

Aranda Device Management

Aquí podrá acceder a las ayudas técnicas para resolver problemas presentados en producción con las funcionalidades de ASEC.

Agente

Ejecutar el agente en modo debug

¿Cómo ejecutar el agente de Aranda Security Compliance en modo debug?

El modo debug ejecuta una única pasada del agente, por línea de comandos, que recopila los productos instalados, analiza las vulnerabilidades del equipo y guarda el resultado en archivos .json. Su utilidad principal es validar y depurar la información que genera el agente cuando se presenta una inconsistencia en producción, por ejemplo, un producto instalado que no aparece en la consola o una vulnerabilidad que no se detecta.

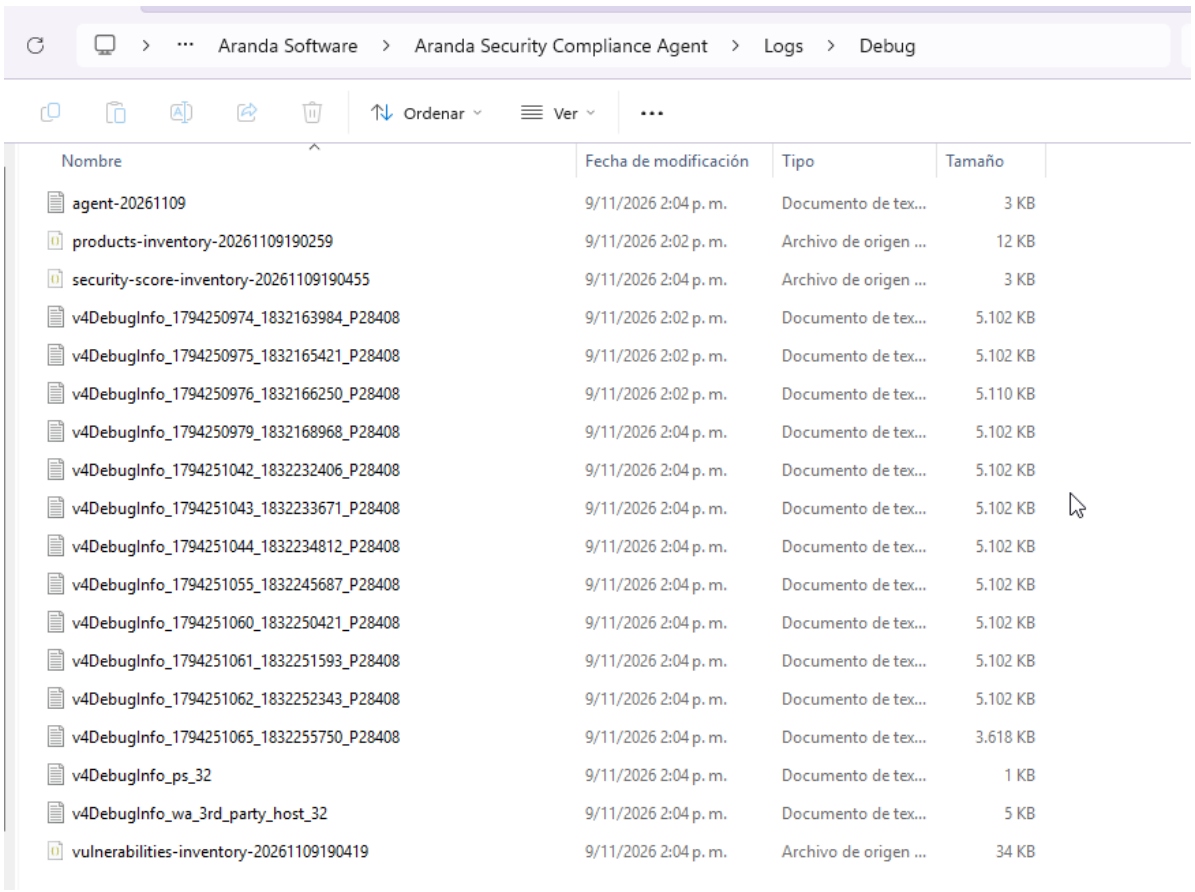
Al finalizar la recopilación y el análisis, el agente se detiene por sí mismo. En este modo no se inicializa la base de datos local ni se activan los módulos de comunicación del agente.

Archivos generados

Al ejecutar el agente en modo debug se generan los siguientes archivos dentro de la carpeta Logs/Debug, ubicada en la carpeta de instalación del agente:

Archivo	Contenido
products-inventory-<AAAAMMDDHHMMSS>.json	Inventario de productos instalados.
vulnerabilities-inventory-<AAAAMMDDHHMMSS>.json	Inventario de vulnerabilidades.
security-score-inventory-<AAAAMMDDHHMMSS>.json	Inventario del puntaje de seguridad. Se genera cuando el equipo cuenta con puntaje.
agent-<AAAAMMDD>.log	Registro de ejecución del agente. Se genera al indicar el parámetro --Logging:PathFormat.
v4DebugInfo_*	Registros detallados del motor de análisis, en nivel máximo (ALL).

En la imagen encuentra un ejemplo de la carpeta Logs/Debug en Windows una vez finalizada la ejecución.



⚐ **Nota:** la fecha y hora del nombre de los archivos .json corresponde a la hora UTC de la ejecución.

⚐ **Nota:** el agente agrega la fecha al nombre del registro, antes de la extensión. Por ejemplo, con el parámetro Logs/Debug/agent.log se genera agent-20261109.log.

⚐ **Nota:** durante la ejecución se pueden mostrar mensajes warn como «Unable to get installation directory» o «Unable to get vulnerabilities», que indican que el agente no encontró un producto específico instalado en el equipo (por ejemplo, LibreOffice o Snap). Son esperados y no impiden la generación de los archivos.

⚠ **Advertencia:** el motor de análisis genera varios archivos v4DebugInfo_* de aproximadamente 5 MB cada uno. Verifique que el equipo cuente con espacio suficiente en disco y elimine la carpeta Logs/Debug al finalizar el análisis.

Parámetros

Parámetro	Descripción
-debug true / --debug true	Habilita el modo debug del agente.
--Logging:PathFormat Logs/Debug/agent.log	Define la ruta del registro del agente. Es opcional.

Prerrequisitos

- Acceso al equipo donde está instalado el agente.
- Permisos de administrador (Windows) o sudo (Linux y macOS).
- Una terminal ubicada en la carpeta de instalación del agente.

Ejecución

Ejecute el comando siempre desde la carpeta de instalación del agente, ya que las rutasLogs/Debug son relativas a esa ubicación.

Windows

1. Abra una consola de comandos (CMD o PowerShell) como administrador y ubíquese en la carpeta de instalación del agente:

```
cd "C:\Program Files\Aranda Software\Aranda Security Compliance Agent"
```

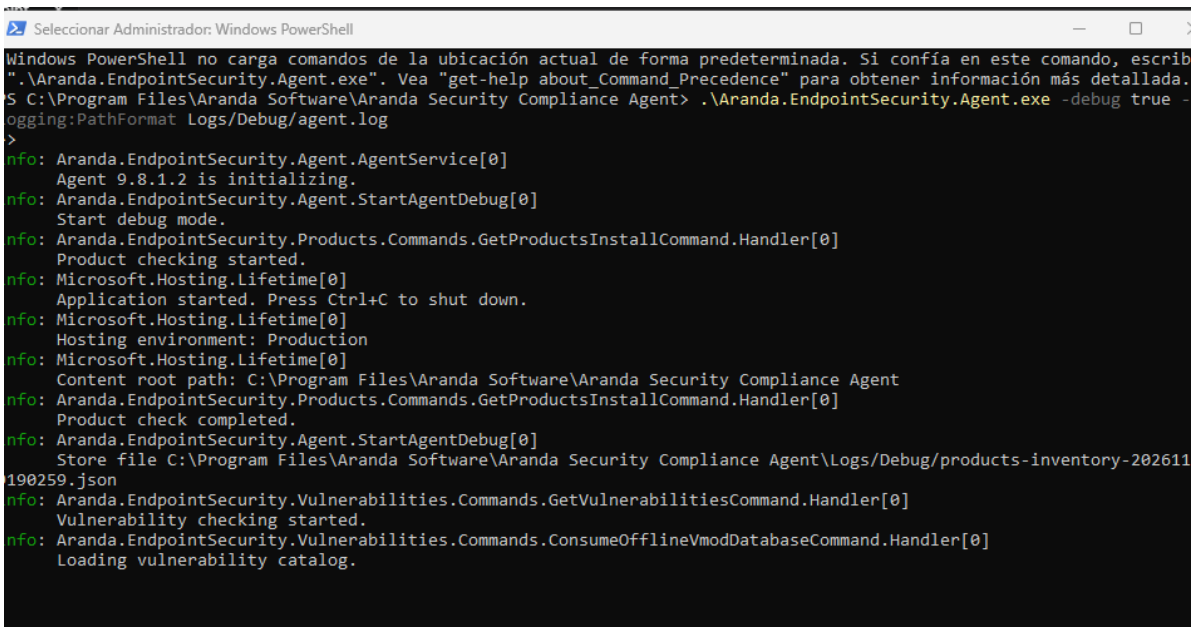
2. Ejecute el agente en modo debug. En CMD:

```
Aranda.EndpointSecurity.Agent.exe -debug true --Logging:PathFormat Logs/Debug/agent.log
```

En PowerShell, anteponga .\ al nombre del ejecutable:

```
.\Aranda.EndpointSecurity.Agent.exe -debug true --Logging:PathFormat Logs/Debug/agent.log
```

En la imagen encuentra el inicio de la ejecución en PowerShell: el agente registra el mensaje Start debug mode. y, al terminar cada proceso, indica la ruta del archivo generado.



⚐ **Nota:** para habilitar únicamente el modo debug, sin el parámetro del registro, utilice Aranda.EndpointSecurity.Agent.exe --debug true.

⚠ **Advertencia:** el ejecutable se encuentra en la carpeta de instalación, no en su subcarpeta Logs. Si el comando se ejecuta desde Logs, se muestra el mensaje «no se reconoce como un comando interno o externo».

⚠ **Advertencia:** PowerShell no ejecuta programas ubicados en la carpeta actual sin el prefijo .\. Si se omite, se muestra el error «El término 'Aranda.EndpointSecurity.Agent.exe' no se reconoce como nombre de un cmdlet».

⚠ **Advertencia:** si el título de la ventana muestra «Seleccionar», la consola se encuentra en modo selección y detiene la ejecución del agente. Presione la tecla Esc para continuar.

Linux

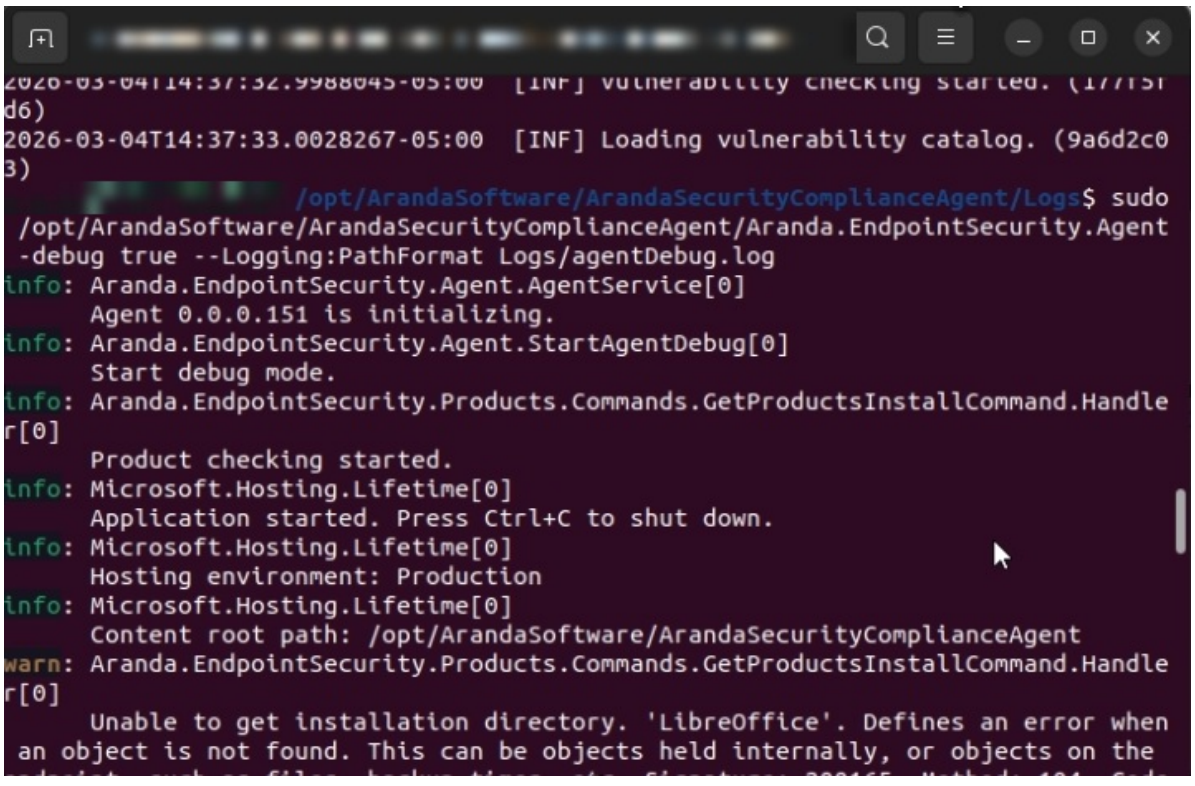
1. Abra una terminal y ubíquese en la carpeta de instalación del agente:

```
cd /opt/ArandaSoftware/ArandaSecurityComplianceAgent
```

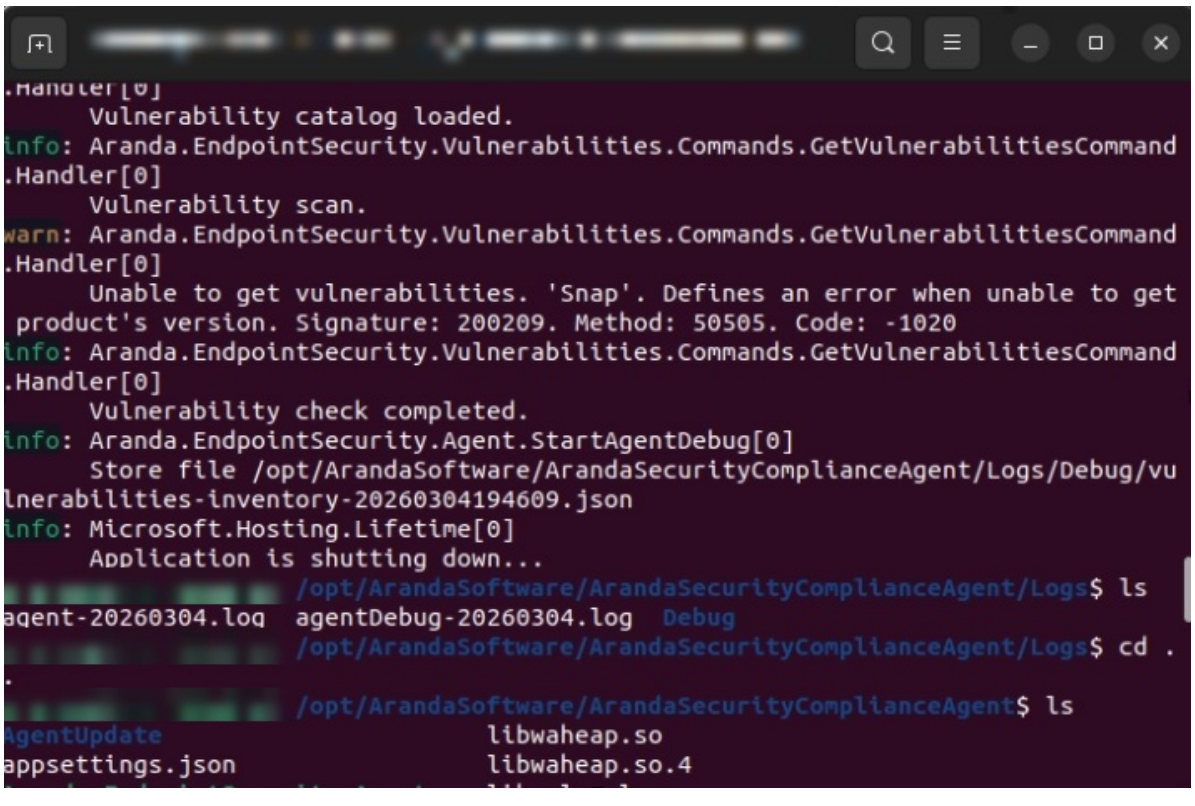
2. Ejecute el agente en modo debug:

```
sudo ./Aranda.EndpointSecurity.Agent -debug true --Logging:PathFormat Logs/Debug/agent.log
```

En la imagen encuentra el inicio de la ejecución en Linux.



Al finalizar, el agente indica la ruta del archivo generado y se detiene por sí mismo, como se observa a continuación.



3. Si no es posible ingresar a la carpeta de debug por falta de permisos, asigne la propiedad de la carpeta al usuario aranda:

```
sudo chown -R aranda:aranda /opt/ArandaSoftware/ArandaSecurityComplianceAgent/Logs/Debug
```

> ⚐ **Nota:** al ejecutar el comando con sudo, los archivos se crean con el usuario root; por esta razón se requiere el ajuste de propiedad.

macOS

1. Abra una terminal con permisos de administrador y ubíquese en la carpeta de instalación del agente:

```
cd "/Library/Application Support/com.arandasoft.asec.osx"
```

2. Ejecute el agente en modo debug:

```
sudo "./Aranda.EndpointSecurity.Agent" -debug true --Logging:PathFormat Logs/Debug/agent.log
```

Validar la generación de los archivos

Una vez el agente finalice su ejecución, valide los resultados así:

1. Ingrese a la carpeta Logs/Debug de la instalación del agente.

2. Verifique que exista el archivo products-inventory-<AAAAMMDDHHMMSS>.json con el inventario de productos instalados.

3. Verifique que exista el archivo vulnerabilities-inventory-<AAAAMMDDHHMMSS>.json con el inventario de vulnerabilidades.

4. Verifique que exista el archivo security-score-inventory-<AAAAMMDDHHMMSS>.json con el puntaje de seguridad, cuando aplique.

5. Abra los archivos y compare su contenido con la información visible en la consola, para identificar diferencias entre lo que el agente detecta y lo que se reporta.

> ⚠ **Advertencia:** los archivos de debug contienen el inventario completo del equipo. Compártalos únicamente por canales autorizados y elimínelos cuando finalice el análisis.