

查看安全终端(CSE)Windows扫描

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[完全扫描](#)

[Flash扫描](#)

[计划扫描](#)

[ScheduledFull Scan](#)

[其他扫描](#)

[故障排除](#)

简介

本文档介绍Windows连接器的不同扫描类型。

先决条件

本文档的前提条件如下：

- Windows终结点
- 安全终端(CSE)版本v.8.0.1.21164或更高版本
- 访问安全终端控制台

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全终端控制台
- Windows 10终端
- 安全终端版本8.0.1.21164

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。

背景信息

扫描是在策略设置为debug的实验室环境中测试的。
安装时闪存扫描已通过连接器下载启用。
扫描是从安全客户端GUI和计划程序执行的。

完全扫描

此日志演示何时从CSE图形用户界面(GUI)请求完全扫描。

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

从用户界面扫描

此处，ScanInitiator进程开始扫描进程。

```
(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上触发的扫描类型，如图所示。

接下来，您有安全标识符(SID)，它是分配给此特定事件的可变长度值，此安全标识符可帮助您跟踪日志中的扫描。

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

发布事件

您可以通过CSE控制台将此事件与事件进行匹配。



G started scan		Scan Started	2022-08-23 23:06:01 UTC
Connector Details	Computer	[Redacted]	
Comments	Connector GUID	fae05a5d-3be2-4948-846e-69efaebc70eb	
	Cisco Secure Client ID	N/A	
	Processor ID	bfebfbff000806d1	
	Current User	None	
Run Scan		Device Trajectory	Management

控制台事件

接下来，在日志中，您可以看到以下内容：

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

发布成功

这意味着事件已成功发布到CSE云。

然后，下一步操作实际上是执行扫描：

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

扫描开始

您可以看到，SID是相同的，因此您处于SID流下1407343。

以下是扫描期间检测到威胁时连接器执行的步骤。

步骤1:连接器将告诉您导致检测的文件，在本示例中，该检测是由Hacksantana Trainer GLS导致的。

```
(2443984, +0 ms) Aug 23 18:23:18 [11964]: Scan_OnObjectScanComplete: threat types: 63  
(2443984, +0 ms) Aug 23 18:23:18 [17664]: imm::CEventManager::FileRoot \\?\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, , , ,  
(2443984, +0 ms) Aug 23 18:23:18 [11964]: Scan_OnObjectScanComplete action: 1 [5, 5]
```

检测到文件

第二步：事件将发布到CSE控制台，其中包含威胁检测名称和发现该事件的路径。

```
(2443984, +0 ms) Aug 23 18:23:18 [17664]: ERROR: imm::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]: imm::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","pbd":0,"pcx":0,"pfc":"0","pfs":"0","sha1d":"69d456e8aeec4c4c99b932d1911feef0328a47
```

检测名称

```
(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.Grafter.596528
```

威胁事件发布

扫描完成后，您可以查看“事件查看器”，了解扫描的摘要。

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.

事件查看器

Flash扫描

闪存扫描速度很快，需要几秒到几分钟才能完成。

在此示例中，您可以看到扫描何时开始，并且与之前一样，这次指定了一个SID，其值为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扫描开始

下一步操作是将事件发布到CSE云。

```
(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
```

扫描完成后，事件将发布到云。

```
(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
```

扫描完成发布

可以在Windows事件查看器中看到该事件。您会发现，该信息与日志中显示的信息相同。

```
- <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>
```

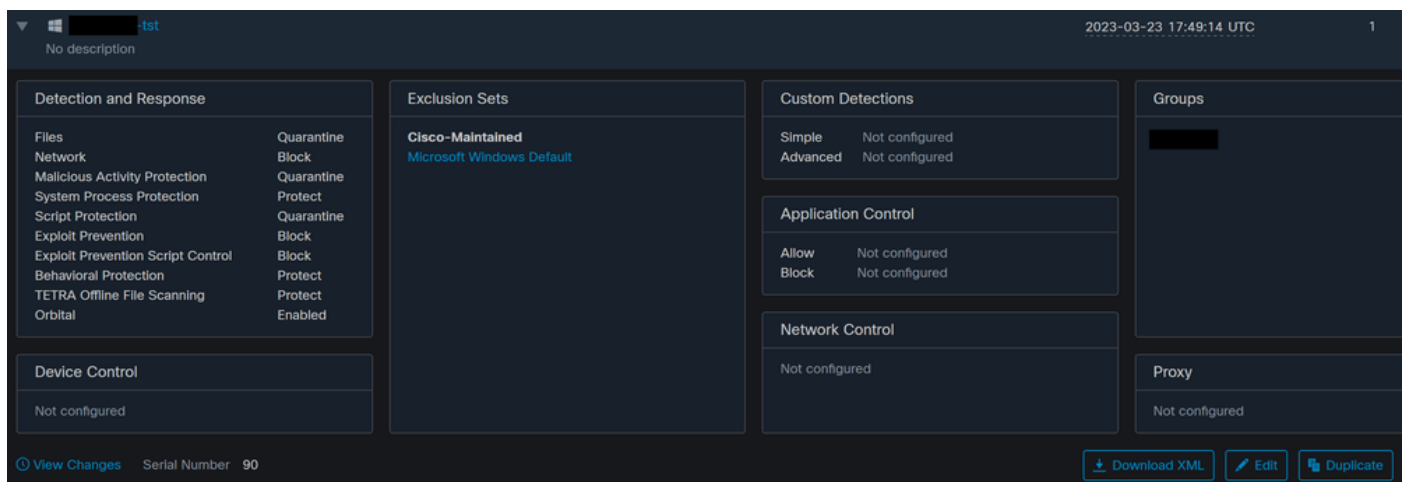
JSON事件

计划扫描

当涉及到计划扫描时，您必须了解一系列方面。

安排扫描后，序列号将发生变化。

此处，测试策略没有任何计划扫描。



策略序列号

如果要安排扫描，请点击编辑。

导航至 [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

高级设置

单击 New。

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

Schedule [+ New](#)

新扫描配置

选项有：

- 扫描间隔
- 扫描时间
- 扫描类型

配置扫描后，单击Add。

Scheduled Scan

Scan Interval


Scan Time :

Scan Type

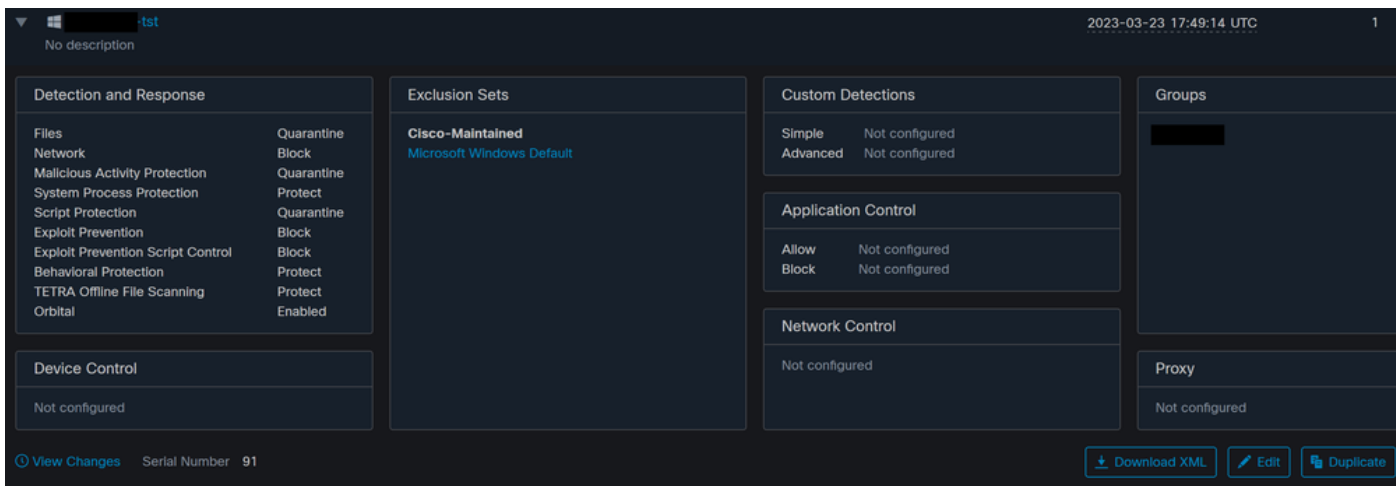
[Cancel](#) [Add](#)

计划扫描配置

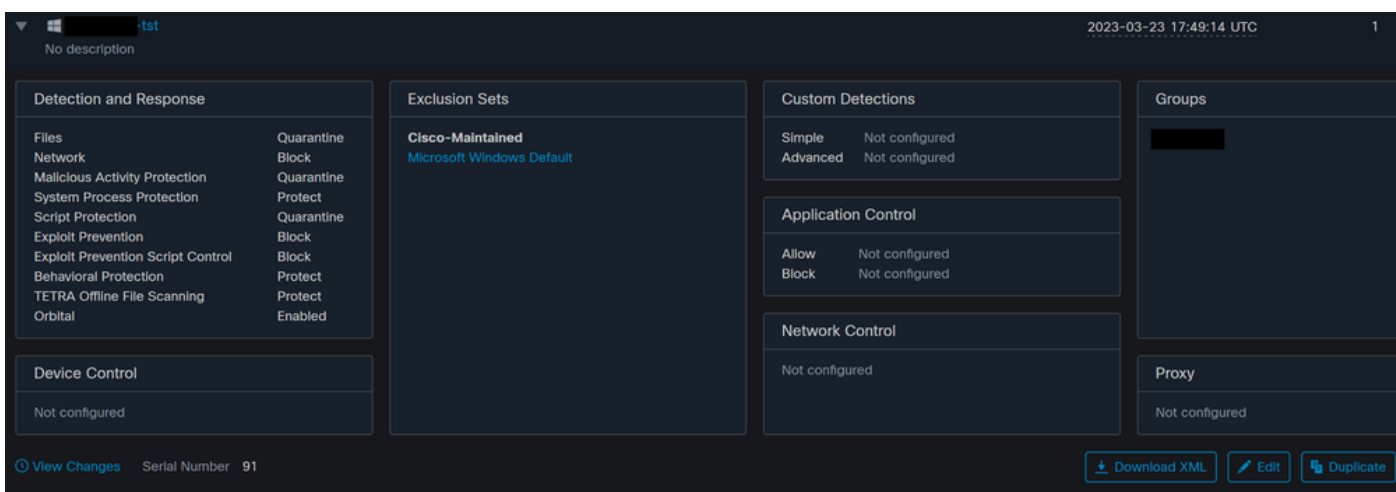
保存策略更改，系统将显示一个弹出窗口，确认您的更改。

 Policy " [redacted] -tst" successfully updated.

弹出窗口



序列号更改



序列号更改

扫描在策略中配置，在本示例中，两个扫描是配置的扫描，一个是闪存扫描，另一个是完全扫描。

```
<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|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|1|0|0|0|0</scheduled>
<maxarchivefilesize>52428800</maxarchivefilesize>
<maxfilesize>52428800</maxfilesize>
```


策略XML

它们将添加到HistoryDB中的调度程序。<scheduled>标记旁的字符是标识扫描的进程ID(PID)。

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

进程 ID

如图所示，它会排队。

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

扫描已排队

您可以在日志中搜索扫描，并注意扫描是否可以立即运行。如果可以，则执行扫描。

```
(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
```

可以执行扫描

您可以看到已加载扫描的选项，并且ScanInitiator进程请求开始扫描。

```
(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: -
```

然后，Process Scan::ScanThreadProcess将启动扫描。

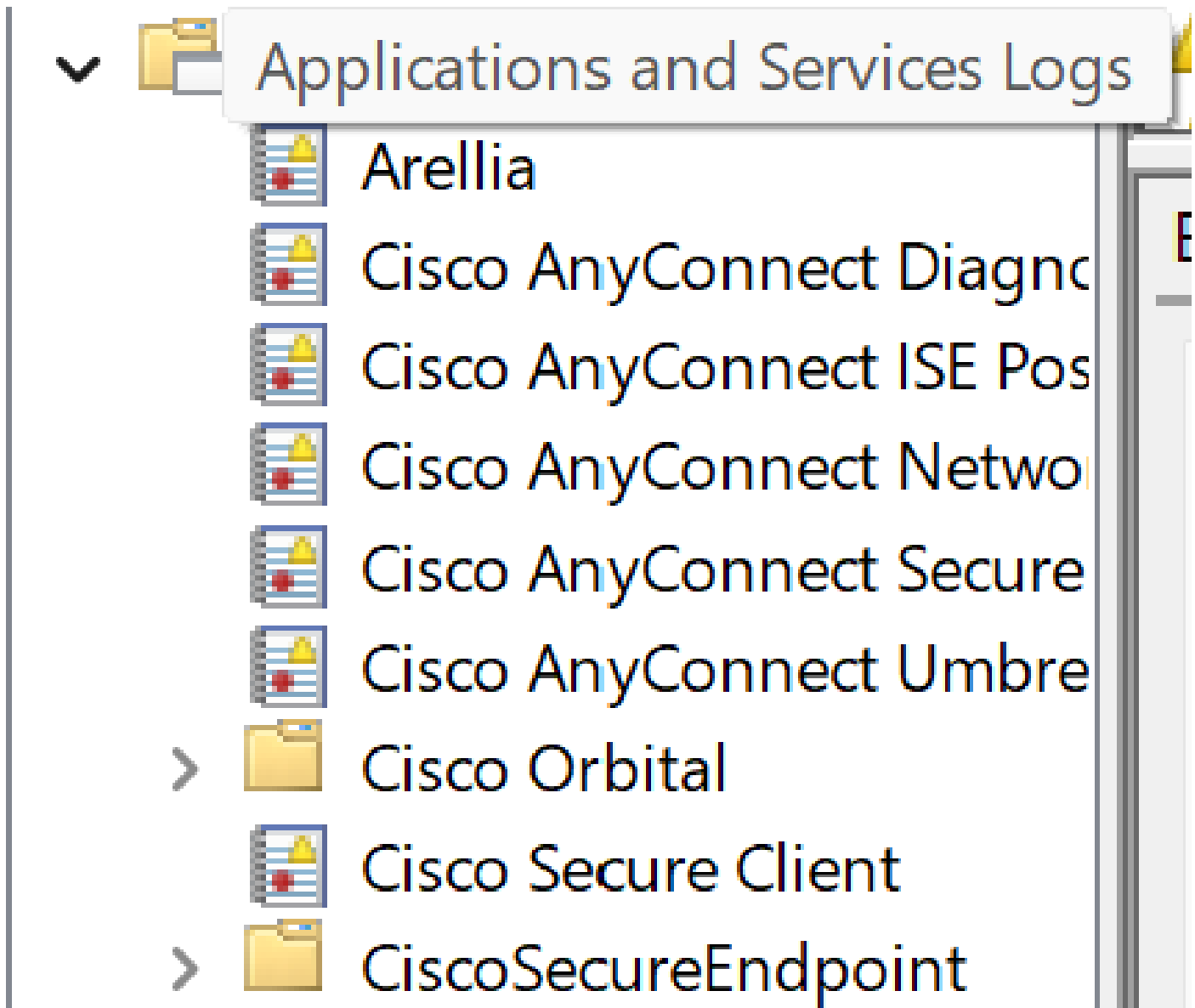
```
(86616093, +0 ms) Aug 25 18:43:59 [15372]: Scan::ScanThreadProcess: beginning scan id: 86616093, [type: 1, options: 3, 3, pid: 1661470488, initiator: 4]
```

与之前的活动相似，需要在CSE云中发布该报告。日志可以告诉您扫描的类型，在本例中为Flash。

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

发布计划扫描事件

您可以导航至 Event Viewer > App and Services Registries.



应用和服务日志

搜索思科安全终端，并打开云和事件。每个选项卡都为您提供不同的视图。

事件:

```
- <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>
```

事件视图

云：

```
- <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>
```

云视图

扫描完成后，您可以看到发布到云的事件。

```
(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
```

扫描完成发布

计划的完全扫描

Windows事件查看器显示Event Scan Started，如图所示。

```

- <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>

```

完成后，您可以比较已发布的事件。

```

(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的事件查看器中看到此消息。

```

- <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>

```

事件查看器

其他扫描

说到自定义扫描或rootkit扫描，您注意到的主要区别是事件查看器或日志中的扫描类型。

故障排除

计划扫描未发生时：

- 确保端点在扫描发生时可用。
- 确保在策略中安排了扫描。如果未看到它，则触发策略同步。

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）。