# 生成安全網路分析裝置的診斷包

### 目錄

<u>簡介</u> <u>程式</u> <u>方法1.從管理器的Web使用者介面(UI)</u> <u>方法2.從每台裝置的管理UI</u> <u>方法3.從每個裝置的命令列介面(CLI)</u> <u>疑難排解</u> <u>相關資訊</u>

## 簡介

本檔案介紹可用於收集安全網路分析(SNA)裝置診斷包的不同程式。

# 程式

0

有三種主要方法可為SNA裝置生成診斷包。建議的方法是**方法1。從Manager Web使用者介面** (UI),但是,如果Manager的Web使用者介面不可用,則可以使用另外兩種方法。

**附註**:如果Manager的Web UI不可用,並且您需要從Manager生成診斷包,請參閱**方法3。從** 每個裝置的命令列介面(CLI)。

### 方法1.從管理器的Web使用者介面(UI)

- 1. 登入到Manager的Web UI。
- 2. 導航到全域性設定>中央管理。

ਓ Network A	nalytics		Dashboards *	Monitor • Analyz	re • Jobs • Conf	igure * Deploy *			a ք 🌣	+ cisco 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
U	Ū	0	Ŭ	Ŭ	U	U	U	0	User Management	U.
									SecureX Configuration	
									Select Language	

3.從列出的裝置找到需要從中建立診斷包的裝置,然後選擇操作(省略號圖示)>檢視裝置統計資訊

÷	Central Management	Appliance Manager	Update Manager	App Manager	Smart Licensing	Database				*	cisco SECURE
In	ventory										
3 Ap	Q Filter Appliance Inventory Table										
	Appliance Status	Host Name		Type		^	IP Address	^	Actions		
	qt			Flow Co	llector			Edit Appliance Configuration	]		
	lp	-		Flow Se	nsor	e waarde waa		View Appliance Statistics			
	da A			Manage	allegen agricolatie <sup>1</sup> op	al anticipation		Support Reboot Appliance Shut Down Appliance	<b>/</b>		
								Remove This Appliance			

4.必須重定向到所選裝置的管理UI。

5.使用admin憑據登入到裝置管理UI。

6.從左側選單導航到**支援>診斷包**。

藯 Manager VE					cisco SECURE
<ul><li>A Home</li><li>✓ Configuration</li></ul>	i This appliance is managed b	oy a Central Manager. Please go to <u>Central Manag</u>	ement to change these settings.		
🛔 Manage Users 🛛 🕫	i Info! This page automatical	y refreshes every minute - last refreshed at 18:56	:54.		
🗲 Support 📕 🛛 🛛					
<ul> <li>Backup/Restore</li> <li>Database</li> </ul>	System				
<ul> <li>Browse Files</li> </ul>	IP Address:	10000			
<ul> <li>Packet Capture</li> </ul>	Host name:		Domain name:		
- Update					
<ul> <li>Backup/Restore Configuration</li> </ul>	Total Memory:		Load Average:		
- Diagnostics Pack	VM Server Memory:		VM Server CPU:		
■ Audit Log	Free Memory:	10	Uptime:		
Q <sup>0</sup> <sub>0</sub> Operations □					
( Logout	Version:		Platform:		
Help B	Build:		Serial No.:	And the second of the second	
G					

7.進入「診斷包」頁後,您需要選擇預設的**公鑰**加密,或提供用於加密的共用金鑰/口令。

**附註**:如果您選擇使用自定義金鑰/密碼,則在將診斷包上傳到支援案例管理器時,必須在檔 案說明中提供該密碼。

8.選擇建立診斷包以生成裝置的診斷包。

藯 Manager VI	E	ensee SECU
<ul> <li>Home</li> <li>Configuration</li> <li>Manage Users</li> </ul>	<ul> <li>Diagnostics Pack</li> <li>Previous Diagnostics Pack</li> </ul>	
Support Audit Log	diagnostic-SMC- diagnostic-SMC- diagnostic-SMC-	
<ul> <li>✿ Operations</li> <li>⊕ Logout</li> <li>⊕ Male</li> </ul>	Create New Diagnostics Pack  Public Key  Public Key	
<b>G</b> Help	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.完成後,您必須看到一個彈出框,其中包含Download按鈕以下載診斷包。

藯 Manager VE							diade SECUR
∯ Home	•	Diagnostics Pa	ack				
🚨 Manage Users	e	Previous Diagno	ostics Pack				
		diagnostic-SMC diagnostic-SMC diagnostic-SMC					
<b>Q</b> <sup>o</sup> Operations	•	Create New Dia	gnostics Pack				
Help	Θ	Encryption Type:	<ul> <li>Public Key</li> <li>Shared Passphrase</li> </ul>				
	9	Password:			Creating Disgnastics Dask		
	l	Confirm Password:			Diagnostics pack created.		
	L	Create Diagnostics Paci	3		Download Close		
	I	Patented	, U.S. Patent Numbers 71853	68, 7290283, 7475426, 7	7512980, and 7644151. Other U.S. and foreign	patents pending. Copyright 2022 Cisco®. All Rights Reserved.	
	I						

### 方法2.從每台裝置的管理UI

對於此方法,您必須通過安全超文本傳輸協定(HTTPS)訪問要從中生成診斷包的裝置。

附註:要直接訪問管理器的管理UI,您必須使用

URL:<u>https://<Manager\_IP\_address>/smc/index.html</u>,否則您將重定向到Manager的Web UI。

例如,要使用此方法生成流量收集器的診斷包,必須執行以下步驟:

- 1. 從Web瀏覽器導航至<u>https://<FC\_IP\_address></u>
- 2. 使用管理員憑據登入到裝置管理員UI。

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

#### 3.從左側選單導航至 **支援>診斷包**.

Flow Collector	r NetFlow VE				CHOR SECURE
∯ Home ✔ Configuration ©	i This appliance is manage	d by a Central Manager. Please go to <u>Central Ma</u>	nagement to change these settings.		
👗 Manage Users 🛛 🕀	i Info! This page automatic	ally refreshes every minute - last refreshed at 19	9:05:29.		
Support - Advanced Settings	System				
<ul> <li>Database Storage Statistics</li> </ul>	IP Address:				
<ul> <li>Backup/Restore</li> <li>Database</li> </ul>	Host name:	10000000	Domain name:		
<ul> <li>Browse Files</li> <li>Packet Capture</li> </ul>	Total Memory:		Load Average:		
- Update	VM Server Memory:	1000 C 1000	VM Server CPU:		
<ul> <li>Backup/Restore Configuration</li> </ul>	Free Memory:		Uptime:	Contraction of the Contraction o	
– Diagnostics Pack 😓	Martin				
E Audit Log	Pullet		Platform:	and the second second second second	
<b>Q</b> <sup>0</sup> <sub>0</sub> Operations ⊕	0010.		Serial NO.:		
🕒 Logout	Engine Status				
🕑 Help 🗉	Engine Status				

4.進入「診斷包」頁後,您需要選擇預設的**公鑰**加密,或提供用於加密的共用金鑰/口令。

**附註**:如果您選擇使用自訂金鑰/密碼短語,那麼在將診斷包上傳到支援個案管理器時,必須 在檔案說明中提供該密碼短語。

5.選擇建立診斷包以生成裝置的診斷包。

Flow Colle	ctor	NetFlow VE					
Home Configuration	e	Diagnostics Pa	ack				
🚨 Manage Users	œ	Previous Diagno	ostics Pack				
<ul> <li>✓ Support</li> <li>≡ Audit Log</li> <li>Q<sup>6</sup> Operations</li> <li>G Logout</li> </ul>	Ð	diagnostic-FlowCollec public.tgz.gpg 189.44/ diagnostic-FlowCollec public.tgz.gpg 171.82/ Create New Diag	tor_NetFlow-FCNFVE M tor_NetFlow-FCNFVE M gnostics Pack				
Help	е О	Encryption Type:	Public Key Shared Passphrase				
		Password:					
		Confirm Password:					
		Create Diagnostics Paci	ĸ				
		Patented,	I, U.S. Patent Numbers 7185	368, 7290283, 7475426, 7512980, ar	nd 7644151. Other U.S. and	oreign patents pending. Copyright 2022 Cisc	co®. All Rights Reserved.

#### 6.完成後,您必須看到一個彈出框,其中包含Download按鈕以下載診斷包。

Flow Collector	r NetFlow VE	teste SECURE
♣ Home         ✔ Configuration         ▲ Manage Users         ♥ Support         ■ Audit Log         Ø Operations         Ø Logout         Ø Help	Diagnostics Pack Previous Diagnostics Pack diagnostic-FlowCollector_NetFlow-FCNFV1 public.tgr.gpp 189.44M diagnostic-FlowCollector_NetFlow-FCNFV1 public.tgr.gpp 171.82M Create New Diagnostics Pack Encryption Type:  Public Key Shared Passbrase	
	Password: Confirm Password: Confirm Password: Create Diagnostics Pack Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644	agnostics Pack * round Common Common Commo Common Common Comm

### 方法3.從每個裝置的命令列介面(CLI)

有時無法使用上述方法生成裝置的診斷包,但可以直接從裝置的CLI生成。完成此任務的步驟如下:

1. 通過安全外殼協定(SSH)或直接通過控制檯訪問連線到所需的SNA裝置。

**附註**:如果您需要從無SSH訪問的硬體裝置收集診斷包,也可以使用思科整合管理控制器 (CIMC)介面中的核心式虛擬機器(KVM)控制檯。

- 2. 使用根憑**據登**錄。
- 输入以下命令之一(這取決於正在使用的SNA版本):
   SNA 7.1.x版到7.3.x版

輸入命令doDiagPack

SNA 7.4.x版

輸入命令diagnostics start

4. 等待任務完成。

5. 任務完成後,診斷包檔案將儲存在/lancope/var/admin/diagnostics/目錄中,其名稱方案為「



6. 使用安全複製協定(SCP)或SSH檔案傳輸協定(SFTP)客戶端(如WinSCP),將生成的檔案從 裝置複製到本地電腦或檔案伺服器。診斷包位於/lancope/var/admin/diagnostics/目錄。

**註**意:值得一提的是,SNA 7.4.0版引入了一項新功能,允許從SystemConfig選單生成診斷包 (使用**root** credentials > Enter **SystemConfig > Navigate to Recovery > Diagnostics Pack的** CLI登入)。

有關此方法的詳細資訊,請參閱<u>安全網路分析系統配置指南7.4.x</u>。

### 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

有時建立診斷包會失敗。最常見的症狀是收到錯誤資訊「There was an error creating the diagnostics pack(建立診斷包時出錯)」。按一下**Create Diagnostics Pack** 按鈕後,沒有檔案可用。



要更正此行為,請按照以下步驟操作:

- 1. 通過SSH使用root憑據登入到具有此行為的裝置。
- 2. 運行Is -I /lancope/var/database/dbs/hsqldb/admin/命令以驗證目錄的內容。
- 3. 確保backup 子目錄存在,且其使用者/組所有者為tomcat。

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

如果/lancope/var/database/dbs/hsqldb/admin/路徑中不存在backup子目錄,則必須建立該子目錄並 分配正確的所有權。為此,請運行以下命令:

- 1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
- 2. chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup
- 4.運行Is -I /lancope/var/admin/命令以驗證目錄的內容。

5.確保backups和diagnostics子目錄存在,並且其使用者/組所有者為root。

	_							
fcnf-cds:~	¢,	11 /14	ancope/va	ar/adm	in/			
total 80								
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-rr	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_mo
-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-odered	#							

如果/lancope/var/admin/path中不存在上述其中一個子目錄,則必須建立這些子目錄並分配正確的 所有權。為此,請運行以下命令:

1. mkdir /lancope/var/admin/backups

2. mkdir /lancope/var/admin/diagnostics

驗證此操作後,請嘗試再次生成SNA裝置的診斷包。

# 相關資訊

- 如需其他協助,請聯絡思科技術協助中心(TAC)。需要有效的支援合約: <u>思科全球支援聯絡人.</u>
- <u>技術支援與文件 Cisco Systems</u>