

Configuración de actualizaciones automáticas para la base de datos de vulnerabilidades en FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Visualización de tareas programadas en el calendario](#)

[Procedimiento](#)

[Resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar las actualizaciones automáticas para la base de datos de vulnerabilidades (VDB) en FMC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense (FTD)
- Centro de administración Firepower (FMC)
- Base de datos de vulnerabilidad (VDB)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FMC 7.0
- FTD 7.0

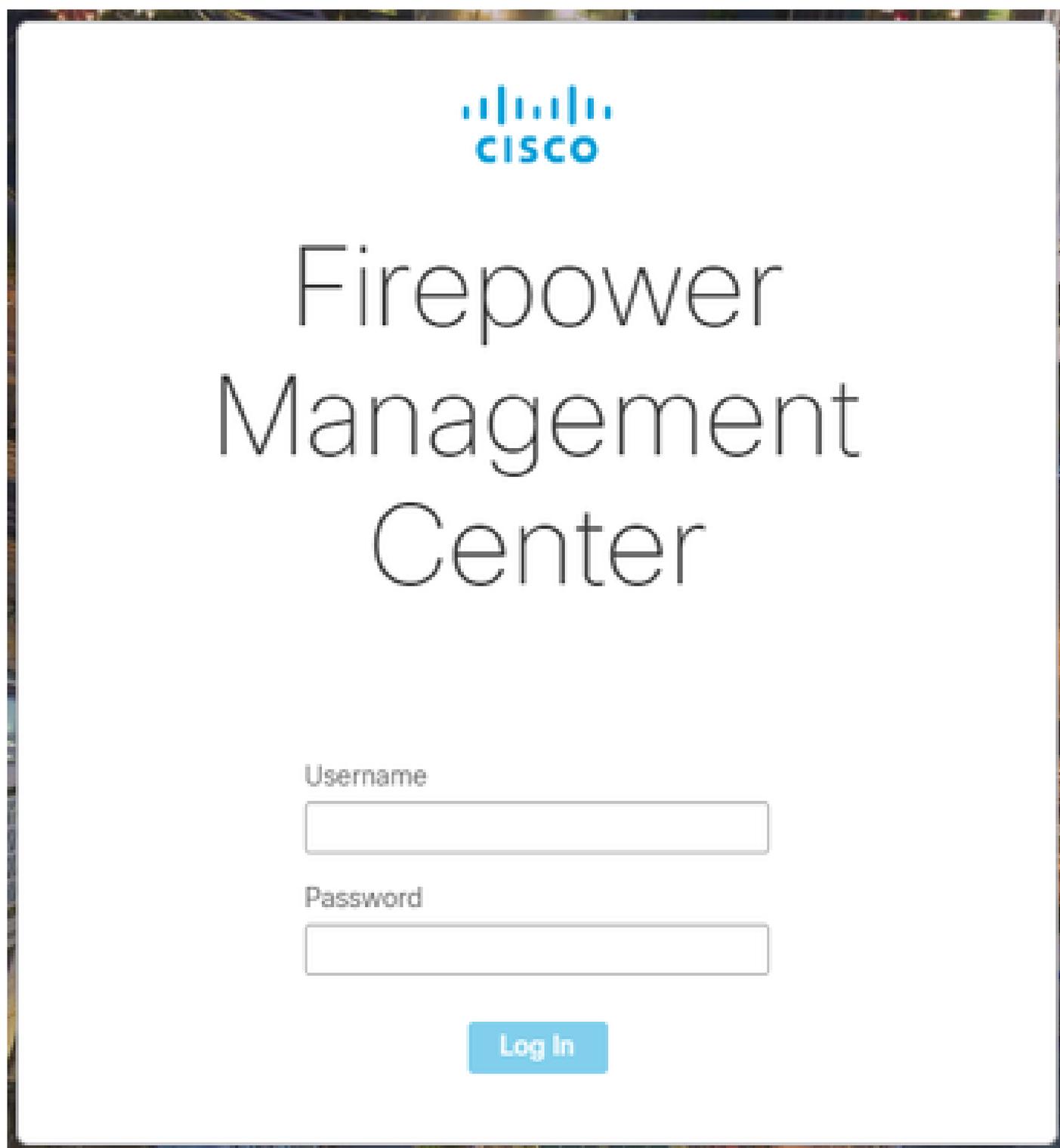
La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

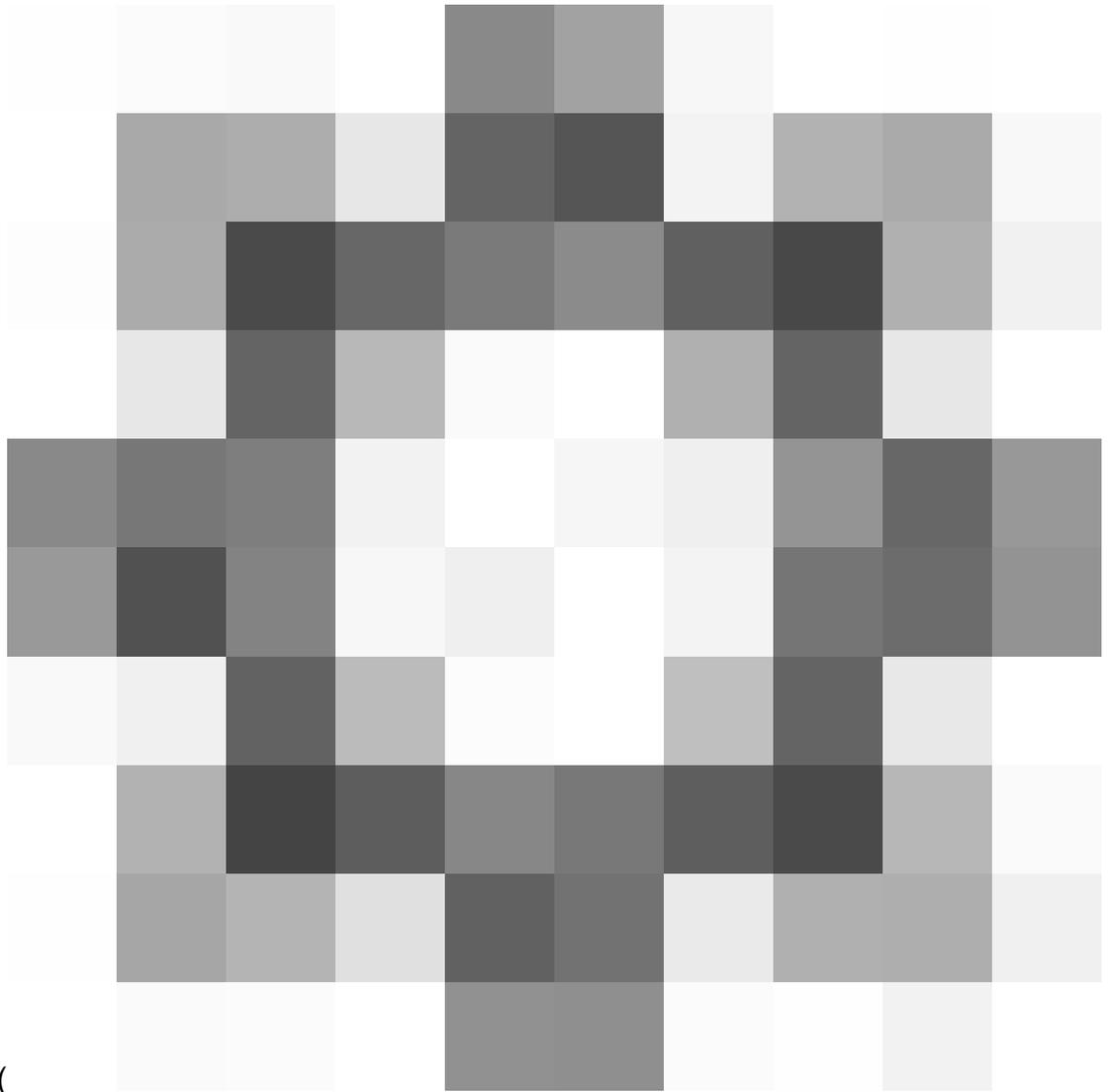
Configurar

Configuraciones

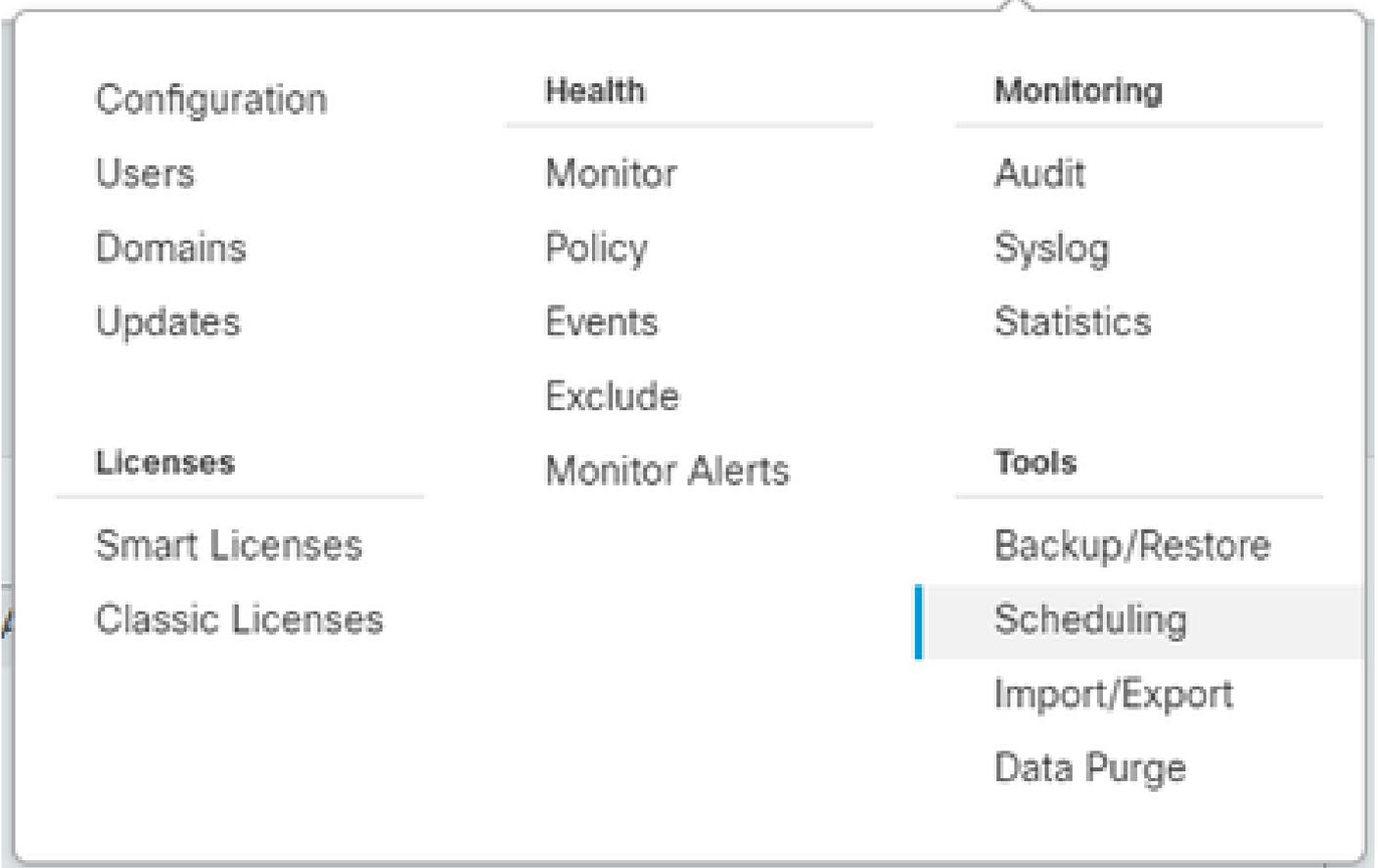
1. Inicie sesión en Firepower Management Center.



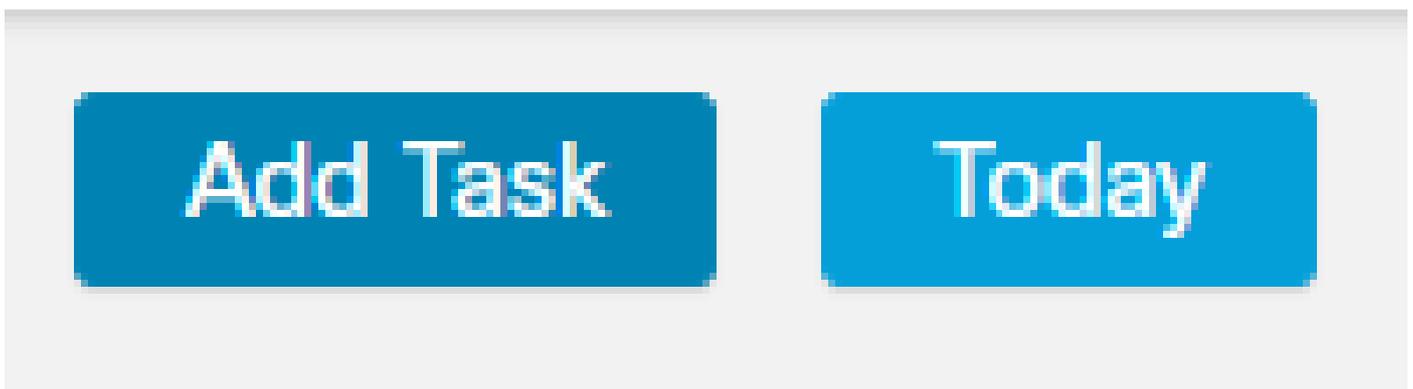
The image shows the login page of the Cisco Firepower Management Center. At the top center is the Cisco logo, consisting of a stylized bridge icon above the word "CISCO" in blue. Below the logo, the text "Firepower Management Center" is displayed in a large, grey, sans-serif font. Underneath the title, there are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields are empty and have a light grey border. At the bottom center of the page is a blue rectangular button with the text "Log In" in white.



2. Acceda a System(
)> Scheduling.



3. En la parte superior derecha de la pantalla Programación, haga clic en el botón Agregar tarea.



4. En la pantalla Nueva Tarea, seleccione Descargar Última Actualización del menú desplegable Tipo de Trabajo y seleccione la configuración que se ajuste a sus necesidades.

En la tarea Planificar para ejecutar, seleccione Recurrente.

En la sección Actualizar elementos, seleccione Base de datos de vulnerabilidades.

A continuación, haga clic en Guardar.

New Task

Job Type

Schedule task to run Once Recurring

Start On

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Update Items Software Vulnerability Database

Comment

Email Status To Not available. You must set up your mail relay host.

5. Repita el paso 3 para volver a la pantalla Nueva Tarea y seleccione Instalar la última actualización en el menú desplegable Tipo de trabajo y utilice la configuración para satisfacer sus necesidades y haga clic en Guardar.

New Task

Job Type

Schedule task to run Once Recurring

Start On

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Update Items Software Vulnerability Database

Device

Comment

Email Status To Not available. You must set up your mail relay host.



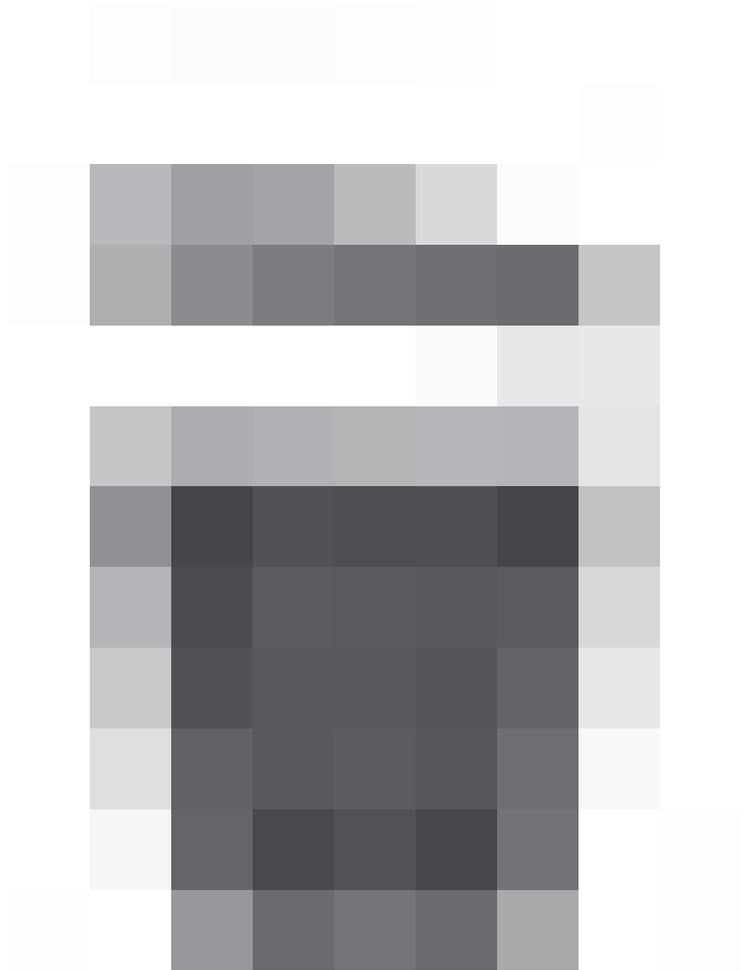
Nota: tenga en cuenta que después de la actualización de VDB, también debe implementar cambios de configuración que puedan interrumpir la inspección y el flujo del tráfico.

Warning

After you update the VDB, you must also deploy configuration changes, which might interrupt traffic inspection and flow.

OK

Puede realizar un ajuste preciso de las tareas programadas haciendo clic en el lápiz de edición (✎)



) o eliminándolas haciendo clic en la papelera () de la sección Detalles de tarea de la pantalla Programación de la pantalla.

Task Details	Name	Start Time	Frequency	Last Run Time	Last Run Status	Next Run Time	Created	Deleted
Download PDF reports	Download PDF reports	06/11/2024 10:00	Every Week on Monday, Wednesday	Not run yet	🛑	Full	Admin	Admin
Export data	Export data reports	06/11/2024 10:00	Every Week on Monday	Not run yet	🛑	Full	Admin	Admin

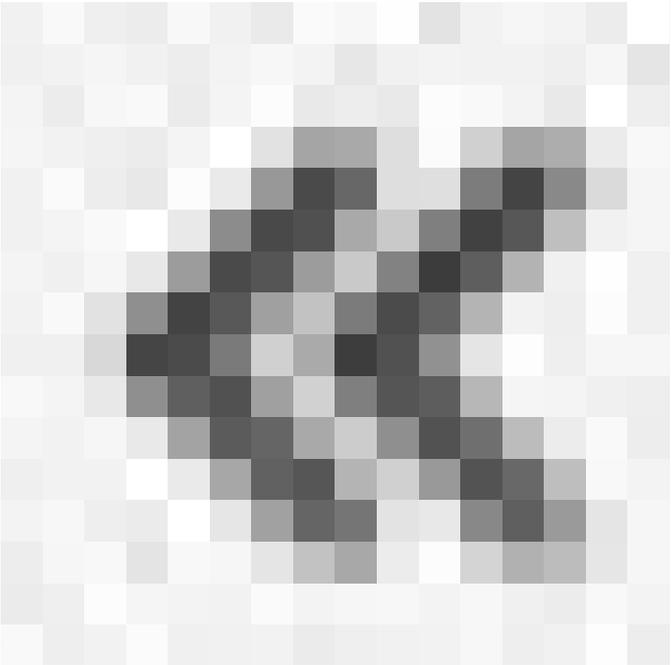
Verificación

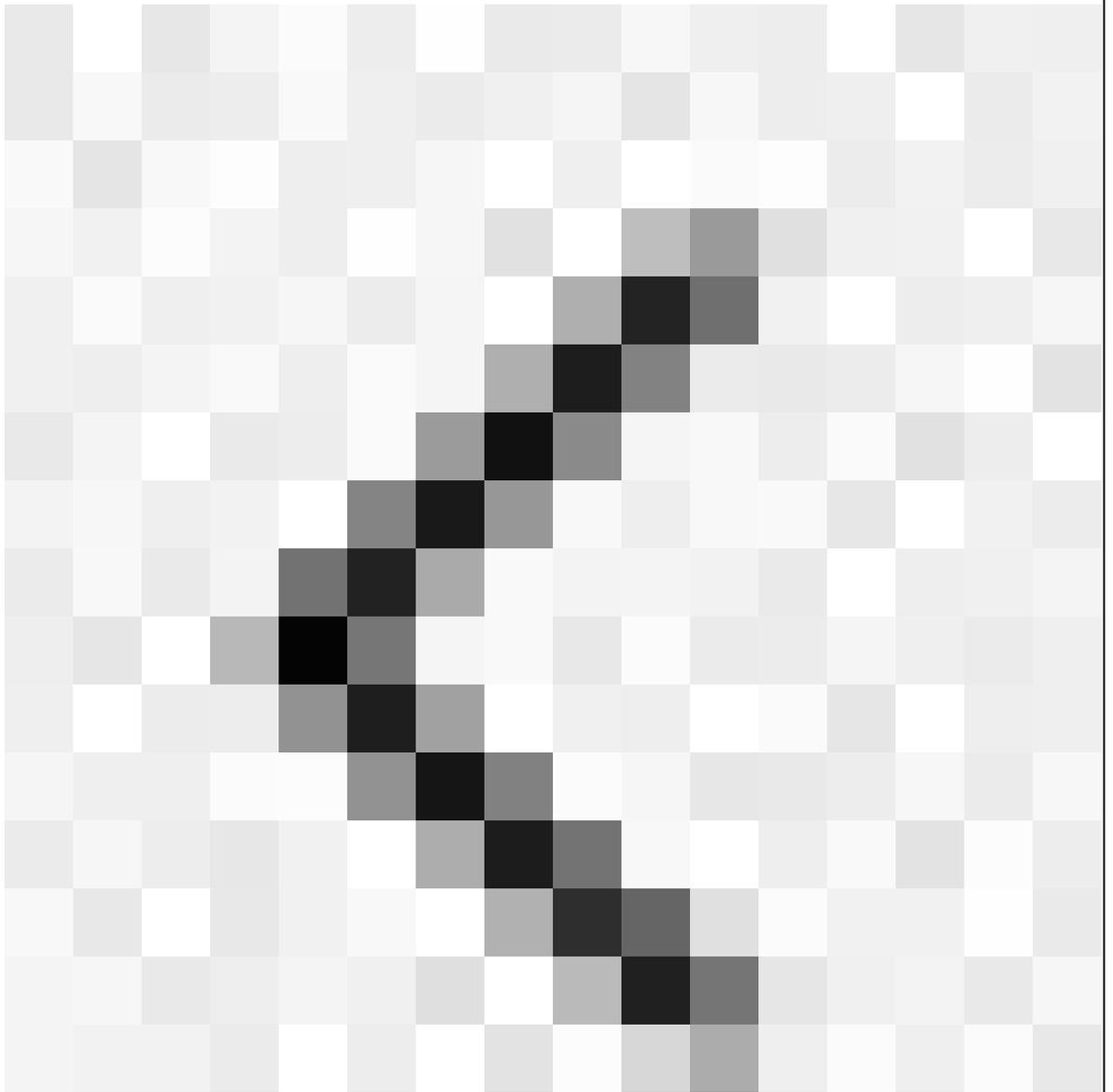
La tarea programada se puede ver en el calendario de la pantalla Programación.

IC	<	2024/4					>	DI
Sun.	Mon.	Tues.	Wed.	Thurs.	Fri.	Sat.		
	1	2	3	4	5	6 Weekly Software Download		
7 Weekly config only backup	8	9	10	11	12	13 Weekly Software Download		
14 Download VOB Update Install VOB Weekly config only backup	15	16	17	18	19	20 Download VOB Update Weekly Software Download		
21 Download VOB Update Install VOB Weekly config only backup	22	23	24	25	26	27 Download VOB Update Weekly Software Download		
28 Download VOB Update Install VOB Weekly config only backup	29	30						

Visualización de tareas programadas en el calendario

Procedimiento

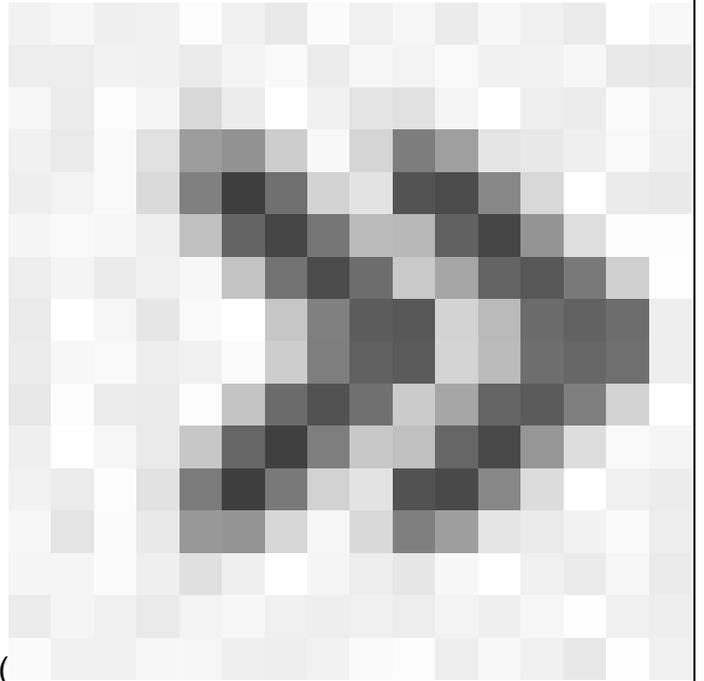
Paso 1	Seleccione Sistema > Herramientas > Programación.
Paso 2	<p>Puede realizar estas tareas mediante la vista de calendario:</p>  <ul style="list-style-type: none"> • Haga clic enDoble flecha izquierda()para retroceder un año. • Haga clic enFlecha única izquierda(



)para retroceder un mes.



- Haga clic en Flecha derecha única()para avanzar un mes.



- Haga clic en Doble flecha derecha() para avanzar un año.
- Haga clic en Hoy para volver al mes y al año actuales.
- Haga clic en Agregar tarea para programar una nueva tarea.
- Haga clic en una fecha para ver todas las tareas programadas para la fecha específica en una tabla de lista de tareas.
- Haga clic en una tarea específica de una fecha para verla en una tabla de lista de tareas.

Resolución de problemas

En caso de que la actualización automática de VDB no funcione como se espera, puede revertir la VDB.

Pasos:

SSH a la CLI del dispositivo de administración (FMC, FDM o bandeja SFR).

Cambie al modo experto y root, y establezca la variable de rollback:

```
<#root>
```

```
expert
```

```
sudo su  
export ROLLBACK_VDB=1
```

Valide que el paquete de VDB al que pretende realizar la actualización se encuentre en el dispositivo en /var/sf/updates e instálelo:

```
<#root>
```

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

Los registros de instalación de vdb normales se pueden encontrar en la ubicación correspondiente en /var/log/sf/vdb-*

Una vez finalizada la instalación de VDB, implemente la política en los dispositivos.

En FMC, para comprobar el estado de instalación de VDB, se puede revisar el contenido de estos directorios:

```
root@firepower:/var/log/sf/vdb-4.5.0-338# ls -la
total 40
drwxr-xr-x 5 root root 4096 15 de mayo de 2023 .
drwxr-xr-x 11 root root 4096 23 de abril 06:00 ..
-rw-r-r— 1 root root 3308 15 de mayo de 2023 flags.conf.complete
drwxr-xr-x 2 root root 4096 instalador de 15 de mayo de 2023
drwxr-xr-x 2 root root 4096 15 de mayo de 2023 post
drwxr-xr-x 2 root root 4096 mayo 15 2023 pre
-rw-r-r— 1 root root 1603 May 15 2023 status.log
-rw-r-r— 1 root root 5703 15 de mayo de 2023 vdb.log
-rw-r-r— 1 root root 5 May 15 2023 vdb.pid
```

En FTD, para verificar el historial de instalaciones de VDB, verifique el contenido de estos directorios:

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

Información Relacionada

[Actualizar base de datos de vulnerabilidades \(VDB\)](#)

[Programación de tareas](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).