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

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

Which API endpoint can be used to discover secrets inside of Conjur?

A. Resources

B. Roles

C. Policies

D. WhoAmi

Correct Answer: A

Conjur is a secrets management solution that securely stores and manages secrets and credentials used by applications, DevOps tools, and other systems. Conjur provides a REST API that enables users to perform various operations on Conjur objects, such as secrets, policies, roles, and resources. The API endpoint for each Conjur object is composed of the base URL of the Conjur server, followed by the object type and identifier. For example, the API endpoint for a secret named db-password in the dev/my-app policy is: https:///secrets/dev/my-app/db-password To discover secrets inside of Conjur, the API endpoint that can be used is Resources. Resources are Conjur objects that have permissions and annotations associated with them, such as secrets, hosts, groups, and layers. The Resources API endpoint allows users to list, search, and filter resources based on various criteria, such as kind, owner, policy, and annotation. For example, the following API request will return a list of all secrets owned by the user alice: https:///resources?kind=variableandowner=user:alice The Resources API endpoint can help users to discover secrets inside of Conjur by providing information such as the name, ID, policy, owner, and annotations of each secret. Users can also use the Resources API endpoint to check the permissions and audit records of each secret, and to retrieve the secret value if they have the read permission. References: Conjur API; Resources API; Secrets API

QUESTION 4

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 5

A customer wants to minimize the Kubernetes application code developers must change to adopt Conjur for secrets access.

Which solutions can meet this requirement? (Choose two.)

A. CPM Push-to-File

B. Secrets Provider

C. authn-Azure

D. Secretless

E. Application Server Credential Provider

Correct Answer: BD

Secrets Provider and Secretless are two solutions that can minimize the Kubernetes application code changes required to adopt Conjur for secrets access. Secrets Provider is a Kubernetes Job or Deployment that runs as an init container or application container alongside the application pod. It retrieves secrets from Conjur and writes them to one or more files in a shared, mounted volume. The application can then consume the secrets from the files without any code changes, as reading local files is a common and platform-agnostic method. Secretless is a sidecar proxy that runs as a separate container in the same pod as the application. It intercepts the application\\'s requests to protected resources, such as databases or web services, and injects the secrets from Conjur into the requests. The application does not need to handle any secrets in its code, as Secretless handles the authentication and authorization for it. References: CyberArk Secrets Provider for Kubernetes, Secretless Broker