تاليلحت ةزهجأل صيخشتلا ةمزح ءاشنإ ةنمآلا ةكبشلاً

تايوتحملا

قمدق ملا عارج[ل] عارج[ل] ريدملاب قصاخلا (UI) بيو مدختسم قمجاو نم 1. ققيرطل زامج لك قرادا مدختسم قمجاو نم 2. ققيرطل زامج لكب قصاخ (CLI) رماوأ رطس قمجاو لك نم 3. ققيرطل امحالصاو عاطخألا فاشكتسا قلص تاذ تامول عم

ەمدقملا

تاليلحت ةزهجأل تاصيخشت ةمزح عمجل ةرفوتملا ةفلتخملا تاءارجإلا دنتسملا اذه فصي ةنمآلا ةكبشلا (SNA).

ءارجإلا

يه ةحرتقملا ةقيرطلاا .SNA ةزهجأل صيخشتلاا ةمزح ءاشنإل ةيسيئر قرط ثالث كانه رايخ امه نييرخألا نيتقيرطلا نإف كلذ عمو ،(U**I) ريدملل بيو مدختسم ةمجاو نم .1 ةقيرطلا** ريدملاب ةصاخلا بيو مدختسم ةمجاو رفوت مدع ةلاح يف.

ءاشنإ ىلا جاتحتو ةرفوتم ريغ ريدملاب ةصاخلا بيو مدختسم ةهجاو تناك اذا :**قظحالم** ر**ماوا رطس ةهجاو لك نم .3 بولسألا** ىلا عوجرلا ءاجرلا ،ريدملا نم تاصيخشت ةمزح.

ريدملاب ةصاخلا (UI) بيو مدختسم ةمجاو نم .1 ةقيرطلا

- ا.ريدملاب ةصاخلا بيو مدختسم ةهجاو يلإ لوخدلا ليجستب مق .
- . **ةيزكرملا ةرادإلا < ةيمومعلا تادادعإلا** علام لقتنا.

ਓ Network A	nalytics		Dashboards *	Monitor • Analyz	e • Jobs • Conf	figure * Deploy *			۹ ք م	+ cisco SECURE
									Global Settings	
Security Insight D	ashboard Inside H	losts							Central Management 🛛 😓	
									Manager Configuration	
Alarming Hosts 0									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	

ددحو صيخشتلا ةمزح ءاشنإ ىلإ هلالخ نم جاتحت يذلا زاهجلا عقوم ددح ،ةجردملا ةزهجألا نم .3 زا<mark>هجلا تايئاصحا ضرع < (يواضيبلا لكشلا ةنوقيأ) تاءارجإلاا</mark>.

Ð	Central Management	Appliance Manager	Update Manager	App Manager	Smart Licensing	Database				Ŧ	cisco SECURE
Inv	entory										
3 Appl	iances found										
	Q Filter Appliance Inventory Table										
Ap	pliance Status	Host Name		_ Туре		^	IP Address	~	Actions		
Up				Flow Co	llector			Edit Appliance Configuration			
Up		-		Flow Se	nsor	e se testilise e a		View Appliance Statistics			
Up				Manage	-	and the second second		Support Reboot Appliance	🖊		
								Shut Down Appliance			
								Remove This Appliance			

- 4. ددحملا زاهجلل Admin مدختسم ةهجاو ىلإ كەيجوت ةداعإ بجي.
- 5. **لوؤسملا** دامتعا تانايب مادختساب زاهجلا لوؤسم مدختسم ةهجاو ىلإ لوخدلا لجس.

藯 Manager VE					cisco SECURE
 Anome ✓ Configuration Manage Users ✓ Support ✓ Backup/Restore 	i This appliance is managed i Infel This page automatica System	by a Central Manager, Please go to <u>Central Man</u> Illy refreshes every minute – last refreshed at 18:	agement to change these settings.		
Database - Browse Files - Packet Capture - Update - Backup/Bestore	IP Address: Host name:		Domain name:		
Configuration Diagnostics Pack	VM Server Memory:		VM Server CPU:		
Audit Log Q ⁶ Operations □	Version:		Platform:	No. of Concession, Name	
G Help ©	Build:		Serial No.:	And the second of the second	

ماعلا حاتفملا ريفشت ديدحت كمزلي ،"صيخشتلا ةمزح" ةحفص ىلإ لوصولا درجمب .7 ريفشتلل اهمادختسال ةكرتشم رورم ةرابع/كرتشم حاتفم ريفوت وأ يضارتفالا.

ةرابع ريفوت كيلع بجيف ،ةصصخم رورم ةملك/حاتفم مادختسإ ترتخأ اذإ :**ةظحالم** معدلا ةلاح ريدم ىلإ صيخشتلا ةمزح ليمحت دنع فلملا فصو يف هذه رورملا

.زاهجلل صيخشتلا ةمزح ءاشنإل **صيخشتلا قمزح ءاشنا** ددح .8

藯 Manager V	Ε	
 A Home ✓ Configuration ▲ Manage Users ✓ Support ⇒ Audit Log 	 Diagnostics Pack Previous Diagnostics Pack diagnostic-SMC- diagnostic-SMC- 	
© Help	Create New Diagnostics Pack	
	Password: Contrm Password: Create Diagnostice 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.	

ةمزح" ليزنتل **ليزنتلا** رز نمضتي قثبنم عبرم كل مدقت نأ بجي ،ءاەتنالا درجمب .9 صيخشتلا.

🐼 Manager VE		ence SECURE
 Home ✓ Configuration Manage Users 	 Diagnostics Pack Previous Diagnostics Pack 	
✓ Support	e diagnostic-SMC diagnostic-SMC	
Ø [®] Operations ⊚	Create New Diagnostics Pack	
Ø Help ⊕	Encryption Type:	
O	Password: Creating Diagnostics Pack	
	Confirm Password: Diagnostics pack created.	
	Create Diagnostics Plack Download Cose	
	Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyrig	ht 2022 Cisco®, All Rights Reserved.

زامج لك ةرادإ مدختسم ةمجاو نم .2 ةقيرطلا

ربع ،ەنم "صيخشتلا ةمزح" ءاشنإ ديرت يذلا زاەجلا ىلإ لوصولا كيلع بجي ةقيرطلا ەذەل نمآلا يبعشتلا صنلا لقن لوكوتورب (HTTPS).

مادختسإ بجي **ريدملاب قصاخلا Admin ا**مدختسم ةمجاو ىلإ ةرشابم لوصولل :**قظحالم** كەيجوت ةداعإ متيسف ال[و ،URL: <u>https://<Manager_IP_ADDRESS>/smc/index.html</u> ناونع ريدملاب ةصاخلا بيو مدختسم ةمجاو ىلإ.

بجي ،ةقييرطلا ەذە مادختساب قفدت عمجمل صيخشتلا ةمزح ءاشنال ،لاثملا ليبس ىلع ةيلاتلا تاوطخلا عابتا كيلع:

- 1. دان من من <u>https://<FC_IP_ADDRESS</u>
- دامتعا تانايب مادختساب زاهجلا لوؤسم مدختسم ةهجاو ىلإ لوخدلا ليجستب مق .2 لوؤسملا.

	Network Analytics	
	Flow Collector NetFlow VE 7.4.0	
Username: Password:	Logn s>	
Si Patented, U.	ure Network Analytics is a trademark of Osco Systems, Inc. Patent Nos. 7155368, 7290283, 7475426, 7512980 and 7644151. © 2000-2022 Cisco Systems, Inc. All rights reserved.	

3. **مىيخشتلا ةمزح < معدلا** ىلإ لقتنا ،راسيلا ىلع ةمئاقلا نم.

Flow Collector NetFlow VE										
🖀 Home	i This appliance is managed	i This appliance is managed by a Central Manager. Please go to Central Management to change these settings.								
💄 Manage Users 🛛 🕫	i Info! This page automatica	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:	10000000						
 Browse Files Packet Capture 	Total Memory:		Load Average:							
- Update	VM Server Memory:		VM Server CPU:	The second se						
 Backup/Restore Configuration 	Free Memory:		Uptime:	100.000						
– Diagnostics Pack 😓										
	Version:		Platform:							
Operations	Build:		Serial No.:							
(+ Logout	Engine Status									
🕜 Help 🙂	Engine Status									

ماعلاا حاتفملا ريفشت ديدحت ىلا امإ جاتحت ،"صيخشتلا ةمزح" ةحفص ىلا لوصولا درجمب .4 ريفشتلل اهمادختسال ةكرتشم رورم ةرابع/كرتشم حاتفم ريفوت وأ يضارتفالا.

رورملا ةرابع ريفوت كيلع بجيف ،رورم ةرابع/صصخم حاتفم مادختسإ ترتخأ اذإ :**قظحالم** معدلا ةلاح ريدم ىلإ صيخشتلا ةمزح ليمحت دنع فلملا فصو يف هذه.

.زاهجلل صيخشتلا ةمزح ءاشنإل **صيخشتلا قمزح ءاشناٍ** ددح .5

Flow Colle	ector	NetFlow VE					
♣ Home ✗ Configuration	e	Diagnostics Pa	ack				
🛔 Manage Users	Ð	Previous Diagno	ostics Pack				
 ✓ Support ⇒ Audit Log ☆⁰₆ Operations (➡ Logout 	e	diagnostic-FlowCollec public.tgz.gpg 189.44 diagnostic-FlowCollec public.tgz.gpg 171.82 Create New Dia	ctor_NetFlow-FCNFVE				
😧 Help	•	Encryption Type:	 Public Key Shared Passphrase 				
		Password:					
		Confirm Password:					
		Create Diagnostics Pac	ek				
		Patented	d, U.S. Patent Numbers 7185	368, 7290283, 7475426, 7512980, and	d 7644151. Other U.S. and	foreign patents pending. Copyright 20	22 Cisco®. All Rights Reserved.

6. ةمزح" ليزنتل **ليزنتلا** رز نمضتي قثبنم عبرم كل مدقت نأ بجي ،ءاەتنالا درجمب صيخشتلا.

Flow Colle	ector	NetFlow VE		cisco SE
 ☆ Home ✓ Configuration ▲ Manage Users ✓ Support ≅ Audit Log ☆ Operations ☞ Logout ♀ Help 	8 8 8	Diagnostics Pack Previous Diagnostics Pack diagnostic-FlowCollector_NetFlow-FCNFVI public.tgr.og/189.44M diagnostic-FlowCollector_NetFlow-FCNFVI public.tgr.ggg 171.82M Create New Diagnostics Pack Encryption Type: O Shared Passphrase		
		Password: Confirm Password: Create Diagnostics Pack Patented, U.S. Patent Numbers 7185368, 72	Orerating Diagnostics Pack Image: Composition pack created. Degrostics pack created. Downloagy Composition pack created. Downloagy Composition pack created. Downloagy Composition pack created. 90283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved.	

زاهج لكب ةصاخ (CLI) رماوأ رطس ةهجاو لك نم .3 ةقيرطلا

مادختساب ام زاهجب ةصاخلا "صيخشتلا ةمزح" ءاشنإ اهيف نكمي ال يتلا تاقوألا ضعب كانه ةصاخلا (CLI) رماوألا رطس ةهجاو نم ةرشابم اهؤاشنإ نكمي كلذ عمو ،اقبسم ةحضوملا قرطلا يه ةمهملا هذه لامكإل تاوطخلا. زاهجلاب:

ربع ةرشابم وأ (SSH) نامألا ةقبط لوكوتورب ربع بولطملا SNA زاهجب لاصتالاب مق .1 مكحتلا ةدحو ىلإ لوصولا.

```
نكمي ،SSH لوصو نودب زاهج نم تاصيخشتلا ةمزح عيمجت ىلإ ةجاحلا ةلاح يف :قظحالم
قدحو ةهجاو نم Kernel ىلإ ةدنتسملا (KVM) يرهاظلا زاهجلا يف مكحتلا قدحو مادختسإ
اضيأ Cisco نم (CIMC) قلماكتملا قرادإلا يف مكحتلا
```

- 2. **رذجلا** دامتعا تانايب مادختساب لوخدلا لجس.
- 3. (مادختسالا ديق SNA رادصإ ىلع اذه دمتعي) ةيلاتلا رماوألا دحأ لخدا. SNA رادصإلا 7.1.x رادصإلا SNA
 - doDiagPack رمألا تلخد

SNA رادصإلا 7.4.x

صيخشتلا أدبي رمألا لاخدإ

.ةمەملا لمتكت ىتح رظتنا

ليلدلا يف تاصيخشتلا ةمزح فلم نيزخت متي ،ةمەملا لامتكا درجمب .5 -<device_type>-يصيخشت ءامساً ماظن عم/lancope/var/admin/diagnostics/ -<device_id>.<YYYMMDD>.<hhmm>-*.tgz.gpg"



تافلم مداخ ىلإ وأ كيدل يلحملا رتويبمكلا ىلإ زاهجلا نم هؤاشنإ مت يذلا فلملا خسنا .6 تافلم لقن لوكوتورب ليمع مادختساب وأ (SCP) نمآلا خسنلا لوكوتورب مادختساب SSH (SFTP) ل كم WinSCP. يف تاصيخشتلا ةمزح دجوت .WinSCP ل ثم LANCOPE/VAR/admin/diagnostic/.

ةمزح ءاشنإب حمست ةديدج ةزيم لخدأ SNA نم 7.4.0 رادصإلاا نأ ىلإ ةراشإلاا ردجت :**قظحالم** لاخدا < **رذجلا** دامتعا تانايب مادختساب لوخدلا لجس) SystemConfig ةمئاق نم صيخشتلا SystemConfig < دادرتسالا ىلإ لقنتلا

<u>قكبشلا تاليلحت ماظن نيوكت ليلد</u> عجار ،ةقيرطلا ەذە لوح تامولعملا نم ديزمل <u>ماطان تاليلحت ماظن تيوكت ليل</u>د

اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسإ كنكمي تامولعم مسقلا اذه رفوي

رثكألاا ضارعألاا دحأ لثمتي ."صيخشتلا ةمزح" ءاشنإ اهيف لشفي يتلاا نايحألاا ضعب كانه تافلم دجوت ال ."صيخشتلا ةمزح ءاشنإ ءانثأ أطخ ثدح" لوقي أطخ ىقلتت كنأ يف اعويش م**يخشتلا ةمزح ءاشنا مزح ءاشن**ا دعب "ةرفوتم.

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

يلاتال وحنالا يالع ةعباتمال مق ،كولساا اذه حيحصتا:

- 1. ربع **رذجلا** دامتعا تانايب عم كولسلا اذه هيدل يذلا زاهجلا ىلإ لوخدلا لجس
- 2. ىوتحم نم ققحتلل /ls -l /lancope/var/database/dbs/hsqldb/admin رمألا ليغشتب مق ليلدلا.
- ةعومجملا كلام/مدختسملا نأ نمو **يطايتحالا خسنلل** يعرفلا ليلدلا دوجو نم دكأت .3 وه هب صاخلا

fcnf-cds:~# ls -l /lancope/var/database/dbs/hsqldb/admin/ total 20 -rw-r--r-- 1 tomcat tomcat 16 Apr 28 00:38 admin.lck -rw-r--r-- 1 tomcat tomcat 0 Apr 27 17:20 admin.log -rw-r--r-- 1 tomcat tomcat 84 Apr 27 17:17 admin.properties -rw-r--r-- 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

راسملا يف دوجوم ريغ **يطايتحالا خسنلل** يعرفلا ليلدلا ناك اذا /lancope/var/database/dbs/hsqldb/admin/، مق ،اذهل .ةحيحصلا ةيكلملا نييعتو هؤاشنإ بجيف ، رماوألا هذه ليغشتب:

- 1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
- 2. رايتخا Tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup
- 4. ليلدلا يوتحم نم ققحتلل /ls -l /lancope/var/admin رمألا ليغشتب مق.

نأ نمو **تاصيخشتل**او **ةيطايتحالا خسنلل** ةيعرفلا لئالدلا دوجو نم دكأت .5 ر**ذج** اهل ةكلاملا ةعومجملا/مدختسملا.

fcnf-cds:~4	ŧ	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-r	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-r	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.							

```
بجيف ،/lancope/var/admin/ راسملا يف ادوجوم ةروكذملا ةيعرفلا قلدألا نم يأ وأ دحأ نكي مل اذا
رماوألا هذه ليغشتب مق ،اذهل .ةحيحصلا ةيكلملا نييعت بجيو اهؤاشنإ:
```

ةيطايتحالا خسنلا/1. mkdir /lancope/var/admin

2. mkdir /lancope/var/admin/l

```
ىرخأ ةرم SNA زاهجل صيخشتلا ةمزح ءاشنإ لواح ،ءارجإلا اذه نم ققحتلا درجمب.
```

ةلص تاذ تامولعم

- نم (TAC) ةينقتلا ةدعاسملا زكرمب لاصتالا ىجري ،ةيفاضإ ةدعاسم ىلع لوصحلل <u>ملاعلا عاجناً عيمج يف Cisco معد لاصتا تامج</u> :حلاص معد دقع مزلي .Cisco
- <u>ادنتسمل او ينقتل معدلا</u> <u>Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما