在FMC上配置漏洞数据库的自动更新

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 配置

验证

- 查看日历上的计划任务
  - 步骤

故障排除

相关信息

简介

本文档介绍如何在FMC上配置漏洞数据库(VDB)的自动更新。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- 漏洞数据库(VDB)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FMC 7.0
- FTD 7.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

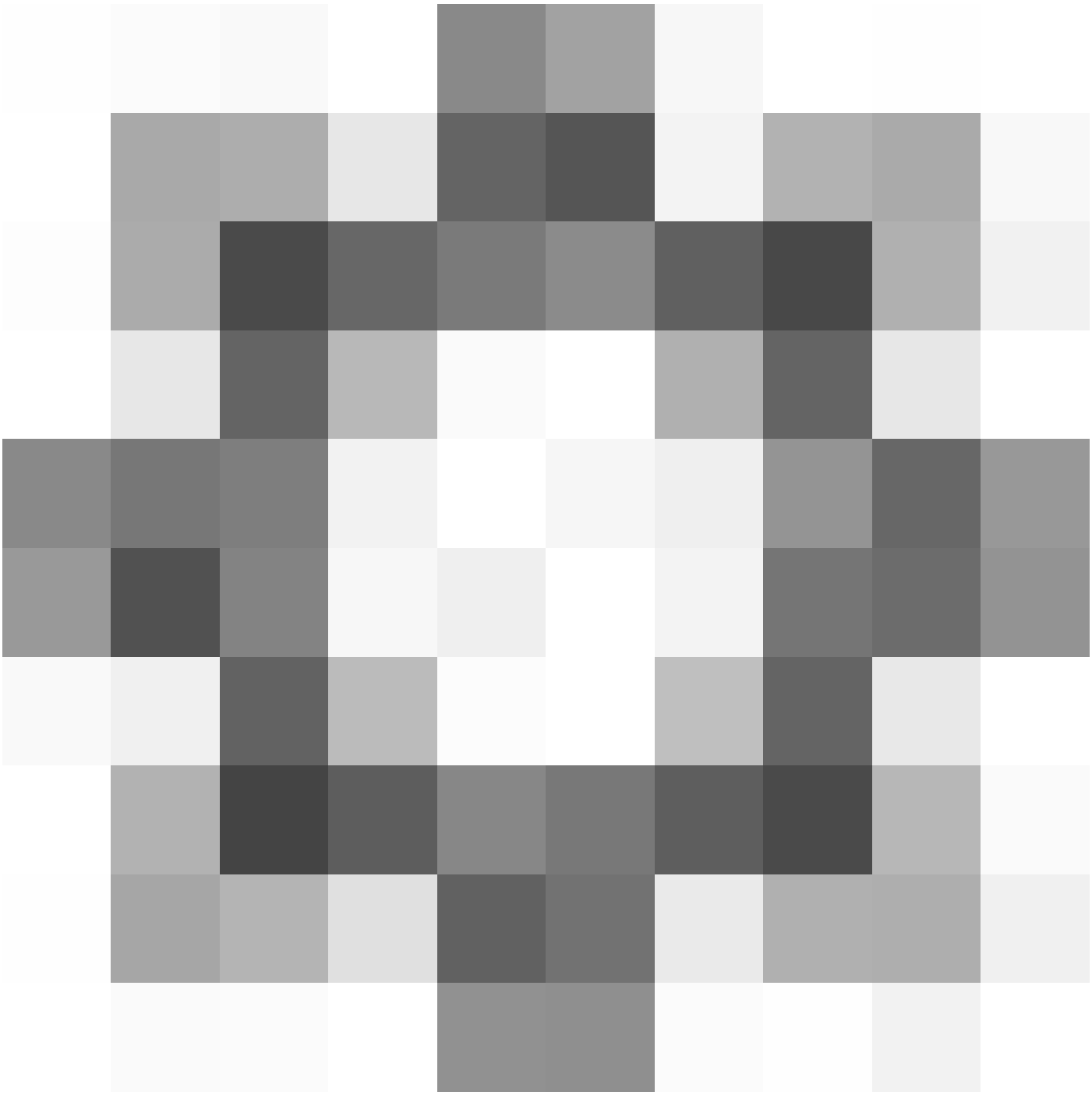
配置

配置

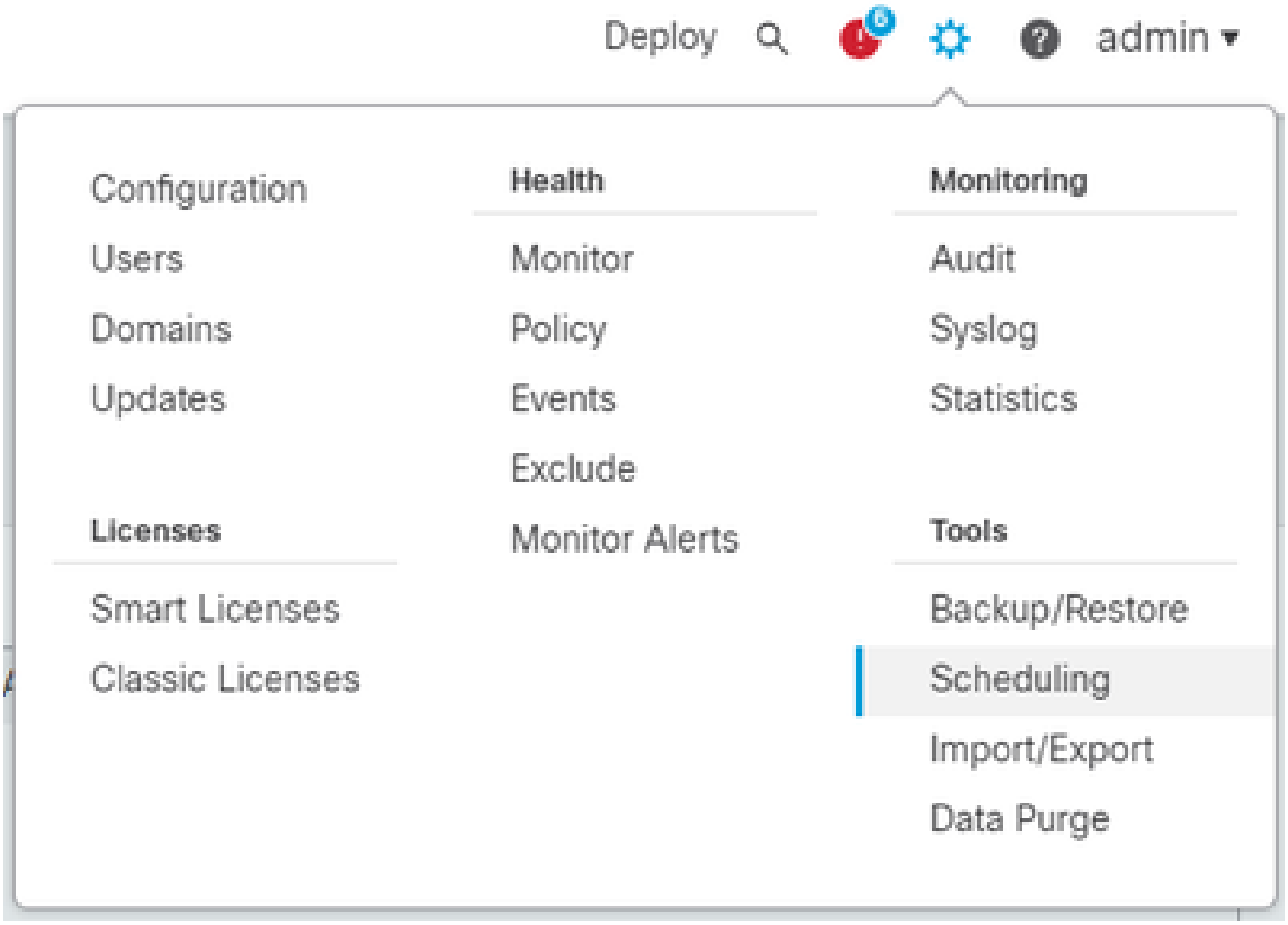
1. 登录Firepower管理中心。



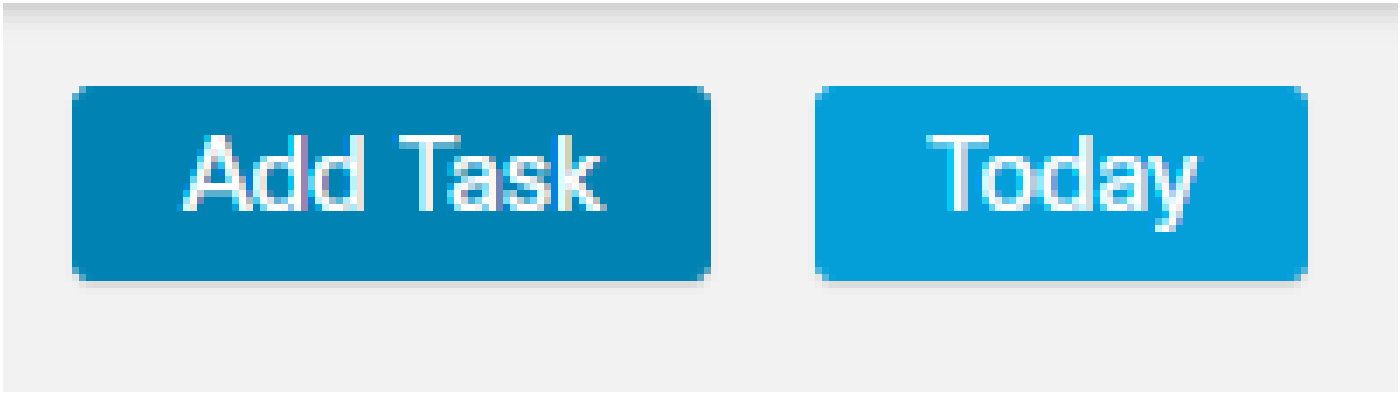
2. 定位至“系统(



)”>“计划”。



3. 在计划屏幕的右上角，单击添加任务按钮。

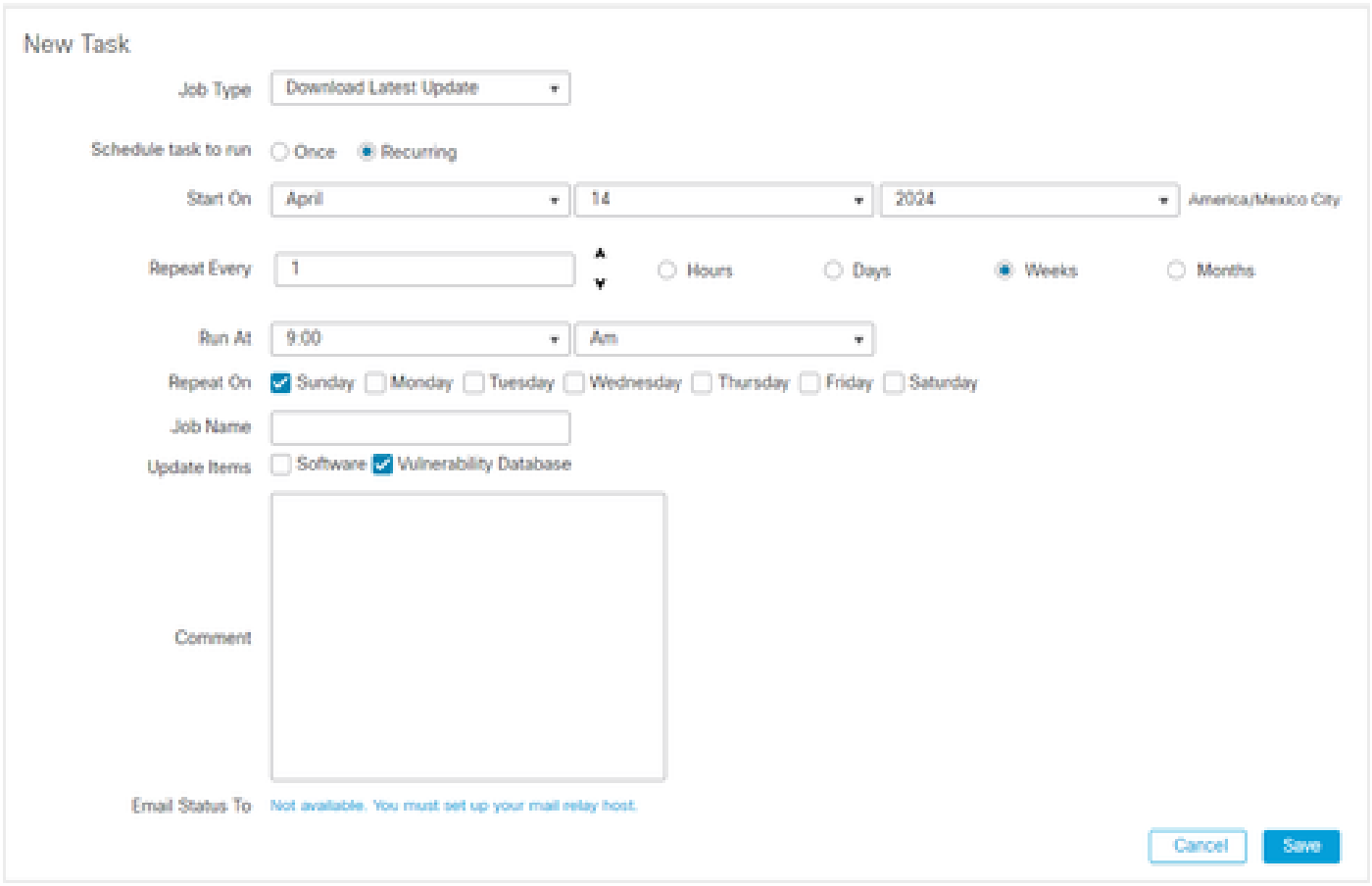


4. 在新任务屏幕上，从作业类型下拉菜单中选择下载最新更新，然后选择适合您的需求的设置。

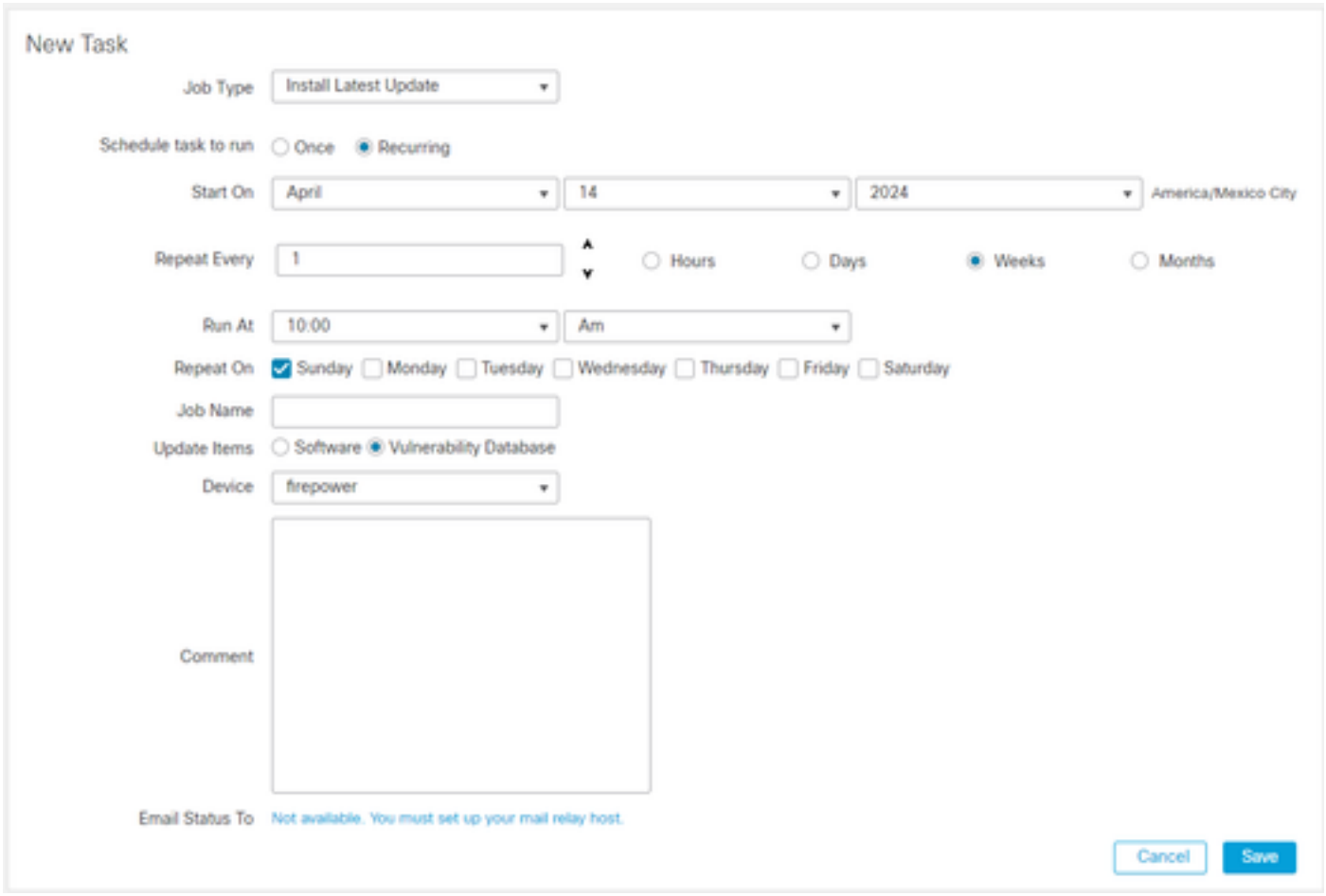
在计划要运行的任务上，选择循环。

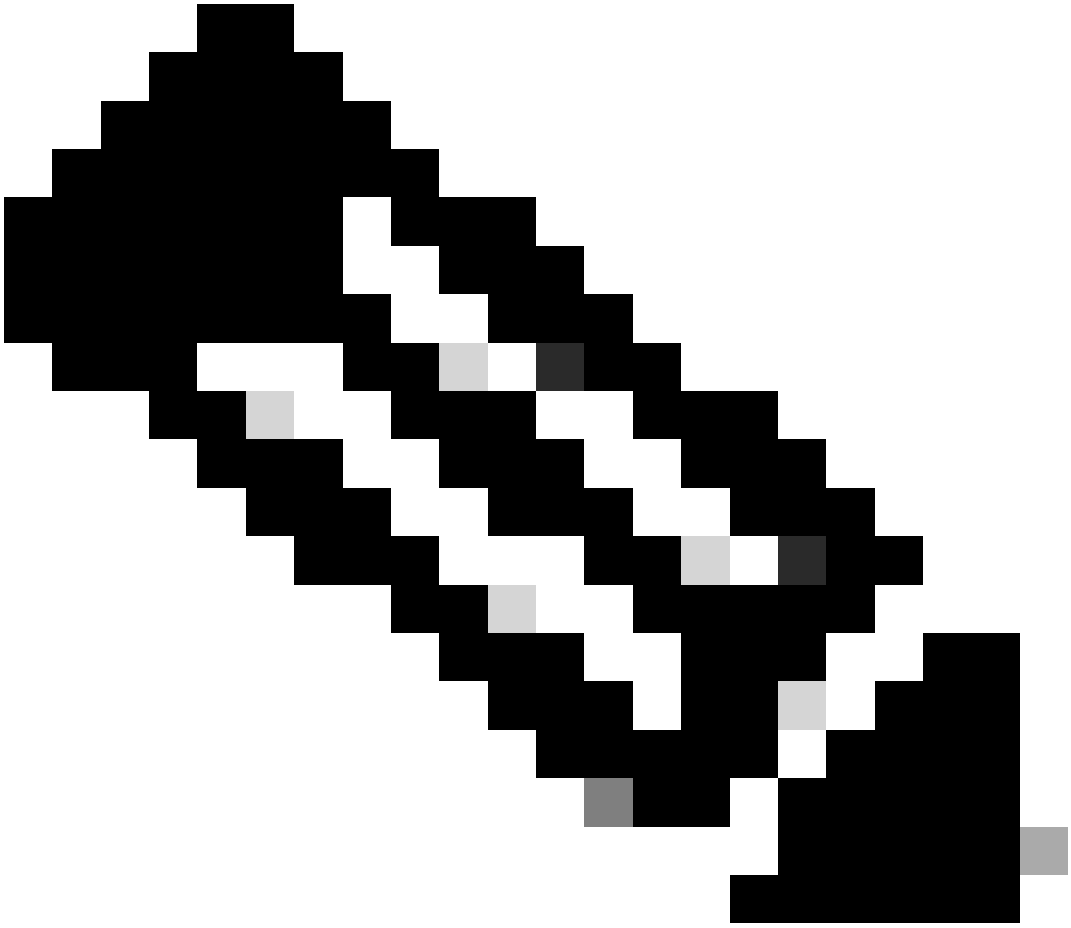
在更新项目部分中，选择漏洞数据库。

然后单击Save。

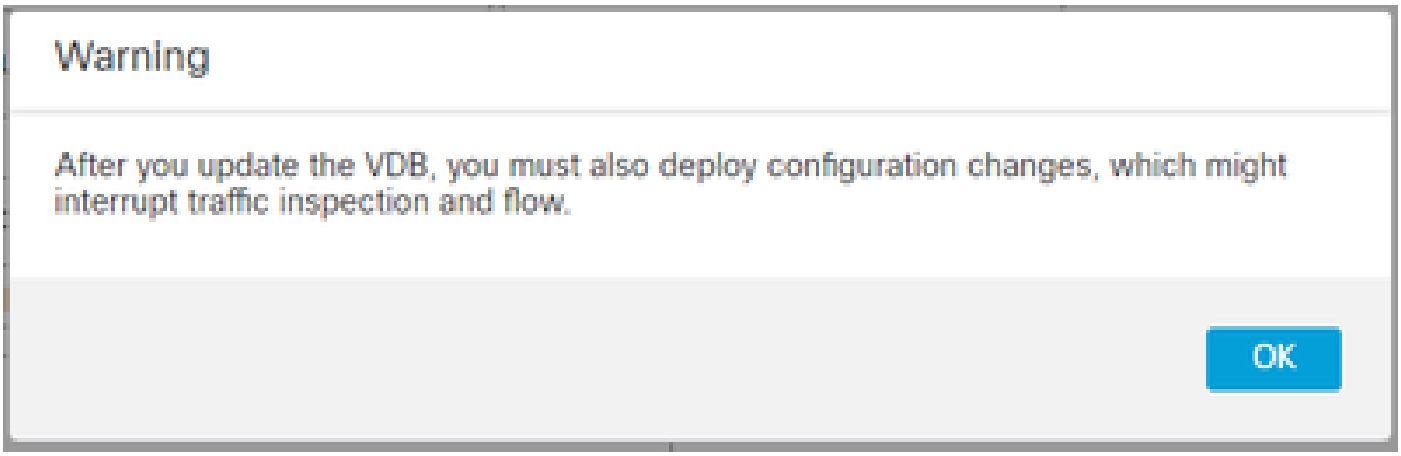


5. 重复步骤3以返回新任务屏幕，并从作业类型下拉菜单中选择安装最新更新，然后使用设置满足您的需要，最后单击保存。

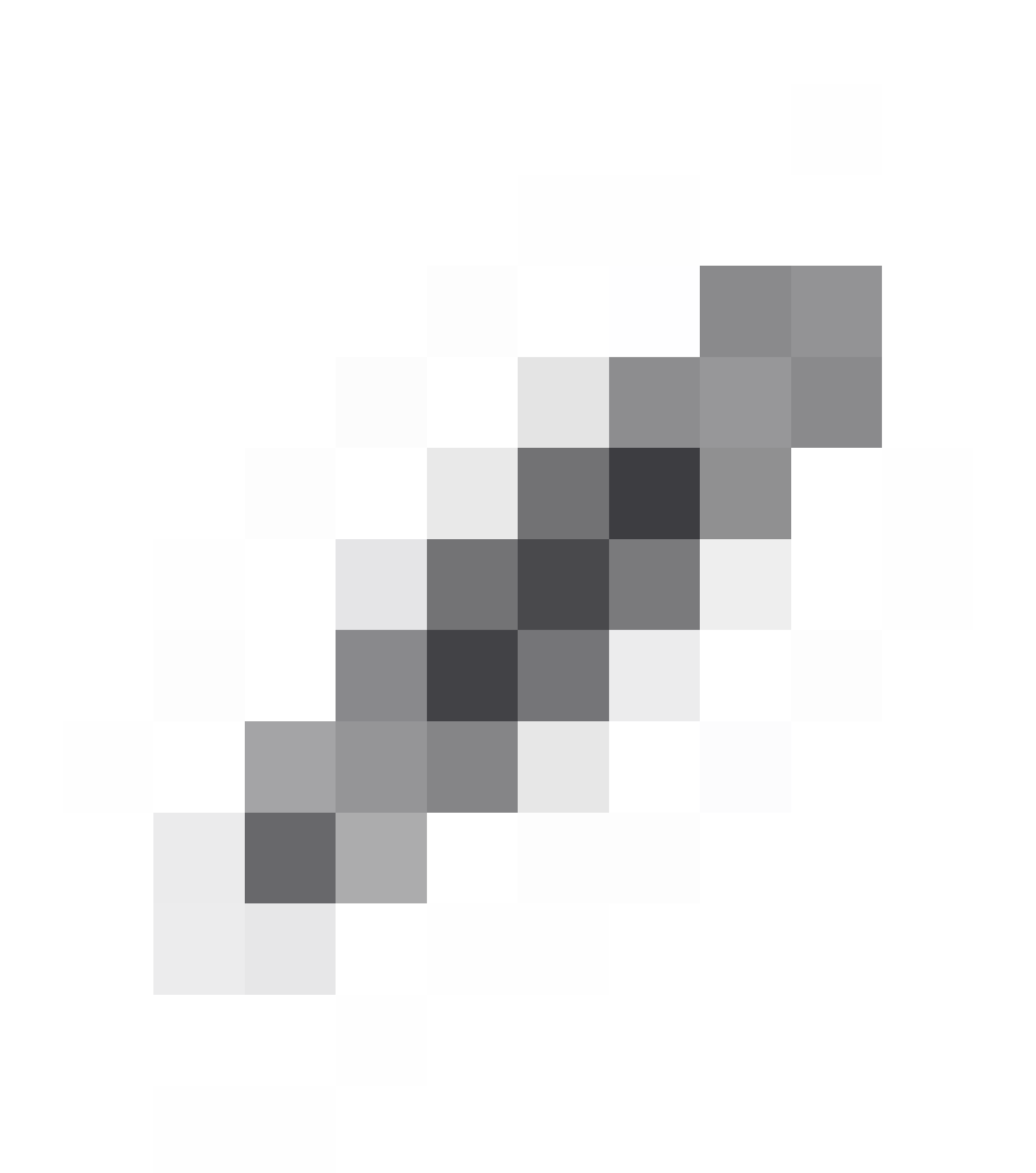

New Task
Job Type
Install Latest Update
Schedule task to run
Once
Recurring
Start On
April
14
2024
America/Mexico City
Repeat Every
1
Hours
Days
Weeks
Months
Run At
10:00
Am
Repeat On
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Job Name
Update Items
Software
Vulnerability Database
Device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



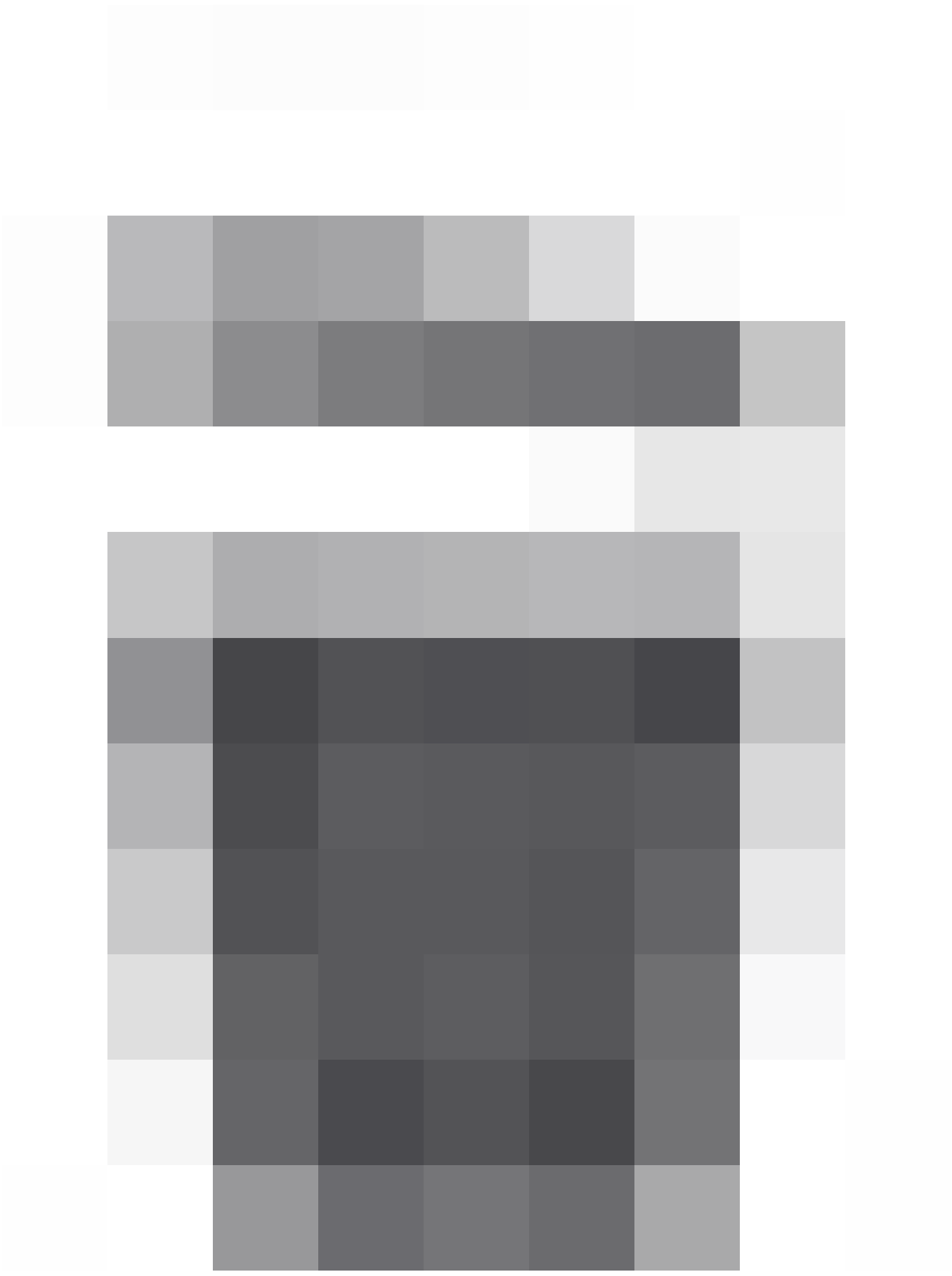
注意：请注意，在VDB更新后，还必须部署可中断流量检查和流量的配置更改。

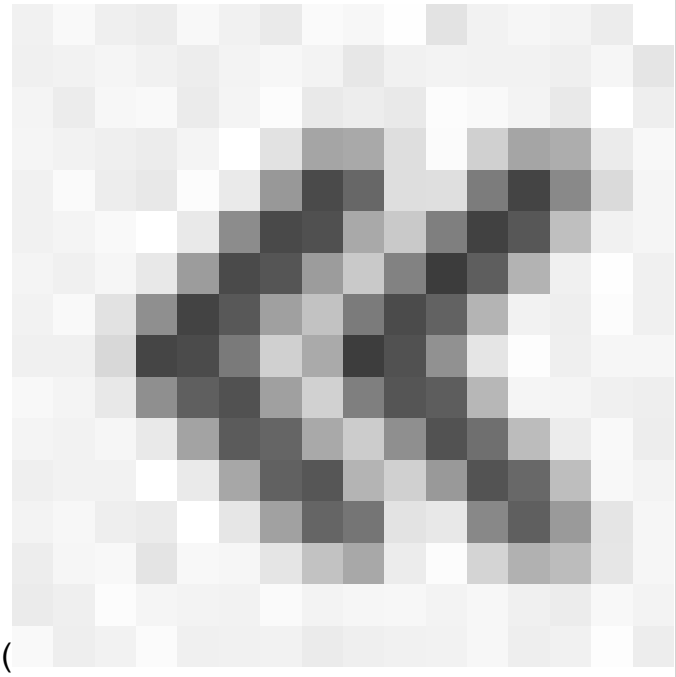
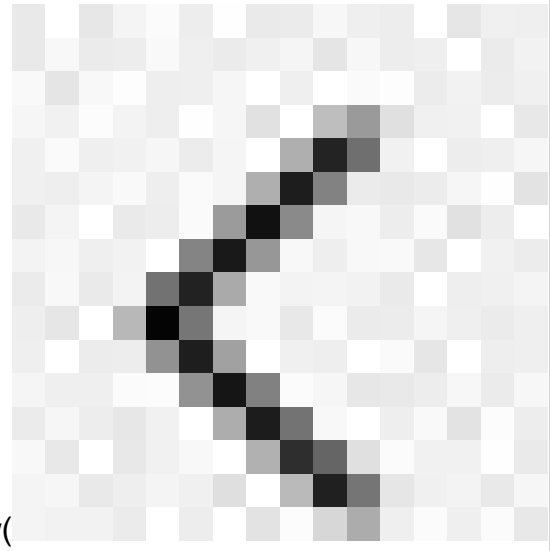
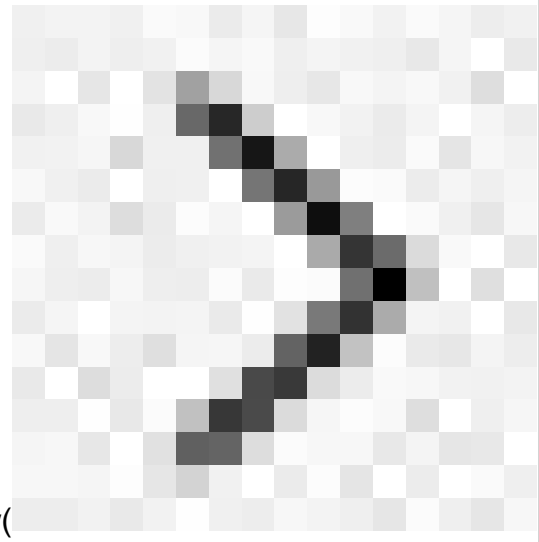


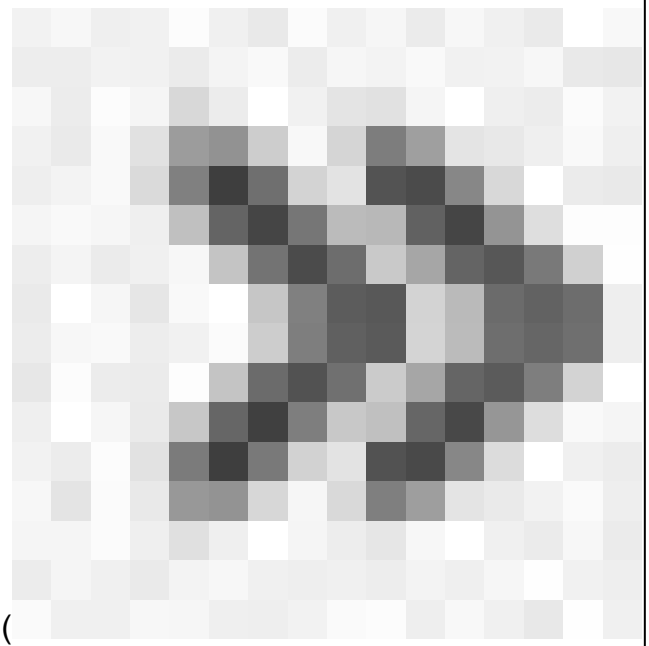
您可以通过点击编辑笔(



)对计划任务进行微调，或通过点击Scheduling屏幕Task Details部分上的垃圾桶(



步骤 2	您可以使用日历视图执行以下任务：  • 单击双左箭头( )向后移动一年。  • 单击“Single Left Arrow( )”向后移动一个月。  • 点击Single Right Arrow(

	)向前移动一个月。  • 点击向右双箭头( )向前移动一年。 • 单击“Today”返回当前月份和年份。 • 单击“添加任务”以安排新任务。 • 单击某个日期，查看任务列表表中特定日期的所有预定任务。 • 单击某个日期的特定任务可在任务列表表中查看该任务。

故障排除

如果VDB自动升级未按预期运行，您可以回滚VDB。

步骤:

通过SSH连接到管理设备（FMC、FDM或SFR机上）CLI。

切换到expert模式和root，并设置回滚变量：

<#root>

expert

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

验证要降级到的VDB软件包位于/var/sf/updates中的设备上，然后进行安装：

<#root>

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

标准vdb安装日志可以在/var/log/sf/vdb-*的适用位置找到

VDB安装完成后，将策略部署到设备。

在FMC上，要检查VDB的安装状态，可以检查以下目录内容：

root@firepower：/var/log/sf/vdb-4.5.0-338# ls -la
总计40
drwxr-xr-x 5根4096 2023年5月15日。
drwxr-xr-x 11 root root root 4096 Apr 23 06:00 ...
-rw-r - r - 1 root root 3308 May 15 2023 flags.conf.complete
drwxr-xr-x 2根4096 2023年5月15日安装程序
drwxr-xr-x 2根4096 2023年5月15日post
drwxr-xr-x 2根4096 2023年5月15日高级版
-rw-r—r— 1根根1603 2023年5月15日status.log
-rw-r - r - 1 root root 5703 May 15 2023 vdb.log
-rw-r—r— 1根根5月15日2023 vdb.pid

在FTD上，要检查VDB安装的历史记录，请检查以下目录内容：

root@firepower：/ngfw/var/cisco/deploy/pkg/var/cisco/packages# ls -al
总72912
drwxr-xr-x 5 root root 130 Sep 1 08:49 。
drwxr-xr-x 4 root root 2016年8月34日14:40 。
drwxr-xr-x 3 root root 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 2016年8月21日14:40 vdb-368
-rw-r—r— 1根根36374219 7月27日15:34 vdb-368.tgz
drwxr-xr-x 3根桥9月1日21 08:49 vdb-369
-rw-r—r— 1根根359084559月1日08:48 vdb-369.tgz

相关信息

更新漏洞数据库(VDB)

任务安排

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。