AMP端點版：Linux中的ClamAV病毒定義選項

目錄

簡介

從Linux Connector 1.11.0版開始，面向終端的AMP現在提供兩個ClamAV病毒定義配置選項：

1. 僅Linux
2. 完整ClamAV

在僅Linux選項可用之前，Linux Connector使用完整的ClamAV病毒定義集掃描檔案。該集合包含用於Linux、macOS、Windows和Android的惡意軟體簽名。雖然這樣可提供全面的覆蓋範圍，但還需要大量運行時資源（即CPU時間和記憶體）。 某些Linux系統可以將AMP配置為使用較小的僅Linux的ClamAV病毒定義集。

僅Linux病毒定義檔案的大小小於完整檔案集的10%。使用較小的集合可以降低計算開銷，並且可以在資源受限系統上運行AMP。儘管具有效能優勢，但減少非Linux惡意軟體的覆蓋範圍使此配置僅適用於某些應用。例如，它適用於只託管/儲存Linux檔案的伺服器（例如應用程式伺服器），但不適用於同時託管/儲存非Linux檔案的伺服器（例如FTP、郵件和SMB檔案伺服器）。 系統管理員必須權衡此權衡，才能選擇適當的病毒定義集。

> **重要！**
>
> 強烈建議在使用新的僅Linux病毒定義選項之前，將所有端點升級到聯結器版本1.11.0或更新版本。雖然1.10.x及更舊版本的聯結器將接受新選項，但在某些情況下，其行為將是不直觀的。有關詳細資訊，請參閱*向後相容*部分。

向後相容性

在將終端配置為使用新的僅Linux病毒定義選項之前，需要考慮重要的向後相容性問題：如果已下載完整版1.10.x和更早版本的聯結器，則將繼續使用完整的病毒定義。如果配置為使用新的僅Linux病毒定義選項，則Connector將停止更新完整的病毒定義集，並且之後將僅更新Linux病毒定義集。這可能導致終端使用最新的Linux病毒定義，但使用過時的macOS、Windows和Android定義。

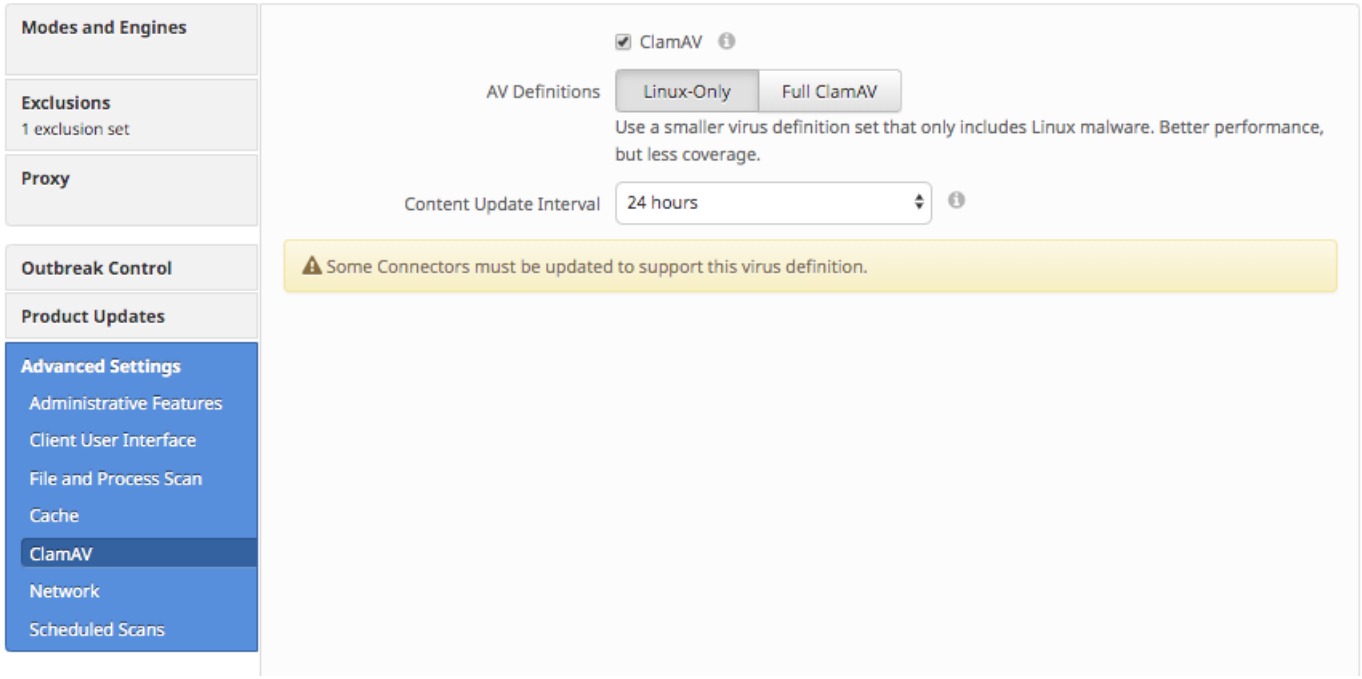
有兩種可能的解決方案：

1. 將聯結器升級到1.11.0或更高版本。
2. 將ClamAV病毒定義設定更改回完整ClamAV。

更改ClamAV病毒定義選項

可使用面向終端的AMP網路門戶配置ClamAV病毒定義選項。可通過導航到以下各項來更改每個策略的選項：

管理>策略> [Linux策略] >編輯>高級設定> ClamAV



更改「AV定義」策略設定後，新設定將在下次計畫病毒定義更新時生效。該延遲由「內容更新內部」策略設定控制。

如果策略管理的至少有一個聯結器運行的是不相容的Linux聯結器版本，則「某些聯結器必須更新以支援此病毒定義」警告可能會出現在ClamAV高級設定螢幕中。強烈建議在使用僅Linux定義設定之前升級聯結器並解決此警告。

驗證終端的新設定

當配置為使用僅Linux定義時，兩個AMP聯結器進程的合併駐留記憶體大小應低於100 MB。

可以使用以下命令檢查此問題：

```
top -p `pidof ampdaemon` -p `pidof ampscansvc`
```

以下是輸出示例：

```
top - 23:52:51 up 15:11,  7 users,  load average: 0.36, 1.10, 0.83
Tasks:   2 total,   0 running,   2 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.5 us,  0.5 sy,  0.0 ni, 97.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3861508 total,   309220 free,  1732560 used,  1819728 buff/cache
KiB Swap:  2097148 total,  2064116 free,    33032 used.  1629348 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
88910 root      20   0 1323172  32904   6752 S   0.7  0.9   3:20.16 ampdaemon
88937 cisco-a+  20   0  258764   8400   2704 S   0.0  0.2   1:23.73 ampscansvc
```