Implementar a versão de reversão do VDB no FMC versão 7.3+

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Configurar Configurações iniciais Processo de reversão Verificar Limitações Informações Relacionadas

Introdução

Este documento descreve o processo de downgrade do banco de dados de vulnerabilidades no Secure Firewall Management Center (FMC) versão 7.3 e posterior.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

• Cisco Secure Firewall Management Center versão 7.3 VDB 361

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.

Configurar

Configurações iniciais

Na GUI do FMC, a versão do VDB é obtida no MainMenu > 2 > Sobre.

w	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	6	≎	0	idmin 🔻
Г	About			Tools					On	screer	Assistance
				Firep	ower Migration	Tool			Pag	ge-lev	el Help
	Product Conte	ent		Appl	lication Detecto	rs			Ho	w-Tos	New
	Sacura Eirau	vall on Cierr	noom								

ahah	×
cisco SECU	RE
Firewall M	anagement Center
Version 7.3.0 (build 69)	
Model	Secure Firewall Management Center for VMware
Serial Number	None
Snort Version	2.9.21 (Build 105)
Snort3 Version	3.1.36.1 (Build 101)
Rule Pack Version	2868
Module Pack Version	3244
LSP Version	lsp-rel-20230712-1621
VDB Version	build 361 (2022-11-15 19:57:46)
Rule Update Version	2023-07-12-002-vrt
Geolocation Update Versi	on Country Code: 2023-06-17-100, IP: 2023-06-17-100
OS	Cisco Firepower Extensible Operating System (FX-OS)
	2.13.0 (build 198)
Hostname	firepower
For technical/system questio 7209. Copyright 2004-2022,	ns, email tac@cisco.com phone: 1-800-553-2447 or 1-408-526- Cisco and/or its affiliates. All rights reserved.
Сору	Close

Na CLI, a versão do VDB é obtida com o comando show version .

<#root>

> show version

------ [firepower]------Model : Secure Firewall Management Center for VMware (66) Version 7.3.0 (Build 69) UUID : e8f4b5de-4da1-11ed-b2ce-4637a3ef82f7 Rules update version : 2023-07-12-002-vrt LSP version : lsp-rel-20230712-1621

VDB version : 361

Processo de reversão

Se a versão anterior do VDB não estiver mais armazenada no FMC, navegue até **Sistema**(*) > **Atualizações > Atualizações do produto > Atualizações disponíveis> Upload de atualizações,** selecione o arquivo VDB no computador local e clique em Upload.

Depois que o arquivo VDB é carregado no FMC, a versão mais antiga do VDB (versão 359 nesse caso) exibe um ícone newRollback em vez do **ícone Install**.

Clique no botão de reversão.

	Firewall Management Center System / Updates / Product Updates	Overview	Analysis	Policies	Devices	Objects	Integration
	Product Updates Rule Updates Geolocation I	Updates					
Currently running software version: 7.3.0 Currently installed VDB version: build 361 (2022-11-15 19:57:46) Available Updates Readiness History Download updates							
	Туре	Version				Date	
	Cisco Vulnerability And Fingerprint Database Updates	361				Tue Nov 15	19:59:36 UTC 2022
	Cisco Vulnerability And Fingerprint Database Updates	359				Tue Oct 4 1	9:46:46 UTC 2022

Em seguida, marque a caixa de seleção FMC e clique em Install.

Product Updates	ates / Product Upda Rule Updates	Geolocation Updates	w Analysis	Policies	Devices	Objects	Integration		De
Currently running sof	tware version: 7.3.0)							
Selected Updat	te Type Cisco V Version 359 Date Tue Oct Reboot No	/ulnerability And Fingerprir	nt Database Updates						
Ungrouped	(1 total)			Compatibility Cl	heck		Readiness C	heck Results	Readiness C
10.10.10.19 - S	cure Firewall Manage	ment Center for VMware v7	.3.0	N/A					
	-								

Um aviso é exibido para informá-lo sobre a possível interrupção de tráfego no caso de você implantar alterações nos firewalls gerenciados após a reversão do VDB.



Verificar

Quando a tarefa de reversão for concluída, a versão do VDB poderá ser confirmada no **Menu** principal > **2 Sobre.**



Finalmente, após a reversão do VDB, uma implantação de política é necessária para enviar a nova configuração do VDB para os firewalls gerenciados do FMC.



Limitações

- O botão de reversão de VDB não está disponível antes do FMC 7.3.
- Você não poderá reverter o VDB para uma versão anterior a 357. Se uma versão do VDB anterior a 357 for carregada no FMC, o botão de reversão ficará esmaecido.

Cisco Vulnerability And Fingerprint Database Updates	354	Wed Apr 27 19:42:09 UTC 2022	No	ð 🖬
				VDB rollback is only supported starting with VDB version 357

 Se a versão do VDB for inferior à versão básica do VDB do FMC, a tarefa de reversão concluída com êxito será exibida; no entanto, a versão do VDB exibida continuará mostrando a mesma versão anterior à tentativa de reversão.



Na CLI do FMC, você pode confirmar que isso ocorreu porque a versão de destino da reversão é inferior à versão de base do FMC. Isso pode ser confirmado na CLI do FMC no arquivo status.log.

sudo su cd /var/log/sf/vdb-4.5.0-<vdb number>/ cat status.log root@firepower:/var/log/sf/vdb-4.5.0-357# cat status.log state:running ui:The install has begun. ui:[0%] Running script pre/000_start.sh... ui:[0%] Running script pre/010_check_versions.sh... ui:[4%] Running script pre/010_check_versions.sh... ui:[4%] Non-Fatal error: Non-Fatal error: Cannot rollback to version(357) lower than default VDB 358 ui:[4%] The install completed successfully. ui:The install has completed. state:finished

Informações Relacionadas

<u>Suporte técnico e downloads da Cisco</u>

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.