Ripristino del servizio Vault su Cisco AsyncOS 15.5.1 e versioni successive per Secure Email e Web Manager (SEWM)

Sommario

[Introduzione](#)

- [Requisiti](#)
- [Componenti usati](#)

[Premesse](#)

[Scenario 1: l'insieme di credenziali Cisco Secure Email and Web Manager (SEWM) non è inizializzato e la crittografia è disabilitata.](#)

[Scenario 2: l'insieme di credenziali Cisco Secure Email and Web Manager (SEWM) non è inizializzato e la crittografia è abilitata](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono fornite le istruzioni per ripristinare il servizio Vault su Cisco Secure Email e Web Manager.

Requisiti

Cisco raccomanda la conoscenza di Async OS for Secure Email e Web Manager versione 15.5.1 e successive

Componenti usati

Le informazioni fornite in questo documento si basano sulla versione 15.5.1 di AsyncOS e sulle versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo articolo di Techzone vengono descritti gli scenari più comuni riscontrati nel campo che potrebbero influire su Cisco AsyncOS for Secure Email and Web Manager. In questo articolo viene inoltre descritto come eseguire le operazioni di risoluzione dei problemi per ripristinare le funzionalità.

Secure Email and Web Manager genera avvisi che segnalano "L'archivio è inattivo e alcuni servizi potrebbero non funzionare correttamente." Oppure "Controllo dello stato dell'archivio non riuscito".

Nota: se la riga di comando del dispositivo è accessibile, usare il comando adminaccessconfig -> encryptconfig CLI per determinare se la crittografia è abilitata. Gli avvisi di errore dell'insieme di credenziali contengono anche queste informazioni.

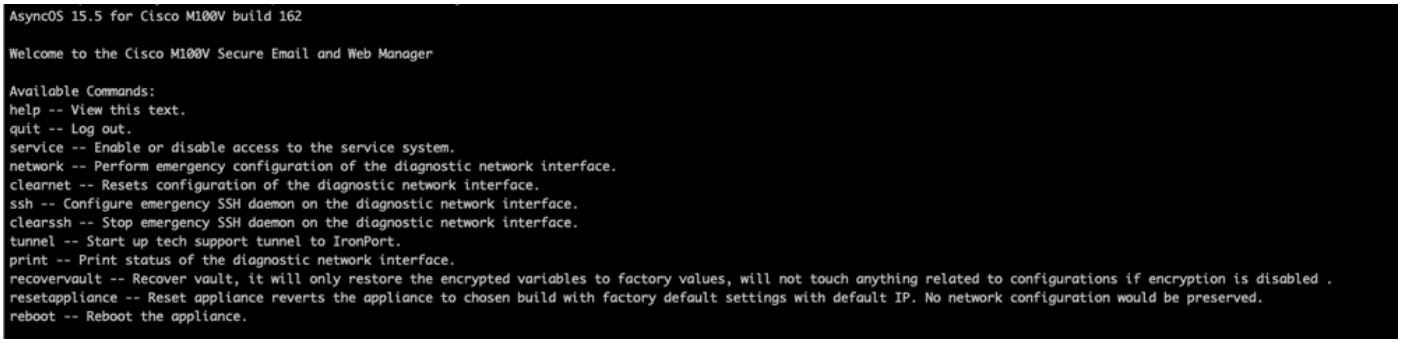
Scenario 1: l'insieme di credenziali Cisco Secure Email and Web Manager (SEWM) non è inizializzato e la crittografia è disabilitata.

1. Accedere a Secure Email e Web Manager tramite una connessione SSH diretta utilizzando le seguenti credenziali:

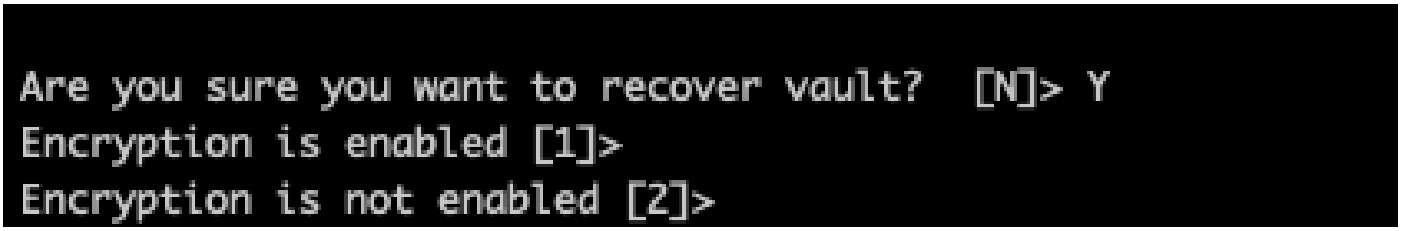
nome utente: enablediag

password: password utente amministratore

Dopo l'autenticazione riuscita, viene visualizzato il menu di abilitazione.



2. Dal menu, inserire il comando recovervault. Confermare con 'Y' e premere Invio.



3. Inserire2,se la crittografia è disabilitata per eseguire il processo VaultRecovery. Il completamento potrebbe richiedere alcuni secondi.

4. Accedere a Secure Email e Web Manager con le credenziali dell'utente admin dopo il completamento del processo e riavviare l'accessorio.Monitorare l'accessorio per un paio d'ore per qualsiasi avviso di vaulting.

Nota: se si desidera assistenza in qualsiasi momento o se le procedure fornite non risolvono il problema, contattare il Cisco Technical Assistance Center (TAC).

Scenario 2: l'insieme di credenziali Cisco Secure Email and Web Manager (SEWM) non è inizializzato e la crittografia è abilitata

Nota: se AsyncOS 15.0 in esecuzione sull'appliance rileva errori di vaulting con la crittografia abilitata, l'interfaccia grafica dell'utente (GUI) o l'interfaccia della riga di comando (CLI) di Secure Email e Web Manager potrebbe non essere più accessibile. In questo caso, accedere a Secure Email e Web Manager utilizzando la console seriale con l'abilitazione dell'utente e contattare TAC con i dettagli di accesso al servizio.

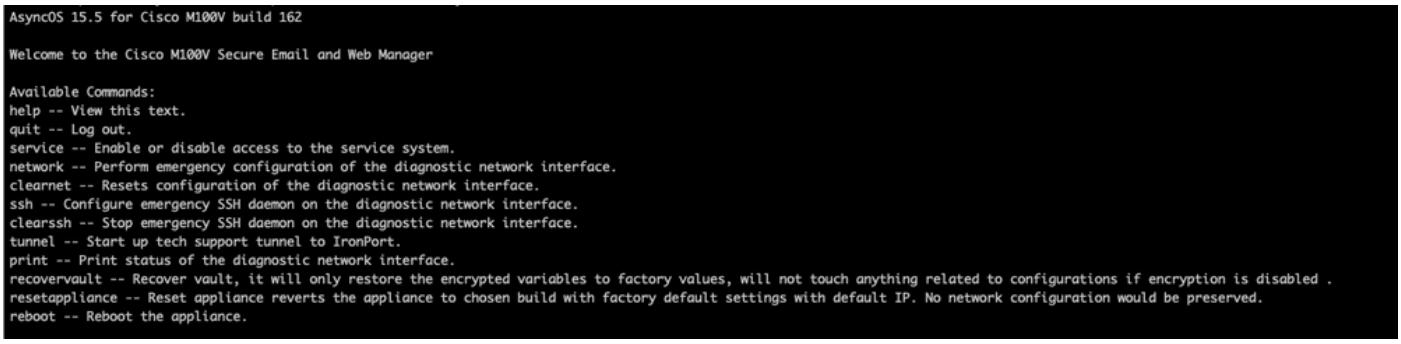
Se il dispositivo è accessibile dalla CLI, effettuare le seguenti operazioni:

1. Accedere a Secure Email e Web Manager tramite una connessione SSH diretta utilizzando le seguenti credenziali:

nome utente: enablediag

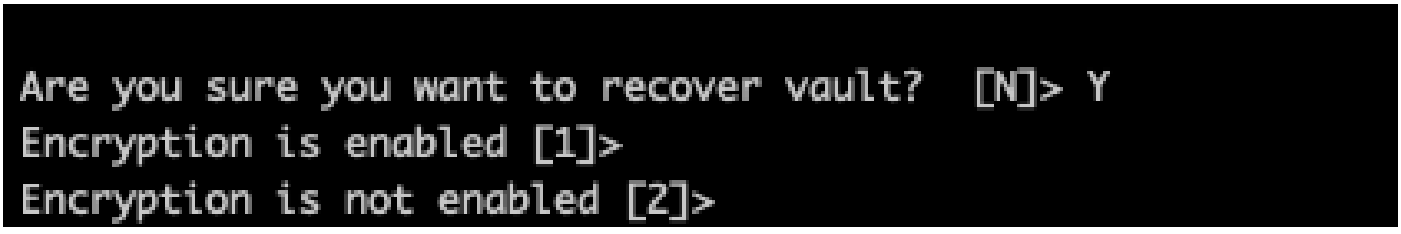
password: password utente amministratore

Dopo l'autenticazione riuscita, viene visualizzato il menu di abilitazione.



Attenzione: accertarsi di disporre di una copia della configurazione salvata del dispositivo con password crittografate che possano essere caricate nuovamente nel dispositivo. L'uso del comando vault recovery sui sistemi con crittografia abilitata ripristina i valori predefiniti delle variabili crittografate ed è necessario riconfigurarle.

2. Dal menu, inserire il comando recovervault. Confermare con 'Y' e premere Invio.



3. Inserire1,se la crittografia è disabilitata per eseguire il processo VaultRecovery. Il completamento potrebbe richiedere alcuni secondi.

4. Accedere a Secure Email e Web Manager con le credenziali dell'utente admin dopo il completamento del processo e riavviare l'accessorio.Controllare l'e-mail e il Web Manager per un paio d'ore per eventuali avvisi di vaulting.

5. Caricare una copia della configurazione salvata del dispositivo per ripristinare le variabili crittografate.

Nota: se si desidera assistenza in qualsiasi momento o se le procedure fornite non risolvono il problema, contattare il Cisco Technical Assistance Center (TAC).

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems
- Cisco Secure Email e Web Manager - Guide per l'utente
- Cisco Secure Email e Web Manager - Note sulla versione

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).