Secure Email Gateway(SEG)用のCisco AsyncOS 15.5.1以降でのVaultサービスの復元

内容

はじめに

このドキュメントでは、Cisco Secure Email GatewayでVaultサービスを復元する手順について説明します。

要件

AsyncOS for Secure Email Gatewayバージョン15.5.1以降のバージョンに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、AsyncOSバージョン15.5.1以降のバージョンに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このTechzoneの記事では、Cisco AsyncOS for Secure Email Gatewayに影響を与える可能性がある、フィールドで発生する一般的なシナリオについて説明します。この記事では、機能を復元するためのトラブルシューティング手順も示します。

Secure Email Gatewayは、「The Vault is down, and some of the services may not work correctly」というアラートを生成します。 または「Vaultのヘルスチェックに失敗しました」

注：デバイスのコマンドラインにアクセスできる場合は、fipsconfig -> encryptconfig CLIコマンドを使用して、暗号化が有効になっているかどうかを確認します。この情報は、ヴォールト障害のアラートにも表示されます。

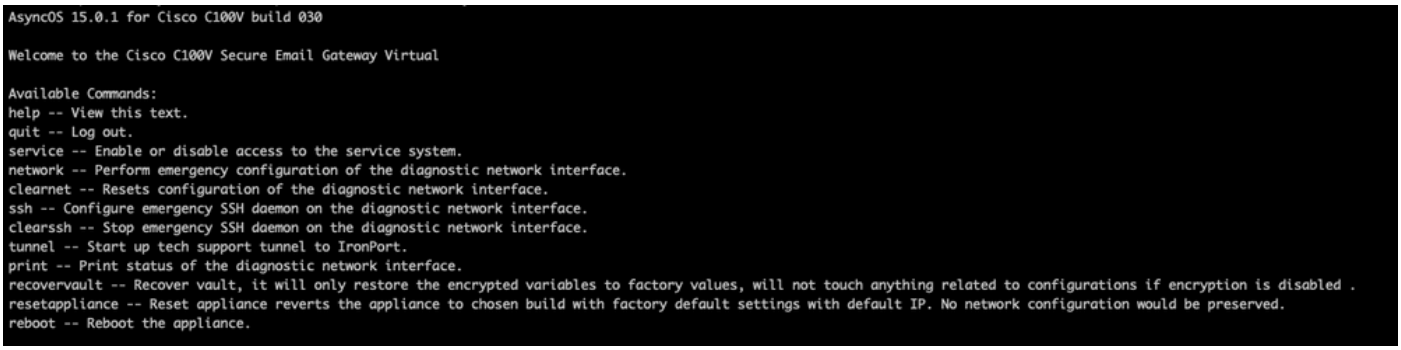
シナリオ1:Cisco Secure Email Gateway(SEG)Vaultが初期化されず、暗号化が無効になっている。

1.次のクレデンシャルを使用して、直接SSH接続を介してSecure Email Gatewayにログインします。

ユーザ名：enablediag

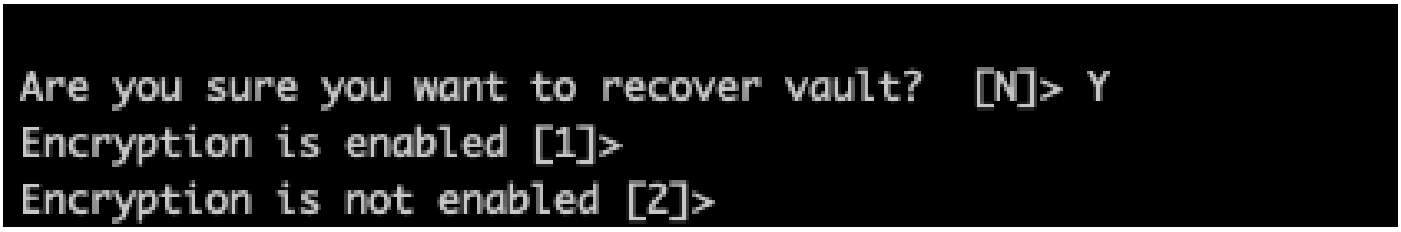
パスワード：adminユーザのパスワード

成功した認証の後、enablediagメニューが表示されます。



注：これらの手順は、暗号化が有効になっていない非同期OS 15.0.1にも適用されます。

2.メニューから、コマンドrecovervaultを入力します。「Y」で確認し、Enterキーを押します。



3. Vault Recoveryプロセスを実行するために暗号化が無効になっている場合は、2を入力します。完了まで数秒かかる場合があります。

4.プロセスが完了したら、管理者ユーザクレデンシャルを使用してセキュアEメールゲートウェイにログインし、アプライアンスをリブートします。Vaultアラートが発生した場合は、Eメールゲートウェイを数時間モニタしてください。

注:サポートが必要な場合、または提供された手順で問題が解決しない場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

シナリオ2:Cisco Secure Email Gateway(SEG)Vaultが初期化されず、暗号化が有効になっている。

注:AsyncOS 15.0.1を実行しているアプライアンスで暗号化が有効な状態でVaultエラーが発生した場合、Secure Email Gatewayのグラフィカルユーザインターフェイス(GUI)またはコマンドラインインターフェイス(CLI)にアクセスできなくなる可能性があります。これが発生した場合は、enablediagユーザを指定したシリアルコンソールを使用してSecure Email Gatewayにアクセスし、サービスアクセスの詳細を指定してTACに連絡してください。

CLIを使用してデバイスにアクセスできる場合は、次の手順を実行します。

1.次のクレデンシャルを使用して、直接SSH接続を介してSecure Email Gatewayにログインします。

ユーザ名：enablediag

パスワード：adminユーザのパスワード

成功した認証の後、enablediagメニューが表示されます。

```
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.
```

注意:デバイスにロードして戻すことができる暗号化パスワードを使用した、デバイスの保存された設定のコピーが存在することを確認してください。暗号化が有効なシステムでVault Recoveryコマンドを使用すると、暗号化変数がデフォルトの工場出荷時の値にリセットされるため、再設定が必要になります。

2.メニューから、コマンドrecovervaultを入力します。「Y」で確定し、Enterキーを押します。

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

3. Vaultのリカバリプロセスを実行するために暗号化が有効になっている場合は、1を入力します。完了まで数秒かかる場合があります。

4.プロセスが完了したら、管理者ユーザクレデンシャルを使用してセキュアEメールゲートウェイにログインし、アプライアンスをリブートします。Vaultアラートが発生した場合は、Eメールゲートウェイを数時間モニタしてください。

5.デバイスの保存済み設定のコピーをロードし、暗号化された変数を復元します。

注:サポートが必要な場合、または提供された手順で問題が解決しない場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems
- Cisco Secure Email Gateway – エンドユーザガイド
- Cisco Secure Email Gateway – リリースノート

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。