SECRET-SEN Q&As

CyberArk Sentry - Secrets Manager

Pass CyberArk SECRET-SEN Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/secret-sen.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CyberArk Official Exam Center

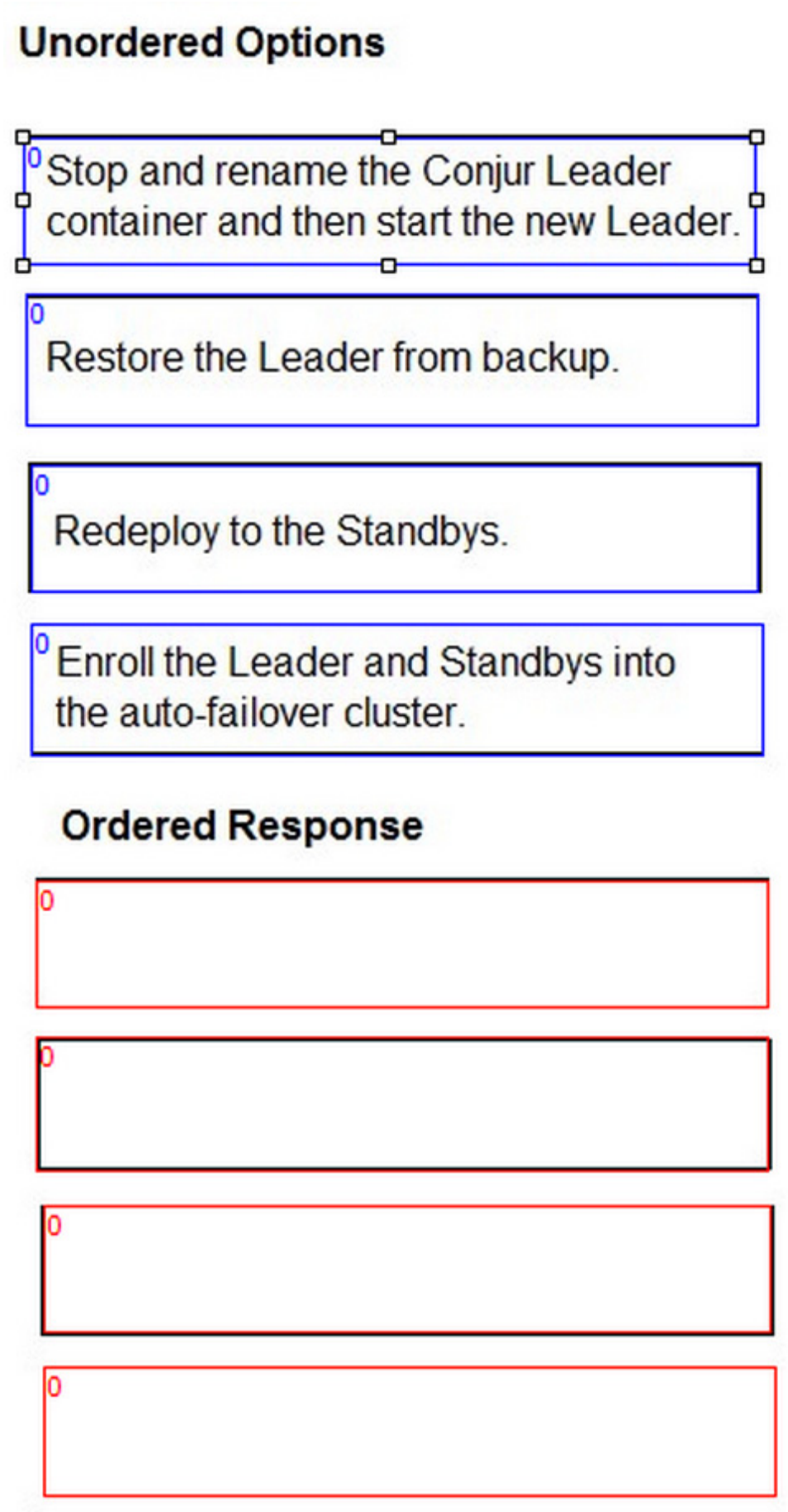
QUESTION 1

DRAG DROP

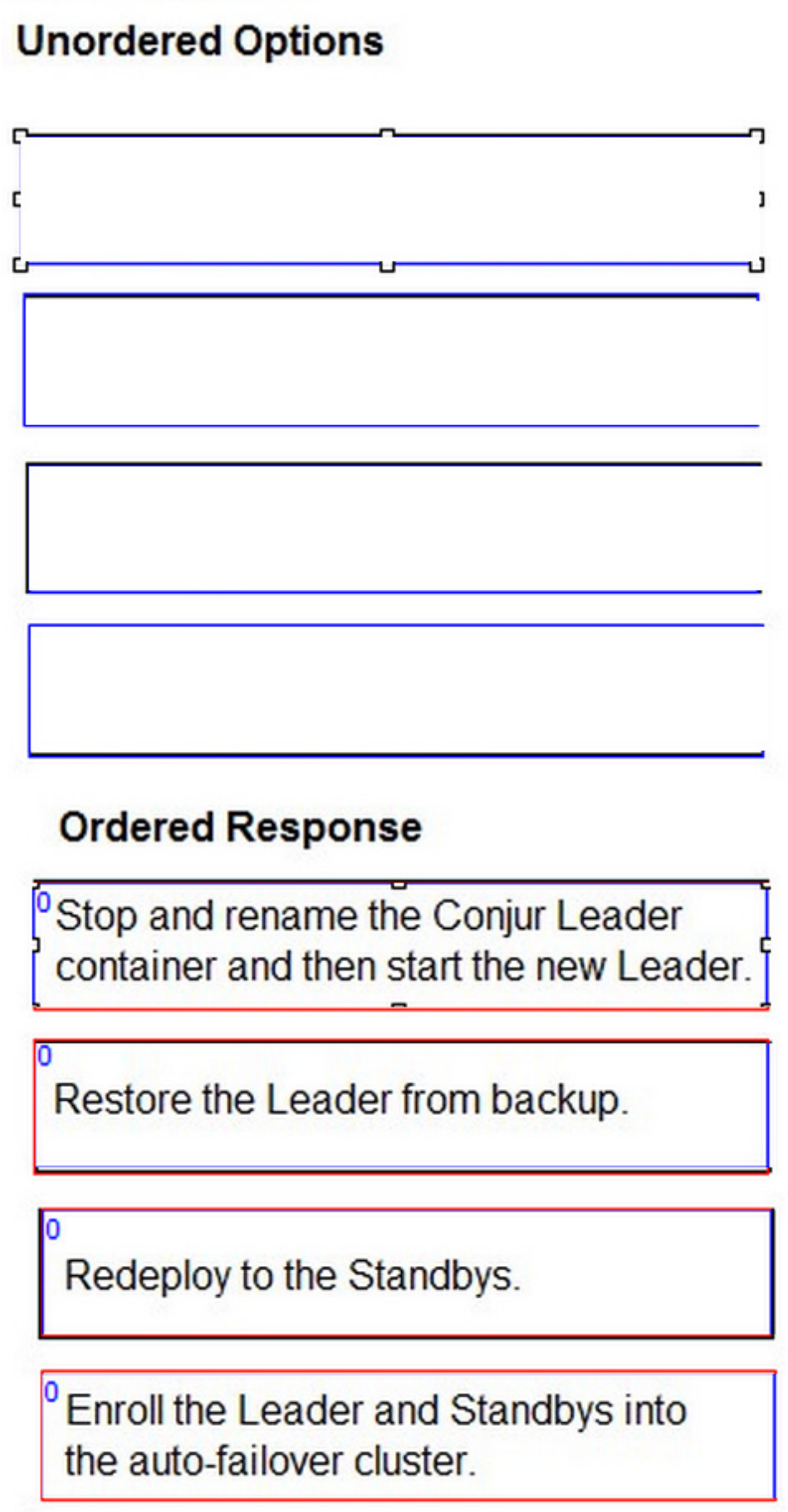
You are upgrading an HA Conjur cluster consisting of 1x Leader, 2x Standbys and 1x Follower. You stopped replication on the Standbys and Followers and took a backup of the Leader.

Arrange the steps to accomplish this in the correct sequence.

Select and Place:


Unordered Options
Stop and rename the Conjur Leader container and then start the new Leader.
Restore the Leader from backup.
Redeploy to the Standbys.
Enroll the Leader and Standbys into the auto-failover cluster.
Ordered Response

Correct Answer:


Unordered Options
Ordered Response
0
Stop and rename the Conjur Leader container and then start the new Leader.
0
Restore the Leader from backup.
0
Redeploy to the Standbys.
0
Enroll the Leader and Standbys into the auto-failover cluster.

To upgrade an HA Conjur cluster, you need to follow these steps: Stop and rename the Conjur Leader container and then start the new Leader. This step ensures that you have a backup of the old Leader container in case something goes wrong with the upgrade. You also need to specify the hostname and master-altnames parameters when starting the new Leader container to match the load balancer and the cluster nodes. Restore the Leader from backup. This step restores the data and configuration from the old Leader to the new Leader. You need to use the evoke restore command with the backup file name and the account name as arguments. Redeploy to the Standbys. This step upgrades the Standbys to the same version as the Leader. You need to stop and rename the old Standby containers and then start the new Standby containers with the evoke configure standby command. You also need to specify the hostname of the Leader and the Standby as arguments. Enroll the Leader and Standbys into the auto-failover cluster. This step enables the auto-failover feature for the cluster, which allows the Standbys to automatically take over the role of the Leader in case of a failure. You need to use the evoke cluster enroll command on the Leader and the evoke cluster join command on the Standbys. You also need to provide the hostname and password of the Leader as arguments. References: You can find more information about the upgrade process in the following resources: Upgrade Conjur Configure the Conjur cluster Conjur architecture and deployment reference Breathe Easy with a Self-Healing Conjur Cluster

QUESTION 2

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?

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.

Correct Answer: A

The log entry shows a failed authentication attempt with Conjur using the authn-jwt method. This method allows

applications to authenticate with Conjur using JSON Web Tokens (JWTs) that are signed by a trusted identity provider. In this case, the application is Jenkins, which is a CI/CD tool that can integrate with Conjur using the Conjur Jenkins plugin. The plugin allows Jenkins to securely retrieve secrets from Conjur and inject them as environment variables into Jenkins pipelines or projects. The log entry indicates that the JWT sent by Jenkins was rejected by Conjur because of an SSL connection error. The error message says that the certificate chain of Jenkins could not be verified by Conjur, and that the certificate authority (CA) that signed the Jenkins certificate was unknown to Conjur. This means that the Jenkins certificate chain is not trusted by Conjur, and that Conjur does not have the CA certificate of Jenkins in its trust store. Therefore, Conjur cannot establish a secure and trusted connection with Jenkins, and cannot validate the JWT signature. To fix this problem, the Jenkins certificate chain needs to be trusted by Conjur. This can be done by copying the CA certificate of Jenkins to the Conjur server, and adding it to the Conjur trust store. The Conjur trust store is a directory that contains the CA certificates of the trusted identity providers for the authn-jwt method. The Conjur server also needs to be restarted for the changes to take effect. References: Conjur Jenkins Plugin; Conjur JWT Authentication; Conjur Trust Store

QUESTION 3

What is a main advantage of using dual accounts in password management?

A. Since passwords are cached for both rotation accounts, it ensures the password for an application will not be changed, reducing the amount of blackout dates when a password expires.

B. It ensures passwords are rotated every 90 days, which respects the expected downtime for a system, database, or application

C. It ensures no delays are incurred when the application needs credentials because a password that is currently used by an application will never be changed

D. Since there are two active accounts, it doubles the probability that a system, database, or application will successfully authenticate.

Correct Answer: C

Dual accounts is a password management method that uses two accounts with identical privileges to access a system, database, or application. One account is active and the other is inactive at any given time. The active account remains untouched during password rotation, while the inactive account has its password changed after a grace period. This way, the application can always use the active account without experiencing any delays or errors due to password expiration or change. The advantage of using dual accounts is that it ensures business continuity and seamless access to the target resource, especially for high load and critical applications. References: Manage Dual Accounts, Configure dual accounts

QUESTION 4

What is a possible Conjur node role change?

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.

Correct Answer: A

According to the CyberArk Sentry Secrets Manager documentation, Conjur is a secrets management solution that consists of a leader node and one or more follower nodes. The leader node is responsible for managing the secrets, policies,

and audit records, while the follower nodes are read-only replicas that can serve secrets requests from applications. Additionally, Conjur supports a standby node, which is a special type of follower node that can be promoted to a leader node

in case of a leader failure. A standby node is synchronized with the leader node and can take over its role in a disaster recovery scenario. A possible Conjur node role change is when a standby node is promoted to a leader node, either

manually or automatically, using the auto-failover feature. A follower node cannot be promoted to a leader node, as it does not have the same data and functionality as the leader node. A standby node cannot be promoted to a follower node,

as it already has the same capabilities as a follower node, plus the ability to become a leader node. A leader node cannot be demoted to a standby node in the event of a failover, as it would lose its data and functionality and would not be able

to resume its role as a leader node.

References:

1: Conjur Architecture

2: Deploying Conjur on AWS

3: Auto-failover

QUESTION 5

What is the correct process to upgrade the CCP Web Service?

A. Run "sudo yum update aimprv" from the CLI.

B. Double-click the Credential Provider installer executable and select upgrade.

C. Double-click the AimWebService.msi and select upgrade.

D. Uninstall and reinstall the CCP Web Service.

Correct Answer: D

The correct process to upgrade the CCP Web Service is D. Uninstall and reinstall the CCP Web Service. The CCP Web Service is a component of the CyberArk Central Credential Provider (CCP) that enables applications to retrieve secrets from the CyberArk Vault using REST API calls. To upgrade the CCP Web Service, you need to first uninstall the existing CCP Web Service from the Windows Server Manager or the Control Panel, and then reinstall the CCP Web Service using the latest installation package from the CyberArk website. The installation package contains both the Credential Provider and the CCP Web Service components, and you need to run the AimWebService.msi file to install the CCP Web Service. You also need to make sure that the CCP Web Service has the correct configuration and permissions, and that the CyberArk CRL (Certificate Revocation List) is open from the CCP server. The other options are not correct processes to upgrade the CCP Web Service. Running "sudo yum update aimprv" from the CLI is a command to update the Credential Provider on Linux, not the CCP Web Service on Windows. Double-clicking the Credential Provider installer executable and selecting upgrade is a process to upgrade the Credential Provider on Windows, not the CCP Web Service. Double-clicking the AimWebService.msi and selecting upgrade is not a valid option, as the CCP Web

Service does not support an upgrade option, and you need to uninstall it first before reinstalling it. References: Upgrade the Central Credential Provider (CCP) - CyberArk, Section "Upgrade the Central Credential Provider (CCP)" Central Credential Provider web service configuration - CyberArk, Section "Central Credential Provider web service configuration"