

Restauração do Vault Service no Cisco AsyncOS 15.5.1 ou posterior para Secure Email and Web Manager (SEWM)

Contents

[Introdução](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Cenário 1: o cofre do Cisco Secure Email and Web Manager \(SEWM\) não foi inicializado e a criptografia está desabilitada.](#)

[Cenário 2: O cofre do Cisco Secure Email and Web Manager \(SEWM\) não foi inicializado e a criptografia está habilitada](#)

[Informações Relacionadas](#)

Introdução

Este documento fornece as instruções para restaurar o serviço do Vault em seu Cisco Secure Email e Web Manager.

Requisitos

A Cisco recomenda que você tenha conhecimento do Async OS for Secure Email e Web Manager versão 15.5.1 e mais recente

Componentes Utilizados

As informações neste documento são baseadas no AsyncOS versão 15.5.1 e versões posteriores.


As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este artigo da Techzone descreve os cenários comuns encontrados no campo que podem afetar o Cisco AsyncOS para Secure Email e Web Manager. Este artigo também o orienta a executar etapas de solução de problemas para restaurar a funcionalidade.

O Secure Email and Web Manager gera alertas informando: "O cofre está desativado e alguns

dos serviços podem não funcionar corretamente." Ou "A verificação de integridade do cofre falhou."

 Observação: se a linha de comando do dispositivo estiver acessível, use o comando da CLI `adminaccessconfig -> encryptconfig` para determinar se a criptografia está habilitada. Os alertas de falha do cofre também contêm essas informações.

Cenário 1: o cofre do Cisco Secure Email and Web Manager (SEWM) não foi inicializado e a criptografia está desabilitada.

1. Efetue login no Secure Email and Web Manager através de uma conexão SSH direta usando as seguintes credenciais:

nome de usuário: `enablediag`

senha: senha do usuário admin

Após a autenticação bem-sucedida, o menu `enablediag` é exibido.

```
AsyncOS 15.5 for Cisco M100V build 162
Welcome to the Cisco M100V Secure Email and Web Manager


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.
```

2. No menu, insira o comando `recovervault`. Confirme com 'Y' e pressione Enter.


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

3. Insira 2, se a criptografia estiver desabilitada para executar o processo `deaVaultRecovery`. Pode levar alguns segundos para concluir.

4. Faça login no Secure Email and Web Manager com credenciais de usuário admin depois que o processo estiver concluído e reinicialize o equipamento. Monitore seu equipamento por algumas horas para qualquer alerta de compartimento.

 Observação: se você precisar de assistência em algum momento ou se as etapas fornecidas não corrigirem o problema, entre em contato com o Cisco Technical Assistance

Cenário 2: O cofre do Cisco Secure Email and Web Manager (SEWM) não foi inicializado e a criptografia está habilitada

 Observação: para que o AsyncOS 15.0 em execução no equipamento encontre erros de cofre com criptografia habilitada, a Interface Gráfica de Usuário (GUI) ou a Interface de Linha de Comando (CLI) do Secure Email e Web Manager pode se tornar inacessível. Se isso ocorrer, acesse o Secure Email and Web Manager usando o console serial com o usuário [enablediag](#) e entre em contato com o TAC com os detalhes de acesso ao serviço.

Se o dispositivo estiver acessível por meio do CLI, execute as seguintes etapas:

1. Efetue login no Secure Email and Web Manager através de uma conexão SSH direta usando as seguintes credenciais:


nome de usuário: enablediag

senha: senha do usuário admin

Após a autenticação bem-sucedida, o menu enablediag é exibido.

```
AsyncOS 15.5 for Cisco M100V build 162
Welcome to the Cisco M100V Secure Email and Web Manager

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.
```

 Cuidado: Verifique se você tem uma cópia da configuração salva do dispositivo com senhas criptografadas disponíveis que possam ser carregadas de volta no dispositivo. O uso do comando vault recovery em sistemas com a criptografia habilitada redefine as variáveis criptografadas para o valor de fábrica padrão e precisa ser reconfigurado.


2. No menu, insira o comando recovervault. Confirme com 'Y' e pressione Enter.

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

3. Insira 1, se a criptografia estiver desabilitada para executar o processo VaultRecovery. Pode levar alguns segundos para concluir.

4. Faça login no Secure Email and Web Manager com credenciais de usuário admin depois que o processo estiver concluído e reinicialize o equipamento. Monitore seu gerenciador de e-mail e Web por algumas horas para qualquer alerta de compartimento.

5. Carregue uma cópia da configuração salva do dispositivo para restaurar as variáveis criptografadas.

 Observação: se você precisar de assistência em algum momento ou se as etapas fornecidas não corrigirem o problema, entre em contato com o Cisco Technical Assistance Center (TAC).

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)
- [Cisco Secure Email and Web Manager - Guias do usuário final](#)
- [Cisco Secure Email and Web Manager - Notas de versão](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.