CyberArk Integration

CyberArk - Status Report

Doküman No	PRO-KL001-G-04
Versiyon	0.4
Yayın Tarihi	01.12.2024

Revision History

Date	Description	Prepared by	Approved by	Version
1 November 2024	First draft	Murat YILDIZ	-	0.1

Table of Contents

Revision History 3
Introduction 4
1. What is CyberArk? 6
1.1. Products That Can Be Used with HSM in CyberArk 6
2. What is CyberArk EPV (Enterprise Password Vault)? 7
3. CyberArk EPV HSM Integration 7
REFERENCES 12

1. What is CyberArk?

CyberArk is a cybersecurity company primarily focused on providing privileged access security solutions. The company's mission is to help organizations securely manage access to critical systems, data, and privileged accounts.

CyberArk's flagship product is the CyberArk Privileged Access Security (PAS) Suite. This solution offers capabilities to secure, monitor, and manage privileged access accounts, identities, and passwords. Privileged access accounts are those with special permissions within corporate networks and systems, granting access to sensitive data or critical systems. By protecting these accounts, CyberArk aims to prevent unauthorized access, mitigate data breaches, and reduce security risks.

While the CyberArk PAS Suite focuses on privileged access management, its other products cover areas such as privileged session management, password management, session recording, identity and access management, and more. These products enhance defenses against cyberattacks and ensure compliance by securing privileged access.

Overall, CyberArk's solutions are designed to help organizations achieve privileged access security, prevent data breaches, and reduce security risks. The company is a leading cybersecurity provider widely used by major organizations worldwide.

1.1. Products That Can Be Used with HSM in CyberArk

CyberArk provides HSM (Hardware Security Module) integration across various products. Below are some CyberArk products that support HSM integration:

1. **CyberArk Enterprise Password Vault (EPV):**
   EPV is a solution designed for the centralized storage, management, and control of access to sensitive credentials. With HSM integration, EPV can support HSM devices for key management and data security.
2. **CyberArk Privileged Session Manager (PSM):**
   PSM is a solution used to secure, monitor, and manage critical privileged sessions. With HSM integration, PSM can securely store privileged session recordings and utilize HSM devices for key management.
3. **CyberArk Secrets Manager:**
   Secrets Manager is a solution designed to control and monitor privileged access for applications, servers, and databases. With HSM integration, Secrets Manager can use HSM devices to securely store and manage privileged access keys and credentials.

This list provides examples of CyberArk products that support HSM integration. CyberArk's product portfolio is continually updated with new features and capabilities. Therefore, it is important to refer to the latest CyberArk documentation and product guides for specific products or solutions where you plan to implement HSM integration.

2. What is CyberArk EPV (Enterprise Password Vault)?

CyberArk Enterprise Password Vault (EPV) is software developed by CyberArk Corporation, designed to centrally store and manage an organization's sensitive credentials (particularly passwords). EPV enhances security and access controls, enabling efficient management of identities and credentials.

The primary purpose of EPV is to ensure the protection of critical account credentials. This software can be used to store, encrypt, and manage passwords, certificates, API keys, and other sensitive information. By restricting access to these credentials to a limited number of authorized individuals, organizations can enhance the security of their information.

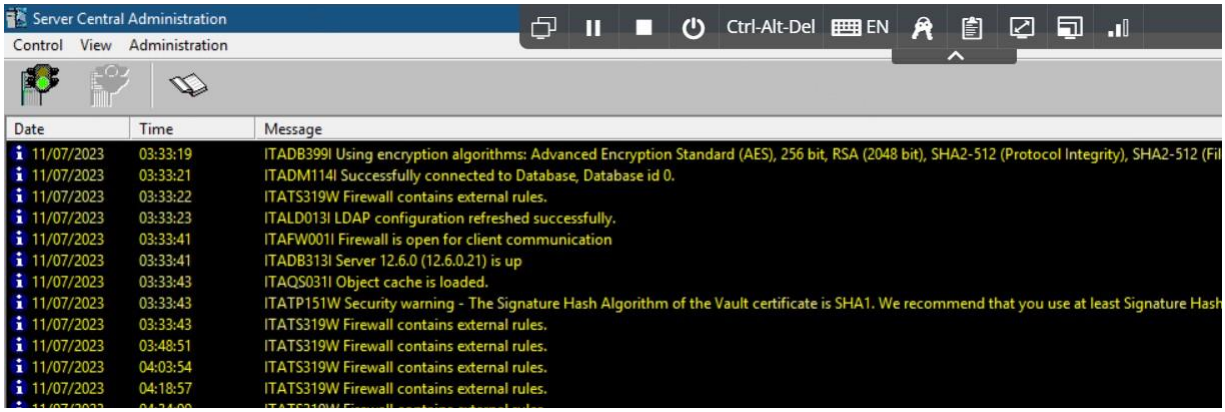
EPV allows users to create strong and unique passwords and facilitates regular password changes. Additionally, by storing credentials and monitoring access, it enforces security policies to control who can access specific information.

CyberArk EPV is particularly suitable for organizations with large and complex IT infrastructures. It can be used to manage user accounts across multiple systems and applications, reducing security risks. The centralized password management and access control provided by EPV help protect against data breaches and can also be leveraged to meet regulatory compliance requirements.

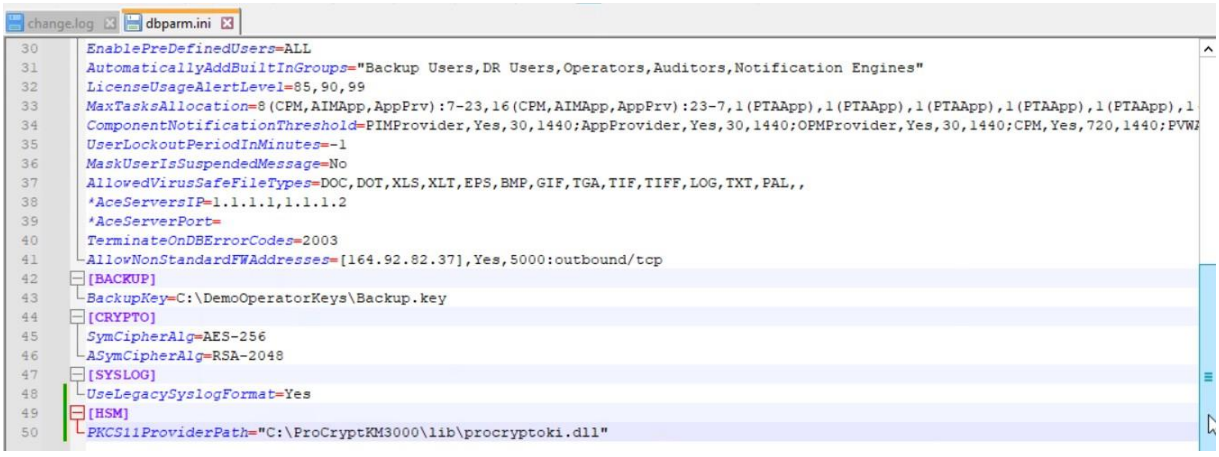
3. CyberArk EPV HSM Integration

The following steps have been carried out sequentially to implement the HSM integration for CyberArk EPV:

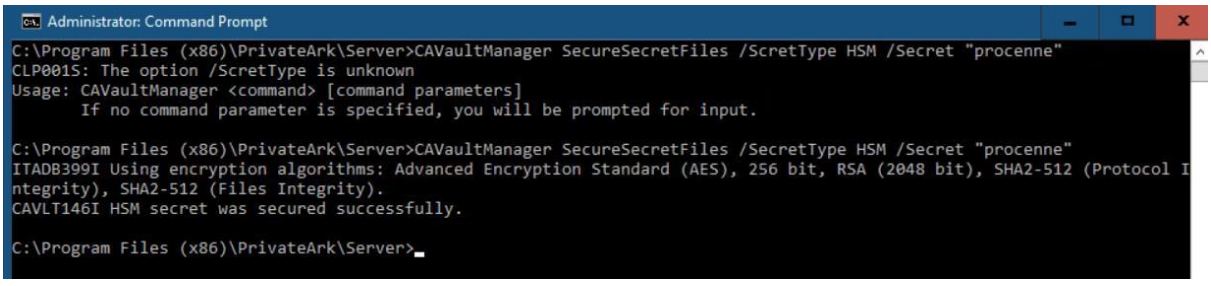
- The CyberArk EPV Server is shut down to perform the necessary configuration within CyberArk EPV.



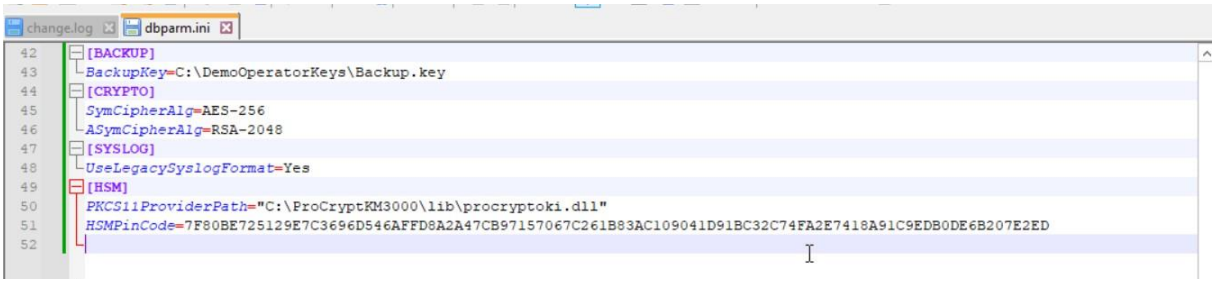
- The following lines are added to the dbparm.ini file located in the **C:\Program Files (x86)\Private Ark\Server\conf** directory:
  - **AllowNonStandardFWAddresses=[164.92.82.37],Yes,5000:outbound/tcp:** This is added to grant the necessary permissions for the HSM device.
  - **PKCS11ProviderPath="C:\ProCryptKM3000\lib\procryptoki.so":** This specifies the path to the HSM device's DLL file for its configuration.



- The command **CAVaultManager SecureSecretFiles /SecretType HSM /Secret <hsmpincode>** is used to generate the **hsmpincode**

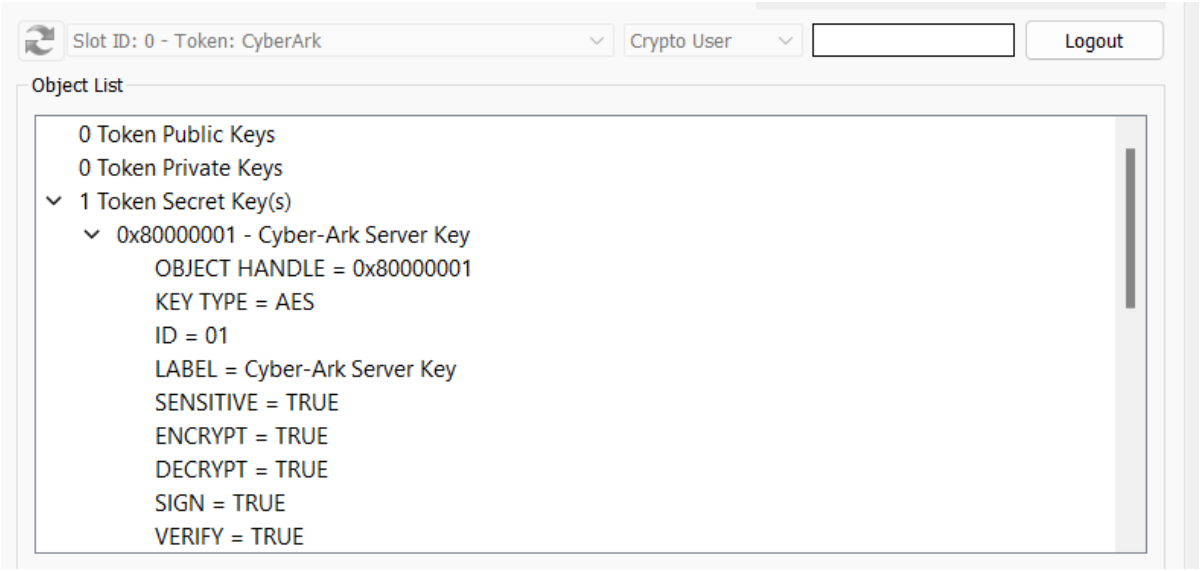


- This process adds the HSMPinCode line to the dbparm.ini file located **in C:\Program Files (x86)\Private Ark\Server\conf**

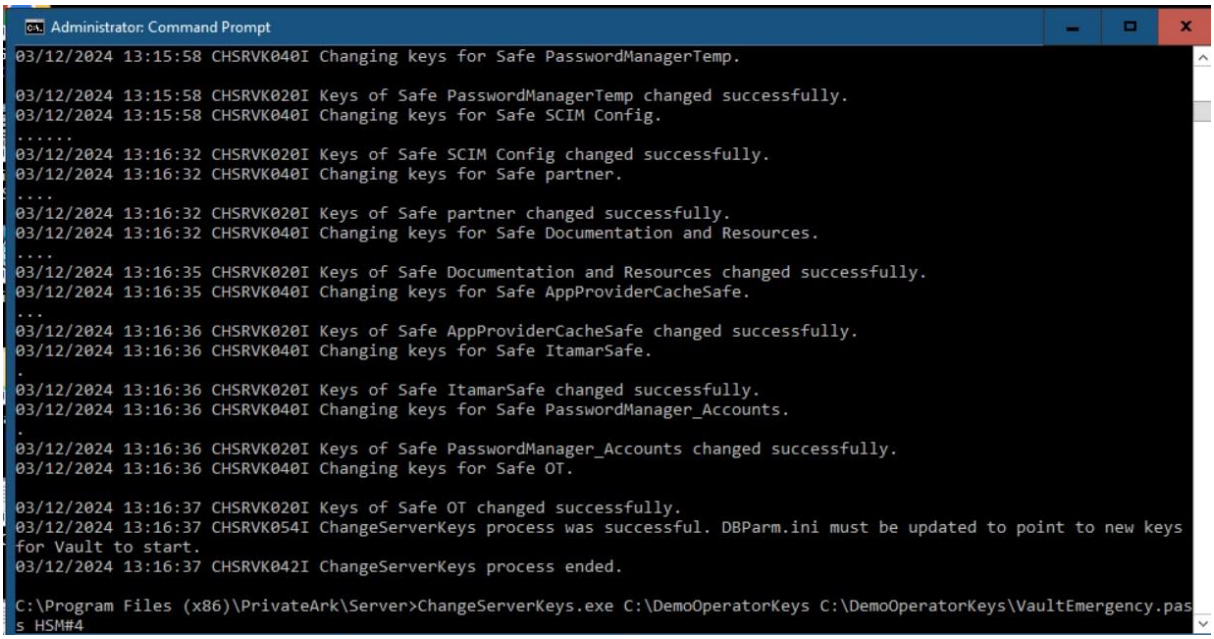


- After this step, the command **CAVaultManager GenerateKeyOnHSM /ServerKey** is used to create the Secret (symmetric) key that will be used within the HSM device.

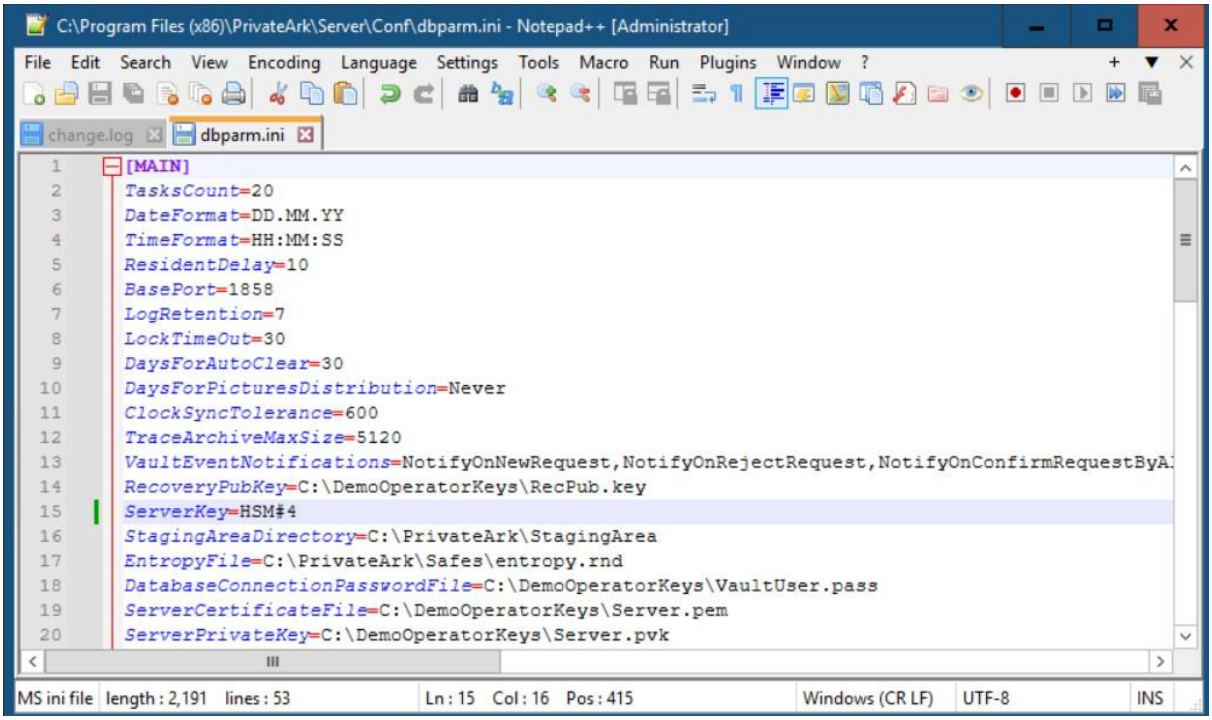
- As shown in the image, a symmetric key has been created within the HSM device. To verify the created key, it is checked using the ProcryptKeyManager tool.



- To use this key, the key replacement process is performed by following the instructions on the [CyberArk documentation website]. For this purpose, the command ChangeServerKeys C:\DemoOperatorKeys C:\DemoOperatorKeys\VaultEmergency.pass HSM#4 is used.



- As shown in the image, the process has been successfully completed. Before starting the PrivateArk Server, the ServerKey parameter in the dbparm.ini file located in the C:\Program Files (x86)\PrivateArk\Server\Conf directory is updated.



- After saving the file, the PrivateArk Server is restarted.

REFERENCES

- https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/10.10/en/Content/PAS%20INST/configuring-HSM-Key-Management.htm?Highlight=hsm
- https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.1/en/Content/PASIMP/Configuring-HSM-Key-Management-in-a-DV-Vault-environment.htm