

Wiederherstellen des Vault Service unter Cisco AsyncOS 15.5.1 und höher für Secure Email Gateway (SEG)

Inhalt

[Einleitung](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[1. Szenario: Der Cisco Secure Email Gateway \(SEG\)-Tresor ist nicht initialisiert, und die Verschlüsselung ist deaktiviert.](#)

[Szenario 2: Der Cisco Secure Email Gateway \(SEG\)-Tresor ist nicht initialisiert, und die Verschlüsselung ist aktiviert.](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument enthält die Anweisungen zur Wiederherstellung des Vault-Service auf Ihrem Cisco Secure Email Gateway.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse von AsyncOS für Secure Email Gateway Version 15.5.1 und höheren Versionen verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AsyncOS-Version 15.5.1 und höheren Versionen.


Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem TechZone-Artikel werden allgemeine Szenarien beschrieben, die sich auf das Cisco AsyncOS für Secure Email Gateway auswirken können. Dieser Artikel führt Sie außerdem durch die Schritte zur Fehlerbehebung, um die Funktionalität wiederherzustellen.

Das sichere E-Mail-Gateway generiert Warnmeldungen mit dem Hinweis: "Der Tresor ist

ausgefallen, und einige Dienste funktionieren möglicherweise nicht richtig." oder "Die Überprüfung des Vault-Zustands ist fehlgeschlagen."

 Hinweis: Wenn auf die Befehlszeile des Geräts zugegriffen werden kann, verwenden Sie den CLI-Befehl `fipsconfig -> encryptconfig`, um festzustellen, ob die Verschlüsselung aktiviert ist. Diese Informationen sind auch in den Warnmeldungen zu Vault-Ausfällen enthalten.

1. Szenario: Der Cisco Secure Email Gateway (SEG)-Tresor ist nicht initialisiert, und die Verschlüsselung ist deaktiviert.

1. Melden Sie sich über eine direkte SSH-Verbindung mit den folgenden Anmeldeinformationen beim sicheren E-Mail-Gateway an:

Benutzername: `enableTag`

Kennwort: Kennwort des Administrators

Nach erfolgreicher Authentifizierung wird das Menü `enable` angezeigt.

```
AsyncOS 15.0.1 for Cisco C100V build 030
Welcome to the Cisco C100V Secure Email Gateway Virtual

Available Commands:
help -- View this text.
quit -- Log out.
service -- Enable or disable access to the service system.
network -- Perform emergency configuration of the diagnostic network interface.
clearnet -- Resets configuration of the diagnostic network interface.
ssh -- Configure emergency SSH daemon on the diagnostic network interface.
clearssh -- Stop emergency SSH daemon on the diagnostic network interface.
tunnel -- Start up tech support tunnel to IronPort.
print -- Print status of the diagnostic network interface.
recovervault -- Recover vault, it will only restore the encrypted variables to factory values, will not touch anything related to configurations if encryption is disabled .
resetappliance -- Reset appliance reverts the appliance to chosen build with factory default settings with default IP. No network configuration would be preserved.
reboot -- Reboot the appliance.
```

 Hinweis: Diese Schritte gelten auch für Async OS 15.0.1, wenn die Verschlüsselung nicht aktiviert ist.


2. Geben Sie im Menü den Befehl `recoveryVault` ein. Bestätigen Sie mit 'Y' und drücken Sie die Eingabetaste.

```
Are you sure you want to recover vault? [N]> Y
Encryption is enabled [1]>
Encryption is not enabled [2]>
```


3. Geben Sie `2` ein, wenn die Verschlüsselung deaktiviert ist, um einen Vault Recovery-Prozess auszuführen. Tresor Recovery Prozess durchzuführen. Der Vorgang kann einige Sekunden dauern.

4. Melden Sie sich nach Abschluss des Prozesses mit Administratoranmeldeinformationen beim

sicheren E-Mail-Gateway an, und starten Sie die Appliance neu. Überwachen Sie das E-Mail-Gateway einige Stunden lang auf alle Vault-Warnungen.

 Hinweis: Wenn Sie zu irgendeinem Zeitpunkt Unterstützung benötigen oder das Problem durch die bereitgestellten Schritte nicht behoben werden kann, wenden Sie sich an das Cisco Technical Assistance Center (TAC).

Szenario 2: Der Cisco Secure Email Gateway (SEG)-Tresor ist nicht initialisiert, und die Verschlüsselung ist aktiviert.

 Hinweis: Wenn auf einer Appliance AsyncOS 15.0.1 bei aktivierter Verschlüsselung Vault-Fehler auftritt, kann der Zugriff auf die grafische Benutzeroberfläche (GUI) oder die Befehlszeilenschnittstelle (CLI) des sicheren E-Mail-Gateways unterbrochen werden. In diesem Fall greifen Sie über eine serielle Konsole mit aktiviertem Benutzer auf das Secure Email Gateway zu und wenden sich mit den Zugriffsdetails an das TAC.

Wenn der Zugriff auf das Gerät über die CLI möglich ist, gehen Sie wie folgt vor:

1. Melden Sie sich über eine direkte SSH-Verbindung mit den folgenden Anmeldeinformationen beim sicheren E-Mail-Gateway an:


Benutzername: enableTag

Kennwort: Kennwort des Administrators

Nach erfolgreicher Authentifizierung wird das Menü enable angezeigt.

```
AsyncOS 15.0.1 for Cisco C100V build 030
Welcome to the Cisco C100V Secure Email Gateway Virtual


Available Commands:
help -- View this text.
quit -- Log out.
service -- Enable or disable access to the service system.
network -- Perform emergency configuration of the diagnostic network interface.
clearnet -- Resets configuration of the diagnostic network interface.
ssh -- Configure emergency SSH daemon on the diagnostic network interface.
clearssh -- Stop emergency SSH daemon on the diagnostic network interface.
tunnel -- Start up tech support tunnel to IronPort.
print -- Print status of the diagnostic network interface.
recovervault -- Recover vault, it will only restore the encrypted variables to factory values, will not touch anything related to configurations if encryption is disabled.
resetappliance -- Reset appliance reverts the appliance to chosen build with factory default settings with default IP. No network configuration would be preserved.
reboot -- Reboot the appliance.
```

 Achtung: Stellen Sie sicher, dass Sie über eine Kopie der gespeicherten Konfiguration des Geräts mit verschlüsselten Kennwörtern verfügen, die in das Gerät zurückgeladen werden können. Mit dem Befehl vault recovery auf Systemen mit aktivierter Verschlüsselung werden verschlüsselte Variablen auf ihren werkseitigen Standardwert zurückgesetzt und müssen neu konfiguriert werden.

2. Geben Sie im Menü den Befehl recoveryVault ein. Bestätigen Sie mit "Y" und betätigen Sie die Eingabetaste.

```
Are you sure you want to recover vault? [N]> Y
Encryption is enabled [1]>
Encryption is not enabled [2]>
```

3. Geben Sie 1 ein, wenn die Verschlüsselung aktiviert ist, um einen Vault Recovery-Prozess auszuführen. Dieser Vorgang kann einige Sekunden dauern.
4. Melden Sie sich nach Abschluss des Prozesses mit Administratoranmeldeinformationen beim sicheren E-Mail-Gateway an, und starten Sie die Appliance neu. Überwachen Sie das E-Mail-Gateway einige Stunden lang auf alle Vault-Warnungen.
5. Laden Sie eine Kopie der gespeicherten Gerätekonfiguration, um verschlüsselte Variablen wiederherzustellen.

 Hinweis: Wenn Sie zu irgendeinem Zeitpunkt Unterstützung benötigen oder das Problem durch die bereitgestellten Schritte nicht behoben werden kann, wenden Sie sich an das Cisco Technical Assistance Center (TAC).

Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)
- [Cisco Secure Email Gateway - Benutzerhandbücher](#)
- [Cisco Secure Email Gateway - Versionshinweise](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.