Generate Diagnostics Pack for Secure Network Analytics Appliances

Contents

Introduction Procedure Method 1. From the Manager's Web User Interface (UI) Method 2. From Each Appliance's Admin UI Method 3. From Each Appliance's Command Line Interface (CLI) **Troubleshoot Related Information**

Introduction

This document describes the different procedures available to collect a Diagnostics Pack for Secure Network Analytics (SNA) Appliances.

Procedure

There are three main methods to generate the Diagnostics Pack for the SNA appliances. The suggested method is Method 1. From the Manager Web User Interface (UI), however the other two methods are an option in case that the Manager's Web UI is not available.

Note: If the Manager's Web UI is unavailable and you need to generate a Diagnostics Pack from the Manager, please refer to Method 3. From Each Appliance's Command Line Interface (CLI).

Method 1. From the Manager's Web User Interface (UI)

2. Navigate to **Global Settings > Central Management**. Network Analytics Dashboards * Monitor * Analyze * Jobs * Configure * + distant SECURE Security Insight Dashboard | Inside Hosts Alarming Hosts lyzer Configuratio Concern Index C&C Target Index Data Hoarding

3. From the listed appliances locate the appliance from which you need to create the Diagnostics Pack and select Actions (Ellipsis icon) > View Appliance Statistics.

- 1. Log in to the Manager's web UI.

÷	Central Management	Appliance Manager	Update Manager	App Manager	Smart Licensing	Database				1	cisco SECURE
In 3 Ap	ventory										
	Q, Filter Appliance Inventory Table										
A	ppliance Status	Host Name		Type		^	IP Address	^	Actions		
U	P			Flow Co	llector			Edit Appliance Configuration]		
U	p	-		Flow Se	nsor	a se total de la cara		View Appliance Statistics			
U	p			Manage		all addression of		Support Reboot Appliance Shut Down Appliance	/		
								Remove This Appliance			

- 4. You must be redirected to the Admin UI of the selected appliance.
- 5. Log in to the appliance Admin UI with **admin** credentials.
- 6. From the menu on the left, navigate to **Support > Diagnostics Pack**.

藯 Manager VE					cisco SECURE
Home Configuration Configurat	This appliance is managed by i InfoI This page automatically System				
Database - Browse Files - Packet Capture - Update	IP Address: Host name:		Domain name:		
Backup/Restore Configuration Diagnostics Pack	Total Memory: VM Server Memory:	-	Load Average: VM Server CPU:	1 1 1 1	
	Free Memory:	-	Uptime:		
C Logout	Version: Build:		Platform: Serial No.:	And the second of the second second	
G					

7. Once in the Diagnostics Pack page, you need to either select the default **Public Key** encryption or provide a shared key/passphrase to use for encryption.

Note: If you choose to use a custom key/password, then you must provide that passphrase in the file description when you upload the Diagnostics pack to the Support Case Manager.

8. Select **Create Diagnostics Pack** to generate the diagnostics pack of the appliance.

藯 Manager VE		ensee SECURE
 ✤ Home ➢ Configuration ⓐ Manage Users ☞ Support ⓐ Audit Loo 	Diagnostics Pack Previous Diagnostics Pack diagnostic-SMC- diagnostic-SMC-	
Audit Log C ₀ Operations E Logout Help C	Create New Diagnostics Pack Encryption Type: Create New Diagnostics Pack	
	Password: Confirm Password: Create Diagnostics Pack 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. Once finished, you must be presented with a pop-up box which includes the **Download** button to download the Diagnostics Pack.

🕤 Manager VE							cited SECURE
∯ Home ⊮ Configuration ©	Diagnostics P	ack					
🚢 Manage Users 🛛 🕀	Previous Diagn	ostics Pack					
✓ Support	diagnostic-SMC diagnostic-SMC diagnostic-SMC						
Operations	Create New Dia	agnostics Pack					
🕞 Logout		Public Key					
🕑 Help 🐵	Encryption Type:	O Shared Passphrase					
0	Password:		Creating	Diagnostics Pack ×			
	Confirm Password:		Diagnostics p	ack created.			
	Create Diagnostics Pa	ck		Download Close			
	Patenter	d, U.S. Patent Numbers 71853	3, 7290283, 7475426, 7512980, and 76	44151. Other U.S. and foreign p	atents pending. Copyright 2022 Cisc	o®, All Rights Reserved.	

Method 2. From Each Appliance's Admin UI

For this method you must access to the appliance from which you want to generate the Diagnostics Pack, via Hypertext Transfer Protocol Secure (HTTPS).

Note: To access directly to the Manager's **Admin UI** you must use the URL: <u>https://<Manager_IP_address>/smc/index.html</u>, otherwise you are redirected to the Manager's Web UI.

For example, in order to generate the Diagnostics Pack of a Flow Collector with this method you must follow the next steps:

- 1. From a web browser, navigate to https://<FC IP_address>
- 2. Log in to the appliance Admin UI with admin credentials.

Network Analytics	
Username: Password:	
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. From the menu on the left, navigate to **Support > Diagnostics Pack**.

Flow Callector NetFlow VE													
44 }	Home	i This appliance is managed by a Central Manager. Please go to <u>Central Management</u> to change these settings.											
2	Manage Users 🛛 🕾		i Info! This page automatically re										
1	Support 🖊 🖯 🖯												
	 Advanced Settings 	S	System										
	 Database Storage Statistics 		IP Address:										
	 Backup/Restore Database 		Host name:	1000 C	Domain name:	The second secon							
ŀ	- Browse Files		Total Memony	-	Load Average:								
	 Packet Capture 		VM Senier Memory		VM Sequer CPLI:								
İ	- Update		vin ourver menory.		VIII ORIVER OF C.								
	 Backup/Restore Configuration 		Free Memory:		Uptime:								
r	- Diagnostics Pack												
	Audit Lon		Version:		Platform:								
			Build:	and the second sec	Serial No.:	the second se							
~	Operations 🗉												
•	Logout	F	noine Status										
6)Help 🗉	-	Engline Status										

4. Once in the Diagnostics Pack page, you need to either select the default **Public Key** encryption or provide a shared key/passphrase to use for encryption.

Note: If you choose to use a custom key/passphrase, then you must provide that passphrase in the file description when you upload the Diagnostics pack to the Support Case Manager.

5. Select **Create Diagnostics Pack** to generate the diagnostics pack of the appliance.

Flow Colle	ector	NetFlow VE										
셝 Home	ē	Diagnostics Pa	ack									
 Manage Users 		Previous Diagno	Previous Diagnostics Pack									
 ✓ Support ⇒ Audit Log ♥ Operations ♥ Logout 	8	diagnostic-FlowCollac public.tgz.gpg 189.44 diagnostic-FlowCollac public.tgz.gpg 171.82 Create New Dia	tor_NetFlow-FCNFVE									
0 Help		Encryption Type:	Public Key O Shared Passphrase									
		Password:										
		Confirm Password:										
		Create Diagnostics Pac	ĸ									
		Patented	I, U.S. Patent Numbers 7185	368, 7290283, 7475426, 7512980,	and 7644151. Other U.S. a	ind foreign patents pending. Copyri	ight 2022 Cisco®. All Rights Reserved.					

6. Once finished, you must be presented with a pop-up box which includes the **Download** button to download the Diagnostics Pack.

Flow Collecto	or NetFlow VE	cisco SECURE
♣ Home ✔ Configuration □ ▲ Manage Users □ ✔ Support □ ➡ Audit Log O ⁶ ₀ Operations □ Image: Content of the second sec	Diagnostics Pack Previous Diagnostics Pack diagnostic-FlowCollector_NetFlow-FCNFVI public.tgz.gpg 188.44M diagnostic-FlowCollector_NetFlow-FCNFVI public.tgz.gpg 171.82M Create New Diagnostics Pack Encryption Type: Public Key Shared Passphrase	
	Password: X Confirm Password: X Diagnostics pack created. Diagnostics pack created. Diagnostics Pack X Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved.	

Method 3. From Each Appliance's Command Line Interface (CLI)

There are some times when it is not possible to generate the Diagnostics Pack of an appliance with the use of the previously described methods, however it can be generated directly from the appliance's CLI. The steps to complete this task are:

1. Connect to the desired SNA appliance via Secure Shell Protocol (SSH) or directly via console access.

Note: In case that you need to collect the diagnostics pack from a hardware appliance with no SSH access, the Kernel-based Virtual Machine (KVM) console from the Cisco Integrated Management Controller (CIMC) interface can be used as well.

- 2. Log in with **root** credentials.
- 3. Enter one of the next commands (this depends on the version of SNA which is in use): **SNA version 7.1.x to 7.3.x**

Enter the command doDiagPack

SNA version 7.4.x

Enter the command diagnostics start

- 4. Wait for the task to be completed.
- 5. Once the task has been completed, the Diagnostics pack file gets stored in the /lancope/var/admin/diagnostics/ directory with a name scheme of "diagnostic-<Device_type>-<Device_ID>.<YYYMMDD>.<HHMM>-*.tgz.gpg"



6. Copy the generated file from the appliance to your local computer or to a file server with Secure Copy Protocol (SCP) or with a SSH File Transfer Protocol (SFTP) client like WinSCP. The diagnostics pack is located in the */lancope/var/admin/diagnostics/* directory.

Note: It is worth to mention that SNA version 7.4.0 introduced a new feature that allows the Diagnostics Pack to be generated from the SystemConfig menu (CLI log in with **root** credentials > Enter **SystemConfig** > Navigate to **Recovery** > **Diagnostics Pack**).

For more information about this method, review the <u>Secure Network Analytics System</u> <u>Configuration Guide 7.4.x</u>.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

There are some times when the creation of the Diagnostics Pack fails. The most common symptom is when you receive an error that reads "There was an error creating the diagnostics pack. No files are available" after the **Create Diagnostics Pack** button is clicked.

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

To correct this behavior, proceed as follows:

- 1. Log in to the appliance that has this behavior with root credentials via SSH.
- 2. Run the Is -I /lancope/var/database/dbs/hsqldb/admin/ command to verify the content of the directory.
- 3. Ensure that the **backup** subdirectory exists and that its user/group owner is **tomcat**.

fcnf-cds:~#	1	ls –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 0	1	tomcat	tomcat	84	Apr	27	17:17	admin.properties
-rw-rr 0	1	tomcat	tomcat	2995	Apr	27	17:17	admin.script
drwxr–xr–x 2	2	tomcat	tomcat	4096	Apr	27	17:20	admin.tmp
drwxr-xr-x 2	2	tomcat	tomcat	4096	Jun	7	2021	backup
2 2 1 1	_		1.5			_		

If the **backup** subdirectory does not exist in the **/lancope/var/database/dbs/hsqldb/admin/** path, it must be created and the correct ownership must be assigned. For this, run these commands:

- 1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
- 2. chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup
- 4. Run the Is -I /lancope/var/admin/ command to verify the content of the directory.

5. Ensure that the **backups** and **diagnostics** subdirectories exist and that their user/group owner is **root**.

fcnf-cds:~4	r I	ll /la	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_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-odered	μ.							

If one or none of the mentioned subdirectories do not exist in the **/lancope/var/admin/** path, they must be created and the correct ownership must be assigned. For this, run these commands:

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

Once this has been verified, try to generate the Diagnostics Pack of the SNA appliance again.

Related Information

 For additional assistance, please contact Cisco Technical Assistance Center (TAC). A valid support contract is required: <u>Cisco Worldwide Support Contacts.</u> <u>Technical Support & Documentation - Cisco Systems</u>