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.pass2lead.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

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 2

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.

QUESTION 3

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

QUESTION 4

An application is having authentication issues when trying to securely retrieve credential\\'s from the Vault using the CCP webservices RESTAPI. CyberArk Support advised that further debugging should be enabled on the CCP server to output a trace file to review detailed logs to help isolate the problem.

What best describes how to enable debug for CCP?

A. Edit web.config. change the "AIMWebServiceTrace" value, restart Windows Web Server (IIS)

B. In the PVWA, go to the Applications tab, select the Application in question, go to Options > Logging and choose Debug.

C. From the command line, run appprvmgr.exe update_config logging=debug.

D. Edit the basic_appprovider.conf, change the "AIMWebServiceTrace" value, and restart the provider.

Correct Answer: A

The best way to enable debug for CCP is to edit the web.config file in the AIMWebService folder and change the value of the AIMWebServiceTrace parameter to 4, which is the verbose level. This will generate detailed logs in the AIMWSTrace.log file in the logs folder. The logs folder may need to be created manually and given the appropriate permissions for the IIS_IUSRS group. After changing the web.config file, the Windows Web Server (IIS) service needs to be restarted to apply the changes. This method is recommended by CyberArk Support and documented in the CyberArk Knowledge Base1. Editing the basic_appprovider.conf file and changing the AIMWebServiceTrace value is not a valid option, as this parameter does not exist in this file. The basic_appprovider.conf file is used to configure the basic provider settings, such as the AppProviderVaultParmsFile, the AppProviderPort, and the AppProviderCacheMode. The AIMWebServiceTrace parameter is only found in the web.config file of the AIMWebService. In the PVWA, going to

the Applications tab, selecting the Application in question, and going to Options > Logging and choosing Debug is not a valid option, as this will only enable debug for the Application Identity Manager (AIM) component, not the CCP component. The AIM component is used to manage the application identities and their access to the Vault. The CCP component is used to provide secure retrieval of credentials from the Vault using web services. Enabling debug for AIM will generate logs in the APPconsole.log, APPtrace.log, and APPaudit.log files in the ApplicationPasswordProvider\Logs folder, but these logs will not help to troubleshoot the CCP authentication issues. From the command line, running appprvmgr.exe update_config logging=debug is not a valid option, as this will only enable debug for the Application Provider Manager (APM) component, not the CCP component. The APM component is used to manage the configuration and operation of the providers, such as the basic provider, the LDAP provider, and the ENE provider. Running appprvmgr.exe update_config logging=debug will generate logs in the appprvmgr.log file in the ApplicationPasswordProvider\Logs folder, but these logs will not help to troubleshoot the CCP authentication issues. References: Enable Debugging and Gather Logs - Central Credential Provider1

QUESTION 5

Which statement is correct about this message?

Message: "[number-of-deleted-rows] rows has successfully deleted "CEADBR009D Finished vacuum"?

A. It notes the number of records deleted from the database and does not require any action.

B. The user specified for Conjur does not have the appropriate permissions to retrieve the audit database (audit .db).

C. When audit retention was performed, the query on the UI audit database (audit.db) generated an error.

D. The Vault Conjur Synchronizer successfully deleted the password objects that were marked for deletion in the PVWA.

Correct Answer: A

This is the correct answer because the message indicates that the audit retention process has successfully completed and deleted the specified number of rows from the audit database (audit.db). The audit retention process is a scheduled task that runs periodically to delete old audit records from the audit database based on the retention period configured in the Conjur UI. The audit retention process also performs a vacuum operation to reclaim the disk space and optimize the database performance. The message does not require any action from the user, as it is a normal and expected outcome of the audit retention process. This answer is based on the CyberArk Secrets Manager documentation1 and the CyberArk Secrets Manager training course2. The other options are not correct statements about the message. The message does not imply that the user specified for Conjur does not have the appropriate permissions to retrieve the audit database, as the message is not an error or a warning, but a confirmation of the audit retention process. The user specified for Conjur is the user that is used to connect to the Conjur server and perform operations on the Conjur resources, such as roles, policies, secrets, and audit records. The user specified for Conjur needs to have the appropriate permissions to access the audit database, but the message does not indicate any problem with the user permissions. The message does not imply that when audit retention was performed, the query on the UI audit database generated an error, as the message is not an error or a warning, but a confirmation of the audit retention process. The query on the UI audit database is the query that is used to display the audit records in the Conjur UI. The query on the UI audit database is not related to the audit retention process, which is a background task that runs on the Conjur server and deletes the old audit records from the audit database. The message does not indicate any problem with the query on the UI audit database. The message does not imply that the Vault Conjur Synchronizer successfully deleted the password objects that were marked for deletion in the PVWA, as the message is not related to the Vault Conjur Synchronizer or the password objects. The Vault Conjur Synchronizer is a service that synchronizes secrets from the CyberArk Vault to the Conjur database. The password objects are the accounts in the CyberArk Vault that store the credentials for various platforms and devices. The message is related to the audit retention process, which deletes the old audit records from the audit database. The message does not indicate any problem or action with the Vault Conjur Synchronizer or the password objects.

Latest SECRET-SEN Dumps | SECRET-SEN Study Guide | SECRET-SEN Exam Questions