

Een regelmatig programma voor het bijwerken van databases voor VDB op FDM configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[Verifiëren](#)

[Probleemoplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een regelmatig programma voor het bijwerken van databases kunt configureren voor Rule of VDB op FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Device Manager
- Vulnerability Database (VDB)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FDM 7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Cisco Vulnerability Database (VDB) is een database van bekende kwetsbaarheden voor gevoelige hosts, evenals vingerafdrukken voor besturingssystemen, clients en toepassingen.

Het firewallstelsel correleert de vingerafdrukken met de kwetsbaarheden om u te helpen bepalen of een bepaalde host uw risico op netwerkcompromis verhoogt. De Cisco Talos Intelligence Group (Talos) geeft periodieke updates voor de VDB uit.

Het wordt aanbevolen om de automatische planner tijdens het instapproces in staat te stellen om regelmatig te controleren op en toe te passen security database updates. Dit zorgt ervoor dat het apparaat up-to-date blijft.

Configureren

Configuraties

1. Log in op Firepower Device Manager



Firepower Device Manager

LOG IN

2. Navigeer op het scherm Apparaten naar Updates > Configuratie bekijken.



Interfaces Connected Enabled 3 of 4 View All Interfaces	Routing 1 static route View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname Time Services SSL Settings See more
Smart License Unregistered View Configuration	Backup and Restore Last Backup: 07 Nov 2023 View Configuration	Troubleshoot Oct 10 2023, 02:44 pm RE-REQUEST FILE TO BE CREATED	

3. Ga op het scherm Updates naar VDB > Configureren.

Device Summary
Updates

Geolocation 2020-04-28-002 Latest Update on 16 May 2023 Configure Set recurring updates UPDATE FROM CLOUD	VDB 384.0 Latest Update on 10 Apr 2024 Configure Set recurring updates UPDATE FROM CLOUD	Security Intelligence Feeds Configure Set recurring updates UPDATE FROM CLOUD
System Upgrade Current version 7.0.4-55 There are no software upgrades available on the system. Upload an upgrade file to install. BROWSE	Intrusion Rule 20210503-2107 Latest Update on 16 May 2023 Configure Set recurring updates UPDATE FROM CLOUD	Snort Inspection Engine: 3.1.0.400-12 Downgrade to 2.0 Snort is the main inspection engine in Firepower Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection. See more

4. Wijzig de standaardinstellingen in het scherm Terugkerende updates instellen op uw behoeften en klik op Opslaan.

Set recurring updates ✕

Frequency

Weekly ▾

Days of Week

Sundays ✕ ▾ at 11 ▾ : 00 ▾

Time (UTC-05:00)
America/Mexico_City

Automatically deploy the update.
(**Note:** The deployment will also deploy all pending configuration changes.)

DELETE CANCEL SAVE

Verifiëren

Op het Updates scherm, in de VDB-sectie, wordt de geselecteerde terugkerende update optie weergegeven.

Updates

✔ **Schedule for VDB updates has been created**

Geolocation 2020-04-28-002

Latest Update on 16 May 2023

Configure

Set recurring updates

UPDATE FROM CLOUD



VDB 384.0

Latest Update on 10 Apr 2024



Weekly

on Sundays at 11:00 AM [Edit](#)

(UTC-05:00) America/Mexico_City

UPDATE FROM CLOUD



Probleemoplossing

Indien de automatische VDB-upgrade niet werkt zoals verwacht, kunt u de VDB terugdraaien.

Stappen:

SSH naar het beheerapparaat (FMC, FDM of SFR onbox) CLI

Switch naar expertmodus, en root en stel de terugdraaivariabele in:

```
<#root>
```

```
expert
```

```
sudo su
```

```
export ROLLBACK_VDB=1
```

Bevestig dat het VDB-pakket dat u wilt downgraden naar zich op het apparaat bevindt in /var/sf/updates en installeer het:

```
<#root>
```

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

Volg normale installatiebestanden van vdb op de toepasselijke locatie op /var/log/sf/vdb-*

Nadat VDB is geïnstalleerd, implementeert u het beleid op apparaten.

Op FTD CLI, om de geschiedenis van VDB-installaties te controleren, is een manier om deze directory-inhoud te controleren:

```
root@firepower:/ngfw/var/cisco/implementation/pkg/var/cisco/packers#ls -al
totaal 72912
drwxr-xr-x 5 wortelwortel 130 Sep 1 08:49 .
drwxr-xr-x 4 wortelwortel 34 aug 16 14:40 ..
drwxr-xr-x 3 wortelwortel 18 aug 16 14:40 exporteur-7.2.4-169
-rw-r—r— 1 wortelwortel 2371661 jul 27 15:34 exporteur-7.2.4-169.tgz
drwxr-xr-x 3 wortelwortel 21 aug 16 14:40 vdb-368
-rw-r—r— 1 wortelwortel 36374219 Jul 27 15:34 vdb-368.tgz
drwxr-xr-x 3 wortelwortel 21 Sep 108:49 vdb-369
-rw-r—r— 1 wortelwortel 35908455 Sep 1 08:48 vdb-369.tgz
```

Gerelateerde informatie

[Bijwerken van systeemdatabases](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.