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

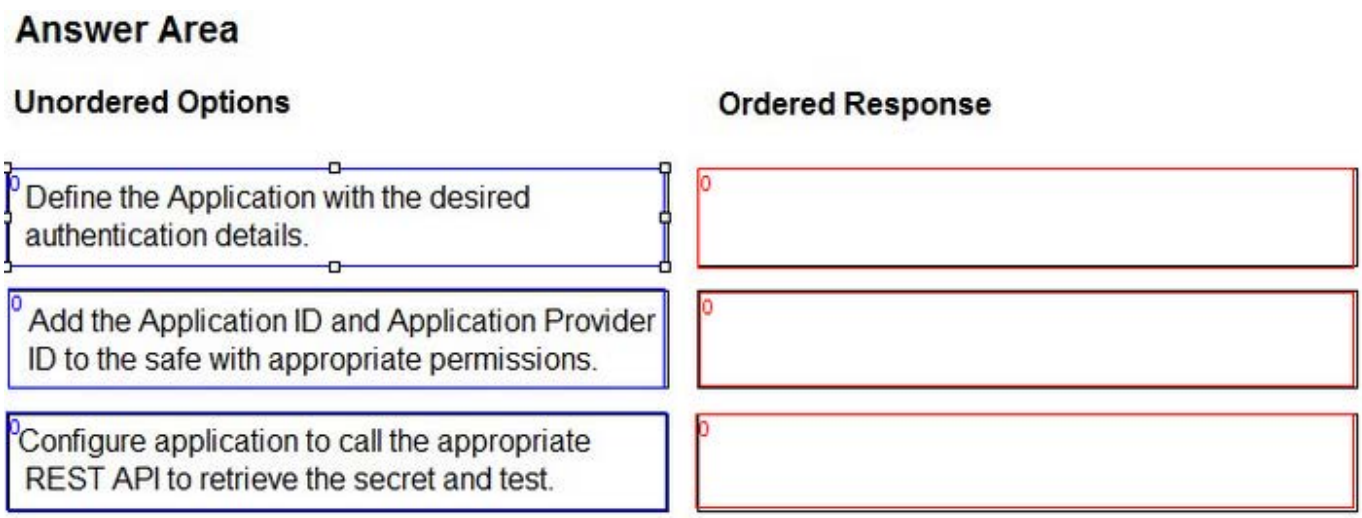
QUESTION 1

DRAG DROP

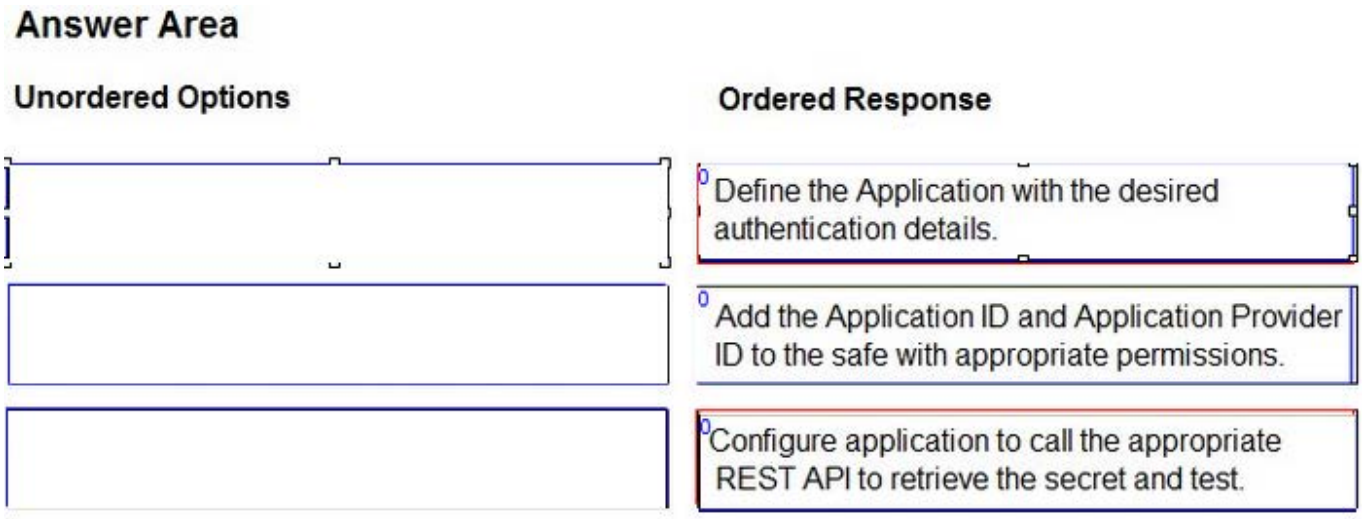
You want to allow retrieval of a secret with the CCP. The safe and the required secrets already exist.

Assuming the CCP is installed, arrange the steps in the correct sequence.

Select and Place:



Correct Answer:



The correct order of the steps is: Define the Application with the desired authentication details Add the Application ID and Application Provider ID to the safe with appropriate permissions Configure application to call the appropriate REST API to retrieve the secret and test To allow an application to retrieve a secret with the CCP, the following steps are required: Define the Application with the desired authentication details: This step involves creating an Application object in the Vault with a unique Application ID and an Application Provider ID. The Application Provider ID is used to identify the CCP instance that will serve the request. The Application object also defines the authentication method and parameters that the application will use to connect to the CCP, such as certificate, password, or AppRole. Add the Application ID and Application Provider ID to the safe with appropriate permissions: This step involves granting the Application object the necessary permissions to access the safe and the secret that it needs. The Application ID and the

Application Provider ID are added as members of the safe with at least List and Retrieve permissions. The secret name or ID can also be specified as a restriction to limit the access to a specific secret within the safe. Configure application to call the appropriate REST API to retrieve the secret and test: This step involves configuring the application to send a REST API request to the CCP endpoint with the required parameters, such as the Application ID, the Application Provider ID, the safe name, and the secret name or ID. The application should also provide the authentication credentials or token that match the method defined in the Application object. The application should receive a JSON response from the CCP with the secret value and other metadata. The application should test the connection and the secret retrieval before deploying to production. References: CyberArk Secrets Manager Sentry - Secrets Manager - Sample Items and Study Guide Sentry - Secrets Secrets Management Essentials for Developers

QUESTION 2

You are deploying Kubernetes resources/objects as Conjur identities.

In addition to Namespace and Deployment, from which options can you choose? (Choose two.)

A. ServiceAccount

B. Replica sets

C. Secrets

D. Tokenreviews

E. StatefulSet

Correct Answer: AE

ServiceAccount and StatefulSet are two of the Kubernetes resources/objects that can be used as Conjur identities, in addition to Namespace and Deployment. Conjur identities are the entities that can authenticate with Conjur and retrieve secrets from it. Conjur supports authenticating Kubernetes resources/objects using the Conjur Kubernetes Authenticator, which is a sidecar or init container that runs alongside the application container and injects the Conjur access token into a shared volume. The application container can then use the access token to fetch secrets from Conjur. A ServiceAccount is a Kubernetes resource that represents an identity for processes that run in a pod. ServiceAccounts can be used to grant specific privileges and permissions to the pod, and to enable communication with the Kubernetes API server. A ServiceAccount can be used as a Conjur identity by annotating it with the Conjur authentication policy branch ID, and by creating a Conjur host entity that matches the ServiceAccount name and namespace. The Conjur Kubernetes Authenticator will then use the ServiceAccount token to authenticate the pod with Conjur and obtain the Conjur access token. A StatefulSet is a Kubernetes resource that manages the deployment and scaling of a set of pods, and provides guarantees about the ordering and uniqueness of these pods. StatefulSets are useful for applications that require stable and persistent identities, such as databases, message brokers, or distributed systems. A StatefulSet can be used as a Conjur identity by annotating it with the Conjur authentication policy branch ID, and by creating a Conjur host entity that matches the StatefulSet name and namespace. The Conjur Kubernetes Authenticator will then use the pod name and namespace to authenticate the pod with Conjur and obtain the Conjur access token. The other options are not valid Kubernetes resources/objects that can be used as Conjur identities. Replica sets are a lower-level resource that are usually managed by higher-level resources such as Deployments or StatefulSets, and do not have their own identity or annotations. Secrets are a Kubernetes resource that store sensitive information such as passwords, tokens, or keys, and are not meant to be used as identities. Tokenreviews are a Kubernetes resource that are used to verify the validity of a ServiceAccount token, and are not meant to be used as identities either. References: Securing Secrets in Kubernetes - CyberArk Developer, Section "Conjur Kubernetes Authentication: A Hands-On Demonstration" GitHub - cyberark/secrets-provider-for-k8s: Cyberark secrets provider ..., Section "Consuming Secrets from CyberArk Secrets Provider" Secure your Kubernetes-deployed applications with CyberArk Conjur, Section "How it works" Simplify and Improve Container Security Using New CyberArk Conjur ..., Section "CyberArk Conjur Enterprise" Keeping Secrets Secure on Kubernetes - CyberArk Developer, Section "The Solution"

QUESTION 3

You start up a Follower and try to connect to it with a REST call using the server certificate, but you get an SSL connection refused error.

What could be the problem and how should you fix it?

A. The certificate does not contain the Follower hostname as a Subject Alternative Name (SAN). Generate a new certificate for the Follower.

B. One of the PostgreSQL ports (5432. 1999) is blocked by the firewall Open those ports.

C. Port 443 is blocked; open that port.

D. The certificate is unnecessary. Use the command option to suppress SSL certificate checking.

Correct Answer: A

The correct answer is A. The certificate does not contain the Follower hostname as a Subject Alternative Name (SAN). Generate a new certificate for the Follower. A possible explanation is: A Follower is a read-only node that replicates data from the Leader node in a Secrets Manager cluster. A Follower can serve requests from clients and applications that need to retrieve secrets or perform other read-only operations. To connect to a Follower with a REST call, the client or application needs to use the server certificate that was generated for the Follower during the installation process. The server certificate is used to establish a secure and trusted connection between the client or application and the Follower. However, if the server certificate does not contain the Follower hostname as a Subject Alternative Name (SAN), the connection will fail with an SSL connection refused error. This is because the SAN is an extension of the X.509 certificate standard that allows the certificate to specify multiple hostnames or IP addresses that the certificate is valid for. If the Follower hostname is not included in the SAN, the client or application will not be able to verify the identity of the Follower, and will reject the connection. To fix this problem, a new server certificate needs to be generated for the Follower, with the Follower hostname added to the SAN. The new certificate can be generated using the openssl command or another tool that supports the SAN extension. The new certificate also needs to be signed by the same certificate authority (CA) that signed the original certificate, and the CA certificate needs to be trusted by the client or application. The new certificate then needs to be copied to the Follower node and configured in the nginx.conf file. The Follower node also needs to be restarted for the changes to take effect. References: Secrets Manager Cluster Installation; Secrets Manager Cluster Configuration; Subject Alternative Name - Wikipedia

QUESTION 4

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 5

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