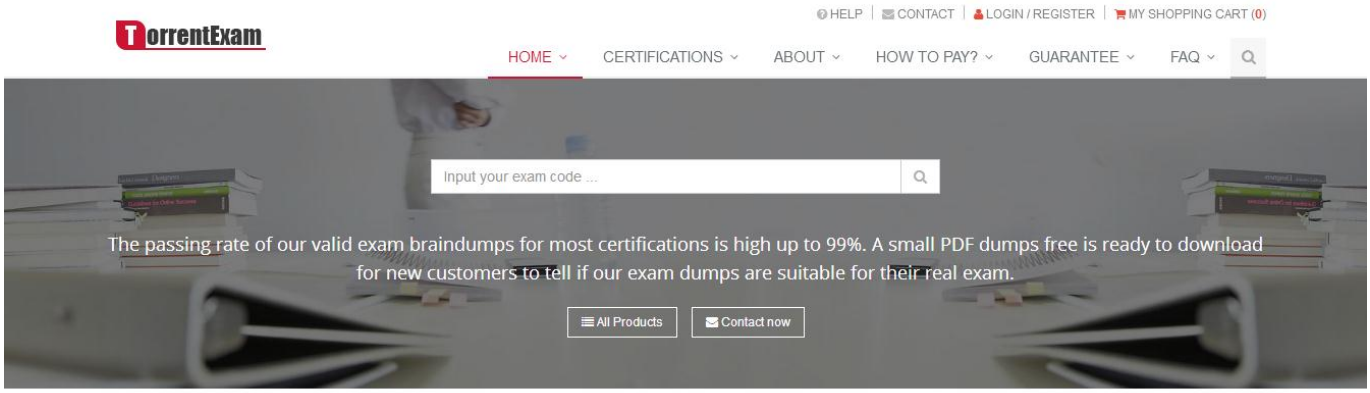
# TorrentExam




## Why Choose Us

### QUALITY AND VALUE

RealExamFree Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

### TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

### EASY TO PASS

If you prepare for the exams using our RealExamFree testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

### TRY BEFORE BUY

RealExamFree offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

## Customer Reviews

I wasted a lot of money and failed twice. Thanks to HPE0-J78 exam collection I pass now.

**Noel**

realexamfree is a reliable company. I pass exam at first shot. Many thanks

**Julie**

Pass BIMF.EN successfully. Really good dumps. It saves me a lot of time. Wonderful!

**Ahern**

online test engine is very useful for me,because i could practice the C-TERP10-67 question dumps in my phone when i was waititng or on the bus even without internet,i could make the most of my time.Last week,i passed the C-TERP10-67. so i want to share the realexamfree with you guys,hope you will get a good result in test.

**Carl**

http://www.torrentexam.com

Best Exam Bootcamp & Excellent VCE Torrent & Satisfying Dumps Torrent

**Exam** : **SECRET-SEN**

**Title** : CyberArk Sentry - Secrets Manager

**Vendor** : CyberArk

**Version** : DEMO

**NO.1** 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.
***Answer:*** A
Explanation
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

**NO.2** A customer wants to minimize the Kubernetes application code developers must change to adopt Conjur for secrets access.
Which solutions can meet this requirement? (Choose two.)

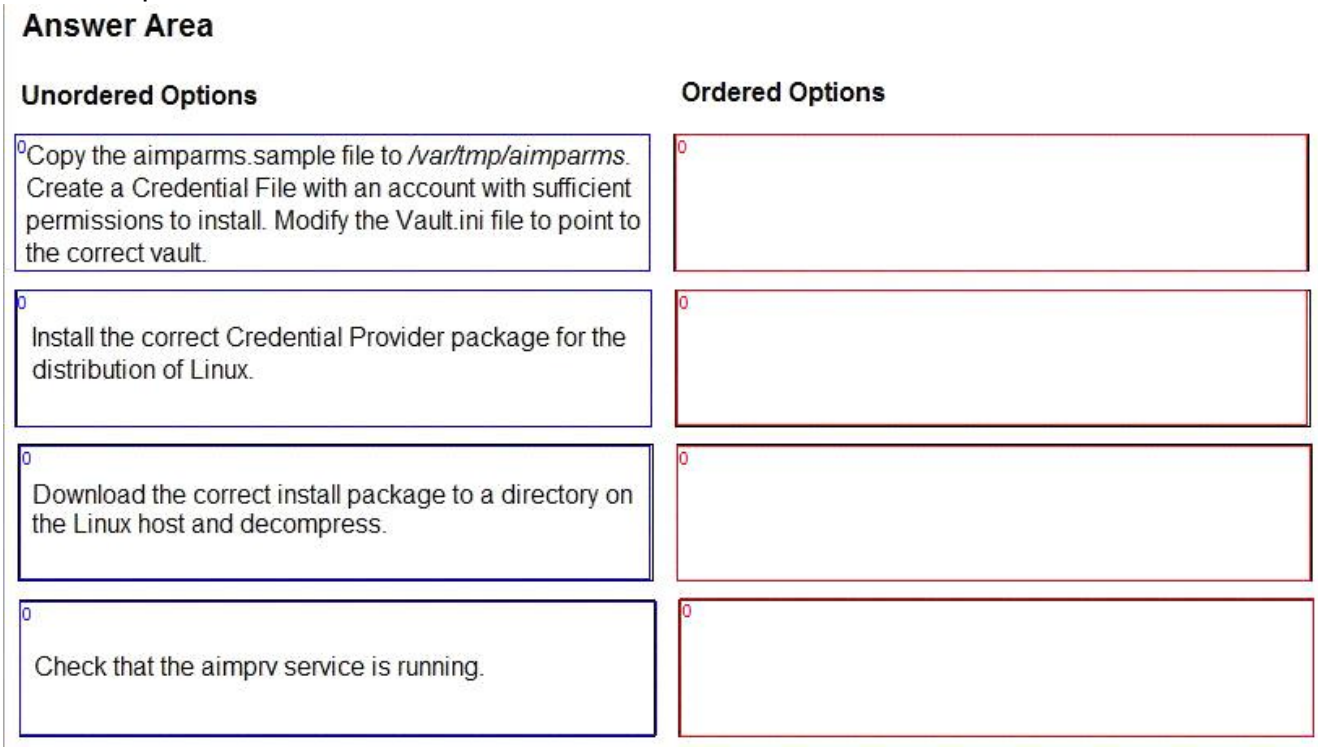
**A.** CPM Push-to-File
**B.** Secrets Provider
**C.** authn-Azure
**D.** Secretless
**E.** Application Server Credential Provider
***Answer:*** B D
Explanation
Secrets Provider and Secretless are two solutions that can minimize the Kubernetes application code changes required to adopt Conjur for secrets access. Secrets Provider is a Kubernetes Job or Deployment that runs as an init container or application container alongside the application pod. It retrieves secrets from Conjur and writes them to one or more files in a shared, mounted volume. The application can then consume the secrets from the files without any code changes, as reading local files is a common and platform-agnostic method. Secretless is a sidecar proxy that runs as a separate container in the same pod as the application. It intercepts the application's requests to protected resources, such as databases or web services, and injects the secrets from Conjur into the requests. The application does not need to handle any secrets in its code, as Secretless handles the authentication and authorization for it. References: CyberArk Secrets Provider for Kubernetes, Secretless Broker

**NO.3** 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.
***Answer:*** A
Explanation
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

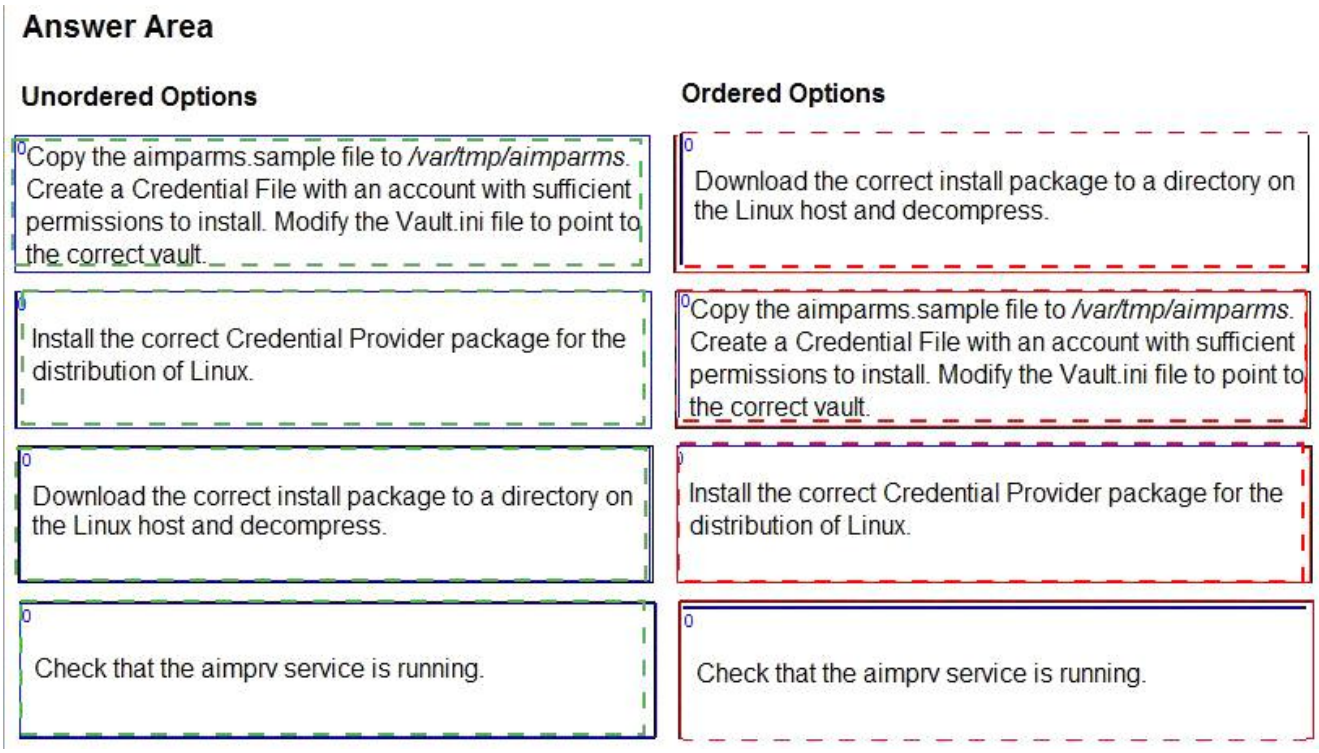
**NO.4** When using the Seed Fetcher to deploy Kubernetes Followers, an error occurs in the Seed Fetcher container.
You check the logs and discover that although the Seed Fetcher was able to authenticate, it shows a 500 error in the log and does not successfully retrieve a seed file. What is the cause?

**A.** The certificate based on the Follower DNS name is not present on the Leader.
**B.** The host you configured does not have access to see the certificates.
**C.** The synchronizer service crashed and needs to be restarted.
**D.** The Leader does not have the authenticator webservice enabled.
***Answer:*** A
Explanation
The cause of the issue is A. The certificate based on the Follower DNS name is not present on the Leader. This means that the Leader does not have a certificate file that matches the Follower DNS name used in the seed request, and therefore cannot generate a valid seed file for the Follower. This results in a 500 error in the Seed Fetcher container log. To resolve the issue, you need to import a certificate with the Follower DNS name as the subject alt name on the Leader, and create a copy of the certificate file with a name that matches the Follower DNS name used in the seed request1.

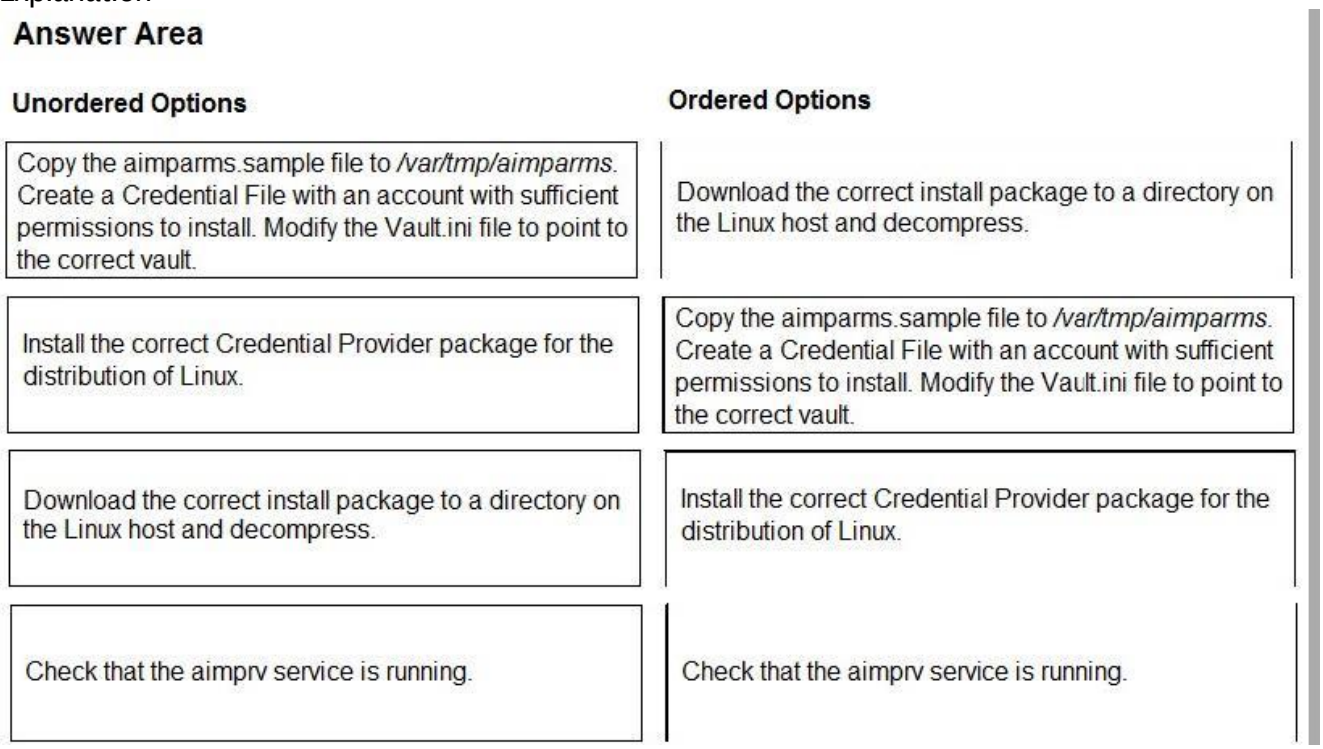
**NO.5** You are installing a Credential Provider on a Linux host. Arrange the installation steps in the correct sequence.




***Answer:***




Explanation




The correct sequence of installation steps for a Credential Provider on a Linux host is as follows:
Download the correct install package to a directory on the Linux host and decompress1.
Copy the aimparms.sample file to /var/tmp/aimparms. Create a Credential File with an account with sufficient permissions to install. Modify the Vault.ini file to point to the correct vault2.
Install the correct Credential Provider package for the distribution of Linux using the command: rpm -ivh CARKaim-<version+build number>.<distribution>.rpm2.
Check that the aimprv service is running using the command: service aimprv status2.
References: 1: Download the Credential Provider 2: Install Credential Provider on Linux / AIX

**NO.6** You are setting up the Secrets Provider for Kubernetes to support rotation with Push-to-File mode.
Which deployment option should be used?
**A.** Init container
**B.** Application container
**C.** Sidecar
**D.** Service Broker
***Answer:*** C
Explanation
According to the CyberArk Sentry Secrets Manager documentation, the Secrets Provider for Kubernetes can be deployed as an init container or a sidecar in Push-to-File mode. In Push-to-File mode, the Secrets Provider pushes Conjur secrets to one or more secrets files in a shared volume in the same Pod as the application container. The application container can then consume the secrets files from the shared volume. The deployment option that should be used to support rotation with Push-to-File mode is the sidecar, because the sidecar can run continuously and check for updates to the secrets in Conjur. If changes are detected, the sidecar can update the secrets files in the shared volume. The init container, on the other hand, runs to completion and does not support rotation. The application container and the service broker are not valid deployment options for the Secrets Provider for Kubernetes in Push-to-File mode. References: 1: Secrets Provider - Init container/Sidecar - Push-to-File mode 2: Secrets Provider - init container/sidecar - Push-to-File mode