配置Cisco Threat Intelligence Director並對其進行故障排除

目錄

簡介

本檔案介紹如何設定和疑難排解Cisco Threat Intelligence Director(TID)。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower管理中心(FMC)管理

在配置Cisco Threat Intelligence Director功能之前，您需要確保滿足以下條件：

- Firepower管理中心(FMC): 必須在6.2.2（或更高版本）版本上運行（可以在物理或虛擬FMC上託管）。必須配置至少15 GB的RAM記憶體。必須在啟用REST API訪問的情況下進行配置。
- 感測器必須運行6.2.2版（或更高版本）。
- 在訪問控制策略選項的「高級設定」頁籤中，必須啟用**Enable Threat Intelligence** Director。
- 向訪問控制策略新增規則（如果規則不存在）。
- 如果您希望SHA-256可觀察結果生成觀察結果和Firepower管理中心事件，請建立一個或多個惡意軟體雲查詢或**阻止惡意軟體**檔案規則，並將檔案策略與訪問控制策略中的一個或多個規則相關聯。
- 如果您希望IPv4、IPv6、URL或域名觀察生成連線和安全情報事件，請在訪問控制策略中啟用連線和安全情報日誌記錄。

採用元件

本檔案中的資訊是根據以下軟體版本：

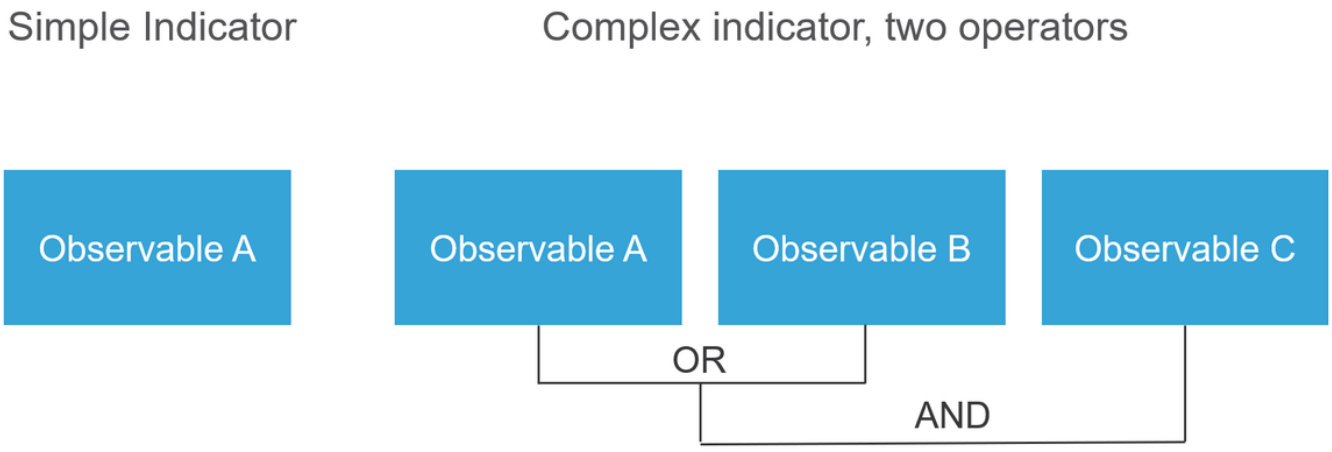
- 執行6.2.2.81的Cisco Firepower威脅防禦(FTD)虛擬
- 運行6.2.2.81的Firepower管理中心虛擬(vFMC)

附註：本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

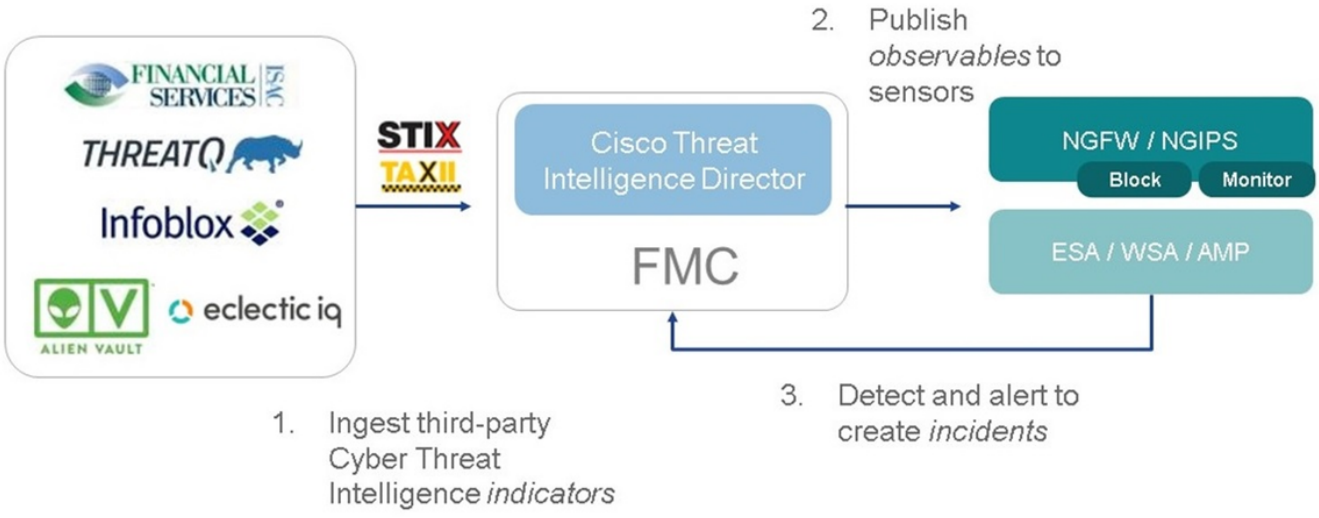
Cisco Threat Intelligence Director(TID)是一個可實施威脅情報資訊的系統。該系統利用並規範化異構第三方網路威脅情報，將情報發佈到檢測技術上，並將來自檢測技術的觀察結果關聯起來。

有三個新術語：**可觀**察、**指標**和**事件**。可觀察只是變數，例如URL、域、IP地址或SHA256。指示符由可觀察量組成。有兩種型別的指示器。一個簡單的指示符僅包含一個可觀察的。在複雜的指示器情況下，有兩個或多個可觀察的指示器使用AND和OR等邏輯函式相互連線。一旦系統檢測到應在FMC上阻止或監控的流量，就會出現事件。



如何運作？

如圖所示，在FMC上，您必須配置要下載威脅情報資訊的來源。然後FMC將資訊（可觀察量）推送到感測器。當流量與可觀察量匹配時，事件將出現在FMC使用者介面(GUI)中。



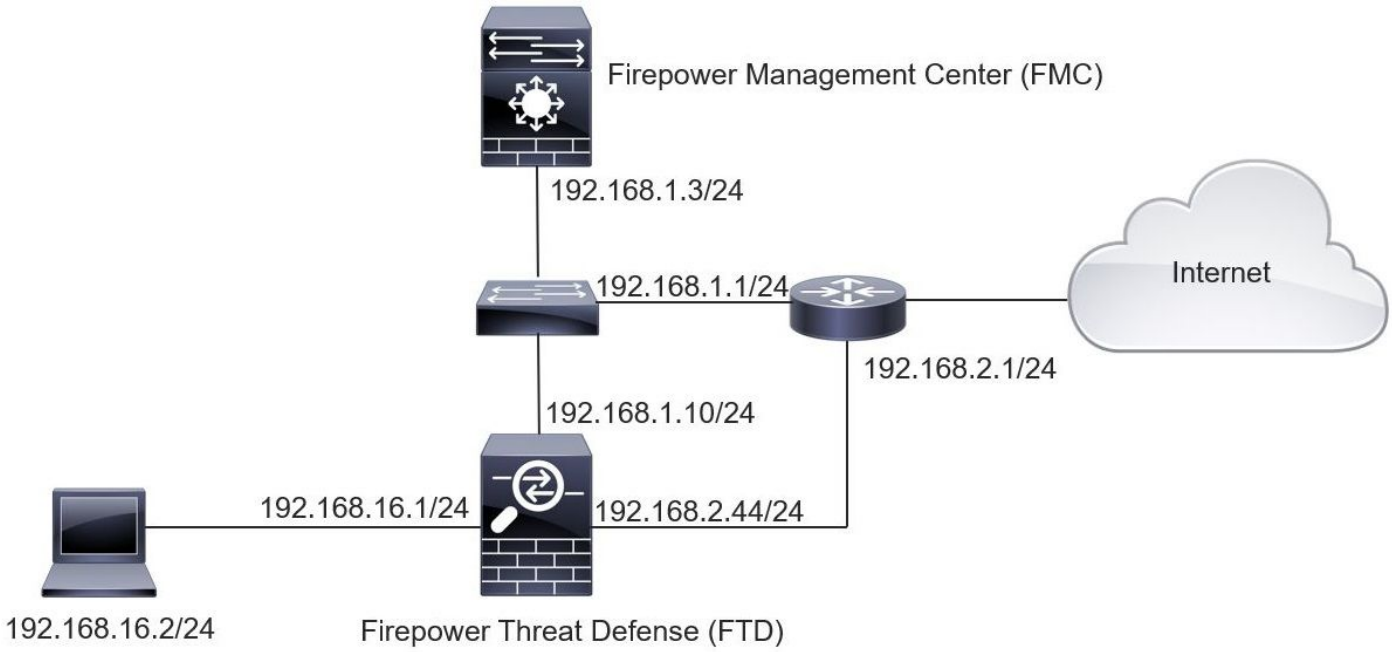
有兩個新術語：

- STIX（結構化威脅情報表達）是共用和使用威脅情報資訊的標準。有三個關鍵功能元素：指標、可觀察資料和事件
- TAXII(Trusted Automated Exchange of Indicator Information)是一種威脅資訊傳輸機制

設定

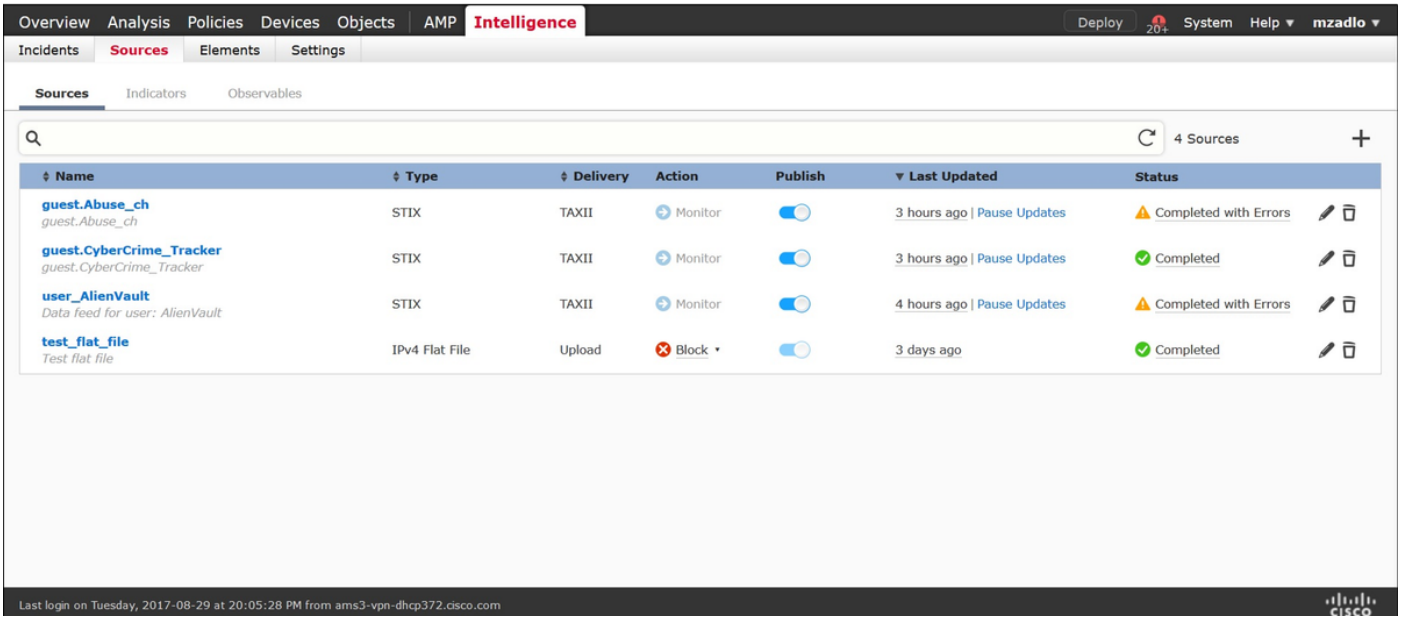
要完成配置，請考慮以下部分：

網路圖表



組態

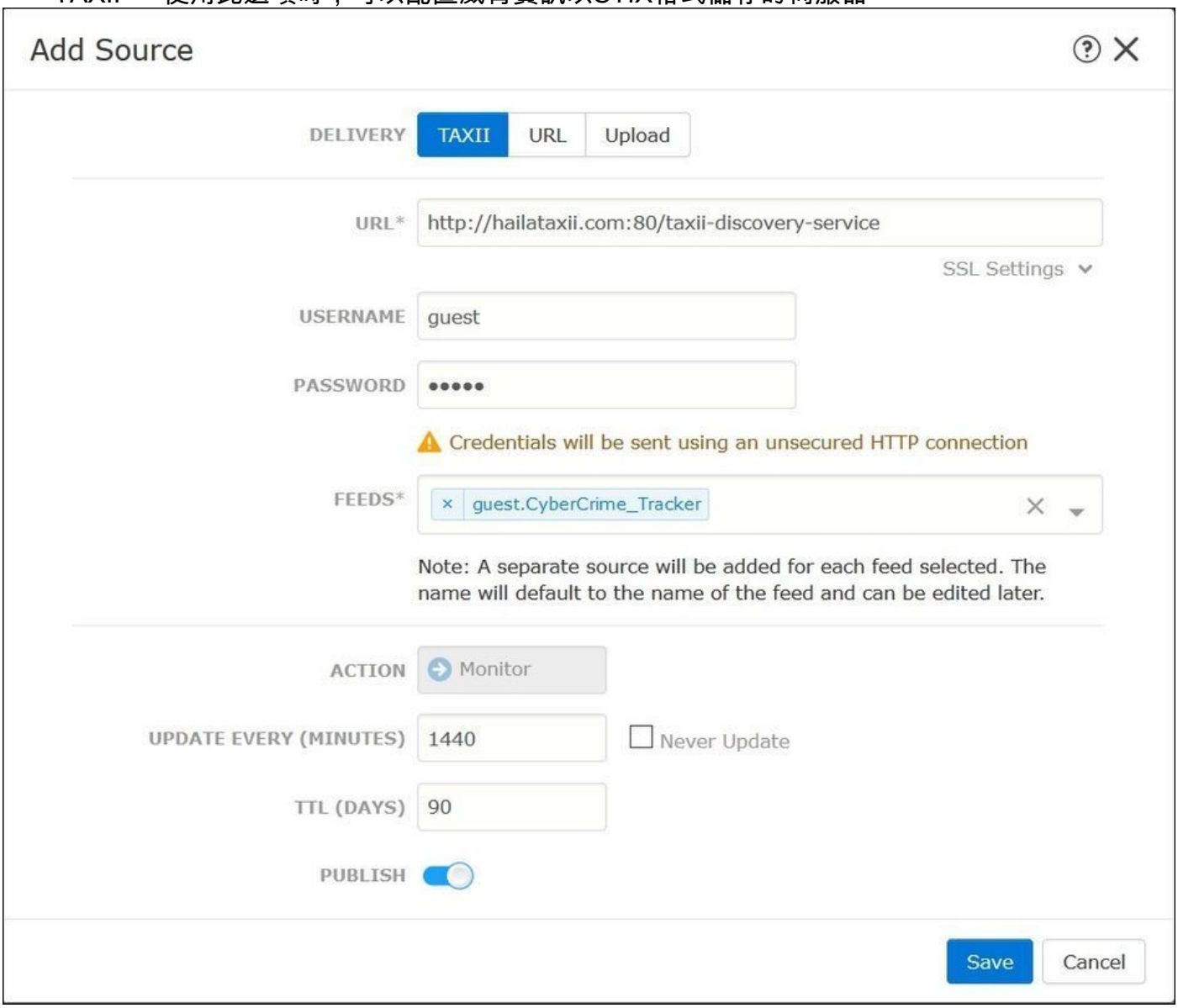
步驟1。若要設定TID，您必須導覽至**Intelligence**索引標籤，如下圖所示。



附註：如果源包含不受支援的觀察值，則狀態應為「Completed with Errors」。

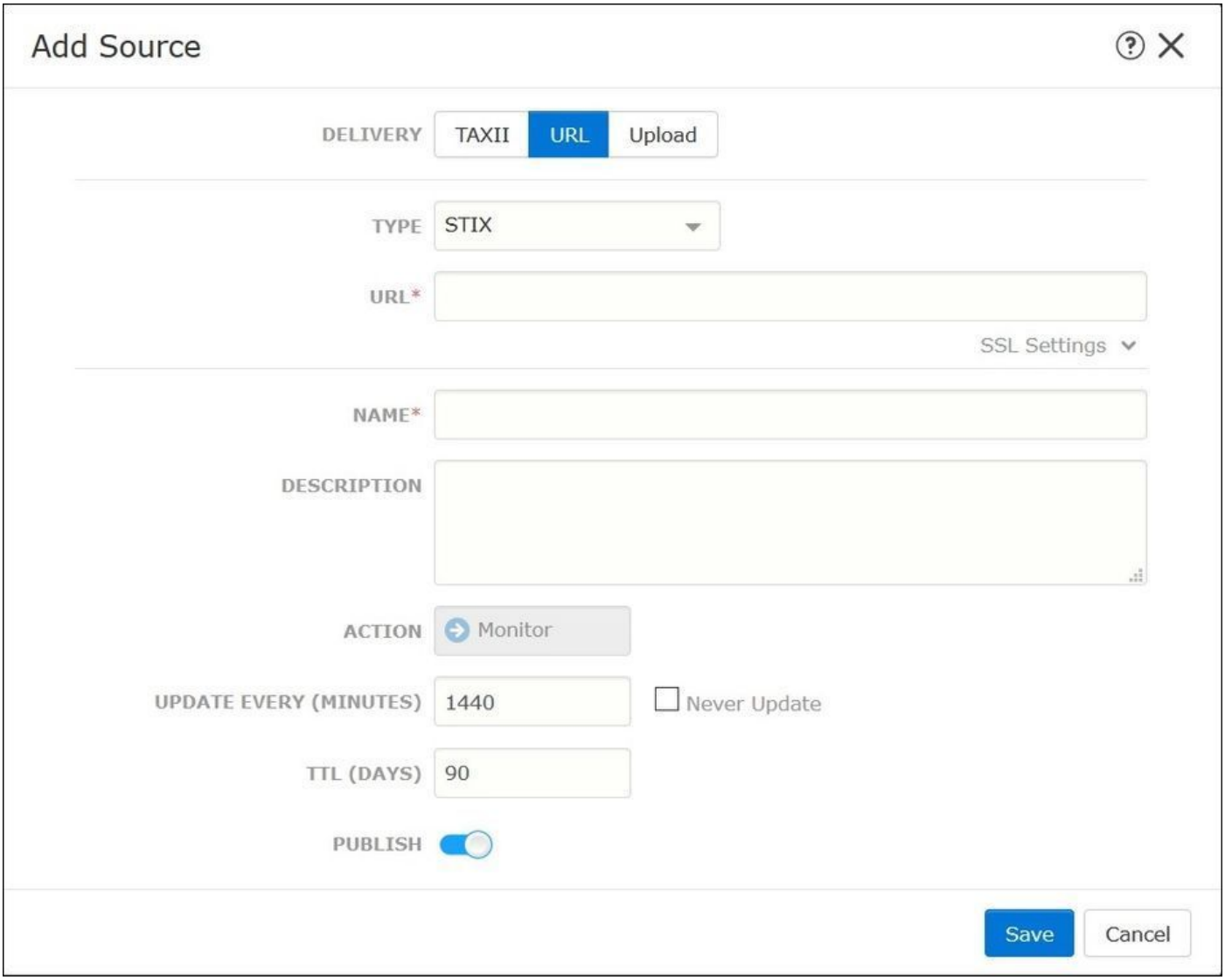
步驟2.必須新增威脅源。有三種新增源的方法：

- TAXII — 使用此選項時，可以配置威脅資訊以STIX格式儲存的伺服器

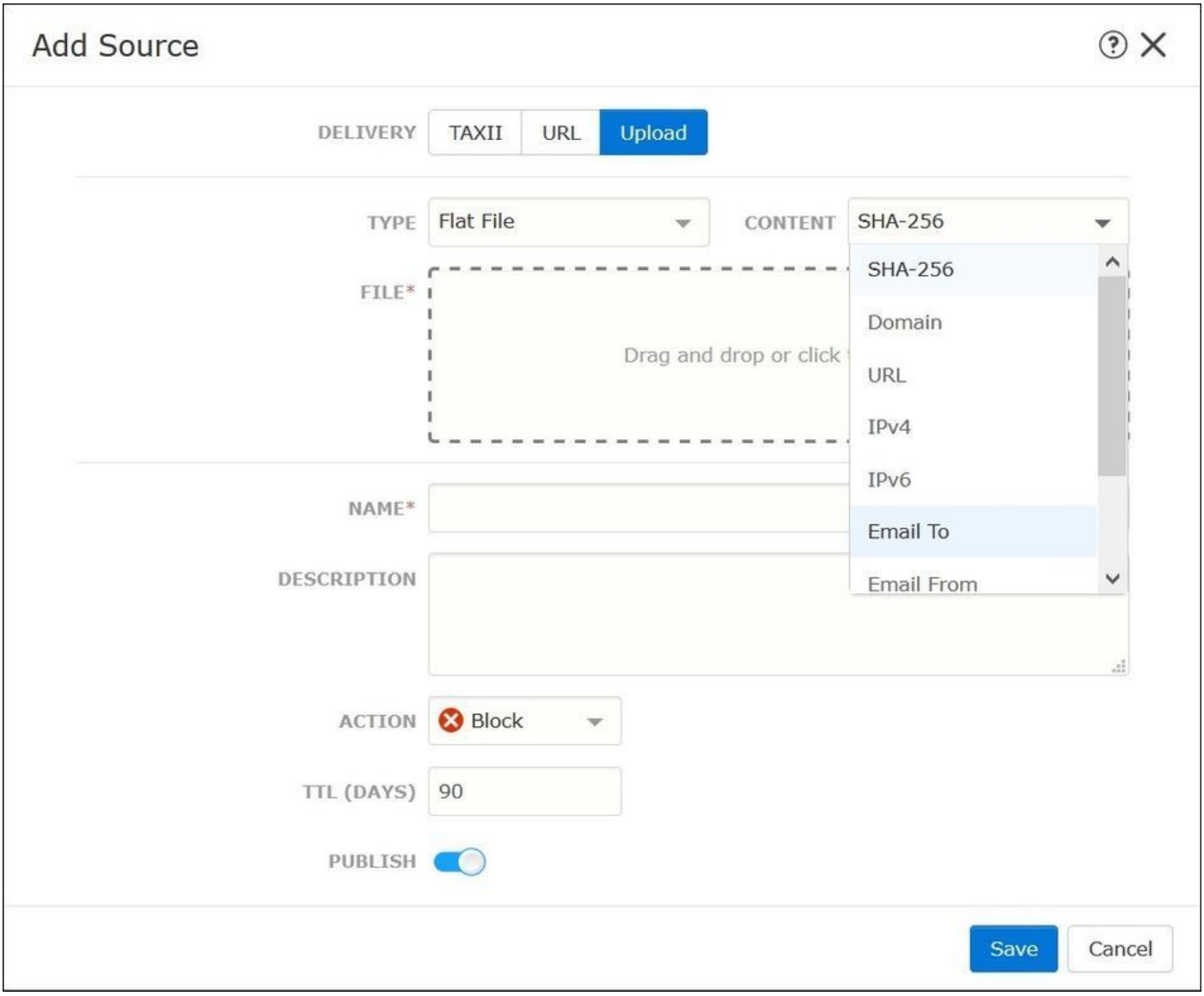


附註：唯一可用的操作是Monitor。不能為STIX格式的威脅配置阻止操作。

- URL — 您可以配置指向STIX威脅或平面檔案所在的HTTP/HTTPS本地伺服器的連結。

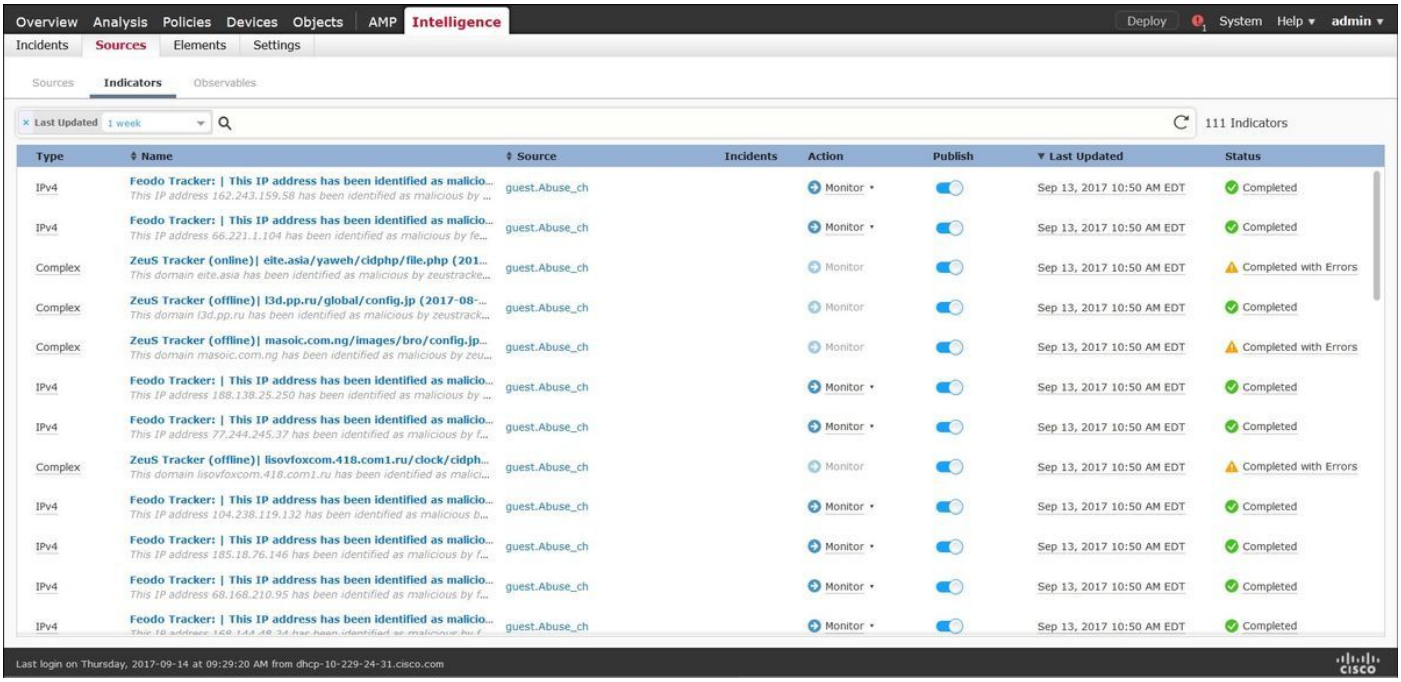


- 平面檔案 — 您可以以***.txt**格式上傳檔案，且必須指定檔案的內容。檔案每行必須包含一個內容條目。



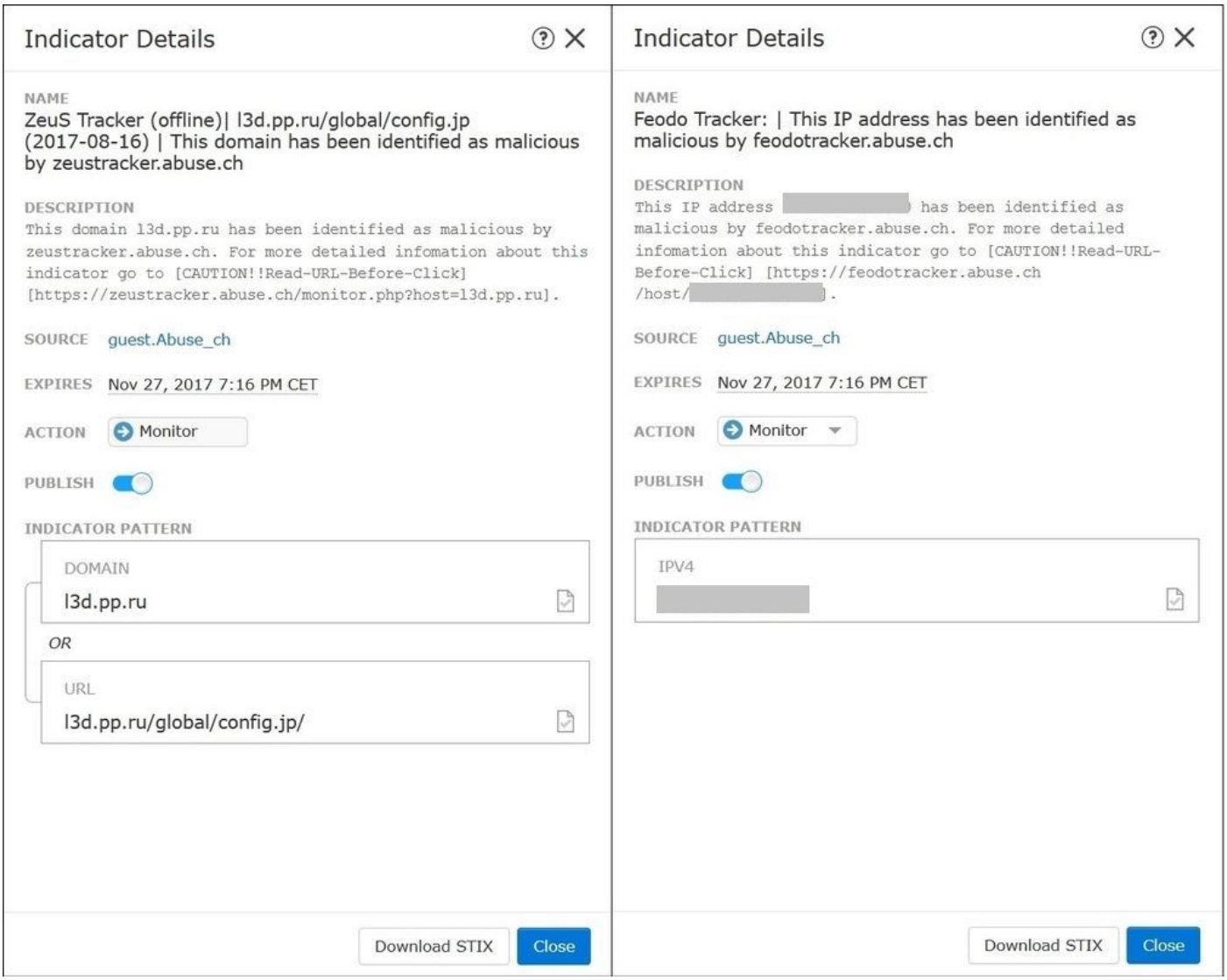
附註：預設情況下，所有源都會發佈，這意味著它們會被推送到感測器。此過程可能需要20分鐘或更長時間。

步驟3.在「指示器」頁籤下，可以確認指示器是否從已配置的源下載屬性：

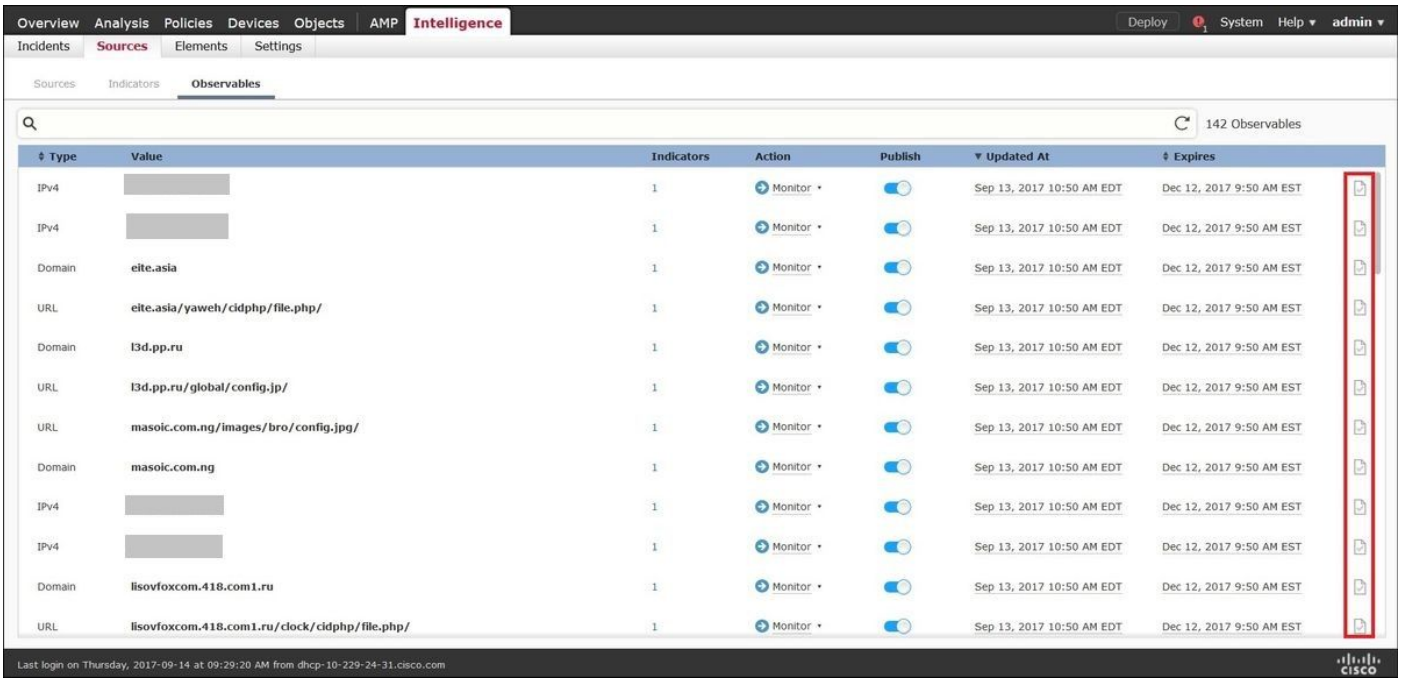


步驟4.選擇指示器的名稱后，可以看到有關它的更多詳細資訊。此外，您可以決定是否要將其發佈到感測器，還是要更改操作（在簡單指示器的情況下）。

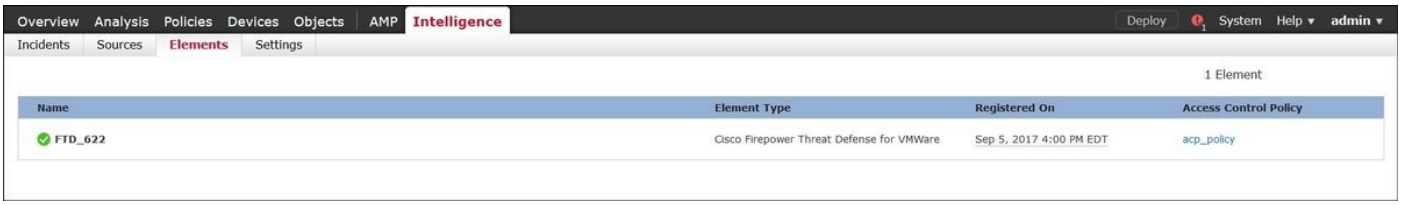
如圖所示，列出一個複數指示符，其中包含由OR運算子連線的兩個可觀察量：



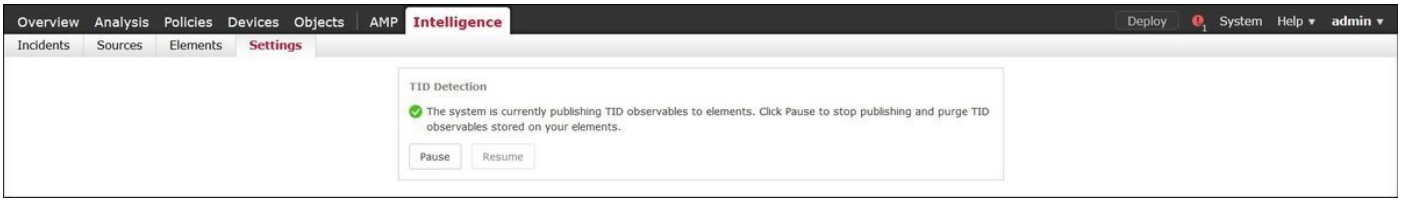
步驟5.導航到「可觀察量」頁籤，從中可以找到指標中包含的URL、IP地址、域和SHA256。您可以決定要將哪些可觀察量推送到感測器，並可以根據需要更改其操作。在最後一列中，有一個白名單按鈕，該按鈕相當於發佈/不發佈選項。



步驟6.導航至Elements頁籤以驗證啟用TID的裝置清單。

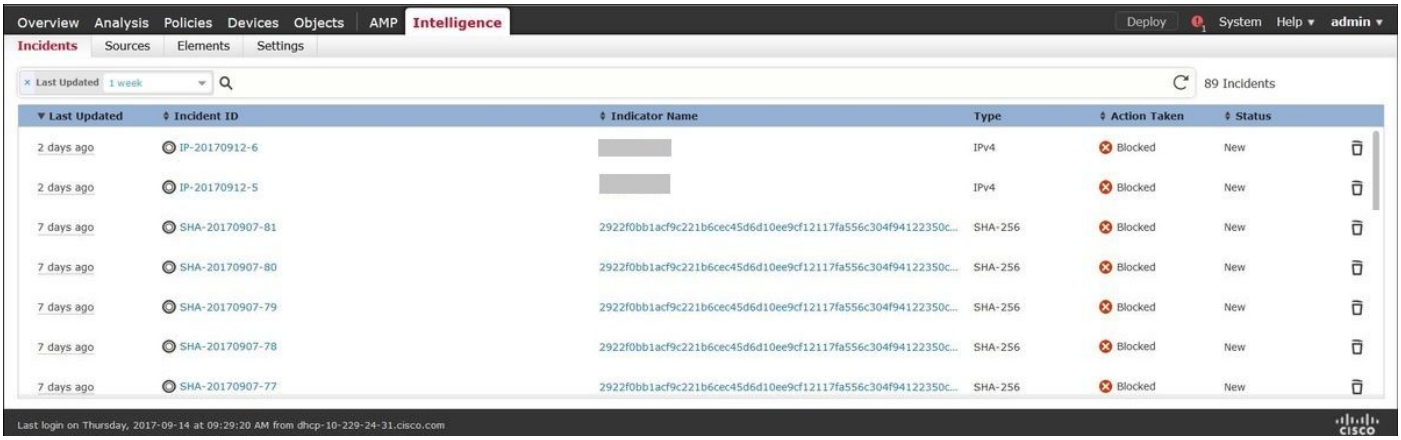


第7步（可選）。 導航到Settings頁籤並選擇Pause按鈕以停止將指示器推送到感測器。此操作最多需要20分鐘。

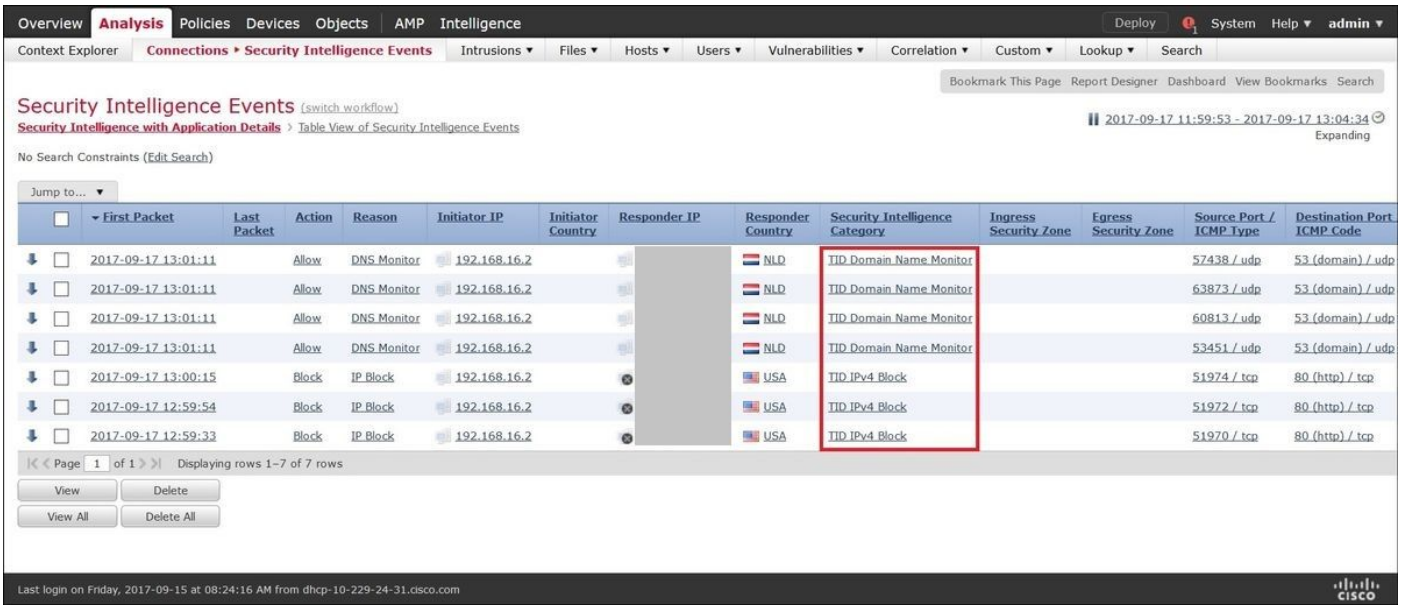


驗證

方法1。為了驗證TID是否對流量執行了操作，您需要導航至「事件」頁籤。



方法2.可在TID標籤下的「安全情報事件」頁籤下找到事件。



附註：TID的儲存容量為100萬次。

方法3.您可以確認FMC和感測器上是否存在已配置的源（源）。為此，您可以在CLI上導航到以下位置：

/var/sf/siurl_download/

/var/sf/sidns_download/

/var/sf/iprep_download/

為SHA256源建立了一個新目錄：/var/sf/sifile_download/。

```
root@ftd622:/var/sf/sifile_download# ls -l
total 32
-rw-r--r-- 1 root root  166 Sep 14 07:13 8ba2b2c4-9275-11e7-8368-f6cc0e401935.lf
-rw-r--r-- 1 root root   38 Sep 14 07:13 8ba40804-9275-11e7-8368-f6cc0e401935.lf
-rw-r--r-- 1 root root   16 Sep 14 07:13 IPRVersion.dat
-rw-rw-r-- 1 root root 1970 Sep 14 07:13 dm_file1.acl
-rw-rw-r-- 1 www  www   167 Sep 14 07:13 file.rules
drwxr-xr-x 2 www  www  4096 Sep  4 16:13 health
drwxr-xr-x 2 www  www  4096 Sep  7 22:06 peers
```

```
drwxr-xr-x 2 www  www  4096 Sep 14 07:13 tmp
root@ftd622:/var/sf/sifile_download# cat 8ba2b2c4-9275-11e7-8368-f6cc0e401935.lf
#Cisco TID feed:TID SHA-256 Block:1
7a00ef4b801b2b2acd09b5fc72d7c79d20094ded6360fb936bf2c65a1ff16907
2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c2bcbdc
```

附註：僅在FMC上的全域性域上啟用TID

附註：如果以高可用性配置（物理FMC裝置）在活動Firepower管理中心託管TID，系統不會將TID配置和TID資料同步到備用Firepower管理中心。

疑難排解

有一個稱為tid的頂層過程。此過程取決於三個過程：**蒙哥**、RabbitMQ、redis。若要驗證程式，請執行**pmtool狀態 | grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "**命令。

```
root@fmc622:/Volume/home/admin# pmtool status | grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "
RabbitMQ (normal) - Running 4221
mongo (system) - Running 4364
redis (system) - Running 4365
tid (normal) - Running 5128
root@fmc622:/Volume/home/admin#
```

為了即時驗證所執行的操作，您可以執行**system support firewall-engine-debug**或**system support trace**命令。

```
> system support firewall-engine-debug

Please specify an IP protocol:
Please specify a client IP address: 192.168.16.2
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
...
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1 URL SI: ShmDBLookupURL("http://www.example.com/")
returned 1
...
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1 URL SI: Matched rule order 19, Id 19, si list id
1074790455, action 4
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1 deny action
```

在行動方面有兩種可能性：

- **URL SI:匹配的規則順序19、Id 19、si list id 1074790455、操作4** — 流量被阻止
- **URL SI:匹配的規則順序20、Id 20、si list id 1074790456、操作6** -流量受到監控。