Configurare gli aggiornamenti automatici per il database delle vulnerabilità su FMC

Sommario

Introduzione

In questo documento viene descritto come configurare gli aggiornamenti automatici per il database delle vulnerabilità (VDB) in FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- VDB (Vulnerability Database)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FMC 7.0
- FTD 7.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

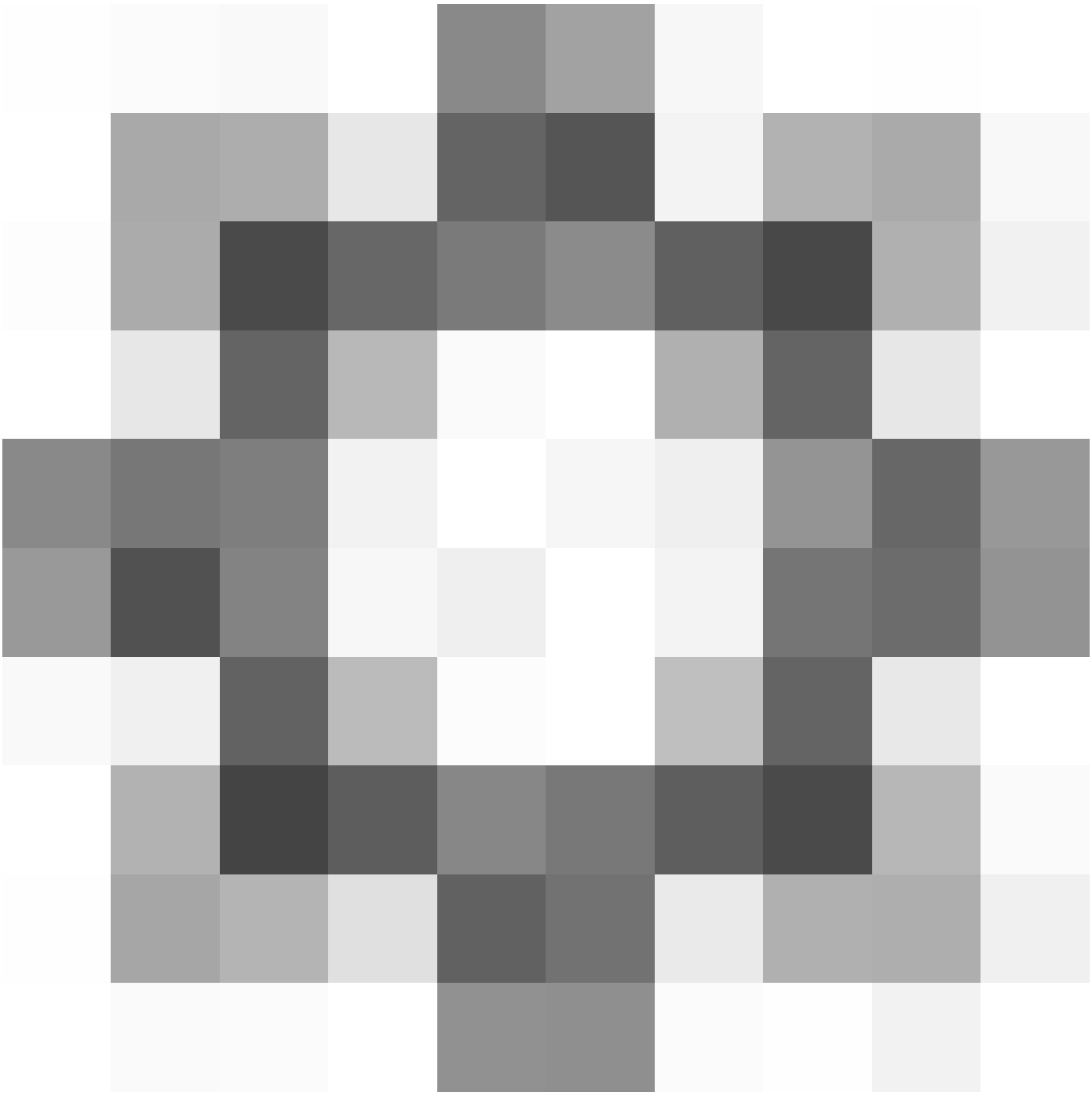
conseguenze derivanti dall'uso dei comandi.

Configurazione

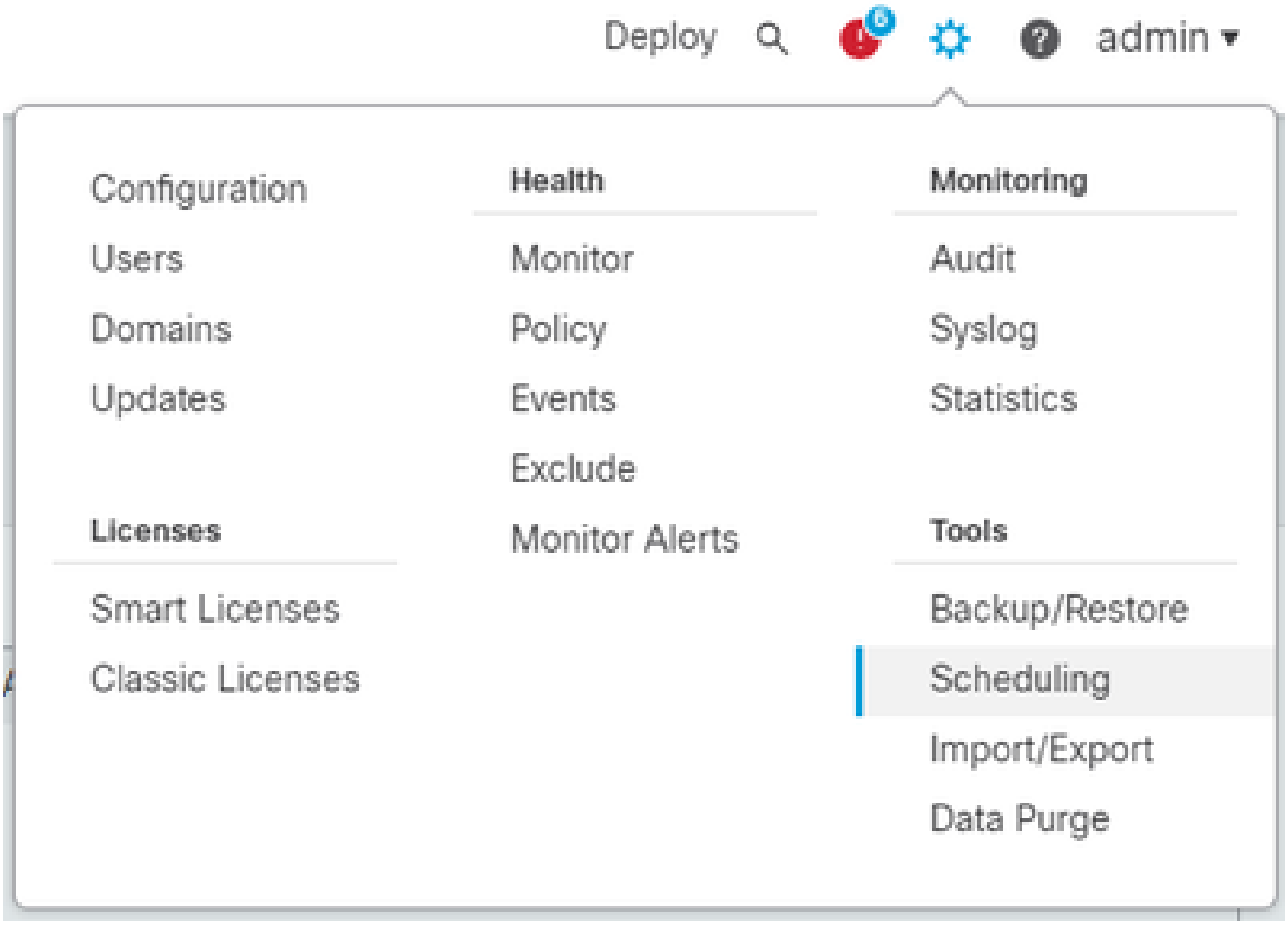
Configurazioni

1. Accedere a Firepower Management Center.

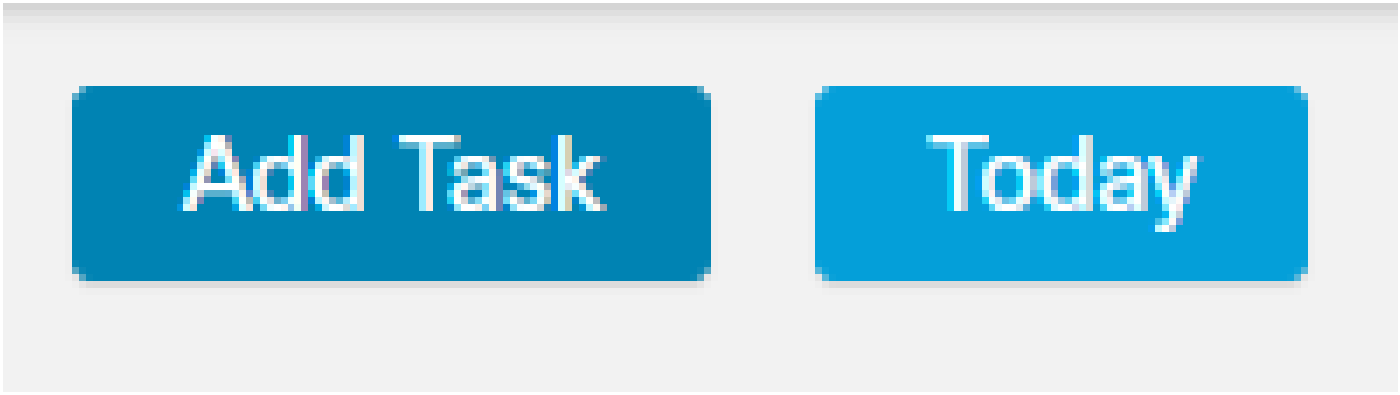
2. Passare a Sistema(



)> Programmazione.



3. Nella parte superiore destra della schermata Programmazione, fare clic sul pulsante Aggiungi operazione.

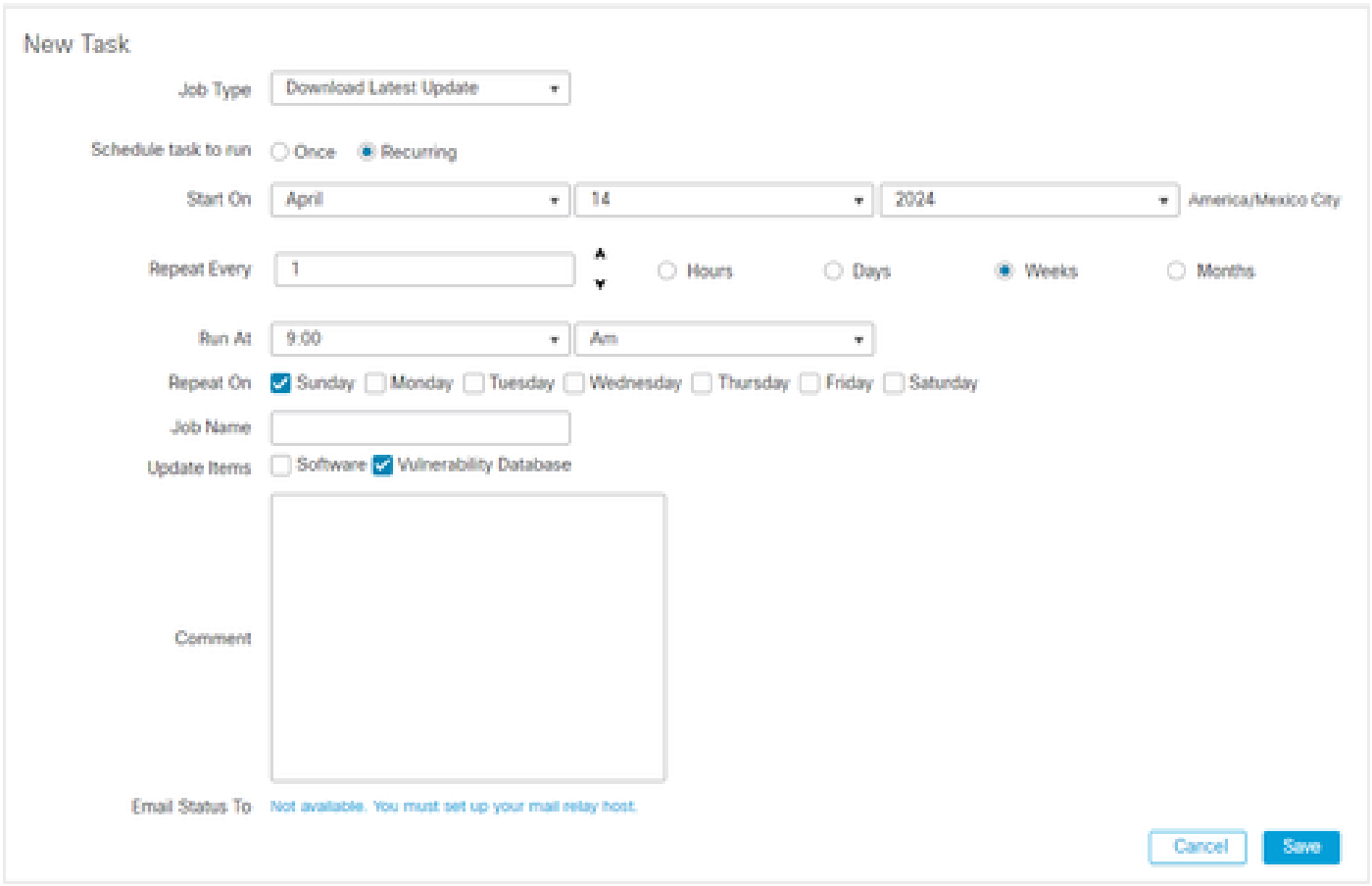


4. Nella schermata New Task, selezionare Download Latest Update (Scarica ultimo aggiornamento) dal menu a discesa Job Type (Tipo di processo) e selezionare le impostazioni appropriate per le proprie esigenze.

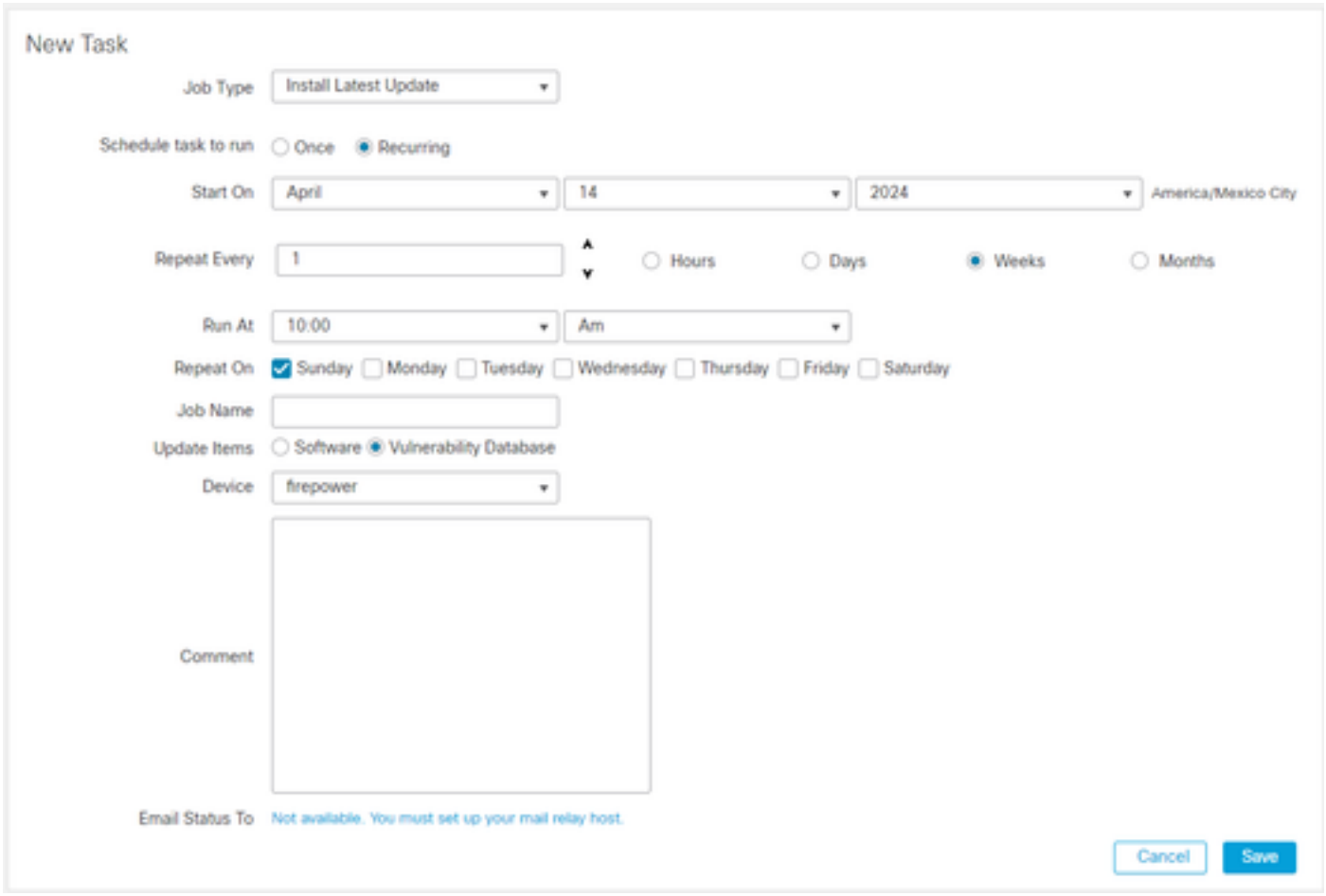
Nell'attività Pianificazione da eseguire selezionare Periodica.

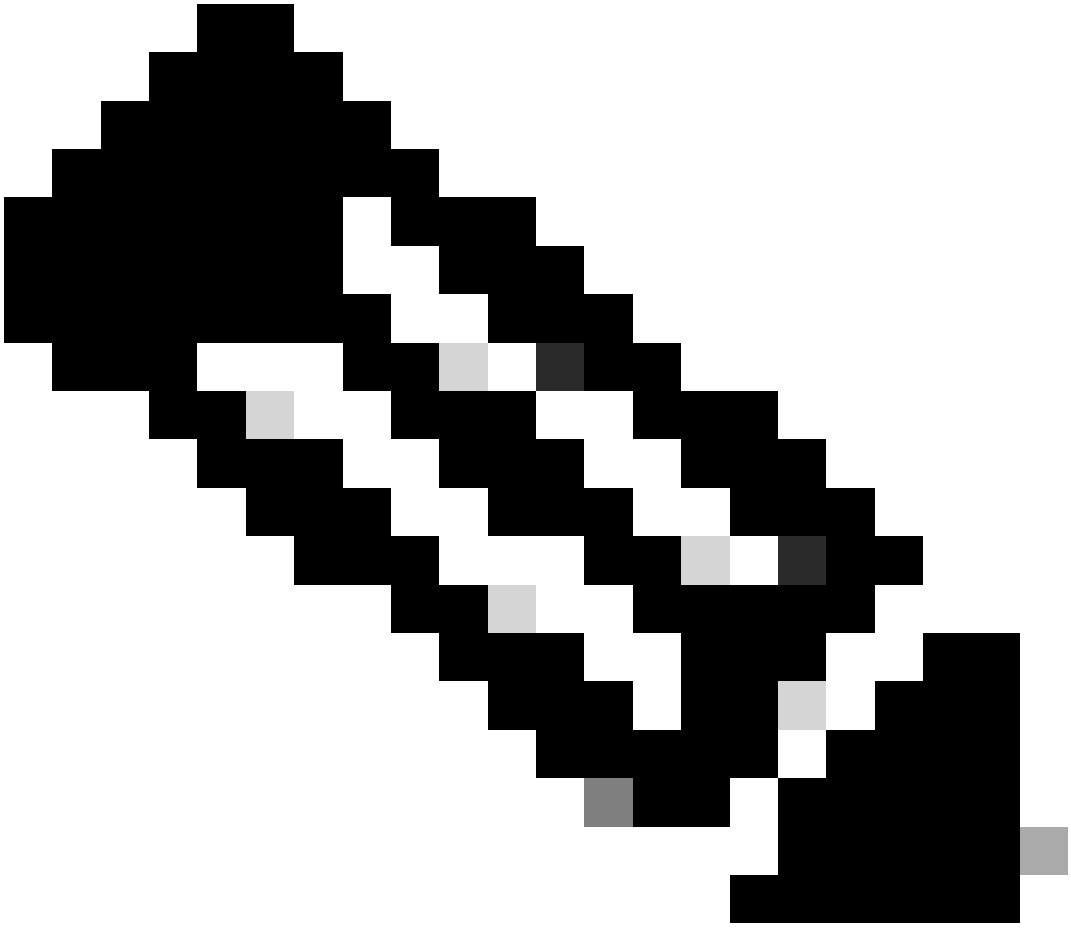
Nella sezione Aggiorna elementi selezionare Database vulnerabilità.

Fare quindi clic su Salva.

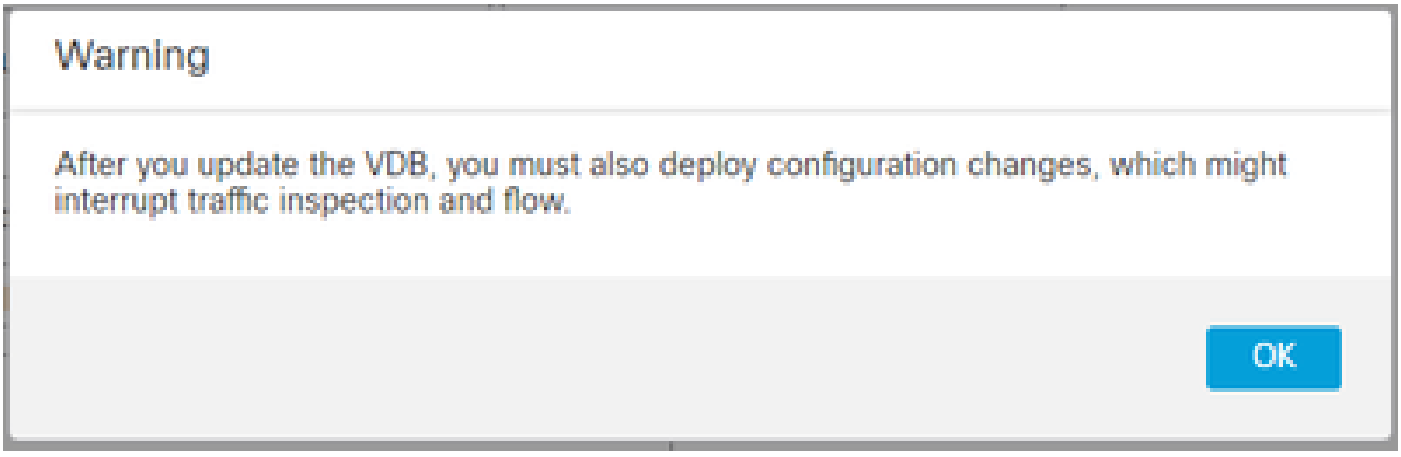


5. Ripetere il punto 3 per tornare alla schermata New Task e selezionare Install Latest Update (Installa l'ultimo aggiornamento) dal menu a discesa Job Type (Tipo di processo) e utilizzare le impostazioni in base alle proprie esigenze, quindi fare clic su Save (Salva).

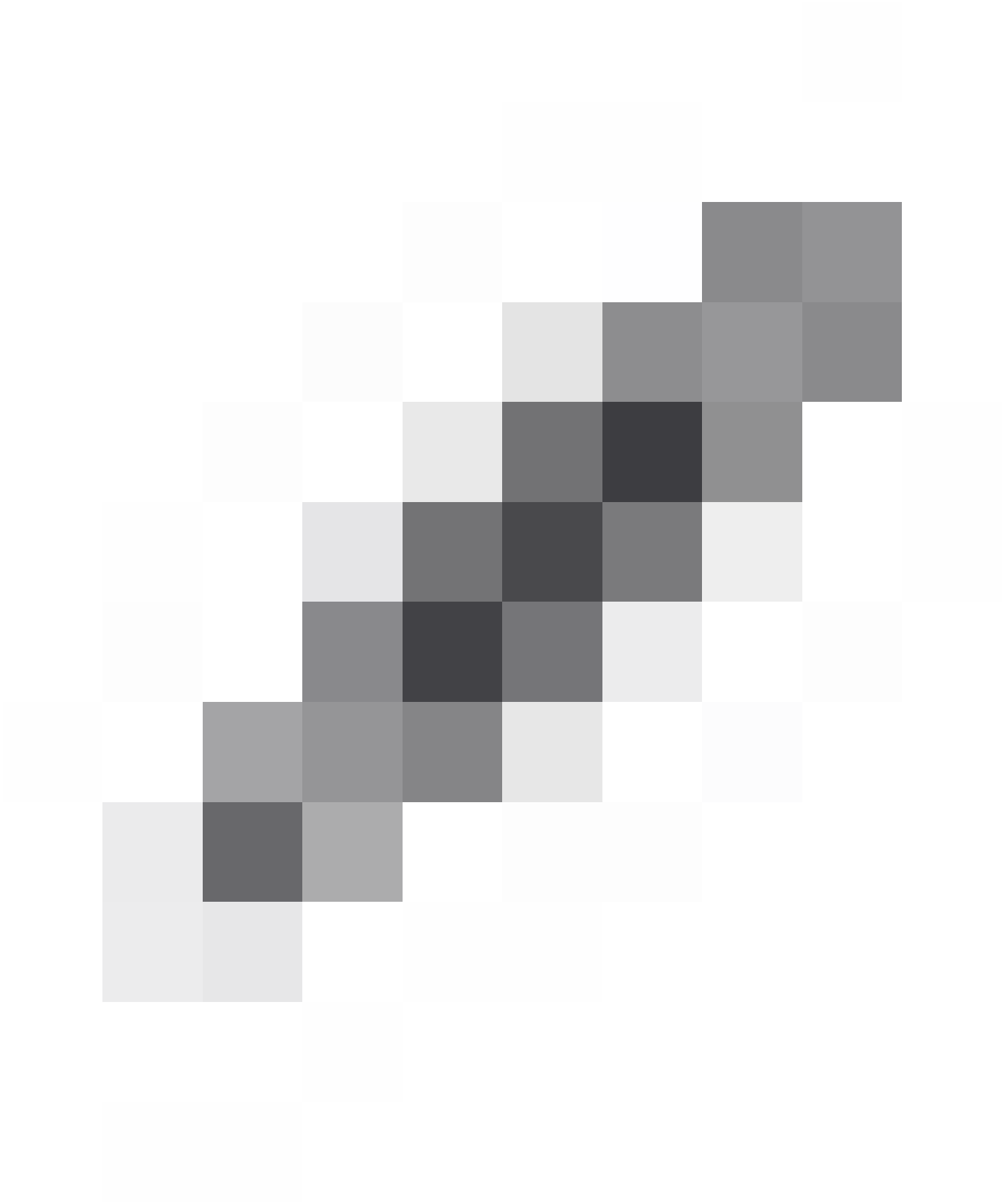

New Task
Job Type
Install Latest Update
Schedule task to run
Once
Recurring
Start On
April
14
2024
America/Mexico City
Repeat Every
1
Hours
Days
Weeks
Months
Run At
10:00
Am
Repeat On
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Job Name
Update Items
Software
Vulnerability Database
Device
firepower
Comment
Email Status To
Not available. You must set up your mail relay host.
Cancel
Save



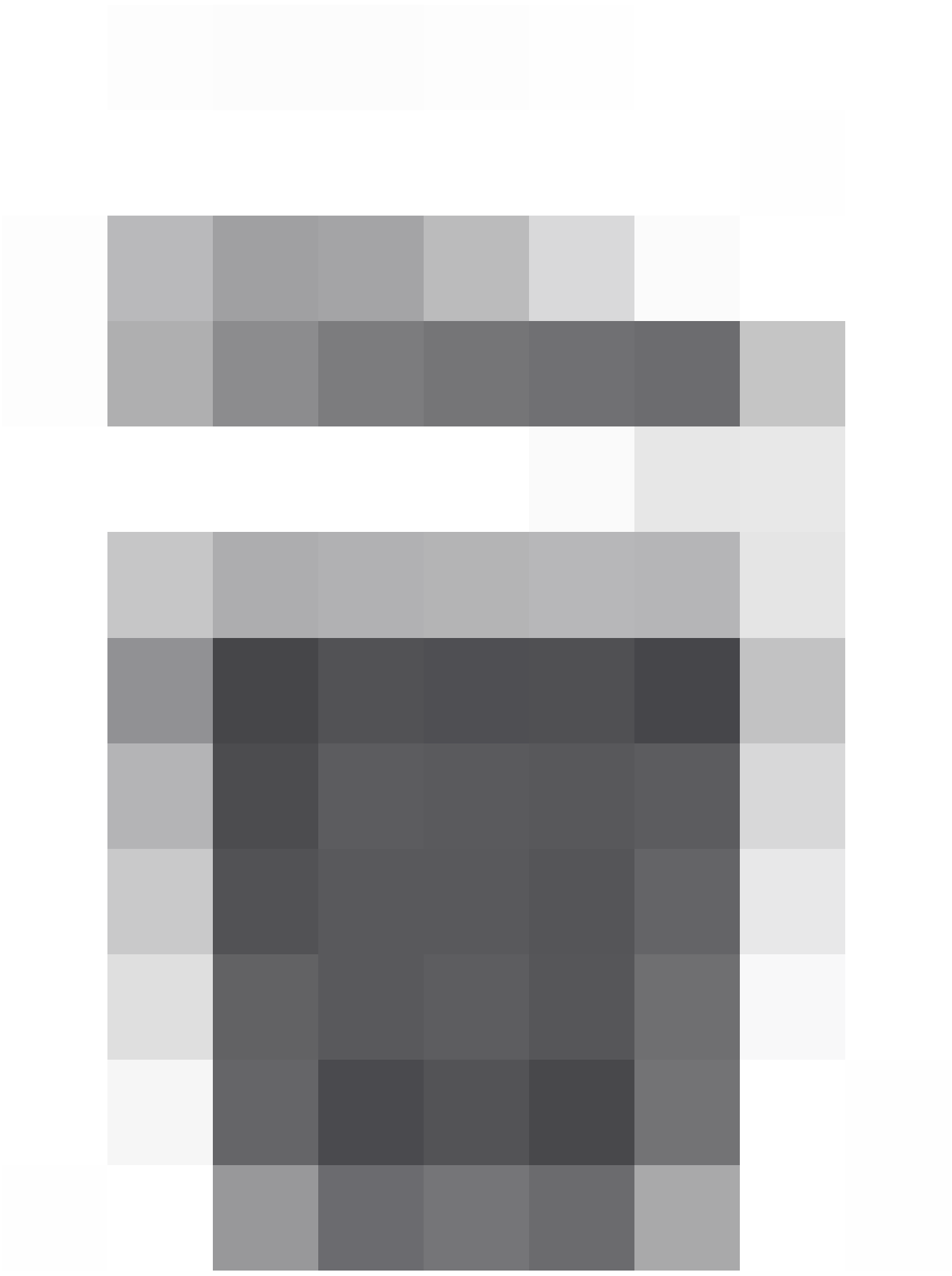
Nota: dopo l'aggiornamento del database virtuale, è necessario distribuire anche le modifiche alla configurazione che possono interrompere l'ispezione e il flusso del traffico.

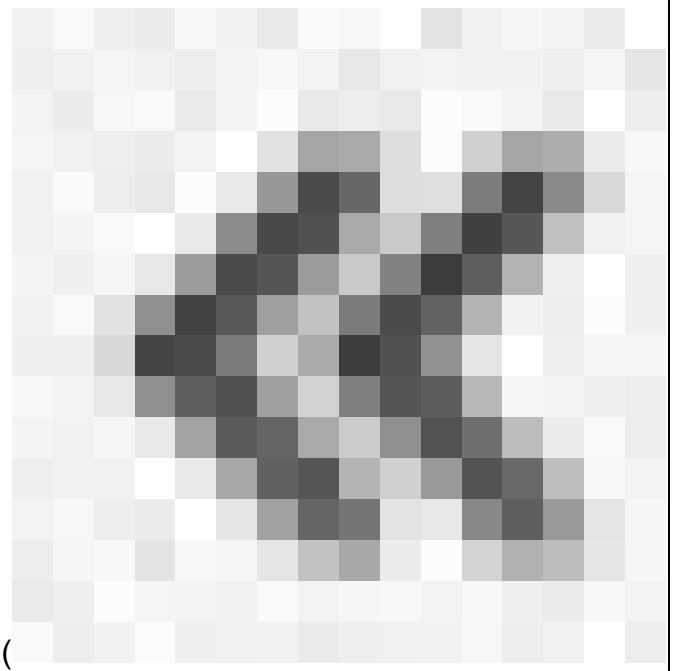
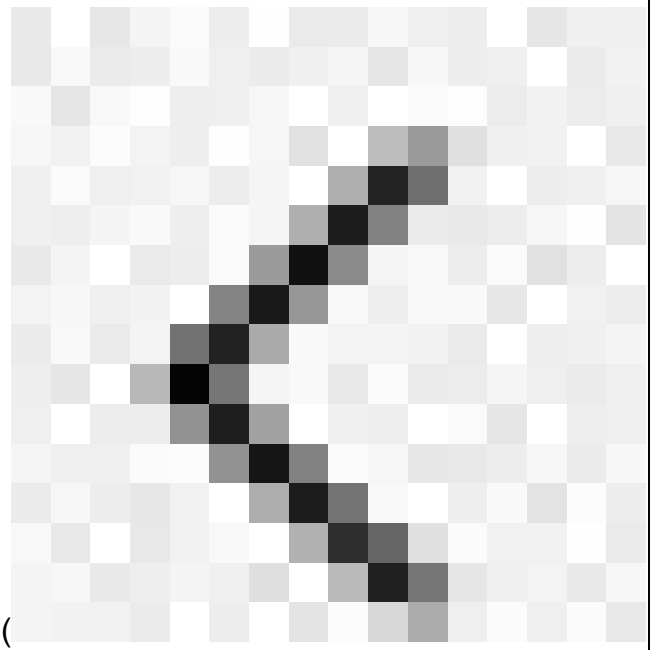


È possibile ottimizzare le operazioni pianificate facendo clic sulla penna di modifica (

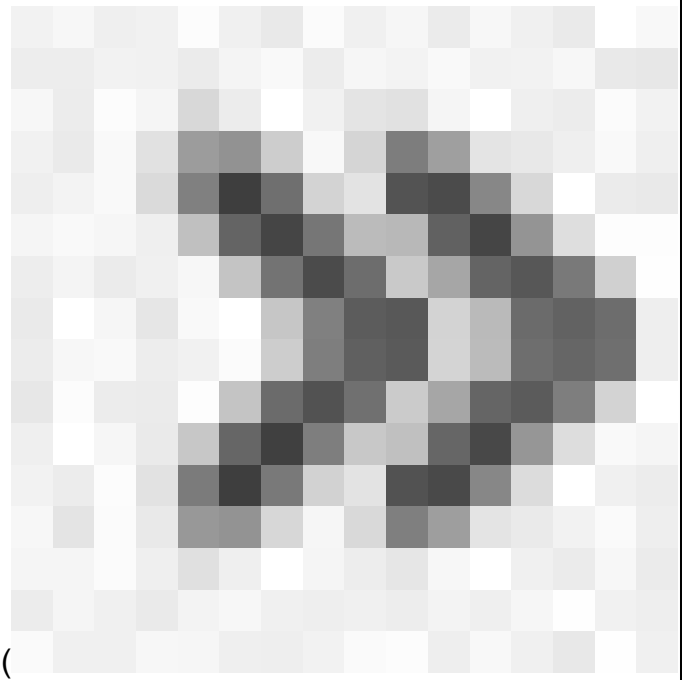


) oppure eliminarle facendo clic sul cestino (



Passaggio 2	È possibile eseguire questi task utilizzando la visualizzazione calendario:  • Fare clic su Doppia freccia sinistra( ) per tornare indietro di un anno.  • Fare clic su Freccia singola sinistra ( ) per tornare indietro di un mese. • Fare clic su Freccia singola a destra(

)per spostarsi in avanti di un mese.



- Fare clic su Doppia freccia destra( )per spostarsi in avanti di un anno.

	• Fare clic su Oggi per tornare al mese e all'anno correnti. • Fare clic su Aggiungi attività per pianificare una nuova attività. • Fare clic su una data per visualizzare tutte le attività pianificate per la data specifica in una tabella di elenchi di attività. • Fare clic su un'attività specifica in una data per visualizzarla in una tabella dell'elenco delle attività.

Risoluzione dei problemi

Se l'aggiornamento automatico di VDB non funziona come previsto, è possibile eseguire il rollback di VDB.

Passaggi:

SSH alla CLI del dispositivo di gestione (FMC, FDM o SFR nella cartella principale).

Passare alla modalità Expert e alla directory principale e impostare la variabile di rollback:

<#root>

expert

sudo su
export ROLLBACK_VDB=1

Verificare che il pacchetto VDB a cui si intende effettuare il downgrade si trovi sul dispositivo in /var/sf/updates e installarlo:

<#root>

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

I normali log di installazione di vdb si trovano nella posizione appropriata in /var/log/sf/vdb-*

Al termine dell'installazione di VDB, distribuire il criterio ai dispositivi.

In FMC, per controllare lo stato di installazione di VDB, è possibile esaminare il contenuto della directory:

root@firepower:/var/log/sf/vdb-4.5.0-338# ls -la
totale 40

drwxr-xr-x 5 root root 4096 15 maggio 2023 .
drwxr-xr-x 11 radice 4096 Apr 23 06:00 ..
-rw-r—r— 1 radice 3308 15 maggio 2023 flags.conf.complete
drwxr-xr-x 2 root root 4096 15 maggio 2023 installer
drwxr-xr-x 2 root root 4096 15 maggio 2023 post
drwxr-xr-x 2 root root 4096 15 maggio 2023 pre
-rw-r—r— 1 radice 1603 15 maggio 2023 status.log
-rw-r—r— 1 radice 5703 15 maggio 2023 vdb.log
-rw-r—r— 1 radice 5 maggio 15 2023 vdb.pid

In FTD, per controllare la cronologia delle installazioni di VDB, controllare il seguente contenuto della directory:

root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages# ls -al
totale 72912
drwxr-xr-x 5 root root 130 set 108:49 .
drwxr-xr-x 4 radice 34 ago 16 14:40 ..
drwxr-xr-x 3 root root 18 ago 16 14:40 export-7.2.4-169
-rw-r—r— 1 radice 2371661 Lug 27 15:34 esportatore-7.2.4-169.tgz
drwxr-xr-x3 radice 21 ago 16 14:40 vdb-368
-rw-r—r— 1 radice 36374219 lug 27 15:34 vdb-368.tgz
drwxr-xr-x 3 root root 21 set 108:49 vdb-369
-rw-r—r— 1 radice 35908455 set 1 08:48 vdb-369.tgz

Informazioni correlate

Aggiorna database vulnerabilità (VDB)

Pianificazione attività

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).