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.certbus.com/secret-sen.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

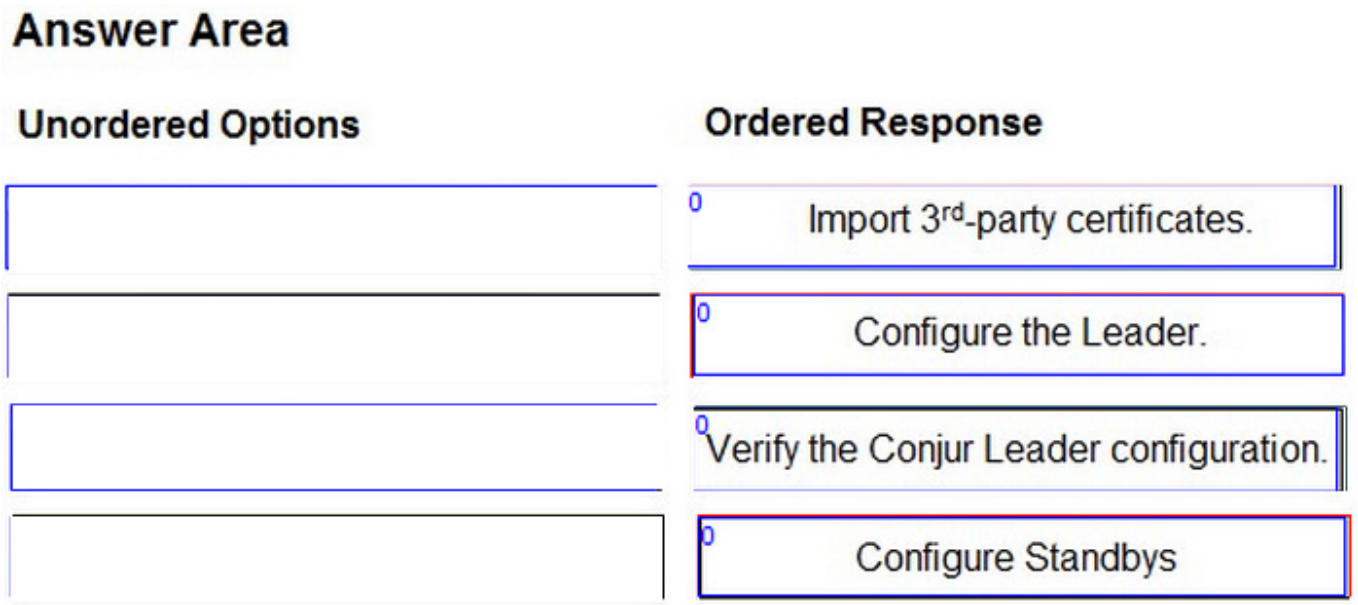
DRAG DROP

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

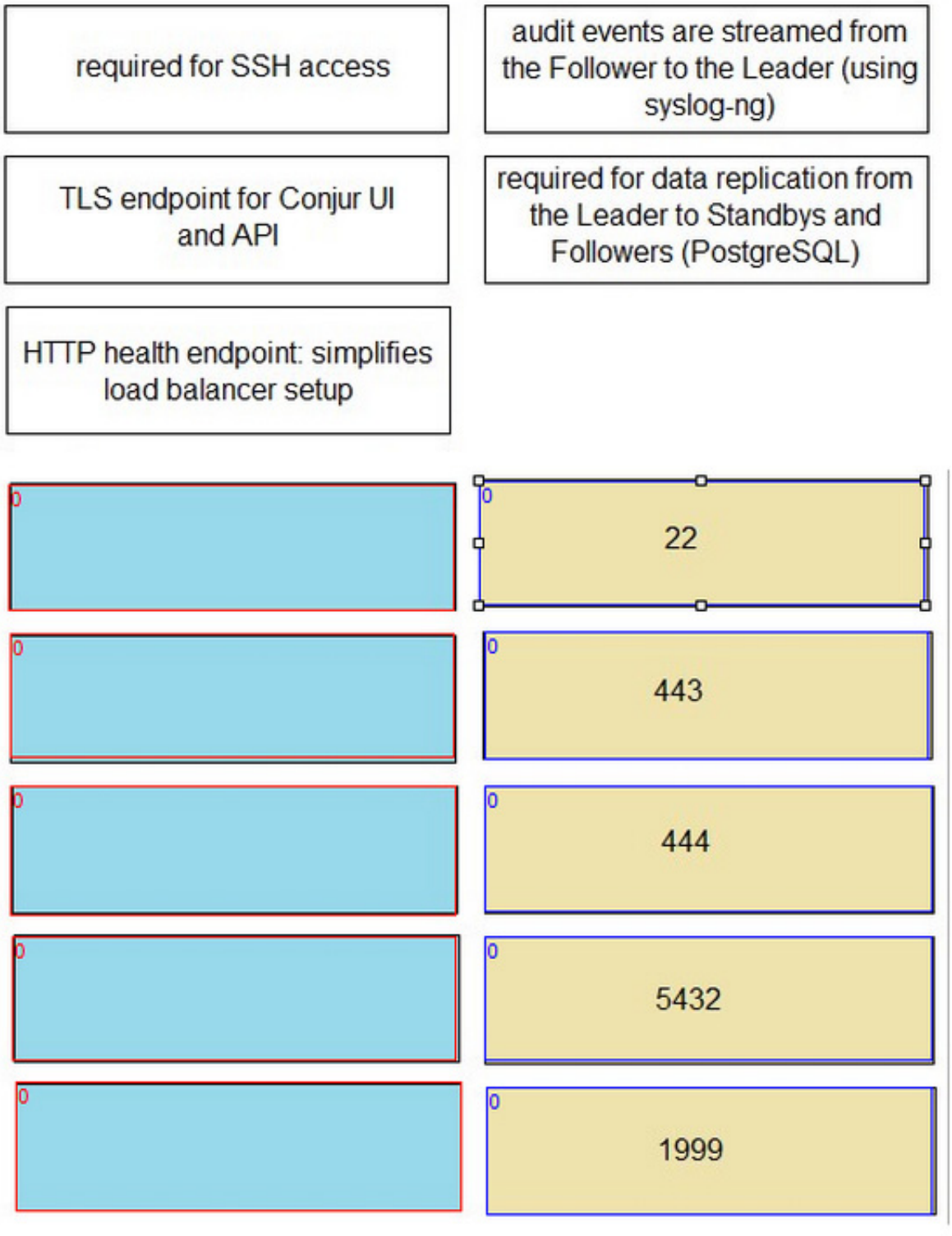
QUESTION 2

DRAG DROP

Match the correct network port to its function in Conjur.

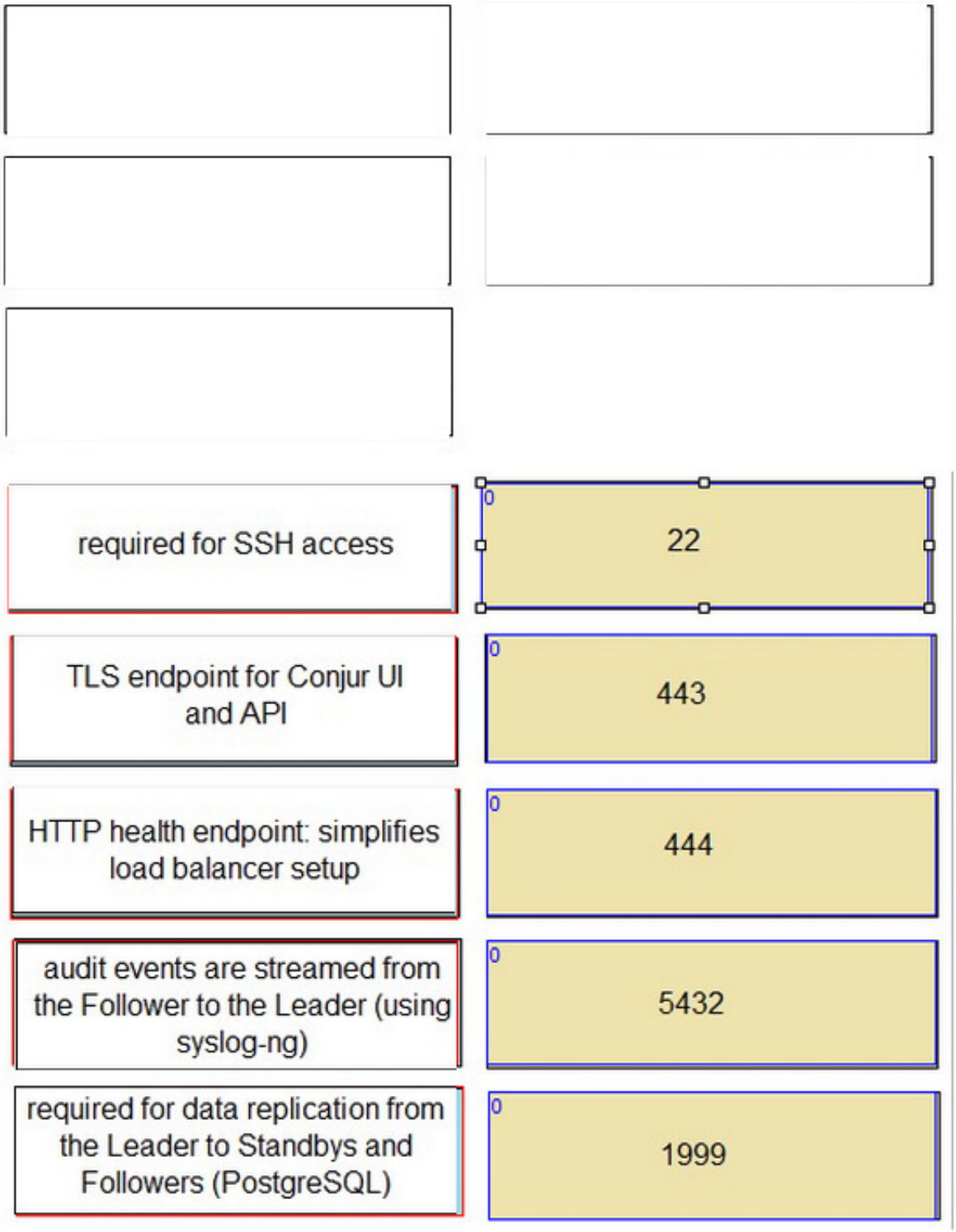
Select and Place:

Answer Area



Correct Answer:

Answer Area



Based on the image you sent, the correct network port to its function in Conjur are:

22: required for SSH access

443: TLS endpoint for Conjur UI and API

444: HTTP health endpoint: simplifies load balancer setup

1999: audit events are streamed from the Follower to the Leader (using syslog-ng)

5432: required for data replication from the Leader to Standbys and Followers (PostgreSQL)

These are the standard ports and protocols used by the Conjur components to communicate with each other and with external clients. The ports can be customized according to the network and security requirements of the organization.

These ports are documented in the CyberArk Secrets Manager documentation1 and the CyberArk Secrets Manager training course2.

QUESTION 3

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 4

During the configuration of Conjur, what is a possible deployment scenario?

A. The Leader and Followers are deployed outside of a Kubernetes environment; Slandbys can run inside a Kubernetes environment.

B. The Conjur Leader cluster is deployed outside of a Kubernetes environment; Followers can run inside or outside the environment.

C. The Leader cluster is deployed outside a Kubernetes environment; Followers and Standbys can run inside or outside the environment.

D. The Conjur Leader cluster and Followers are deployed inside a Kubernetes environment.

Correct Answer: C

Conjur is a secrets management solution that securely stores and manages secrets and credentials used by applications, DevOps tools, and other systems. Conjur can be deployed in different scenarios, depending on the needs and preferences of the organization. One of the possible deployment scenarios is to deploy the Leader cluster outside a Kubernetes environment, and the Followers and Standbys inside or outside the environment. The Leader cluster is the primary node that handles all write operations and coordinates the replication of data to the Follower and Standby nodes. The Leader cluster consists of one active Leader node and one or more Standby nodes that can be promoted to Leader in case of a failure. The Leader cluster can be deployed outside a Kubernetes environment, such as on a virtual machine or a physical server, using Docker or other installation methods. This can provide more control and flexibility over the configuration and management of the Leader cluster, as well as better performance and security. The Follower and Standby nodes are read-only replicas of the Leader node that can serve requests from clients and applications that need to retrieve secrets or perform other read- only operations. The Follower and Standby nodes can be deployed inside or outside a Kubernetes environment, depending on the use case and the availability requirements. For example, if the clients and applications are running inside a Kubernetes cluster, it may be convenient and efficient to deploy the Follower and Standby nodes inside the same cluster, using Helm charts or other methods. This can reduce the network latency and complexity, and leverage the Kubernetes features such as service discovery, load balancing, and health checks. Alternatively, if the clients and applications are running outside a Kubernetes cluster, or if there is a need to distribute the Follower and Standby nodes across different regions or availability zones, it may be preferable to deploy the Follower and Standby nodes outside the Kubernetes cluster, using Docker or other methods. This can provide more scalability and resiliency, and avoid the dependency on the Kubernetes cluster. References: Conjur Deployment Scenarios; Conjur Cluster Installation; Conjur Kubernetes Integration

QUESTION 5

In a 3-node auto-failover cluster, the Leader has been brought down for patching that lasts longer than the configured TTL. A Standby has been promoted.

Which steps are required to repair the cluster when the old Leader is brought back online?

A. On the new Leader, generate a Standby seed for the old Leader node and add it to the cluster member list. Rebuild the old Leader as a new Standby and then re-enroll the node to the cluster.

B. Generate a Standby seed for the newly promoted Leader. Stop and remove the container on the new Leader, then rebuild it as a new Standby. Re-enroll the Standby to the cluster and re-base replication of the 3rd Standby back to the old Leader.

C. Generate standby seeds for the newly-promoted Leader and the 3rd Standby Stop and remove the containers and then rebuild them as new Standbys. On both new Standbys, re-enroll the node to the cluster.

D. On the new Leader, generate a Standby seed for the old Leader node and re-upload the auto-failover policy in "replace" mode. Rebuild the old Leader as a new Standby, then re-enroll the node to the cluster.

Correct Answer: A

The correct answer is A. On the new Leader, generate a Standby seed for the old Leader node and add it to the cluster member list. Rebuild the old Leader as a new Standby and then re-enroll the node to the cluster. This is the recommended way to repair the cluster health after an auto-failover event, according to the CyberArk Sentry Secrets Manager documentation1. This method reuses the original Leader as a new Standby, without affecting the new Leader or the other Standby. The steps are as follows: On the new Leader, generate a Standby seed for the old Leader node using the command evoke seed standby . This will create a file named .tar in the current directory. On the new Leader, add the old Leader node to the cluster member list using the command evoke cluster add . On the old Leader server, stop and remove the container using the commands docker stop and docker rm . On the old Leader server, copy the Standby seed file from the new Leader using the command scp :.tar . On the old Leader server, create a new container using the same name as the one you just destroyed, and load the Standby seed file using the command docker run --name -d --restart=always -v /var/log/conjur:/var/log/conjur -v /opt/conjur/backup:/opt/conjur/backup -p "443:443" -p "5432:5432" -p "1999:1999" cyberark/conjur:latest seed fetch .tar On the old Leader server, re-enroll the node to the

cluster using the command evoke cluster enroll The other options are not correct, as they either involve unnecessary or harmful steps, such as rebuilding the new Leader or the other Standby, or re-uploading the auto-failover policy in replace mode, which may cause data loss or inconsistency.

QUESTION 6

What is the correct command to import the root CA certificate into Conjur?

A. docker exec evoke ca import --no-restart --root;

B. docker exec evoke import --no-restart --root;

C. docker exec evoke ca import --no-restart;

D. docker exec ca import

Correct Answer: C

C. docker exec evoke ca import --no-restart

This is the correct command to import the root CA certificate into Conjur. The evoke ca import command is used to import a certificate authority (CA) certificate into the Conjur appliance. The certificate can be either a root CA or an

intermediate CA. The --no-restart option prevents the Conjur appliance from restarting after importing the certificate. The parameter specifies the path and name of the root CA certificate file to be imported. This command will

add the root CA certificate to the trusted CA store of the Conjur appliance, which is used to validate the certificates of the clients and servers that communicate with Conjur. This command is documented in the Conjur documentation and the

Conjur training course.

The other options are not correct commands to import the root CA certificate into Conjur. The evoke import command does not exist.

The --root option is not a valid option for the evoke ca import command. The ca import command is not a valid docker exec command.

QUESTION 7

When installing the Vault Conjur Synchronizer, you see this error:

Forbidden

Logon Token is Empty ?Cannot logon

Unauthorized

What must you ensure to remediate the issue?

A. This admin user must not be logged in to other sessions during the Vault Conjur Synchronizer installation process.

B. You specified the correct url for Conjur and it is listed as a SAN on that url\\'s certificate.

C. You correctly URI encoded the url in the installation script.

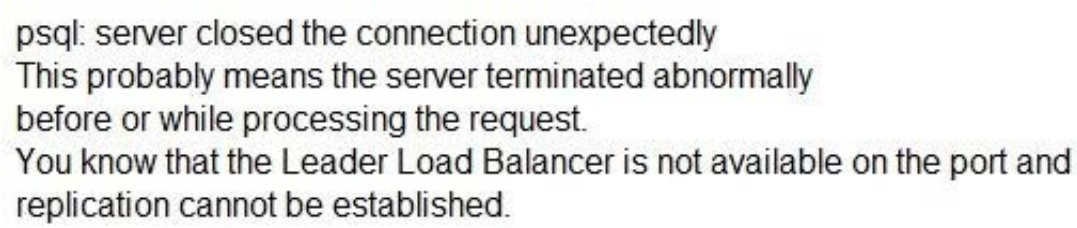
D. You ran powershell as Administrator and there is sufficient space on the server on which you are running the installation.

Correct Answer: A

This error occurs when the Vault Conjur Synchronizer installation script tries to log in to the Vault using the admin user credentials, but the admin user is already logged in to other sessions. The Vault has a limit on the number of concurrent sessions per user, and the default value is one. Therefore, the installation script fails to authenticate the admin user and returns the error message: Forbidden Logon Token is Empty - Cannot logon Unauthorized. To remediate the issue, the admin user must log out of any other sessions before running the installation script, or increase the limit on the number of concurrent sessions per user in the Vault configuration file12. References: = Troubleshoot CyberArk Vault Synchronizer 1, Error: Forbidden Logon Token is Empty - Cannot logon Unauthorized Vault.ini File Parameters 2, ConcurrentSessionsPerUser

QUESTION 8

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



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 9

When installing the CCP and configuring it for use behind a load balancer, which authentication methods may be affected? (Choose two.)

A. Allowed Machines authentication

B. [Client Certificate authentication

C. OS User

D. Path

E. Hash

Correct Answer: AB

The CCP (Central Credential Provider) is a tool that enables applications to securely retrieve credentials from CyberArk Secrets Manager without hard-coding or storing them in files. The CCP can be installed on a single server or on multiple servers behind a load balancer for high availability and scalability. The load balancer is a device or service that distributes the network traffic among the CCP servers based on predefined rules and criteria. The CCP supports multiple methods to authenticate applications, such as Allowed Machines, Client Certificate, OS User, Path, and Hash. These methods are based on registering information in the Vault with the unique application ID. For more information about the supported authentication methods, see Application authentication methods1. When installing the CCP and configuring it for use behind a load balancer, some authentication methods may be affected by the load balancer\\'s behavior and settings. Specifically, the following authentication methods may be affected: Allowed Machines authentication: This method authenticates applications based on their IP address or hostname. If the load balancer replaces the source IP or hostname of the routed packets with its own IP or hostname, the CCP will not be able to authenticate the application that initiated the credential request. To enable the CCP to resolve the IP or hostname of the application, the load balancer needs to be configured as a transparent proxy or to attach the X-Forwarded-For header to the routed packets. For more information, see Load balance the Central Credential Provider2. Client Certificate authentication: This method authenticates applications based on their client certificate that is signed by a trusted certificate authority (CA). The client certificate is used to establish a secure and trusted connection between the application and the CCP. If the load balancer terminates the SSL connection before proxying the traffic to the CCP, the CCP will not be able to verify the client certificate of the application. To enable the CCP to validate the client certificate, the load balancer needs to be configured as a pass-through proxy or to forward the client certificate to the CCP. For more information, see Load balance the Central Credential Provider2. The other authentication methods are not affected by the load balancer, as they do not rely on the IP, hostname, or certificate of the application. For example, the OS User method authenticates applications based on their Windows domain user, the Path method authenticates applications based on their URL path, and the Hash method authenticates applications based on a hash value that is generated from the application ID and a shared secret. These methods do not require any special configuration on the load balancer or the CCP.

QUESTION 10

You are setting up the Secrets Provider for Kubernetes to support rotation with Push-to-File mode.

Which deployment option should be used?

A. Init container

B. Application container

C. Sidecar

D. Service Broker

Correct Answer: C

According to the CyberArk Sentry Secrets Manager documentation, the Secrets Provider for Kubernetes can be

deployed as an init container or a sidecar in Push- to-File mode. In Push-to-File mode, the Secrets Provider pushes Conjur secrets to one or more secrets files in a shared volume in the same Pod as the application container. The application container can then consume the secrets files from the shared volume. The deployment option that should be used to support rotation with Push-to-File mode is the sidecar, because the sidecar can run continuously and check for updates to the secrets in Conjur. If changes are detected, the sidecar can update the secrets files in the shared volume. The init container, on the other hand, runs to completion and does not support rotation. The application container and the service broker are not valid deployment options for the Secrets Provider for Kubernetes in Push-to-File mode. References: 1: Secrets Provider - Init container/Sidecar - Push-to-File mode 2: Secrets Provider - init container/sidecar - Push-to-File mode