

セキュアエンドポイント(CSE)Windowsスキャンの確認

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[フルスキャン](#)

[フラッシュスキャン](#)

[スケジュール済みスキャン](#)

[スケジュール済みフルスキャン](#)

[その他のスキャン](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Windowsコネクタのさまざまなタイプのスキャンについて説明します。

前提条件

このドキュメントの前提条件は次のとおりです。

- Windowsエンドポイント
- セキュアエンドポイント(CSE)バージョンv.8.0.1.21164以降
- セキュアエンドポイントコンソールへのアクセス

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュアなエンドポイントコンソール
- Windows 10エンドポイント
- セキュアエンドポイントバージョンv.8.0.1.21164

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

スキャンは、ポリシーがデバッグに設定されたラボ環境でテストされました。インストール時のフラッシュスキャンは、コネクタのダウンロードによって有効になりました。スキャンは、Secure Client GUIおよびスケジューラから実行されました。

フルスキャン

このログは、CSEグラフィックユーザインターフェイス(GUI)からフルスキャンが要求された場合に表示されます。

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

ユーザインターフェイスからのスキャン

ここで、ScanInitiatorプロセスがScanプロセスを開始します。

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

図に示すように、フルスキャンはGUIでトリガーされるスキャンのタイプであることがわかります。

次に、この特定のイベントに割り当てられた可変長の値であるセキュリティ識別子(SID)があり、このセキュリティ識別子はログ内のスキャンの追跡に役立ちます。

```
(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
```

公開イベント

これをCSEコンソールからのイベントと照合できます。

G started scan		Scan Started	2022-08-23 23:06:01 UTC
Connector Details	Computer	YI	
Comments	Connector GUID	f5e05a5d-3be2-4946-846e-69efaebc70ab	
	Cisco Secure Client ID	N/A	
	Processor ID	bfebfbff000806d1	
	Current User	None	
	Run Scan		Device Trajectory Management

コンソールイベント

次に、ログで次の内容を確認できます。

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: PublishScanStartEvent publishing event succeeded for 1407343, (null)
```

発行に成功しました

これは、イベントがCSEクラウドに正常に公開されたことを意味します。

次のアクションは、実際にスキャンを実行することです。

```
(1407343, +0 ms) Aug 23 18:06:01 [17268]: Scan::ScanThreadProcess: published event. Starting Scan: 1407343, [type: 5]
```

スキャン開始

SIDは同じであるため、SID 1407343のストリームの下にあります。

これらは、スキャン中に脅威が検出されたときにコネクタが実行する手順です。

ステップ 1: コネクタは検出を引き起こしたファイルを示します。この例では、Hacksantana Trainer GLSによって引き起こされています。

```
(2443984, +0 ms) Aug 23 18:23:18 [11964]: Scan_OnObjectScanComplete: threat types: 63
(2443984, +0 ms) Aug 23 18:23:18 [17664]: imm::EventManager::FileRoot \\?\C:\Users\
\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\4\Attachments\HackSantana Trainer GLS And GIS By
PollinxD 27-12[1829].rar, , ,
(2443984, +0 ms) Aug 23 18:23:18 [11964]: Scan_OnObjectScanComplete action: 1 [5, 5]
```

検出されたファイル

ステップ 2：イベントは、脅威検出名と検出されたパスを使用してCSEコンソールに発行されます。

```
(2443984, +0 ms) Aug 23 18:23:18 [17664]: ERROR: imn::GetProcessInfo ProcessId is zero
(2443984, +0 ms) Aug 23 18:23:18 [17268]: IsFileSizeWithinScanLimit: dwMinFileSize = 0, dwMaxFileSize = 52428800
(2443984, +0 ms) Aug 23 18:23:18 [17664]: imn::CEventManager::PublishEvent: publishing type=1090519054, json={"am":0,"dete":64,"dfc":"13305770598","dfs":0,"dfsl":"","did":"7135216275352977414","dnm":"Gen:Variant.Graftor.596528","fcr":"","fcx":2148204800,"ffv":"","fnd":"HackSantana Trainer GLS And GIS By PollinxD 27-12[1829].rar","fnp":"","fpd":"\\\\?\\C:\\Users\\[redacted]\\\\AppData\\Local\\Packages\\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\\LocalState\\Files\\S0\\4\\Attachments\\HackSantana Trainer GLS And GIS By PollinxD 27-12[1829].rar","fpn":"","fpv":"","ft":"0x00000000000000000000000000000001","ftd":"0x00000000000000000000000000000001","ftnd":0,"is":1,"md5d":"888949798249ad7c53f8e30725a0361","phd":0,"pcx":0,"pfc":0,"pfs":0,"sha1d":"69d456e8aee4c4c99b932d1911feef0328a47"
(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
```

検出名

```
(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
```

脅威イベントの公開

スキャンが完了したら、イベントビューアでスキャンの概要を確認できます。

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.

イベントビューア

フラッシュスキャン

フラッシュスキャンは短時間で実行でき、完了までに数秒から数分かかります。この例では、スキャンがいつ開始されるかを確認できます。以前と同様に、SIDが指定されており、今回は値2458015が指定されています。

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

フラッシュスキャンの開始

次のアクションは、イベントをCSEクラウドに公開することです。

```
(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
```

スキャンが完了すると、イベントがクラウドに公開されます。

```
(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
```

スキャン終了パブリッシュ

イベントはWindowsイベントビューアで確認できます。ご覧のように、情報はログに表示される情報と同じです。

```
- <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>
```

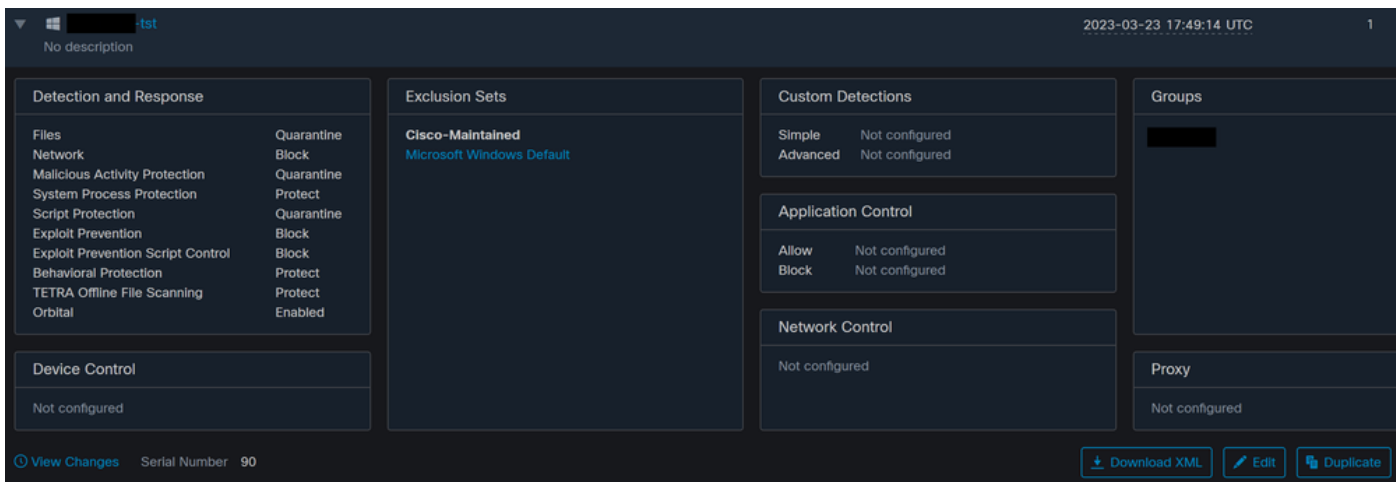
JSONイベント

スケジュール済みスキャン

スケジュール設定されたスキャンについては、一連の側面に注意する必要があります。

スキャンがスケジュールされると、シリアル番号が変更されます。

ここでは、テストポリシーにスケジュールされたスキャンはありません。



ポリシーのシリアル番号

スキャンをスケジュールする場合は、[編集]をクリックします。

移動先 [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

高度な設定

[New] をクリックします。

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

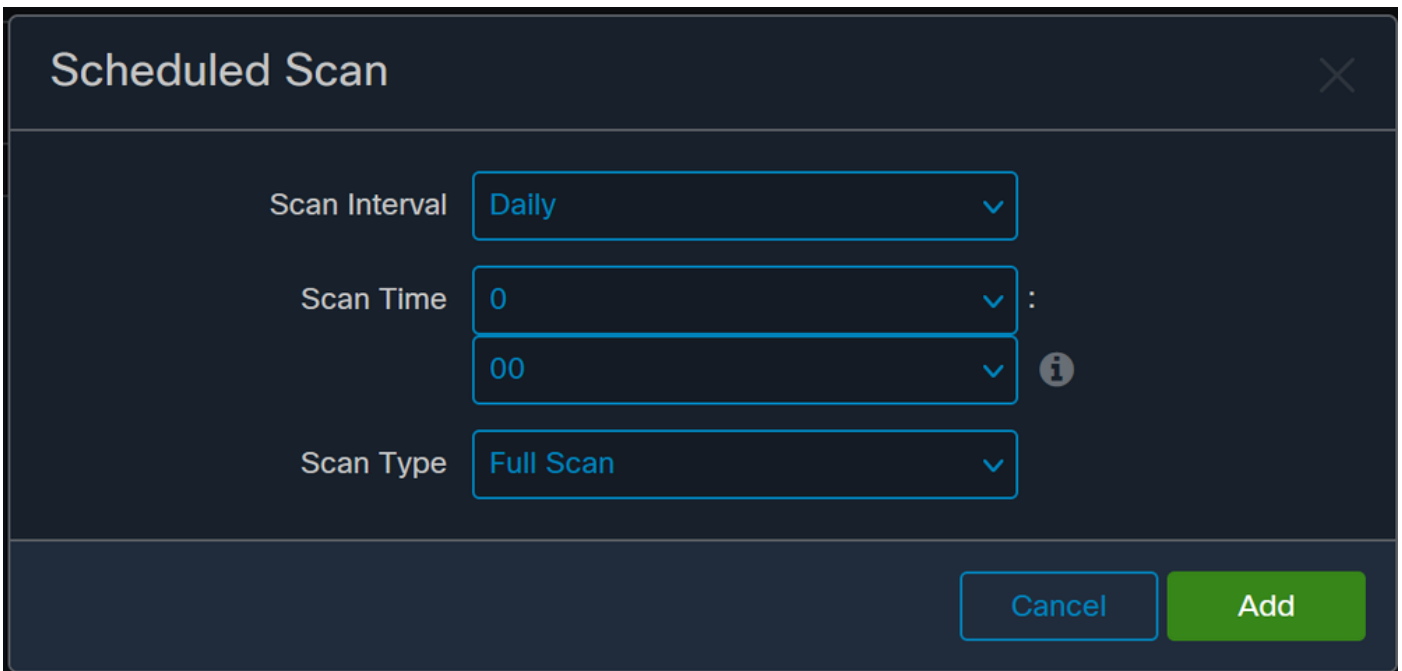
Schedule [+ New](#)

新しいスキャン構成

次のオプションがあります。

- スキャン間隔
- スキャン時間
- スキャンタイプ

スキャンを設定したら、Addをクリックします。



Scheduled Scan

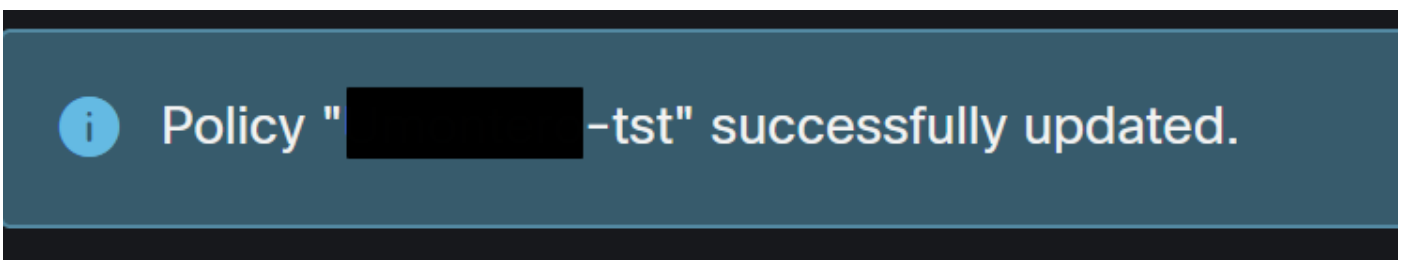
Scan Interval

Scan Time : ⓘ

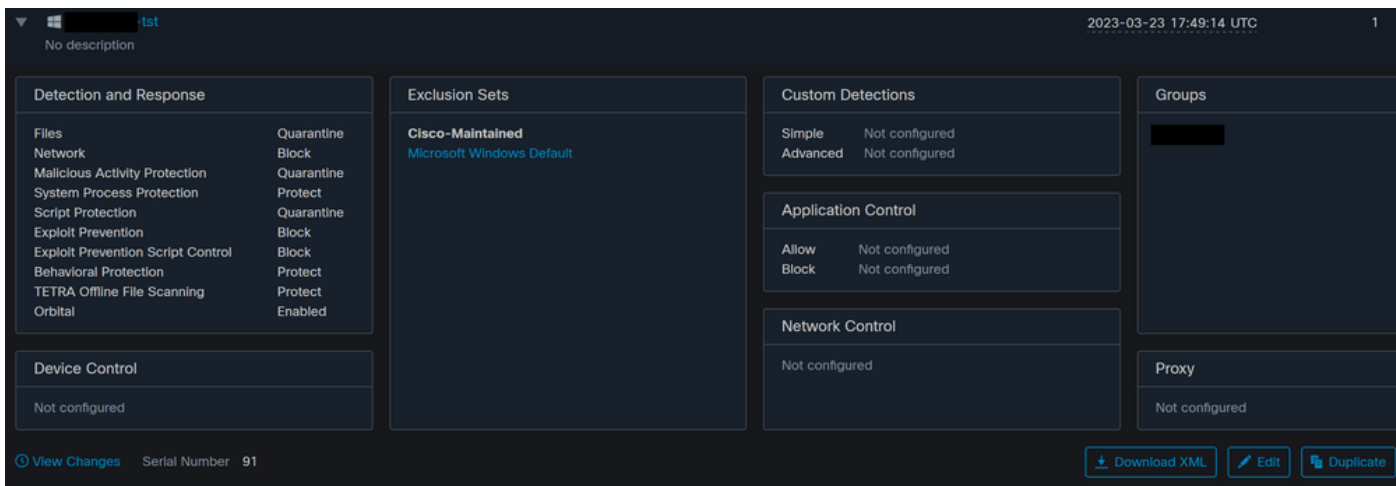
Scan Type

スケジュールされたスキャンの構成

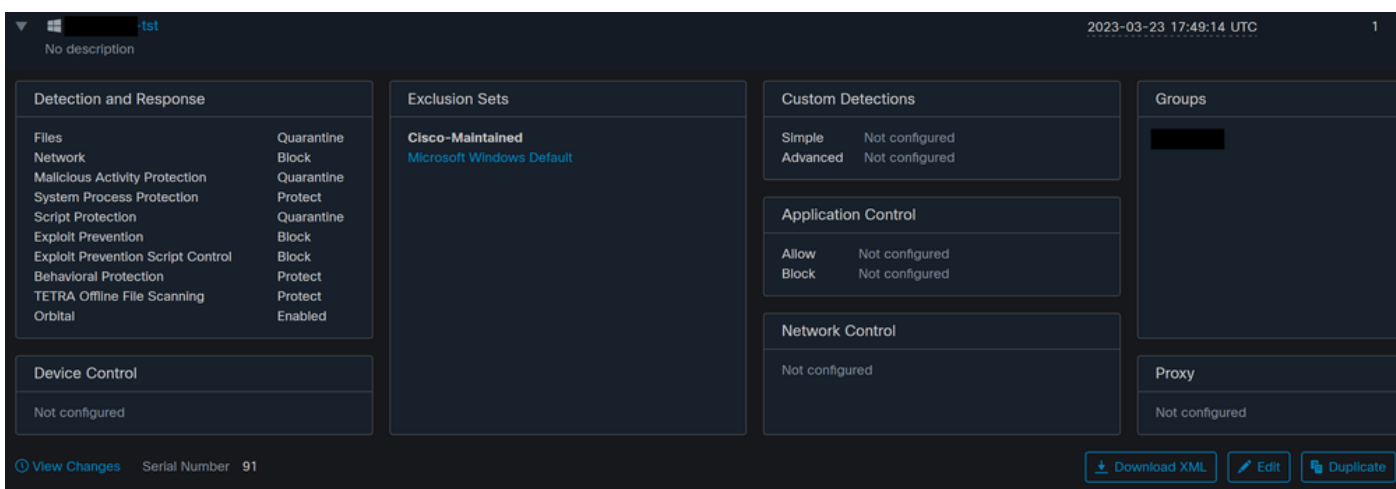
ポリシーの変更を保存すると、変更を確認するポップアップが表示されます。



ポップアップ



シリアル番号の変更



シリアル番号の変更

スキャンはポリシーで設定します。この例では、フラッシュスキャンとフルスキャンの2つのスキャンが設定されています。

```
<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>
```

ポリシーXML

HistoryDBのスケジューラに追加されます。<scheduled>タグの横の文字は、スキャンを識別するプロセスID(PID)です。

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

プロセス ID

図に示すように、それはキューに入れられます。

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

キューにスキャン

ログでスキャンを検索し、スキャンを今すぐ実行できるかどうかを確認できます。可能な場合は、スキャンが実行されます。

```
(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
```

スキャンは実行可能

スキャンのオプションがロードされ、ScanInitiatorプロセスがスキャンの開始を要求していることを確認できます。

```
(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: -
```

次に、プロセスScan::ScanThreadProcessがスキャンを開始します。

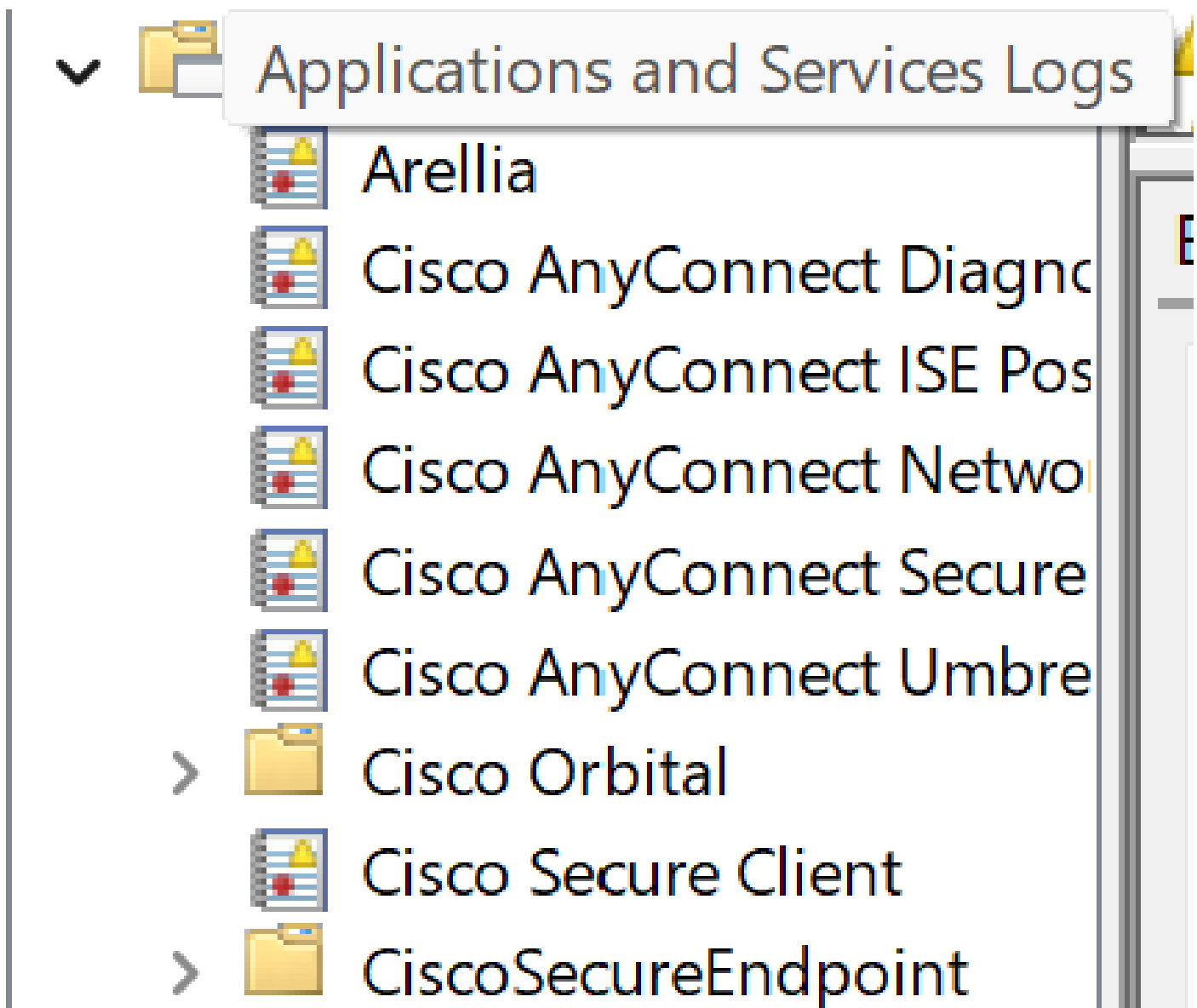
```
(86616093, +0 ms) Aug 25 18:43:59 [15372]: Scan::ScanThreadProcess: beginning scan id: 86616093, [type: 1, options: 3, 3, pid: 1661470488, initiator:
4]
```

前のイベントと同様に、CSEクラウドで公開する必要があります。ログからスキャンのタイプがわかります。この場合はFlashです。

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

スケジュールされたスキャンの発行イベント

次の場所に移動できます。 Event Viewer > App and Services Registries.



アプリケーションとサービスのログ

Cisco Secureエンドポイントを検索し、クラウドとイベントを開きます。各タブには異なるビューが表示されます。

イベント:

```
- <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>
```

イベントビュー

クラウド:

```
- <EventData>
  <Data Name="JsonEvent">{"iqlsa":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>
```

クラウドビュー

スキャンが完了すると、クラウドに公開されたイベントを確認できます。

```
(86641515, +0 ms) Aug 25 18:44:24 [3116]: imn::EventManager::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
```

スキャン終了パブリッシュ

スケジュールされたフルスキャン

図に示すように、Windows イベントビューアに「Event Scan Started」と表示されます。

```
- <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>
```

完了したら、パブリッシュされたイベントを比較できます。

```
(88165093, +0 ms) Aug 25 19:09:48 [18536]: imn::CEventManager::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
```

これは、Windowsのイベントビューアで確認できます。

```
- <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>
```

イベント ビューア

その他のスキャン

カスタムスキャンまたはルートキットスキャンの場合、主な違いは、イベントビューアまたはログのスキャンタイプです。

トラブルシュート

スケジュールスキャンが実行されない場合：

- スキャンが実行される時間までにエンドポイントが使用可能であることを確認します。
- スキャンがポリシーでスケジュールされていることを確認します。表示されない場合は、ポリシー同期をトリガーします。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。