Generate diagnostiek pack voor Secure Network Analytics-applicaties

Inhoud

Inleiding Procedure Methode 1. Van de gebruikersinterface van het Web van de Manager (UI) Methode 2. Van Admin UI van elk apparaat Methode 3. Van de interface van elke applicatie (CLI) Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft de verschillende procedures die beschikbaar zijn om een diagnostisch pack voor Secure Network Analytics (SNA)-applicaties te verzamelen.

Procedure

Er zijn drie belangrijke methoden om het diagnostische pakket voor de SNA-apparaten te produceren. De voorgestelde methode is **Methode 1. Van de Gebruiker Interface van het Web van de Manager (UI)**, echter zijn de andere twee methodes een optie voor het geval dat het Web UI van de Manager niet beschikbaar is.

Opmerking: Als het Web UI van de Manager niet beschikbaar is en u moet een Diagnostics Pack van de Manager genereren, verwijs dan naar **Methode 3. Van de Interface van de Lijn van het Applicatie (CLI)**.

Methode 1. Van de gebruikersinterface van het Web van de Manager (UI)

- 1. Meld u aan bij de Manager web UI.
- 2. Navigeer naar Global Settings > Central Management.

ਓ Network A	nalytics		Dashboards •	Monitor • Analy:	ze • Jobs • Con	igure * Deploy *			۵ ք ې	+ cisco SECURE
									Global Settings	
Security Insight D	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	U	U	U	U	U	0	U	0	User Management	0
									SecureX Configuration	
									Select Language	

3. Pak het apparaat uit op de lijst van apparatuur waar u het diagnostische pack voor wilt maken en selecteer **Handelingen (pictogram Ellips) > Toestuisstatistieken bekijken**.

÷	Ö Central Management	Appliance Manager	Update Manager	App Manager	Smart Licensing	Database				Ŧ	cisco SECURE
In	ventory										
3 App	liances found										
	Q Filter Appliance Inventory Table										
A	ppliance Status	Host Name		Type Type		^	IP Address	^	Actions		
U	p			Flow Co	lector			Edit Appliance Configuration			
U	p	-		Flow Se	insor			View Appliance Statistics			
U	p			Manage	-	-		Support Reboot Appliance	📈		
								Shut Down Appliance			
								Remove This Appliance			

- 4. U moet worden omgeleid naar de Admin UI van het geselecteerde apparaat.
- 5. Meld u aan bij de ABBYY FineReader-applicatie met Admin-referenties.
- 6. Klik in het menu links op **Support > Diagnostiek Pack**.

A.	🖸 Manager VE					cisco SECURE						
** ~ & ~	Home Configuration © Manage Users ©	 i This appliance is managed i i Info! This page automatical 	This appliance is managed by a Central Manager. Please go to <u>Central Management</u> to change these settings. Infol This page automatically refreshes every minute - last refreshed at 18:56:54.									
ŀ	Backup/Restore Database	System										
-		IP Address:	100000									
-		Host name:		Domain name:								
-												
ŀ	Backup/Restore Configuration	Total Memory:		Load Average:								
F	Diagnostics Pack 🖕	VM Server Memory:		VM Server CPU:								
=	Audit Log	Free Memory:	10	Uptime:								
¢0												
		Version:		Platform:								
0	Help B	Build:		Serial No.:	And the second of the second							
	U U											

7. Eenmaal in de pagina Diagnostics Pack moet u de standaard **Public Key**-encryptie selecteren of een gedeelde sleutel/wachtwoord opgeven voor codering.

Opmerking: Als u ervoor kiest een aangepaste sleutel/wachtwoord te gebruiken, moet u dat wachtwoord in de bestandsindeling opgeven wanneer u het pakket diagnostiek naar de Support Case Manager uploaden.

8. Selecteer Diagnostiek Pack maken om het diagnostische pakket van het apparaat te genereren.

藯 Manager \	VE								enco S
🖀 Home	œ	Diagnostics Pa	ack						
🛔 Manage Users	⊕	Previous Diagno	ostics Pack						
Support Audit Log	۲	diagnostic-SMC- diagnostic-SMC- diagnostic-SMC-							
Operations	₽	Create New Dia	gnostics Pack						
C+ Logout	۲	Encryption Type:	 Public Key Shared Passphrase 						
	G	Password:							
		Confirm Password:							
		Create Diagnostics Paci	×						
		Patented,	, U.S. Patent Numbers 7185	68, 7290283, 7475426, 7	512980, and 7644151. Oth	er U.S. and foreign patents pe	nding. Copyright 2022 Cisco®, All Rights	Reserved.	

9. Zodra deze klaar is, moet u een pop-upvakje ontvangen met de knop Downloaden om het diagnostische pakket te downloaden.

💭 Manager VE				cisco SECURE
🖀 Home	Diagnostics P	ack		
👗 Manage Users 🛛 🖗	Previous Diagn	ostics Pack		
Support 6 E Audit Log	diagnostic-SMC diagnostic-SMC diagnostic-SMC			
Operations 6	Create New Dia	agnostics Pack		
🕒 Logout		Dublic Key		
🚱 Help 🛛	Encryption Type:	O Shared Passphrase		
C	Password:		Creating Diagnostics Pack	
	Confirm Password:		Diagnostics pack created.	
	Create Diagnostics Pa	ck	Download Close	
	Patenter	d, U.S. Patent Numbers 718536	18, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved.	

Methode 2. Van Admin UI van elk apparaat

Bij deze methode moet u toegang hebben tot het apparaat waarmee u het diagnostische pack wilt genereren, via Hypertext Transfer Protocol Secure (HTTPS).

Opmerking: U moet de URL gebruiken om rechtstreeks toegang te hebben tot de **Admin UI** van de Manager: <u><Manager_IP_adres>/smc/index.html</u>, anders wordt u terugverwezen naar de Web UI van de Manager.

Om bijvoorbeeld het Diagnostics Pack van een Flow Collector met deze methode te genereren, moet u de volgende stappen volgen:

- 1. Vanuit een webbrowser, navigeer naar https://<FC_IP_Address>
- 2. Log in op het apparaat Admin UI met admin-referenties.

Image: Additional and the second s	
Secure Network Analytics is a trademark of Cisco Systems, Inc. Patented, U.S. Patent Nos. 7185368, 7290283, 7475426, 7512990 and 7644151. © 2000-2022 Cisco Systems, Inc. All rights reserved.	

3. Klik in het menu links op **Ondersteuning > Diagnostiek Pack**.

Flow Collecto	Flow Collector NetFlow VE											
섉 Home 🗲 Configuration 🛛 🔅	i This appliance is manage	This appliance is managed by a Central Manager. Please go to <u>Central Management</u> to change these settings.										
📥 Manage Users 🛛 🕀	i Info! This page automation	i Infol This page automatically refreshes every minute - last refreshed at 19:05:29.										
Support Advanced Settings	System	System										
 Database Storage Statistics 	IP Address:											
 Backup/Restore Database 	Host name:	10000000	Domain name:									
Browse Files Recket Canture	Total Memory:		Load Average:									
- Update	VM Server Memory:	the second second	VM Server CPU:									
 Backup/Restore Configuration 	Free Memory:		Uptime:									
- Diagnostics Pack 🖕												
	Version:		Platform:									
Q ⁰ ₀ Operations ⊚	Build:		Senai No.:									
🕞 Logout	Facine Clature											
🕑 Help 🗉	Engine Status											

4. Eenmaal in de pagina Diagnostics Pack moet u de standaard **Public Key**-encryptie selecteren of een gedeelde sleutel/wachtwoord opgeven voor codering.

Opmerking: Als u ervoor kiest een aangepaste sleutel/wachtwoord te gebruiken, moet u dat wachtwoord in de bestandsindeling opgeven wanneer u het pack voor diagnostiek naar de Support Case Manager uploadt.

5. Selecteer **Diagnostiek Pack maken** om het diagnostische pakket van het apparaat te genereren.

💭 Flow Colle	ctor	NetFlow VE			
👫 Home	e	Diagnostics Pa	ack		
 ▲ Manage Users ✓ Support ➡ Audit Log ♥ Operations 	8	Previous Diagno diagnostic-FlowCollec public.tgz.gpg 189.44 diagnostic-FlowCollec public.tgz.gpg 171.827 Create New Dia	astics Pack		
€ Logout	в С	Encryption Type:	Public Key Shared Passphrase		
		Confirm Password:	3		
		Patented,	, U.S. Patent Numbers 7185	368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved.	

6. Na voltooiing moet u een pop-upvakje ontvangen met de knop Downloaden om het diagnostische pakket te downloaden.

Flow Collecto	r NetFlow VE	cisco SECUR
♣ Home ▶ Configuration ∅ ▲ Manage Users ∅ ▶ Support ∅ ➡ Audit Log ∅ ♦ Copout ∅ ♦ Help ∅	Diagnostics Pack Previous Diagnostics Pack diagnostic-FlowCollector_NetFlow-FCNFV1 public tg2.gpg 179.82M Create New Diagnostics Pack Encryption Type: Public key Shared Passphrase	
	Password: Creating Diagnostics Pack X 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.	

Methode 3. Van de interface van elke applicatie (CLI)

Er zijn momenten waarop het niet mogelijk is om het diagnostische pakket van een apparaat te genereren met behulp van de eerder beschreven methoden, maar deze kunnen rechtstreeks worden gegenereerd via de CLI van het apparaat. De stappen om deze taak te voltooien zijn:

1. Connect met het gewenste SNA-apparaat via Secure Shell Protocol (SSH) of rechtstreeks via console-toegang.

Opmerking: Als u het diagnostische pakket moet ophalen van een hardwareapparaat zonder SSH-toegang, kan de Kernel-gebaseerde Virtual Machine (KVM)-console van Cisco Integrated Management Controller (CIMC) ook worden gebruikt.

- 2. Meld u aan bij wortelreferenties.
- 3. Voer een van de volgende opdrachten in (dit is afhankelijk van de versie van SNA die in gebruik is):

SNA versie 7.1.x tot 7.3.x

Voer de opdracht doDiagPack in

SNA versie 7.4.x

Voer de opdrachtdiagnostiek in

- 4. Wacht tot de taak is voltooid.
- 5. Nadat de taak is voltooid, wordt het bestand Diagnostiek-pakketbestand opgeslagen in de /lancope/var/admin/diagnostiek/folder met een naamsschema van "diagnostiek-<device_type>-<apparaattype_ID>.<YYYYMMDD>.<HMM>-*.tgz.gpg"



6. Kopieer het gegenereerde bestand van het apparaat naar uw lokale computer of naar een bestandsserver met Secure Copy Protocol (SCP) of met een SSH File Transfer Protocol (SFTP) client zoals WinSCP. Het diagnostische pakket bevindt zich in het /lancope/var/admin/diagnostiek/directory.

Opmerking: het is de moeite waard om te vermelden dat SNA versie 7.4.0 een nieuwe functie heeft geïntroduceerd die het mogelijk maakt om het diagnostische pack te genereren uit het menu SystemConfig (CLI-inloggen met **wortel** aanmeldingsgegevens > Voer **SystemConfig** > Navigeren in naar **herstel** > **Diagnostics Pack**).

Kijk voor meer informatie over deze methode in de <u>Secure Network Analytics System</u> <u>Configuration Guide 7.4.x</u>.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Er zijn een paar keren dat de creatie van het diagnostische pakket mislukt. Het meest voorkomende symptoom is wanneer je een fout ontvangt die luidt: "Er was een fout bij het maken van het diagnostische pakket. Er zijn geen bestanden beschikbaar" nadat op de knop **Diagnostiek** maken is gedrukt.



Ga als volgt te werk om dit gedrag te corrigeren:

- 1. Meld u aan bij het apparaat dat dit gedrag vertoont met wortelreferenties via SSH.
- 2. Start de l /lancope/var/database/dbs/hsqldb/admin/opdracht om de inhoud van de directory te controleren.
- 3. Zorg ervoor dat de back-upsubdirectory bestaat en dat de gebruiker/groepseigenaar klaar is.

fcnf-cds:~#	٦	.s –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

Als de **back-**upsubdirectory niet bestaat in het **/lancope/var/database/dbs/hsqldb/admin/**pad, moet deze worden aangemaakt en moet de juiste eigenaar worden toegewezen. Draai deze opdrachten voor dit programma:

- 1. mkdir /lancope/var/database/dbs/hsqldb/admin/back-up
- 2. Chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/back-up
- 4. Start de opdracht I /lancope/var/admin/om de inhoud van de map te controleren.

5. Zorg ervoor dat de **back-ups** en **diagnostische** subdirectories bestaan en dat hun gebruiker/groepseigenaar **root** is.

fcnf-cds:~4 total 80	ŧ I	ll /la	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	<u>clustered datab</u> ase
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

Indien één of geen van de bovengenoemde subdirectoraten niet bestaat in het /lancope/var/admin/pad, moeten zij worden aangelegd en moet de juiste eigendom worden toegewezen. Draai deze opdrachten voor dit programma:

- 1. mkdir /lancope/var/admin/back-ups
- 2. mkdir /lancope/var/admin/diagnostiek

Nadat dit is geverifieerd, probeert u het diagnostische pakket van het SNA-apparaat opnieuw te genereren.

Gerelateerde informatie

- Neem voor extra assistentie contact op met Cisco Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: <u>Cisco's wereldwijde contactgegevens voor</u> <u>ondersteuning.</u>
- Technische ondersteuning en documentatie Cisco Systems