Configurer une planification de mise à jour de base de données régulière pour VDB sur FDM

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Configurations
Vérifier
<u>Dépannage</u>
Informations connexes

Introduction

Ce document décrit comment configurer un planning de mise à jour de base de données normal pour Rule ou VDB sur FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de périphériques Firepower
- Base de données des failles (VDB)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• FDM 7.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La base de données des vulnérabilités Cisco (VDB) est une base de données répertoriant les vulnérabilités connues des hôtes susceptibles d'être infectés, ainsi que les empreintes digitales des systèmes d'exploitation, des clients et des applications.

Le système de pare-feu établit une corrélation entre les empreintes digitales et les vulnérabilités pour vous aider à déterminer si un hôte particulier augmente le risque de compromission du réseau. Le Cisco Talos Intelligence Group (Talos) émet des mises à jour périodiques de la VDB.

Il est recommandé d'activer le planificateur automatique pendant le processus d'intégration afin de vérifier et d'appliquer régulièrement les mises à jour de la base de données de sécurité. Cela permet de s'assurer que le périphérique reste à jour.

Configurer

Configurations

1. Connectez-vous au Gestionnaire de périphériques Firepower

CISCO™
Firepower Device Manager
Username
Password
LOG IN
LOG IN

2. Dans l'écran Périphériques, accédez à Mises à jour > Afficher la configuration.



3. Dans l'écran Mises à jour, accédez à VDB > Configurer.

Device Summary Updates			
Geolocation 2020-04-28-002 Latest Update on 16 May 2023	VDB 384.0 Latest Update on 10 Apr 2024	Security Intelligence Feeds	
Configure Set recurring updates	Configure Set recurring updates	Configure Set recurring updates	
	OPOLITE FILOW CLOUD		
System Upgrade Current version 7.0.4-55		Intrusion Rule 20210503-2107 Latest Update on 16 May 2023	
There are no software upgrades available Upload an upgrade file to install.	on the system.	Configure Set recurring updates Short UPDATE FROM CLOUD V Short is the main inspection engine in Firepower Thm Defense. It is used for intrusion and file policy analys SSL decryption, and layer 7 inspection. See, more V	eat ps.

4. Sur l'écran Définir les mises à jour périodiques, modifiez les paramètres par défaut selon vos besoins et cliquez sur Enregistrer.

Set recurring updates	×
Frequency Weekly	~
Days of Week Time (UTC-05:00) America/Mexico_City	
 Sundays × → at 11 × : 00 × Automatically deploy the update. (Note: The deployment will also deploy all pending configuration 	changes.)
DELETE CANCEL	SAVE

Vérifier

Dans l'écran Updates, dans la section VDB, l'option de mise à jour récurrente sélectionnée est reflétée.

Device Summary Updates



Dépannage

Si la mise à niveau automatique de la VDB ne fonctionne pas comme prévu, vous pouvez restaurer la VDB.

Étapes :

Connexion SSH à l'interface de ligne de commande du périphérique de gestion (FMC, FDM ou SFR onbox)

Passez en mode expert et en mode racine, puis définissez la variable d'annulation :

<#root>

expert

sudo su export ROLLBACK_VDB=1

Vérifiez que le package VDB vers lequel vous souhaitez effectuer la rétrogradation se trouve sur le périphérique dans /var/sf/updates et installez-le :

<#root>

install_update.pl --detach /var/sf/updates/<name of desired VDB Package file>

Suivez les journaux d'installation de vdb normaux à l'emplacement approprié sur /var/log/sf/vdb-*

Une fois l'installation de VDB terminée, déployez la stratégie sur les périphériques.

Sur l'interface de ligne de commande FTD, pour vérifier l'historique des installations de VDB, vous pouvez vérifier le contenu de ces répertoires :

root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages#ls -al total 72912 drwxr-xr-x 5 root 130 sep 1 08:49 . drwxr-xr-x 4 root root 34 Aug 16 14:40 .. drwxr-xr-x 3 root 18 août 16 14:40 exporter-7.2.4-169 -rw-r—r— 1 racine 2371661 juil 27 15:34 exporter-7.2.4-169.tgz drwxr-xr-x 3 root 21 août 16 14:40vdb-368 -rw-r—r— 1 racine 36374219 juil 27 15:34 vdb-368.tgz drwxr-xr-x 3 root 21 sep 1 08:49vdb-369 -rw-r—r— 1 racine 35908455 sept. 1 08:48 vdb-369.tgz

Informations connexes

Mise à jour des bases de données système

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.