Générer un kit de diagnostics pour les appliances Secure Network Analytics

Contenu

Introduction Procédure Méthode 1. À partir de l'interface utilisateur Web du gestionnaire Méthode 2. À partir de l'interface utilisateur Admin de chaque appareil Méthode 3. À partir de l'interface de ligne de commande (CLI) de chaque appareil Dépannage Informations connexes

Introduction

Ce document décrit les différentes procédures disponibles pour collecter un pack de diagnostics pour les appliances SNA (Secure Network Analytics).

Procédure

Il existe trois méthodes principales pour générer le pack de diagnostics pour les appliances SNA. La méthode suggérée est **la méthode 1. À partir de l'interface utilisateur Web du gestionnaire**, les deux autres méthodes sont toutefois une option au cas où l'interface utilisateur Web du gestionnaire n'est pas disponible.

Note: Si l'interface utilisateur Web du gestionnaire n'est pas disponible et que vous devez générer un pack de diagnostics à partir du gestionnaire, reportez-vous à la méthode 3. À partir de l'interface de ligne de commande de chaque appareil.

Méthode 1. À partir de l'interface utilisateur Web du gestionnaire

- 1. Connectez-vous à l'interface utilisateur Web du manager.
- 2. Accédez à Paramètres globaux > Gestion centrale.

ਓ Network A	nalytics		Dashboards •	Monitor • Analy:	ze • Jobs • Conf	figure * Deploy *			۹ ք م	+ diada SECURE
Security Insight D	ashboard Inside Ho	osts							Global Settings Central Management 😽	
Alarming Hosts 💿									Manager Configuration Packet Analyzer Configuration	- Z
Concern Index	Target Index	Recon	Cac	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltratio	UDP Director Configuration External Lookup Configuration	Anomaly
									SecureX Configuration	

3. Dans les appliances répertoriées, localisez l'appliance à partir de laquelle vous devez créer le pack de diagnostics et sélectionnez Actions (icône Ellipse) > Afficher les statistiques de l'appliance.

ਓ Central Management	Appliance Manager	Update Manager	App Manager	Smart Licensing	Database				+	essee SECURE
Inventory										
Q Filter Appliance Inventory Table										
Appliance Status	∧ Host Name		Type		^	IP Address	^	Actions		
Up			Flow Co	vilector			Edit Appliance Configuration]		
Up			Flow Se	insor			View Appliance Statistics 😓			
Up			Manage	H.			Support	🖌		
							Reboot Appliance			
							Shut Down Appliance			
							Remove This Appliance			

4. Vous devez être redirigé vers l'interface utilisateur Admin de l'appareil sélectionné.

5. Connectez-vous à l'interface utilisateur Admin de l'appliance avec les informations d'identification **admin**.

6. Dans le menu de gauche, accédez à **Support > Diagnostics Pack**.

ਓ Manager VE					disco SECURE								
∯ Home ✔ Configuration ®	i This appliance is manage	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 automatic	i Infol This page automatically refreshes every minute - last refreshed at 18:56:54.											
🗲 Support 📈 🛛													
 Backup/Restore Database 	System												
 Browse Files 	IP Address:												
 Packet Capture 	Host name:		Domain name:										
- Update													
 Backup/Restore Configuration 	Total Memory:		Load Average:										
– Diagnostics Pack 🍃	VM Server Memory:		VM Server CPU:										
	Free Memory:		Uptime:										
Operations													
🕒 Logout	Version:		Platform:										
@ Help @	Build:	the second se	Serial No.:	And the second second second									
C													

7. Une fois dans la page Pack de diagnostics, vous devez sélectionner le chiffrement de **clé publique** par défaut ou fournir une clé/phrase de passe partagée à utiliser pour le chiffrement.

Note: Si vous choisissez d'utiliser une clé/un mot de passe personnalisé, vous devez fournir cette phrase de passe dans la description du fichier lorsque vous téléchargez le pack Diagnostics dans le Gestionnaire de dossiers d'assistance.

8. Sélectionnez Create Diagnostics Pack pour générer le pack de diagnostics de l'appliance.

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. Une fois terminé, vous devez disposer d'une fenêtre contextuelle comprenant le bouton **Télécharger** pour télécharger le Pack de diagnostics.

🕤 Manager VE				cisco SECURE
♣ Home ✔ Configuration ©	Diagnostics P	ack		
🚢 Manage Users 🗉	Previous Diagn	ostics Pack		
✓ Support	diagnostic-SMC diagnostic-SMC diagnostic-SMC			
Q ⁰ ₀ Operations ⊕	Create New Dia	agnostics Pack		
🕒 Logout		Public Key		
🕜 Help 🗉	Encryption Type:	O Shared Passphrase		
G	Password:		Creating Diagnostics Pack	
	Confirm Password:		Degnostics pack created.	
	Create Diagnostics Pa	ck	Download Come	
	Patente	d, U.S. Patent Numbers 71853	18, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved.	

Méthode 2. À partir de l'interface utilisateur Admin de chaque appareil

Pour cette méthode, vous devez accéder à la solution matérielle-logicielle à partir de laquelle vous souhaitez générer le pack de diagnostics, via HTTPS (Hypertext Transfer Protocol Secure).

Note: Pour accéder directement à l'**interface utilisateur Admin** du manager, vous devez utiliser l'URL suivante : <u>https://<Manager_IP_address>/smc/index.html</u>, sinon vous êtes redirigé vers l'interface utilisateur Web du manager.

Par exemple, afin de générer le pack de diagnostics d'un collecteur de flux avec cette méthode, vous devez suivre les étapes suivantes :

- 1. Àpartir d'un navigateur Web, accédez à https://<adresse_IP_FC>
- 2. Connectez-vous à l'interface utilisateur Admin de l'appliance avec les informations d'identification admin.

Identific SECURE Network Analytics Prove Collector NetFlow VE 7.0 Username:
Username: Password:
Login >>
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. Dans le menu de gauche, accédez à Support > Diagnostics Pack.

Flow Collector NetFlow VE										
 Home Configuration Manage Users 										
Support Advanced Settings	System									
 Database Storage Statistics 	IP Address:									
 Backup/Restore Database 	Host name:	1000000	Domain name;							
 Browse Files Packet Capture 	Total Memory:		Load Average:							
- Update	VM Server Memory:	100 C 100 C 100 C	VM Server CPU:	The second s						
 Backup/Restore Configuration 	Free Memory:		Uptime:	CONCERNING AND A DESCRIPTION OF A DESCRI						
– Diagnostics Pack 🖕										
	Version:		Platform:	and the second se						
Operations	Duno:		Senal No.:							
🕒 Logout	Engine Status									
Ø Help	Engine Status									

4. Une fois dans la page Pack de diagnostics, vous devez sélectionner le chiffrement de **clé publique** par défaut ou fournir une clé/phrase de passe partagée à utiliser pour le chiffrement.

Note: Si vous choisissez d'utiliser une clé/phrase de passe personnalisée, vous devez fournir cette phrase de passe dans la description du fichier lorsque vous téléchargez le pack de diagnostics dans le Gestionnaire de dossiers d'assistance.

5. Sélectionnez Create Diagnostics Pack pour générer le pack de diagnostics de l'appliance.

Flow Colle	ctor	NetFlow VE						
🙀 Home		Diagnostics Pa	ack					
Configuration Anage Users	e	Previous Diagno	ostics Pack					
 ✓ Support ■ Audit Log Ø[®]₂ Operations 	æ	diagnostic-FlowCollec public.tgz.gpg 189.44 diagnostic-FlowCollec public.tgz.gpg 171.82 Create New Dia	tor_NetFlow-FCNFVE					
Ø Help	8 0	Encryption Type:	 Public Key Shared Passphrase 					
		Password:						
		Confirm Password:						
		Create Diagnostics Paci	ĸ					
		Patented	I, U.S. Patent Numbers 7185	368, 7290283, 7475426, 7512980, an	d 7644151. Other U.S. and	foreign patents pending. Copyrig	ht 2022 Cisco®. All Rights Reserved.	

6. Une fois terminé, vous devez disposer d'une fenêtre contextuelle comprenant le bouton **Télécharger** pour télécharger le Pack de diagnostics.

Flow Collecto	or NetFlow VE	see SECURE
Image: Home ✓ Configuration ▲ Manage Users ✓ Support ■ Audit Log OC Operations © Image: Logout Image: Logout Image: Logout Image: Logout Image: Logout Image: Logout	Diagnostics Pack Previous Diagnostics Pack diagnostic-FlowCollector_NatFlow-FCNFV1 public.tgr.gog 189.44M Create New Diagnostics Pack Previous Diagn	
G	O Shared Passphrase Password: Confirm Password: Confirm Password: Consist Dispositics Pack Password: Destroyed Password: Destroyed Password: Destroyed Password: Destroyed Destroyed Password: Destroyed Destroyed Pastented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Clisco®, All Rights Reserved.	

Méthode 3. À partir de l'interface de ligne de commande (CLI) de chaque appareil

Il arrive parfois qu'il soit impossible de générer le pack de diagnostics d'un appareil à l'aide des méthodes décrites précédemment, mais il peut être généré directement à partir de l'interface de ligne de commande de l'appareil. Pour effectuer cette tâche, procédez comme suit :

1. Connectez-vous à l'appliance SNA souhaitée via le protocole SSH (Secure Shell Protocol) ou directement via l'accès à la console.

Note: Si vous avez besoin de collecter le pack de diagnostics à partir d'un matériel sans accès SSH, la console de machine virtuelle basée sur le noyau (KVM) de l'interface CIMC (Integrated Management Controller) de Cisco peut également être utilisée.

- 2. Connectez-vous avec les informations d'identification racine.
- 3. Entrez l'une des commandes suivantes (cela dépend de la version de SNA utilisée) : SNA version 7.1.x à 7.3.x

Entrez la commande doDiagPack

SNA version 7.4.x

Entrez la commande diagnostics start

- 4. Attendez que la tâche soit terminée.
- 5. Une fois la tâche terminée, le fichier du pack de diagnostics est stocké dans le répertoire /lancope/var/admin/diagnostics/ avec un modèle de nom "diagnostic-<type_périphérique>-<ID_périphérique>.<YYYMMDD>.<HHMM>-*.tgz.gpg"



6. Copiez le fichier généré depuis l'appliance vers votre ordinateur local ou vers un serveur de fichiers avec le protocole SCP (Secure Copy Protocol) ou avec un client SFTP (SSH File Transfer Protocol) tel que WinSCP. Le pack de diagnostics se trouve dans le répertoire /lancope/var/admin/diagnostics/.

Note : Il est utile de mentionner que SNA version 7.4.0 a introduit une nouvelle fonctionnalité qui permet de générer le pack de diagnostics à partir du menu SystemConfig (CLI se connecte avec les informations d'identification **racine** > Enter **SystemConfig** > Navigate to **Recovery** > **Diagnostics Pack**).

Pour plus d'informations sur cette méthode, consultez le <u>Guide de configuration de Secure</u> <u>Network Analytics System 7.4.x</u>.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Il arrive que la création du pack de diagnostics échoue. Le symptôme le plus courant est lorsque vous recevez une erreur qui dit : « Une erreur s'est produite lors de la création du pack de diagnostics. Aucun fichier n'est disponible » après avoir cliqué sur le bouton **Créer un pack de diagnostics**.

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

Pour corriger ce comportement, procédez comme suit :

- 1. Connectez-vous à l'appliance qui a ce comportement avec les informations d'identification **racine** via SSH.
- 2. Exécutez la commande **Is -I /lancope/var/database/dbs/hsqldb/admin/** pour vérifier le contenu du répertoire.
- 3. Assurez-vous que le sous-répertoire **de sauvegarde** existe et que son utilisateur/propriétaire de groupe est **tomcat**.

fcnf-cds:~#	٦	.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 3	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 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 le sous-répertoire de sauvegarde n'existe pas dans le

/lancope/var/database/dbs/hsqldb/admin/path, il doit être créé et la propriété correcte doit être attribuée. Pour cela, exécutez les commandes suivantes :

- 1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
- 2. chown tomcat : tomcat /lancope/var/database/dbs/hsqldb/admin/backup
- 4. Exécutez la commande ls -l /lancope/var/admin/ pour vérifier le contenu du répertoire.

5. Assurez-vous que les sous-répertoires **des sauvegardes** et **diagnostics** existent et que leur propriétaire utilisateur/groupe est **racine**.

fcnf-cds:~4 total 80	ŧ	(1 /ն	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-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.							

Si l'un ou l'autre des sous-répertoires mentionnés n'existe pas dans le chemin /lancope/var/admin/chemin, ils doivent être créés et la propriété correcte doit être attribuée. Pour cela, exécutez les commandes suivantes :

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

Une fois cette vérification effectuée, essayez de générer à nouveau le pack de diagnostics de

l'appliance SNA.

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique Cisco (TAC). Un contrat d'assistance valide est requis : <u>Coordonnées du service d'assistance Cisco</u> <u>à l'échelle mondiale.</u>
- <u>Support et documentation techniques Cisco Systems</u>