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

During the configuration of Conjur, what is a possible deployment scenario?

A. The Leader and Followers are deployed outside of a Kubernetes environment; Slandbys can run inside a Kubernetes environment.

B. The Conjur Leader cluster is deployed outside of a Kubernetes environment; Followers can run inside or outside the environment.

C. The Leader cluster is deployed outside a Kubernetes environment; Followers and Standbys can run inside or outside the environment.

D. The Conjur Leader cluster and Followers are deployed inside a Kubernetes environment.

Correct Answer: C

Conjur is a secrets management solution that securely stores and manages secrets and credentials used by applications, DevOps tools, and other systems. Conjur can be deployed in different scenarios, depending on the needs and preferences of the organization. One of the possible deployment scenarios is to deploy the Leader cluster outside a Kubernetes environment, and the Followers and Standbys inside or outside the environment. The Leader cluster is the primary node that handles all write operations and coordinates the replication of data to the Follower and Standby nodes. The Leader cluster consists of one active Leader node and one or more Standby nodes that can be promoted to Leader in case of a failure. The Leader cluster can be deployed outside a Kubernetes environment, such as on a virtual machine or a physical server, using Docker or other installation methods. This can provide more control and flexibility over the configuration and management of the Leader cluster, as well as better performance and security. The Follower and Standby nodes are read-only replicas of the Leader node that can serve requests from clients and applications that need to retrieve secrets or perform other read- only operations. The Follower and Standby nodes can be deployed inside or outside a Kubernetes environment, depending on the use case and the availability requirements. For example, if the clients and applications are running inside a Kubernetes cluster, it may be convenient and efficient to deploy the Follower and Standby nodes inside the same cluster, using Helm charts or other methods. This can reduce the network latency and complexity, and leverage the Kubernetes features such as service discovery, load balancing, and health checks. Alternatively, if the clients and applications are running outside a Kubernetes cluster, or if there is a need to distribute the Follower and Standby nodes across different regions or availability zones, it may be preferable to deploy the Follower and Standby nodes outside the Kubernetes cluster, using Docker or other methods. This can provide more scalability and resiliency, and avoid the dependency on the Kubernetes cluster. References: Conjur Deployment Scenarios; Conjur Cluster Installation; Conjur Kubernetes Integration

QUESTION 2

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 3

Followers are replications of the Leader configured for which purpose?

A. synchronous replication to ensure that there is always an up-to-date database

B. asynchronous replication from the Leader which allows secret reads at scale

C. asynchronous replication from the Leader with read/write operations capability

D. synchronous replication to ensure high availability

Correct Answer: B

Followers are read-only replicas of the Leader that perform asynchronous replication from the Leader. This means that they receive updates from the Leader periodically, but not in real time. Followers are designed to handle all types of read requests from workloads and applications, such as authentication, permission checks, and secret fetches. Followers can scale horizontally to support a large number of concurrent requests and reduce the load on the Leader. Followers also provide high availability and disaster recovery by serving as backup nodes in case of Leader failure or network partition. References: Set up Follower, Deploy the Conjur Follower, Follower architecture

QUESTION 4

In the event of a failover of the Vault server from the primary to the DR, which configuration option ensures that a CP will continue being able to refresh its cache?

A. Add the DR Vault IP address to the "Address" parameter in the file main_appprovider.conf. . found in the AppProviderConf safe.

B. Add the IP address of the DR vault to the "Address" parameter in the file Vault.ini.file on the machine on which the CP is installed.

C. In the Password Vault Web Access UI, add the IP address of the DR Vault in the Disaster Recovery section under Applications > Options.

D. In the Conjur UI, add the IP address of the DR Vault in the Disaster Recovery section under Cluster Config > Credential Provider > Options.

Correct Answer: B

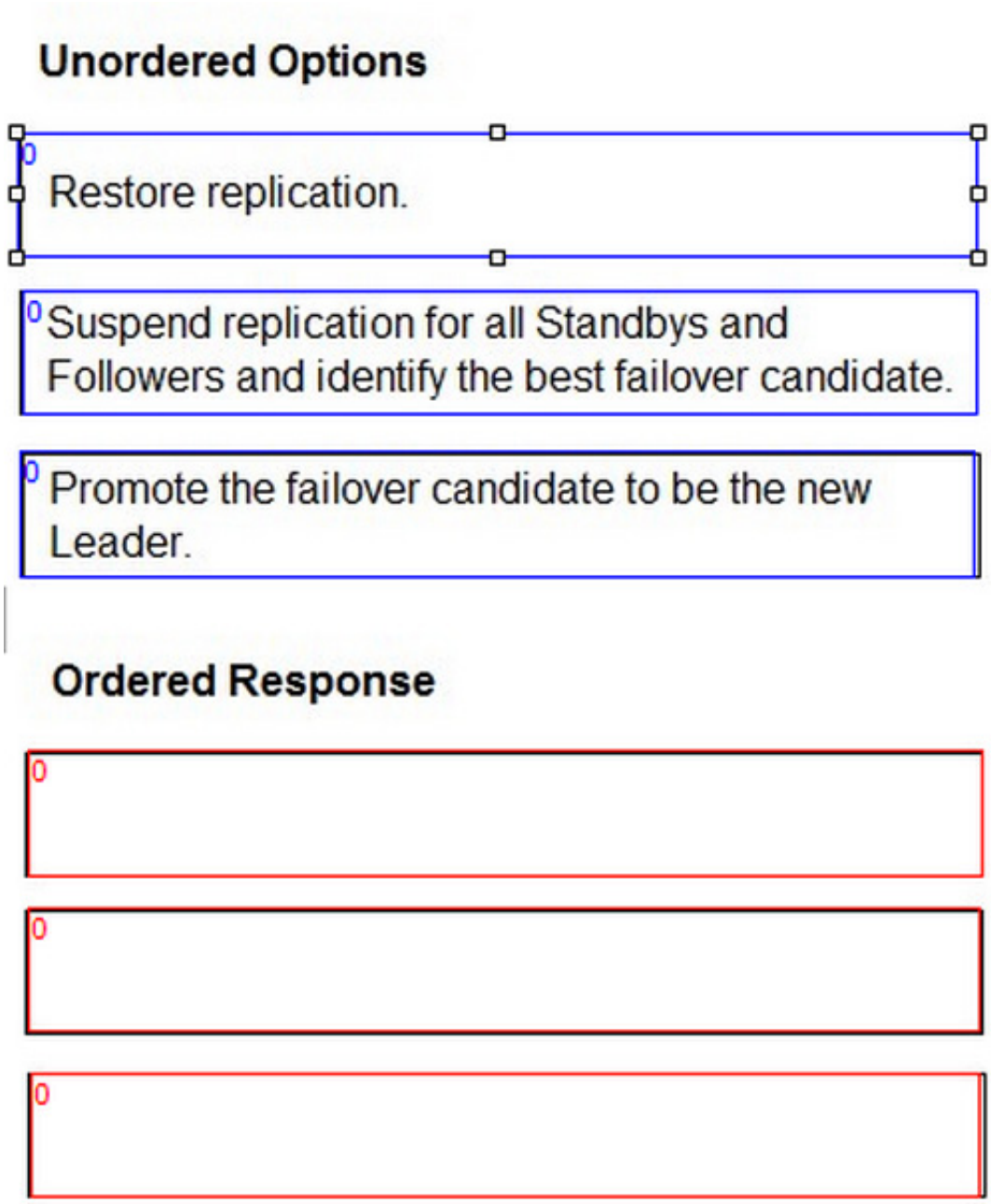
This is the correct answer because the Vault.ini file on the CP machine contains the configuration settings for the CP to connect to the Vault server. The Address parameter specifies the IP address or hostname of the Vault server that the CP will use to communicate with the Vault. In the event of a failover of the Vault server from the primary to the DR, the CP needs to update the Address parameter with the IP address of the DR Vault server in order to continue being able to refresh its cache. The cache is a local storage of credentials that the CP retrieves from the Vault and provides to the applications. The cache is refreshed periodically based on the RefreshInterval parameter in the Vault.ini file. 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 ensure that the CP will continue being able to refresh its cache in the event of a failover of the Vault server from the primary to the DR. Adding the DR Vault IP address to the Address parameter in the main_appprovider.conf.. file in the AppProviderConf safe is not a valid option, as this file does not contain the Address parameter. The main_appprovider.conf file contains the configuration settings for the basic provider, such as the AppProviderVaultParmsFile, the AppProviderPort, and the AppProviderCacheMode. The Address parameter is only found in the Vault.ini file on the CP machine. In the Password Vault Web Access (PVWA) UI, adding the IP address of the DR Vault in the Disaster Recovery section under Applications > Options is not a valid option, as this section does not exist in the PVWA UI. The PVWA UI does not have a Disaster Recovery section under Applications > Options. The PVWA UI has a Disaster Recovery section under Administration > Options, but this section is used to configure the DR Vault settings, such as the DR Vault IP address, the DR Vault user, and the DR Vault password. These settings are not related to the CP configuration or cache refresh. In the Conjur UI, adding the IP address of the DR Vault in the Disaster Recovery section under Cluster Config > Credential Provider > Options is not a valid option, as this section does not exist in the Conjur UI. The Conjur UI does not have a Cluster Config, Credential Provider, or Options 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. These settings are not related to the CP configuration or cache refresh.

QUESTION 5

DRAG DROP

Arrange the manual failover configuration steps in the correct sequence.

Select and Place:



Correct Answer:

In the event of a Leader failure, you can perform a manual failover to promote one of the Standbys to be the new Leader. The manual failover process consists of the following steps:

Suspend replication for all Standbys and Followers and identify the best failover candidate. This step ensures that no data is lost or corrupted during the failover process. The best failover candidate is the Standby with the most advanced

replication timeline, which means it has the most up-to-date data from the Leader. Promote the failover candidate to be the new Leader. This step changes the role of the failover candidate from a Standby to a Leader, and updates its

configuration accordingly. The new Leader can now accept write requests from clients and replicate data to other nodes.

Restore replication. This step re-establishes the replication connections between the new Leader and the other nodes, and rebases the replication of the other Standbys and Followers to the new Leader. This ensures that all nodes have the

same data and are in sync with the new Leader.

References: The manual failover configuration steps are explained in detail in the Configure Manual Failover section of the CyberArk Conjur Enterprise documentation. The image in the question is taken from the same source.

QUESTION 6

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

QUESTION 7

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 8

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 9

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

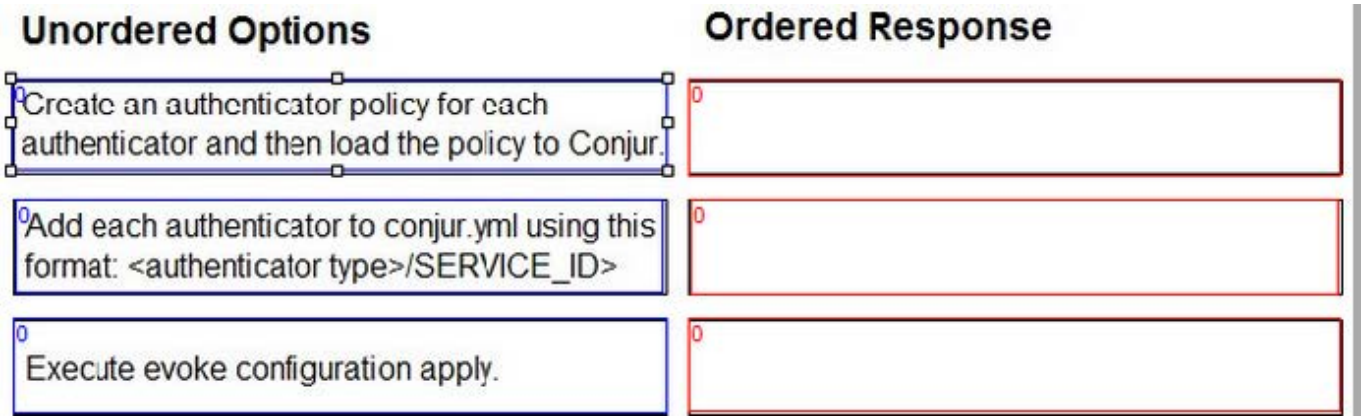
According to the CyberArk Sentry Secrets Manager documentation, JWT- based authentication is the recommended method for authenticating Kubernetes pods with Conjur. JWT-based authentication uses JSON Web Tokens (JWTs) that are issued by the Kubernetes API server and signed by its private key. The JWTs 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 10

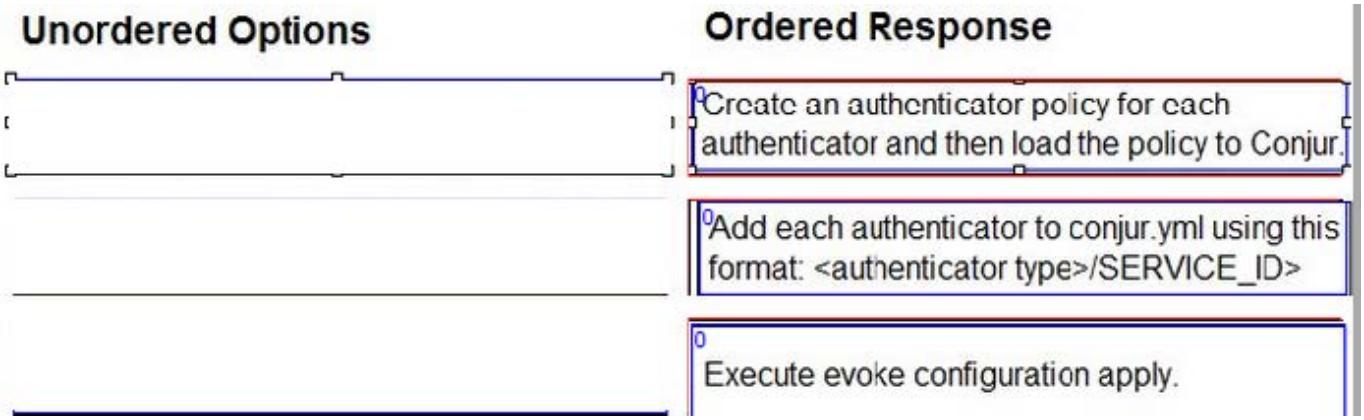
DRAG DROP

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.