Recopilación de datos de diagnóstico de AMP para terminales Conector Linux

Contenido

Introducción

Este documento describe los pasos para generar un archivo de diagnóstico desde AMP para terminales Linux Connector. Si experimenta un problema técnico con Linux Connector, un ingeniero de soporte técnico de Cisco podría querer analizar los mensajes de registro disponibles en un archivo de diagnóstico.

Generar archivo de diagnóstico

Con el uso de este comando, puede generar un archivo de diagnóstico directamente desde la interfaz de línea de comandos (CLI) de Linux:

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

Esto crea un archivo .7z en el escritorio. Puede proporcionar este archivo al centro de asistencia técnica Cisco Technical Assistance Center (TAC) para su posterior análisis.

Modo de depuración

El modo de depuración del conector proporciona una verbosidad adicional al registro. Permite obtener más información sobre un problema con el conector. Esta sección describe cómo habilitar el modo de depuración en un conector.

> **Advertencia:** El modo de depuración sólo se debe habilitar si Cisco solicita estos datos. Si habilita el modo de depuración durante más tiempo, puede llenar el espacio en disco muy rápidamente y evitar que el archivo de diagnóstico de soporte recopile el **registro del**

conector debido al tamaño excesivo del archivo.

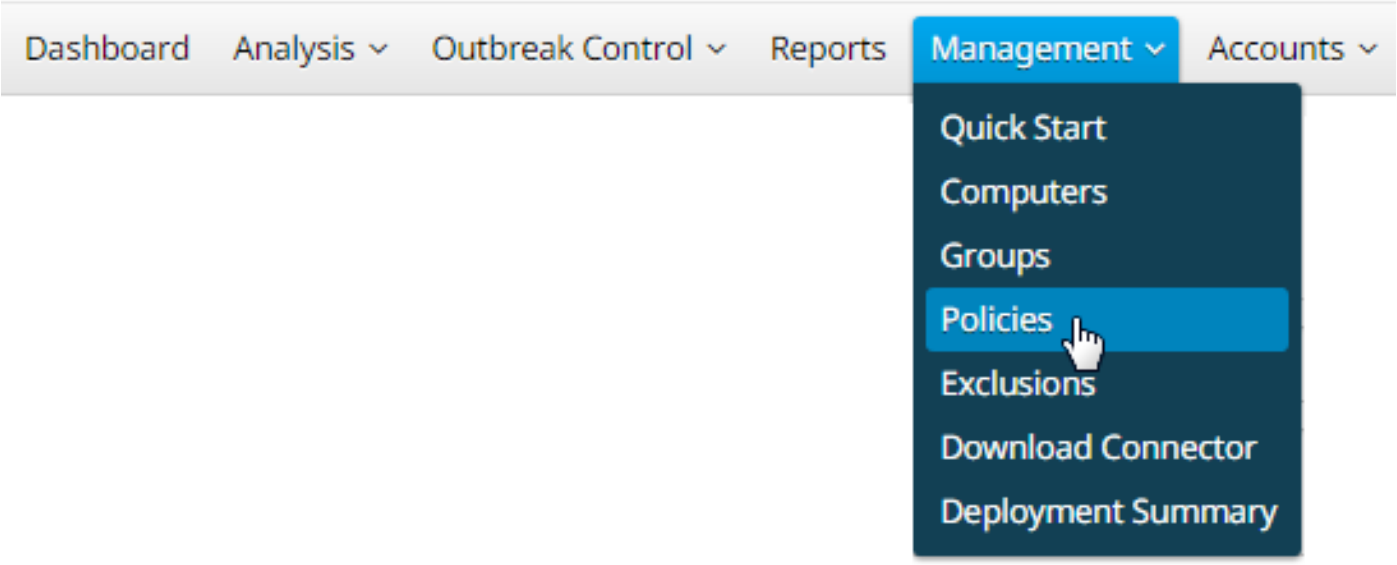
Usar consola AMP

Activar modo de depuración

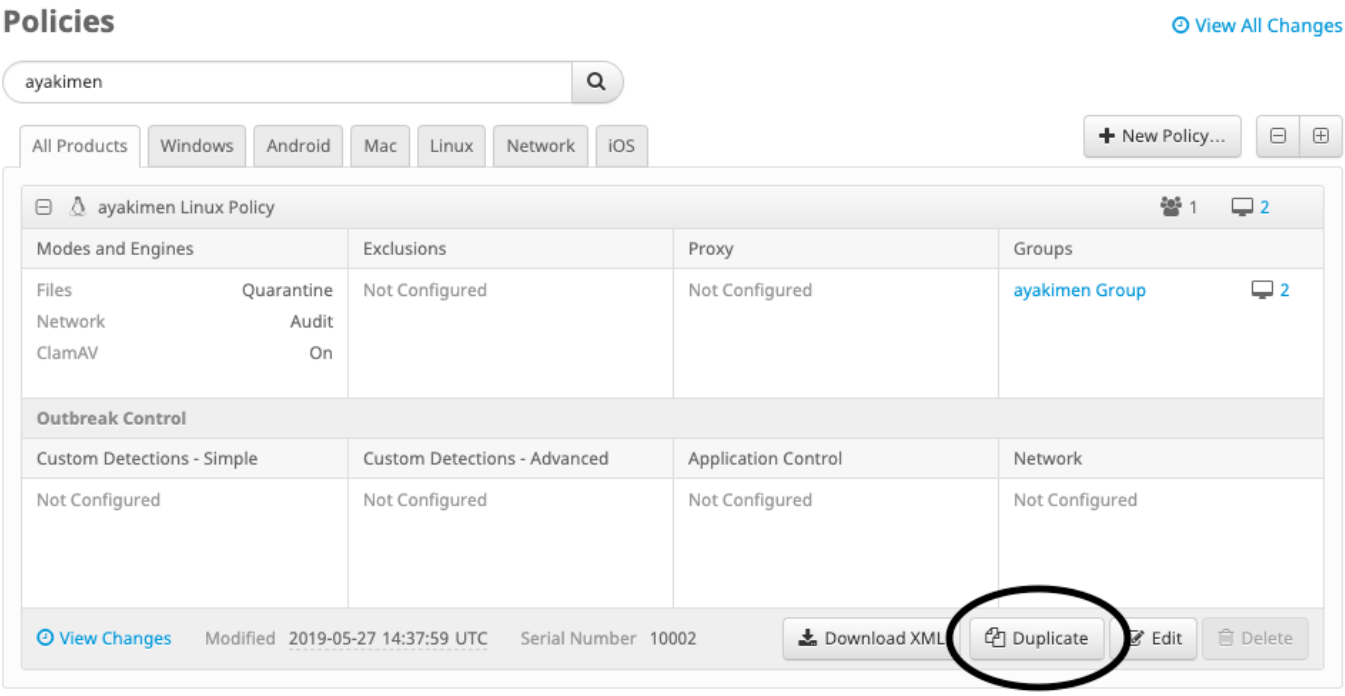
Puede habilitar el modo de depuración en la política actual con los pasos 5 a 7 o crear una nueva política en el modo de depuración con todos estos pasos:

Paso 1. Inicie sesión en la consola de AMP.

Paso 2. Seleccione **Administración > Políticas**.

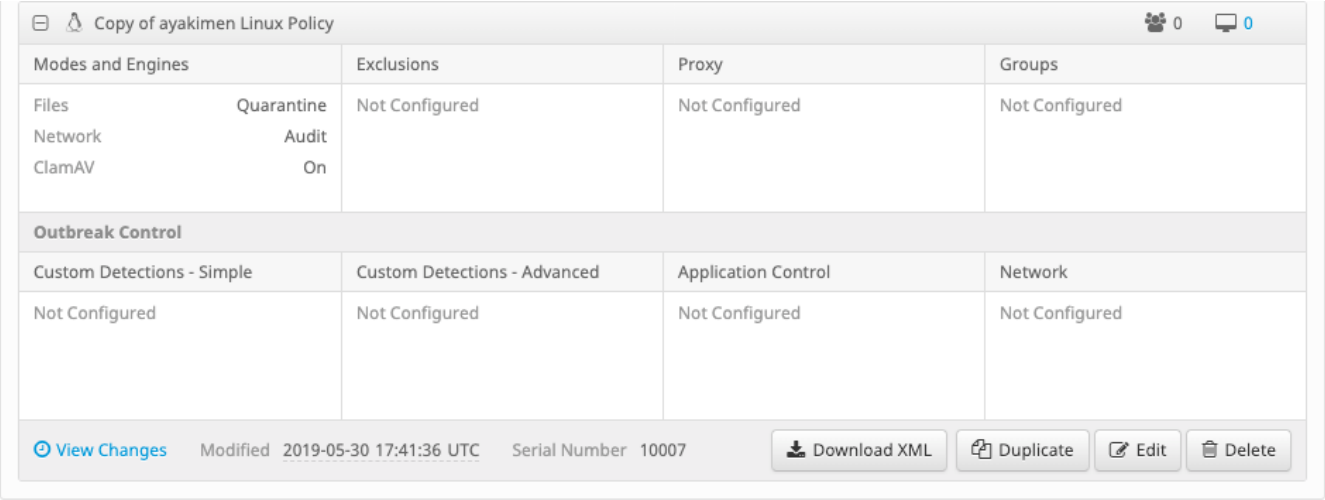


Paso 3. Busque la directiva que se aplica al dispositivo o equipo final y haga clic en la directiva. Esto expandirá la ventana Política. **Haga clic enDuplicar**.

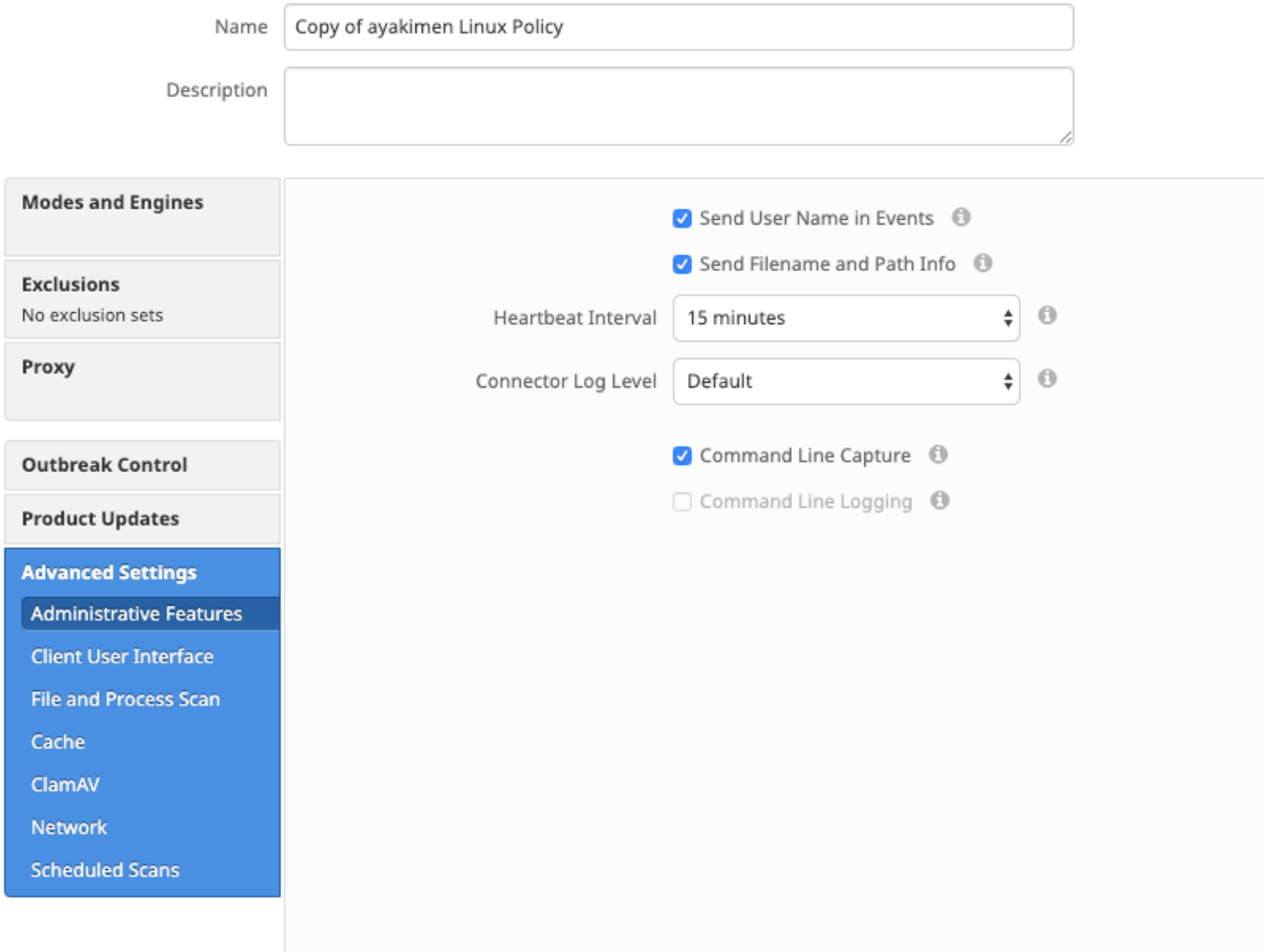


Paso 4. Después de **hacer clic en Duplicar**, la consola de AMP se actualiza con la política

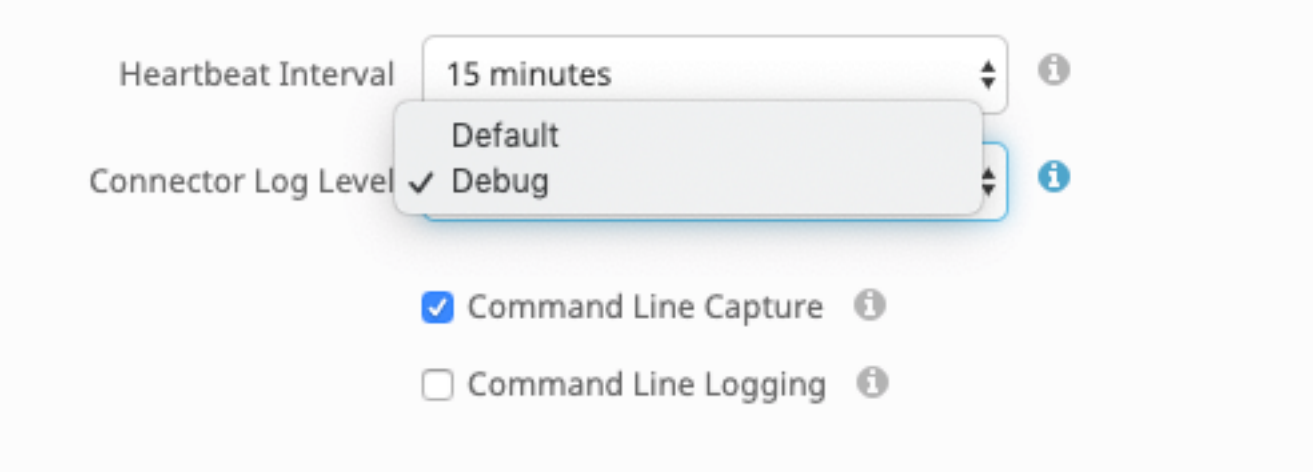
copiada.



Paso 5. Haga clic en Editar, **haga clic en Configuración avanzada** y seleccione **haga clic en** Funciones administrativas en la barra lateral.



Paso 6. **ParaNivel de registro del conector**, seleccioneDepurar en las listas desplegables.



Paso 7. Haga clic en Guardar para guardar los cambios.

Paso 8. Después de guardar la nueva política, debe crear/cambiar un grupo para incluir *la nueva política*, y el dispositivo *final* donde desea generar información de depuración.

Desactivar modo de depuración

Para inhabilitar el modo de depuración, siga los mismos pasos que completó para habilitar el modo de depuración, pero cambie el **Nivel de registro del conector** a **Predeterminado**.

Usar línea de comandos

Activar modo de depuración

Si experimenta problemas de conectividad en la consola y desea habilitar el modo de depuración, ejecute estos comandos en la CLI:

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

Este es el resultado:

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

Desactivar modo de depuración

Para inhabilitar el modo debug, utilice estos comandos:

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

Herramienta de soporte Ajuste durante la depuración

El demonio del conector debe ponerse en el modo de registro de depuración antes de comenzar el ajuste del archivo de soporte. Esto se realiza a través de la consola de AMP, a través de la configuración de políticas del conector *enManagement -> Policies*. Edite la política y vaya a *la*

sección *de* Funciones *Administrativas bajo la* ficha Configuración avanzada. Cambie *la* configuración del nivel de *registro del conector* **aDebug**.

A continuación, guarde la política. Una vez guardada la directiva, asegúrese de que se ha sincronizado con el conector. Ejecute el conector en este modo durante al menos 15-20 minutos antes de continuar con el resto del ajuste.

Nota: Una vez finalizada la sintonización, no olvide cambiar *la* configuración *del* nivel de registro del conector a Default para que el conector se ejecute en su modo más eficiente y efectivo.

Herramienta de soporte en ejecución

Este método implica el uso de la herramienta Support Tool, una aplicación instalada con AMP Mac Connector. Se puede acceder a él desde la carpeta Aplicaciones haciendo doble clic en /Applications->Cisco AMP->Support Tool.app. Esto generará un paquete de soporte completo que contiene archivos de diagnóstico adicionales.

Un alternativa, y más rápido, el método es ejecutar el línea de comandos siguientedesde a Terminal sesión:

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

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

La primera opción dará como resultado un archivo de soporte mucho más pequeño que contiene solamente los archivos de ajuste relevantes. La segunda opción proporciona un paquete de soporte completo que contiene más información, como registros, que pueden ser necesarios para ajustar las exclusiones de procesos (disponibles en las versiones 1.11.0 y posteriores del conector).

De cualquier manera que elija ejecutarlo, Support Tool generará un archivo zip en su ~home que contiene dos archivos de soporte de ajuste: fileops.txt y execs.txt. fileops.txt contiene una lista de los archivos creados y modificados con más frecuencia en su equipo, que serán útiles para las exclusiones de ruta/comodín. execs.txt contendrá la lista de los archivos ejecutados con mayor frecuencia, que serán útiles para las exclusiones de procesos. Ambas listas se ordenan por recuento de escaneo, lo que significa que las rutas exploradas más frecuentemente aparecen en la parte superior de la lista.

Deje el conector en modo Debug durante un período de 15-20 minutos y, a continuación, ejecute la herramienta de soporte. Una buena regla general es que cualquier archivo o ruta de acceso con un promedio de 1000 visitas o más durante ese tiempo son buenos candidatos para ser excluidos.

Ajuste de exclusión

Creación de Exclusiones de Ruta, Comodín, Nombre de Archivo y Extensión de Archivo

Una forma de comenzar con las reglas de exclusión de rutas es encontrar las rutas de acceso de archivos y carpetas más exploradas de fileops.txt y, a continuación, considerar la posibilidad de crear reglas para esas rutas. Una vez descargada la política, monitoree el nuevo uso de CPU. Puede tardar entre 5 y 10 minutos después de que se actualice la política antes de que observe la caída del uso de la CPU, ya que podría tardar el demonio en ponerse al día. Si todavía está viendo problemas, vuelva a ejecutar la herramienta para ver qué rutas nuevas observa.

- Una buena regla general es que cualquier cosa con una extensión de archivo de registro o diario debe considerarse un candidato de exclusión adecuado.

Crear exclusiones de procesos

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).`

Para obtener información sobre las prácticas recomendadas en relación con las exclusiones de procesos, consulte: AMP para terminales: Exclusiones de procesos en MacOS y Linux

Un buen patrón de ajuste primero es identificar los procesos con un alto volumen de ejecuciones de execs.txt, encontrar la trayectoria al ejecutable y crear una exclusión para esta trayectoria. Sin embargo, hay algunos procesos que no deben incluirse, entre ellos:

- Programas generales de servicios públicos: no se recomienda excluir programas generales de servicios públicos (p. ej.: usr/bin/grep) sin tener en cuenta lo siguiente. El usuario puede determinar qué aplicación llama al proceso (p. ej.: busque el proceso primario que está ejecutando grep) y excluya el proceso primario. Esto se debe hacer si el proceso principal puede convertirse en una exclusión de proceso de manera segura, y sólo si lo

hace si el proceso principal puede convertirse en una exclusión de proceso. Si la exclusión principal se aplica a los elementos secundarios, también se excluirán las llamadas a cualquier elemento secundario del proceso principal.Se puede determinar el usuario que está ejecutando el proceso. (p. ej.: si el usuario "root" llama a un proceso con un volumen alto, se puede excluir el proceso, pero sólo para el usuario "root" especificado, esto permitirá a AMP monitorear los ejecutados de un proceso determinado por cualquier usuario que no sea "root").**NOTA: Las exclusiones de procesos son nuevas en las versiones 1.11.0 y posteriores del conector. Debido a esto, los programas de utilidad general pueden utilizarse como una exclusión de trayectoria en las versiones 1.10.2 y posteriores del conector. Sin embargo, esta práctica sólo se recomienda cuando es absolutamente necesario realizar un intercambio de resultados.**

Encontrar el proceso principal es importante para las exclusiones de procesos. Una vez que se encuentra el proceso principal y/o el usuario del proceso, el usuario puede crear la exclusión para un usuario específico y aplicar la exclusión del proceso a procesos secundarios, lo que a su vez excluirá los procesos ruidosos que no pueden convertirse en exclusiones del proceso.

Identificación del proceso principal

1. Siga los pasos 1-3 de Identificación del proceso principal desde arriba.
2. Identifique al usuario de un proceso utilizando uno de los siguientes métodos: Busque la ID de usuario del proceso dado desde `U:` en la línea de registro (p. ej.: U:0).Desde la ventana Terminal, ejecute el siguiente comando: `getent passwd # | cortar -d: -f1`, donde # es la ID de usuario.Debería ver un resultado similar a: `Nombre de usuario`, donde Nombre de usuario es el Usuario del proceso dado.
3. Esto El nombre de usuario se puede agregar a una exclusión de proceso en la categoría Usuario para reducir el alcance de la exclusión, que para ciertas exclusiones de proceso es importante. **NOTA: si el usuario de un proceso es el usuario local de la máquina y esta exclusión debe aplicarse a varios equipos con diferentes usuarios locales, la categoría Usuario debe dejarse en blanco para permitir que la Exclusión del proceso se aplique a todos los usuarios.**

Información Relacionada

- Recopilación de datos de diagnóstico de un conector de FireAMP que se ejecuta en Windows
- Recopilación de datos de diagnóstico de un conector FireAMP que se ejecuta en Mac OS
- **Soporte Técnico y Documentación - Cisco Systems**