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

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

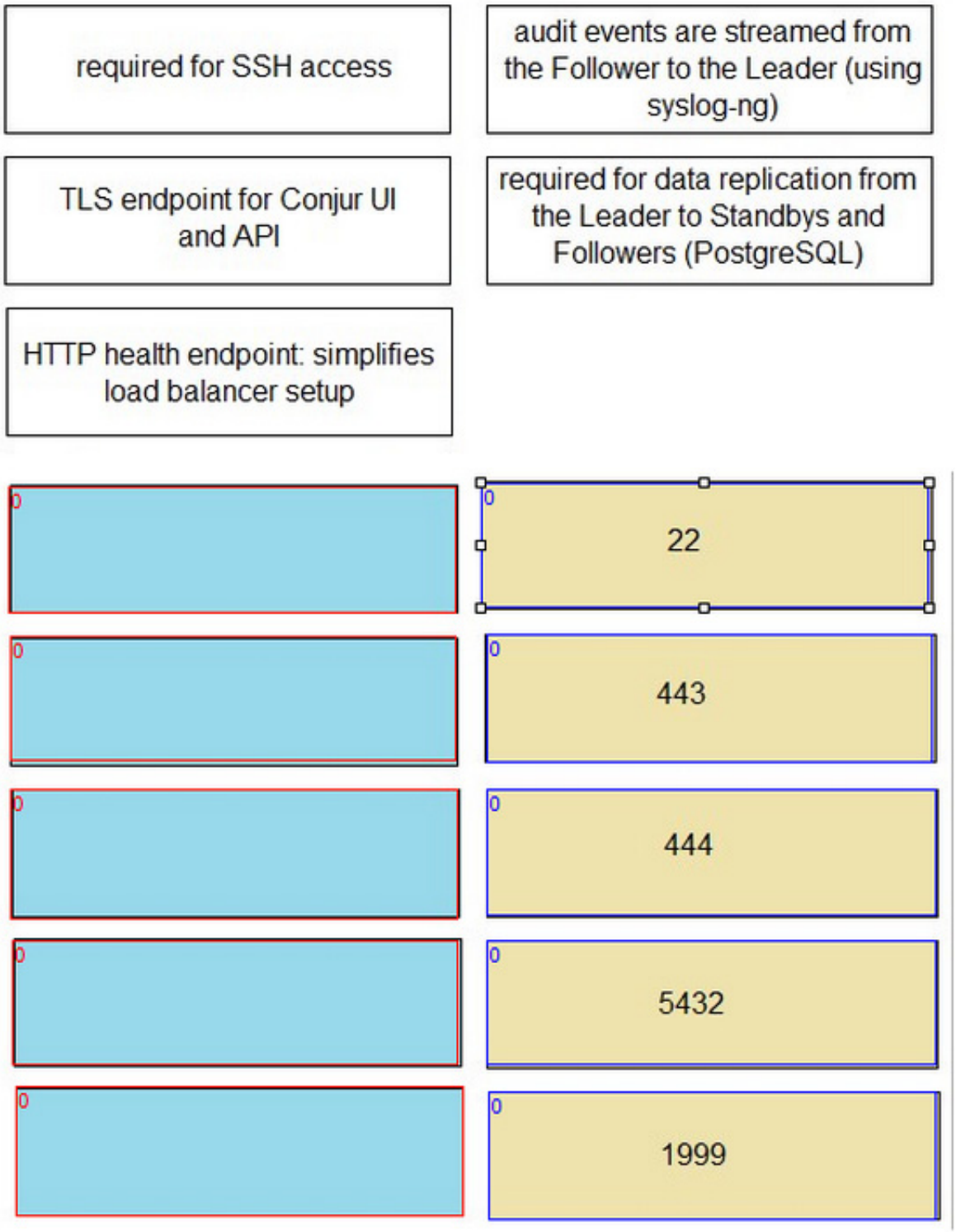
QUESTION 1

DRAG DROP

Match the correct network port to its function in Conjur.

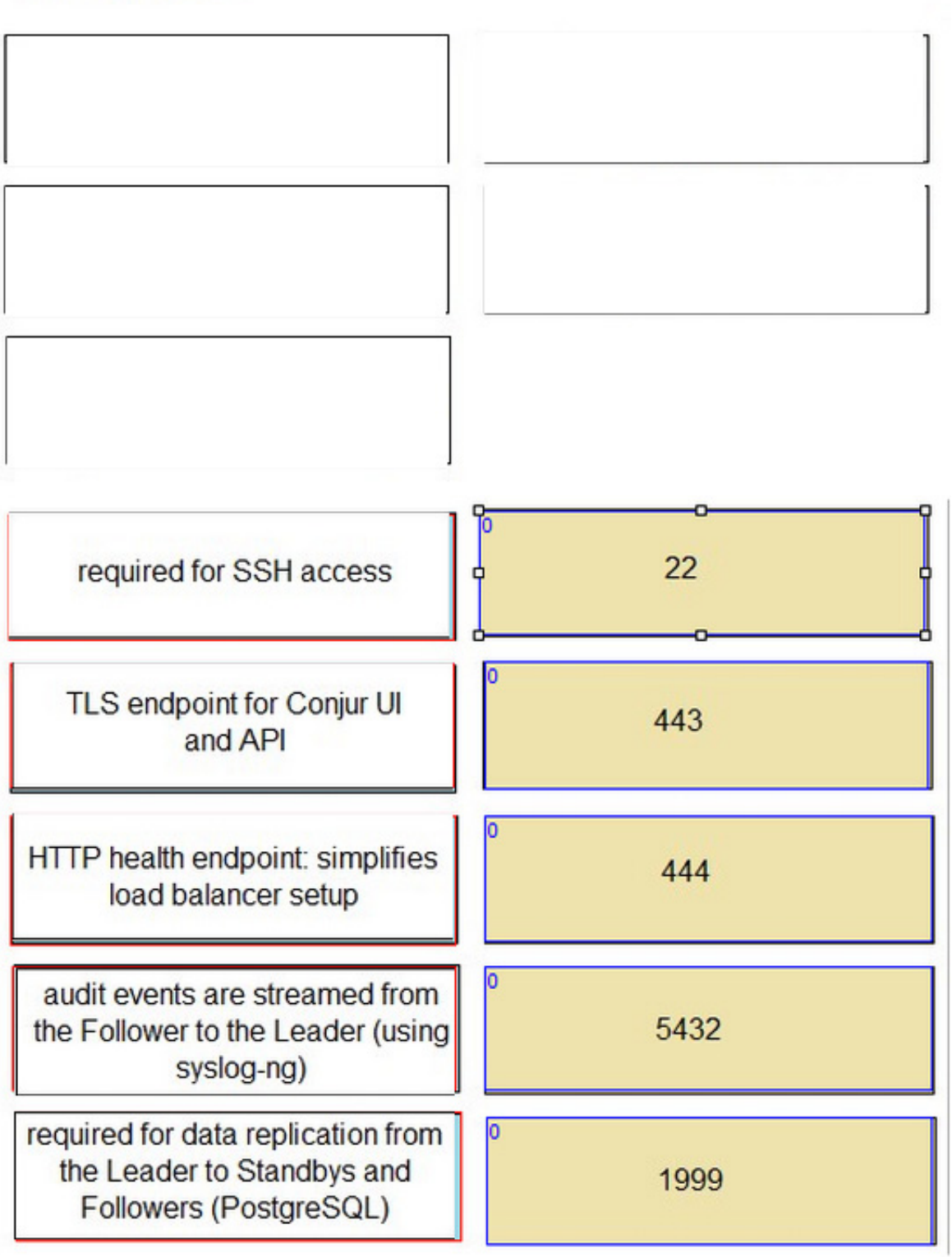
Select and Place:

Answer Area



Correct Answer:

Answer Area



Based on the image you sent, the correct network port to its function in Conjur are:

22: required for SSH access

443: TLS endpoint for Conjur UI and API

444: HTTP health endpoint: simplifies load balancer setup

1999: audit events are streamed from the Follower to the Leader (using syslog-ng)

5432: required for data replication from the Leader to Standbys and Followers (PostgreSQL)

These are the standard ports and protocols used by the Conjur components to communicate with each other and with external clients. The ports can be customized according to the network and security requirements of the organization.

These ports are documented in the CyberArk Secrets Manager documentation1 and the CyberArk Secrets Manager training course2.

QUESTION 2

While retrieving a secret through REST, the secret retrieval fails to find a matching secret. You know the secret onboarding process was completed, the secret is in the expected safe with the expected object name, and the CCP is able to provide secrets to other applications.

What is the most likely cause for this issue?

A. The application ID or Application Provider does not have the correct permissions on the safe.

B. The client certificate fingerprint is not trusted.

C. The service account running the application does not have the correct permissions on the safe.

D. The OS user does not have the correct permissions on the safe

Correct Answer: A

The most likely cause for this issue is A. The application ID or Application Provider does not have the correct permissions on the safe. The CyberArk Central Credential Provider (CCP) is a web service that enables applications to retrieve secrets from the CyberArk Vault using REST API calls. The CCP requires an application ID or an Application Provider to authenticate and authorize the application before returning the requested secret. The application ID or Application Provider must have the Retrieve and List permissions on the safe where the secret is stored, otherwise the CCP will not be able to find the matching secret and will return an error. To resolve this issue, you should verify that the application ID or Application Provider has the correct permissions on the safe, and that the safe name and object name are correctly specified in the REST API call. You can use the CyberArk Privileged Access Security Web Access (PVWA) or the PrivateArk Client to check and modify the permissions on the safe. You can also use the CyberArk REST API Tester or a tool like Postman to test the REST API call and see the response from the CCP. For more information, refer to the following resources: Credential Providers - Centralized Credential Management | CyberArk, Section "Central Credential Provider" Credential Provider - CyberArk, Section "Using the Credential Provider" How to Build Your Secrets Management REST API\\'s into Postman, Section "How to Build Your Secrets Management REST API\\'s into Postman"

QUESTION 3

While installing the first CP in an environment, errors that occurred when the environment was created are displayed; however, the installation procedure continued and finished successfully.

What should you do?

A. Continue configuring the application to use the CP. No further action is needed since the successful installation

makes the error message benign.

B. Review the lag file \\'CreateEnv.loq\\' and investigate any error messages it contains.

C. Run setup.exe again and select \\'Recreate Vault Environment\\'. Provide the details of a user with more privileges when prompted by the installer.

D. Review the PV WA lags to determine which REST API call used during the installation failed.

Correct Answer: B

B. Review the log file `CreateEnv.log\\' and investigate any error messages it contains. This is the best option because the CreateEnv.log file records the steps and results of creating the CP environment in the Vault during the installation. The CP environment includes the safe, the provider user, the application user, and the application identity. If any errors occurred when creating the CP environment, they will be logged in this file and may indicate a problem with the Vault connection, the credential file, the permissions, or the configuration. Reviewing the log file can help to identify and resolve the root cause of the errors and ensure the CP environment is properly set up. Continuing configuring the application to use the CP without further action is not a good option because it may lead to unexpected or inconsistent behavior of the CP or the application. The errors that occurred when creating the CP environment may affect the security, availability, or integrity of the credentials or the application. Ignoring the errors may also make it harder to troubleshoot or fix them later. Running setup.exe again and selecting `Recreate Vault Environment\\' is not a good option because it may overwrite or delete the existing CP environment and cause more errors or conflicts. Recreating the Vault environment should only be done after reviewing the log file and understanding the cause of the errors. Moreover, recreating the Vault environment may require more privileges than creating it for the first time, as some objects may be already in use or locked. Reviewing the PVWA logs to determine which REST API call used during the installation failed is not a good option because it may not provide enough information or context to understand or resolve the errors. The PVWA logs may show the HTTP status codes or messages of the REST API calls, but they may not show the details or parameters of the calls or the responses. The PVWA logs may also contain other unrelated or irrelevant entries that may confuse or distract from the errors. The CreateEnv.log file is a more specific and reliable source of information for the errors that occurred when creating the CP environment.

QUESTION 4

An application owner reports that their application is suddenly receiving an incorrect password. CPM logs show the password was recently changed, but the value currently being retrieved by the application is a different value. The Vault Conjur Synchronizer service is running.

What is the most likely cause of this issue?

A. The Vault Conjur Synchronizer is not configured with the DR Vault IP address and there has been a failover event.

B. Dual Accounts are in use, but after the CPM changed the password for the Inactive account, it accidentally updated the password for the Active account instead.

C. The CPM is writing password changes to the Primary Vault while the Vault Conjur Synchronizer is configured to replicate from the DR Vault.

D. The application has been configured to retrieve the wrong password.

Correct Answer: C

This is the most likely cause of this issue because it creates a discrepancy between the passwords stored in the Primary Vault and the DR Vault, which affects the Vault Conjur Synchronizer service (Synchronizer) and the application. The

Synchronizer is a service that synchronizes secrets from the CyberArk Vault to the Conjur database. The application is

a client that retrieves secrets from the Conjur database using the Conjur REST API. The CPM is a component that

manages the lifecycle of the passwords stored in the CyberArk Vault, such as changing, verifying, and reconciling them. If the CPM is writing password changes to the Primary Vault while the Synchronizer is configured to replicate from the

DR Vault, the following scenario may occur:

The CPM changes the password for an account in the Primary Vault and updates the password value in the Vault database.

The Synchronizer does not detect the password change in the DR Vault, as the DR Vault database has not been updated yet with the new password value. The Synchronizer does not sync the new password value to the Conjur database, as

it assumes that the password value in the DR Vault database is the latest and correct one.

The application requests the password value from the Conjur database and receives the old password value, which is different from the new password value in the Primary Vault database.

The application tries to use the old password value to access the target platform or device and fails, as the target platform or device expects the new password value. This answer is based on the CyberArk Secrets Manager documentation1

and the CyberArk Secrets Manager training course2.

QUESTION 5

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