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.geekcert.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

If you rename an account or Safe, the Vault Conjur Synchronizer recreates these accounts and safes with their new name and deletes the old accounts or safes.

What does this mean?

A. Their permissions in Coniur must also be recreated to access them.

B. Their permissions in Coniur remain the same.

C. You can not rename an account or safe.

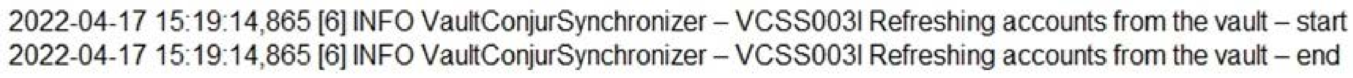
D. The Vault-Conjur Synchronizer will recreate these accounts and safes with their exact same names.

Correct Answer: A

When an account or Safe is renamed in the Vault, the Vault Conjur Synchronizer will create new variables in Conjur with the new name and delete the old variables with the old name. This means that the permissions that were granted to the old variables in Conjur will not apply to the new variables, and they will need to be recreated using delegation policies. Otherwise, the users or hosts that had access to the old variables will not be able to access the new ones. References: Manage Accounts and Safes During Synchronization; Vault Synchronizer full policy guide

QUESTION 2

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.

QUESTION 3

A customer has 100 .NET applications and wants to use Summon to invoke the application and inject secrets at run time.

Which change to the NET application code might be necessary to enable this?

A. It must be changed to include the REST API calls necessary to retrieve the needed secrets from the CCP.

B. It must be changed to access secrets from a configuration file or environment variable.

C. No changes are needed as Summon brokers the connection between the application and the backend data source through impersonation.

D. It must be changed to include the host API key necessary for Summon to retrieve the needed secrets from a Follower

Correct Answer: B

Summon is a utility that allows applications to access secrets from a variety of trusted stores and export them as environment variables to a sub-process environment. Summon does not require any changes to the application code to retrieve secrets from the CyberArk Central Credential Provider (CCP), as it uses a provider plugin that handles the communication with the CCP. However, the application code must be able to access secrets from a configuration file or environment variable, as these are the methods that Summon uses to inject secrets into the application. Summon reads a secrets.yml file that defines the secrets that the application needs and maps them to environment variables. Then, Summon fetches the secrets from the CCP using the provider plugin and exports them as environment variables to the application sub-process. The application can then read the secrets from the environment variables as if they were hard-coded in the configuration file. References: Summon-inject secrets, .NET Application Password SDK

QUESTION 4

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 5

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.