Automatische Updates für Schwachstellendatenbank auf FMC konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration automatischer Updates für die Vulnerability Database (VDB) auf FMC beschrieben.

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

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

- FMC 7.0
- FTD 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,

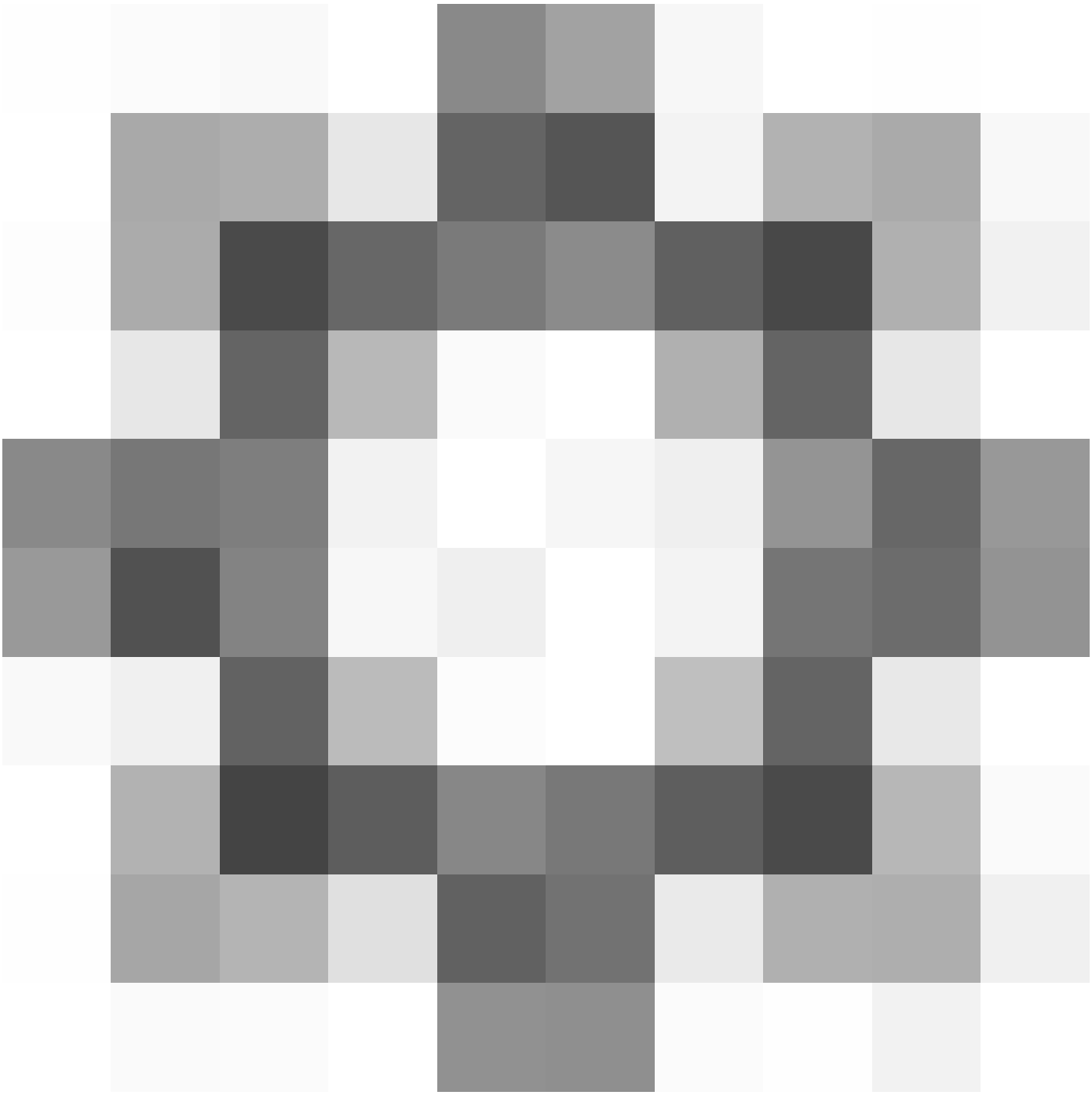
dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

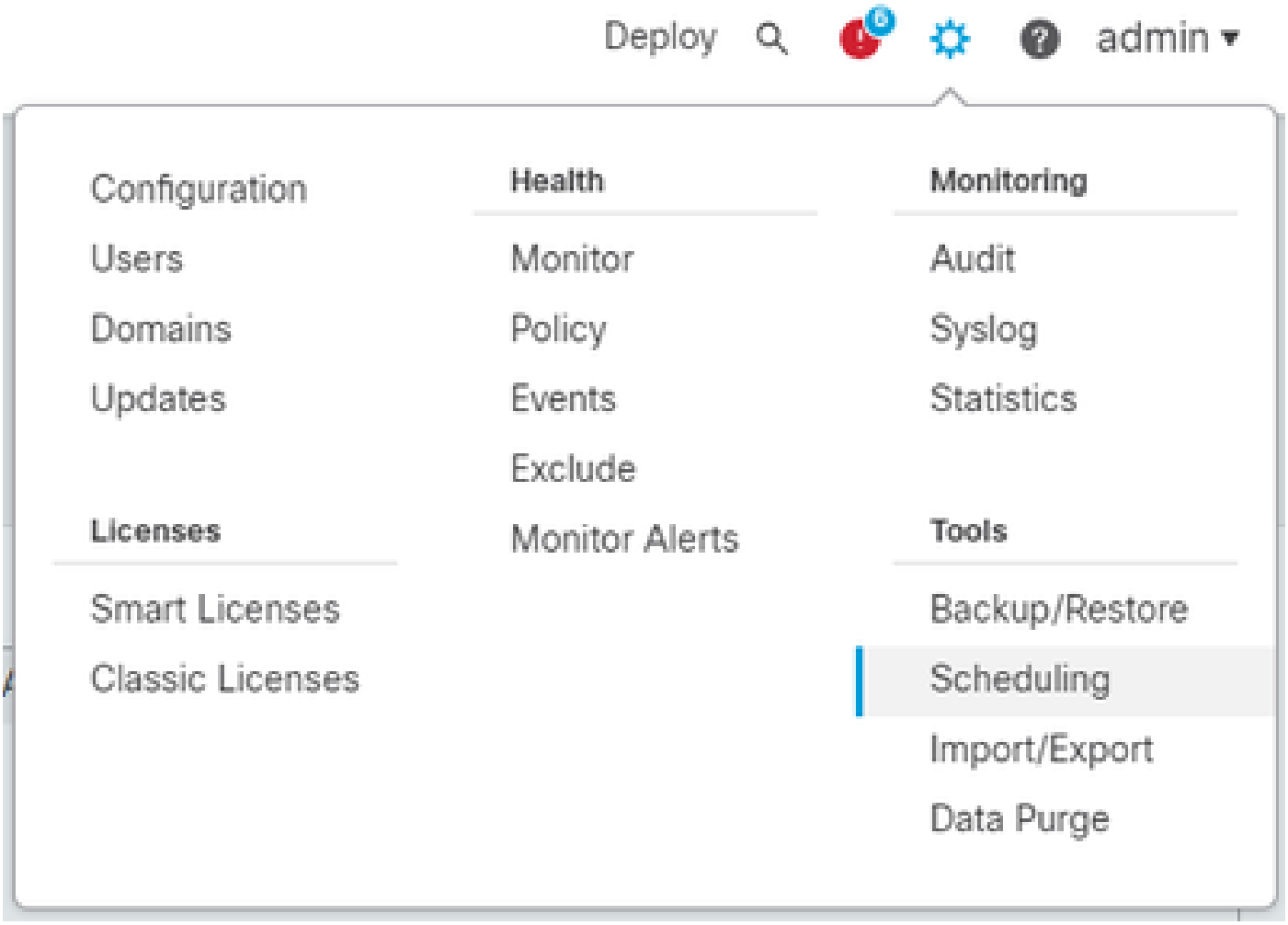
Konfigurationen

1. Melden Sie sich bei FirePOWER Management Center an.

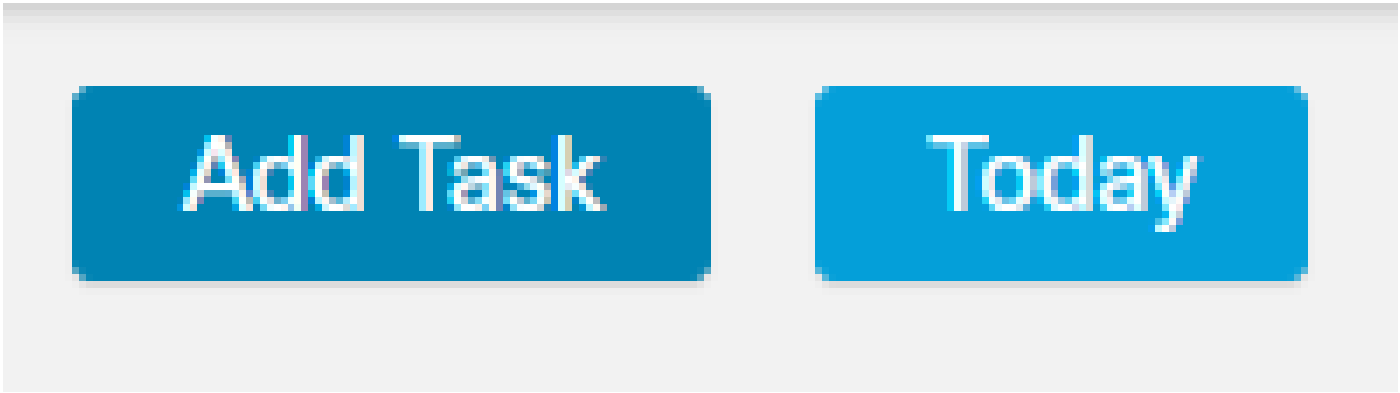
2. Navigieren Sie zu System(



)> Planung.



3. Klicken Sie oben rechts im Bildschirm "Planung" auf die Schaltfläche Task hinzufügen.

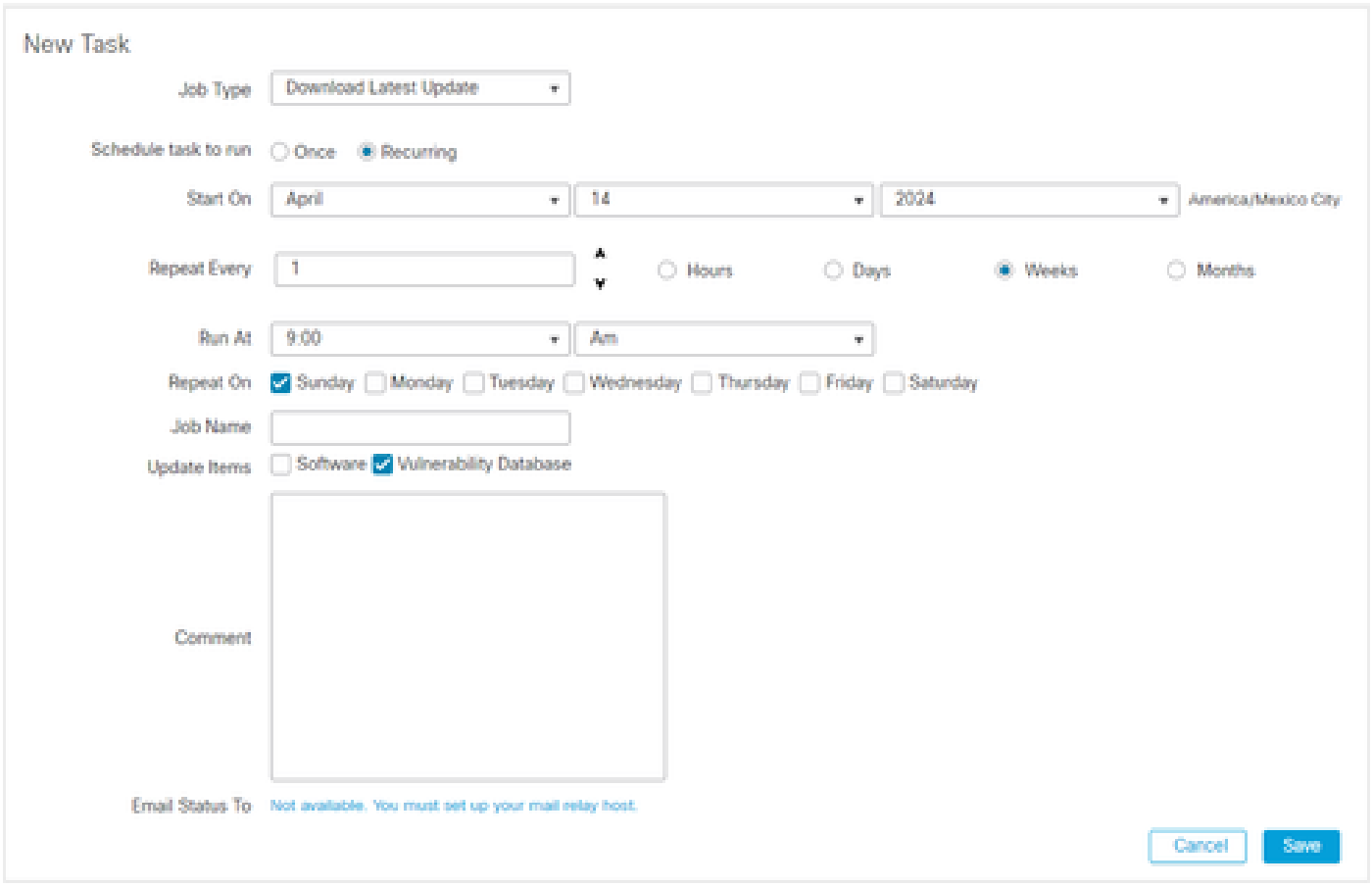


4. Wählen Sie im Bildschirm "Neue Aufgabe" die Option Letzte Aktualisierung aus dem Dropdown-Menü Auftragstyp herunterladen und wählen Sie die gewünschten Einstellungen aus.

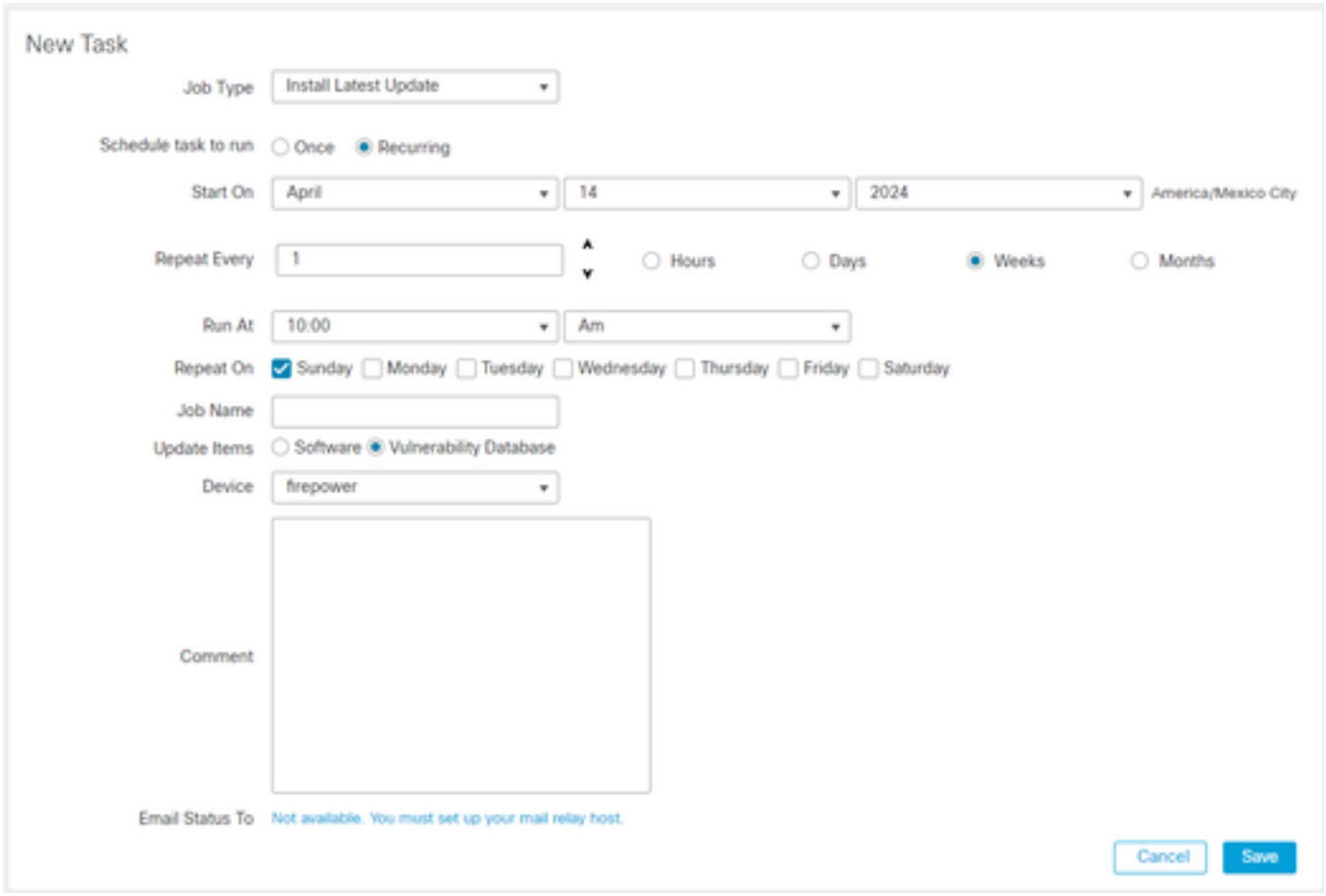
Wählen Sie im Task Zeitplan, der ausgeführt werden soll, die Option Wiederholt aus.

Wählen Sie im Abschnitt "Update Items" (Elemente aktualisieren) die Option Vulnerability Database aus.

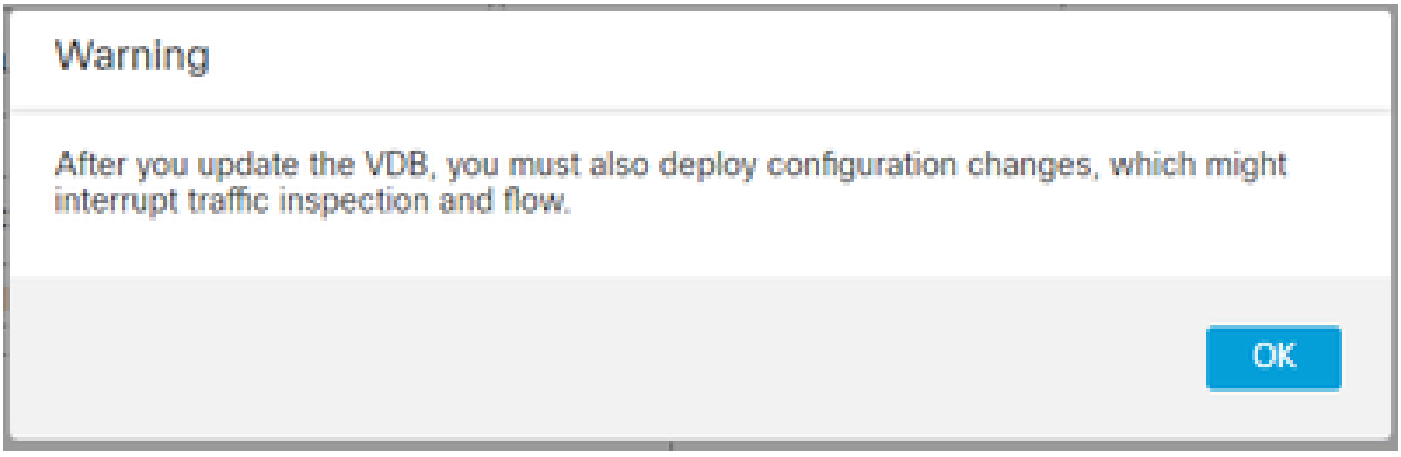
Klicken Sie dann auf Speichern.



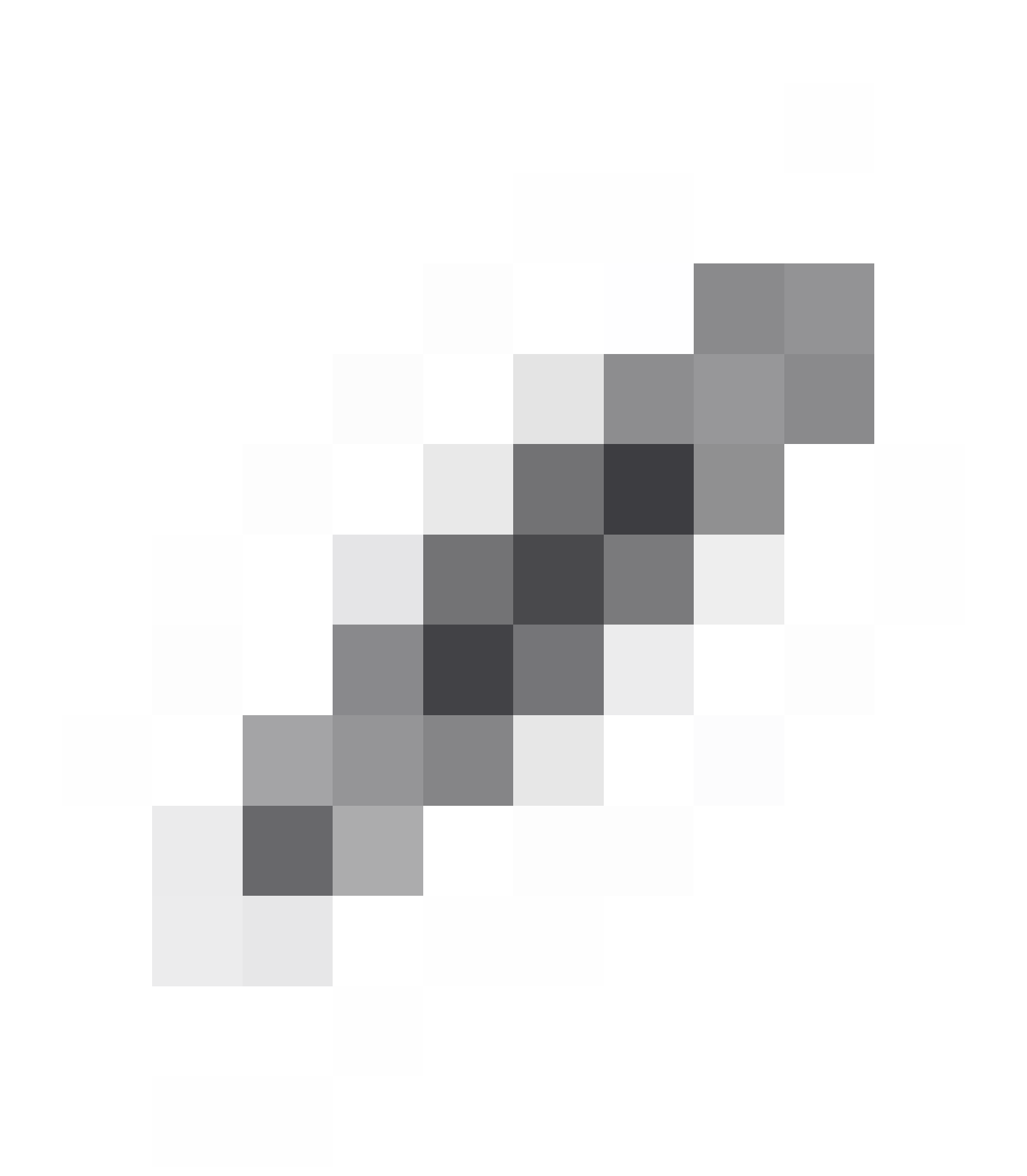
5. Wiederholen Sie Schritt 3, um zum Bildschirm "Neue Aufgabe" zurückzukehren, und wählen Sie im Dropdown-Menü "Auftragstyp" die Option "Neueste Aktualisierung installieren" aus. Verwenden Sie die Einstellungen, um Ihre Anforderungen zu erfüllen, und klicken Sie auf "Speichern".


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

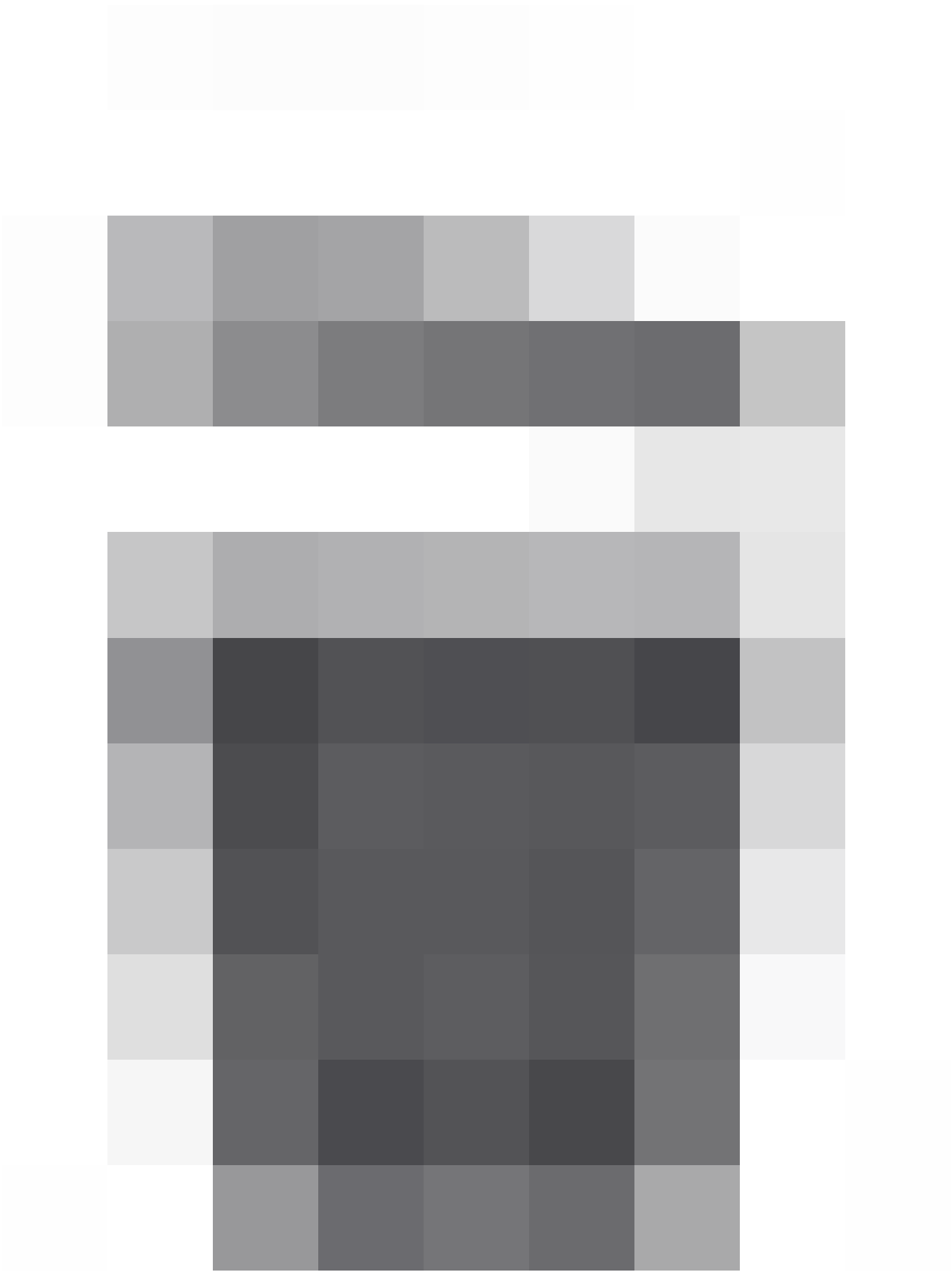
Hinweis: Beachten Sie, dass Sie nach dem VDB-Update auch Konfigurationsänderungen bereitstellen müssen, die die Datenverkehrsanalyse und den Datenfluss unterbrechen können.



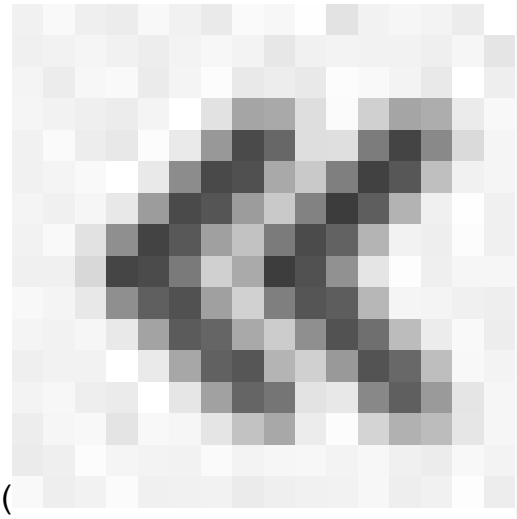
Sie können die geplanten Aufgaben optimieren, indem Sie auf den Stift zum Bearbeiten (

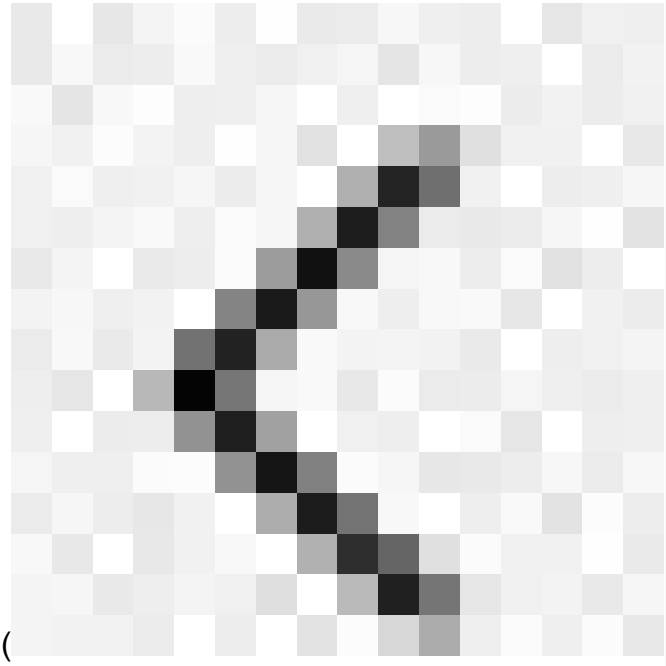


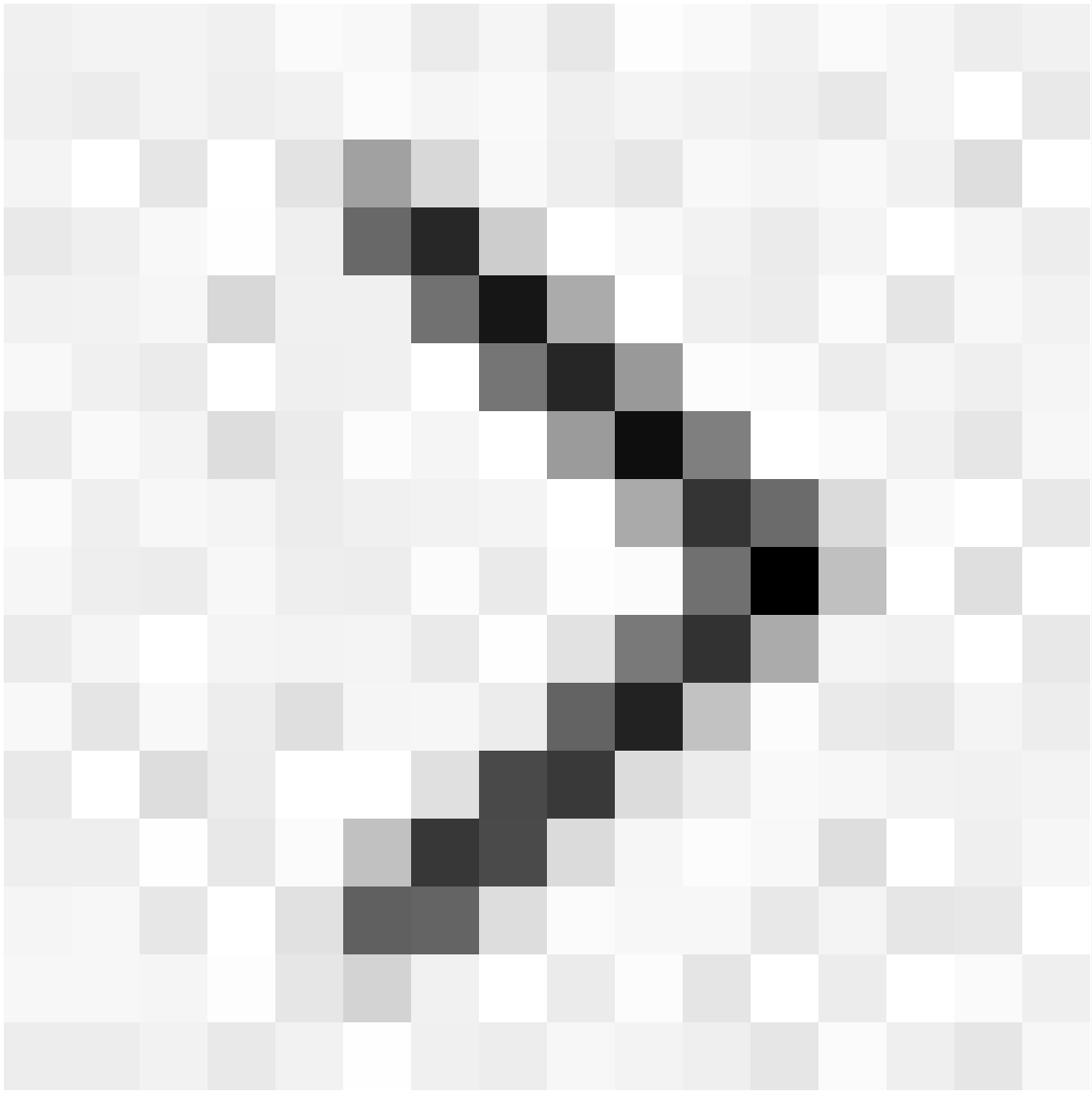
) klicken oder sie löschen, indem Sie im Abschnitt Aufgabendetails des Bildschirms Planung auf den Abfalleimer (



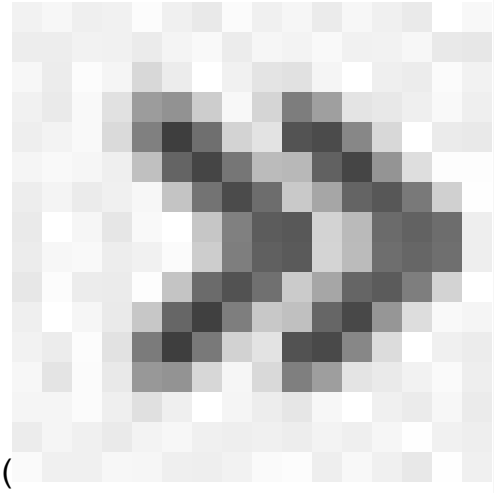
Schritt 2	Sie können diese Aufgaben in der Kalenderansicht ausführen: • Klicken Sie auf den doppelten Pfeil nach links ( ), um ein Jahr zurückzukehren. • Klicken Sie auf den Pfeil nach links ( ), um einen Monat zurückzukehren. • Klicken Sie auf den Pfeil nach rechts (







), um den Vorgang einen Monat lang fortzusetzen.



- Klicken Sie auf den doppelten Pfeil nach rechts ( ), um ein Jahr vorwärts zu fahren.
- Klicken Sie auf Heute, um zum aktuellen Monat und Jahr zurückzukehren.
- Klicken Sie auf Task hinzufügen, um einen neuen Task zu planen.

	• Klicken Sie auf ein Datum, um alle geplanten Aufgaben für das jeweilige Datum in einer Aufgabenlistentabelle anzuzeigen. • Klicken Sie auf eine bestimmte Aufgabe an einem Datum, um sie in einer Aufgabenlistentabelle anzuzeigen.

Fehlerbehebung

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

Schritte:

SSH an die CLI des verwaltenden Geräts (FMC, FDM oder SFR onBox)

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>

Normale vdb-Installationsprotokolle finden Sie am entsprechenden Speicherort unter /var/log/sf/vdb-*.

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

Auf FMC können zur Überprüfung des Installationsstatus von VDB die folgenden Verzeichnisinhalte überprüft werden:

root@firepower:/var/log/sf/vdb-4.5.0-338# ls -la
insgesamt 40
drwxr-xr-x 5 root 4096 15. Mai 2023 .

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

Auf FTD können Sie den Verlauf der VDB-Installationen anhand der 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 14:40 vdb-368
-rw-r-r— 1 root root 36374219 Jul 27 15:34 vdb-368.tgz
drwxr-xr-x 3 root 21 Sep 1 08:49 vdb-369
-rw-r-r— 1 root root 35908455 Sep 1 08:48 vdb-369.tgz

Zugehörige Informationen

Schwachstellendatenbank aktualisieren (VDB)

Aufgabenplanung

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.