

Configurar uma Programação de Atualização de Banco de Dados Regular para VDB no FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar um agendamento de atualização de banco de dados regular para Regra ou VDB no FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Gerenciador de dispositivos Firepower
- Banco de dados de vulnerabilidade (VDB)

Componentes Utilizados

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

- FDM 7.0

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.

Informações de Apoio

O Cisco Vulnerability Database (VDB) é um banco de dados de vulnerabilidades conhecidas para hosts susceptíveis, bem como impressões digitais para sistemas operacionais, clientes e aplicativos.

O sistema de firewall correlaciona as impressões digitais com as vulnerabilidades para ajudá-lo a determinar se um host específico aumenta o risco de comprometimento da rede. O Cisco Talos Intelligence Group (Talos) emite atualizações periódicas para o VDB.

É recomendável ativar o agendador automático durante o processo de integração para verificar e aplicar regularmente atualizações de banco de dados de segurança. Isso garante que o dispositivo permaneça atualizado.

Configurar

Configurações

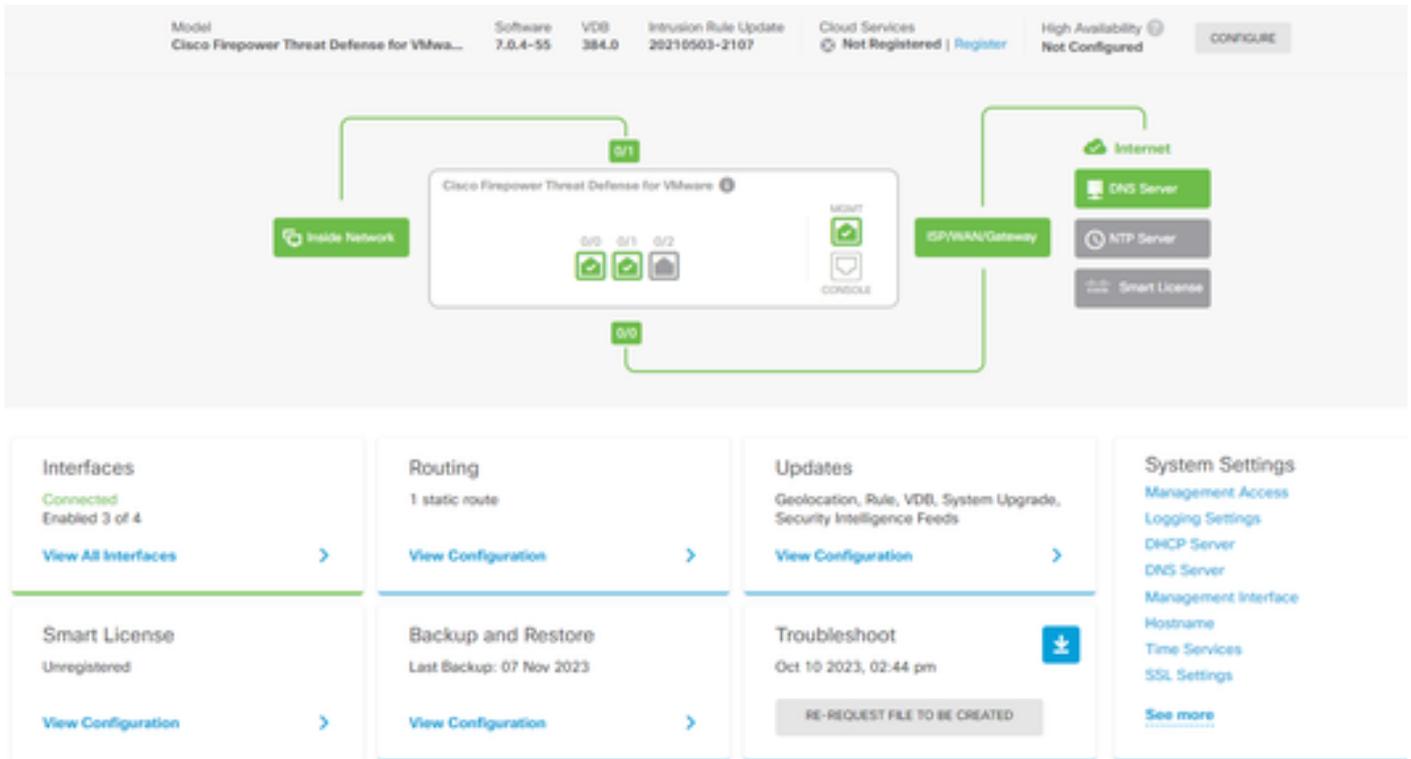
1. Faça login no Firepower Device Manager



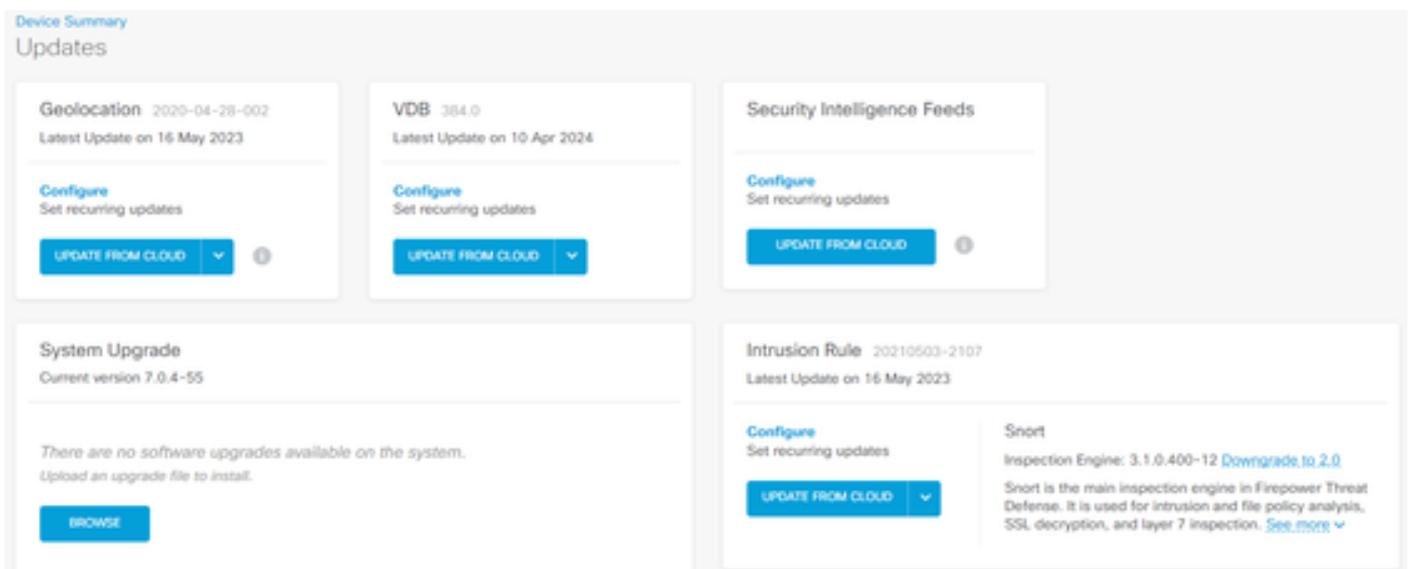
Firepower Device Manager

LOG IN

2. Na tela Dispositivo, navegue para **Atualizações > Exibir configuração**.



3. Na tela Atualizações, navegue para VDB > Configurar.



4. Na tela Definir atualizações recorrentes, altere as configurações padrão de acordo com suas necessidades e clique em Salvar.

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

Verificar

Na tela Updates, na seção VDB, a opção de atualização recorrente selecionada é refletida.

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



Troubleshooting

Caso a atualização automática do VDB não esteja funcionando conforme esperado, você poderá reverter o VDB.

Etapas:

SSH para a CLI do dispositivo de gerenciamento (FMC, FDM ou SFR onbox)

Mude para o modo especialista e para a raiz e defina a variável de reversão:

```
<#root>
```

```
expert
```

```
sudo su
```

```
export ROLLBACK_VDB=1
```

Verifique se o pacote VDB para o qual você pretende fazer downgrade está localizado no dispositivo em `/var/sf/updates` e instale-o:

```
<#root>
```

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

Siga os registros normais de instalação do vdb no local aplicável em /var/log/sf/vdb-*

Quando a instalação do VDB for concluída, implante a política nos dispositivos.

Na CLI do FTD, para verificar o histórico de instalações do VDB, uma maneira é verificar o conteúdo destes diretórios:

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

Informações Relacionadas

[Atualizando Bancos de Dados do Sistema](#)

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.