从面向终端的AMP的终端Linux连接器收集诊断数据

目录

简介

本文档介绍从面向终端的AMP Linux连接器生成诊断文件的步骤。如果您遇到Linux连接器的技术问题，思科技术支持工程师可能想分析诊断文件中可用的日志消息。

生成诊断文件

使用此命令，您可以直接从Linux命令行界面(CLI)生成诊断文件：

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

这会在桌面上创建。7z文件。您可以将此文件提供给思科技术支持中心(TAC)以供进一步分析。

调试模式

连接器的调试模式为日志记录提供了更多详细信息。它可更深入地了解连接器的问题。本节介绍如何在连接器中启用调试模式。

> **警告**：只有在思科请求此数据时，才应启用调试模式。如果您启用调试模式的时间更长，则它可以非常快地填满磁盘空间，并可能由于文件大小过大而阻止支持诊断**文件**收集连接器日志。

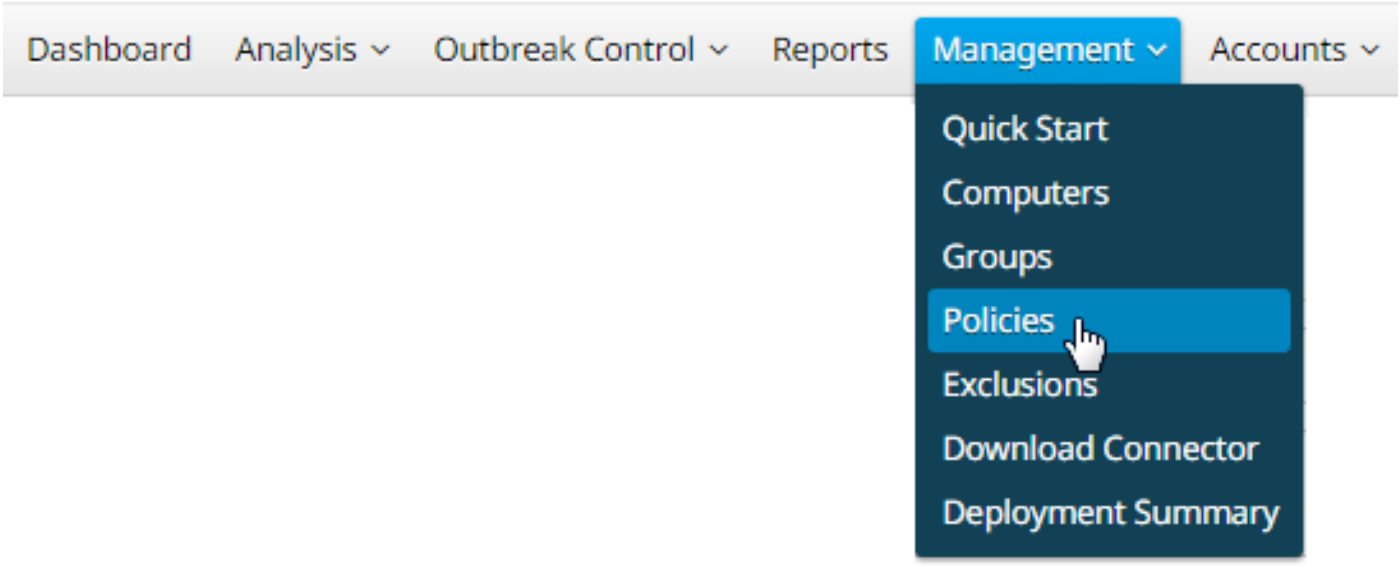
使用AMP控制台

启用调试模式

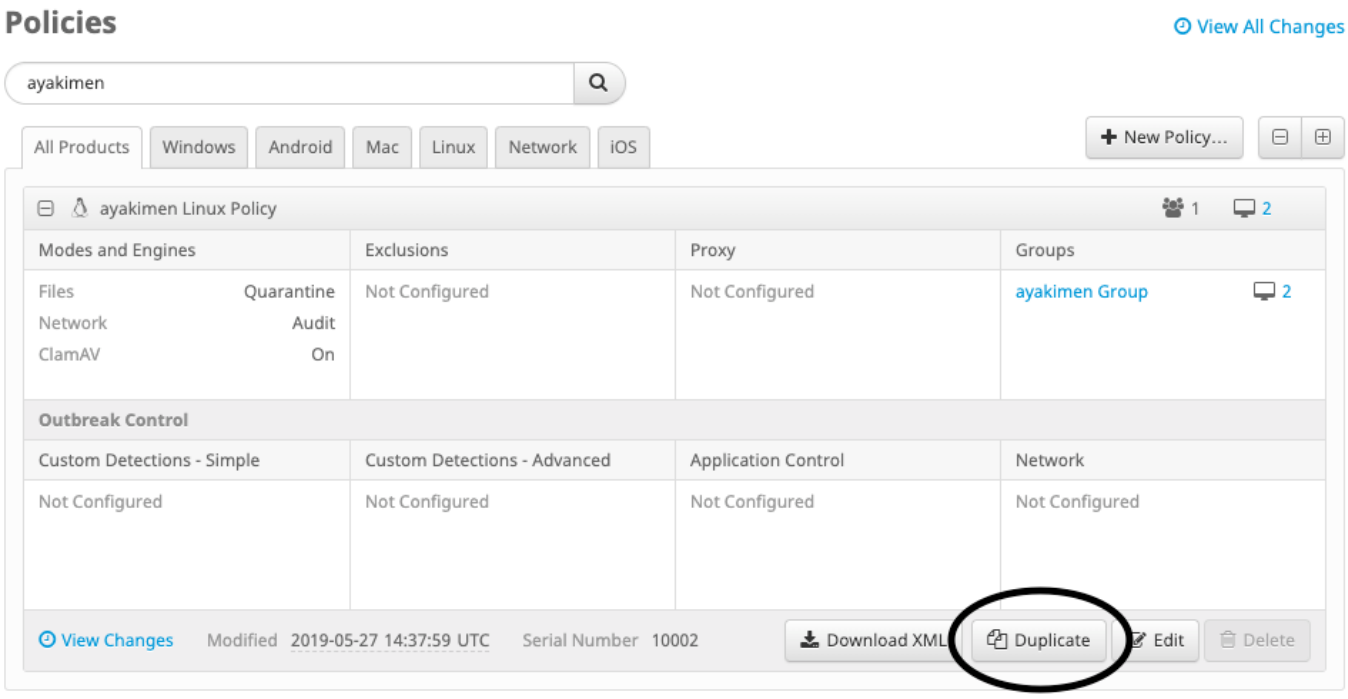
您可以在当前策略中启用调试模式（步骤5 - 7），或在调试模式下创建新策略(步骤如下：

步骤1.登录AMP控制台。

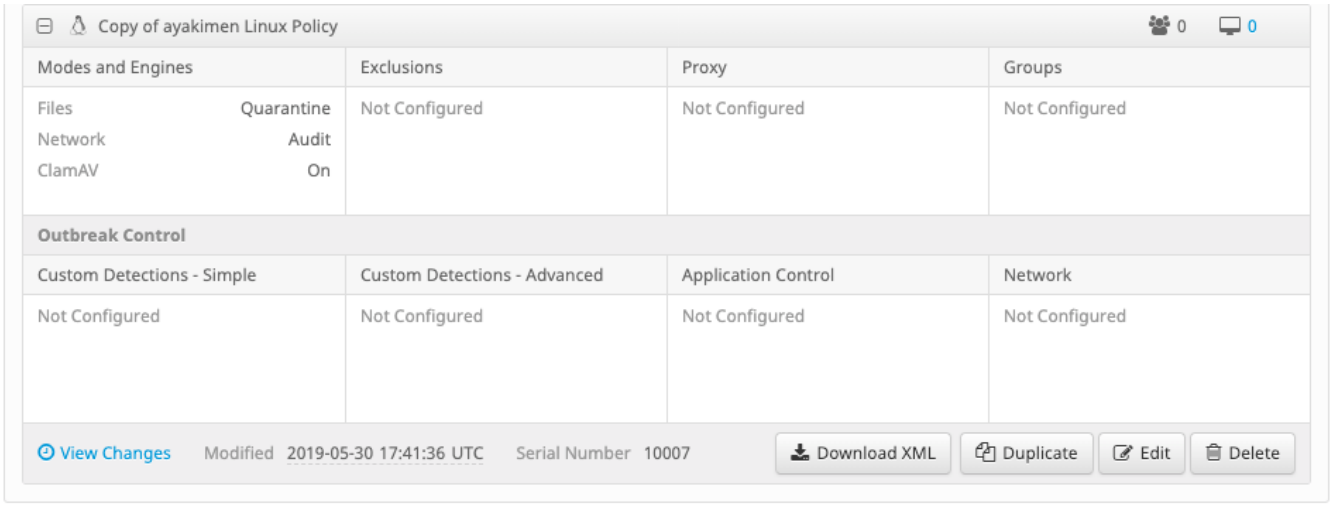
步骤2.选择**Management > Policies**。



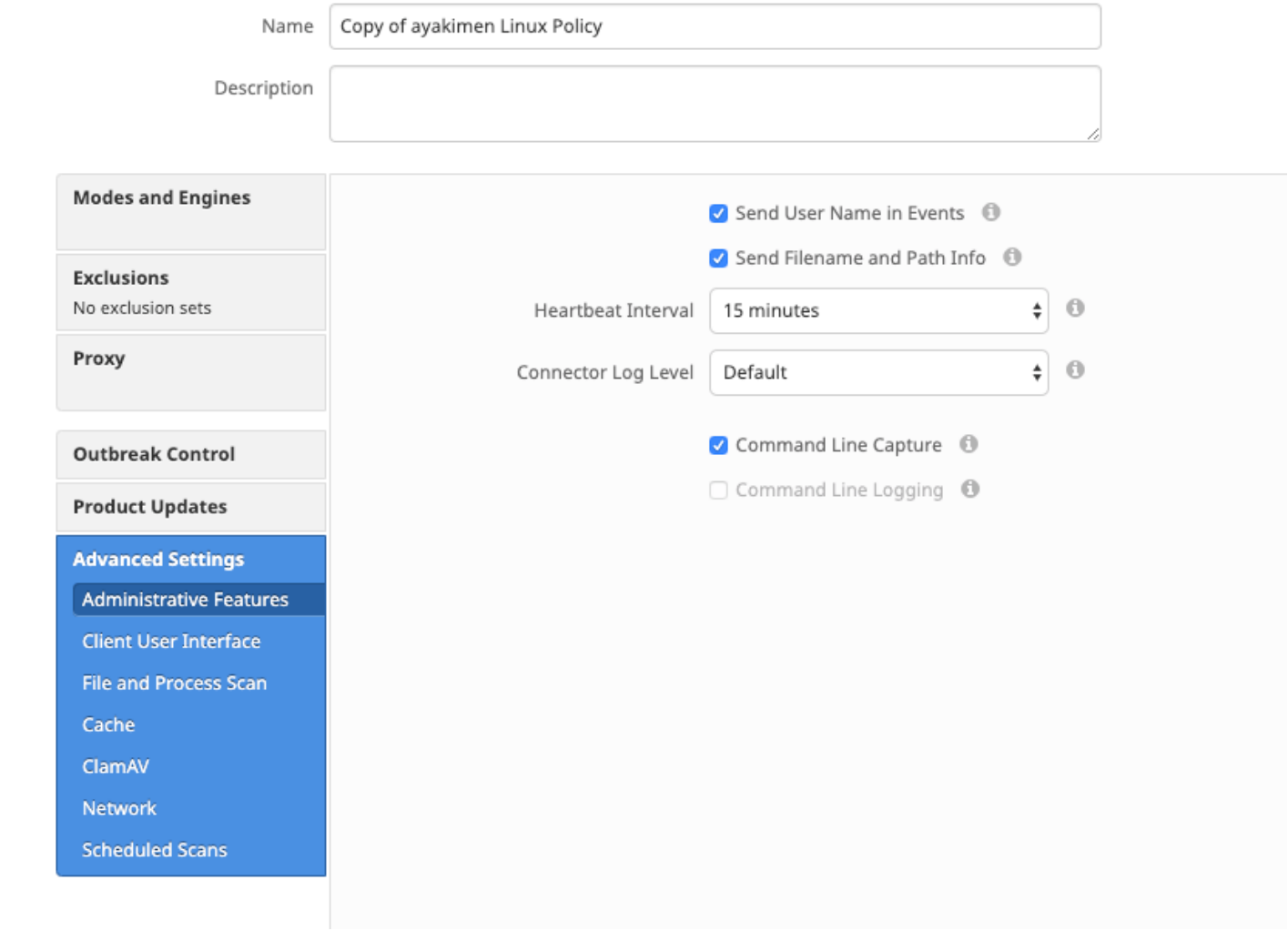
步骤3.找到应用于终端设备或计算机的策略，然后点击策略，这将展开策略窗口。**单击"复制**"。



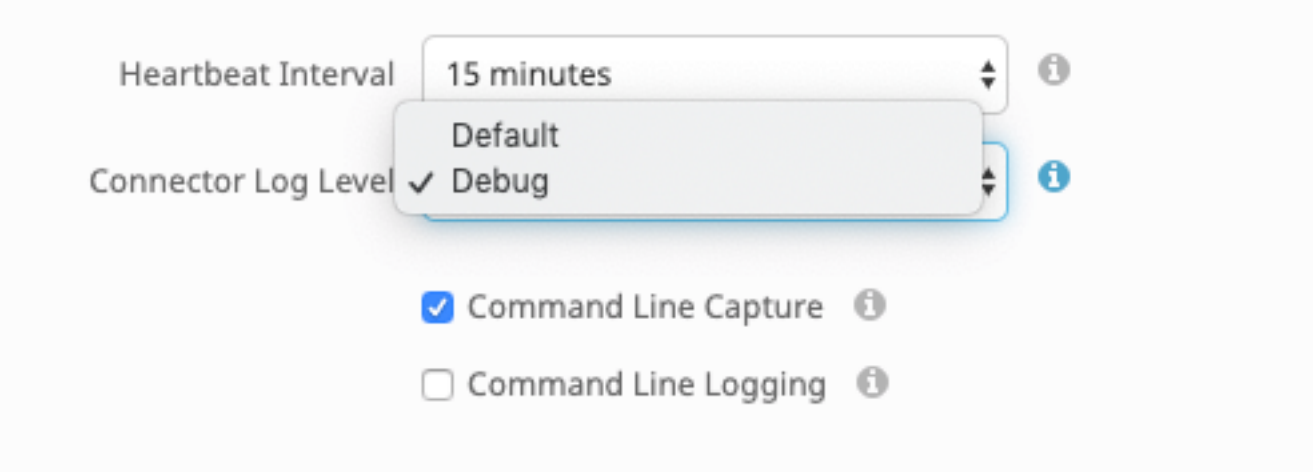
步骤4.单击"重复"**后**,AMP控制台将使用复制的策略进行更新。



步骤5.单击**“编辑”**,**单击“高级设置”**，然后从侧栏中选择**单击“管理功能”**。



步骤6.对**于Connector日志级别**,从下拉列表中选择Debug。



步骤7.单击“保存”以保存更改。

步骤8.保存新策略后，需要创建/更改组以包括新策*略和*要生*成调试*信息的终端设备。

禁用调试模式

要禁用调试模式，请按照完成的步骤启用调试模式，但将“Connector Log Level（连接器日志级别）”更**改为“Default(默**认)**”**。

使用命令行

启用调试模式

如果在控制台上遇到任何连接问题，并且要启用调试模式，请在CLI上运行以下命令：

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

这是输出：

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

禁用调试模式

要禁用调试模式，请使用以下命令：

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

支持工具 调试时调整

连接器的守护程序需要进入调试日志记录模式，然后才能开始调整支持文件。这通过AMP控制台，通过Management -> Policies中连接器的策略设*置完成*。编辑策略并转到“高级设*置*”选项卡下的*“管理*功能”部分。将Connector *Log Level*设置更改**为Debug**。

接下来，保存策略。保存策略后，请确保它已同步到连接器。在此模式下运行连接器至少15-20分钟

，然后继续其余调整。

NB:当调整完成时，不要忘记将连接器日志*级别设*置改回Defaultso，即连接器以其最有效模式运行。

运行支持工具

此方法包括使用支持工具，该工具是随AMP Mac连接器安装的应用。通过双击/Applications->Cisco AMP->Support Tool.app，可从Applications文件夹访问它。这将生成包含其他诊断文件的完整支持包。

安 替代, 更快, 方法是运行 以下命令行从 a 终端 会话：

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

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

第一个选项将生成一个小得多的支持文件，其中仅包含相关调整文件。第二个选项提供完整的支持包，其中包含调整进程排除项（连接器版本1.11.0及更高版本中提供）可能需要的更多信息（如日志）。

无论您选择哪种方式运行它，支持工具都会在您的~home上生成一个包含两个优化支持文件的zip文件：fileops.txt和execs.txt。fileops.txt包含计算机上最频繁创建和修改的文件的列表，这些文件对路径/通配符排除非常有用。execs.txt将包含最频繁执行的文件列表，这些文件对进程排除非常有用。两个列表都按扫描计数排序，这意味着最频繁扫描的路径出现在列表顶部。

使连接器在调试模式下运行15-20分钟，然后运行支持工具。一个好的经验法则是，在此期间平均点击次数达到或超过1000次的任何文件或路径都是应该排除的优秀候选者。

排除调整

创建路径、通配符、文件名和文件扩展名排除

开始使用路径排除规则的一种方法是从fileops.txt中查找最常扫描的文件和文件夹路径，然后考虑为这些路径创建规则。下载策略后，监控新的CPU使用率。策略更新后可能需要5到10分钟，您才会注意到CPU使用率下降，因为守护程序可能需要一些时间才能赶上。如果您仍在看到问题，请再次运行该工具以查看您观察到的新路径。

- 一个好的经验法则是，任何具有日志或日志文件扩展名的内容都应被视为合适的排除候选项。

创建进程排除

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).
有关流程排除的最佳实践，请参阅： 面向终端的AMP:MacOS和Linux中的进程排除

一个好的调整模式是首先从execs.txt中识别执行量较大的进程，找到可执行文件的路径，并为此路径创建排除项。但是，有些进程不应包括，这包括：

- 一般公用程序 — 不建议排除一般公用程序(例如：usr/bin/grep)，但不考虑以下因素。 用户可以确定调用该流程的应用程序(例如：查找正在执行grep的父进程)并排除父进程。如果且仅当父进程可以安全地设置为进程排除时，才应执行此操作。如果父排除适用于子代，则父进程中对任何子代的调用也将被排除。可以确定正在执行该进程的用户。（例如：如果用户“root”在大量调用进程，则可以排除该进程，但仅针对指定用户“root”，这将允许AMP监控任何非“root”用户对给定进程的执行。)**注意：Process Exclusions是连接器版本1.11.0及更高版本中的新增功能。因此，一般实用程序可能用作连接器版本1.10.2及更早版本中的路径排除。但是，只有在绝对需要取舍性能时，才建议采用此做法。**

查找父进程对于进程排除非常重要。一旦找到进程的父进程和/或用户，用户就可以为特定用户创建排除项并将进程排除项应用到子进程，子进程又将排除本身不能被设置为进程排除项的噪声进程。

确定父进程

1. 按照上述“识别父进程”的步骤1-3操作。
2. 使用以下方法之一确定进程的用户： 从U：在日志行中查找给定进用户ID(例如：U:0)。在“终端”窗口中，运行以下命令：`getent passwd # | – d:-f1`，其中#是用户ID。您应看到类似于`Username`的输出，其中Username是给定进程的用户。
3. 此 用户名可以添加到“用户”类别下的“进程排除”(Process Exclusion)中，以缩小排除范围，这对于某些“进程排除”(Process Exclusions)非常重要。 **注意**

：如果进程的用户是计算机的本地用户，并且此排除必须应用于具有不同本地用户的多台计算机，则必须将“用户”类别留空，以允许进程排除应用于所有用户。

相关信息

- 从Windows上运行的FireAMP连接器收集诊断数据
- 从Mac OS上运行的FireAMP连接器收集诊断数据
- **技术支持和文档 - Cisco Systems**