生成安全終端私有雲支援快照並啟用即時支援會 話

簡介

本文檔介紹從思科安全終端私有雲裝置收集支援快照並啟用即時支援會話的步驟。

背景資訊

與TAC合作時,有時需要收集支援快照或允許TAC建立到您的安全終端(之前稱為高級惡意軟體防 護)私有雲裝置的支援隧道。這有助於徹底調查或遠端應用修復。

此方法可節省時間,並為TAC工程師提供有效解決問題所需的全面資訊。

支援快照

從管理入口網站產生支援快照

要從管理門戶收集支援快照,請執行以下步驟:

第1步:登入管理門戶。

第2步:選擇支援,然後選擇支援快照,如圖所示。

Secure Endpoint Private Cloud Administration Portal	Support Announcements	? Help 🕞 Logout
Configuration - Operations - Status -	Integrations - Support -	Console
Key Metrics	Live Support Session Support Snapshots	
CPU Usage 25%	Memory Usage 83% * Details	Cisco Cloud Query Failure Rate
Cisco Cloud Query Latency 10 ms	Fullest Partition : /var 71% Details	Active Connections 1
第3步:點選建立快照。	Support Announcements	? Help (➡ Logout
Private Cloud Administration Portal	•••	

A support snapshot contains log files and system information that can assist with the diagnosis of problems with your device. Once generated, they can be downloaded and forwarded to support or submitted to a Cisco support server.

Configuration - Operations - Status - Integrations - Support -

Console 😃 -

		Create Snapshot		
State	🕀 Size	∰ Started	⁽²⁾ Duration	I Operations

第4步:您可以選擇包括核心檔案和其他記憶體轉儲以及快照,預設情況下未選擇這些快照,如圖所 示。



Home / Support - Snapshots / Create

Support snapshot

Snapshots include system analysis, configuration, network, and log information. Select one or more of the appropriate checkboxes below to include it in the snapshot if a core dump is required. The information collected will be saved into a snapshot file for later submission to Cisco support.

Useinclude-cores; includes core files and crash dumps.
Useinclude-server-core; includes a disposition server memory dump.

第5步:您會看到快照已啟動,這可能需要一些時間。要監控進度,請按一下Details,如圖所示。

	Secure Endpoint Private Cloud Administration Portal			Support	Announcements	? Help	🕩 Logout	cisco SI	ECURE	
*	Configuration $-$	Operations -	Status 👻	Integrations -	Support -			I	Console	Ф. •

A support snapshot contains log files and system information that can assist with the diagnosis of problems with your device. Once generated, they can be downloaded and forwarded to support or submitted to a Cisco support server.

Create Snapshot

## State	🖨 Size	∰ Started	O Duration	I Operations
► Running		Mon Jul 29 2024 09:44:42 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 23 seconds ago	less than a minute	🕞 Details 🕹 🔇 🛈

第6步:完成快照生成後,您必須能夠選擇



圖示,以將快照下載到您訪問門戶的本地電腦上。

從管理門戶SSH生成支援快照

要從管理門戶SSH建立支援快照,請執行以下步驟:

第1步:透過SSH連線到管理門戶。

第2步:這是可用於生成快照的CLI。

[root@fireamp ~]# amp-support snapshot -A <Path where to store the Snapshot>

usage: /opt/opadmin/embedded/bin/amp-support snapshot [options] <snapshot_file>

Create a snapshot of the current system; this includes log files, system status, run processes, crash dumps, and other information that can be used by a support engineer to diagnose problems with your system. If no explicit options are provided the default ones are assumed. The default options are: include-configs, include-logs, include-network, include-cores, and include-status

-A, -	a11	Include everything.	
-a, -	include-analysis	Include system analysis. (SI	_OW!)

-C,	include-configs	Include	configuration files.
-с,	include-cores	Include	core files.
-F,	include-firehose-cassandra	Include	firehose-cassandra status.
-i,	include-inodes	Include	filesystem inode usage.
-I,	include-integrations	Include	appliance integration information.
-k,	include_kafka	Include	Kafka status.
-L,	include-flink	Include	Flink status.
-1,	include-logs	Include	log files.
-m,	include-mongo	Include	MongoDB status.
-N,	include-cassandra	Include	Cassandra status.
-n,	<pre>include-network</pre>	Include	network analysis.
-r,	include-redis	Include	Redis status.
-S,	include-server-core	Include	a disposition server memory dump.
-s,	include-status	Include	system status.
-d,	include-docker	Include	docker status.
-z,	<pre>include_zookeeper</pre>	Include	Zookeeper status.
-f,	fs-check FILE	Include	filesystem check results from file.
-v,	verbose	Increase	e output verbosity.

從裝置控制檯生成支援快照

要從Private Cloud Appliance Console建立支援快照,請執行以下步驟:

第1步:登入私有雲裝置控制檯。

第2步:選擇SUPPORT_SNAPSHOT。

AMP Private Cloud Advanced Malware Prote	ction (ver.)
--	---------------

ur AMP Private Clou L: htt	d device can be managed at:
C Address :	14-76-762-722
secure password has	been set, and will be required to login.
CONFIG_NETWORK CONSOLE INFO SUPPORT_SESSION SUPPORT_SNAPSHOT	Configure the Web administration interface Start command-line console / shell. Display device status / information. Start a live support session. Create and submit a support snapshot.
	< <u>○</u> K >

第3步:輸入管理門戶密碼,如圖所示。

AMP	Private	Cloud	Advance	l Malware	e Protect	tion (ver	·.)			
				Au	uthentica	tion Req	(u i red		1	
	Ple	ease ei	nter you	r passwor	rd.					
	Ŀ									
				<u>(</u>	OK N		(Cancel)			
	L			×			Cuncerr			

第4步:您可以選擇包括核心檔案和其他記憶體轉儲以及快照,預設情況下未選擇這些快照,如圖所 示。

AMP Pr	rivate Cloud	Advanced	Malware	Protection	(ver.))
--------	--------------	----------	---------	------------	--------	---

Support Snapshot
Select one or more types of data to include in your support snaps
The information will be collected for analysis by a support engine
[]] include-cores Include core / crash dumps. []] include-server-core Include disposition server memory dumps.
Cancel>

第5步:完成此操作後,選擇確定,然後開始快照。

即時支援工作階段

從管理入口網站啟用即時支援工作階段

若要從管理入口網站建立啟用即時支援工作階段,請執行下列步驟:

第1步:登入管理門戶。

第2步:點選或選擇支援並選擇即時支援會話。

Secure Endpoint Private Cloud Administration Portal	📞 Support 🛛 🌲 Announceme	ents ? Help @ Logout dialo SECURE
Configuration - Operations - Status -	Integrations - Support -	🔎 Console 😃 🗸
Key Metrics	Live Support Session Support Snapshots	
CPU Usage	Memory Usage	Cisco Cloud Query Failure Rate
35 % → Details	83 % → Details	O % ← Details
Cisco Cloud Query Latency	Fullest Partition : /var	Active Connections
10 _{ms}	71 "	1
→ Details	→ Details	r Details

第3步:按一下或選擇啟動支援會話(如圖所示),然後選擇下載以獲取TAC遠端連線到裝置所需的 SSH身份。然後按一下或選擇Start以啟動即時支援會話,如圖所示。



Step 1: Send your support identity

Before continuing, you must open a support case and attach the key from the Support Identity box below.

Support Identity	
Statistics (Statistics) - Constrainty and Constrainty Reserved. Property in statistics processing the Network Statistics (Statisty Reservice) - Reserved and Statistic Reserved and the property Reserved and Statistics (Statistics) Protocology in Constrainty Reserved and Statistics (Statistics). Reserved Reserved and Statistics) - Statistics (Reserved and Statistics). Reserved and Statistics) - Reserved Reserved Reserved and Statistics (Statistics).	🛓 Download
Description of the contract of the second state of the second s	

Step 2: Initiate support session

Support	Session			
Peer	Support-sessions.amp.cisco.com	:	22]
	Start			

第4步:裝置成功連線即時支援會話後,您會看到如圖所示的日誌,如圖所示。

	Secure Endp Private Cloud Adr	DOINT ministration Portal		📞 Suppo	rt 🌲 Announcement	s ?Help 🕩 Lo	gout	cisco SE	CUR
*	Configuration -	Operations - Status -	Integrations - Su	ipport -			100	Console	<u>ں</u> •
	O Support Ses	sion Active							
н	ome / Support - Live	Sessions /							
	State	🛗 Started		🛗 Finished	O Duration	II Operations			
	► Running	1 minute ago		O Please wait	O Please wait	🝃 Details	×		
	≣ Output 🛛 🗮 Su	pport Log							
									•
d	ebug1: Exit statu	s 0	_						
s	upport session est	ablished successfull running!	/.						-
				Lownload Output					

從管理入口網站SSH啟用即時支援工作階段

要從管理門戶SSH建立啟用即時支援會話,請執行以下步驟:

第1步:登入管理門戶SSH。

第2步:這是可用於從SSH啟用即時支援會話的CLI。

[root@fireamp ~]# amp-support session -1 support.log -s support-sessions.amp.cisco.com -p 22 <UUID>
usage: /opt/opadmin/embedded/bin/amp-support session [options] <uuid>

Manage a support session with a remote server; this facilitates a secure method of provide unrestricted shell access to your machine to an engineer on a remote system. Note that when restart a session, the same parameters as the previous session are used unless new parameters are supplied. The UUID is expected to be version 4.

Note that the `--log` option provides an optional log file for the support engineer to log their shell activity to. A script is provided to the remote user to collect this log data, but it is not and cannot be enforced by the support script.

OPTIONS

-b,batch		Use batch (non-interactive) mode.
-d,delete		Delete a support session and all files.
-l,log FILE		Log remote shell commands to file.
-p,port POR	Т	Connect to an alternative port.
-s,support-	server SERVER	Set the server of a session.
-t,terminat	e	Terminate an active session.
-v,verbose		Increase output verbosity.

NOTE: UUID can be any random string as long as it has the format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxx-xxxx.

EXAMPLES

從裝置控制檯啟用即時支援會話

要從Private Cloud Appliance Console建立啟用即時支援會話,請執行以下步驟:

第1步:登入私有雲裝置控制檯。

第2步:選擇SUPPORT_SESSION啟用即時支援會話,如下圖所示。

Main Menu-
Your AMP Private Cloud device can be managed at:
URL : https://
A secure password has been set, and will be required to login.
CONFIG_NETWORK CONSOLEConfigure the Web administration interface. Start command-line console < shell.

第3步:輸入管理門戶密碼,如圖所示。

步驟4:您可以保留所有預設設定不變。選擇確定啟用即時支援會話,如圖所示。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。