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

What is the most maintenance-free way to ensure a Conjur host\\'s access reflects any changes made to accounts in a safe in the CyberArk vault?

A. Write an automation script to update and load the host\\'s policy using PATCH/update.

B. Use yami anchor [and] and wildcard (*) syntax to maintain its list of permission grants.

C. Grant the consumers group/role created by the Synchronizer for the Safe to the host.

D. Use PVWA to add the Conjur host ID as a member of the Safe.

Correct Answer: C

The most maintenance-free way to ensure a Conjur host\\'s access reflects any changes made to accounts in a safe in the CyberArk vault is to grant the consumers group/role created by the Synchronizer for the Safe to the host. This means

that the host will inherit the read and execute permissions on all the secrets in the Safe from the consumers group/role, and will automatically get access to any new or updated secrets in the Safe without requiring any manual intervention or

policy changes. The consumers group/role is created by the Vault Conjur Synchronizer, which is a service that synchronizes secrets between the CyberArk vault and Conjur. The Synchronizer creates a policy branch for each Safe in Conjur,

and assigns the consumers group/role to have read and execute permissions on all the secrets in the Safe. The Synchronizer also creates a delegation policy for each Safe, which allows the Safe admins to grant permissions to other users,

hosts, groups, or layers12.

The other options are not the most maintenance-free ways to ensure a Conjur host\\'s access reflects any changes made to accounts in a safe in the CyberArk vault. Writing an automation script to update and load the host\\'s policy using

PATCH/update may work, but it requires additional effort and maintenance to ensure the script is always running and up to date with the changes in the Safe. Using yami anchor [and] and wildcard (*) syntax to maintain its list of permission

grants may simplify the policy writing, but it still requires manual editing and loading of the policy whenever a new secret is added or removed from the Safe. Using PVWA to add the Conjur host ID as a member of the Safe may not be

possible or advisable, as the PVWA is designed for managing human users and not Conjur hosts, and it may not have the necessary integration or authorization to do so3.

References:

Vault Conjur Synchronizer 1, Synchronizer Policy Structure Grant permissions on secrets 2, Grant role permissions on all secrets in a Safe Privileged Access Manager - Self-Hosted 3, Privileged Web Access (PVWA)

QUESTION 2

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

QUESTION 3

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 4

What does "Line of business (LOB)" represent?

A. a business group requiring access to secrets from the Vault/Privilege Claud to facilitate syncing accounts to Conjur

B. the services that Conjur offers and typically refers to a group of application identities in Conjur

C. a business group that meets a certain set of Conjur policies for entitlements and policy management

D. the services that Conjur offers and typically refers to the list of configured and enabled authenticators in Conjur

Correct Answer: B

Line of business (LOB) is a term used by CyberArk Secrets Manager to describe the services that Conjur offers and typically refers to a group of application identities in Conjur. A LOB can be defined by a Conjur policy that grants permissions and access to secrets for a specific set of applications. For example, a LOB can represent a business unit, a project, a product, or a team within an organization. A LOB can also have sub-LOBs that inherit the permissions and secrets from the parent LOB, but can also have their own specific policies and secrets. A LOB can help organize and manage secrets for different applications in a hierarchical and scalable way. References: CyberArk Secrets Manager - Line of Business; CyberArk Secrets Manager - Policy Management; CyberArk Secrets Manager - Application Identity Management

QUESTION 5

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

Correct Answer: C

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