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

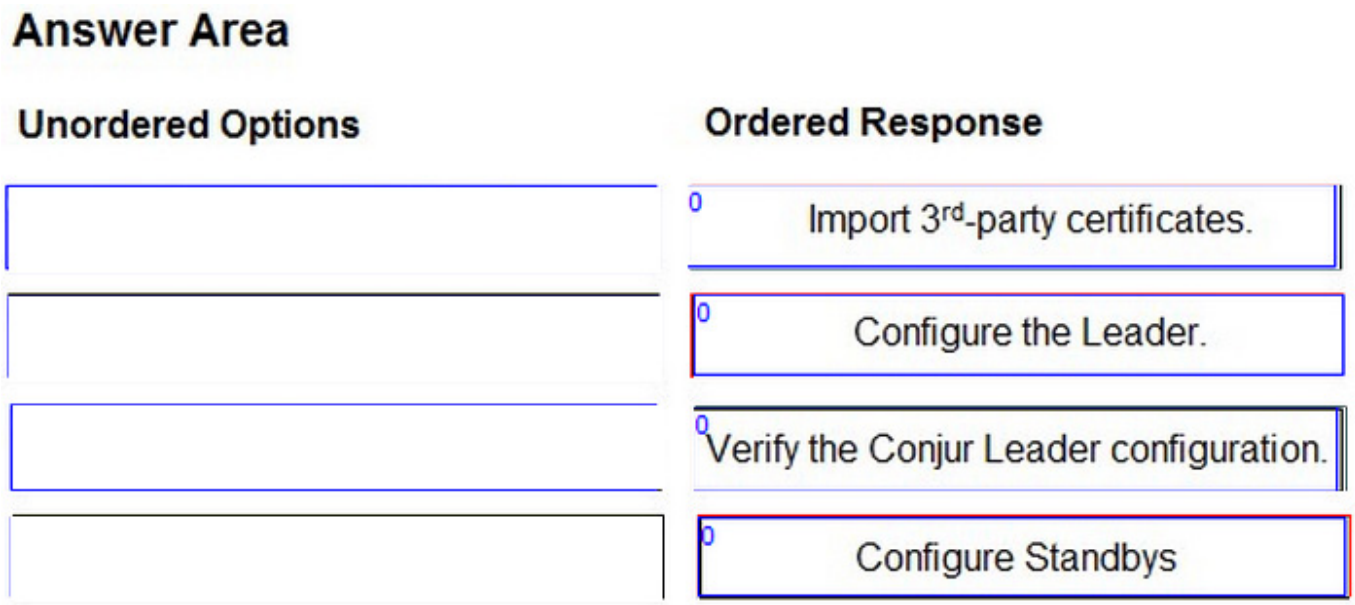
DRAG DROP

You are configuring the Conjur Cluster with 3rd-party certificates.

Arrange the steps to accomplish this in the correct sequence.

Select and Place:

Correct Answer:



The correct sequence of steps to configure the Conjur Cluster with 3rd-party certificates is as follows: Import 3rd-party certificates to the Leader using the command: docker exec mycontainer evoke ca import --force --root --chain 1 Configure the Leader using the command: docker exec mycontainer evoke configure master --accept-eula --hostname

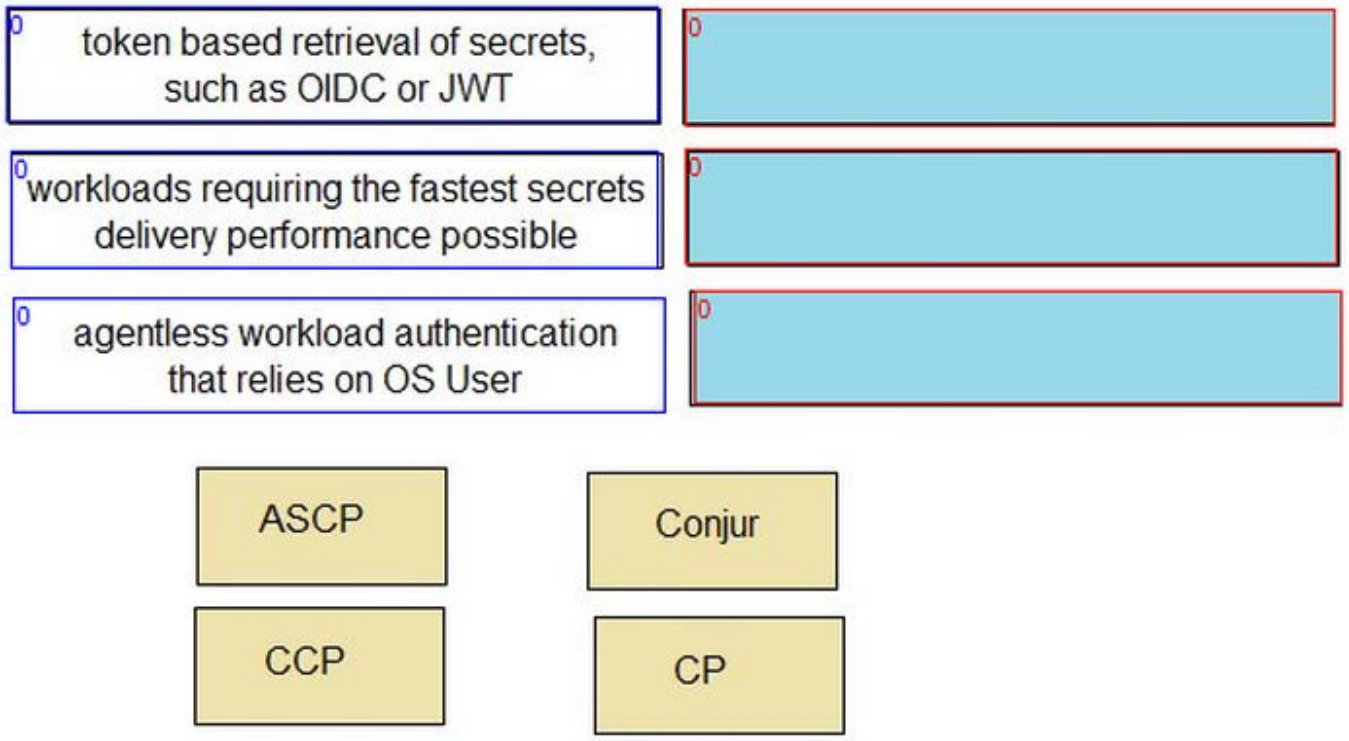
--admin-password 1 Verify the Conjur Leader configuration using the command: docker exec mycontainer evoke role Configure the Standbys using the command: docker exec mycontainer evoke configure standby --master-address --master-fingerprint 1 References: Certificate requirements

QUESTION 2

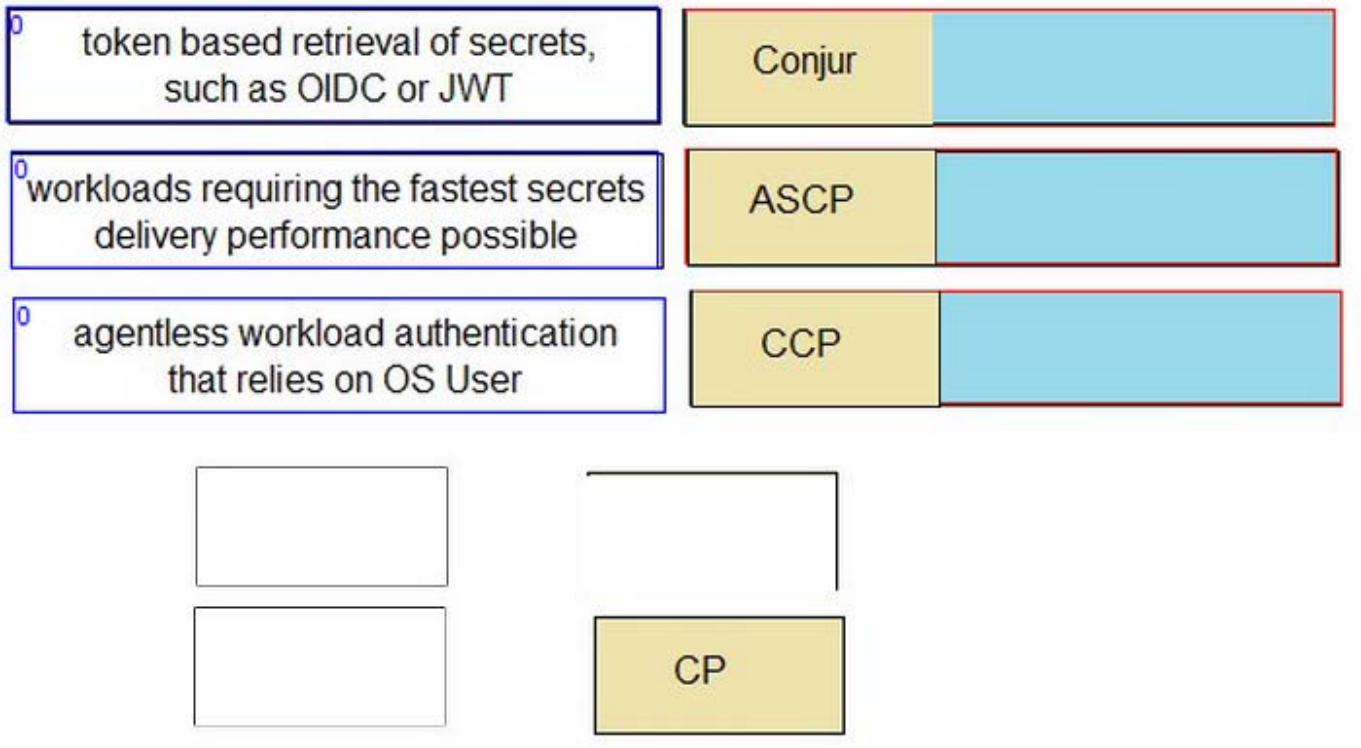
DRAG DROP

Match each scenario to the appropriate Secrets Manager solution.

Select and Place:



Correct Answer:



The appropriate Secrets Manager solution for each scenario is as follows: token based retrieval of secrets, such as OIDC or JWT: Conjur workloads requiring the fastest secrets delivery performance possible: ASCP agentless workload authentication that relies on OS User: CCP These solutions are described in the Secrets Management Tools page of the CyberArk website

QUESTION 3

When using the Seed Fetcher to deploy Kubernetes Followers, an error occurs in the Seed Fetcher container. You check the logs and discover that although the Seed Fetcher was able to authenticate, it shows a 500 error in the log and does not successfully retrieve a seed file. What is the cause?

A. The certificate based on the Follower DNS name is not present on the Leader.

B. The host you configured does not have access to see the certificates.

C. The synchronizer service crashed and needs to be restarted.

D. The Leader does not have the authenticator webservice enabled.

Correct Answer: A

The cause of the issue is A. The certificate based on the Follower DNS name is not present on the Leader. This means that the Leader does not have a certificate file that matches the Follower DNS name used in the seed request, and therefore cannot generate a valid seed file for the Follower. This results in a 500 error in the Seed Fetcher container log. To resolve the issue, you need to import a certificate with the Follower DNS name as the subject alt name on the Leader, and create a copy of the certificate file with a name that matches the Follower DNS name used in the seed request1.

QUESTION 4

You are enabling synchronous replication on Conjur cluster.

What should you do?

A. Execute this command on the Leader: docker exec sh -c" evoke replication sync that

B. Execute this command on each Standby: docker exec sh -c" evoke replication sync that

C. In Conjur web UI, click the Tools icon in the top right corner of the main window. Choose Conjur Cluster and click "Enable synchronous replication" in the entry for Leader.

D. In Conjur web UI, click the Tools icon in the top right corner of the main window. Choose Conjur Cluster and click "Enable synchronous replication" in the entry for Standbys.

Correct Answer: A

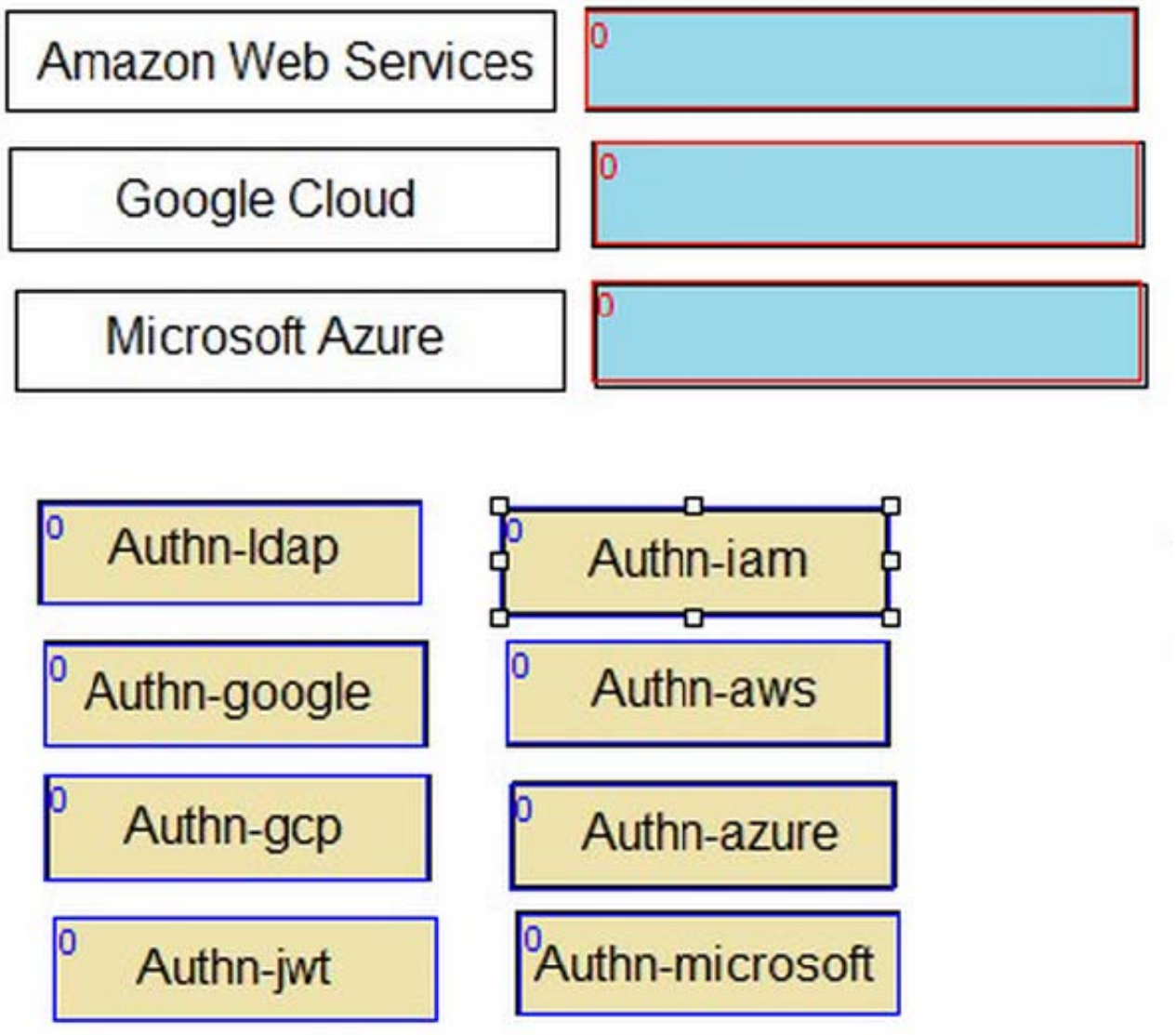
enable synchronous replication on a Conjur cluster, you need to run the command evoke replication sync that on the Leader node of the cluster. This command will configure the Leader to wait for confirmation from all Standbys before committing any transaction to the database. This ensures that the data is consistent across all nodes and prevents data loss in case of a failover. However, this also increases the latency and reduces the throughput of the cluster, so it should be used with caution and only when required by the business or compliance needs. References: Conjur Cluster Replication Sentry - Secrets Manager - Sample Items and Study Guide

QUESTION 5

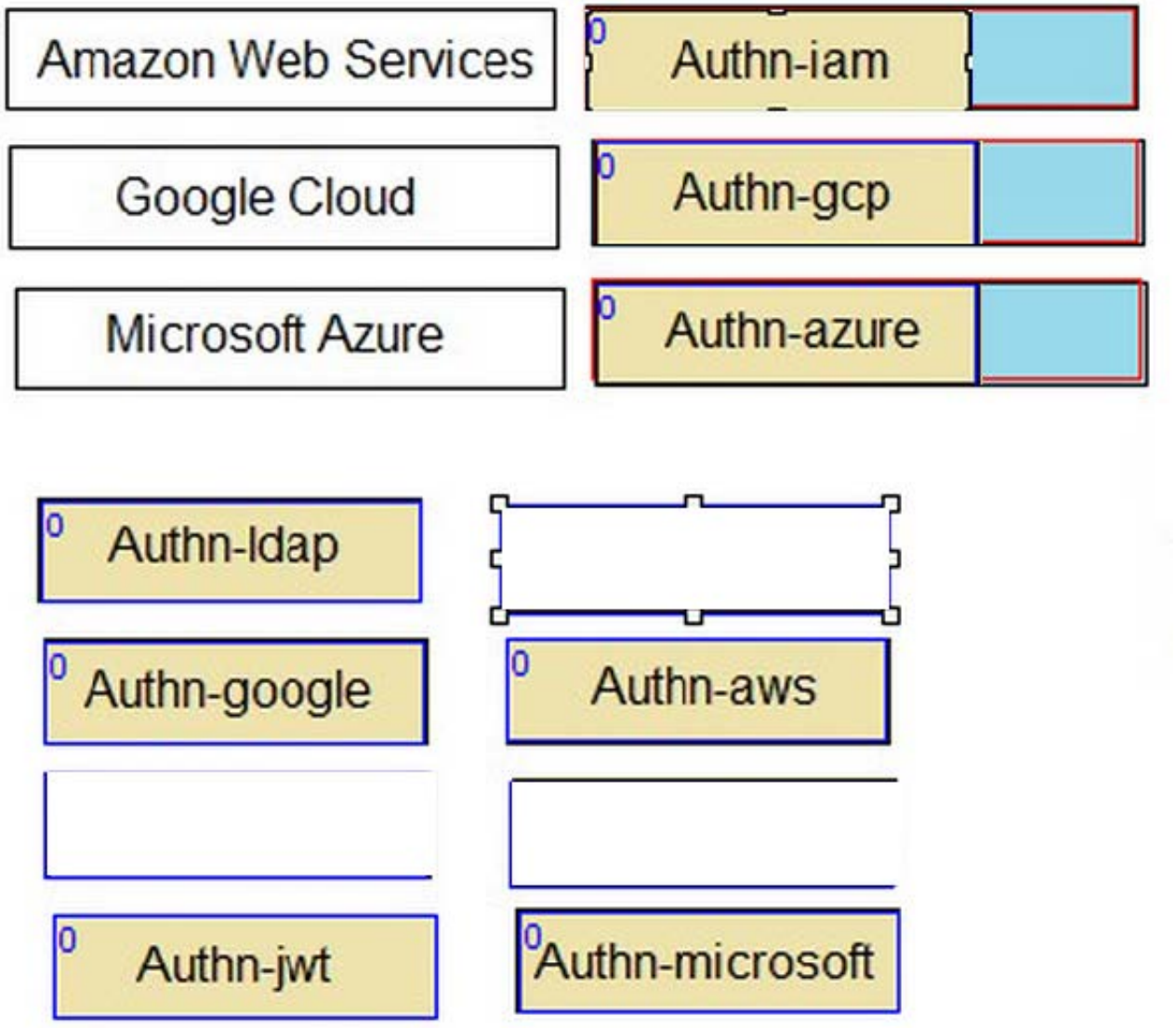
DRAG DROP

Match each cloud platform to the correct Conjur authenticator.

Select and Place:



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