# Konfigurieren eines regelmäßigen Zeitplans für die Datenbankaktualisierung für VDB auf FDM

# Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Konfigurationen
Überprüfung
Fehlerbehebung
Zugehörige Informationen

# Einleitung

In diesem Dokument wird beschrieben, wie Sie einen regelmäßigen Zeitplan für Datenbankaktualisierungen für Regel oder VDB auf FDM konfigurieren.

#### Voraussetzungen

#### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER-Gerätemanager
- Vulnerability Database (VDB)

#### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

• FDM 7.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

### Hintergrundinformationen

Die Cisco Vulnerability Database (VDB) ist eine Datenbank mit bekannten Schwachstellen für anfällige Hosts sowie Fingerprints von Betriebssystemen, Clients und Anwendungen.

Das Firewall-System korreliert die Fingerabdrücke mit den Schwachstellen, um festzustellen, ob ein bestimmter Host das Risiko einer Netzwerkkompromittierung erhöht. Die Cisco Talos Intelligence Group (Talos) führt regelmäßige Updates der VDB durch.

Es wird empfohlen, den automatischen Scheduler während des Onboarding-Prozesses zu aktivieren, um regelmäßig nach Aktualisierungen der Sicherheitsdatenbank zu suchen und diese anzuwenden. So wird sichergestellt, dass das Gerät immer auf dem neuesten Stand ist.

#### Konfigurieren

#### Konfigurationen

1. Melden Sie sich beim FirePOWER Geräte-Manager an.

uluulu cisco⊾
Firepower Device Manager
Username
Password
LOG IN

2. Navigieren Sie im Bildschirm "Geräte" zu "Updates" > "Konfiguration anzeigen".



3. Navigieren Sie im Bildschirm "Updates" zu VDB > Configure.

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	
System Upgrade Current version 7.0.4-55		Intrusion Rule 20210503-210 Latest Update on 16 May 2023	7
There are no software upgrades available Upload an upgrade file to install.	on the system.	Configure Set recurring updates	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 v

4. Ändern Sie im Bildschirm Serienaktualisierungen festlegen die Standardeinstellungen entsprechend Ihren Anforderungen, und klicken Sie auf Speichern.

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

# Überprüfung

Im Bildschirm "Updates" im VDB-Abschnitt wird die ausgewählte Option für regelmäßige Updates angezeigt.

#### Device Summary Updates



#### Fehlerbehebung

Falls das automatische VDB-Upgrade nicht wie erwartet funktioniert, können Sie ein Rollback der VDB durchführen.

Schritte:

SSH an der CLI des verwaltenden Geräts (FMC, FDM oder SFR am Gerät)

Wechseln Sie in den Expertenmodus und in den Root-Modus, und legen Sie die Rollback-Variable fest:

<#root>

expert

sudo su export ROLLBACK\_VDB=1

Überprüfen Sie, ob sich das VDB-Paket, auf das Sie ein Downgrade durchführen möchten, auf dem Gerät in /var/sf/updates befindet, und installieren Sie es:

<#root>

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

Befolgen Sie die normalen vdb-Installationsprotokolle am entsprechenden Speicherort unter /var/log/sf/vdb-\*.

Sobald die VDB-Installation abgeschlossen ist, stellen Sie die Richtlinie auf den Geräten bereit.

Auf der FTD CLI kann man zum Überprüfen des Verlaufs der VDB-Installationen die folgenden Verzeichnisinhalte überprüfen:

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

# Zugehörige Informationen

Aktualisieren von Systemdatenbanken

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.