面向终端的AMP:Linux中的ClamAV病毒定义选项

目录

简介

从Linux连接器版本1.11.0开始，面向终端的AMP现在提供两个ClamAV病毒定义配置选项：

1. 仅Linux
2. 全ClamAV

在仅Linux选项可用之前，Linux连接器使用完整的ClamAV病毒定义集扫描文件。此集包括Linux、MacOS、Windows和Android的恶意软件签名。虽然这提供了全面的覆盖，但它也需要大量运行时资源（即CPU时间和内存）。 某些Linux系统可以从配置AMP以使用较小的仅Linux ClamAV病毒定义集中获益。

仅Linux的病毒定义文件大小不到完整集的10%。使用较小的集可减少计算开销，并使在资源受限的系统上运行AMP成为可能。尽管具有性能优势，但非Linux恶意软件的覆盖范围缩小使此配置仅适用于某些应用。例如，它适用于仅托管/存储Linux文件（如应用服务器）的服务器，但不适用于同时托管/存储非Linux文件（如FTP、邮件和SMB文件服务器）的服务器。 系统管理员必须平衡此权衡，才能选择适当的一组病毒定义。

> **重要！**
>
> 强烈建议在使用新的仅Linux病毒定义选项之前，将所有终端升级到连接器版本1.11.0或更高版本。虽然1.10.x及更旧的连接器版本将接受新选项，但在某些情况下，其行为将不直观。有关详细信息，*请参阅向后*兼容部分。

向后兼容性

在将终端配置为使用新的仅Linux病毒定义选项之前，需要考虑一个重要的向后兼容性问题：1.10.x和更旧的连接器将继续使用完整病毒定义（如果已下载完整集）。如果配置为使用新的仅Linux病毒定义选项，连接器将停止更新完整病毒定义集，并且仅在此后更新Linux病毒定义集。这可能导致终端使用最新的Linux病毒定义，但使用过时的macOS、Windows和Android定义。

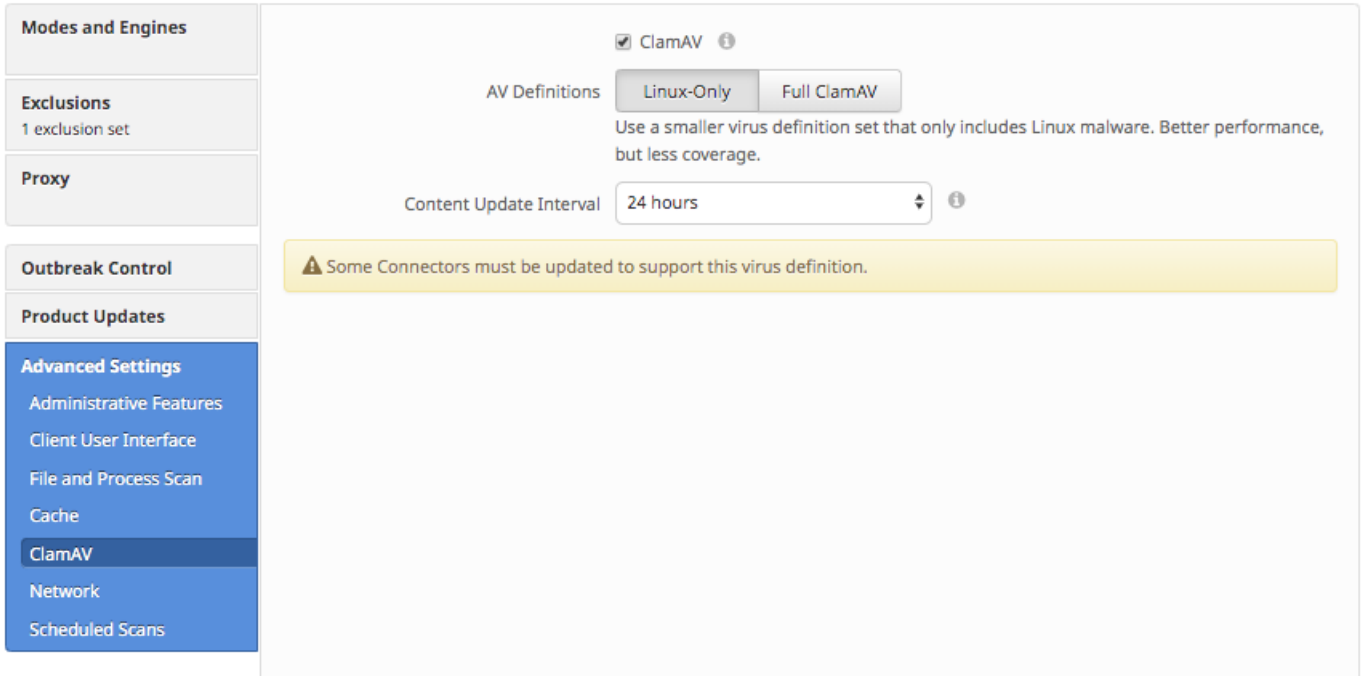
有两种可能的解决方案：

1. 将连接器升级到1.11.0或更高版本。
2. 将ClamAV病毒定义设置改回Full ClamAV。

更改ClamAV病毒定义选项

ClamAV病毒定义选项可以使用面向终端的AMP Web门户进行配置。导航至以下位置可更改每个策略的选项：

管理>策略> [Linux策略] >编辑>高级设置> ClamAV



更改AV定义策略设置后，新设置将在下次计划的病毒定义更新时对终端生效。该延迟受“内容更新内部”策略设置控制。

如果策略管理的至少一个连接器运行的Linux连接器版本不兼容，ClamAV Advanced Settings（ClamAV高级设置）屏幕中可能会显示“Some Connectors must be updated to support this virus definition（必须更新某些连接器以支持此病毒定义）”警告。强烈建议在使用仅Linux定义设置之前升级连接器并解决此警告。

在终端验证新设置

当配置为使用仅Linux定义时，两个AMP连接器进程的合并驻留内存大小应低于100 MB。

可以使用以下命令检查此问题：

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

以下是输出示例：

```
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
```