Diagnosepaket für Appliances für sichere Netzwerkanalysen erstellen

Inhalt

Einleitung Vorgehensweise Methode 1. Über die Webbenutzeroberfläche des Managers Methode 2. Über die Admin-Benutzeroberfläche jeder Appliance Methode 3: über die Befehlszeilenschnittstelle (CLI) jeder Appliance Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument werden die verschiedenen verfügbaren Verfahren zum Erfassen eines Diagnosepakets für SNA-Appliances (Secure Network Analytics) beschrieben.

Vorgehensweise

Es gibt drei Hauptmethoden zum Generieren des Diagnosepakets für die SNA-Appliances. Die empfohlene Methode ist **Methode 1. Über die Manager-Webbenutzeroberfläche (UI)** sind jedoch die beiden anderen Methoden optional, falls die Webbenutzeroberfläche des Managers nicht verfügbar ist.

Anmerkung: Wenn die Webbenutzeroberfläche des Managers nicht verfügbar ist und Sie ein Diagnosepaket vom Manager generieren müssen, finden Sie weitere Informationen in Methode 3. über die Befehlszeilenschnittstelle (CLI).

Methode 1. Über die Webbenutzeroberfläche des Managers

- 1. Melden Sie sich bei der Webbenutzeroberfläche des Managers an.
- 2. Navigieren Sie zu Globale Einstellungen > Zentrale Verwaltung.

藯 Network A	nalytics		Dashboards *	Monitor • Analyz	e • Jobs • Conf	gure * Deploy *			۹ 🕹 ۵	+ disco SECURE
Security Insight D	ashboard Inside Ho	sts							Global Settings Central Management	ì I
									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
									User Management	
									SecureX Configuration	
									Select Language	

3. Suchen Sie in den aufgeführten Appliances die Appliance, von der Sie das Diagnosepaket erstellen möchten, und wählen Sie **Aktionen (Ellipsis-Symbol) > Einheitenstatistik anzeigen aus**.

ਓ Central Management	Appliance Manager	Update Manager	App Manager	Smart Licensing	Database				Ŧ	essee SECURE
Inventory										
3 Appliances found										
Q Filter Appliance Inventory Table										
Appliance Status	 Host Name 		– Туре		^	IP Address	~	Actions		
Up			Flow Co	llector			Edit Appliance Configuration]		
Up	-		Flow Ser	nsor			View Appliance Statistics 😓			
Up			Manager	r			Support	🔟		
			BHC-81	Mana Conta 110	No other Constants		Reboot Appliance			
							Shut Down Appliance			
							Remove This Appliance			

4. Sie müssen zur Admin-Benutzeroberfläche der ausgewählten Appliance umgeleitet werden.

5. Melden Sie sich mit **admin-**Anmeldeinformationen bei der Appliance-Admin-Benutzeroberfläche an.

6. Navigieren Sie im Menü links zu **Support > Diagnostics Pack**.

ਓ Manager VE					tisto SECURE						
∯ Home ✔ Configuration ®	i This appliance is managed	i 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 automatica	ally refreshes every minute - last refreshed at 18:5	6:54.								
🔎 Support 📕 🛛											
 Backup/Restore Database 	System										
- Browse Files	IP Address:	10000									
 Packet Capture 	Host name:		Domain name:								
- Update											
 Backup/Restore Configuration 	Total Memory:		Load Average:								
- Diagnostics Pack	VM Server Memory:		VM Server CPU:								
■ Audit Log	Free Memory:	-	Uptime:								
Q [®] Operations □											
🕞 Logout	Version:		Platform:								
Help ®	Build:		Serial No.:								
O											

7. Wenn Sie die Seite Diagnostics Pack geöffnet haben, müssen Sie entweder die standardmäßige **Public Key-**Verschlüsselung auswählen oder einen gemeinsam genutzten Schlüssel/eine Passphrase zur Verschlüsselung bereitstellen.

Anmerkung: Wenn Sie einen benutzerdefinierten Schlüssel/ein benutzerdefiniertes Kennwort verwenden, müssen Sie diese Passphrase in der Dateibeschreibung angeben, wenn Sie das Diagnosepaket in den Support Case Manager hochladen.

8. Wählen Sie Diagnosepaket erstellen, um das Diagnosepaket der Einheit zu generieren.

藯 Manager VE		the SECURE
def Home	Diagnostics Pack	
🚢 Manage Users 🛛 🕀	Previous Diagnostics Pack	
🖋 Support 🛛 🗉	diagnostic-SMC-	
■ Audit Log	diagnostic-SMC-	
Ø ⁰ ₀ Operations □	Create New Diagnostics Pack	
(Logout	Challe Key	
🕜 Help 🛛	Encryption Type: Shared Passphrase	
G	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. Nach Abschluss des Vorgangs muss ein Popup-Fenster mit der **Download-**Schaltfläche angezeigt werden, um das Diagnosepaket herunterzuladen.

🐼 Manager VE							diale SECURE
섉 Home✓ Configuration	Diagnostics P	ack					
🚢 Manage Users 🛛 🕀	Previous Diagn	ostics Pack					
Support E Audit Log	diagnostic-SMC diagnostic-SMC diagnostic-SMC						
Ø [®] Operations □	Create New Dia	agnostics Pack					
🕀 Logout							
🛛 Help 🐵	Encryption Type:	Public Key Shared Passphrase					
G	Password:		Creating Diagn	ostics Pack ×			
	Confirm Password:		Diagnostics pack create	1			
	Create Diagnostics Pa	ck		Download Close			
	Patente	d, U.S. Patent Numbers 71853	7290283, 7475426, 7512980, and 7644151. C	ther U.S. and foreign pater	nts pending. Copyright 2022 Cisco	. All Rights Reserved.	

Methode 2. Über die Admin-Benutzeroberfläche jeder Appliance

Für diese Methode müssen Sie über Hypertext Transfer Protocol Secure (HTTPS) auf die Appliance zugreifen, von der Sie das Diagnosepaket generieren möchten.

Anmerkung: Um direkt auf die Admin-Benutzeroberfläche des Managers zuzugreifen, müssen Sie die URL verwenden: <u>https://<Manager_IP_address>/smc/index.html</u>, andernfalls werden Sie an die Webbenutzeroberfläche des Managers weitergeleitet.

Um beispielsweise das Diagnosepaket eines Flow Collectors mit dieser Methode zu generieren, müssen Sie die folgenden Schritte ausführen:

- 1. Navigieren Sie in einem Webbrowser zu https://<FC_IP_address>
- 2. Melden Sie sich mit Administratoranmeldeinformationen an der Benutzeroberfläche der Appliance Admin an.

3. Navigieren Sie im Menü links zu Support > Diagnosepaket.

0.4.0	Flow Collector NetFlow VE												
14 }	Home Configuration ®	ome i 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 automatical	i Infol This page automatically refreshes every minute - last refreshed at 19:05:29.										
۶	Support 🖊 🗉	Ountern											
ŀ	Advanced Settings	System											
ŀ	Database Storage Statistics	IP Address:											
ŀ	Backup/Restore Database	Host name:	100000	Domain name:									
	Browse Files												
ŀ	Packet Capture	Total Memory:		Load Average:									
ŀ	Update	VM Server Memory:	100000	VM Server CPU:	The second se								
┢	Backup/Restore Configuration	Free Memory:		Uptime:									
F	Diagnostics Pack 👦												
	Audit Log	Version:		Platform:									
_	Occupitore	Build:	and the second second	Serial No.:	The second se								
0	, Operations III												
۲	Logout	Engine Status											
0	Help 🗉	Ligino otatus											

4. Wenn Sie die Seite Diagnostics Pack geöffnet haben, müssen Sie entweder die standardmäßige **Public Key-**Verschlüsselung auswählen oder einen gemeinsam genutzten Schlüssel/eine Passphrase zur Verschlüsselung bereitstellen.

Anmerkung: Wenn Sie einen benutzerdefinierten Schlüssel/eine benutzerdefinierte Passphrase verwenden möchten, müssen Sie diese Passphrase in der Dateibeschreibung eingeben, wenn Sie das Diagnosepaket in den Support Case Manager hochladen.

5. Wählen Sie **Diagnosepaket erstellen**, um das Diagnosepaket der Einheit zu generieren.

Flow Colle	ctor	NetFlow VE						
🖀 Home	e	Diagnostics Pa	ack					
💄 Manage Users	Ð	Previous Diagno	ostics Pack					
 ✓ Support ≕ Audit Log ✿^o Operations Ge Logout 	æ	diagnostic-FlowCollec public.tgz.gpg 189.441 diagnostic-FlowCollec public.tgz.gpg 171.821 Create New Diag	tor_NetFlow-FCNFVE M tor_NetFlow-FCNFVE M gnostics Pack					
🕜 Help	е С	Encryption Type:	Public Key Shared Passphrase					
		Password:						
		Confirm Password:						
		Create Diagnostics Pack	k					
		Patented,	I, U.S. Patent Numbers 7185	368, 7290283, 7475426, 7512980, a	and 7644151. Other U.S. a	nd foreign patents pending. C	opyright 2022 Cisco®. All Rights Reserver	1.

6. Nach Abschluss des Vorgangs muss ein Popup-Fenster mit der **Download-**Schaltfläche angezeigt werden, um das Diagnosepaket herunterzuladen.

Flow Collecto	or NetFlow VE	cisco SECURE
♣ Home ✔ Configuration □ ▲ Manage Users □ ✔ Support □ ➡ Audit Log □ O [®] ₀ Operations □ □ € Help □	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: Creating Diagnostics Pack * Confirm Password: Diagnostics pack created. Diagnostics Pack Diagnostics pack created. Diagnostics Pack Diagnostics Pack * Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Clisco*. All Rights Reserved.	

Methode 3: über die Befehlszeilenschnittstelle (CLI) jeder Appliance

In manchen Fällen ist es nicht möglich, das Diagnosepaket einer Appliance mit den zuvor beschriebenen Methoden zu generieren. Es kann jedoch direkt über die Kommandozeile der Appliance generiert werden. Die Schritte zum Durchführen dieser Aufgabe sind:

1. Stellen Sie über Secure Shell Protocol (SSH) oder direkt über den Konsolenzugriff eine Verbindung zur gewünschten SNA-Appliance her.

Anmerkung: Falls Sie das Diagnosepaket von einer Hardware-Einheit ohne SSH-Zugriff abholen müssen, kann auch die Kernel-basierte KVM-Konsole von der CIMC-Schnittstelle (Cisco Integrated Management Controller) verwendet werden.

- 2. Melden Sie sich mit Root-Anmeldeinformationen an.
- 3. Geben Sie einen der folgenden Befehle ein (dies hängt von der verwendeten SNA-Version ab):

SNA Version 7.1.x bis 7.3.x

Geben Sie den Befehl doDiagPack ein.

SNA Version 7.4.x

Geben Sie den Befehl diagnostics start ein.

- 4. Warten Sie, bis die Aufgabe abgeschlossen ist.
- 5. Nachdem die Aufgabe abgeschlossen ist, wird die Diagnosepaket-Datei im /lancope/var/admin/diagnostics/Verzeichnis gespeichert, das ein Namensschema von "diagnostisch-<Gerätetyp>-<Geräte-ID>.<JJJMMTT>.<HHMM>-*.tgz.gpg" enthält.



 Kopieren Sie die generierte Datei von der Appliance auf Ihren lokalen Computer oder auf einen Dateiserver mit Secure Copy Protocol (SCP) oder einem SSH File Transfer Protocol (SFTP)-Client wie WinSCP. Das Diagnosepaket befindet sich im Verzeichnis /lancope/var/admin/diagnostics/Directory.

Hinweis: Es ist zu erwähnen, dass die SNA Version 7.4.0 eine neue Funktion eingeführt hat, mit der das Diagnosepaket aus dem Menü SystemConfig (Systemkonfiguration) generiert werden kann (CLI-Anmeldung mit Stammanmeldeinformationen > Systemkonfiguration eingeben > Navigieren zu Wiederherstellung > Diagnosepaket).

Weitere Informationen zu dieser Methode finden Sie im <u>Konfigurationshandbuch für Secure</u> <u>Network Analytics System 7.4.x</u>.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Es gibt Fälle, in denen die Erstellung des Diagnosepakets fehlschlägt. Das häufigste Symptom ist die Fehlermeldung "Beim Erstellen des Diagnosepakets ist ein Fehler aufgetreten. No files are available (Keine Dateien verfügbar)" (Nach Klicken auf die Schaltfläche **Create Diagnostics Pack** (Diagnosepaket erstellen)).



So korrigieren Sie dieses Verhalten:

- 1. Melden Sie sich bei der Appliance an, die dieses Verhalten mit **Root-**Anmeldeinformationen über SSH hat.
- 2. Führen Sie den Befehl **Is -I /lancope/var/database/dbs/hsqldb/admin/**aus, um den Inhalt des Verzeichnisses zu überprüfen.
- 3. Stellen Sie sicher, dass das **Backup-**Unterverzeichnis vorhanden ist und dass der Benutzer-/Gruppenbesitzer **Tomcat** ist.

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

Wenn das **Backup-**Unterverzeichnis nicht im **/lancope/var/database/dbs/hsqldb/admin/**path vorhanden ist, muss es erstellt und der korrekte Eigentümer zugewiesen werden. Führen Sie dazu die folgenden Befehle aus:

- 1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
- 2. Wählen Sie tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup

4. Führen Sie den Befehl **Is -I /lancope/var/admin/**aus, um den Inhalt des Verzeichnisses zu überprüfen.

5. Stellen Sie sicher, dass die **Backups** und **Diagnoseunterverzeichnisse** vorhanden sind und dass der Benutzer-/Gruppenbesitzer **root** ist.

fcnf-cds:~# total 80	1	l /la	ancope/va	ar/adm:	in/			
drwxrwxr-x	2	root	root	4096	Apr	27	06:25	backups
drwxr-xr-x 2	2	root	root	4096	Apr	7	21:39	cds
-rw-r)	1	root	root	0	Apr	6	22:10	clustered database
drwxrwxr-x 2	2	root	root	4096	Sep	7	2021	diagnostics
-rw-rr	1	root	root	40	Apr	27	17:18	hwserial
-rw-r 0	1	root	root	8	Apr	27	17:18	meminfo
-rw-r 0	1	root	root	69	Apr	27	17:18	model
-rw-r 0	1	root	root	23	Apr	27	17:18	platform
drwxr-xr-x 3	3	root	root	4096	Sep	15	2021	plugins
-rw-rw-rw-	1	root	root	2	Apr	27	18:13	previous_engine_startup_mode
-rw-r 0	1	root	root	47	Apr	27	17:18	serial
drwxr-xr-x 2	2	root	root	4096	Apr	7	21:22	ssh
drwxr-xr-x 2	2	root	root	4096	Apr	8	02:51	system.d
-rw-rw 0	1	root	swadmin	12756	Apr	8	02:56	system.xml
drwxrwxrwx 2	2	root	root	4096	Apr	28	00:25	tmp
drwxr-xr-x 2	2	root	root	4096	Sep	7	2021	update
drwxrwxr-x 4	4	root	tomcat	4096	Apr	8	02:49	upgrade
-rw-r 0	1	root	root	36	Apr	27	17:18	uuid
feaf-edere#								

Wenn ein oder keines der genannten Unterverzeichnisse im **/lancope/var/admin/**path nicht vorhanden ist, müssen diese erstellt und der korrekte Eigentümer zugewiesen werden. Führen Sie dazu die folgenden Befehle aus:

- 1. mkdir /lancope/var/admin/backup
- 2. mkdir/lancope/var/admin/diagnose

Nach der Überprüfung sollten Sie erneut versuchen, das Diagnosepaket der SNA-Appliance zu generieren.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Cisco Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: <u>Weltweiter Kontakt zum Cisco Support</u>.
- Technischer Support und Dokumentation für Cisco Systeme