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

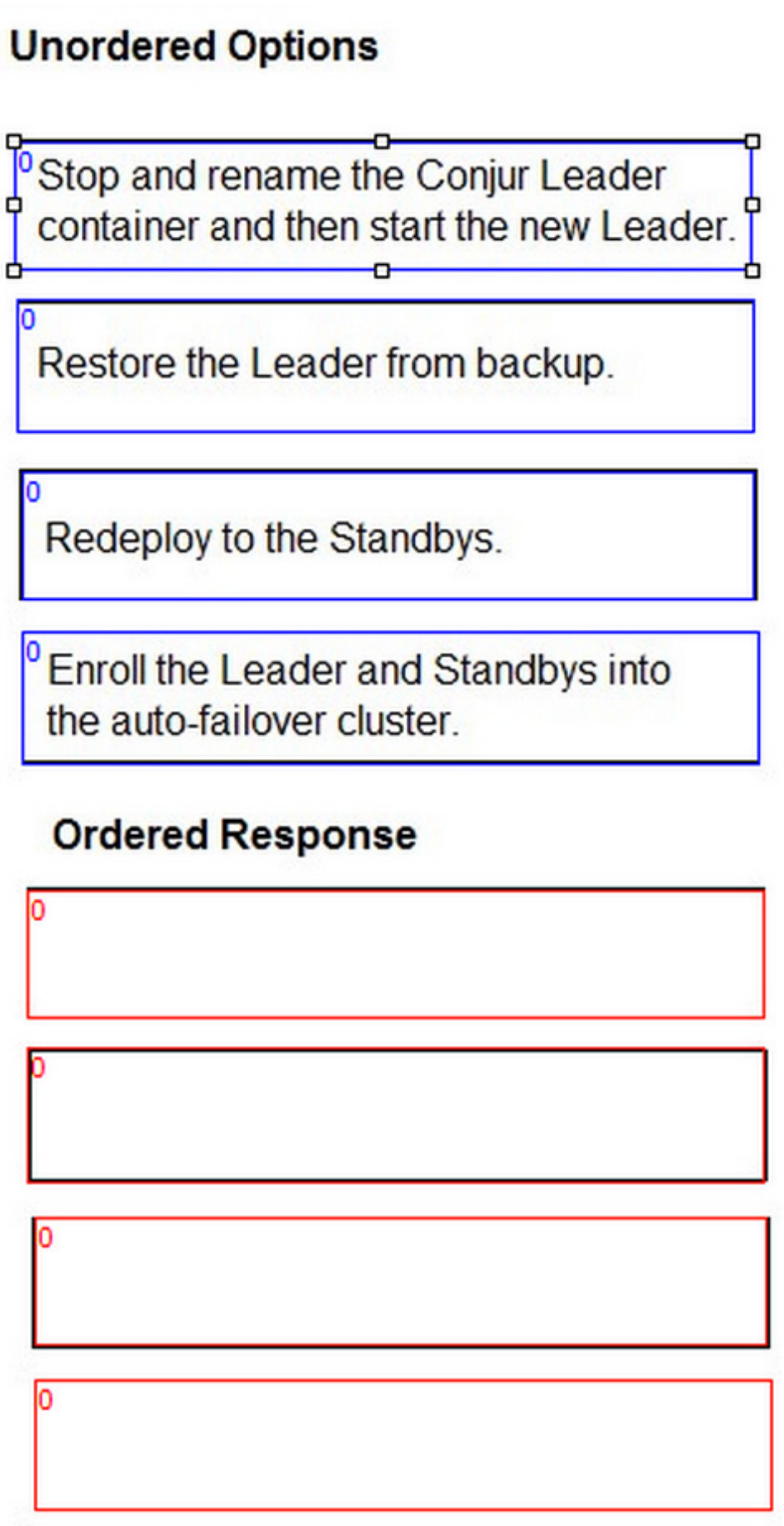
QUESTION 1

DRAG DROP

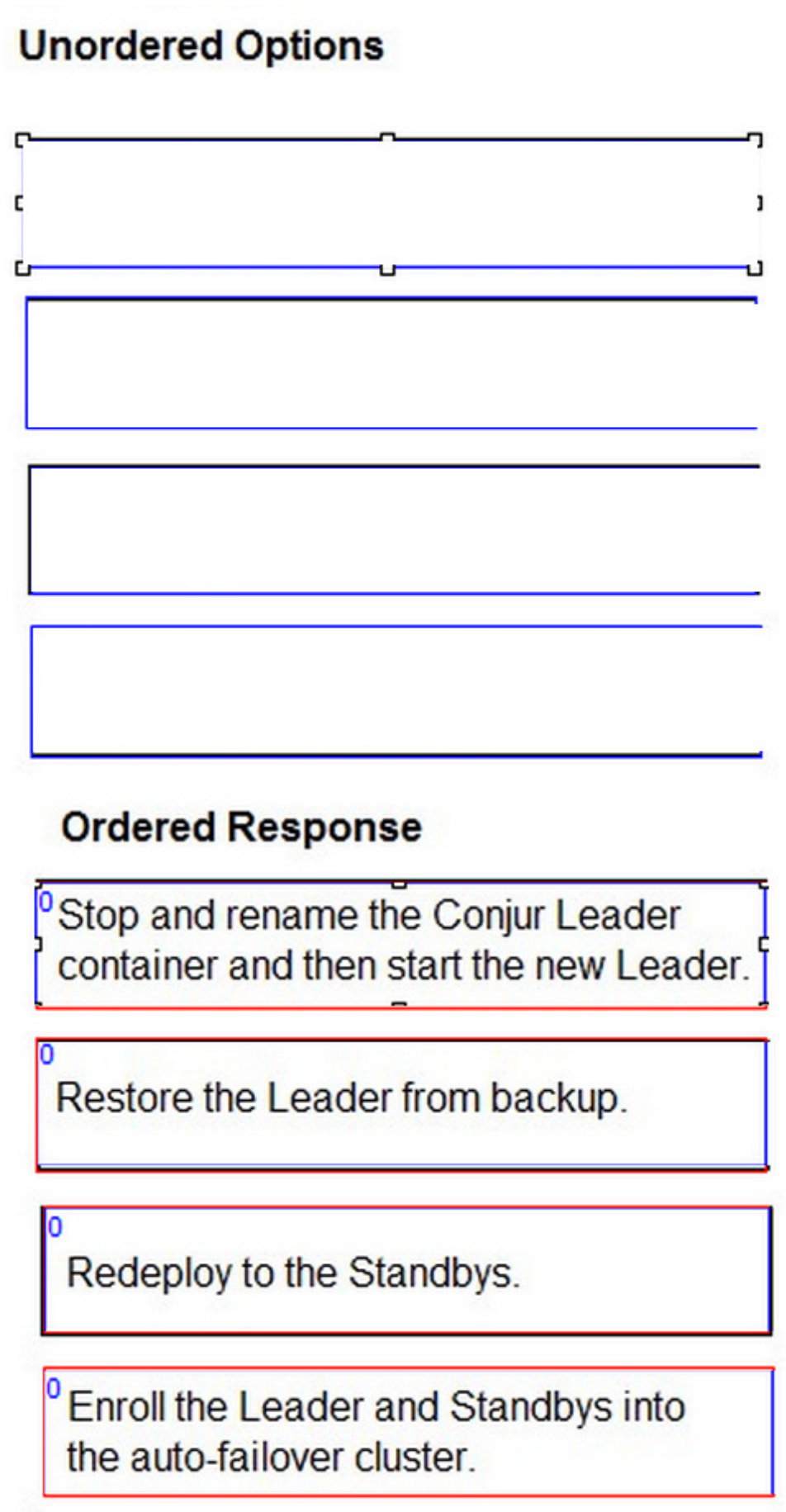
You are upgrading an HA Conjur cluster consisting of 1x Leader, 2x Standbys and 1x Follower. You stopped replication on the Standbys and Followers and took a backup of the Leader.

Arrange the steps to accomplish this in the correct sequence.

Select and Place:


Unordered Options
Stop and rename the Conjur Leader container and then start the new Leader.
Restore the Leader from backup.
Redeploy to the Standbys.
Enroll the Leader and Standbys into the auto-failover cluster.
Ordered Response

Correct Answer:


Unordered Options
Ordered Response
0
Stop and rename the Conjur Leader container and then start the new Leader.
0
Restore the Leader from backup.
0
Redeploy to the Standbys.
0
Enroll the Leader and Standbys into the auto-failover cluster.

To upgrade an HA Conjur cluster, you need to follow these steps: Stop and rename the Conjur Leader container and then start the new Leader. This step ensures that you have a backup of the old Leader container in case something goes wrong with the upgrade. You also need to specify the hostname and master-altnames parameters when starting the new Leader container to match the load balancer and the cluster nodes. Restore the Leader from backup. This step restores the data and configuration from the old Leader to the new Leader. You need to use the evoke restore command with the backup file name and the account name as arguments. Redeploy to the Standbys. This step upgrades the Standbys to the same version as the Leader. You need to stop and rename the old Standby containers and then start the new Standby containers with the evoke configure standby command. You also need to specify the hostname of the Leader and the Standby as arguments. Enroll the Leader and Standbys into the auto-failover cluster. This step enables the auto-failover feature for the cluster, which allows the Standbys to automatically take over the role of the Leader in case of a failure. You need to use the evoke cluster enroll command on the Leader and the evoke cluster join command on the Standbys. You also need to provide the hostname and password of the Leader as arguments. References: You can find more information about the upgrade process in the following resources: Upgrade Conjur Configure the Conjur cluster Conjur architecture and deployment reference Breathe Easy with a Self-Healing Conjur Cluster

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

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

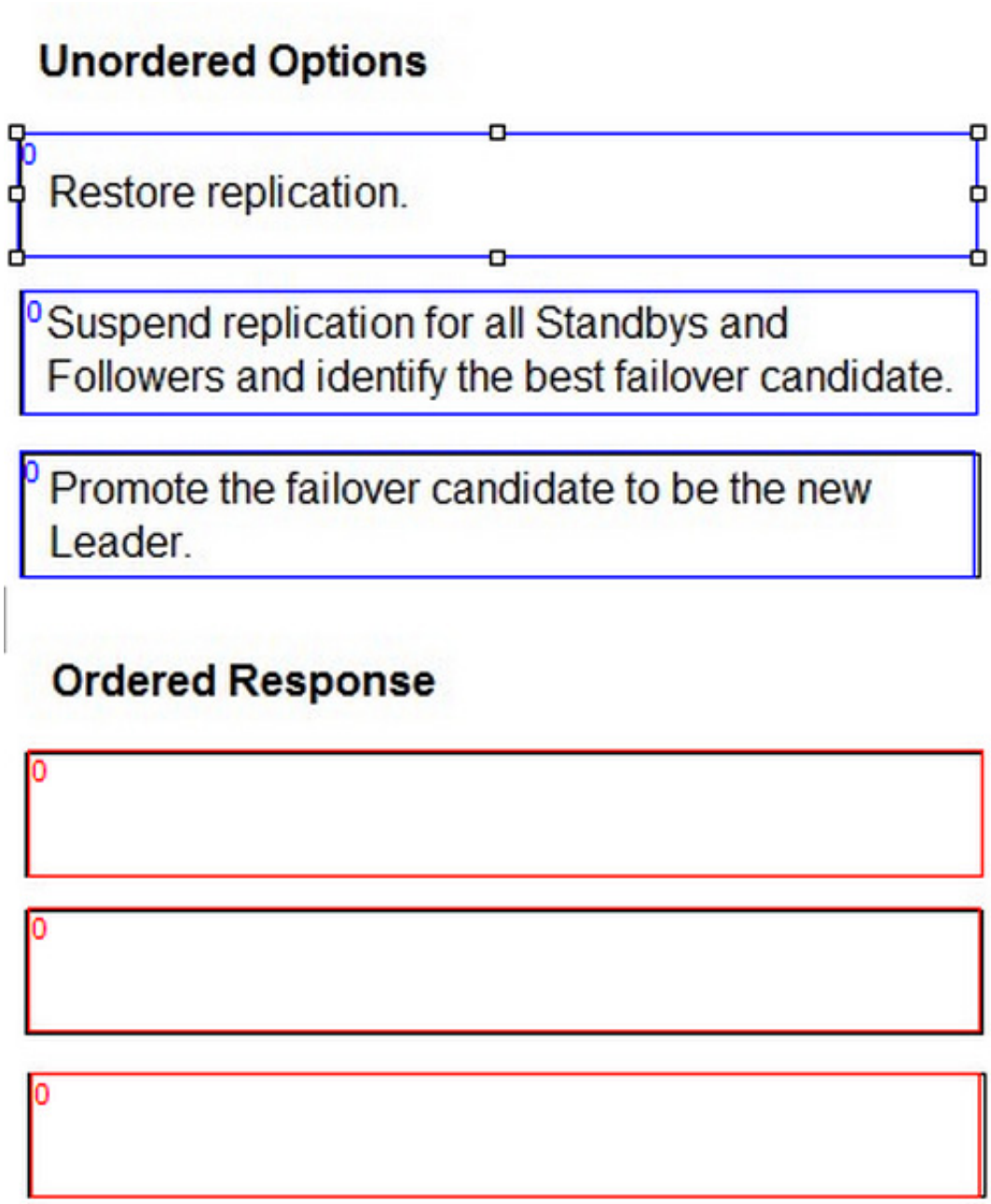
Followers are read-only replicas of the Leader that perform asynchronous replication from the Leader. This means that they receive updates from the Leader periodically, but not in real time. Followers are designed to handle all types of read requests from workloads and applications, such as authentication, 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

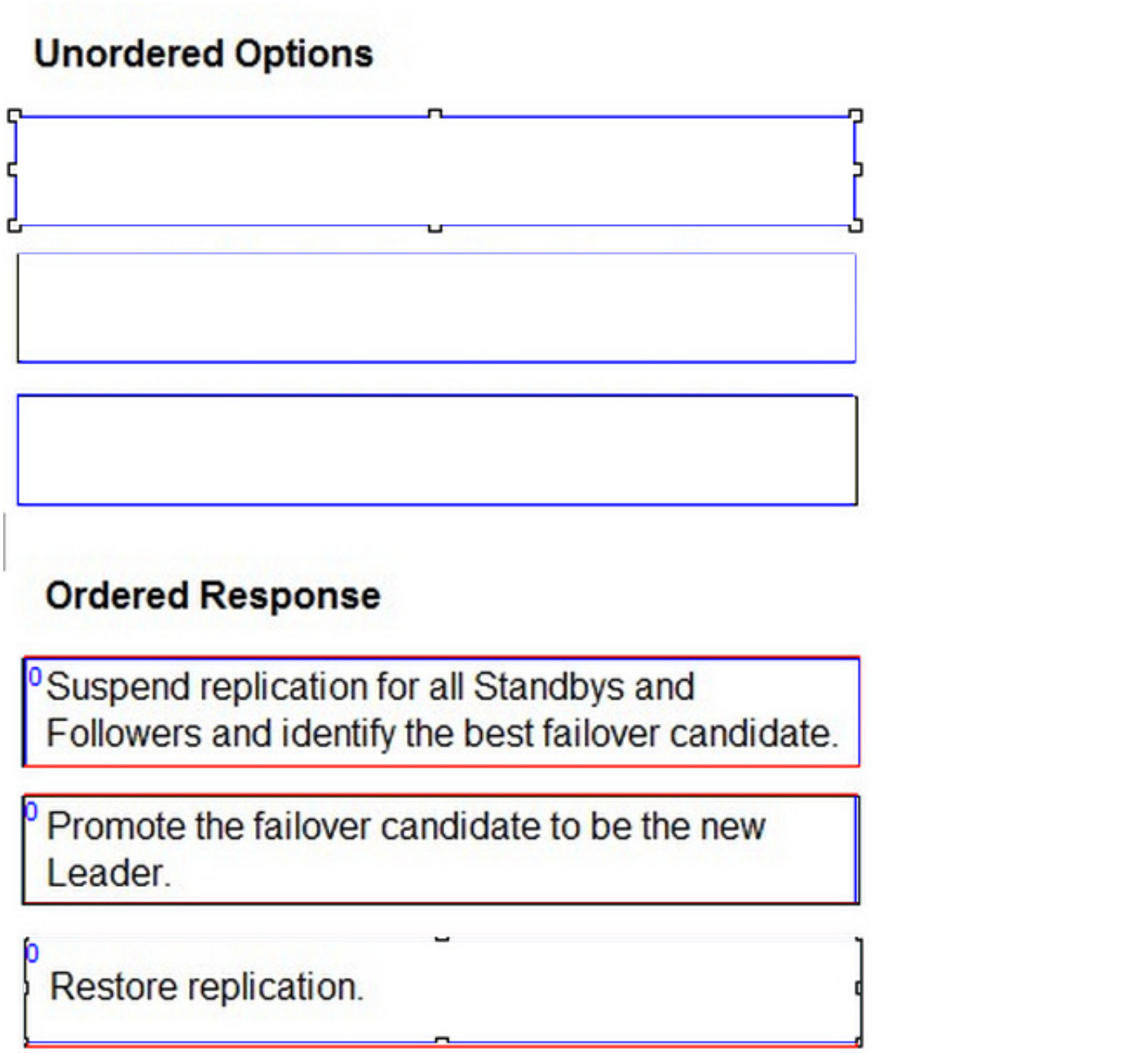
DRAG DROP

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 5

Which API endpoint can be used to discover secrets inside of Conjur?

A. Resources

B. Roles

C. Policies

D. WhoAmi

Correct Answer: A

Conjur is a secrets management solution that securely stores and manages secrets and credentials used by applications, DevOps tools, and other systems. Conjur provides a REST API that enables users to perform various operations on Conjur objects, such as secrets, policies, roles, and resources. The API endpoint for each Conjur object is composed of the base URL of the Conjur server, followed by the object type and identifier. For example, the API endpoint for a secret named db-password in the dev/my-app policy is: https:///secrets/dev/my-app/db-password To discover secrets inside of Conjur, the API endpoint that can be used is Resources. Resources are Conjur objects that have permissions and annotations associated with them, such as secrets, hosts, groups, and layers. The Resources API endpoint allows users to list, search, and filter resources based on various criteria, such as kind, owner, policy, and annotation. For example, the following API request will return a list of all secrets owned by the user alice: https:///resources?kind=variableandowner=user:alice The Resources API endpoint can help users to discover secrets inside of Conjur by providing information such as the name, ID, policy, owner, and annotations of each secret. Users can also use the Resources API endpoint to check the permissions and audit records of each secret, and to retrieve the secret value if they have the read permission. References: Conjur API; Resources API; Secrets API