

AMP für Endgeräte Ubuntu-Anschluss

Inhalt

[Betriebssystem-Mindestanforderungen](#)

[Umgebungseinrichtung](#)

[Installation](#)

[Deinstallation](#)

[Revisionsverlauf](#)

In diesem Artikel werden die Änderungen und Schritte beschrieben, die Administratoren durchführen können, um AMP für Endgeräte Linux Connector unter Ubuntu bereitzustellen.

Betriebssystem-Mindestanforderungen

AMP für Endgeräte Linux Connector 1.15.0 unterstützt die folgenden Ubuntu-Versionen:

- Ubuntu 20.04.0 LTS.
- Ubuntu 20.04.1 LTS.

Umgebungseinrichtung

Der Linux Connector für AMP für Endgeräte unter Ubuntu verwendet eBPF für die Datei- und Netzwerküberwachung. Auf dem Computer muss das richtige Linux-Header-Softwarepaket installiert sein. Andernfalls löst Connector den Fehler 11 (fehlende Systemabhängigkeit) aus und führt ohne Datei- und Netzwerküberwachung in einem heruntergestuften Zustand aus. Eine Anleitung zur Behebung dieses Fehlers finden Sie im [Linux Kernel-Devel Fault](#) Artikel.

Installation

Um Connector zu installieren, führen Sie den folgenden Befehl aus, wobei [deb-Paket] der Name der Datei ist, z. B. amp_test.deb:

```
sudo dpkg -i [deb package]
```

WICHTIG! Wenn Sie andere Sicherheitsprodukte in Ihrer Umgebung ausführen, besteht die Möglichkeit, dass diese das AMP für Endpoints-Connector-Installationsprogramm als Bedrohung erkennen. Um den Connector erfolgreich zu installieren, fügen Sie AMP zu einer zulässigen Liste hinzu oder schließen AMP aus den anderen Sicherheitsprodukten aus, und versuchen Sie es erneut.

WICHTIG! Während der Connector-Installation werden ein Benutzer und eine Gruppe mit dem Namen cisco-amp-scan-svc auf dem System erstellt. Wenn dieser Benutzer oder diese Gruppe bereits vorhanden, aber anders konfiguriert ist, versucht das Installationsprogramm, diese zu löschen und dann mit der erforderlichen Konfiguration erneut zu erstellen. Das Installationsprogramm schlägt fehl, wenn der Benutzer und die Gruppe nicht mit der erforderlichen Konfiguration erstellt werden konnten.

Deinstallation

Führen Sie den folgenden Befehl aus, um den AMP für Endpoints-Linux-Connector zu deinstallieren:

```
sudo dpkg --remove ciscoampconnector
```

Hinweis: Damit bleiben lokale Daten zurück, einschließlich Verlauf, isolierte Dateien sowie der Benutzer und die Gruppe cisco-amp-scan-svc. Wenn Sie die Neuinstallation des Connectors nicht planen und die übrigen Dateien entfernen möchten, führen Sie den folgenden Befehl aus:

```
sudo dpkg --purge ciscoampconnector
```

Revisionsverlauf

10. Dez. 2020

- Erstversion