Erfassen von Diagnosedaten von AMP für Endgeräte Linux Connector

Inhalt

Einführung

In diesem Dokument werden die Schritte zum Generieren einer Diagnosedatei über den Linux Connector für AMP für Endgeräte beschrieben. Wenn bei Ihnen ein technisches Problem mit dem Linux Connector auftritt, kann ein Techniker der technischen Unterstützung von Cisco die in einer Diagnosedatei verfügbaren Protokollmeldungen analysieren.

Diagnosedatei erstellen

Mit diesem Befehl können Sie eine Diagnosedatei direkt über die Linux Command Line Interface (CLI) generieren:

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

Dadurch wird auf Ihrem Desktop eine .7z-Datei erstellt. Sie können diese Datei dem Cisco Technical Assistance Center (TAC) zur weiteren Analyse bereitstellen.

Debugmodus

Der Debugmodus des Connectors bietet zusätzliche Ausführlichkeit zur Protokollierung. Sie bietet einen besseren Einblick in ein Problem mit dem Connector. In diesem Abschnitt wird beschrieben, wie der Debugmodus in einem Connector aktiviert wird.

> **Warnung**: Der Debug-Modus sollte nur aktiviert werden, wenn Cisco diese Daten anfordert. Wenn Sie den Debug-Modus für eine längere Zeit aktivieren, kann dies den Festplattenspeicherplatz sehr schnell füllen und die Support Diagnostic-Datei daran hindern,

das **Connector-Protokoll** aufgrund einer übergroßen Dateigröße zu erfassen.

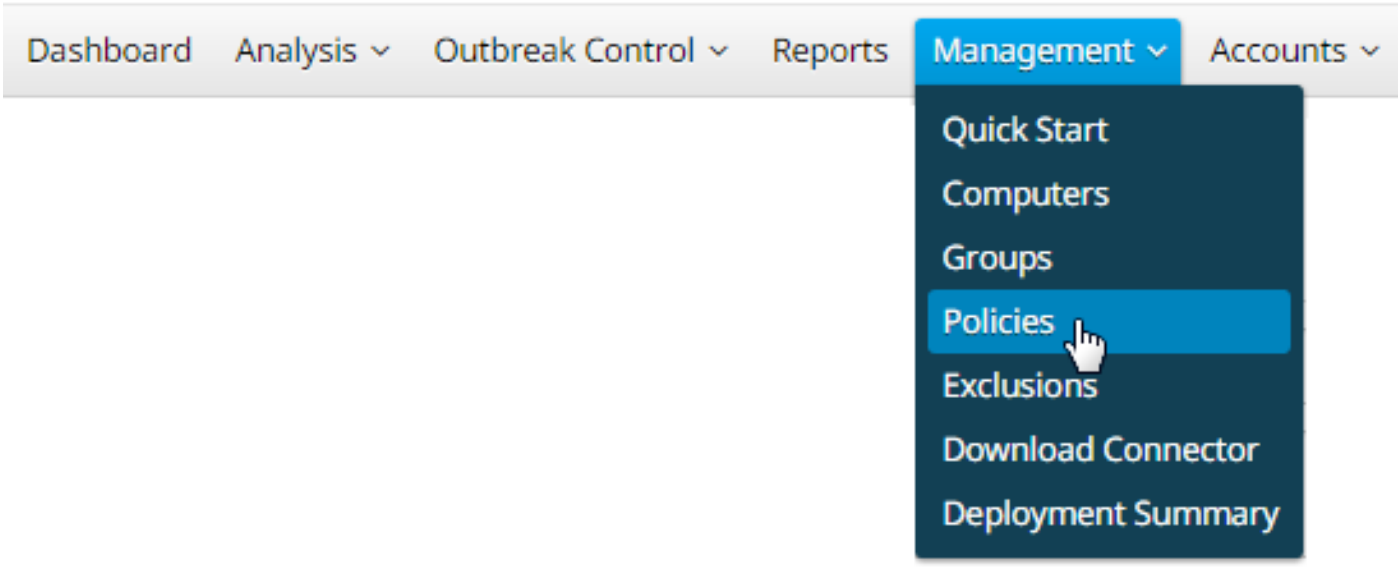
AMP-Konsole verwenden

Debug-Modus aktivieren

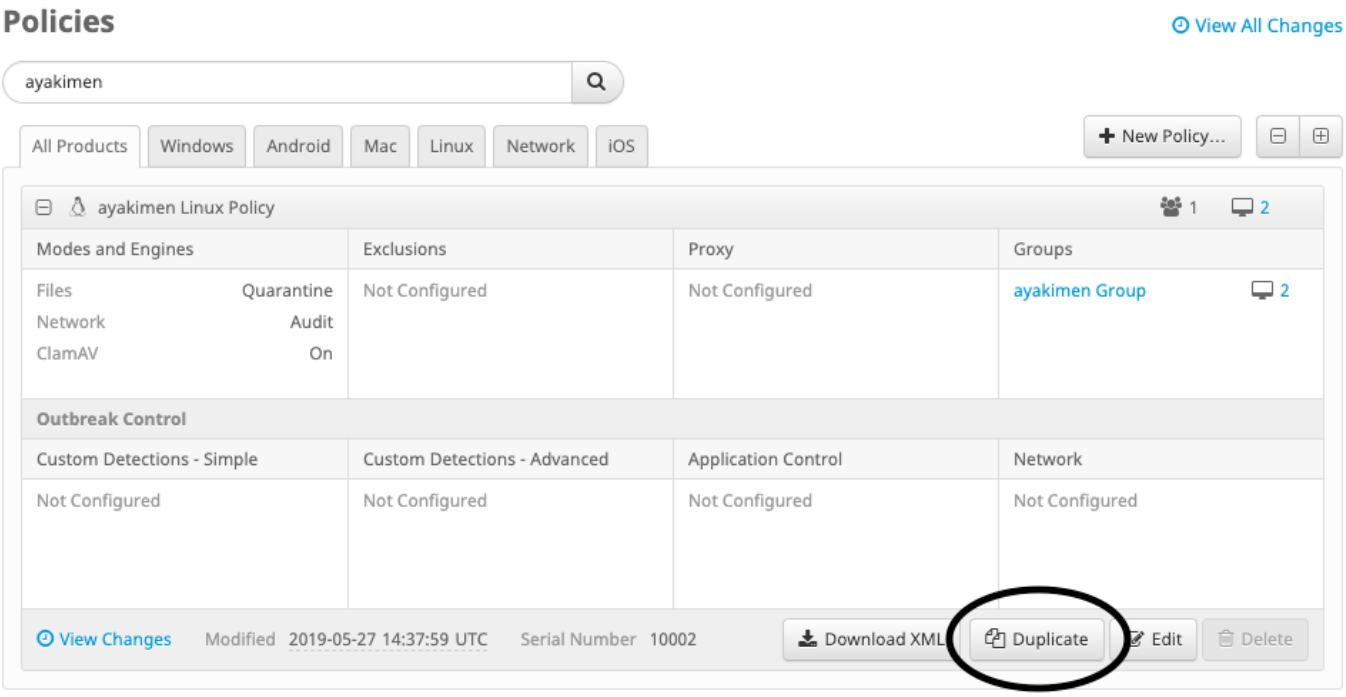
Sie können den Debugmodus in der aktuellen Richtlinie mit den Schritten 5 bis 7 aktivieren oder eine neue Richtlinie im Debugmodus mit allen folgenden Schritten erstellen:

Schritt 1: Melden Sie sich bei der AMP-Konsole an.

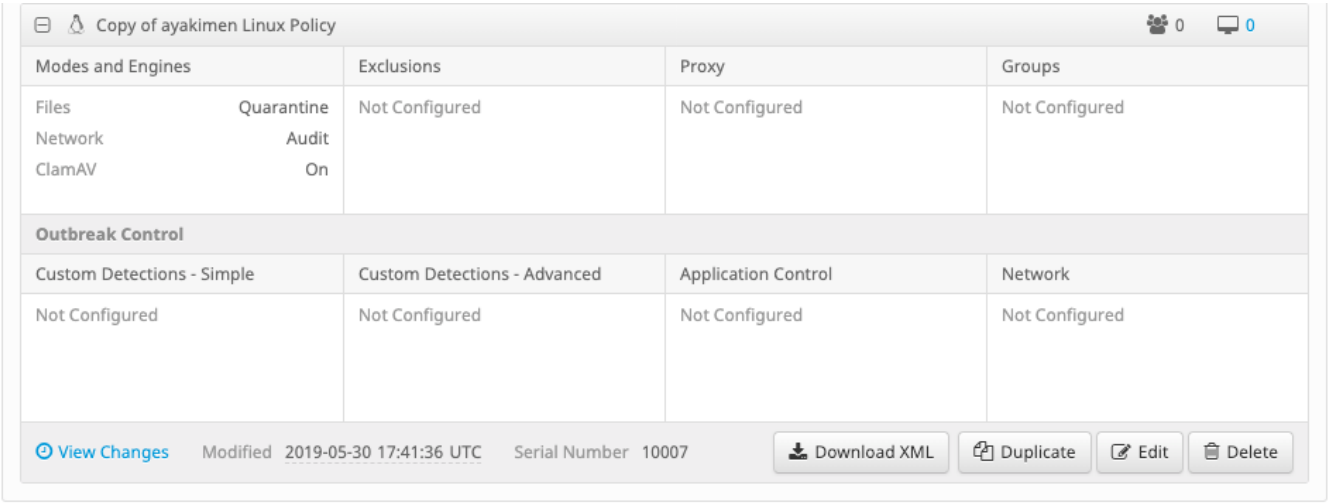
Schritt 2: Wählen Sie **Verwaltung > Richtlinien aus**.



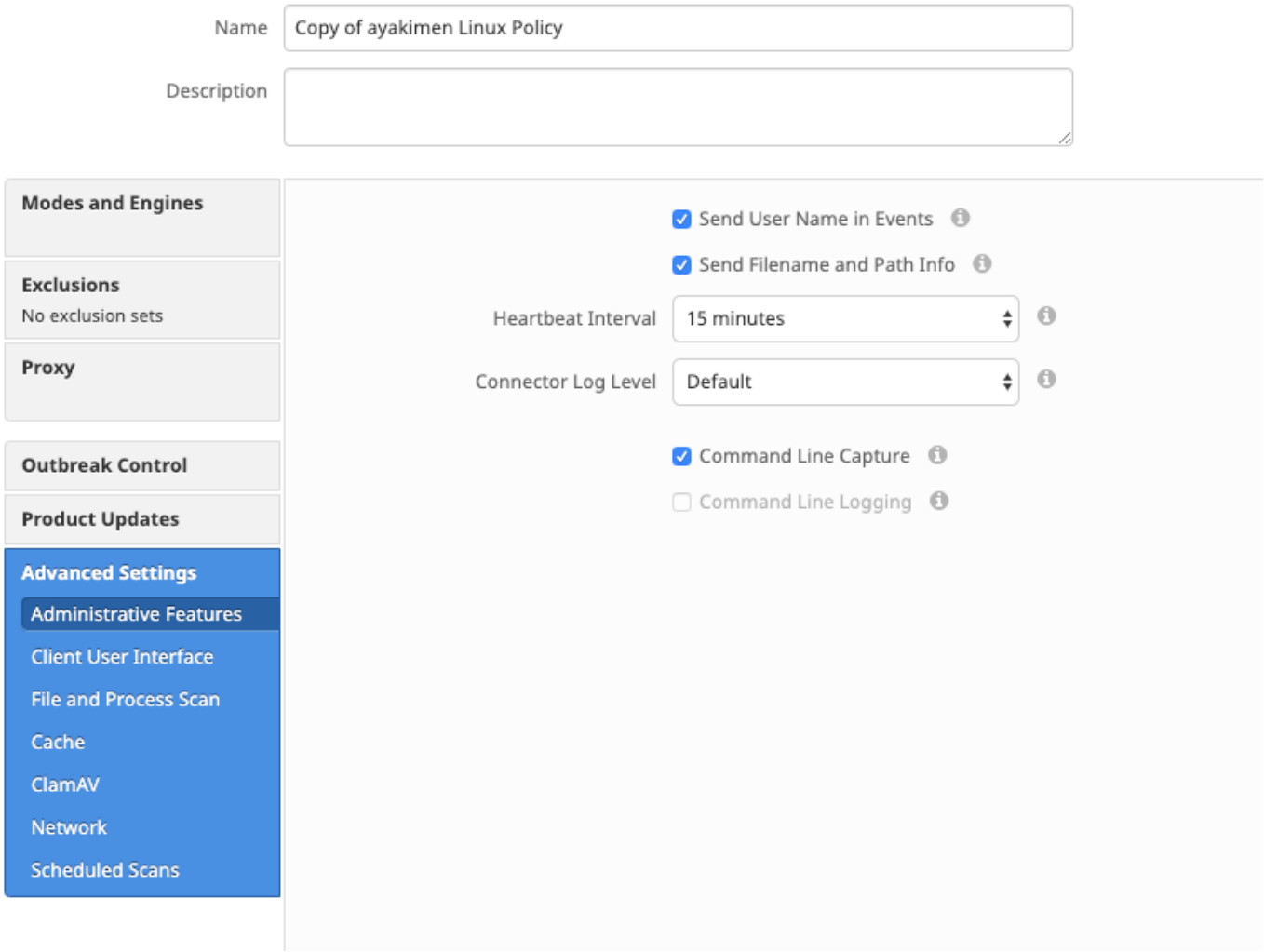
Schritt 3: Suchen Sie die Richtlinie, die auf das Endgerät oder den Computer angewendet wird, und klicken Sie auf die Richtlinie, um das Fenster Richtlinie zu erweitern. **Klicken Sie auf Duplizieren**.



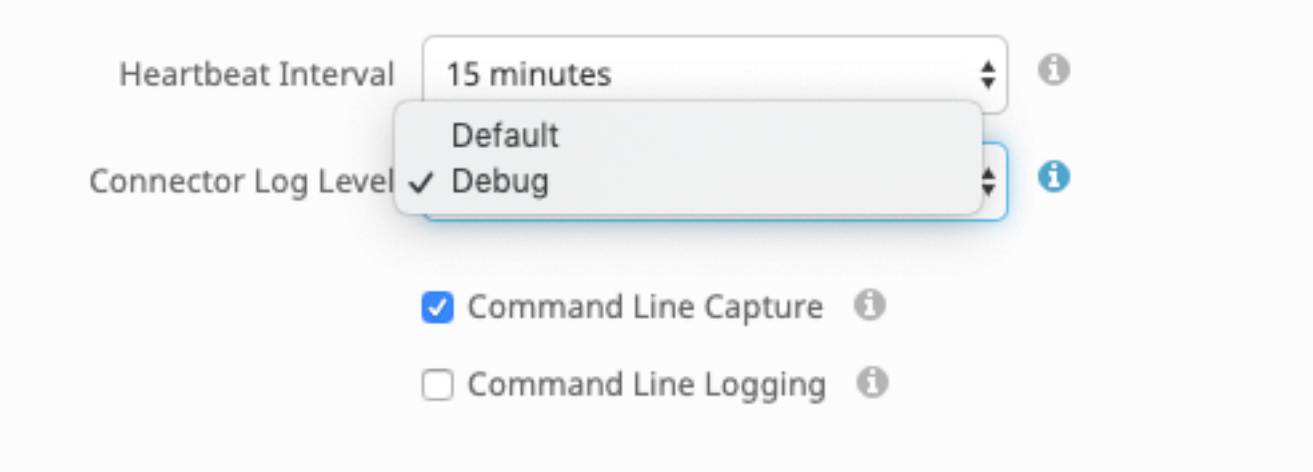
Schritt 4: Nachdem Sie **auf Duplizieren geklickt haben**, wird die AMP-Konsole mit der kopierten Richtlinie aktualisiert.



Schritt 5: **Klicken Sie auf Bearbeiten**, **klicken Sie auf Erweiterte Einstellungen**, und wählen Sie in der Seitenleiste die **Option** Verwaltungsfunktionen aus.



Schritt 6: **Wählen Sie fürConnector-Protokollstufe** in den Dropdown-Listen die Option Debuggen aus.



Schritt 7: Klicken Sie auf Speichern, um die Änderungen zu speichern.

Schritt 8: Nachdem Sie die neue Richtlinie gespeichert haben, müssen Sie eine Gruppe erstellen/ändern, um *die neue Richtlinie* einzuschließen, und *dann* Geräte, auf denen Sie Debuginformationen generieren möchten.

Debug-Modus deaktivieren

Um den Debug-Modus zu deaktivieren, gehen Sie wie zuvor vor, um den Debugmodus zu aktivieren. Ändern Sie jedoch die **Verbindungsprotokollstufe** auf **Standard**.

Befehlszeile verwenden

Debug-Modus aktivieren

Wenn Verbindungsprobleme in der Konsole auftreten und Sie den Debugmodus aktivieren möchten, führen Sie diese Befehle in der CLI aus:

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

Dies ist die Ausgabe:

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

Debug-Modus deaktivieren

Um den Debugmodus zu deaktivieren, verwenden Sie die folgenden Befehle:

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

Support-Tool Optimieren während der Debugsitzung

Der Connector-Daemon muss in den Debug-Protokollierungsmodus gesetzt werden, bevor die Unterstützung für die Dateioptimierung beginnt. Dies erfolgt über die AMP-Konsole, über die

Richtlinieneinstellungen des Connectors *unter Management -> Policies (Verwaltung -> Richtlinien)*. Bearbeiten Sie die Richtlinie, und gehen Sie unter *der* Schaltfläche Erweiterte Einstellungen zum Abschnitt *Verwaltungsfunktionen*. Ändern Sie *die* Einstellung für *das* Verbindungsprotokoll **in Debuggen**.

Speichern Sie anschließend Ihre Richtlinie. Nachdem Ihre Richtlinie gespeichert wurde, stellen Sie sicher, dass sie mit dem Connector synchronisiert wurde. Führen Sie den Connector in diesem Modus mindestens 15-20 Minuten aus, bevor Sie mit dem restlichen Tuning fortfahren.

Anmerkung: Wenn die Einstellung abgeschlossen ist, vergessen Sie nicht, *die EinstellungConnector Log* Levelt (*Verbindungsprotokollstufe)* auf Default (Standard) zurückzusetzen, sodass der Connector im effizientesten und effektivsten Modus ausgeführt wird.

Ausführen des Support-Tools

Diese Methode umfasst die Verwendung des Support-Tools, einer Anwendung, die mit dem AMP Mac Connector installiert ist. Sie können auf die Anwendung im Ordner Anwendungen zugreifen, indem Sie auf /Applications->Cisco AMP->Support Tool.app doppelklicken. Dadurch wird ein vollständiges Support-Paket generiert, das zusätzliche Diagnosedateien enthält.

Ein Alternative, und schneller, die Methode ist, folgende Befehlszeilevon eine Terminal Sitzung:

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

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

Die erste Option führt dazu, dass eine deutlich kleinere Unterstützungsdatei nur die relevanten Tuning-Dateien enthält. Die zweite Option bietet ein vollständiges Support-Paket mit weiteren Informationen, wie z. B. Protokollen, die möglicherweise für die Anpassung von Prozessausschlüssen erforderlich sind (verfügbar in Connector-Versionen 1.11.0 und höher).

Das Support-Tool generiert auf beide Arten eine ZIP-Datei auf Ihrem ~home, die zwei Tuning-Support-Dateien enthält: fileops.txt und Execs.txt. fileops.txt enthält eine Liste der am häufigsten erstellten und geänderten Dateien auf Ihrem Computer. Diese Dateien sind für Ausschlüsse von Pfad und Platzhalter nützlich. Execs.txt enthält die Liste der am häufigsten ausgeführten Dateien. Diese sind für Ausschlüsse von Prozessen nützlich. Beide Listen sind nach Anzahl der Scans sortiert, d. h. die am häufigsten gescannten Pfade werden oben in der Liste angezeigt.

Lassen Sie den Connector 15-20 Minuten lang im Debug-Modus ausgeführt, und führen Sie dann das Support-Tool aus. Eine gute Faustregel ist, dass alle Dateien oder Pfade, die durchschnittlich 1000 Treffer oder mehr in dieser Zeit sind gute Kandidaten, ausgeschlossen werden.

Abstimmung von Ausschlüssen

Ausschlüsse für Pfad, Platzhalterzeichen, Dateinamen und Dateierweiterungen erstellen

Eine Möglichkeit, mit Pfadausschlussregeln zu beginnen, besteht darin, die am häufigsten gescannten Datei- und Ordnerpfade aus fileops.txt zu finden und dann die Erstellung von Regeln für diese Pfade in Betracht zu ziehen. Überprüfen Sie nach dem Herunterladen der Richtlinie die CPU-Auslastung. Es kann 5 bis 10 Minuten dauern, bis die Richtlinie aktualisiert ist, bevor Sie feststellen, dass die CPU-Auslastung abnimmt, da es für den Daemon Zeit dauern kann, den Vorgang abzufangen. Wenn immer noch Probleme auftreten, führen Sie das Programm erneut aus, um zu sehen, welche neuen Pfade Sie beobachten.

- Eine gute Faustregel ist, dass alles mit einer Protokoll- oder Journaldateierweiterung als geeigneter Ausschlusskandidat betrachtet werden sollte.

Erstellen von Prozessausschlüssen

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).
Best Practices für Prozessausschlüsse finden Sie unter: AMP für Endgeräte: Prozessausschlüsse in MacOS und Linux

Ein gutes Tuning-Muster besteht zunächst darin, die Prozesse zu identifizieren, bei denen ein hohes Volumen an ausführbaren Dateien von Execs.txt ausgeführt wird, den Pfad zur ausführbaren Datei zu finden und einen Ausschluss für diesen Pfad zu erstellen. Es gibt jedoch einige Prozesse, die nicht einbezogen werden sollten, darunter:

- Allgemeine Dienstprogramme - Es wird nicht empfohlen, allgemeine Dienstprogramme auszuschließen (z. B.: usr/bin/grep) ohne Berücksichtigung der folgenden Punkte. Der Benutzer kann bestimmen, welche Anwendung den Prozess aufruft (z. B.: Suchen Sie den übergeordneten Prozess, der grep

ausführt), und schließen Sie den übergeordneten Prozess aus. Dies sollte nur dann erfolgen, wenn der übergeordnete Prozess sicher in einen Prozessausschluss umgewandelt werden kann. Wenn der Elternausschluss für Kinder gilt, werden auch Aufrufe von Kindern aus dem Elternprozess ausgeschlossen.Der Benutzer, der den Prozess ausführt, kann bestimmt werden. (Bsp.: Wenn ein Prozess auf einem hohen Volumen von Benutzer "root" aufgerufen wird, kann man den Prozess ausschließen, aber nur für den angegebenen Benutzer "root", dies ermöglicht es AMP, die Ausführung eines bestimmten Prozesses durch einen Benutzer zu überwachen, der nicht "root" ist.)**HINWEIS: Ausschlüsse von Prozessen sind neu in Connector-Versionen 1.11.0 und neuer. Aus diesem Grund können allgemeine Dienstprogramme als Pfadausschluss in Connector Version 1.10.2 und älter verwendet werden. Diese Vorgehensweise wird jedoch nur empfohlen, wenn ein Leistungskompromiss unbedingt erforderlich ist.**

Für Ausschlüsse von Prozessen ist es wichtig, den übergeordneten Prozess zu finden. Sobald der Parent Process bzw. User des Prozesses gefunden wurde, kann der Benutzer den Ausschluss für einen bestimmten Benutzer erstellen und den Prozessausschluss auf Kindprozesse anwenden, was wiederum laute Prozesse ausschließt, die nicht selbst in Prozessausschlüsse umgewandelt werden können.

Übergeordneter Prozess identifizieren

1. Befolgen Sie die Schritte 1-3 zur Identifikation des übergeordneten Prozesses von oben.
2. Identifizieren Sie Benutzer eines Prozesses mithilfe einer der folgenden Methoden: Suchen Sie die Benutzer-ID des angegebenen Prozesses von `U:` in der Protokollzeile (z. B.: U:0).Führen Sie im Terminal-Fenster den folgenden Befehl aus: `Get passwd # | cut -d: -f1`, wobei # die Benutzer-ID ist.Die Ausgabe sollte ähnlich wie bei:`Benutzername` angezeigt werden, wobeiBenutzername der Benutzer des angegebenen Prozesses ist.
3. Diese Der Benutzername kann einem Prozess-Ausschluss unter der Kategorie Benutzer hinzugefügt werden, um den Umfang des Ausschlusses zu reduzieren, der für bestimmte Prozessausschlüsse wichtig ist. **HINWEIS: Wenn der Benutzer eines Prozesses der lokale Benutzer des Computers ist und dieser Ausschluss auf mehrere Computer mit unterschiedlichen lokalen Benutzern angewendet werden muss, muss die Benutzerkategorie leer gelassen werden, damit der Prozessausschluss auf alle Benutzer angewendet werden kann.**

Zugehörige Informationen

- Erfassen von Diagnosedaten eines unter Windows laufenden FireAMP-Connectors
- Erfassen von Diagnosedaten eines FireAMP Connectors unter Mac OS
- **Technischer Support und Dokumentation - Cisco Systems**