader with read/write operations capability

D- synchronous replication to ensure high availability

Answer:

B

Question 3

You are diagnosing this log entry:

From Conjur logs:

USERNAME_MISSING failed to authenticate with authenticator authn-jwt service team-a:webservice:conjur/
authn-jwt/jenkins-test: CONJ00087E Failed to fetch JWKS from
'https://jenkins.tst.acme.com/jwtauth/conjur
jwk-set'. Reason: '#<OpenSSL::SSL::SSLError:SSL_connect returned=1 errno=o state=error:
certificate verify
failed (unable to get local issuer certificate)>'

Apr 25, 2022 11:35:06 AM FINE org.conjur.jenkins.jwauth.impl.JwtToken sign
Signing Token
Apr 25, 2022 11:35:07 AM FINE org.conjur.jenkins.api.ConjurAPI getAuthorizationToken
Authenticating with Conjur (JWT) authnPath=authn-jwt/jenkins-test
Apr 25, 2022 11:35:08 AM FINEST org.conjur.jenkins.api.ConjurAPI getAuthorizationToken
Conjur Authenticate response 401 – Unauthorized
Apr 25, 2022 11:35:08 AM FINE org.conjur.jenkins.credentials.CredentialsSupplier get
EXCEPTION: CredentialSuplier => Error authenticating to Conjur [401 – Unauthorized

Given these errors, which problem is causing the breakdown?

Options:

A- The Jenkins certificate chain is not trusted by Conjur.

B- The Conjur certificate chain is not trusted by Jenkins.

C- The JWT sent by Jenkins does not match the Conjur host annotations.

D- The Jenkins certificate is malformed and will not be trusted by Conjur.

Answer:

B

Question 4

Question Type: **MultipleChoice**

You have a PowerShell script that is being used on 1000 workstations. It requires a Windows Domain credential that is currently hard coded in the script.

What is the simplest solution to remove that credential from the Script?

Options:

A- Modify the script to use the CLI SDK to fetch the secret at runtime using Credential Providers installed on each workstation.

B- Modify the script to make a SOAP call to retrieve the secret from the Central Credential Provider.

C- Modify the script to run on WebSphere using the Application Server Credential Provider to retrieve the secret.

D- Use Conjur Summon to invoke the script and inject the secret at run time.

Answer:

D

Question 5

When an application is retrieving a credential from Conjur, the application authenticates to Follower

Options:

A- Follower B receives the next request to retrieve the credential.

What happens next?

A- The Coniur Token is stateless and Follower B is able to validate the Token and satisfy the request.

B- The Coniur Token is stateful and Follower B is unable to validate the Token promptinq the application to re-authenticate.

C- The Coryur Token is stateless and Follower B redirects the request to Follower A to satisfy the request.

D- The Coniur Token is stateful and Follower B redirects the request to Follower A to satisfy the request.

Answer:

A, A

Question 6

Question Type: MultipleChoice

A Kubernetes application attempting to authenticate to the Follower load balancer receives this error:

ERROR: 2024/10/30 06:07:08 authenticator.go:139: CAKC029E Received invalid response to certificate signing request. Reason: status code 401

When checking the logs, you see this message:

authn-k8s/prd-cluster-01 is not enabled

How do you remediate the issue?

Options:

A- Check the info endpoint on each Follower behind the load balancer and enable the authenticator on the Follower.

B- Modify conjur.conf in /opt/conjur/etc/authenticators addinqthe authenticator webservice.

C- A network issue is preventing the application from reaching the Follower; correct the issue and verity that it is resolved.

D- Enable the authenticator in the UI > Webservices > Authenticators > Enable and enable the appropriate authenticator webservice.

Answer:

A

Question 7

Question Type: MultipleChoice

Which API endpoint can be used to discover secrets inside of Conjur?

Options:

A- Resources

B- Roles

C- Policies

D- WhoAmi

Answer:

A

Question 8

Question Type: MultipleChoice

Where can all the self-signed/imported certificates be found in Conjur?

Options:

A- /opt/conjur/etc/ssl from the Conjur containers

B- /opt/conjur/certificates from the Conjur containers

C- /opt/cyberark/dap/certs from the Conjur containers

D- Log in to the Conjur UI > Conjur Cluster > Certificates > view.

Answer:

A

Question 9

How many Windows and Linux servers are required for a minimal Conjur deployment that integrates with an existing CyberArk PAM Vault environment, supports high availability, and is redundant across two geographically disparate regions?

Options:

A- 5 Linux servers, 2 Windows servers

B- 9 Linux servers, 2 Windows servers

C- 3 Linux servers, 1 Windows server

D- 10 Linux servers, 2 Windows server

Answer:

B

Question 10

What is a possible Conjur node role change?

Options:

A- A Standby may be promoted to a Leader.

B- A Follower may be promoted to a Leader.

C- A Standby may be promoted to a Follower.

D- A Leader may be demoted to a Standby in the event of a failover.

Answer:

A