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

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

QUESTION 1

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 2

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.

QUESTION 3

When attempting to retrieve a credential, you receive an error 401 ?Malformed Authorization Token.

What is the cause of the issue?

A. The token is not correctly encoded.

B. The token you are trying to retrieve does not exist.

C. The host does not have access to the credential with the current token.

D. The credential has not been initialized.

Correct Answer: A

= The cause of the issue is that the token is not correctly encoded. A token is a string of characters that represents a credential or an authorization grant for accessing a resource. A token must be encoded according to a specific format and standard, such as Base64, JSON Web Token (JWT), or OAuth 2.0. If the token is malformed, meaning that it does not follow the expected format or standard, the server will reject the token and return an error 401 - Malformed Authorization Token. This error indicates that the token is invalid or expired, and the request is unauthorized. To resolve the issue, the token must be regenerated or refreshed using the correct encoding method and parameters12. References: = CyberArk Identity: Getting 401 unauthorized Error when using API calls with OAuth2 Client 2, Resolution

1 Troubleshoot CyberArk Vault Synchronizer 1, Error: Forbidden Logon Token is Empty - Cannot logon Unauthorized

QUESTION 4

You modified a Conjur host policy to change its annotations for authentication.

How should you load the policy to make those changes?

A. Use the default "append" method (e.g. conjur policy load).

B. Use the "replace" method (e.g. conjur policy load ??eplace;;).

C. Use the "delete" method (e.g. conjur policy load ??elete;;).

D. Use the "update" method (e.g. conjur policy load ??pdate;;).

Correct Answer: B

= According to the CyberArk Sentry Secrets Manager documentation, the replace method is used to overwrite an existing policy branch with a new policy file. This method is suitable for making changes to the existing resources, such as modifying their annotations, permissions, or attributes. The replace method preserves the existing data and secrets associated with the resources, but removes any resources that are not defined in the new policy file. Therefore, to change the annotations for authentication of a Conjur host, the replace method is the best option. The append method is used to add new resources or data to an existing policy branch, without affecting the existing resources. This method is suitable for creating new hosts, groups, variables, or secrets, but not for modifying the existing ones. The append method will ignore any changes to the existing resources, such as annotations, and will only load the new resources or data. The delete method is used to remove resources or data from an existing policy branch, without affecting the other resources. This method is suitable for deleting hosts, groups, variables, or secrets, but not for modifying them. The delete method will remove any resources or data that are defined in the policy file, and will ignore any resources or data that are not defined in the policy file. The update method is used to modify the data or secrets associated with existing resources, without affecting the resources themselves. This method is suitable for changing the values of variables or secrets, but not for changing the annotations, permissions, or attributes of the resources. The update method will only load the data or secrets that are defined in the policy file, and will ignore any resources or data that are not defined in the policy file. References: = Annotation reference | CyberArk Docs; Policy load modes | CyberArk Docs; Policy - docs.cyberark.com

QUESTION 5

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