Generate Snapshot File on Secure Workload (Tetration)

Contents

Introduction Prerequisites Components Used Background Information Collect the Snapshot Bundle Generate the Classic Snapshot Bundle Generate the CIMC Bundle Generate the Tetration Agent Log Bundle Generate the Virtual Appliance Connector Snapshot Bundle Upload Bundle to the Cisco Service Request (SR) Related Information

Introduction

This document describes how to generate a Snapshot bundle file on a Cisco Secure Workload (Tetration) for different types of log collection.

Prerequisites

Components Used

Cisco recommends that you have knowledge of these products:

- Cisco Secure Workload (Tetration)
- Cisco Integrated Management Controller (CIMC)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: You must have a Customer Support role to access the snapshot tool.

Warning: The instructions on this document are applicable to the Cisco Secure Workload (Tetration) which runs software Version 3.4.1.x or later.

Background Information

The snapshot bundles used to determine the status of the Tetration Cluster's hardware, software, and integration are:

- Classical Snapshot bundle: Collects a collection of log messages, configuration data, command outputs, alerts, time-series database (tsdb), and so on, of the Cluster-related data.
- CIMC Snapshot bundle: Collects technical support files from the Unified Computing System (UCS) and it is applicable for the hardware appliance (8RU, 39RU) cluster.
- Software Agent bundle: Contains logs of the Tetration agent which gets installed on the end systems for telemetry data collection.
- Virtual Appliance Connector bundle: Contains logs from the Tetration Virtual appliance which supports flow ingestion, inventory enrichments, and alert notification.

If a Cisco engineer requests you to send a Snapshot bundle from the Secure Workload cluster, you can use the instructions provided in this document.

Collect the Snapshot Bundle

Generate the Classic Snapshot Bundle

Log in to the Secure Workload User Interface (UI), navigate to the left navigation panel, and choose the option **Troubleshoot > Snapshot** [Maintenance > Snapshot (3.4.x or 3.5.x)]. Click **Create Snapshot**, and choose **Classic Snapshot**. The snapshot page appears with the default option. You can override the default option if the Cisco TAC engineer specifically requests you to.

Cisco Secure Workload							0~ 1 ~	esco SECURE
≡		Snap	shots					
ы	Overview							
**	Organize >				Select Type 2 Create Snapshot			
E,	Defend >							
s	Investigate >		logs					
٥	Manage >		max log days					
	Platform >		2	days				
*	Troubleshoot ~	h –	number of days of logs to collect, der max log size	ault 2				
E	Service Status		131072	bytes				
	Cluster Status		maximum number of bytes per log to default 128kb	collect,				
	Virtual Machines		hosts					
C		h -	host1,host2					
	Snapshots)	hosts to get logs/status from, default	all				
Maintenance Explorer			logfiles					
	/web="_/worker=" Resque recey of loos to be fetched_default all							
	Hawkeye (Charts)		✓ yam					
	Abuse (Dinalina)		yarn app state					
	Abyss (ripenie)		RUNNING, FAILED, KILLED, UNASSIG	NED				
		application states (RUNNING, FAILED, KILLED, UNASSIGNED, etc) to get information for, default all						
			alerts					

Scroll down to the bottom of the page and use the comment section to specify the case number or problem description, and click **Create Snapshot** to initiate the procedure to generate the classic snapshot bundle. It can take a while to complete the snapshot generation. Once the snapshot generation reaches 100%, click **Download** to download the Classic Snapshot bundle. Scroll down to get an option to upload the file to the case number.

Generate the CIMC Bundle

Log in to the Secure Workload UI, navigate to the left navigation panel, and choose to **Troubleshoot > Snapshot** [Maintenance > Snapshot (3.4.x or 3.5.x)]. Click Create

Snapshot, and choose **CIMC Snapshot**. The CIMC snapshot page appears with the drop-down option to choose the node serial number. Search or choose the node and click **Create Snapshot** to initiate the procedure to generate the CIMC snapshot bundle.

K.	Cisco Secure W	Default • @• 1.	ence SECURE	
≡		Snapshots		
ы s	Overview Organize	Select Type Create Snapshot		
۴,	Defend >			
# \$	Investigate >	CIMC serial number select cluster node serial numbers		
=	Platform >	select a node's serial number to collect climc logs for		
*	Troubleshoot ~			
	Service Status Cluster Status		< Previous Creat	e Snapshot
	Virtual Machines			
	Snapshots			
	Maintenance Explorer			
	Resque			
	Hawkeye (Charts)			
	Abyss (Pipeline)			

It can take a while to complete the snapshot generation. Once the snapshot generation reaches 100%, click **Download** to download the CIMC Snapshot bundle. Scroll down to get an option to upload the file to the case number.

Generate the Tetration Agent Log Bundle

In order to collect the Log bundle, the Tetration agent must be active.

- For the 3.6.x version, navigate to the left navigation panel, choose **Manage > Agent**, and click **Agent List**.
- For the 3.4.x and 3.5.x versions, navigate to **Monitoring from** the right top drop-down menu and choose **Agent List**.

Utilize the filter option to search the agent, and click the **Agent**. It takes you to the workload profile of the Agent. Here you can find details about the Agent configuration, status, and so on.

At the left side navigation panel of the workload profile page (3.6.x), choose **Download Logs** (in the 3.4.x and 3.5.x and follow the summary tab). Click **Initiate Log Collection** to initiate the log collection from the Tetration Agent. It can take a while to complete the log collection. Once the log collection is complete, click the **Download here** option to download the logs. Scroll down to get an option to upload the file to the case number.

Disco Tetratien' WORKLOAD	PROFILE		🗢 Default 🗧 💬 Monitoring			
Summary Long Lived Processes	Process Snapshot Interfaces Package	s Vulnerabilities Config Stats Network Anomalies File Hashes Visit H	fistory			
Apr 13 6:03am - Apr 14 6:03am 👻	JBLOMART-WIN-1	3.4.x and 3.5.x Version				
Host Name jölomart-vin-1 Last Check-in Apr 14 2022 05:56:19 am (CEST) Scopes		Agtent Type S Deep Visibility SW Deployed Nov 18 2020 06 59:43 am (CET) User Annotations	OS Platform MSServer/2012R2Standard - Version 6.3 (OS Build 9600 20144) (x86_64) Agent Version 🖂 3.4.1 20 win64-sensor Enforcement Groups			
Default1 more Experimental Groups jol_tenant		None Interfaces 20	jøt_tenant Packapes 159			
Traffic Volume ④						
Total Bytes		Total Bytes Total Packets				
900- 900- 1704- 800- 800- 800- 200- 200- 200- 200- 200		hu	70 H			
Download Logs	+ Initiate Log Collection					
Requested at: x and 3.5.x versio	Apr 13 2022 06 11 35 pm (CE	ST)				
Cisco Secure Worklo	ad		© Default - ● ↓ deface SECU			
Agent List / Workload Profile / Log	Download	3.6.x Version				
Log Download						
worker1 # Enforcement CentOS 7.9		Agent Health Agent Active Flow Export Operational Upgrade Success Cpu Usage Normal Mem Usage Normal Agent Version Not Current 	Enforcement Health Good 			
LABELS AND SCOPES	Download Logs					
AGENT HEALTH	LONG LIVED PROCESSES Download Logs					
PROCESS SNAPSHOTS						
INTERFACES	Initiate log collection from the Status:	agent and download logs	+ instate Log Collection			
PACKAGES	Log collection is complete	and they can be downloaded here +				
VULNERABILITIES	Requested at: Apr 13 2022 09:30:27 pm ()\$1)				
CONFIG	Available for download at:					
	Apr 13 2022 09:30:59 pm (IST Size:	7				
CHPORGEMENT REALTH	33.86 MB					

3.6.x ver	sion
-----------	------

CONCRETE POLICIES CONTAINER POLICIES NETWORK ANOMALIES FILE HASHES DOWNLOAD LOGS

Generate the Virtual Appliance Connector Snapshot Bundle

To get the Snapshot bundle of Virtual Appliance, you need to ensure that the virtual appliances are in **Active** State.

- For the 3.6.x version, navigate to the left navigation panel, and choose **Manage > Virtual Appliance**.
- For the 3.4.x and 3.5.x versions, navigate to the left navigation panel and choose Connectors

> Virtual Appliance.

Choose the Virtual Appliance for which you like to generate the Snapshot bundle. Click **Troubleshoot**, and then again click the **Troubleshoot** option. Click **Run a New Command**, and a Dialog box opens up. The dialog box has a drop-down menu to choose the command. From the drop-down menu, choose **Collect Snapshot from the Appliance** and specify the time range in minutes (for example, 20 minutes), and click **Run Selected Command**. It initiates the procedure to collect the snapshot bundle from the Virtual appliance. It can take a while to collect the log bundle from the Virtual Appliance.

\odot	Cisco Secure Workload				Default.	• Ov Lv disds SECURE
Ξ	Virtual Appliance		Run a New Command			
ы А Б	Tetration Data Ingest Appliance 🖌 🚾	Cl Sep 13 202	Select one of the supported commands Collect Snapshot from Applance Maximum time for collection (in minutes)			Decommission
	Connectors		range from 1 to 20			
•	AnyConnect	۰		Cancel Run Selected Command		Run a New Command
*	NetScaler	۰	Collect Snapshot from Appliance	Jun 2 07:10:22 pm (IST)	Ready 🔘	View
	+ Enable Another Connector					

Once the collection of the snapshot bundle completes, click **View** to download the snapshot bundle. Scroll down to get an option to upload the file to the case number.

0	Cisco Secure Workload	Commenting	0. Describe		-	● Default + ● ↓ ↓ dudu SECURE
≡	Virtual Appliance	Command into & Results			_	
ы А Б	Tetration Data Ingest Appliance 🖉 🛛 🗛	Collect Snapshot Jun 2 07:10:22 pm	from Appliance IST) utput File	Maximum time for collection (in minutes) 20		Decommission
8	Connectors			Clos	•	
۰	AnyConnect	_			fore	Run a New Command
•			Issued Commands			
*	NetScaler	•	Collect Snapshot from Appliance	Apr 14 09:51:39 am (IST)	Pending	C View 🗑
	+ Enable Another Connector		Collect Snapshot from Appliance	Jun 2 07:10:22 pm (IST)	Ready	o Vev i

Upload Bundle to the Cisco Service Request (SR)

There are multiple ways to upload the snapshot bundle to the case (SR). For more information, check the <u>Customer File Uploads to the Cisco Technical Assistance Center</u> page.

Related Information

- <u>Cisco Secure Workload (Tetration)</u>
- <u>Cisco Secure Workload (Tetration) Product Overview</u>
- <u>Technical Support & Documentation Cisco Systems</u>