SECRET-SEN$^{Q\&As}$

CyberArk Sentry - Secrets Manager

Pass CyberArk SECRET-SEN Exam with 100% Guarantee

QUESTION 1

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

Correct Answer: A

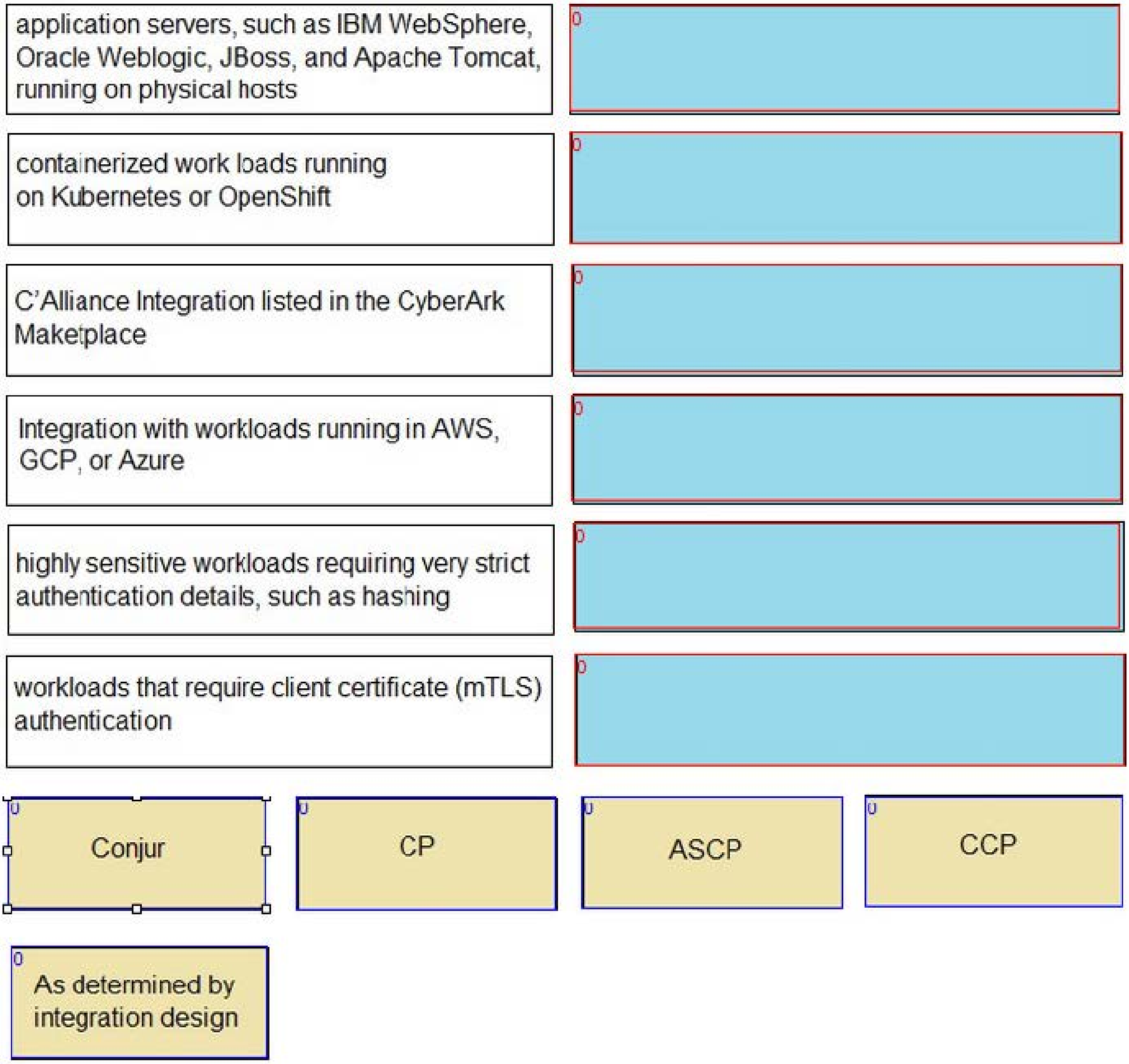
This is the correct answer because the Conjur Token is a JSON Web Token (JWT) that is signed by the Conjur master and contains the identity and permissions of the application. The Conjur Token is stateless, meaning that it does not depend on any stored session or transaction information on the server side. Therefore, any Conjur follower can validate the Token by verifying the signature and the expiration time, and satisfy the request by retrieving the credential from the local database. This allows the Conjur followers to be horizontally scalable and load balanced, and to provide high availability and performance for the applications. This answer is based on the Conjur documentation1 and the Conjur training course2.

QUESTION 2

DRAG DROP

Match each use case to the appropriate Secrets Manager Solution.

Select and Place:



application servers, such as IBM WebSphere, Oracle Weblogic, JBoss, and Apache Tomcat, running on physical hosts

containerized work loads running on Kubernetes or OpenShift

C'Alliance Integration listed in the CyberArk Maketplace

Integration with workloads running in AWS, GCP, or Azure

highly sensitive workloads requiring very strict authentication details, such as hashing

workloads that require client certificate (mTLS) authentication

Conjur

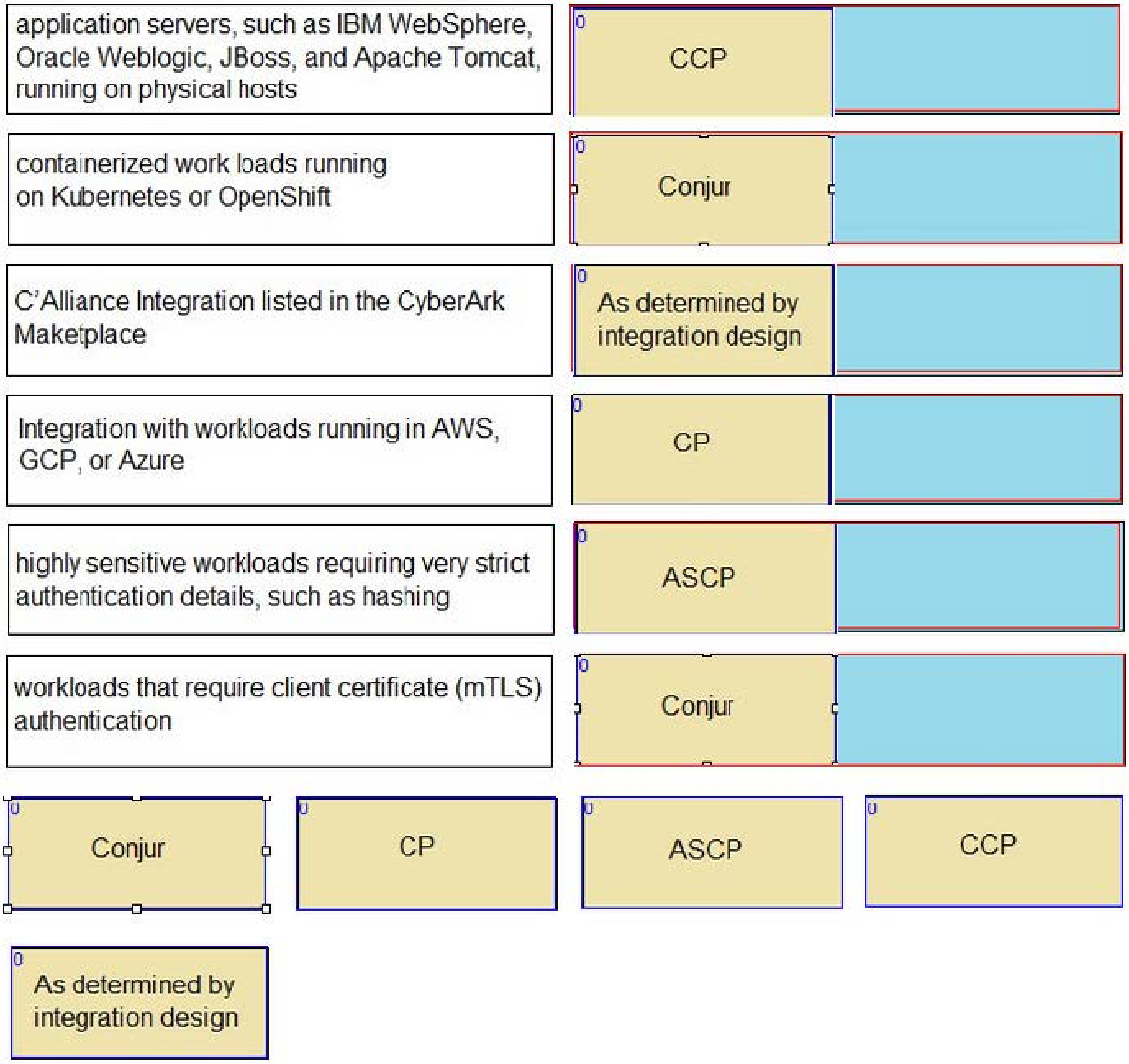
CP

ASCP

CCP

As determined by integration design

Correct Answer:



application servers, such as IBM WebSphere, Oracle Weblogic, JBoss, and Apache Tomcat, running on physical hosts	CCP	
containerized work loads running on Kubernetes or OpenShift	Conjur	
C'Alliance Integration listed in the CyberArk Maketplace	As determined by integration design	
Integration with workloads running in AWS, GCP, or Azure	CP	
highly sensitive workloads requiring very strict authentication details, such as hashing	ASCP	
workloads that require client certificate (mTLS) authentication	Conjur	

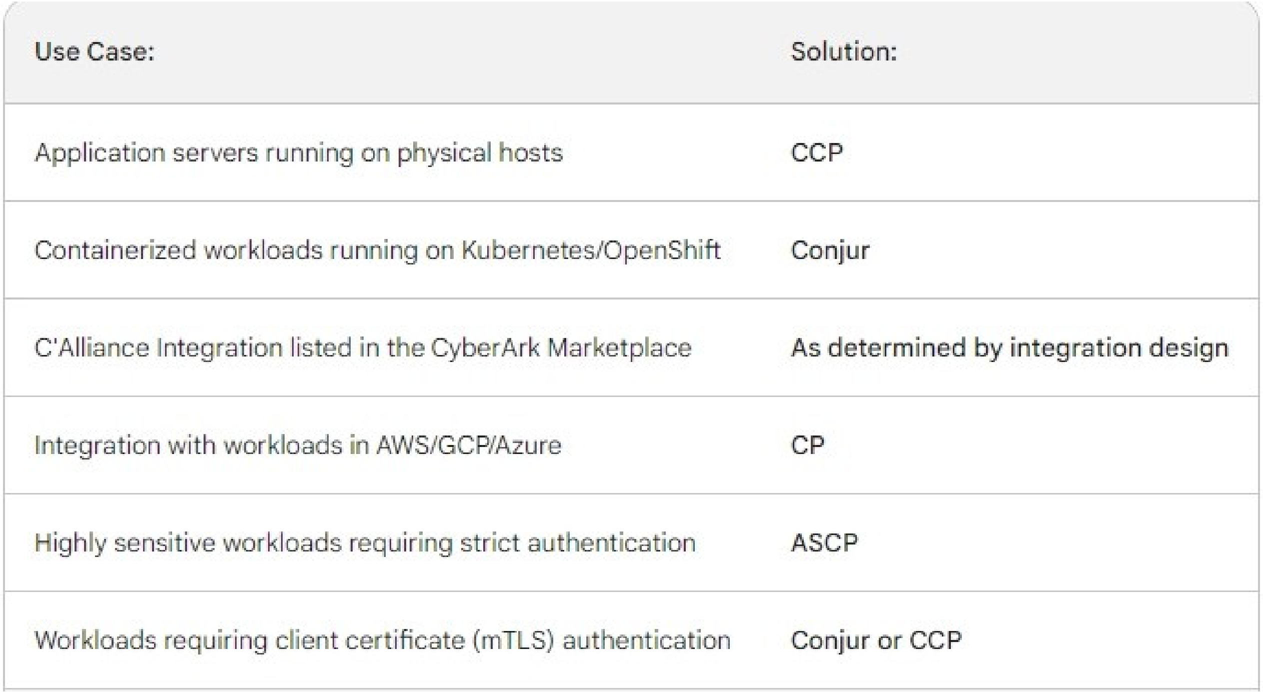
Conjur

CP

ASCP

CCP

As determined by integration design



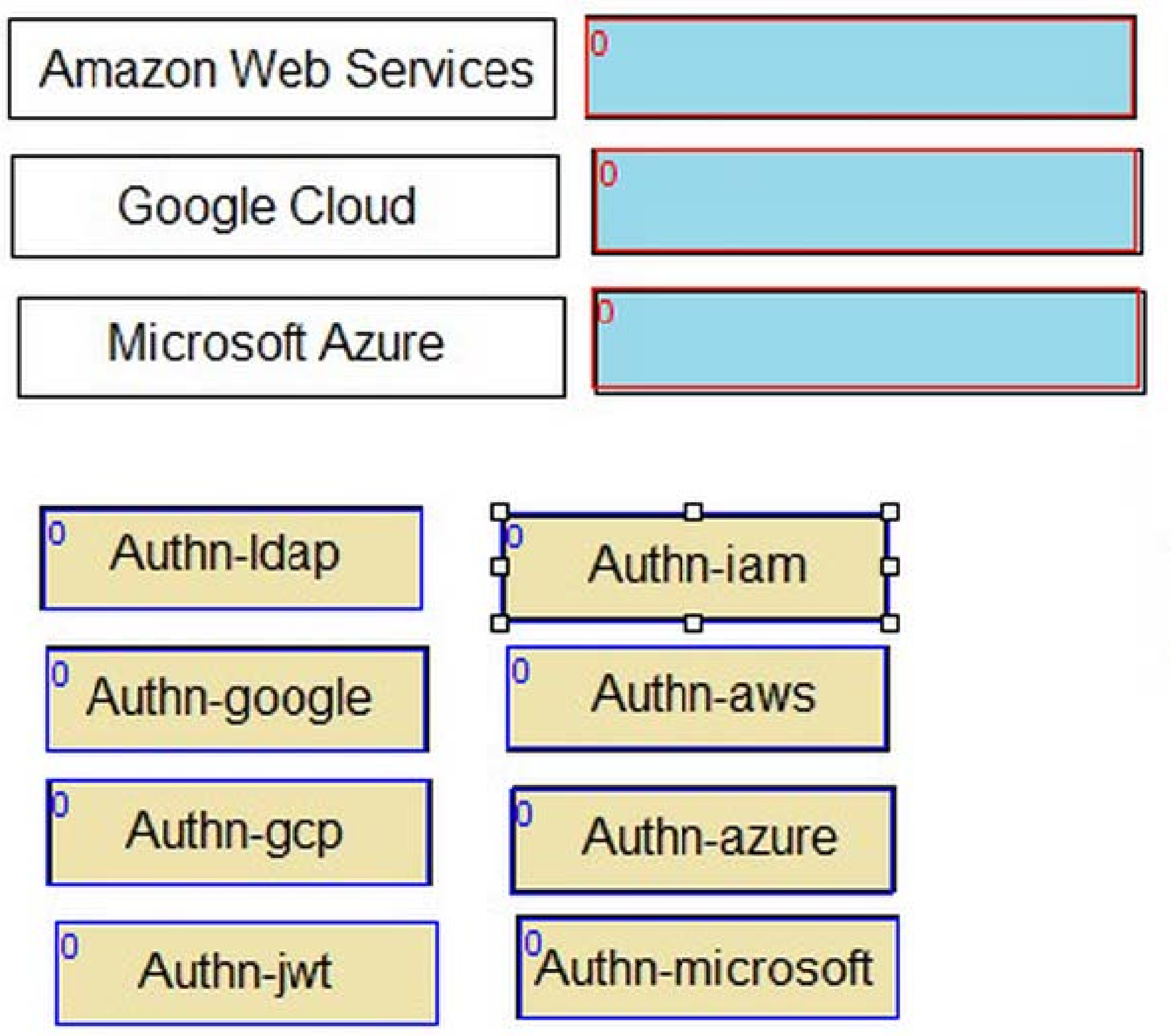
Use Case:	Solution:
Application servers running on physical hosts	CCP
Containerized workloads running on Kubernetes/OpenShift	Conjur
C'Alliance Integration listed in the CyberArk Marketplace	As determined by integration design
Integration with workloads in AWS/GCP/Azure	CP
Highly sensitive workloads requiring strict authentication	ASCP
Workloads requiring client certificate (mTLS) authentication	Conjur or CCP

QUESTION 3

DRAG DROP

Match each cloud platform to the correct Conjur authenticator.

Select and Place:



Amazon Web Services

Google Cloud

Microsoft Azure

Authn-ldap

Authn-iam

Authn-google

Authn-aws

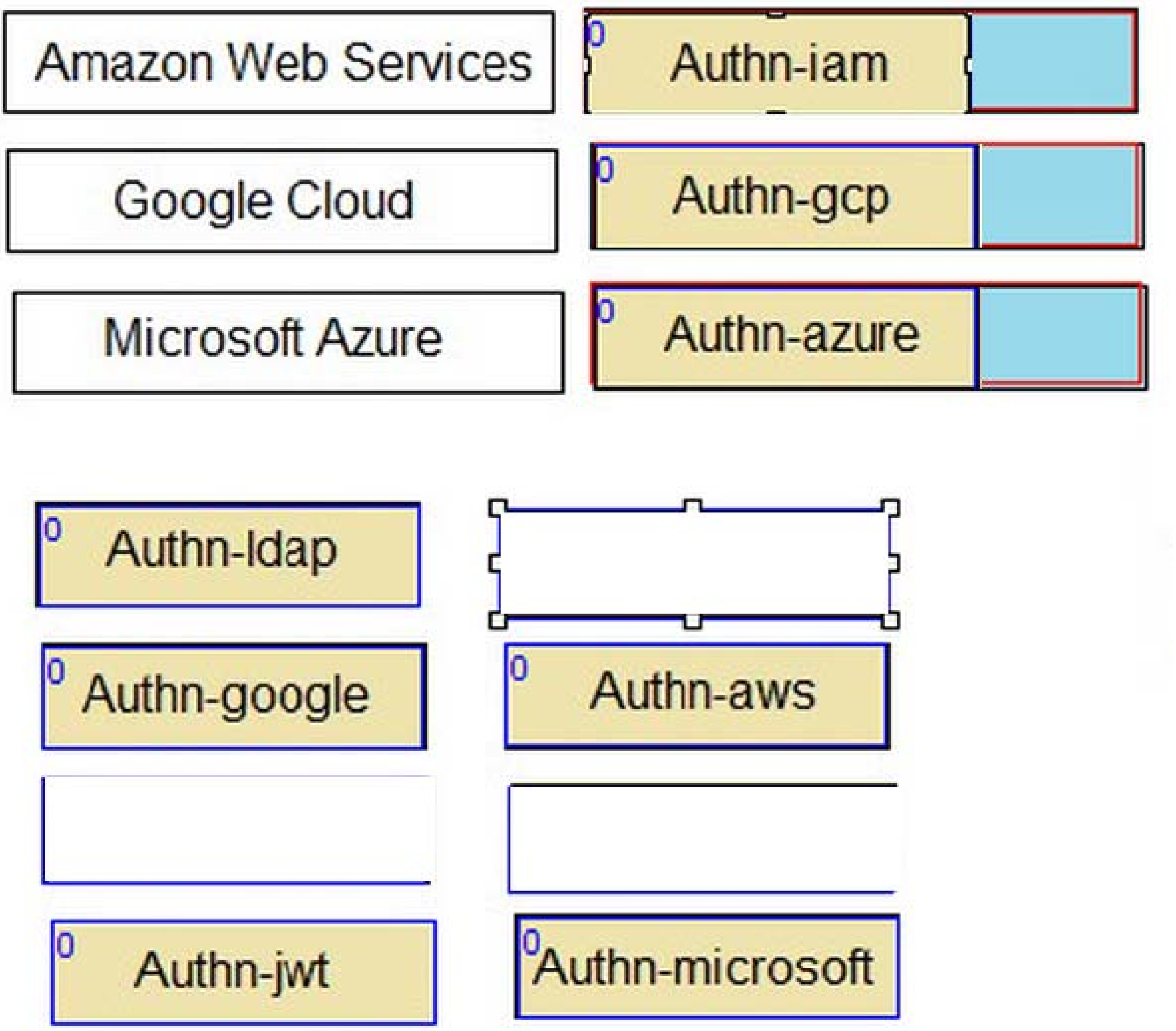
Authn-gcp

Authn-azure

Authn-jwt

Authn-microsoft

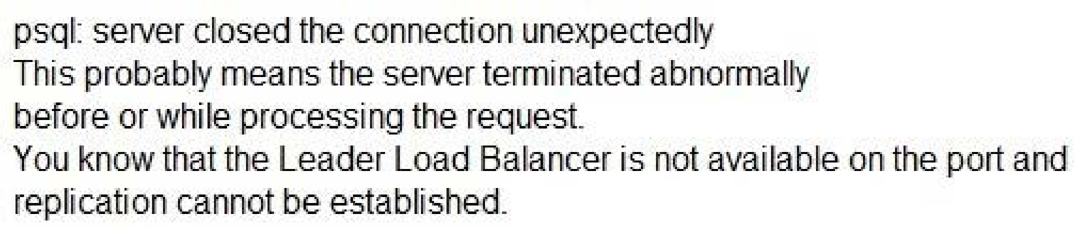
Correct Answer:



AWS -> authn-iam Azure -> authn-azure GCP -> authn-gcp JWT Provider -> authn-jwt Conjur supports different authenticators for different cloud platforms. Each authenticator allows a resource or service running on the cloud platform to authenticate to Conjur using a unique identity token signed by the cloud provider. The following are the descriptions of each authenticator: authn-iam: Enables an AWS resource to use its AWS IAM role to authenticate with Conjur. The resource sends a request to the AWS Security Token Service (STS) to get a signed AWS access token, and then sends the token to Conjur for verification. authn-azure: Enables an Azure resource to authenticate with Conjur. The resource sends a request to the Azure Instance Metadata Service (IMDS) to get a signed Azure access token, and then sends the token to Conjur for verification. authn-gcp: Enables a Google Cloud Platform resource to authenticate with Conjur. The resource sends a request to the Google Cloud Identity and Access Management (IAM) service to get a signed Google identity token, and then sends the token to Conjur for verification. authn-jwt: Enables an application to authenticate to Conjur using a JWT from a JWT Provider. The application obtains a JWT from the JWT Provider, and then sends the JWT to Conjur for verification. References: You can find more information about the Conjur authenticators in the following resources: Supported Conjur Cloud authenticators Configure Conjur Cloud authenticators GCP Authenticator

QUESTION 4

When attempting to configure a Follower, you receive the error:



```
psql: server closed the connection unexpectedly
This probably means the server terminated abnormally
before or while processing the request.
You know that the Leader Load Balancer is not available on the port and
replication cannot be established.
```

Which port is the problem?

A. 5432

B. 1999

C. 443

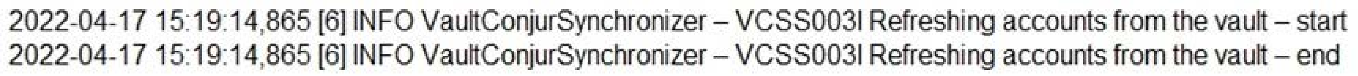
D. 1858

Correct Answer: A

The error message "psql: server closed the connection unexpectedly" means that the server terminated abnormally before or while processing the request. This is likely due to the Leader Load Balancer not being available on the port and replication cannot be established. The port that is the problem is 5432, which is the default port for PostgreSQL database connections. The Follower needs to connect to the Leader Load Balancer on this port to receive the replication data from the Leader. If the port is blocked or unreachable, the Follower will fail to sync with the Leader and display the error message. References: [Set up Follower], [Troubleshoot Follower]

QUESTION 5

While troubleshooting an issue with accounts not syncing to Conjur, you see this in the log file:



```
2022-04-17 15:19:14,865 [6] INFO VaultConjurSynchronizer – VCSS003I Refreshing accounts from the vault – start
2022-04-17 15:19:14,865 [6] INFO VaultConjurSynchronizer – VCSS003I Refreshing accounts from the vault – end
```

What could be the issue?

A. Connection timed out to the Vault.

B. Safe permissions for the LOB user are incorrect.

C. Connection timed out during loading policy through SDK.

D. At first Vault Conjur Synchronizer start up, the number of LOBs is exceeded.

Correct Answer: D

This is the correct answer because the log file shows the error message "CEADBR009E Failed to load policy through SDK" and the exception message "The number of LOBs exceeds the limit". This indicates that the Vault Conjur Synchronizer service (Synchronizer) encountered a problem when trying to sync the secrets from the CyberArk Vault to the Conjur database using the Conjur SDK. The Conjur SDK is a library that allows the Synchronizer to interact with the Conjur REST API and perform operations on the Conjur resources, such as roles, policies, secrets, and audit records. The number of LOBs refers to the number of lines of business (LOBs) that are configured in the Synchronizer. A LOB is a logical grouping of secrets that belong to a specific business unit or function. Each LOB has its own configuration file that specifies the source safe, the target policy, and the mapping rules for the secrets. The Synchronizer can sync multiple LOBs concurrently using multiple threads. However, there is a limit on the number of threads that the Synchronizer can use, which depends on the hardware and software specifications of the Synchronizer machine. If the number of LOBs exceeds the number of threads, the Synchronizer will not be able to sync all the LOBs and will generate an error. This answer is based on the CyberArk Secrets Manager documentation and the CyberArk Secrets Manager training course.

Latest SECRET-SEN Dumps   SECRET-SEN VCE Dumps   SECRET-SEN Practice Test