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

## Contenido

Introducción					
Antecedentes					
<u>Generar datos de diagnóstico</u>					
Generar datos de diagnóstico localmente mediante la herramienta de soporte					
Generar datos de diagnóstico mediante la consola de terminal seguro					
Resolución de problemas					
Activar modo de depuración					
Habilitar el modo de depuración mediante Secure Endpoint Console					
Habilitar el modo de depuración mediante la interfaz de línea de comandos del conector					
Deshabilitar modo de depuración					
Deshabilitar el modo de depuración mediante Secure Endpoint Console					
Deshabilitar el modo de depuración mediante la interfaz de línea de comandos del conector					
<u>Vea también</u>					

## 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...

Dashboard		Computers							© Vie	w All Changes
Inbox		1	0	0		1		0	0	
Overview		1	0	0				0	0	
Events		Computers	Not Seen in Over 7 Days	Need AV Update	Need	Connector Update 🚱	Con	nputers With Faults	Cisco Security Risk Score Critical 🚱	
		Filters Hostname   Operating Syste	ms						Select a Filter	~
네 Analysis	$\sim$									
3 Outbreak Control	~	All Windows Mac Linux A	ndroid IOS Network							
CE Management	~	🔲 💩 Move to Group 🔋 Delete								88
Computers		🗌 🔻 👌 centos-8-5-template in group Inst	allation Demo						Definitions Up To Date	14
Groups		Hostname	centos-8-5-template			Group		Installation Demo		
B-F-I		Operating System	▼ centos linux release 8.5			Policy	0	Demo Policy		
Policies		Connector Version	▼ 124.0.1005 + Download			Internal IP		10.85.219.143, 192.168.122.1		
Exclusions		Install Date	2024-01-10 16:40:04 UTC			External IP		10.85.219.143		
Device Control		Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f014			Last Seen		2024-01-15 16:10:08 UTC		
11		Definition Version	ClamAV Linux-Full (daily.ovd: 27154, main.o	wd: 62, bytecode.cvd: 334)		Definitions Last Updated		2024-01-14 16:44:02 UTC		
Plost Pirewall		Update Server	clam-defs.qa1.immunet.com							
Download Connector		Take Forensic Snapshot View Snapshot	C. Investigate in Orbital						4 Events (P Device Trajectory (9 Diagnostics (0)	View Changes
Deploy Clarity for iOS								9, Scan 19 Diago	ose 🔺 Move to Group	Telete
Deployment Summary		1				41 5				
AV Definition Summary		1 record	25 ^ /	page	< 1	011 2			10	port to CSV
O: Admin	~									

 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.

New Connector Dia	gnostic for centos-8-5-template	$\times$
Debug session	5 minutes V Historical Data Kernel Log	
Diagnostic files are generate.	imited to 50MB in size and can take up to 24 hours to	
	Cancel	te

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

O View All Change
0 0
pdate 🕘 Computers With Faults Cisco Security Risk Score Critical 🚱
Select a Filter 🗸 🗸
88
✓ Definitions Up To Date 😕
du Installation Demo
O Demo Policy
10.85.219.143, 192.168.122.1
10.85.219.143
2024-01-15 16-10:08 UTC
st Updated 2024-01-14 16:44.02 UTC
4 Events 12 Device Trajectory 19 Diagnostics 10 View Changes
Q. Scan   1/3 Diagnose   & Move to Group   1/3 Uninstall Connector   🛊 Delete
± Export to CSV

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.

E	3 Dashboard		File Repository			Connector Diagnostics Feature Overview				() View All Changes						
5 11 12	) Inbox 5 Overview ) Events		Search Search by SHA-256 or file	e name			τ	pe Connector Diagnost	cs v Group Installation	Demo v Apply Fiters						
			AI Available Requested	Being Processed Failed Rejected						88						
	1 Analysis	^	File				Status	Requested By	Date ~	Actions						
	Reports		▼ Connector diagnostics for cent	tos-8-5-template			Available 😡		2024-01-15 16:27:12 UTC							
	File Analysis		Connector Diagnostics Requested	2024-01-15 16:19:20 UTC												
	File Repository		Original File Name	ampsupport_47086935_20240115_092702.zip												
	Vulnerable Software		File Size	10.1 MB												
	Indicators								O View Changes	centos-o-o-tempate					à Druin	and B Data
	iOS Clarity		o na olaga						1							
	Prevalence			1-1 of 1 item	25 ^ / page	< 1 of 1 >										
	Threat Root Cause															
	Talos Threat Hunting															
	Orbital															
3	© Outbreak Control	~														
¢8	Management	~														
я	Admin	~														



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:

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

Dashboard		Policies	© Vi	w All Changes	New Policy ~
1 Inbox		Search by policy name, description, or GUID			
Overview     Events		All all Windows & Mac & Linux & Android C IOS To Network		Show Description	tions 😑 🗵
		Nano	^ Modified	Groups	Computers
刭 Anatysis	~	No description	2018-05-01 19:57-47 UTC	0	0
3c Outbreak Control	ř	b     b     poly for linux testing	2020-05-27 20:51:28 UTC	0	٥
Computers	î	this is somewhat of a test.	2018-05-01 19:57:19 UTC	1	0
Groups		No description	2023-12-15 20:36:52 UTC	i	0
Exclusions		► 8 Madesorption	2022-11-25 00:19:11 UTC	1	0
Device Control Host Firewall		No description	2020-09-21 23:20:49 UTC	1	0
Download Connector		► #	2023-05-19 21:52:33 UTC	٥	0
Deploy Clarity for iOS Deployment Summary		No description	2018-05-01 19:57:22 UTC	1	٥
AV Definition Summary		No description	2022-02-24 23:24:31 UTC	1	0

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

Policies			⊙ View All Changes + New Policy ∨		
"Demo Policy" X					
All 🗱 Windows 🔹 Mac 🛆 Linux 🗣 Android 📋 iOS 🕾 Ne	twork		Show Descriptions		
Name			Modified Groups Computers		
A Demo Policy     No description			2024-01-10 22:03:19 UTC 1 1		
Detection and Response	Exclusion Sets	Custom Detections	Groups		
Files Quarantine Network Audit Behavioral Protection Protect Oten M	Net configured	Simple Not configured Advanced Not configured	Installation Demo 1		
Orbital Enabled		Application Control			
		Allow Not configured Block Not configured			
Device Control		Network Control	Proxy		
Not available for this type of policy		Not configured	Not configured		
View Changes Serial Number 9610			🛓 Download XML 🖉 Edit 📲 Duplicate 🗑 Delete		
1-1 of 1 item	25 ~ / page < 1	of 1 >			

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

	Policy Copy of Demo Policy was created.		×			
Policies				() View	All Changes +	New Policy ~
"Demo Policy" X 🤉						
All 🖽 Windows 📽 Mac 👌 Linux 🗣 Android 🔲 iOS 😒	Network				Show Descript	Jons 😑 🗄
Namo			^	Modified	Groups	Computers
A Copy of Demo Policy     No description				2024-01-10 22:06:47 UTC	0	0
Demo Policy     No description				2024-01-10 22:03:19 UTC	1	1
Detection and Response	Exclusion Sets	Custom Detections	Grou	ps		Ţ
Files Quarantine Network Audit Behavioral Protection Protect	Not configured	Simple Not configured Advanced Not configured	Instal	Installation Demo		1
ClamAV Protect Orbital Enabled		Application Control				
		Allow Not configured Block Not configured				
Device Control		Network Control	Prox	у		
Not available for this type of policy		Not configured	Not o	onfigured		
View Changes Serial Number 9610				🛓 Download XML	it 🖣 Duplicate	) 🗑 Delete
1-2 of 2 items	25 v ) / page	of 1 义				

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

Policies			() View	v All Changes + New Policy
"Demo Policy" X Q				
All 🛤 Windows 📽 Mac 🛆 Linux 🗣 Android 🔲 iOS 🕾 Ne	twork			Show Descriptions
Name			^ Modified	Groups Computers
Copy of Demo Policy     No description			2024-01-10 22:06:47 UTC	0 0
Detection and Response	Exclusion Sets	Custom Detections	Groups	Ţ
Files Quarantine Network Audit Behavioral Protection Protect	Not configured	Simple Not configured Advanced Not configured	No groups	
ClamAV Protect Orbital Enabled		Application Control		
		Allow Not configured Block Not configured		
Device Control		Network Control	Proxy	
Not available for this type of policy		Not configured	Not configured	
View Changes Serial Number 9611			Download XML     Ec	dit 🖣 Duplicate 🗑 Delete

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

← Policies <b>Edit Policy</b> <sup></sup> ∆ Linux	
Name	Debug TechZone Linux Policy
Description	
Modes and Engines	Conviction Modes
Exclusions No exclusion sets	files
Proxy	Quarantine         Audit           Remove and report malicious files.
Outbreak Control	Network
Product Updates	Audit Disabled
Advanced Settings	Report malicious network connections, but take no other action.
	Protect Audit Disabled
	Detect malicious activity, take remedial actions as needed, and report it.
	Detection Engines
	ClamAV 🚯
	Cancel Save

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.

	Dashboard		Groups		
	Inbox		Search Q	Create Group	
≡Þ	Overview				
-0	Events		test O View Changes	🖌 Edit 🗑 Delete	Groups allow the computers in your organization to be managed according to their function, location, or other criteria determined by the administrator. When you first log into Secure Endpoint, a
네	Analysis	~	No description		Default Group will already have been created for you. Clicking on a group in the list will expand details on that group,
Э¢	Outbreak Control	~	© View Changes	Zedit Delete	including the policies assigned to it and the members of the group. You can also create new groups, edit existing ones, and delete
ςB	Management	^	No description		groups from this screen.
	Computers		O View Changes	Zedit Delete	
1	Groups		No description		
1	Policies		O View Changes	Zedit Delete	
	Exclusions		No description		
	Device Control		() View Changes	🖌 Edit 🗑 Delete	
	Host Firewall		Audit Group for Your Company		
	Download Connector		© View Changes	🖊 Edit 🔋 Delete	
	Deploy Clarity for iOS		Default group with Linux Only cyd for the Linux Policy		
	Deployment Summary		O View Changes	🖊 Edit 🗑 Delete	
	AV Definition Summary		No description		
Q.	Admin	$\sim$	© View Changes	🖌 Edit 🗑 Delete	
			No description		
			© View Changes	🖌 Edit 🗑 Delete	
			No description		
			③ View Changes	🖌 Edit 🔋 Delete	
			≪ < 1 2 3 4 5 - > >		

- 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.

← Groups <b>New Group</b>		
Name	Debug TechZone Linux Group	Computers
Description	This group will be used to debug Cisco Secure Endpoint connectors running on Linux.	Assign computers from the Computers page after you have saved the new group
Parent Group		
Windows Policy	Default Policy (Default FireAMP Windows 🗸	
Android Policy	Default Policy (Default FireAMP Android) 🗸	
Mac Policy	Default Policy (Default Policy for Mac - A	
Linux Policy	Debug TechZone Linux Policy	
Network Policy	Default Policy (Default Network)	
iOS Policy	Default Policy (Default iOS eh)	
	Cancel 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...

	Dashboard		Computers							© Vie	w All Changes
U	Inbox		4	•	•		4		•	0	
	Overview		1	0	0		1		0	0	
-4	Events		Computers	Not Seen in Over 7 Days	Need AV Update	Need	i Connector Update 🔞	Com	puters With Faults	Cisco Security Risk Score Critical 🚱	
*			Elitere Montenen Desertion Sociales     v								
	Analysis		L 1005 testamin fabrican fabrican								
101	Analysis	÷	Al Windows Mac Linux Android IDS Network								
30	Outbreak Control										
48	Management	^	A de More to Geope, B Celete								
1	Computers		🔁 🔻 🛆 centes-8-5-template in group lastallation Demo							14	
- 1	Groups		Hostname	centos-8-5-template			Group		Installation Demo		
			Operating System	T centos linux release 8.5			Policy	0	Demo Policy		
	Policies		Connector Version	T 1.24.0.1005 + Download			Internal IP		10.85.219.143, 192.168.122.1		
	Exclusions		Install Date	2024-01-10 16:40:04 UTC			External IP		10.85.219.143		
	Device Control		Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f01	14		Last Seen		2024-01-12 22:11:23 UTC		
	Mast Firewall		Definition Version	ClamAV Linux-Full (daily.cvd: 27152, main.	.cvd: 62, bytecode.cvd: 334)		Definitions Last Updated		2024-01-12 16:42:41 UTC		
	Plost Pirewall		Update Server	clam-defs.ga1.immunet.com							
	Download Connector		Take Forensic Snapshot View Snapshot		4 Events 12 Device Trajectory 13 Diagnostics 10 V	few Changes					
	Deploy Clarity for iOS	Q. Scan									Delete
	Deployment Summary										
	AV Definition Summary		1 record	25 ^	) bađe	1	1 of 1 >			Export to CSV	

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.

Move Co	Move Computer to Group								
∆ centos-8-	centos-8-5-template in group Installation Demo								
	Move To	Existing Group New Group							
	Select Group	Debug TechZone Linux Group	~						
			Cancel Mov	e					

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 <u>habilitar el modo Debug usando</u> <u>Secure Endpoint Console</u>, 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).