

# 檢視安全終結點(CSE)Windows掃描

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[完全掃描](#)

[Flash掃描](#)

[計畫的掃描](#)

[計畫完全掃描](#)

[其他掃描](#)

[疑難排解](#)

---

## 簡介

本文檔介紹Windows聯結器的不同掃描型別。

## 必要條件

本檔案的前提條件如下：

- Windows終結點
- 安全終結點(CSE)版本8.0.1.0或21164高版本
- 對安全終端控制檯的訪問

## 需求

本文件沒有特定需求。

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全終端主控台
- Windows 10終結點
- 安全終結點版本8.0.1.21164

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

在策略設定為debug的實驗室環境中測試了掃描。  
已通過連結器下載啟用安裝時的快閃記憶體掃描。  
掃描是從安全客戶端GUI和計畫程式執行的。

## 完全掃描

此日誌演示何時從CSE圖形使用者介面(GUI)請求完全掃描。

```
(1407343, +0 ms) Aug 23 18:06:01 [9568]: Processing AMP_UI_SCAN action: 1, type 2
```

從使用者介面掃描

此處，ScanInitiator進程將開始掃描進程。

```
(1407343, +0 ms) Aug 23 18:06:01 [9568]: ScanInitiator::RequestScan: Attempting to start scan: dConnect
```

您可以看到，Full Scan是GUI上觸發的掃描型別，如下圖所示。

接下來，您將具有安全識別符號(SID)，這是一個指定給此特定事件的長度可變的值，此安全識別符號可幫助您跟蹤日誌中的掃描。

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"iclsa": "0", "sce": 108, "scx": "Full Scan", "sid": 1407343, "sit": 2, "sop": 0, "stp": 5}, ui64EventId=7135211821471891460
```

發佈事件

您可以將此項與CSE控制檯中的事件進行匹配。



The screenshot shows a table with connector details for a scan event. The table has two columns: 'Connector Details' and 'Comments'. The 'Connector Details' column lists various identifiers and the current user. The 'Comments' column is empty. At the bottom of the table, there is a 'Run Scan' button. The top of the screenshot shows the event title 'G started scan', a search icon, and the event name 'Scan Started' with a timestamp '2022-08-23 23:06:01 UTC'.

Connector Details	Comments
Computer	
Connector GUID	
Cisco Secure Client ID	
Processor ID	
Current User	

控制檯事件



```
(2443984, +0 ms) Aug 23 18:23:18 [8744]: Successfully configured endpoints: https://mgmt.amp.cisco.com/agent/v1/ https://intake.amp.cisco.com/event/
(2443984, +0 ms) Aug 23 18:23:18 [17664]: UIPipe::SendDisposition file: HackSantana Trainer GLS And GIS By PollinxD 27-12[1829].rar(3), detect:
Gen:Variant.Graftor.596528
```

威脅事件發佈

掃描完成後，您可以檢視「事件檢視器」，瞭解掃描的摘要。

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	23/08/2022 06:29:40 p. m.	CiscoSecureEndpoint	1249	Scan
Error	23/08/2022 06:23:18 p. m.	CiscoSecureEndpoint	1311	Quarantine
Información	23/08/2022 06:23:18 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:14:24 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:14:24 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:11:55 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:11:55 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:11:25 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:11:25 p. m.	CiscoSecureEndpoint	1300	Detection
Información	23/08/2022 06:11:24 p. m.	CiscoSecureEndpoint	1310	Quarantine
Información	23/08/2022 06:11:24 p. m.	CiscoSecureEndpoint	1300	Detection

Evento 1249, CiscoSecureEndpoint

General Detalles

Scan (Full Scan) completed successfully. A total of 278172 files were scanned and 6 threats were detected.

事件檢視器

## Flash掃描

快閃記憶體掃描速度很快，需要幾秒鐘到幾分鐘才能完成。

在此示例中，您可以看到掃描何時開始，並且與前面一樣，這次給定了SID，其值為2458015。

```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: Scan::ScanThreadProcess: beginning scan id: 2458015, [type: 1, options: 3, 3, pid: 0, initiator: 2]
```

Flash掃描開始

下一步操作是將事件發佈到CSE雲。

```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"iclsa":"0","sce":108,"scx":"Flash Scan","sid":2458015,"sit":2,"sop":3,"stp":1}, ui64EventId=7135602311308509188
```

掃描完成後，事件將發佈到雲。

```
(2458015, +0 ms) Aug 24 19:21:19 [17500]: imn::CEventManager::PublishEvent: publishing type=554696714, json={"iclsa":"0","sce":108,"scx":"Flash Scan","sid":2458015,"sit":2,"sop":3,"stp":1}, ui64EventId=7135602311308509188
```

掃描完成發佈

可在Windows事件檢視器中看到該事件。您可以發現，該資訊與日誌中顯示的資訊相同。

```
- <EventData>
  <Data Name="JsonEvent">{"dios":0,"ds":0,"hi":0,"scx":"Flash Scan","sdds":0,"sdfs":10951,"sdps":215,"sid":2458015,"sios":0,"sit":2,"sop":3,"sspc":0,"stp":1}
  </Data>
  <Data Name="EventTypeId">554696715</Data>
  <Data Name="TimeStamp">133058605022030000</Data>
  <Data Name="EventId">7135602410092756997</Data>
  <Data Name="Description">EVENT_SCAN_COMPLETED_CLEAN</Data>
</EventData>
</Event>
```

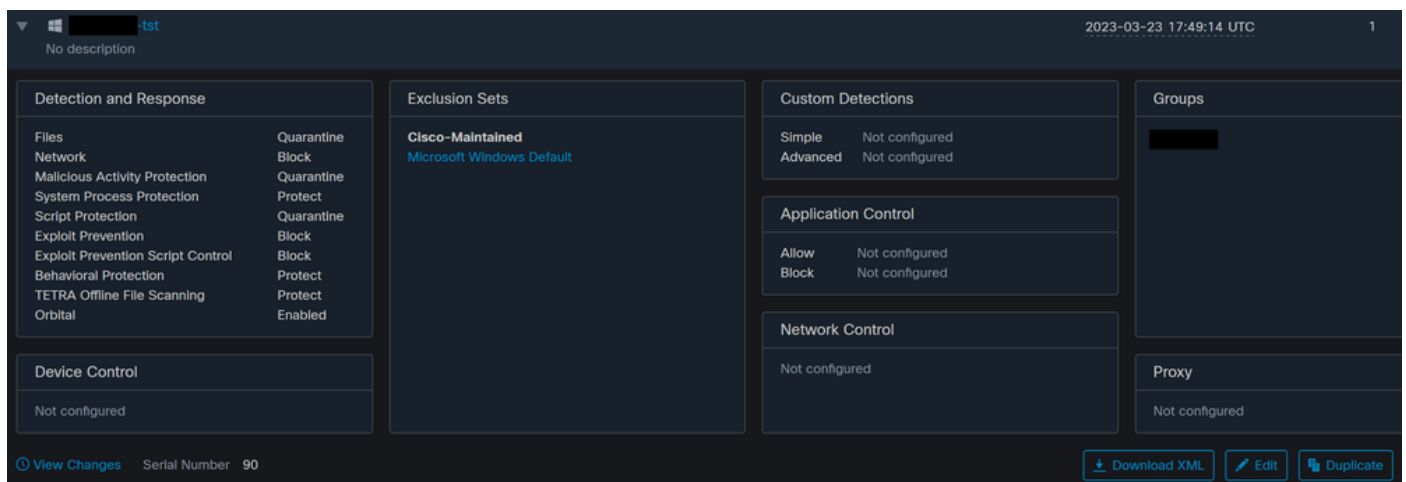
JSON事件

## 計畫的掃描

當涉及到預設掃描時，您必須瞭解一系列方面。

安排掃描後，序列號將發生變化。

在這裡，測試策略沒有任何計畫的掃描。



策略序列號

如果要安排掃描，請按一下編輯。

導航至 [Advanced Settings > Scheduled Scans](#).

## Product Updates

### Advanced Settings

#### Administrative Features

Client User Interface

File and Process Scan

Cache

Endpoint Isolation

Orbital

Engines

TETRA

Network

Scheduled Scans

高級設定

按一下「New」。

You can add multiple scan schedules for a given policy. Each scheduled scan will run at local computer time.

Schedule [+ New](#)

新掃描配置

選項包括：

- 掃描間隔
- 掃描時間
- 掃描型別

配置掃描後，按一下Add。

### Scheduled Scan


Scan Interval

Scan Time  :

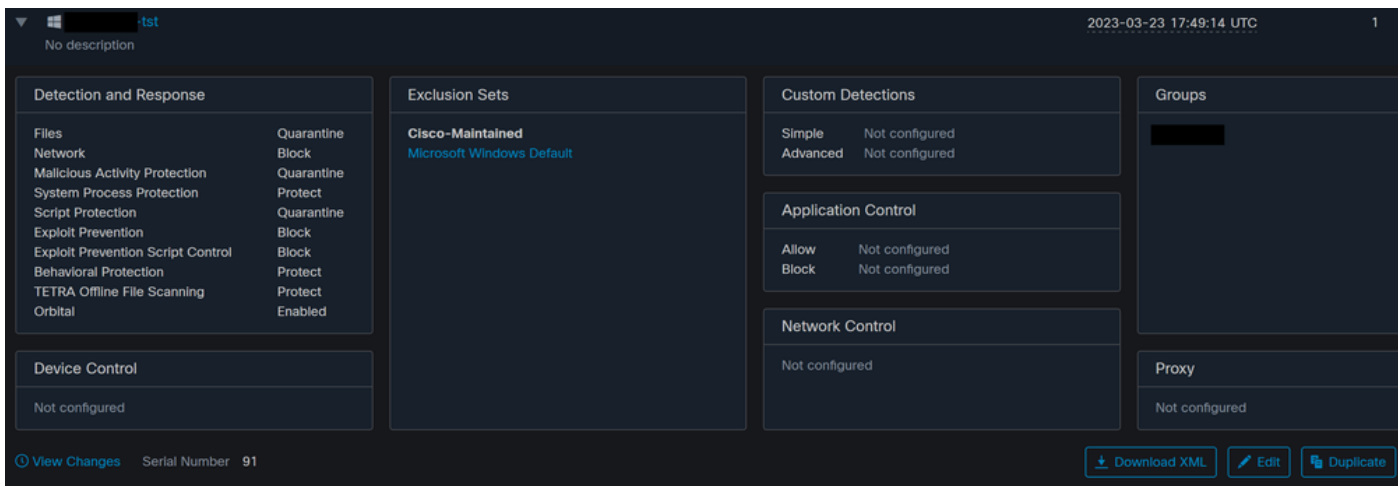
Scan Type

計畫掃描配置

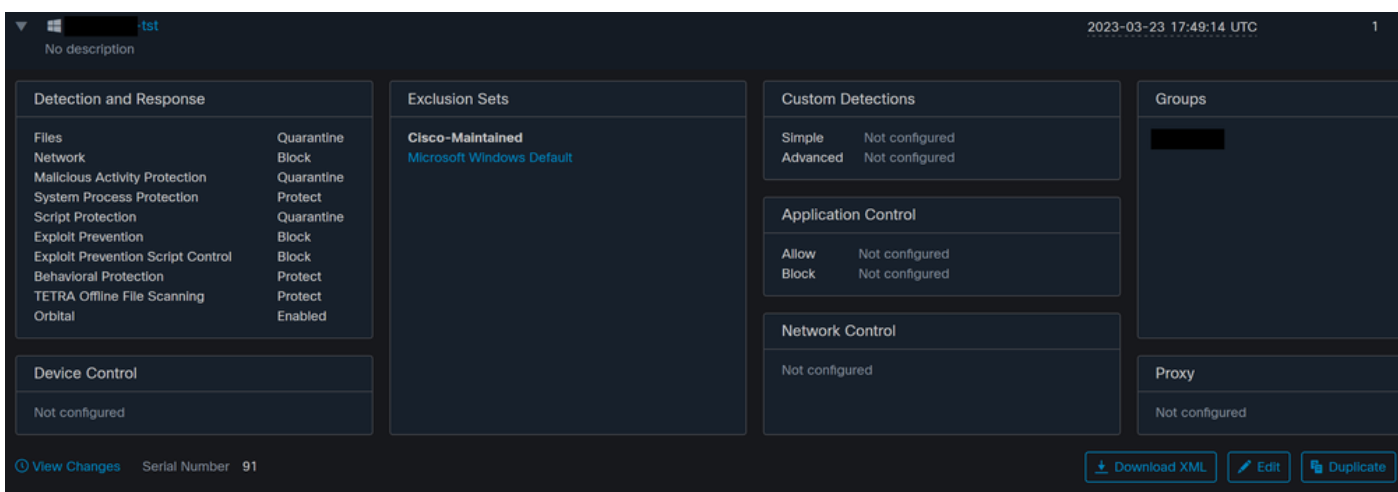
儲存策略更改，系統將顯示一個彈出視窗，確認您的更改。

 Policy "[redacted]-tst" successfully updated.

快顯視窗



序列號更改



序列號更改

掃描在「策略」中配置，在本示例中，兩個掃描是已配置的掃描，一個是快閃記憶體掃描，另一個是完全掃描。



```
<sched_userlogon>0</sched_userlogon>
<scheduled>20|1661470488|Daily Flash Scan (18:40)|1|3|-|48|0|2022|8|24|2122|8|24|18|40|0|0|1|1|0|0|0|0</scheduled>
<scheduled>20|1661470489|Daily Full Scan (18:50)|5|0|-|48|0|2022|8|24|2122|8|24|18|50|0|0|1|1|0|0|0|0</scheduled>
<maxarchivefilesize>52428800</maxarchivefilesize>
<maxfilesize>52428800</maxfilesize>
```

策略XML

它們被新增到HistoryDB中的排程程式。<scheduled>標籤旁邊的字元是標識掃描的進程ID(PID)。

```
(86616093, +0 ms) Aug 25 18:43:59 [12408]: AddScheduledScanExecStatusToHistoryDB Queued 1661470488 scan. last run status: 0x0 with status: 0x0
```

進程ID

如圖所示，它會排隊。

```
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScheduledScanMgr::CheckAndTriggerScheduledScans scan_id: 1661470488 queued execution status: 0x0
```

掃描已排隊

您可以在日誌中搜尋掃描，並注意掃描是否可以立即運行。如果可以，則執行掃描。

```
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScheduledScanMgr::CanTriggerNow: [TASK_TIME_TRIGGER_DAILY] executing 1661470488 scheduled scan,
bShouldTrigger: true, timeDiff: 0, days_interval: 1
(86616093, +0 ms) Aug 25 18:43:59 [8472]: ClEngineInterface::ReadOptions 1, 1, 0, 0, 120000
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScanInitiator::RequestScan loading scheduled scan ID 1661470488
```

可以執行掃描

您可以看到已載入掃描的選項，並且ScanInitiator進程請求開始掃描。

```
(86616093, +0 ms) Aug 25 18:43:59 [8472]: ClEngineInterface::SetOptions setting scanner options
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScanInitiator::RequestScan: successfully loaded scheduled scan:
(86616093, +0 ms) Aug 25 18:43:59 [8472]: ClEngineInterface::SetOptions 1, 1, 0, 0, 120000
(86616093, +0 ms) Aug 25 18:43:59 [12408]: ScanInitiator::RequestScan: Name: Daily Flash Scan (18:40), Type: 1, Options: 3, ScanPath: -
```

然後，Process Scan::ScanThreadProcess將啟動掃描。

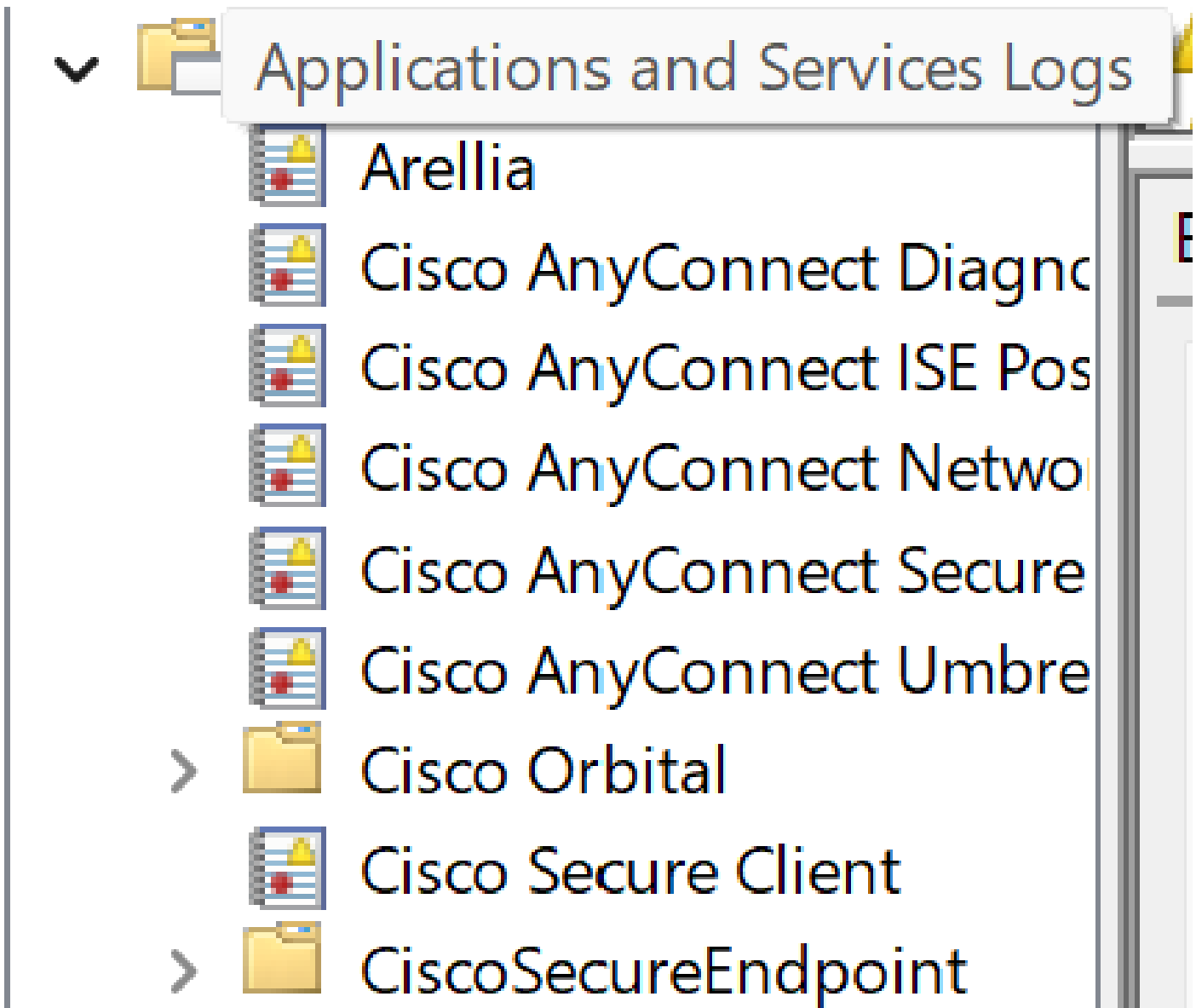
```
(86616093, +0 ms) Aug 25 18:43:59 [15372]: Scan::ScanThreadProcess: beginning scan id: 86616093, [type: 1, options: 3, 3, pid: 1661470488, initiator:
4]
```

與先前的事件類似，需要在CSE雲中發佈該事件。日誌可以告訴您掃描的型別，在本例中為Flash。

```
(86616093, +0 ms) Aug 25 18:43:59 [15372]: imn:CEEventManager::PublishEvent: publishing type=554696714, json={"iclsa":"","sce":108,"scx":"Flash Scan","sid":86616093,"sit":4,"sop":3,"stp":1}, ui64EventId=7135963775756140548
```

發佈計畫掃描事件

您可以導航至 [Event Viewer > App and Services Registries](#).



應用和服務日誌

搜尋思科安全終端，並開啟雲和事件。每個頁籤都為您提供不同的檢視。

活動:

```
- <EventData>
  <Data Name="ScanId">86616093</Data>
  <Data Name="ScanType">1</Data>
  <Data Name="FilesScanned">11575</Data>
  <Data Name="Threats">0</Data>
  <Data Name="ScanInitiator">4</Data>
  <Data Name="ScanContext">Flash Scan</Data>
  <Data Name="ErrorCode">0</Data>
  <Data Name="ErrorContext" />
</EventData>
</Event>
```

事件檢視

雲：

```
- <EventData>
  <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Flash Scan","sid":86616093,"sit":4,"sop":3,"stp":1}</Data>
  <Data Name="EventTypeId">554696714</Data>
  <Data Name="TimeStamp">133059446390220000</Data>
  <Data Name="EventId">7135963775756140548</Data>
  <Data Name="Description">EVENT_SCAN_STARTED</Data>
</EventData>
</Event>
```

雲端檢視

掃描完成後，您可以看到發佈到雲中的事件。

```
(86641515, +0 ms) Aug 25 18:44:24 [3116]: imn::CEventManager::PublishEvent: publishing type=554696715, json={"dios":0,"ds":0,"hi":0,"scx":"Flash Scan","sdds":0,"sdfs":11575,"sdps":218,"sid":86616093,"sios":0,"sit":4,"sop":3,"sspc":0,"stp":1}, ui64EventId=7135963883130322951
```

掃描完成發佈

## 計畫的完全掃描

Windows事件檢視器顯示「Event Scan Started」，如下圖所示。

```
- <EventData>
  <Data Name="JsonEvent">{"iclsa":"0","sce":108,"scx":"Full Scan","sid":87216125,"sit":4,"sop":0,"stp":5}</Data>
  <Data Name="EventTypeId">554696714</Data>
  <Data Name="TimeStamp">133059452390500000</Data>
  <Data Name="EventId">7135966352736518152</Data>
  <Data Name="Description">EVENT_SCAN_STARTED</Data>
</EventData>
</Event>
```

完成後，您可以比較已發佈的事件。

```
(88165093, +0 ms) Aug 25 19:09:48 [18536]: imn::CEEventManager::PublishEvent: publishing type=1091567628, json={"dios":0,"ds":2,"hi":0,"scx":"Full Scan","sdds":46012,"sdfs":280196,"sdps":224,"sid":87216125,"sios":0,"sit":4,"sop":0,"sspc":0,"stp":5}, ui64EventId=7135970428660482061
```

您可以在Windows的事件檢視器中看到這一點。

```
- <EventData>
  <Data Name="JsonEvent">{"dios":0,"ds":2,"hi":0,"scx":"Full Scan","sdds":46012,"sdfs":280196,"sdps":224,"sid":87216125,"sios":0,"sit":4,"sop":0,"sspc":0,"stp":5}</Data>
  <Data Name="EventTypeId">1091567628</Data>
  <Data Name="TimeStamp">133059461880170000</Data>
  <Data Name="EventId">7135970428660482061</Data>
  <Data Name="Description">EVENT_SCAN_COMPLETED_DIRTY</Data>
</EventData>
</Event>
```

事件檢視器

## 其他掃描

說到自定義掃描或rootkit掃描，您注意到的主要區別是事件檢視器或日誌中的掃描型別。

## 疑難排解

計畫掃描未發生時：

- 確保端點在掃描發生時可用。
- 確保在策略中安排了掃描。如果您沒有看到它，則觸發策略同步。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。