

設定FDM上VDB的一般資料庫更新排程

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何為FDM上的規則或VDB配置常規資料庫更新計畫。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower裝置管理器
- 漏洞資料庫(VDB)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FDM 7.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

思科漏洞資料庫(VDB)是一個資料庫，列出了易受攻擊主機的已知漏洞，以及作業系統、客戶端和應用程式的指紋。

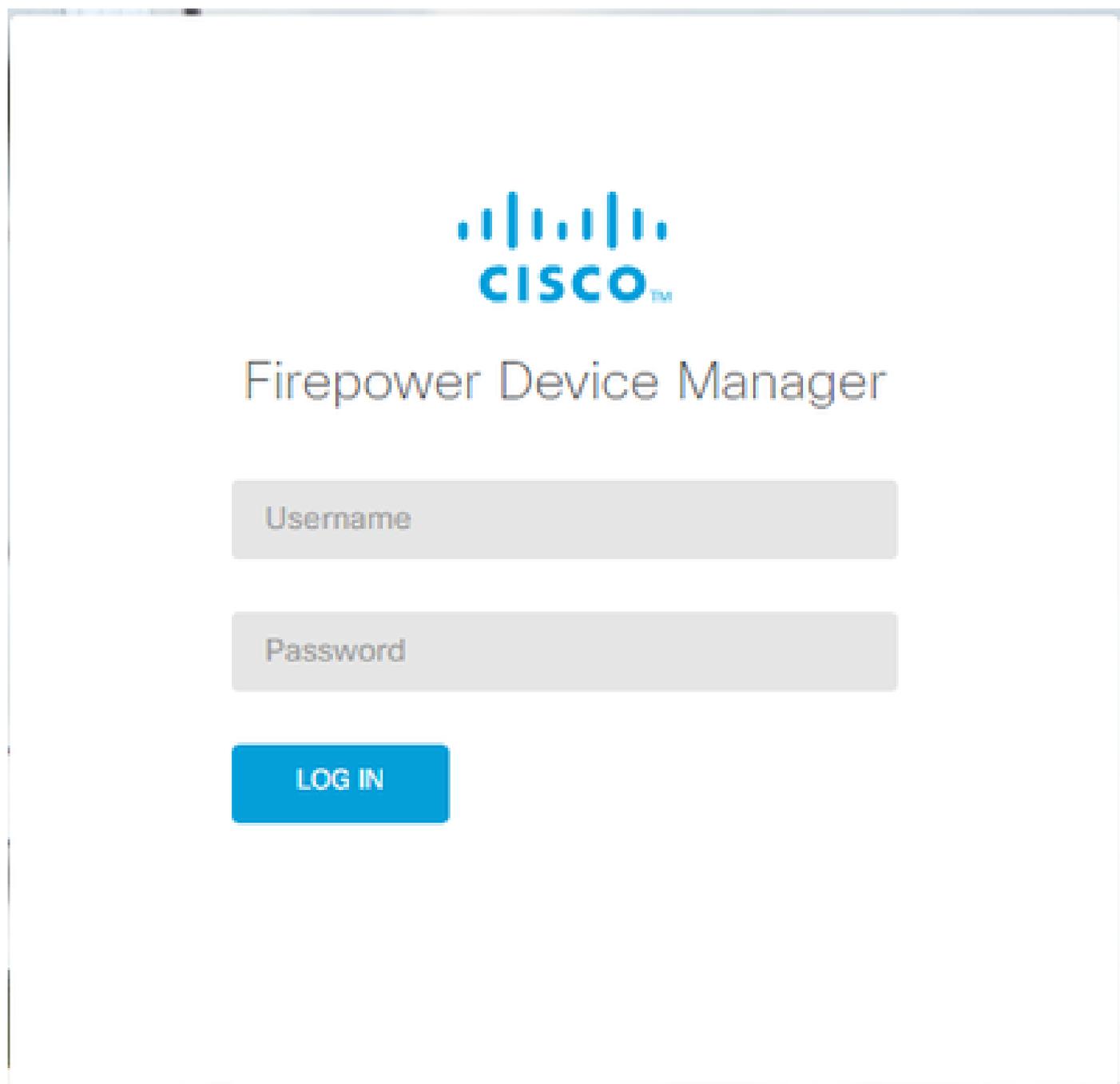
防火牆系統會將指紋與漏洞相關聯，以幫助您確定特定主機是否增加網路受損的風險。Cisco Talos Intelligence Group (Talos)向VDB發出定期更新。

建議在自行啟用過程中啟用自動排程程式，以定期檢查和應用安全資料庫更新。這樣可確保裝置保持最新。

設定

組態

1. 登入Firepower裝置管理器



The screenshot shows the login interface for Cisco Firepower Device Manager. At the top center is the Cisco logo, consisting of a stylized signal icon above the word "CISCO" with a trademark symbol. Below the logo, the text "Firepower Device Manager" is displayed in a large, sans-serif font. Underneath, there are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields are currently empty. Below the password field is a blue button with the text "LOG IN" in white, uppercase letters.

2. 在Devicescreen上，切換作業選項至更新>檢視組態。



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. 在更新螢幕上，導航到VDB >配置。

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. 在設定定期更新螢幕上，根據需要更改預設設定，然後按一下儲存。

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

驗證

在更新螢幕的VDB 部分上，將反映所選的反覆更新選項。

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



疑難排解

如果VDB自動升級未按預期運行，您可以回滾VDB。

步驟：

SSH至管理裝置（FMC、FDM或SFR機上盒）CLI

切換到專家模式和root，並設定回滾變數：

```
<#root>
```

```
expert
```

```
sudo su
```

```
export ROLLBACK_VDB=1
```

驗證您想要降級到的VDB軟體套件位於/var/sf/updates中的裝置上，然後進行安裝：

```
<#root>
```

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

在相應位置(位於/var/log/sf/vdb-*)遵循正常的vdb安裝日誌

VDB安裝完成後，將策略部署到裝置。

在FTD CLI上，若要檢查VDB安裝的歷史記錄，一種方法是檢查以下目錄內容：

```
root@firepower : /ngfw/var/cisco/deploy/pkg/var/cisco/packages#ls -al
總72912
drwxr-xr-x 5 根根 130 Sep 1 08:49 。
drwxr-xr-x 4 根根 34 Aug 16 14:40 。
drwxr-xr-x 3 root 2016年8月18日 14:40 exporter-7.2.4-169
-rw-r - r - 1 根根 2371661 7月27日 15:34 exporter-7.2.4-169.tgz
drwxr-xr-x 3 root 21 Aug 16 14:40 vdb-368
-rw-r - r - 1 根根 36374219 7月27日 15:34 vdb-368.tgz
drwxr-xr-x 3 根根 21 Sep 1 08:49 vdb-369
-rw-r - r - 1 根根 35908455 9月1日 08:48 vdb-369.tgz
```

相關資訊

[更新系統資料庫](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。