SECRET-SEN$^{Q\&As}$

CyberArk Sentry - Secrets Manager

Pass CyberArk SECRET-SEN Exam with 100% Guarantee

QUESTION 1

When installing the Vault Conjur Synchronizer, you see this error:

Forbidden

Logon Token is Empty ?Cannot logon

Unauthorized

What must you ensure to remediate the issue?

A. This admin user must not be logged in to other sessions during the Vault Conjur Synchronizer installation process.

B. You specified the correct url for Conjur and it is listed as a SAN on that url\\'s certificate.

C. You correctly URI encoded the url in the installation script.

D. You ran powershell as Administrator and there is sufficient space on the server on which you are running the installation.

Correct Answer: A

This error occurs when the Vault Conjur Synchronizer installation script tries to log in to the Vault using the admin user credentials, but the admin user is already logged in to other sessions. The Vault has a limit on the number of concurrent sessions per user, and the default value is one. Therefore, the installation script fails to authenticate the admin user and returns the error message: Forbidden Logon Token is Empty - Cannot logon Unauthorized. To remediate the issue, the admin user must log out of any other sessions before running the installation script, or increase the limit on the number of concurrent sessions per user in the Vault configuration file12. References: = Troubleshoot CyberArk Vault Synchronizer 1, Error: Forbidden Logon Token is Empty - Cannot logon Unauthorized Vault.ini File Parameters 2, ConcurrentSessionsPerUser

QUESTION 2

What is the correct process to upgrade the CCP Web Service?

A. Run "sudo yum update aimprv" from the CLI.

B. Double-click the Credential Provider installer executable and select upgrade.

C. Double-click the AimWebService.msi and select upgrade.

D. Uninstall and reinstall the CCP Web Service.

Correct Answer: D

The correct process to upgrade the CCP Web Service is D. Uninstall and reinstall the CCP Web Service. The CCP Web Service is a component of the CyberArk Central Credential Provider (CCP) that enables applications to retrieve secrets from the CyberArk Vault using REST API calls. To upgrade the CCP Web Service, you need to first uninstall the existing CCP Web Service from the Windows Server Manager or the Control Panel, and then reinstall the CCP Web Service using the latest installation package from the CyberArk website. The installation package contains both the Credential Provider and the CCP Web Service components, and you need to run the AimWebService.msi file to install the CCP Web Service. You also need to make sure that the CCP Web Service has the correct configuration and permissions, and that the CyberArk CRL (Certificate Revocation List) is open from the CCP server. The other options are not correct processes to upgrade the CCP Web Service. Running "sudo yum update aimprv" from the CLI is a command to update the Credential Provider on Linux, not the CCP Web Service on Windows. Double-clicking the Credential Provider installer executable and selecting upgrade is a process to upgrade the Credential Provider on Windows, not the CCP Web Service. Double-clicking the AimWebService.msi and selecting upgrade is not a valid option, as the CCP Web Service does not support an upgrade option, and you need to uninstall it first before reinstalling it. References: Upgrade the Central Credential Provider (CCP) - CyberArk, Section "Upgrade the Central Credential Provider (CCP)" Central Credential Provider web service configuration - CyberArk, Section "Central Credential Provider web service configuration"

QUESTION 3

An application owner reports that their application is suddenly receiving an incorrect password. CPM logs show the password was recently changed, but the value currently being retrieved by the application is a different value. The Vault Conjur Synchronizer service is running.

What is the most likely cause of this issue?

A. The Vault Conjur Synchronizer is not configured with the DR Vault IP address and there has been a failover event.

B. Dual Accounts are in use, but after the CPM changed the password for the Inactive account, it accidentally updated the password for the Active account instead.

C. The CPM is writing password changes to the Primary Vault while the Vault Conjur Synchronizer is configured to replicate from the DR Vault.

D. The application has been configured to retrieve the wrong password.

Correct Answer: C

This is the most likely cause of this issue because it creates a discrepancy between the passwords stored in the Primary Vault and the DR Vault, which affects the Vault Conjur Synchronizer service (Synchronizer) and the application. The

Synchronizer is a service that synchronizes secrets from the CyberArk Vault to the Conjur database. The application is a client that retrieves secrets from the Conjur database using the Conjur REST API. The CPM is a component that

manages the lifecycle of the passwords stored in the CyberArk Vault, such as changing, verifying, and reconciling them. If the CPM is writing password changes to the Primary Vault while the Synchronizer is configured to replicate from the

DR Vault, the following scenario may occur:

The CPM changes the password for an account in the Primary Vault and updates the password value in the Vault database.

The Synchronizer does not detect the password change in the DR Vault, as the DR Vault database has not been updated yet with the new password value. The Synchronizer does not sync the new password value to the Conjur database, as

it assumes that the password value in the DR Vault database is the latest and correct one.

The application requests the password value from the Conjur database and receives the old password value, which is different from the new password value in the Primary Vault database.

The application tries to use the old password value to access the target platform or device and fails, as the target platform or device expects the new password value. This answer is based on the CyberArk Secrets Manager documentation1

and the CyberArk Secrets Manager training course2.

QUESTION 4

What is a main advantage of using dual accounts in password management?

A. Since passwords are cached for both rotation accounts, it ensures the password for an application will not be changed, reducing the amount of blackout dates when a password expires.

B. It ensures passwords are rotated every 90 days, which respects the expected downtime for a system, database, or application

C. It ensures no delays are incurred when the application needs credentials because a password that is currently used by an application will never be changed

D. Since there are two active accounts, it doubles the probability that a system, database, or application will successfully authenticate.

Correct Answer: C

Dual accounts is a password management method that uses two accounts with identical privileges to access a system, database, or application. One account is active and the other is inactive at any given time. The active account remains untouched during password rotation, while the inactive account has its password changed after a grace period. This way, the application can always use the active account without experiencing any delays or errors due to password expiration or change. The advantage of using dual accounts is that it ensures business continuity and seamless access to the target resource, especially for high load and critical applications. References: Manage Dual Accounts, Configure dual accounts

QUESTION 5

A customer wants to ensure applications can retrieve secrets from Conjur in three different data centers if the Conjur Leader becomes unavailable. Conjur Followers are already deployed in each of these data centers.

How should you architect the solution to support this requirement?

A. No changes are required.

B. Deploy a Standby in each data center that can be promoted to the role of Leader.

C. Extend the auto failover cluster to include Standby?in each data center and allow for automatic recovery should the Leader become unavailable.

D. Deploy a CP provider on the Follower server to provide offline caching capabilities for the Follower.

Correct Answer: C

Conjur Followers are read-only replicas of the Leader that can serve client requests for authentication, authorization, and secret retrieval. However, Followers cannot perform write operations, such as creating or updating secrets, policies, or roles. If the Leader becomes unavailable, the Followers will not be able to sync with the latest data and will eventually become stale. To ensure high availability and data consistency, the customer should extend the auto-failover cluster to include Standbys in each data center. Standbys are also replicas of the Leader, but they can participate in replication and promotion. One Standby is configured for synchronous replication, which means it receives the same updates as the Leader at the same time. The other Standbys are configured for asynchronous replication, which means they receive updates from the Leader periodically, but not in real time. In case of Leader failure, the synchronous Standby can be automatically promoted to become the new Leader, and one of the asynchronous Standbys can become the new synchronous Standby. This way, the customer can ensure that there is always an up-to-date Leader that can serve write requests and sync with the Followers in different data centers. References: Set up Follower, Set up auto-failover cluster, Conjur architecture and deployment reference