Restauration du service Vault sur Cisco AsyncOS 15.5.1 et versions ultérieures pour Secure Email and Web Manager (SEWM)

Table des matières

Introduction

- Exigences
- Composants utilisés

Informations générales

Scénario 1 : Le coffre-fort Cisco Secure Email and Web Manager (SEWM) n'est pas initialisé et le cryptage est désactivé.

Scénario 2 : Le coffre Cisco Secure Email and Web Manager (SEWM) n'est pas initialisé et le cryptage est activé

Informations connexes

Introduction

Ce document fournit les instructions pour restaurer le service Vault sur votre Cisco Secure Email and Web Manager.

Exigences

Cisco recommande que vous connaissiez Async OS pour Secure Email et Web Manager version 15.5.1 et ultérieure

Composants utilisés

Les informations contenues dans ce document sont basées sur AsyncOS version 15.5.1 et les versions ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Cet article de Techzone décrit les scénarios courants rencontrés sur le terrain qui pourraient avoir un impact sur Cisco AsyncOS pour Secure Email and Web Manager. Cet article vous guide également dans la procédure de dépannage à suivre pour restaurer la fonctionnalité.

Secure Email and Web Manager génère des alertes indiquant : « Le coffre-fort est en panne et certains services risquent de ne pas fonctionner correctement. » Ou « Le contrôle d'intégrité du

coffre-fort a échoué. »

Remarque : Si la ligne de commande du périphérique est accessible, utilisez la commande adminaccessconfig -> encryptconfig CLI pour déterminer si le chiffrement est activé. Les alertes de défaillance du coffre-fort contiennent également ces informations.

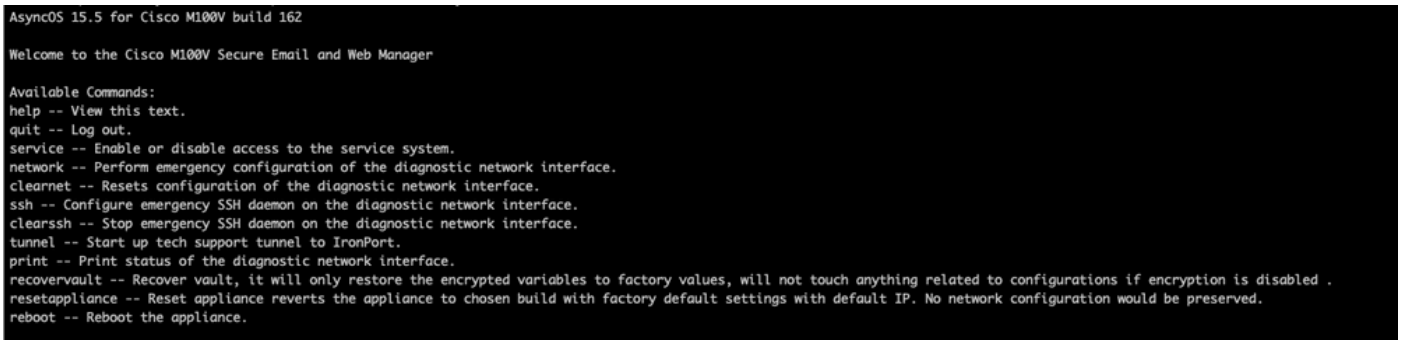
Scénario 1 : Le coffre-fort Cisco Secure Email and Web Manager (SEWM) n'est pas initialisé et le cryptage est désactivé.

1. Connectez-vous à Secure Email and Web Manager via une connexion SSH directe à l'aide des informations d'identification suivantes :

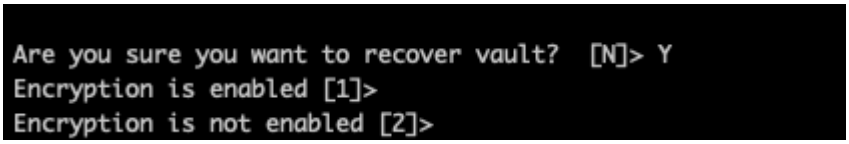
username (nom d’utilisateur) : activation du dialogue

password (mot de passe) : mot de passe d'administrateur

Une fois l'authentification réussie, le menu enable diag s'affiche.



2. Dans le menu, entrez la commande recovervault. Confirmez avec 'Y' et appuyez sur Entrée.



3. Entrez2, si le cryptage est désactivé pour exécuter un processus VaultRecovery. Cela peut prendre quelques secondes.

4.Connectez-vous à Secure Email and Web Manager avec les informations d'identification de l'utilisateur admin une fois le processus terminé et redémarrez l'appliance.Surveillez votre appliance pendant quelques heures pour détecter d'éventuelles alertes de coffre-fort.

Remarque : si vous avez besoin d'assistance à un moment ou à un autre ou si les étapes fournies ne permettent pas de résoudre le problème, contactez le centre d'assistance technique Cisco (TAC).

Scénario 2 : Le coffre Cisco Secure Email and Web Manager

(SEWM) n'est pas initialisé et le cryptage est activé

Remarque : si l'appliance AsyncOS 15.0 rencontre des erreurs de coffre-fort avec le cryptage activé, l'interface graphique utilisateur (GUI) ou l'interface de ligne de commande (CLI) de Secure Email and Web Manager peuvent devenir inaccessibles. Dans ce cas, accédez à Secure Email and Web Manager à l'aide de la console série avec l'utilisateur enable diag et contactez le TAC avec les détails d'accès au service.

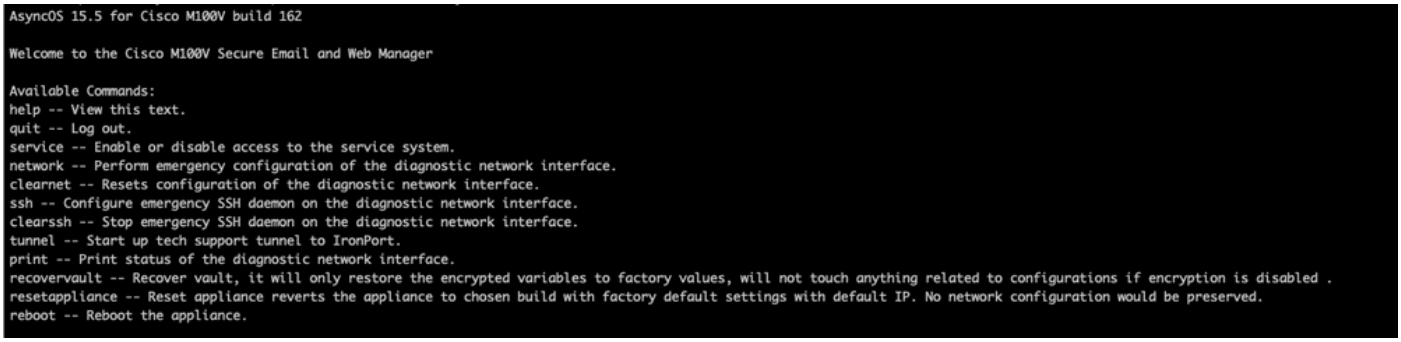
Si le périphérique est accessible via l'interface de ligne de commande, procédez comme suit :

1. Connectez-vous à Secure Email and Web Manager via une connexion SSH directe à l'aide des informations d'identification suivantes :

username (nom d'utilisateur) : activation du dialogue

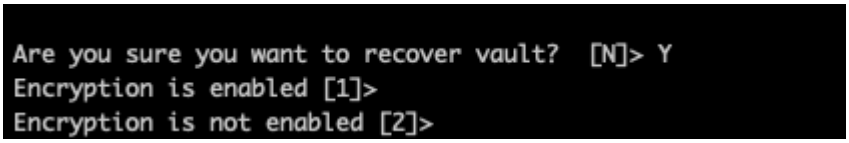
password (mot de passe) : mot de passe d'administrateur

Une fois l'authentification réussie, le menu enable diag s'affiche.



Attention : assurez-vous que vous disposez d'une copie de la configuration enregistrée du périphérique avec des mots de passe chiffrés disponibles qui peuvent être rechargés dans le périphérique. L'utilisation de la commande vault recovery sur les systèmes où le cryptage est activé réinitialise les variables cryptées à leur valeur d'usine par défaut et doit être reconfigurée.

2. Dans le menu, entrez la commande recovervault. Confirmez avec 'Y' et appuyez sur Entrée.



3. Entrez1, si le cryptage est désactivé pour exécuter un processus VaultRecovery. Cela peut prendre quelques secondes.

4.Connectez-vous à Secure Email and Web Manager avec les informations d'identification de l'utilisateur admin une fois le processus terminé et redémarrez l'appliance.Surveillez votre gestionnaire de messagerie et Web pendant quelques heures pour détecter d'éventuelles alertes

de coffre-fort.

5. Chargez une copie de la configuration enregistrée du périphérique pour restaurer les variables chiffrées.

Remarque : si vous avez besoin d'assistance à un moment ou à un autre ou si les étapes fournies ne permettent pas de résoudre le problème, contactez le centre d'assistance technique Cisco (TAC).

Informations connexes

- Assistance et documentation techniques - Cisco Systems
- Cisco Secure Email and Web Manager - Guides d'utilisation
- Cisco Secure Email and Web Manager - Notes de version

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.