Generar paquete de diagnóstico para dispositivos de análisis de red seguros

Contenido

Introducción Procedimiento Método 1. Desde la interfaz de usuario web del jefe Método 2. Desde la interfaz de usuario del administrador de cada dispositivo Método 3. Desde la interfaz de línea de comandos (CLI) de cada dispositivo Troubleshoot Información Relacionada

Introducción

Este documento describe los diferentes procedimientos disponibles para recopilar un paquete de diagnóstico para dispositivos de Secure Network Analytics (SNA).

Procedimiento

Hay tres métodos principales para generar el paquete de diagnóstico para los dispositivos SNA. El método sugerido es el **Método 1. Desde la interfaz de usuario del administrador Web**, sin embargo, los otros dos métodos son una opción en caso de que la interfaz de usuario Web del jefe no esté disponible.

Nota: Si la interfaz de usuario web del jefe no está disponible y necesita generar un paquete de diagnóstico desde el administrador, consulte el **método 3. Desde la interfaz de línea de comandos (CLI)** de cada dispositivo.

Método 1. Desde la interfaz de usuario web del jefe

- 1. Inicie sesión en la interfaz de usuario web del jefe.
- 2. Vaya a Configuración global > Administración central.

藯 Network A	nalytics		Dashboards *	Monitor Analyz	re * Jobs * Conf	igure * Deploy *			۵ ք ۵	+ disco SECURE
									Global Settings	
Security Insight Da	ashboard Inside Ho	osts							Central Management 🛛 😓	
									Manager Configuration	
Alarming Hosts									Packet Analyzer Configuration	- 2
Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltratio	UDP Director Configuration	Anomaly
0	0	0	0	0	0	0	0	0	External Lookup Configuration	0
									Oser Management	
									Select Language	_

3. En los dispositivos enumerados, localice el dispositivo desde el que debe crear el paquete de diagnóstico y seleccione Acciones (icono de puntos suspensivos) > Ver estadísticas del dispositivo.

😴 Ce	entral Management	Appliance Manager	Update Manager	App Manager	Smart Licensing	Database				+	cisco SECURE
Inventor	ry .										
3 Appliances	found										
Q Filte	er Appliance Inventory Table										
Appliance	Status	∧ Host Name		∧ Type		~	IP Address	~	Actions		
Up				Flow Co	xliector			Edit Appliance Configuration]		
Up		-		Flow Se	Insor			View Appliance Statistics			
Up				Manage	ər			Support	🖊		
				8404	March 100000-110	CALIFORNIA CONTRACTOR		Reboot Appliance			
								Shut Down Appliance			
								Remove This Appliance			

4. Debe ser redirigido a la interfaz de usuario del administrador del dispositivo seleccionado.

5. Inicie sesión en la interfaz de usuario de administración del dispositivo con credenciales **de administrador**.

6. En el menú de la izquierda, vaya a **Soporte > Paquete de diagnóstico**.

ਓ Manager VE					esco SECURE						
Home	This appliance is managed by a Central Manager. Please go to <u>Central Management</u> to change these settings.										
Support	System										
 Backup/Restore Database Browse Files 	IP Address:				1						
 Packet Capture Update 	Host name:		Domain name:								
 Backup/Restore Configuration 	Total Memory:		Load Average:								
- Diagnostics Pack 😓	VM Server Memory:		VM Server CPU:								
■ Audit Log	Free Memory:		Uptime:								
Ø Operations	Version:		Platform:	ALC: NOTE: NOT: NOT: NOT: NOT: NOT: NOT							
🕜 Help 🗉	Build:		Serial No.:	And the second of the second							
G	>										

7. Una vez en la página Diagnostics Pack (Paquete de diagnóstico), debe seleccionar la encriptación **Public Key predeterminada** o proporcionar una clave compartida/frase de paso para utilizarla en el cifrado.

Nota: Si decide utilizar una clave/contraseña personalizada, debe proporcionar esa frase de paso en la descripción del archivo cuando cargue el paquete de diagnóstico en el Support Case Manager.

8. Seleccione Create Diagnostics Pack para generar el paquete de diagnóstico del dispositivo.

藯 Manager VE		diable SECURE
♣ Home ✔ Configuration □ ▲ Manage Users □ ✔ Support □	Diagnostics Pack Previous Diagnostics Pack diagnostic-SMC-	
 Audit Log Operations ☺ Logout 	diagnostic-SMC- diagnostic-SMC- Create New Diagnostics Pack	
P Help ©	Encryption Type: Oshared Passphrase Password:	
	Confirm Password:	
	Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved.	

9. Una vez finalizado, se le debe presentar un cuadro emergente que incluya el botón **Descargar** para descargar el paquete de diagnóstico.

🐼 Manager VE					esco SECURE
∯ Home ✗ Configuration ☺	Diagnostics Pa	ack			
🚨 Manage Users 🛛 🕀	Previous Diagn	ostics Pack			
Support E Audit Log	diagnostic-SMC diagnostic-SMC diagnostic-SMC				
Operations	Create New Dia	agnostics Pack			
🕞 Logout		C D L H = Marc			
🕜 Help 🐵	Encryption Type:	Shared Passphrase			
٥	Password:		Creating Diagnostics Pack ×		
	Confirm Password:		Diagnostics pack created.		
	Create Diagnostics Par	ck	Download Close		
	Patenteo	d, U.S. Patent Numbers 718536	290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. C	pyright 2022 Cisco®. All Rights Reserved.	

Método 2. Desde la interfaz de usuario del administrador de cada dispositivo

Para este método, debe tener acceso al dispositivo desde el que desea generar el paquete de diagnóstico, a través de Hypertext Transfer Protocol Secure (HTTPS).

Nota: Para acceder directamente a la **interfaz de usuario del administrador**, debe utilizar la dirección URL: <u>https://<Manager_IP_address>/smc/index.html</u>, de lo contrario se le redirige a la interfaz de usuario web del jefe.

Por ejemplo, para generar el paquete de diagnóstico de un Flow Collector con este método, debe seguir los siguientes pasos:

- 1. Desde un navegador web, navegue hasta https://<FC_IP_address>
- 2. Inicie sesión en la interfaz de usuario del administrador del dispositivo con las credenciales del administrador.

Network Analytics	
Usernamo: Password:	
Secure Network Analytics is a trademark of Oisco Systems, Inc. Patented, U.S. Patent Nos. 7185368, 7290283, 7475426, 7512980 and 7644151. © 2000-2022 Cisco Systems, Inc. All rights reserved.	

3. En el menú de la izquierda, vaya a **Support > Diagnostics Pack**.

0.4.0	Flow Collector	NetFlow VE				elsee SECURE							
14 }	Home Configuration	guration											
4	Manage Users 🗉	i Info! This page autor	i Infol This page automatically refreshes every minute - last refreshed at 19:05:29.										
۶	Support 🖊 🖯												
ŀ	Advanced Settings	System											
╞	Database Storage Statistics	IP Address:											
ŀ	Backup/Restore Database	Host name:	100000	Domain name:	and the second sec								
╞	Browse Files	Total Mamons		Lord Augrope									
ŀ	Packet Capture	VM Conner Memory		Luou Average.									
	Update	vivi Server Memory,		VM Server CPO.									
ŀ	Backup/Restore Configuration	Free Memory:		Uptime:	the second se								
r.	Diagnostics Pack												
-	Audit Lan	Version:	1000	Platform:									
	. Audit Log	Build:	and the second second	Serial No.:	the second se								
0	Operations 🗉												
۲	Logout	Engine Status											
6	Help 🗉	Engine Status											

4. Una vez en la página Diagnostics Pack (Paquete de diagnóstico), debe seleccionar la encriptación **Public Key predeterminada** o proporcionar una clave compartida/frase de paso para utilizarla en el cifrado.

Nota: Si decide utilizar una clave o frase de paso personalizada, debe proporcionar esa frase de paso en la descripción del archivo cuando cargue el paquete de diagnóstico en el Support Case Manager.

5. Seleccione Create Diagnostics Pack para generar el paquete de diagnóstico del dispositivo.

Flow Colle	ctor	NetFlow VE						
♣ Home ✓ Configuration	e	Diagnostics Pa	ack					
🚨 Manage Users	œ	Previous Diagno	ostics Pack					
 ✓ Support ≕ Audit Log ✿^o₆ Operations ☞ Logout 	Ð	diagnostic-FlowCollec public.tgz.gpg 189.444 diagnostic-FlowCollec public.tgz.gpg 171.827 Create New Dia	tor_NetFlow-FCNFVE M tor_NetFlow-FCNFVE M gnostics Pack					
Ø Help	B O	Encryption Type:	Public Key O Shared Passphrase					
		Password:						
		Confirm Password:						
		Create Diagnostics Paci						
		Patented	U.S. Patent Numbers 71853	58, 7290283, 7475426, 7512980,	and 7644151. Other U.S. a	nd foreign patents pending. Cop	oyright 2022 Cisco®. All Rights Reserved.	

6. Una vez finalizado, se le debe presentar un cuadro emergente que incluya el botón **Descargar** para descargar el paquete de diagnóstico.

Flow Collector	n NetFlow VE	diade SECURE
♣ Home ✔ Configuration □ ▲ Manage Users □ ✔ Support □ Ξ Audit Log □ Φ [®] ₀ Operations □ ଢ Logout € Help □	Diagnostics Pack Previous Diagnostics Pack diagnostic-FlowCollector_NetFlow-FCNFVI public.tgz.gpg 178.44M diagnostic-FlowCollector_NetFlow-FCNFVI public.tgz.gpg 171.82M Create New Diagnostics Pack Encryption Type: Public Key Shared Passphrase	
	Password: Creating Diagnostics Pack Confirm Password: Diagnostics pack created. Create Diagnostics Pack Diagnostics pack created. Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved.	

Método 3. Desde la interfaz de línea de comandos (CLI) de cada dispositivo

Hay ocasiones en las que no es posible generar el paquete de diagnóstico de un dispositivo con el uso de los métodos descritos anteriormente, sin embargo, se puede generar directamente desde la CLI del dispositivo. Los pasos para completar esta tarea son:

1. Conéctese al dispositivo SNA deseado mediante el protocolo Secure Shell (SSH) o directamente a través del acceso a la consola.

Nota: En caso de que necesite recopilar el paquete de diagnóstico de un dispositivo de hardware sin acceso SSH, también se puede utilizar la consola de máquina virtual (KVM) basada en el núcleo de la interfaz del controlador de gestión integrada (CIMC) de Cisco.

- 2. Inicie sesión con las credenciales raíz.
- 3. Ingrese uno de los siguientes comandos (esto depende de la versión de SNA que está en uso):

SNA versión 7.1.x a 7.3.x

Ingrese el comando doDiagPack

SNA versión 7.4.x

Ingrese el comando diagnostics start

- 4. Espere a que se complete la tarea.
- Una vez finalizada la tarea, el archivo de paquete de diagnóstico se almacena en el directorio /lancope/var/admin/diagnostics/ con un esquema de nombre de "diagnostic-<Device_type>-<Device_ID>.<YYYMMDD>.<HHMM>-*.tgz.gpg"



6. Copie el archivo generado del dispositivo en su equipo local o en un servidor de archivos con protocolo de copia segura (SCP) o con un cliente de protocolo de transferencia de archivos (SFTP) SSH como WinSCP. El paquete de diagnóstico se encuentra en el /lancope/var/admin/diagnostics/ directorio.

Nota: Cabe mencionar que SNA versión 7.4.0 introdujo una nueva función que permite que el paquete de diagnóstico se genere desde el menú SystemConfig (inicio de sesión de CLI con credenciales **root** > Introducir **SystemConfig** > Navegar a **Recuperación** > Paquete de diagnóstico).

Para obtener más información sobre este método, revise la <u>Guía de Configuración de</u> <u>Secure Network Analytics System 7.4.x</u>.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Hay ocasiones en las que la creación del paquete de diagnóstico falla. El síntoma más común es cuando recibe un error que dice "Se produjo un error al crear el paquete de diagnóstico. No hay archivos disponibles" después de hacer clic en el botón **Create Diagnostics Pack**.

Creating Diagnostics Pack ×
There was an error creating the diagnostics pack. No files are available.
Close

Para corregir este comportamiento, continúe de la siguiente manera:

- 1. Inicie sesión en el dispositivo que tiene este comportamiento con las credenciales **raíz** a través de SSH.
- 2. Ejecute el comando **Is -I /lancope/var/database/dbs/hsqldb/admin/** para verificar el contenido del directorio.
- 3. Asegúrese de que el subdirectorio **de copia de seguridad** existe y que el propietario del usuario/grupo es **tomcat**.

fcnf-cds:~#	l	.s –l /	/lancope	e/var/	/data	abas	se/dbs/	/hsqldb/admin/
total 20								
-rw-rr 0	1	tomcat	tomcat	16	Apr	28	00:38	admin.lck
-rw-rr 0	1	tomcat	tomcat	0	Apr	27	17:20	admin.log
-rw-rr 3	1	tomcat	tomcat	84	Apr	27	17:17	admin.properties
-rw-rr 3	1	tomcat	tomcat	2995	Apr	27	17:17	admin.script
drwxr-xr-x 3	2	tomcat	tomcat	4096	Apr	27	17:20	admin.tmp
drwxr−xr−x 3	2	tomcat	tomcat	4096	Jun	7	2021	backup

Si el subdirectorio **de respaldo** no existe en la **/lancope/var/database/dbs/hsqldb/admin/** path, se debe crear y asignar la propiedad correcta. Para esto, ejecute estos comandos:

- 1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
- 2. chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup
- 4. Ejecute el comando ls -l /lancope/var/admin/ para verificar el contenido del directorio.

5. Asegúrese de que existan **copias de seguridad** y **diagnósticos** subdirectorios y de que el usuario/grupo propietario sea **root**.

fcnf-cds:~4	ŧ.	11 /հ	ancope/va	ar/adm:	in/			
drwxrwxr-x	2	root	root	4096	Apr	27	06:25	backups
drwxr-xr-x	2	root	root	4096	Apr	7	21:39	cds
-rw-rr	1	root	root	0	Apr	6	22:10	clustered database
drwxrwxr-x	2	root	root	4096	Sep	7	2021	diagnostics
-rw-rr	1	root	root	40	Apr	27	17:18	hwserial
-rw-rr	1	root	root	8	Apr	27	17:18	meminfo
-rw-rr	1	root	root	69	Apr	27	17:18	model
-rw-r	1	root	root	23	Apr	27	17:18	platform
drwxr-xr-x	3	root	root	4096	Sep	15	2021	plugins
-rw-rw-rw-	1	root	root	2	Apr	27	18:13	previous_engine_startup_mode
-rw-rr	1	root	root	47	Apr	27	17:18	serial
drwxr-xr-x	2	root	root	4096	Apr	7	21:22	ssh
drwxr-xr-x	2	root	root	4096	Apr	8	02:51	system.d
-rw-rw	1	root	swadmin	12756	Apr	8	02:56	system.xml
drwxrwxrwx	2	root	root	4096	Apr	28	00:25	tmp
drwxr-xr-x	2	root	root	4096	Sep	7	2021	update
drwxrwxr-x	4	root	tomcat	4096	Apr	8	02:49	upgrade
-rw-rr	1	root	root	36	Apr	27	17:18	uuid
foof-odcust	μ.							

Si uno o ninguno de los subdirectorios mencionados no existe en la ruta **/lancope/var/admin/**, se deben crear y asignar la propiedad correcta. Para esto, ejecute estos comandos:

- 1. mkdir /lancope/var/admin/backups
- 2. mkdir /lancope/var/admin/diagnostics

Una vez que se haya verificado, intente generar el paquete de diagnóstico del dispositivo SNA de nuevo.

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el Centro de asistencia técnica de Cisco (TAC). Se requiere un contrato de soporte válido: <u>Contactos de soporte a nivel</u> <u>mundial de Cisco.</u>
- Soporte Técnico y Documentación Cisco Systems