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.leads4pass.com/secret-sen.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CyberArk Official Exam Center

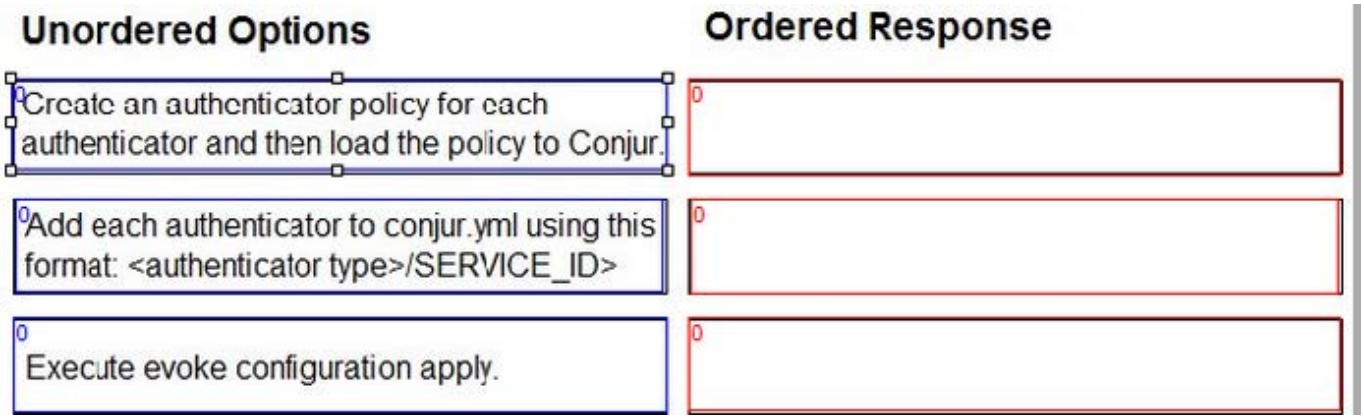
- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

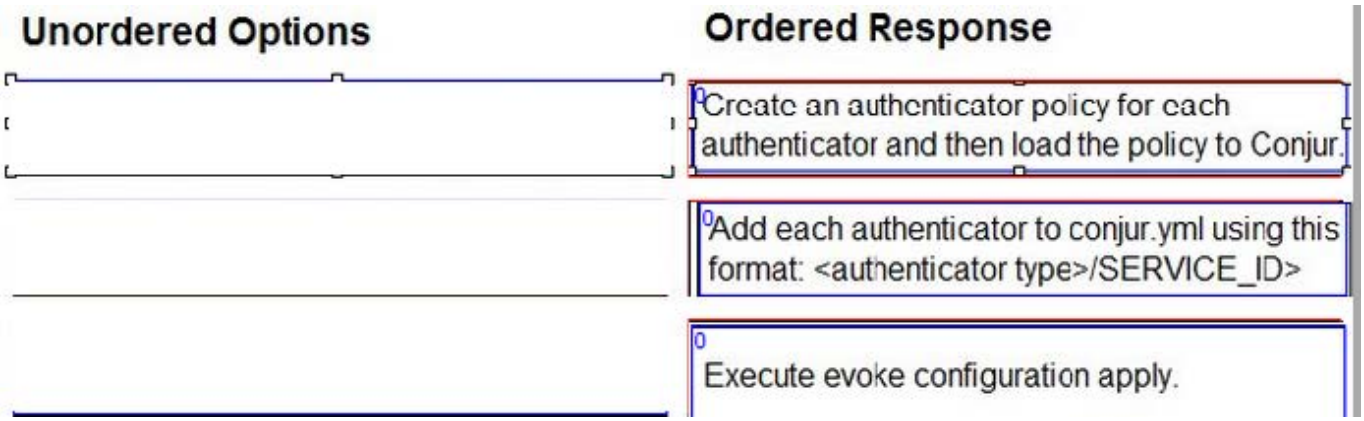
DRAG DROP

Arrange the steps to configure authenticators in the correct the sequence.

Select and Place:



Correct Answer:



Create an authenticator policy for each authenticator and then load the policy to Conjur.

Add each authenticator to conjur.yml using this format: .

Execute evoke configuration apply.

Comprehensive Authenticators are plugins that enable Conjur to authenticate requests from different types of clients, such as Kubernetes, Azure, or LDAP. To configure authenticators, you need to follow these steps:

Create an authenticator policy for each authenticator and then load the policy to Conjur. This step defines the authenticator as a resource in Conjur and grants permissions to the users or hosts that can use it. You can use the policy templates

provided by Conjur for each authenticator type, or create your own custom policy. For more information, see Define Authenticator Policy. Add each authenticator to conjur.yml using this format: . This step

enables the authenticator service on the Conjur server and specifies the service ID that identifies the authenticator

instance. The service ID must match the one used in the policy. For more information, see Enable Authenticators.

Execute evoke configuration apply. This step applies the changes made to the conjur.yml file and restarts the Conjur service. This is necessary for the authenticator configuration to take effect. For more information, see Apply Configuration

Changes.

References: The steps to configure authenticators are explained in detail in the Configure Authenticators section of the CyberArk Conjur Enterprise documentation. The image in the question is taken from the same source.

QUESTION 2

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 3

You have a request to protect all the properties around a credential object. When configuring the credential in the Vault, you specified the address, user and password for the credential.

How do you configure the Vault Conjur Synchronizer to properly sync all properties?

A. Modify VaultConjurSynchronizer.exe.config, uncomment SYNCALLPROPERTIES and update its value to true.

B. Modify SynchronizerReplication.config, uncomment SYNCALLPROPERTIES and update its value to true.

C. Modify Vault.ini, uncomment SYNCALLPROPERTIES and update its value to true.

D. In the Conjur UI under Cluster > Synchronizer > Config, change SYNCALLPROPERTIES and update its value to true.

Correct Answer: B

This is the correct answer because the SynchronizerReplication.config file contains the configuration settings for the Vault Conjur Synchronizer service (Synchronizer) to sync secrets from the CyberArk Vault to the Conjur database. The SYNCALLPROPERTIES parameter specifies whether to sync all the properties of the accounts in the Vault or only the password property. By default, the SYNCALLPROPERTIES parameter is set to false, which means that only the password property is synced. To sync all the properties, such as the address and the user, the SYNCALLPROPERTIES parameter needs to be set to true. This answer is based on the CyberArk Secrets Manager documentation1 and the CyberArk Secrets Manager training course2. The other options are not correct because they do not configure the Synchronizer to properly sync all properties. Modifying VaultConjurSynchronizer.exe.config, uncommenting SYNCALLPROPERTIES and updating its value to true is not a valid option, as this file does not contain the SYNCALLPROPERTIES parameter. The VaultConjurSynchronizer.exe.config file contains the configuration settings for the Synchronizer service, such as the log level, the log path, and the service name. The SYNCALLPROPERTIES parameter is only found in the SynchronizerReplication.config file. Modifying Vault.ini, uncommenting SYNCALLPROPERTIES and updating its value to true is not a valid option, as this file does not contain the SYNCALLPROPERTIES parameter. The Vault.ini file contains the configuration settings for the CyberArk Central Credential Provider (CCP) to connect to the Vault server and provide credentials to the applications. The SYNCALLPROPERTIES parameter is not related to the CCP configuration or functionality. In the Conjur UI under Cluster > Synchronizer > Config, changing SYNCALLPROPERTIES and updating its value to true is not a valid option, as this section does not exist in the Conjur UI. The Conjur UI does not have a Cluster, Synchronizer, or Config section. The Conjur UI has a Cluster Config section under Settings, but this section is used to configure the Conjur cluster settings, such as the master IP address, the follower IP address, and the seed fetcher IP address. The SYNCALLPROPERTIES parameter is not related to the Conjur cluster configuration or functionality.

QUESTION 4

What is a possible Conjur node role change?

A. A Standby may be promoted to a Leader.

B. A Follower may be promoted to a Leader.

C. A Standby may be promoted to a Follower.

D. A Leader may be demoted to a Standby in the event of a failover.

Correct Answer: A

According to the CyberArk Sentry Secrets Manager documentation, Conjur is a secrets management solution that consists of a leader node and one or more follower nodes. The leader node is responsible for managing the secrets, policies,

and audit records, while the follower nodes are read-only replicas that can serve secrets requests from applications. Additionally, Conjur supports a standby node, which is a special type of follower node that can be promoted to a leader node

in case of a leader failure. A standby node is synchronized with the leader node and can take over its role in a disaster recovery scenario. A possible Conjur node role change is when a standby node is promoted to a leader node, either

manually or automatically, using the auto-failover feature. A follower node cannot be promoted to a leader node, as it does not have the same data and functionality as the leader node. A standby node cannot be promoted to a follower node,

as it already has the same capabilities as a follower node, plus the ability to become a leader node. A leader node cannot be demoted to a standby node in the event of a failover, as it would lose its data and functionality and would not be able

to resume its role as a leader node.

References:

1: Conjur Architecture

2: Deploying Conjur on AWS

3: Auto-failover

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.

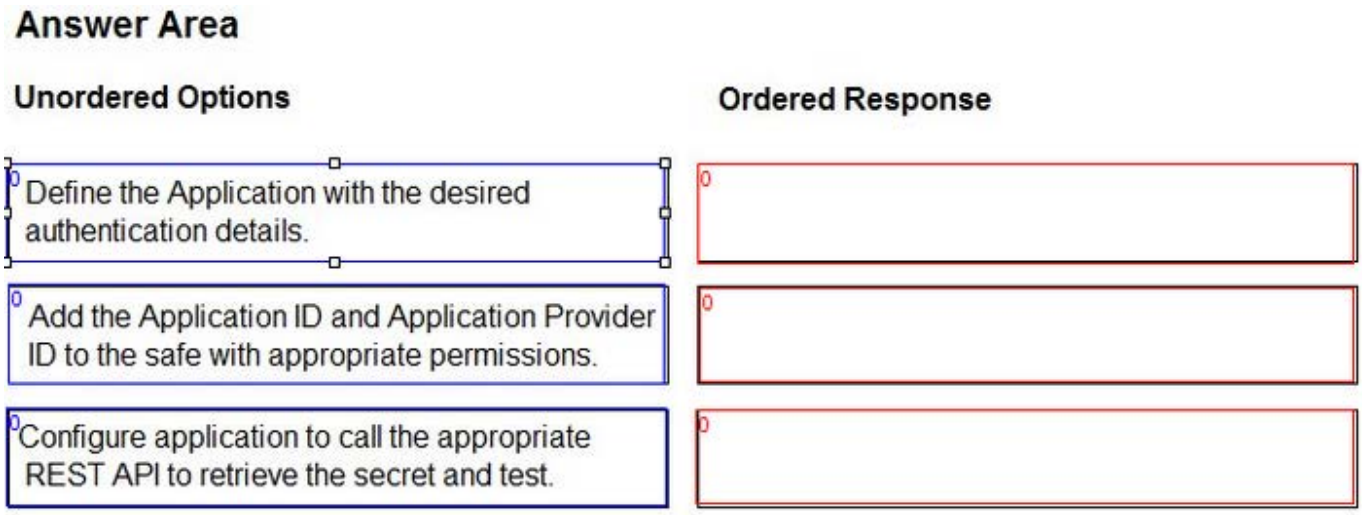
QUESTION 6

DRAG DROP

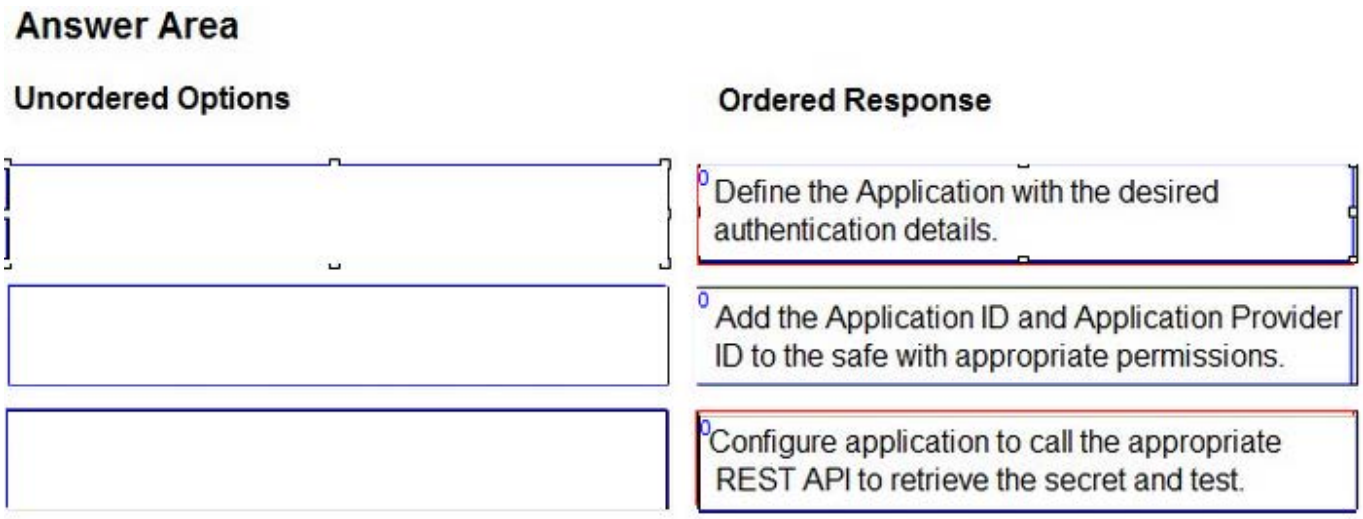
You want to allow retrieval of a secret with the CCP. The safe and the required secrets already exist.

Assuming the CCP is installed, arrange the steps in the correct sequence.

Select and Place:



Correct Answer:



The correct order of the steps is: Define the Application with the desired authentication details Add the Application ID and Application Provider ID to the safe with appropriate permissions Configure application to call the appropriate REST API to retrieve the secret and test To allow an application to retrieve a secret with the CCP, the following steps are required: Define the Application with the desired authentication details: This step involves creating an Application object in the Vault with a unique Application ID and an Application Provider ID. The Application Provider ID is used to identify the CCP instance that will serve the request. The Application object also defines the authentication method and parameters that the application will use to connect to the CCP, such as certificate, password, or AppRole. Add the Application ID and Application Provider ID to the safe with appropriate permissions: This step involves granting the Application object the necessary permissions to access the safe and the secret that it needs. The Application ID and the Application Provider ID are added as members of the safe with at least List and Retrieve permissions. The secret name or ID can also be specified as a restriction to limit the access to a specific secret within the safe. Configure application to call the appropriate REST API to retrieve the secret and test: This step involves configuring the application to send a REST API request to the CCP endpoint with the required parameters, such as the Application ID, the Application Provider ID, the safe name, and the secret name or ID. The application should also provide the authentication credentials or token that match the method defined in the Application object. The application should receive a JSON response from the CCP with the secret value and other metadata. The application should test the connection and the secret retrieval before deploying to production. References: CyberArk Secrets Manager Sentry - Secrets Manager - Sample Items and Study Guide Sentry - Secrets Secrets Management Essentials for Developers

QUESTION 7

You are setting up a Kubernetes integration with Conjur. With performance as the key deciding factor, namespace and service account will be used as identity characteristics.

Which authentication method should you choose?

A. JWT-based authentication

B. Certificate-based authentication

C. API key authentication

D. Connect (OIDC) authentication

Correct Answer: A

According to the CyberArk Sentry Secrets Manager documentation, JWT- based authentication is the recommended method for authenticating Kubernetes pods with Conjur. JWT-based authentication uses JSON Web Tokens (JWTs)

that are issued by the Kubernetes API server and signed by its private key. The JWTs contain the pod\\'s namespace and service account as identity characteristics, which are verified by Conjur against a policy that defines the allowed namespaces and service accounts. JWT-based authentication is fast, scalable, and secure, as it does not require any additional certificates, secrets, or sidecars to be deployed on the pods. JWT-based authentication also supports rotation and revocation of the Kubernetes API server\\'s private key, which enhances the security and resilience of the authentication process. Certificate-based authentication is another method for authenticating Kubernetes pods with Conjur, but it is not the best option for performance. Certificate-based authentication uses X.509 certificates that are generated by a Conjur CA service and injected into the pods as Kubernetes secrets. The certificates contain the pod\\'s namespace and service account as identity characteristics, which are verified by Conjur against a policy that defines the allowed namespaces and service accounts. Certificate-based authentication is secure and reliable, but it requires more resources and steps to generate, inject, and manage the certificates and secrets. Certificate-based authentication also does not support rotation and revocation of the certificates, which may pose a security risk if the certificates are compromised or expired. API key authentication and Connect (OIDC) authentication are not valid methods for authenticating Kubernetes pods with Conjur. API key authentication is used for authenticating hosts, users, and applications that have a Conjur identity and an API key. Connect (OIDC) authentication is used for authenticating users and applications that have an OpenID Connect identity and a token. These methods are not suitable for Kubernetes pods, as they do not use the pod\\'s namespace and service account as identity characteristics, and they require additional secrets or tokens to be stored and managed on the pods. References: = JWT Authenticator | CyberArk Docs; Certificate Authenticator | CyberArk Docs; API Key Authenticator | CyberArk Docs; Connect Authenticator | CyberArk Docs

QUESTION 8

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 9

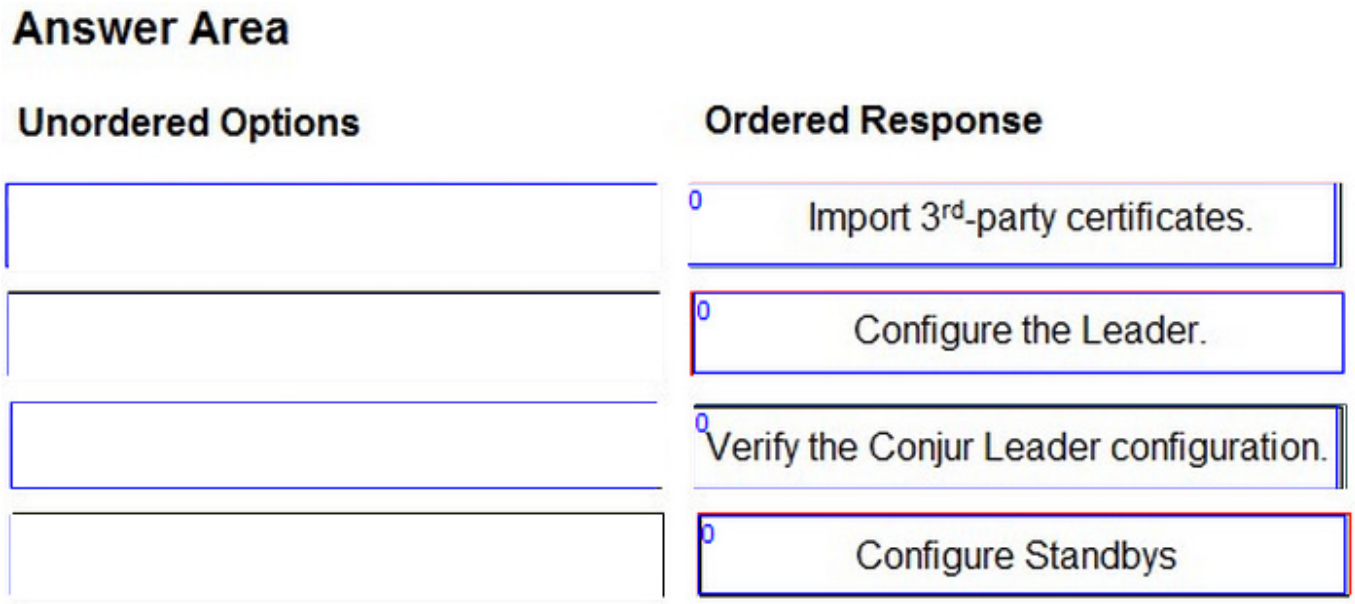
DRAG DROP

You are configuring the Conjur Cluster with 3rd-party certificates.

Arrange the steps to accomplish this in the correct sequence.

Select and Place:

Correct Answer:



The correct sequence of steps to configure the Conjur Cluster with 3rd-party certificates is as follows: Import 3rd-party certificates to the Leader using the command: docker exec mycontainer evoke ca import --force --root --chain 1 Configure the Leader using the command: docker exec mycontainer evoke configure master --accept-eula --hostname --admin-password 1 Verify the Conjur Leader configuration using the command: docker exec mycontainer evoke role Configure the Standbys using the command: docker exec mycontainer evoke configure standby --master-address

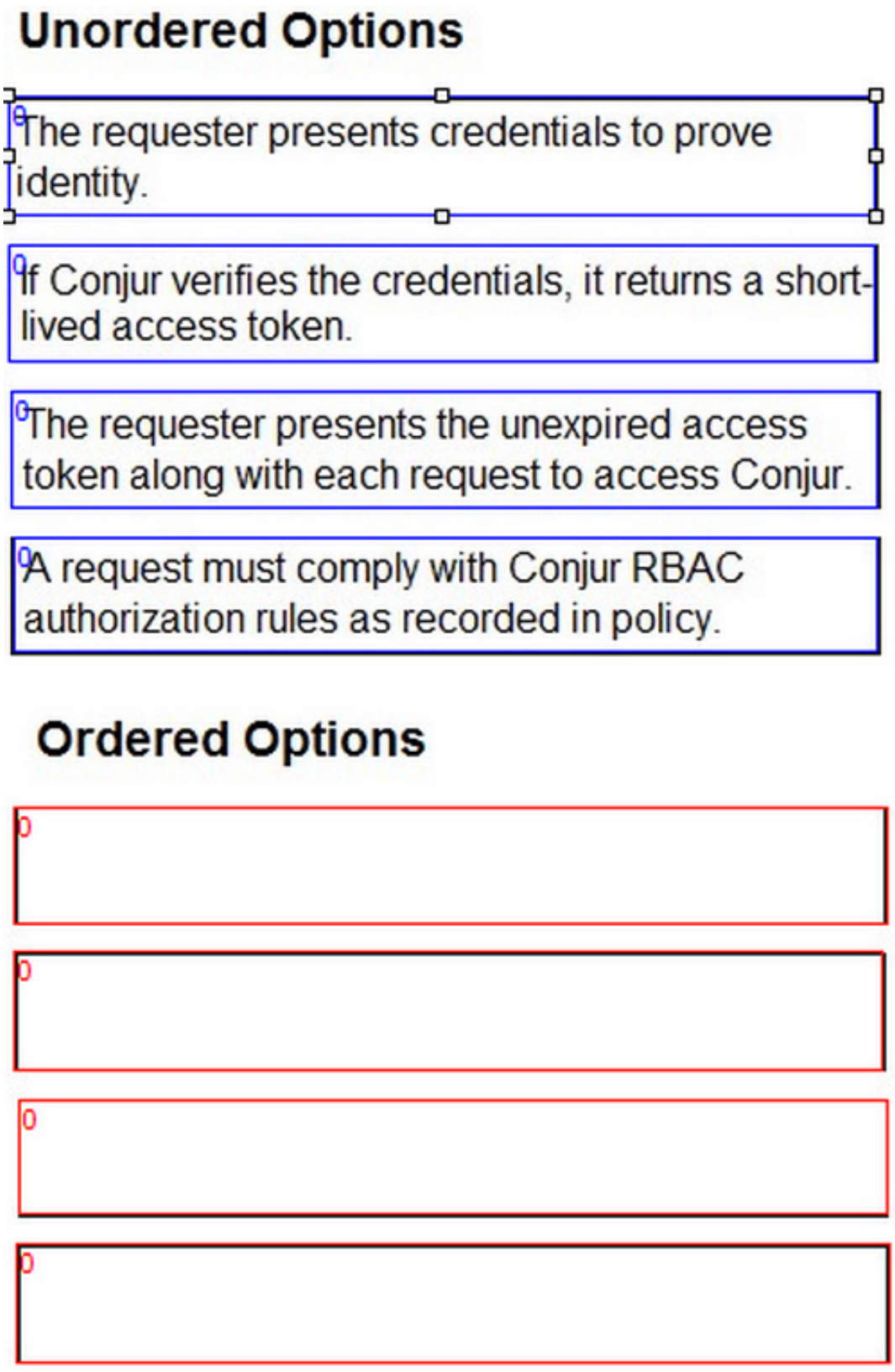
--master-fingerprint 1 References: Certificate requirements

QUESTION 10

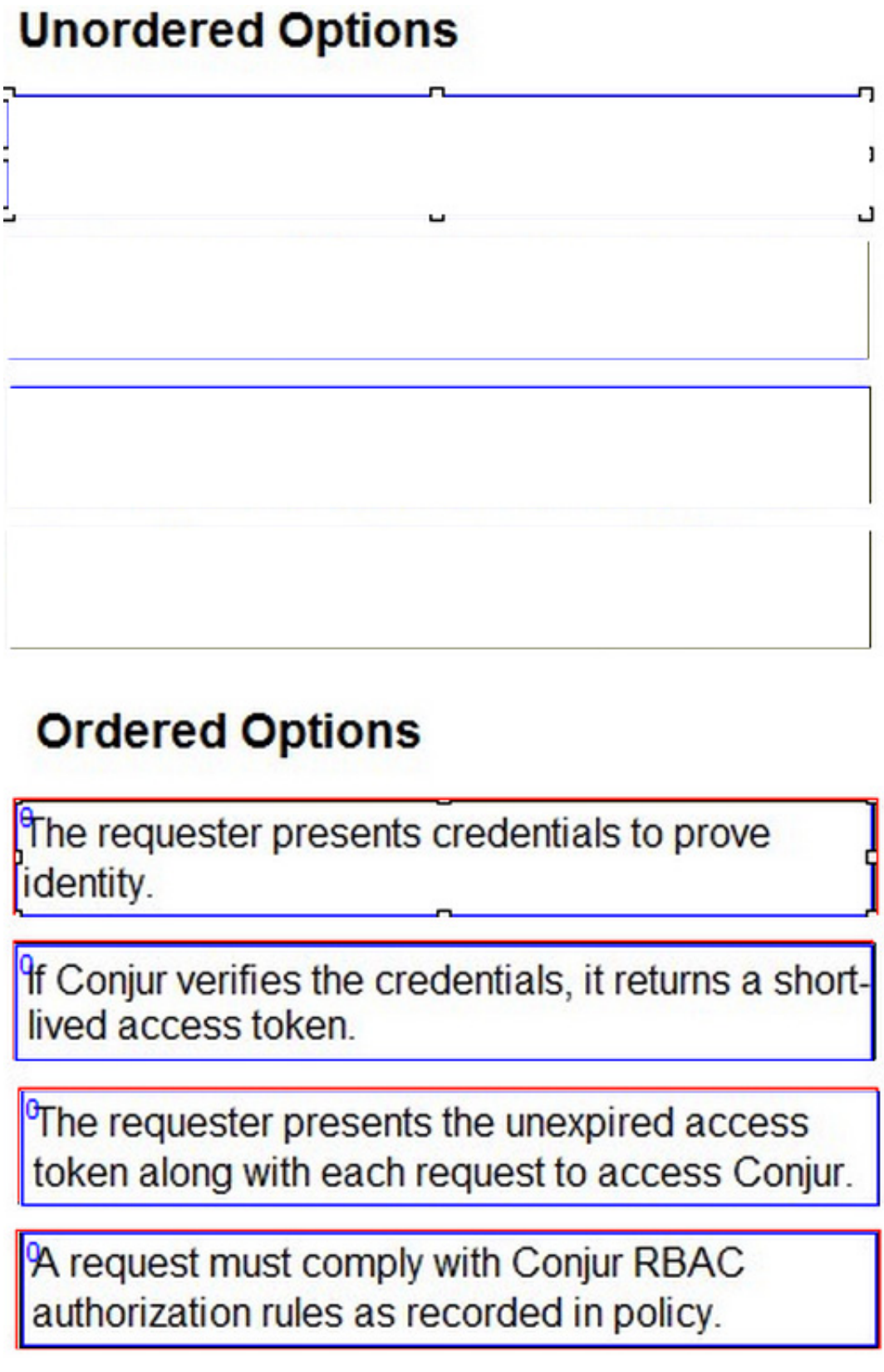
DRAG DROP

Arrange the steps of a Conjur authentication flow in the correct sequence.

Select and Place:



Correct Answer:



References:

CyberArk Sentry Secrets Manager

documentation: https://docs.cyberark.com/Portal/Content/Resources/_TopNav/cc_ Portal.htm

CyberArk Sentry Secrets Manager course

materials: https://training.cyberark.com/learn

CyberArk whitepapers and technical

resources: https://www.cyberark.com/resources/home/cyberark-secrets-manager

The authentication flow begins with the requester presenting their credentials to Conjur. This can be in the form of a username and password, an API key, or another supported method.

Conjur verifies the presented credentials against its internal database. If the credentials are valid, Conjur generates and returns a short-lived access token to the requester.

The requester includes the access token with every subsequent request to access Conjur resources. This allows Conjur to identify the requester and authorize their access to specific secrets and functionalities based on configured policies.

Finally, each request is evaluated against the Conjur RBAC (Role-Based Access Control) rules defined in its policy. These rules determine which users and roles have access to specific resources and what actions they can perform. Only

requests that comply with these rules are granted access.

SECRET-SEN Practice Test SECRET-SEN Exam Questions SECRET-SEN Braindumps