從面向終端的AMP Linux聯結器收集診斷資料

目錄

簡介

本文檔介紹從AMP端點版Linux聯結器生成診斷檔案的步驟。如果您遇到Linux聯結器的技術問題，思科技術支援工程師可能希望分析診斷檔案中可用的日誌消息。

生成診斷檔案

使用此命令，可以直接從Linux命令列介面(CLI)生成診斷檔案：

```
/opt/cisco/amp/bin/ampsupport
```

這樣會在案頭上建立。7z檔案。您可以將此檔案提供給思科技術協助中心(TAC)以進行進一步分析。

偵錯模式

聯結器的調試模式為日誌記錄提供了更多詳細資訊。它有助於深入瞭解聯結器問題。本節介紹如何在聯結器中啟用調試模式。

> **警告：**只有思科要求此資料時，才應啟用偵錯模式。如果啟用調試模式的時間更長，則它可能很快地耗盡磁碟空間，並且可能會由於檔案過大而阻止支援診斷檔案收集聯結器日誌。

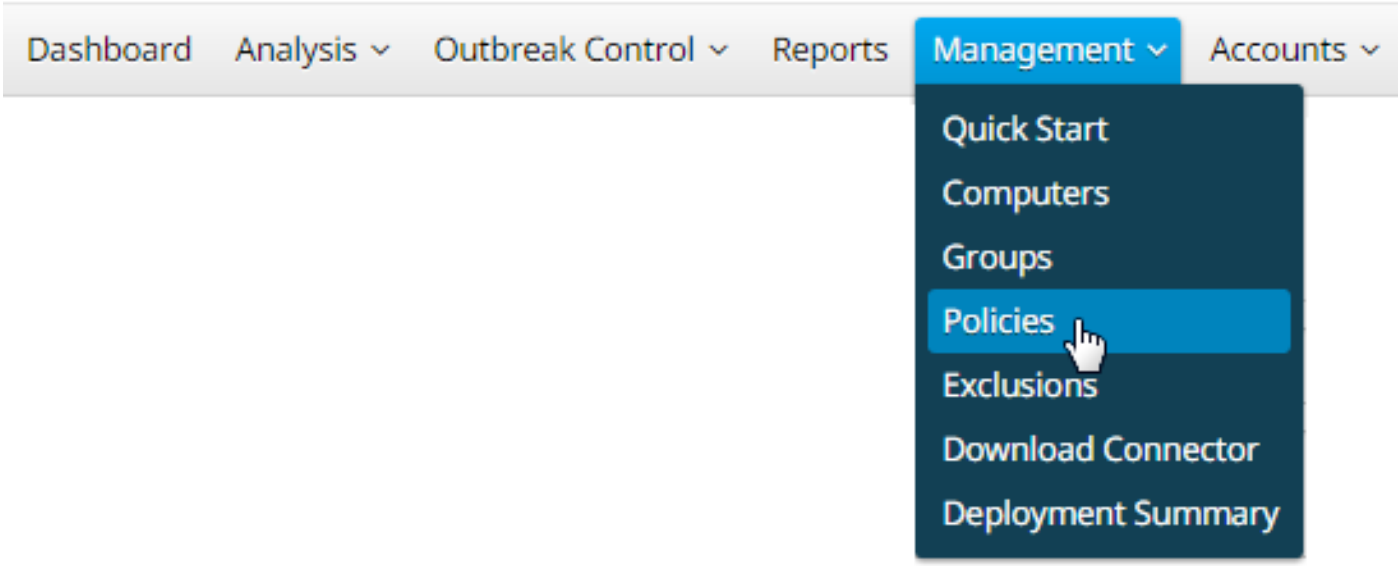
使用AMP控制檯

啟用調試模式

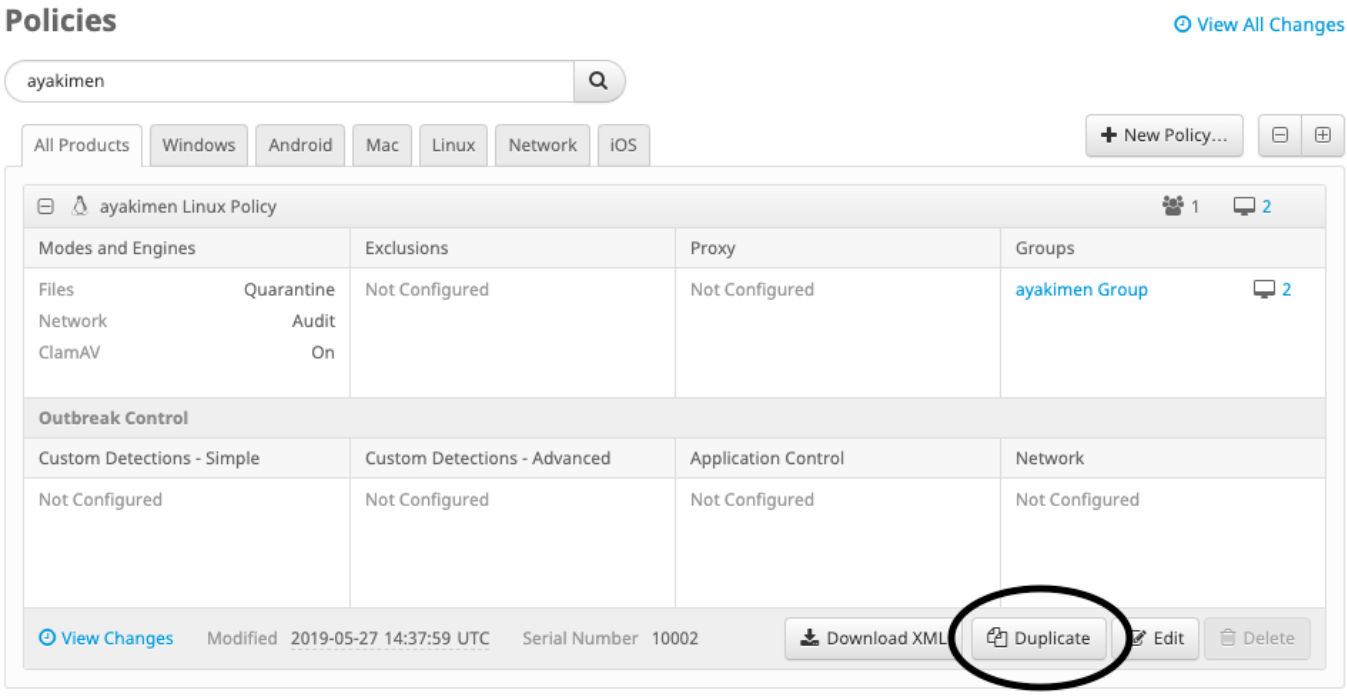
您可以使用步驟5至7在當前策略中啟用調試模式，或者使用以下所有步驟在調試模式下建立新策略：

步驟1.登入AMP控制檯。

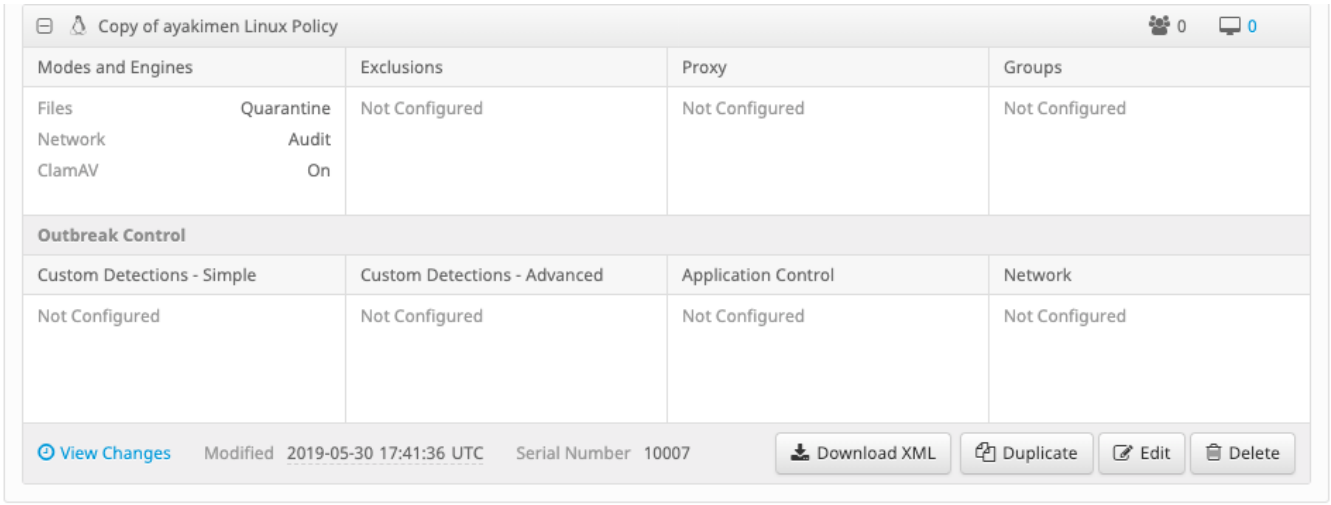
步驟2.選擇**管理>策略**。



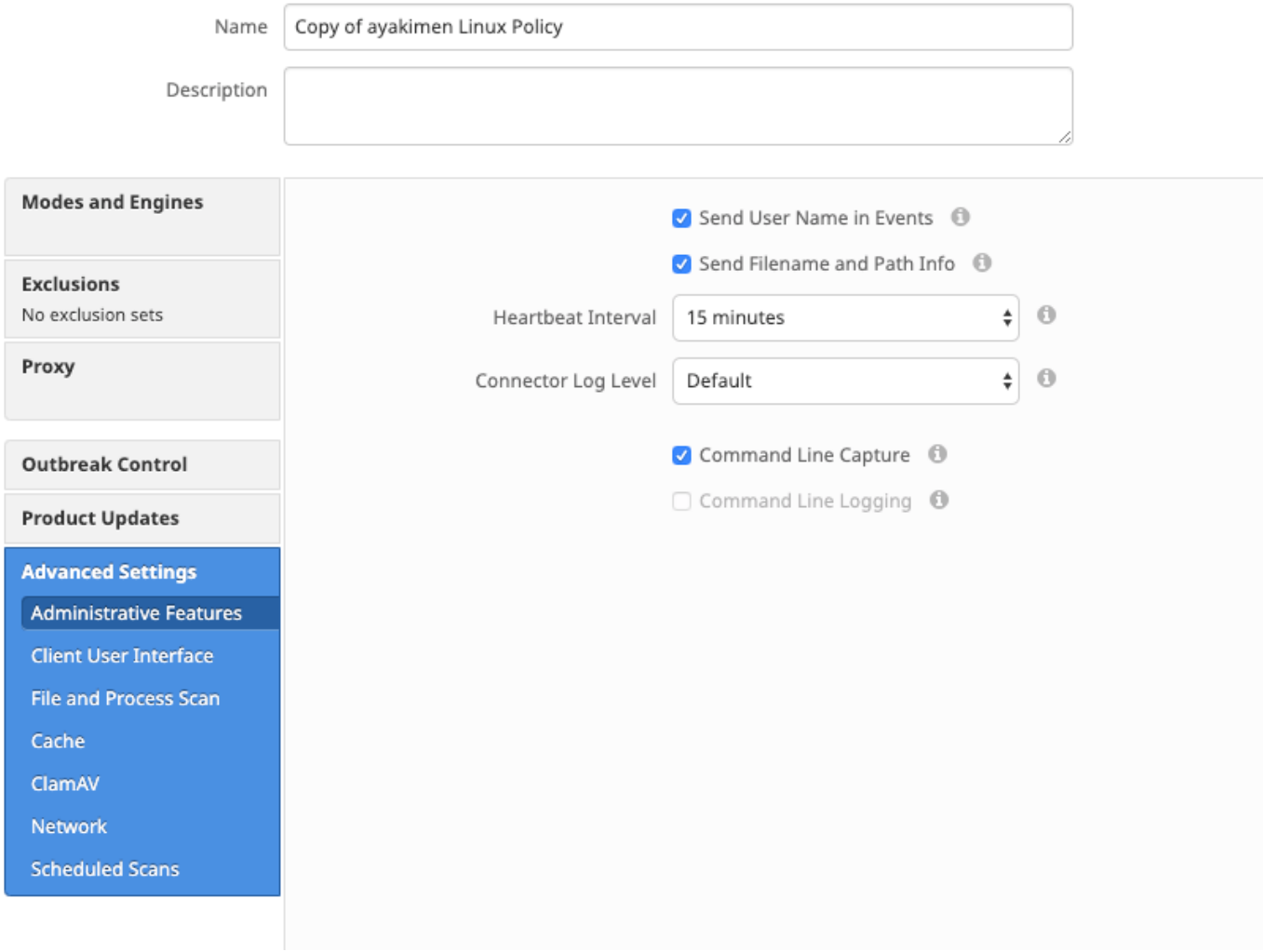
步驟3.找到應用到終端裝置或電腦的Policy，然後按一下Policy，這將展開Policy視窗。**按一下「複製」**。



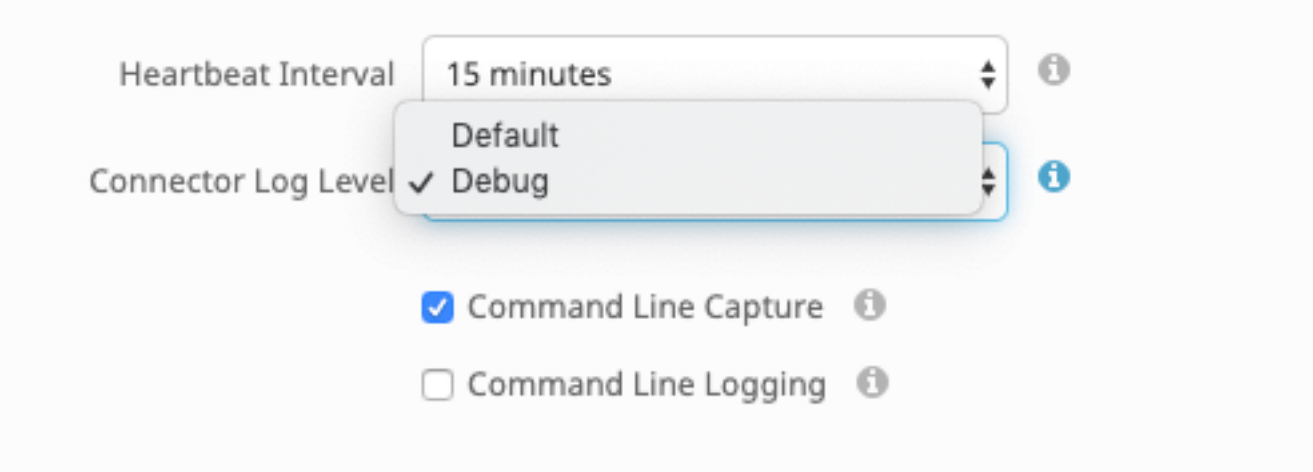
步驟4.按一下**Duplicate**後，AMP控制檯將使用複製的策略進行更新。



步驟5. **按一下Edit**，按一下**Advanced Settings**，然後從邊欄中選擇按一下Administrative功能。



步驟6. **ForConnector Log Level**，從下拉選單中選擇Debug。



步驟7.按一下Saveve以儲存變更內容。

步驟8.儲存新策略後，需要建立/更改組以包含新策略，並建立/更改要在其中生成調試資訊的*end* 裝置。

禁用調試模式

若要停用偵錯模式，請按照完成時的相同步驟執行以啟用偵錯模式，但將**Connector Log Level**變更為**Default**。

使用命令列

啟用調試模式

如果您遇到與控制檯的任何連線問題，並且想要啟用調試模式，請在CLI上運行以下命令：

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 1
```

輸出如下：

```
ampcli>debuglevel 1
Daemon now logging at 'info' level until next policy update
```

禁用調試模式

要禁用調試模式，請使用以下命令：

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

支援工具 調試時調整

在開始支援檔案調整之前，需要將聯結器的後台程式置於調試日誌記錄模式。此操作通過AMP控制檯通過*Management* -> Policies處的聯結器策*略設定完成*。編輯策略並轉到*Advanced Settings頁籤*下的*Administrative Features*部分。將*Connector Log Level*設定**更改為Debug**。

接下來，儲存策略。儲存策略後，請確保已將其同步到聯結器。在此模式下運行聯結器至少15-20分鐘，然後繼續調整其餘部分。

NB:調節完成後，不要忘記將*Connector Log* Levelsetting更改為Defaultso，以便聯結器以最有效率和最有效的模式運行。

運行支援工具

此方法涉及使用支援工具，該工具是隨AMP Mac聯結器一起安裝的應用程式。可通過按兩下/Applications->Cisco AMP->Support Tool.app從Applications資料夾訪問該應用程式。這將生成包含其他診斷檔案的完整支援包。

安 備選中， 更快中， 方法是運行 以下命令列自 答 終端 會話：

```
sudo /opt/cisco/amp/bin/ampsupport -x
```

```
sudo /opt/cisco/amp/bin/ampsupport
```

第一個選項將導致支援檔案大大減少，僅包含相關的最佳化檔案。第二個選項提供了一個完整的支援包，其中包含調整進程排除項（聯結器版本1.11.0及更新版本提供此項）可能需要的其他資訊，例如日誌。

無論您選擇哪種方式運行它，支援工具都會在~home上生成一個zip檔案，其中包含兩個最佳化支援檔案：fileops.txt和execs.txt。fileops.txt包含您電腦上最頻繁建立和修改的檔案清單，這些清單對於路徑/萬用字元排除非常有用。execs.txt將包含最常執行檔案的清單，這些檔案對於「進程排除」非常有用。這兩個清單均按掃描計數排序，表示最頻繁掃描的路徑出現在清單頂部。

使聯結器在調試模式下運行15-20分鐘，然後運行支援工具。經驗法則表明，在該時間內，平均命中次數為1000次或以上的任何檔案或路徑都是要排除的良好候選路徑。

排除調整

建立路徑、萬用字元、檔名和副檔名排除項

開始使用路徑排除規則的一種方法是，從fileops.txt中查詢最頻繁掃描的檔案和資料夾路徑，然後考慮為這些路徑建立規則。下載策略後，監控新的CPU使用情況。在更新策略後可能需要5到10分鐘才能注意到CPU使用率下降，因為守護程式可能需要一段時間才能趕上。如果仍然遇到問題，請再次運行該工具以檢視您觀察到的新路徑。

- 一個好的經驗法則是，任何具有日誌或日誌副檔名的事物都應被視為合適的排除候選對象。

建立進程排除

NOTE: Process Exclusions on Linux can only be implemented for ELF files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts).
有關流程排除的最佳實踐，請參閱： AMP端點版：MacOS和Linux中的進程排除

一個好的最佳化模式是，首先從execs.txt中識別執行量大的進程，找到執行檔的路徑，然後建立此路徑的排除。但是，有些流程不應包括在內，其中包括：

- 常規實用程式 — 建議不要排除常規實用程式(例如：usr/bin/grep)，而不考慮以下情況。 使用者可以確定哪個應用程式正在呼叫該過程(例如：查詢執行grep)的父進程，並排除父進程。若且唯若父進程可以安全轉換為進程排除時，才應執行此操作。如果父項排除應用於子項，則來自父進程的任何子項的呼叫也將被排除。可以確定正在執行此過程的使用者。(例如：如果使用者「root」正在大批次呼叫進程，則可以排除該進程，但只能針對指定的使用者「root」，這將允許AMP監控非「root」的任何使用者執行給定進程。**注意：Process Exclusions是Connector 1.11.0及更新版本中的新增功能。因此，通用實用程式可能會被用作聯結器1.10.2版及更舊版本中的路徑排除。但是，只有在絕對有必要進行效能折衷時，才建議使用此方法。**

查詢父進程對於進程排除非常重要。一旦找到該進程的父進程和/或使用者，該使用者就可以為特定使用者建立排除，並將該進程排除應用於子進程，而子進程又將排除本身不能成為進程排除的雜訊進程。

標識父進程

1. 按照上述步驟1-3確定父進程。
2. 使用以下方法之一確定進程的使用者： 從U：在日誌行中查詢給定進程的使用者ID(例如：U:0)。在Terminal視窗中運行以下命令：`getent passwd # | — d:-f1`，其中#是使用者ID。您應該會看到類似以下的輸出：`Username`，其中Username是給定進程的使用者。

3. 此 可以將使用者名稱新增到User類別下的Process Exclusion中，以減小排除的範圍，對於某些Process Exclusions而言，此作用非常重要。 **注意：如果進程的使用者是電腦的本地用戶，並且此排除必須應用於具有不同本地使用者的多個電腦，則「使用者」類別必須保留空白以允許「進程排除」應用於所有使用者。**

相關資訊

- 從Windows上運行的FireAMP聯結器收集診斷資料
- 從Mac OS上運行的FireAMP聯結器收集診斷資料
- **技術支援與文件 - Cisco Systems**