Cisco Secure Endpoint Connector para la recopilación de datos de diagnóstico de Linux

Contenido

Introducción

Este documento describe cómo generar datos de diagnóstico para el conector de Cisco Secure Endpoint Linux.

Antecedentes

El conector de Cisco Secure Endpoint Linux viene empaquetado con la aplicación Support Tool, que se utiliza para generar datos de diagnóstico sobre el terminal y el conector que está instalado en él. Los datos de diagnóstico incluyen información como:

- Utilización de recursos (disco, CPU y memoria).
- Registros específicos del conector.
- Información de configuración del conector.

Generar datos de diagnóstico

Los datos de diagnóstico se pueden generar mediante dos métodos diferentes:

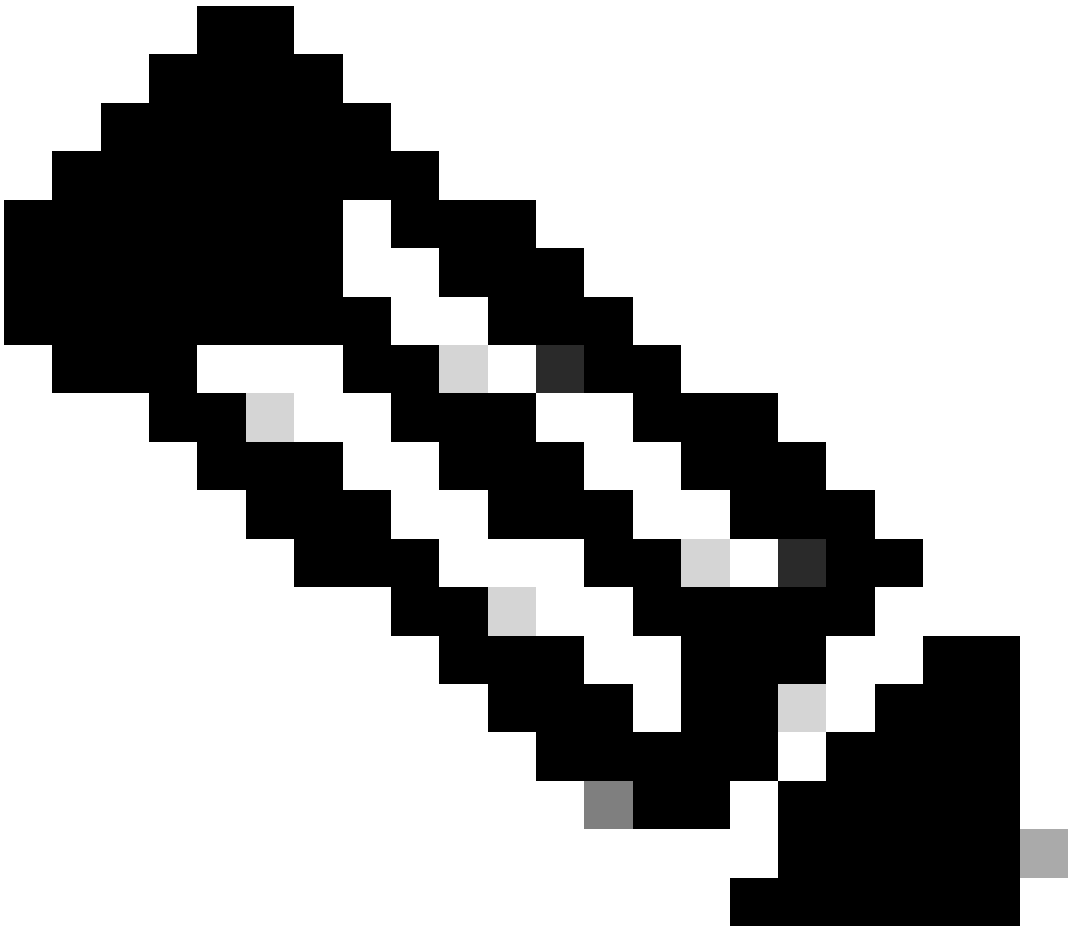
- Localmente mediante la herramienta de asistencia.
- De forma remota mediante Secure Endpoint Console.

Los datos de diagnóstico generados se pueden proporcionar al centro de asistencia técnica Cisco Technical Assistance Center (TAC) para su posterior análisis.

Generar datos de diagnóstico localmente mediante la herramienta de soporte

Ejecute el siguiente comando para generar datos de diagnóstico para el conector de Linux mediante la Herramienta de soporte:

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



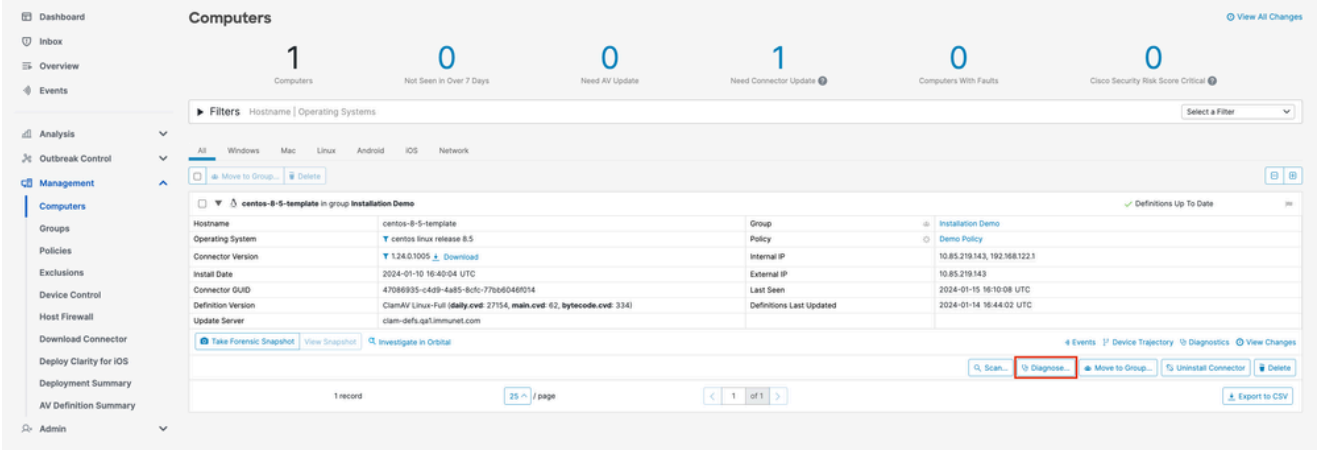
> Nota: Debe tener privilegios suficientes para ejecutar la herramienta de soporte, así que asegúrese de que precede el comando con sudo.

La herramienta de soporte crea un archivo `.zip` llamado `AMP_Support_<timestamp>.zip` en el directorio del escritorio del usuario conectado actualmente si existe, de lo contrario el archivo de almacenamiento se creará en el directorio principal del usuario conectado actualmente.

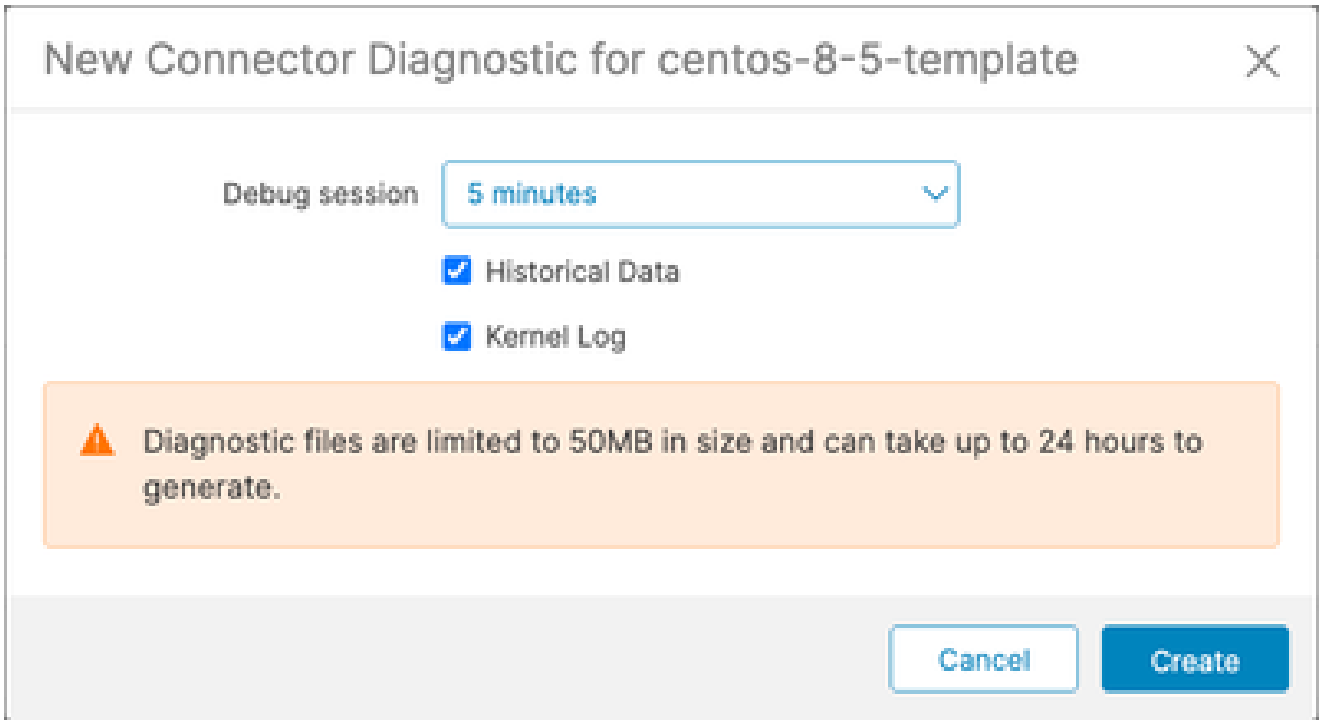
Generar datos de diagnóstico mediante la consola de terminal seguro

Complete estos pasos para generar datos de diagnóstico para el conector de Linux a través de Secure Endpoint Console:

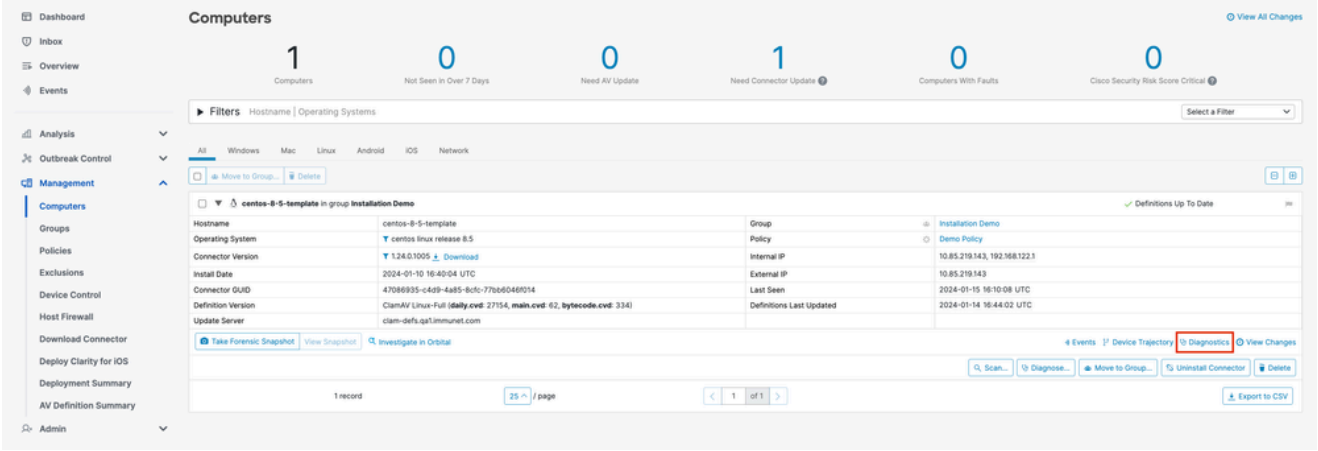
1. Vaya a la página Equipos seleccionando `Administración` -> `Equipos` e identifique su equipo en la lista. Haga clic en `Diagnosticar...`



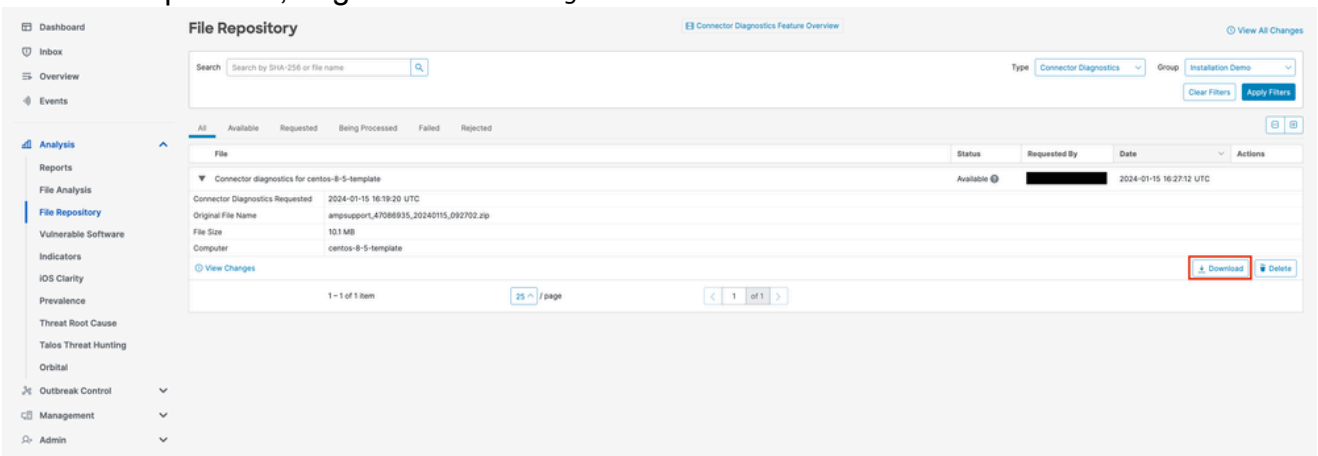
2. En la ventana emergente Nuevo diagnóstico del conector, seleccione la duración de la sesión de depuración en el menú desplegable y asegúrese de que las casillas de verificación de Datos históricos y Registro del núcleo estén seleccionadas. Haga clic en `Crear`.

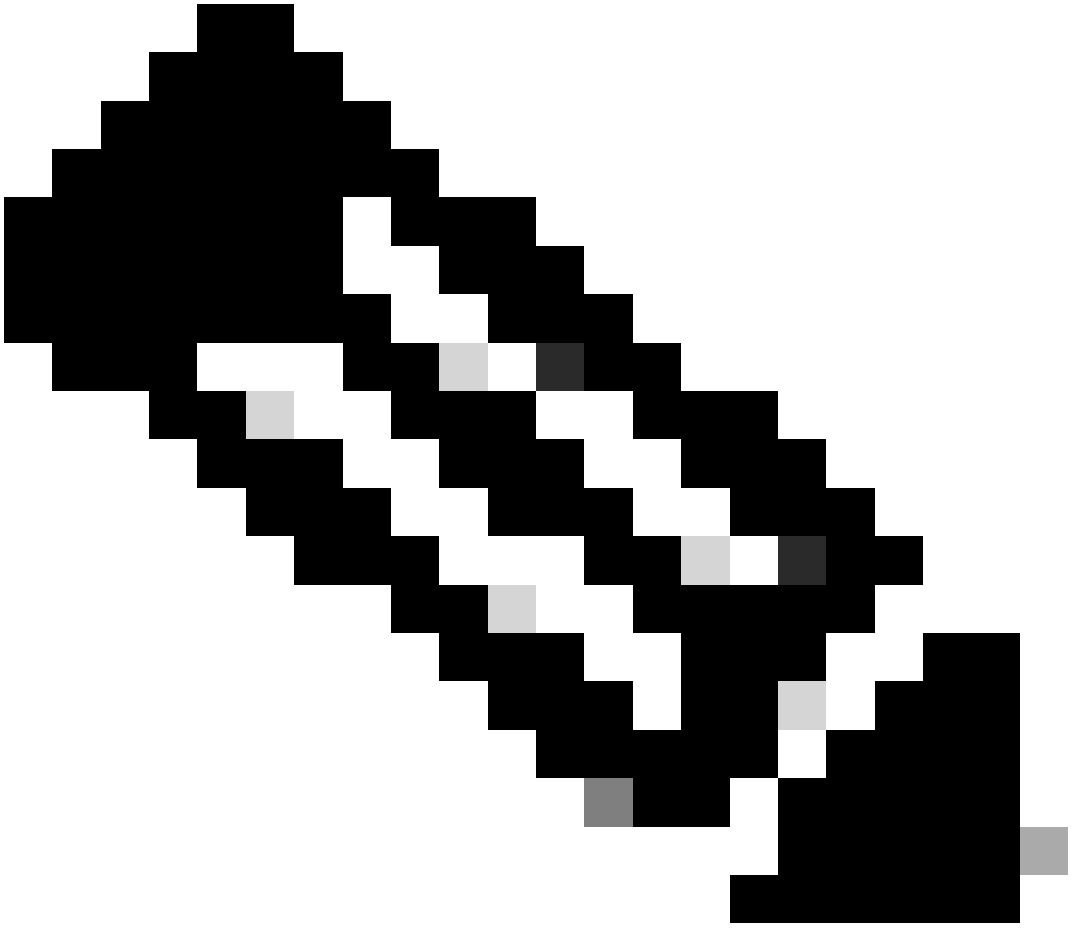


3. En la página Equipos, haga clic en `Diagnóstico` para el conector. Accederá a la página Repositorio de archivos de la sección Análisis.



4. En la página Repositorio de archivos, puede ver los estados de los diagnósticos solicitados. Busque los diagnósticos del equipo mediante los filtros. Cuando el diagnóstico tenga el estado "Disponible", haga clic en `Descargar`.

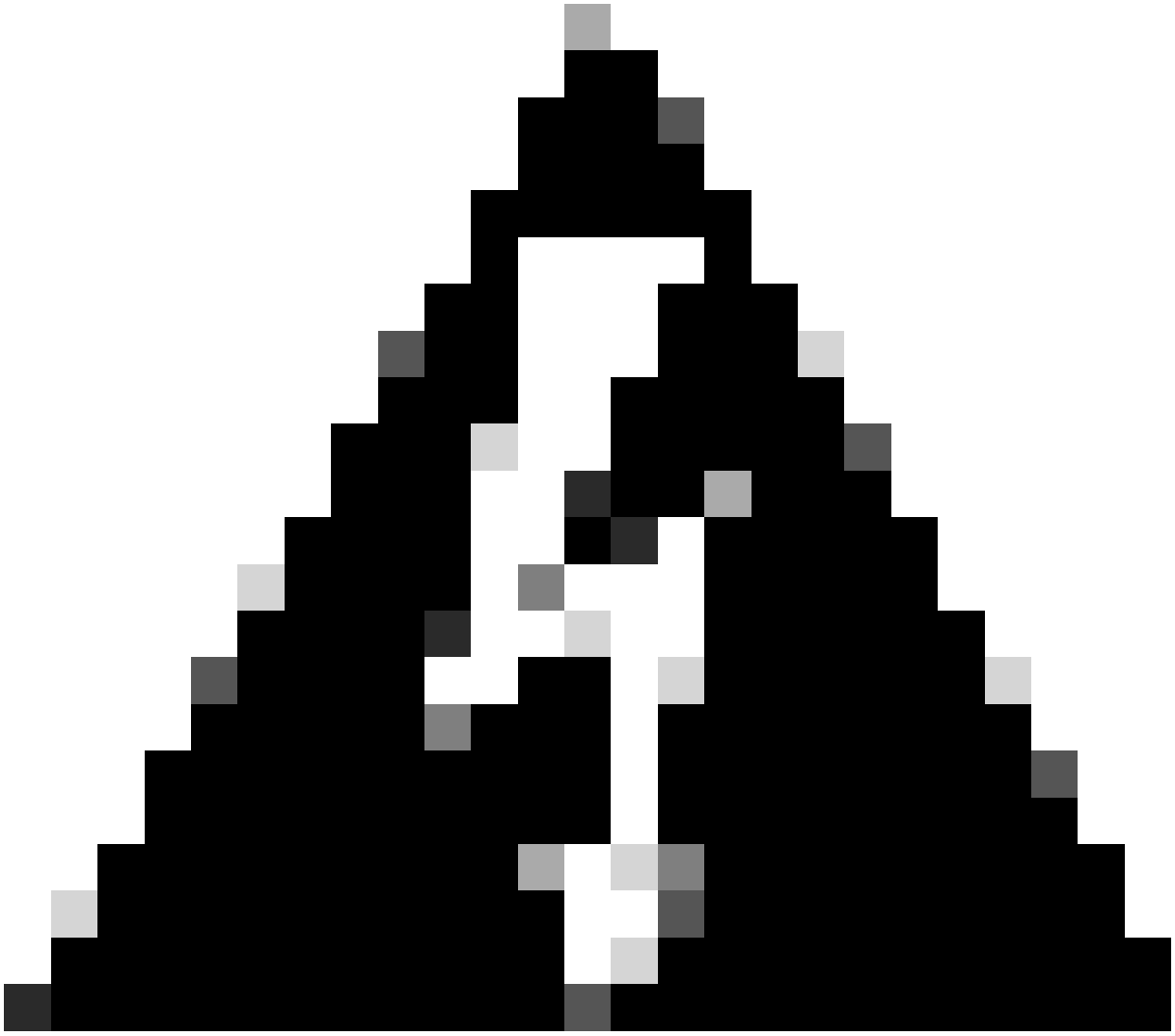




Nota: también recibirá un mensaje de correo electrónico de Cisco Secure Endpoint cuando los datos de diagnóstico solicitados estén disponibles para su descarga.

Resolución de problemas

El registro del modo de depuración se puede habilitar para el conector Secure Endpoint Linux para proporcionar información más detallada sobre la solución de problemas en los datos de diagnóstico. El modo de depuración puede activarse/desactivarse remotamente mediante Secure Endpoint Console o localmente mediante la herramienta de línea de comandos del conector Linux.



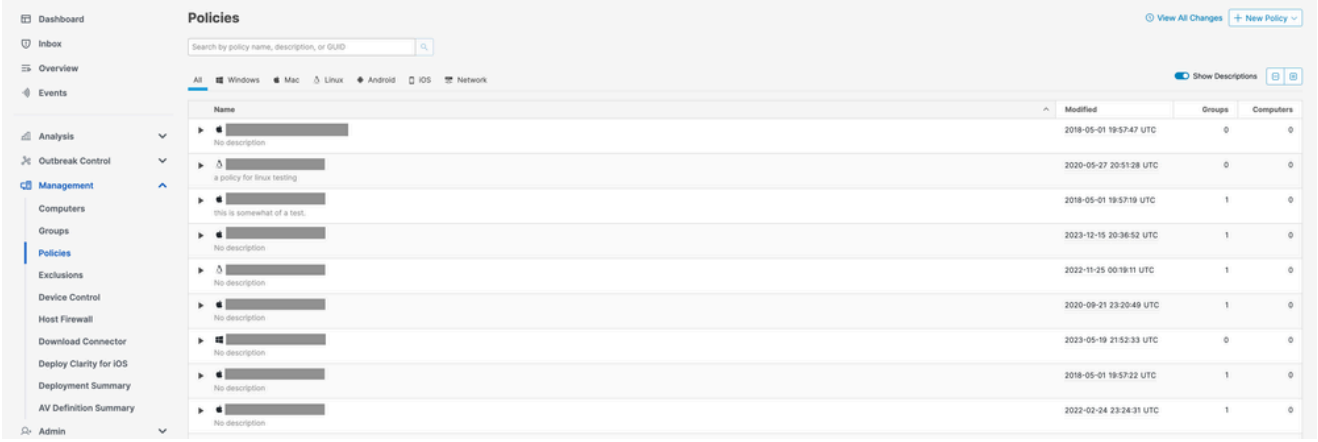
Advertencia: el modo de depuración solo debe habilitarse si un ingeniero de soporte técnico de Cisco realiza una solicitud para estos datos. Si mantiene activado el modo de depuración durante un período de tiempo prolongado, puede llenar el espacio en disco muy rápidamente y puede impedir que los datos del registro del conector y del registro de la bandeja se recopilen en el archivo de diagnóstico de compatibilidad debido al tamaño excesivo del archivo.

Activar modo de depuración

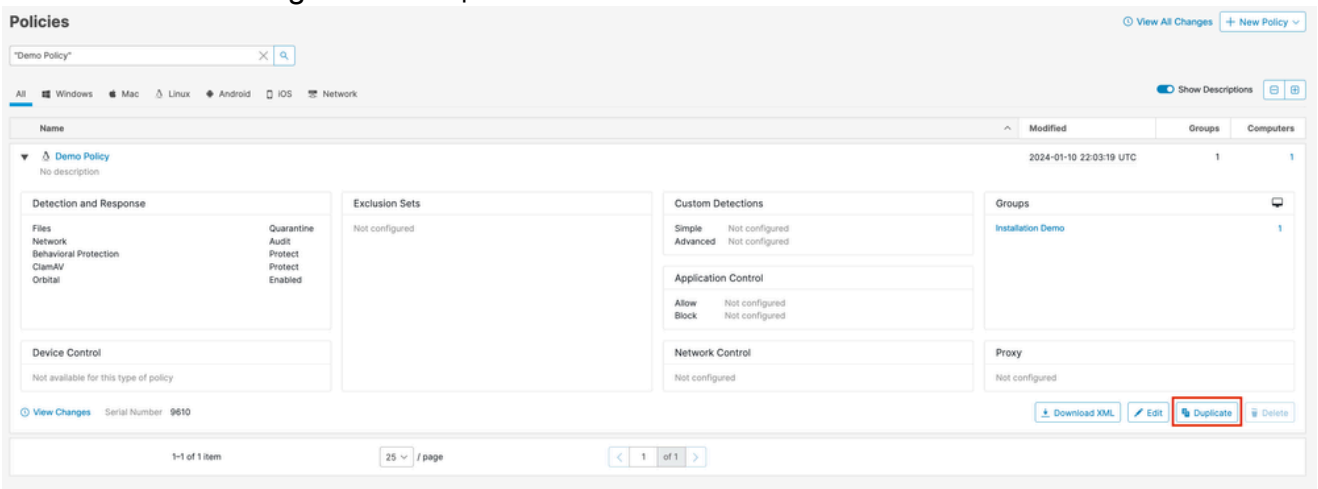
Habilitar el modo de depuración mediante Secure Endpoint Console

Complete estos pasos para habilitar el modo de depuración y recopilar datos de diagnóstico mediante Secure Endpoint Console:

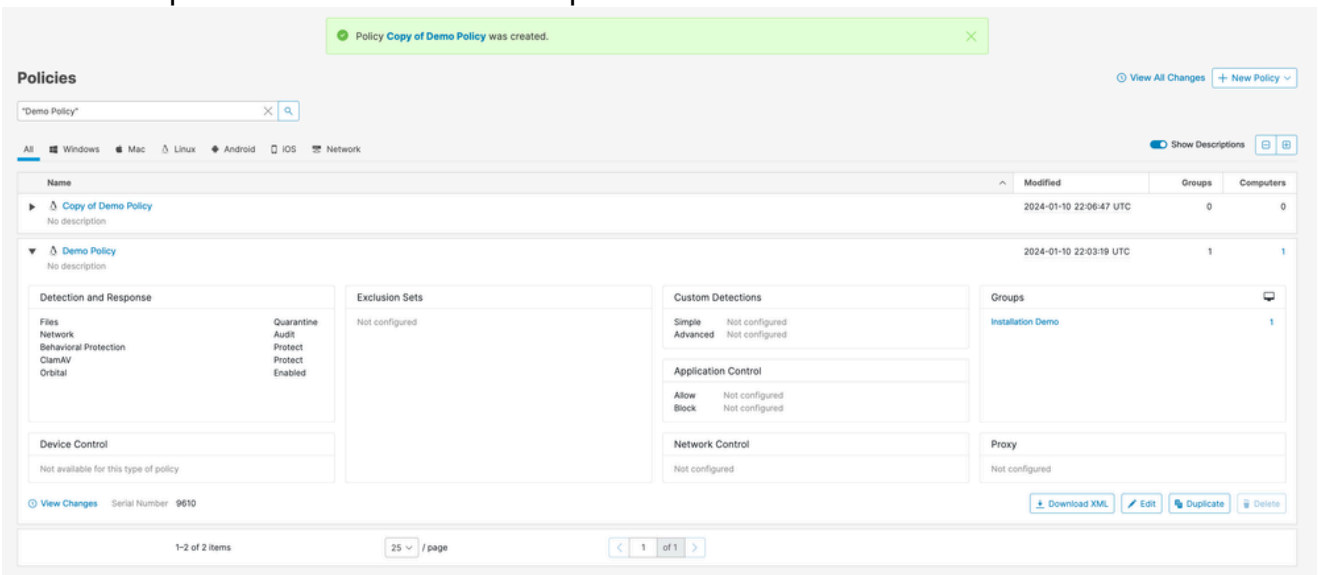
1. En Secure Endpoint Console, acceda a la página Políticas seleccionando `Management` -> `Policies`.



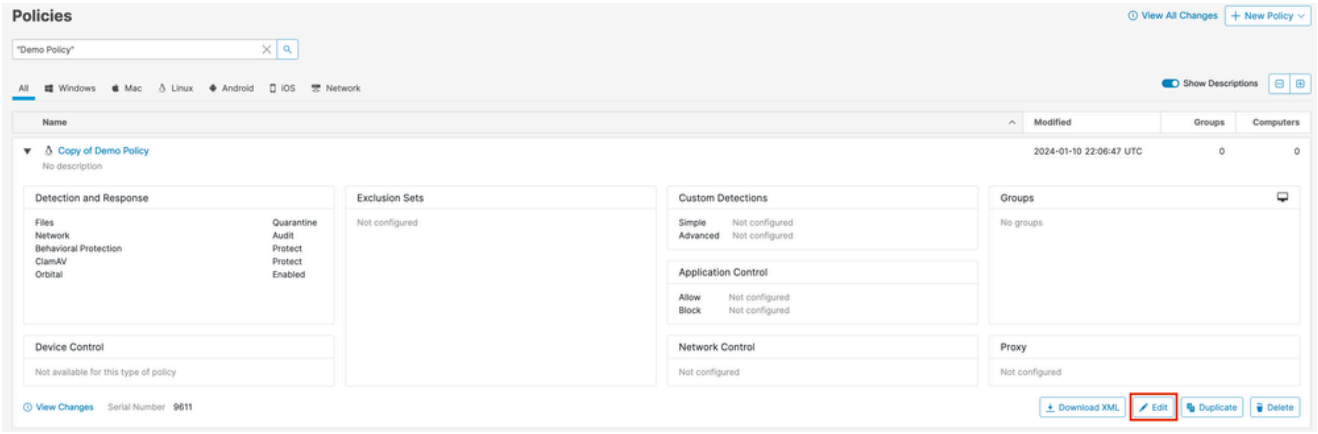
2. Localice y seleccione la política que se aplica al terminal; de este modo, se expandirá la ventana Política. Haga clic en `Duplicar`.



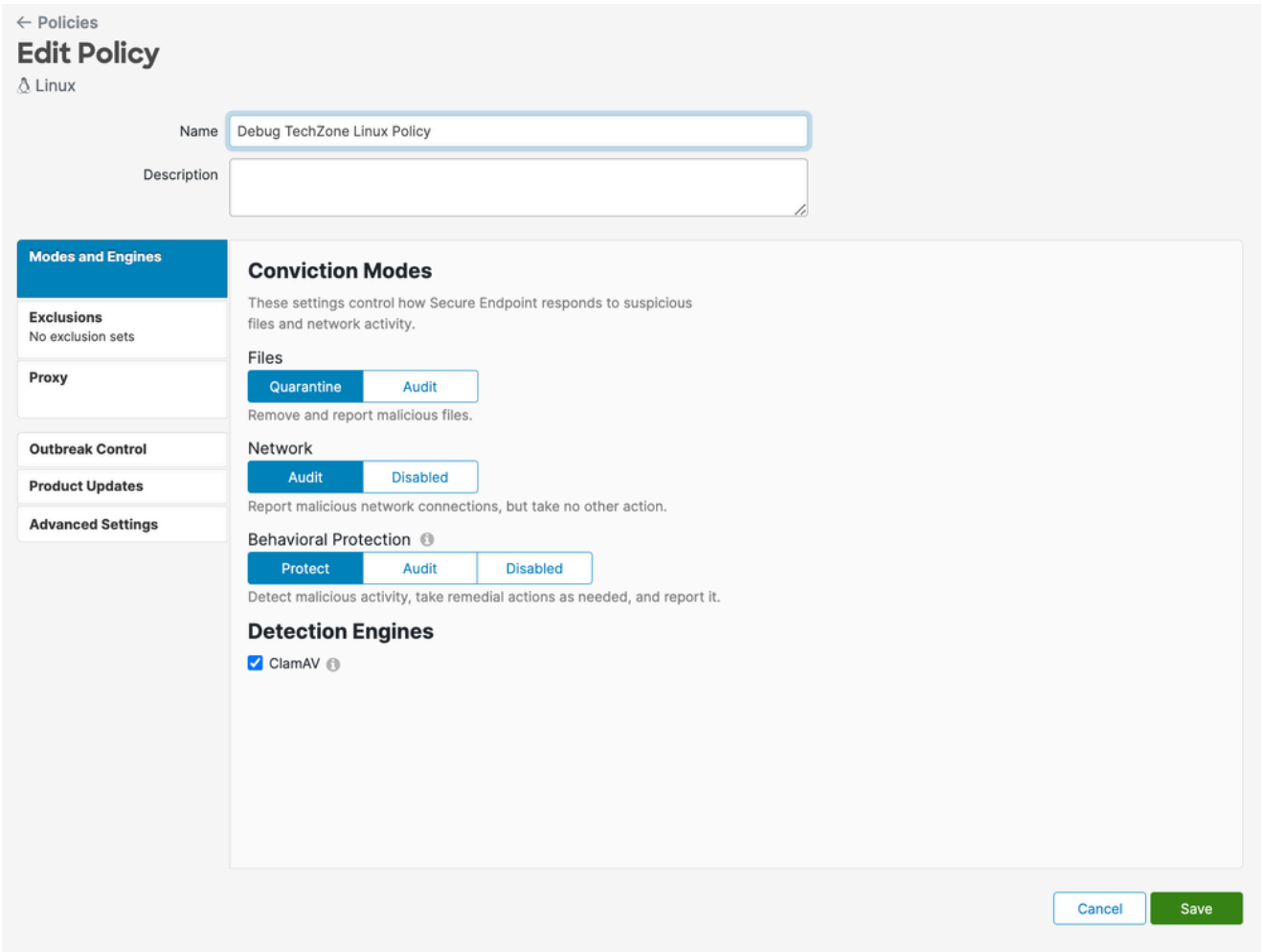
3. Secure Endpoint Console creará una copia de la directiva solicitada.



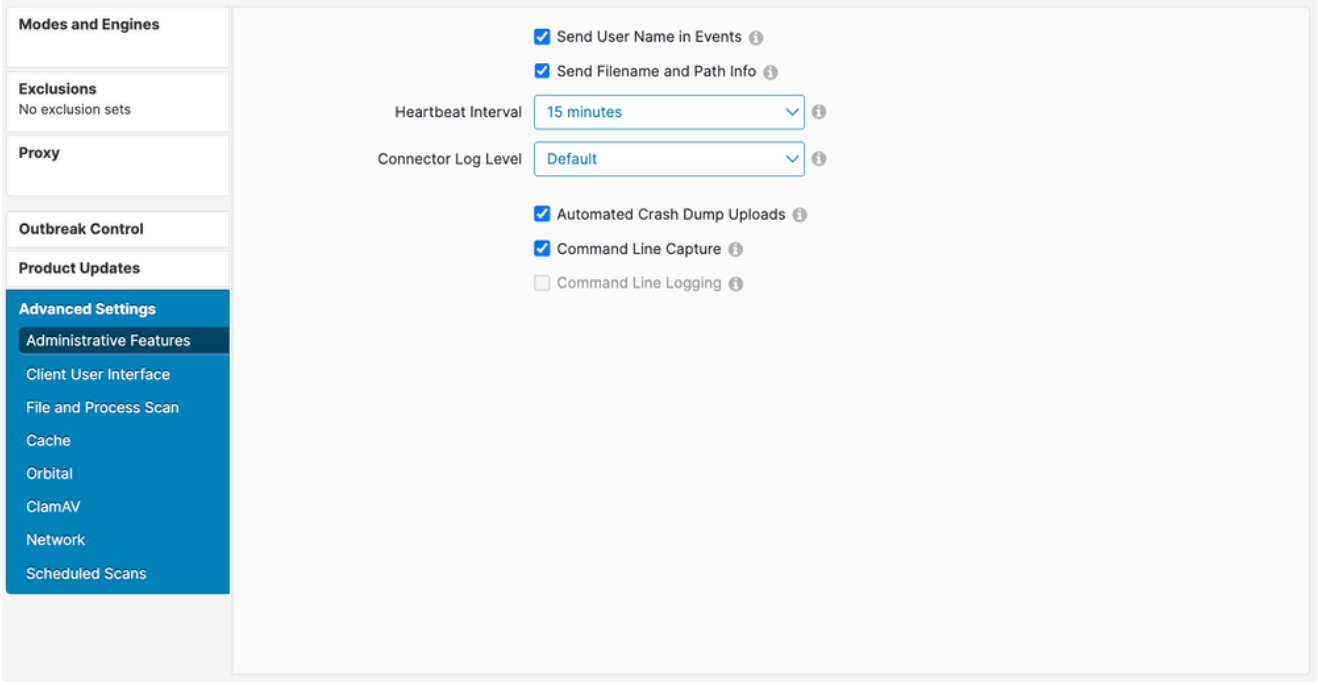
4. Seleccione y expanda la directiva duplicada y haga clic en `Editar`. Accederá a la página Editar directiva correspondiente a dicha directiva.



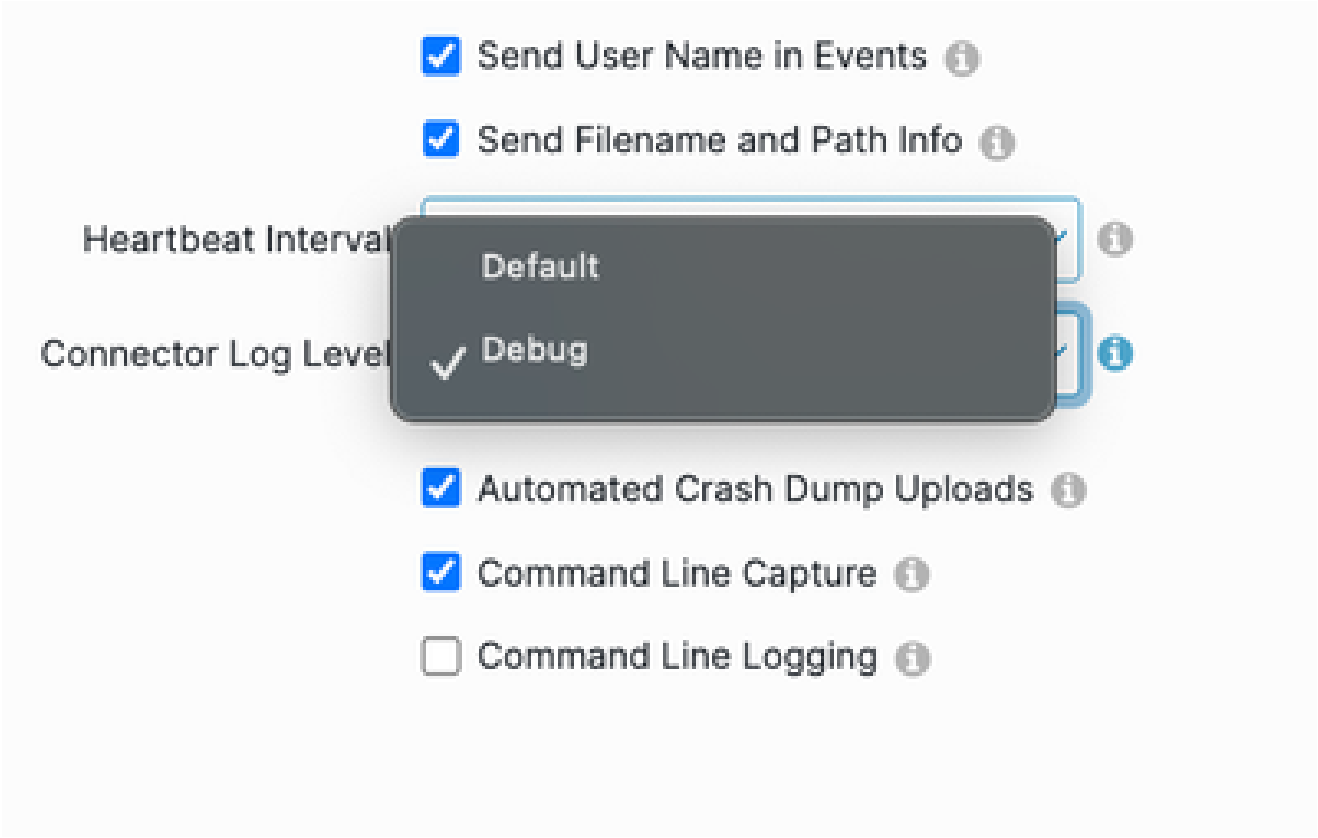
5. Cambie el nombre de la directiva. Por ejemplo, podría utilizar la política de Linux Debug TechZone.



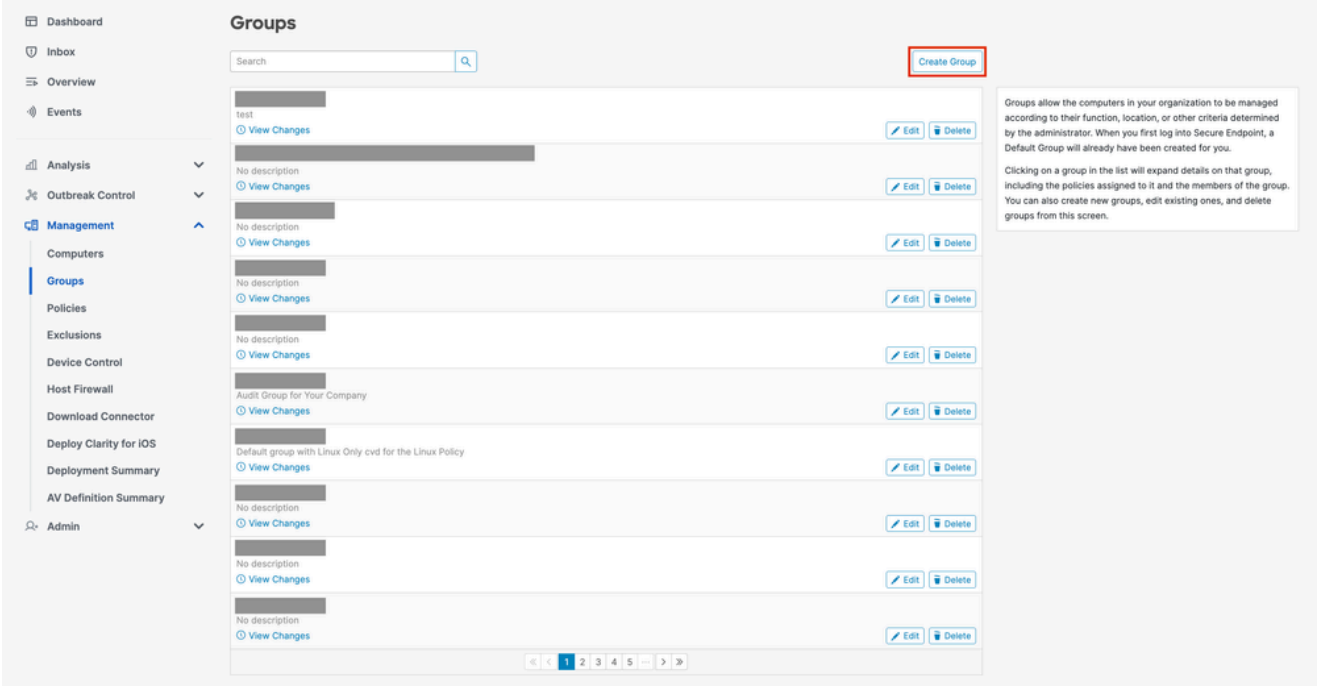
6. Seleccione `Advanced Settings`, y seleccione `Administrative Features` en la barra lateral.



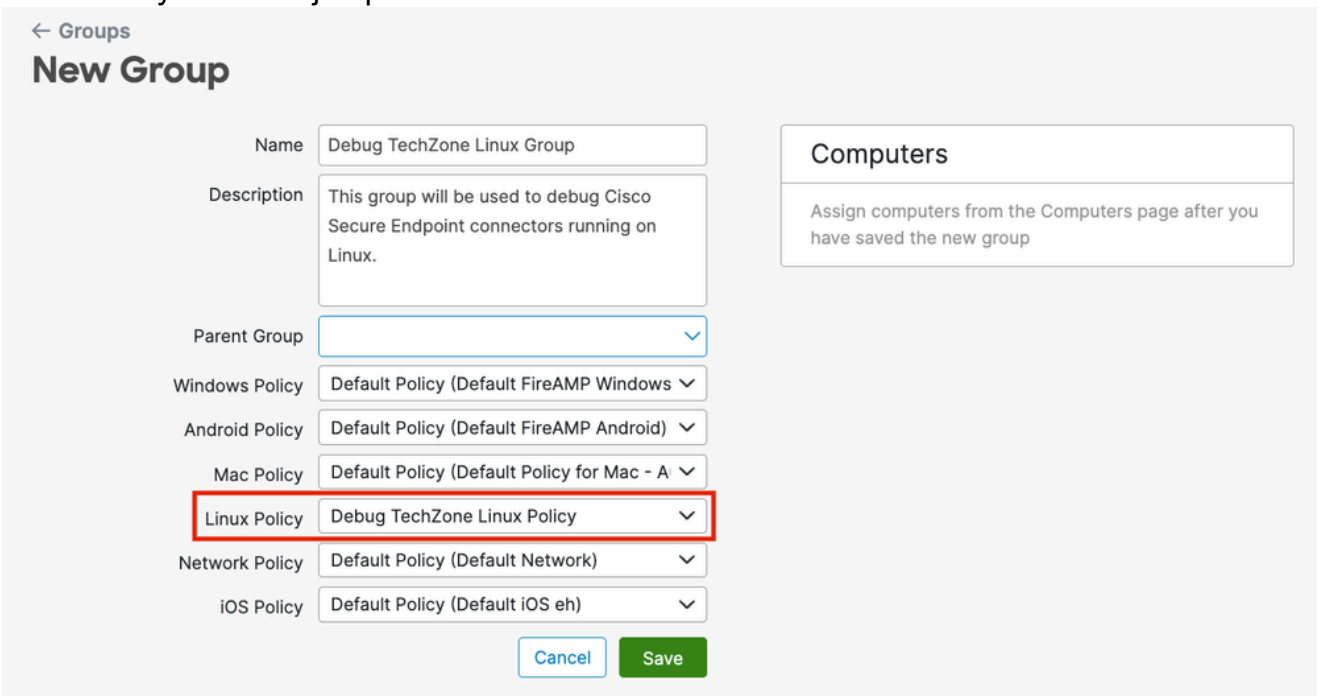
7. Expanda el menú desplegable Nivel de registro del conector y haga clic en "Depurar".



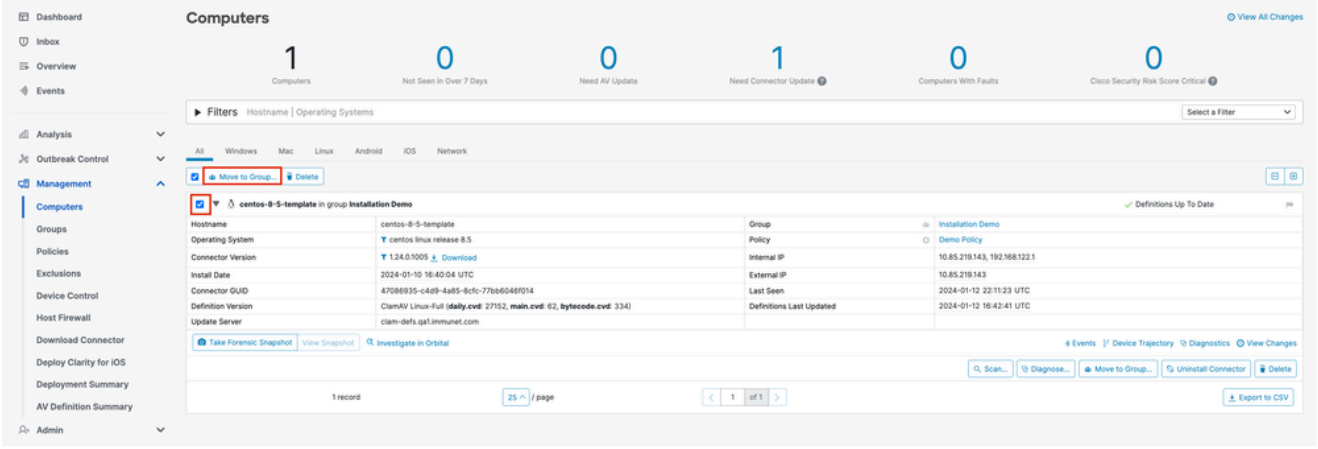
8. Haga clic en `Guardar para guardar los cambios.`
9. Vaya a la página Grupos seleccionando `Management` -> `Groups` y haga clic en `Create Group`. Accederá a la página Nuevo grupo.



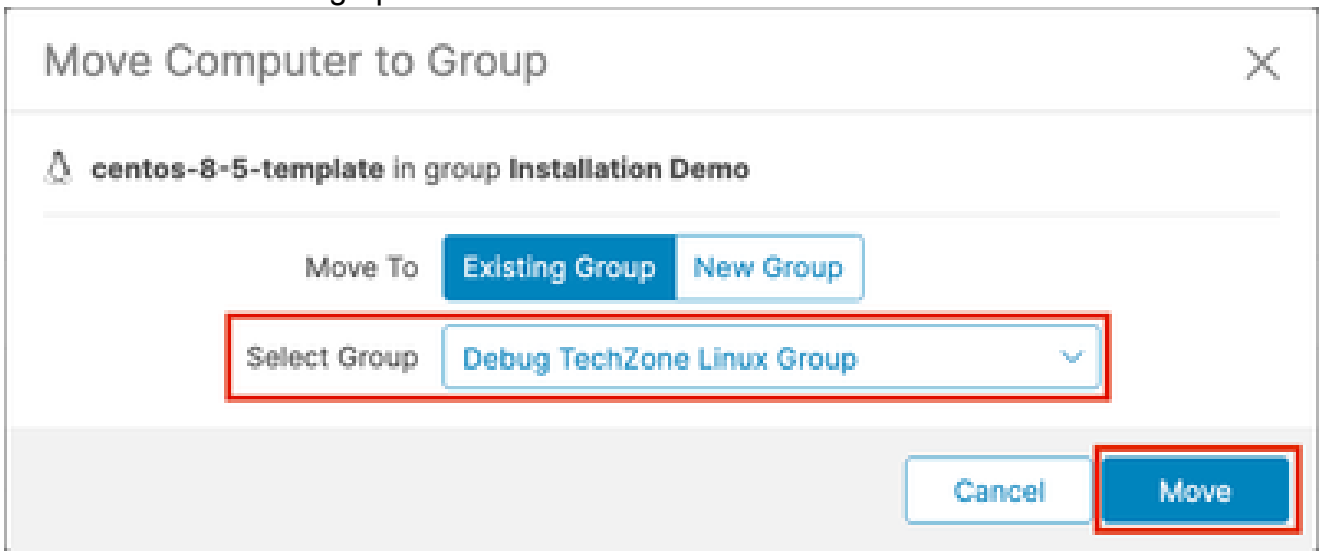
10. Introduzca un nombre para el grupo. Por ejemplo, podría utilizar Debug TechZone Linux Group.
11. Cambie la política Linux por la nueva política que acaba de crear, que es Debug TechZone Linux Policy en este ejemplo. Click `Save`.



12. Vaya a la página Equipos seleccionando `Administración` -> `Equipos` e identifique su equipo en la lista. Selecciónelo y haga clic en `Mover al grupo...`



13. En la ventana emergente Mover conector al grupo que aparece, seleccione el grupo recién creado en el menú desplegable `Seleccionar grupo`. Haga clic en `Mover` para mover el equipo seleccionado al nuevo grupo.



Habilitar el modo de depuración mediante la interfaz de línea de comandos del conector

Para habilitar el modo de depuración a través de la interfaz de línea de comandos (CLI) del conector de Linux, ejecute el siguiente comando:

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

Se debe mostrar el siguiente resultado:

```
Daemon now logging at 'info' level until next policy update
```

Deshabilitar modo de depuración

Después de obtener los datos de diagnóstico en el modo de depuración, debe volver al modo

normal al conector Secure Endpoint. El modo de depuración se puede desactivar utilizando Secure Endpoint Console o la herramienta de línea de comandos de conectores de Linux.

Deshabilitar el modo de depuración mediante Secure Endpoint Console

Para inhabilitar el modo Debug, siga los mismos pasos para habilitar el modo Debug usando Secure Endpoint Console, pero cambie el nivel de registro del conector a "Predeterminado" en el paso 7.

Deshabilitar el modo de depuración mediante la interfaz de línea de comandos del conector

Para inhabilitar el modo de depuración a través de la CLI del conector de Linux, ejecute el siguiente comando:

```
/opt/cisco/amp/bin/ampcli debuglevel 0
```

Se debe mostrar el siguiente resultado:

```
Daemon now logging at policy-specified log level
```

Vea también

- Recopilación de datos de diagnóstico de Cisco Secure Endpoint Connector para Mac
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).