终端的AMP ：在macOS和Linux的进程排除

Contents

Introduction

开始从连接器版本1.11.0，终端的AMP添加进程排除的技术支持在macOS和Linux。以前，配置AMP忽略macOS或Linux应用程序的活动要求了路径、文件扩展和通配符排除规则的组合。因为这些规则目标文件和目录，并且不可能与程序或进程产生关联，多个规则为每个程序经常是需要的，并且每个规则可能从超过一个程序不必要地排除活动。进程排除提供一个更加直接和更加准确的方式排除应用程序的活动。当使用适当地，进程排除能极大改进与最小的负面作用的AMP性能对系统安全。

进程排除规则在终端Web控制台的AMP管理。每个规则包括：

- 充分的(绝对)路径向程序可执行，
- 进程的用户名(可选)，和
- 是否应该也排除子进程(默认值：否)

当进程排除规则匹配一个运行的进程、该进程执行的所有活动和可选地其子进程时，从扫描被排除。

> **重要!**
>
> 增加在Mac和Linux连接器1.11.0的进程排除，现有路径的解释，文件扩展和通配符规则也更改。没有在工作情况上的变化1.10.x和更旧的连接器的。然而，在1.11.0的同样规则不会适用作为宽广地。*参考对路径、文件扩展和通配符排除规则的*部分*更改*关于详细资料。

准备进程排除

有三个重要考虑在升级您的macOS和Linux终端前：

1. 1.10.x和更旧的连接器忽略进程排除规则。
2. 1.11.0和更新的连接器荣誉称号进程排除规则，但是解释路径，文件扩展，并且通配符跟更旧的连接器不同地规定。这可能相反影响系统性能。
3. Mac连接器1.10.0和Linux连接器1.11.0介绍通用的在执行缓和在(2)描述的新的解释性能损失的扫描最优化。

对路径、文件扩展和通配符排除规则的更改

在1.10.x和更旧的连接器版本中：文件、路径和通配符规则从这些文件操作的扫描排除目标文件或目录：

- 创建
- 修改
- 改名
- 执行

在1.11.0和更新的连接器版本中：路径、文件扩展和通配符规则的解释更改了这样在匹配，文件执行将触发扫描而不是被排除。文件创建，修改，并且改名继续被排除。此更改的动机是：

1. 当排除数据文件目录时，它避免不需要的排除执行活动。
2. 它更好的补足进程排除规则通过使成为可能独立地排除执行并且非执行在同一条路径的操作。
3. 它与在Windows的AMP对齐这些规则的macOS和Linux解释。

在许多情况下，安培的CPU使用情况增量估计是少于20%。有时，安培的CPU使用情况可能减少。如果通用的新的连接器的版本的比排除规则在执行扫描最优化有效在使用中，这是可能的。

连接器升级指导

对于使用排除以前被调整的系统，注意是需要在到1.11.0以后(或更新的)保证系统性能的升级是令人满意的。推荐的升级步骤是：

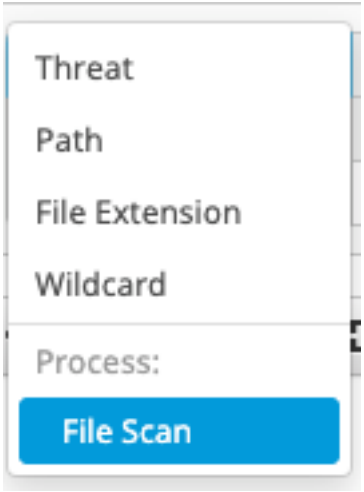
1. 没有做任何排除变动，请升级连接器。
2. 在升级以后评估系统性能。
3. 如果系统性能，在升级是令人满意的后，请删除路径、文件扩展和通配符排除规则目标程序可执行软件而不是数据文件。那些规则不再必要。续签过程排除规则可能然后增加进一步改进性能在便利。
4. 如果系统性能，在升级不是令人满意的后，替换路径，文件扩展，并且通配符排除规定该目标程序可执行软件与对应的进程排除规则。系统性能应该改善到是相同的或更好比在升级前的级别。

在连接器在阶段内被升级的更大的配置，推荐延迟修改或删除路径、文件扩展和通配符排除规则，直到，在所有连接器被升级了到1.11.0或更新后。这保证依靠现有的排除规则没有相反受影响的更旧的连接器，在终端被升级前。

增加进程排除规则

使用终端Web门户的， AMP进程排除规则可以被创建。步骤为：

1. 查找排除设置您希望修改。点击`添加排除`并且选择`进程：文件扫描`。



2. 输入程序的充分的(绝对)路径能排除，将运行程序的用户帐户(可选)，并且排除是否应该适用于程序创建的所有子进程。

3. 点击`添加排除`增加更多规则(重复步骤1-2)，或者点击`保存`保存排除集。

处理排除最佳实践

- **请勿排除启动进程：** 启动进程(即，`在macOS的launchd ``init在Linux的`或`systemd `)对创建在系统的其他进程负责并且是在进程层次结构顶部。除了启动进程和所有其子进程，将有效禁用AMP监控。
- **请指定用户，当可能：** 如果用户字段空出空白，排除适用于运行指定的程序的所有进程。当适用于所有用户时的规则可能是更加灵活的，此清楚的范围可能无心地排除应该监控的活动。指定用户对适用于共有的程序例如运行时引擎的规则是特别重要(即，`Java `)即和脚本解译器(`打击``Python `)。指定用户限制范围并且处理AMP忽略特定实例，当监控其他实例时。
- **避免在进程排除和路径/文件扩展/通配符之间的重叠规则：** 当排除程序的执行从扫描时，一个好保障维护是发现那的修改委托的程序和触发器文件扫描。保证在进程排除规则指定的路径没有由路径/文件扩展/通配符规则包括保证文件修改从扫描不会无心地被排除。

从Windows实施的区别

添加进程排除技术支持和减少范围路径，文件扩展和通配符规则带来macOS和Linux排除由于更加接近的对准线与Windows。然而，有重要设备区别：

1. macOS和Linux进程排除规则接受一个可选的用户名随附于进程可执行的完整路径，而Windows接收一个可选的SHA-256 Hash值。除了由其SHA-256的一个进程macOS和Linux当前不支持Hash值。

2. 恶意活动和系统进程引擎是独有的对Windows和，因此那些排除类型不是可用的在macOS和Linux。