

Falha na Implantação Virtual do Firewall Seguro Devido ao Extrator de Arquivos do Windows

Contents

Problema

A implantação do dispositivo virtual do Cisco Secure Firewall (ASAv, FTDv, FMCv ou FMCv300) no VMware vCenter ou ESXi falha com este erro mostrado durante a implantação da VM:

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Import OVF package	ITOps	Failed to deploy OVF package. Cause: A general system error occurred: Transfer failed: Invalid response code: 500.		vsphere.local/dlungu	99 ms	04/23/2026, 12:29:31 PM	04/23/2026, 12:47:53 PM
Deploy OVF template	ITOps	Failed to deploy OVF package. Cause: A general system error occurred: Transfer failed: Invalid response code: 500.	Copying Virtual Machine configuration	VSPHERE.LOCAL\content-library-user-3cc31137-fd28-4bd1-bf2b-ccc9babeb6d1	4 ms	04/23/2026, 12:30:50 PM	04/23/2026, 12:47:53 PM
Clone virtual machine	RegalSQL22	Completed	Reconfiguring Virtual Mac	VSPHERE.LOCAL\horizonAd	507 ms	04/23/2026, 12:42:4	04/23/2026, 12:42:5

A soma de verificação MD5 do pacote é verificada no site software.cisco.com. Após o download do arquivo do site, o MD5 permanece o mesmo e ainda não há nenhuma evidência de qualquer arquivo corrompido.

Advisories

Details

Description : FMCv: VMware install package for ESXi 6.5, 6.7, 7.0, 8.0

Release : 7.6.5

Release Date : 17-Feb-2026

FileName : Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-7.6.5-106.tar.gz

Size : 2142.02 MB (2246074566 bytes)

MD5 Checksum : d3a4976b8c0702b91af00623413e1bcb

SHA512 Checksum : 06343c9ad99ab33ae90854b6c1d5cde5

Documentation Landing Page Release Notes for 7.6.5 Advisories

17-Feb-20262340.50 MB

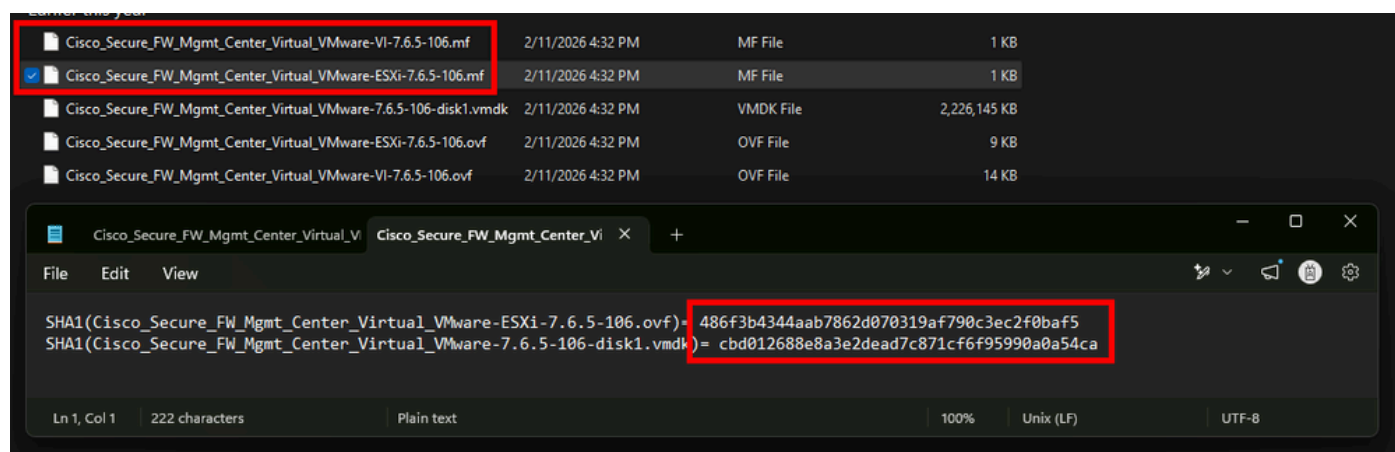
17-Feb-20262143.59 MB

17-Feb-20262284.81 MB

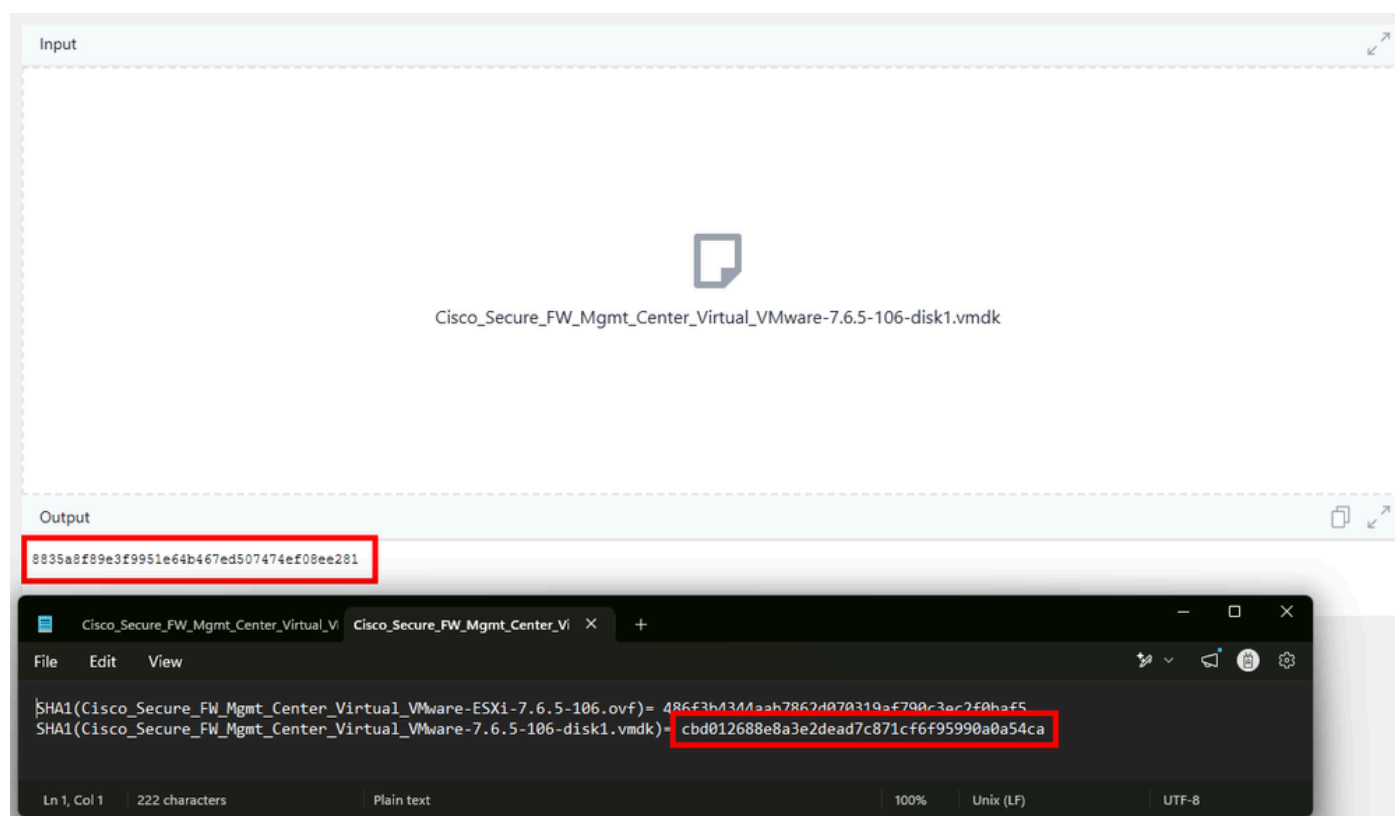
FMCv: VMware install package for ESXi 6.5, 6.7, 7.0, 8.0Cisco_Secure_FW_Mgmt_Center_Virtual_VM62142.02 MB

Quando o pacote é extraído, o conteúdo contém um arquivo *.mf como

"Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.mf". Este arquivo contém os hashes SHA1 fornecidos pela Cisco para os arquivos de imagem.



Ao usar o comando nativo do Windows "Extrair tudo..." em vez de um extrator de arquivos de terceiros, as imagens do ficam corrompidas e os hashes SHA1 desses arquivos não correspondem aos hashes de arquivo *.mf da Cisco.



Como os hashes SHA1 não correspondem, os arquivos se tornam inválidos para uso no VMWare e resultam no erro 500.

! Failed to deploy OVF package.
Cause: A general system error occurred:

Transfer failed: Invalid response code: 500.

Ambiente

- VMware vCenter Server 9.0, VMware ESXi 8.0.3
- Pacotes de instalação de dispositivo virtual do Cisco Secure Firewall usando arquivos VMDK
- Sistema operacional Windows usado para extração e carregamento de pacotes no vCenter ou ESXi

Resolução

Solução:

- 1.- Confirme a correspondência de hashes MD5 antes e depois do download do pacote VMWare zipado.
- 2.- Baixe e instale um extrator de arquivos de terceiros, como o 7-Zip, de um site oficial para usar em vez da ferramenta de extração nativa do Windows.
- 3.- Extraia o pacote zipado usando o extrator de arquivos de terceiros e anote os hashes SHA1 para cada arquivo dos arquivos Cisco *.mf em um bloco de notas.
- 4.- Gere o hash SHA1 para o arquivo de imagem necessário (OVF/VMDK) com qualquer ferramenta de hash on-line e certifique-se de que ele corresponda ao mostrado nos arquivos Cisco *.mf.
- 5.- Implante o FMCv usando o arquivo OVF apropriado com base em seu método de implantação:
 - Para implantações do vCenter: Usar o arquivo VI OVF e VMDK
 - Para implantações ESXi independentes: Usar o arquivo ESXi OVF e VMDK

Causa

O problema é causado pela corrupção do arquivo durante a extração quando o extrator de arquivos nativo do Windows é usado para descompactar o pacote de instalação .tar.gz. Embora a soma de verificação MD5 do pacote baixado seja válida, o utilitário de extração nativo do Windows altera a integridade do arquivo durante a extração, resultando em arquivos OVF/VMDK inválidos que fazem com que o VMware retorne um erro HTTP 500 genérico durante a implantação. Esse comportamento se alinha ao bug da Cisco ID CSCwp3802, que documenta problemas na extração de imagens virtuais do Firewall Seguro usando ferramentas nativas do Windows. Isso é resolvido com imagens do Firepower 10.0.0.

Conteúdo relacionado

- [ID de bug Cisco CSCwp33802 - \[DOC\] Falha ao implantar VM: falha de postNFCData: \[STREAMVMDK\] cmpSize inválido lido: 3225899676](#)
- [Guia de introdução virtual do Cisco Secure Firewall Management Center](#)
- [Suporte técnico e downloads da Cisco](#)
- [Extrator de Arquivos 7-zip](#)
- [Ferramenta de soma de verificação do arquivo Github](#)

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.