NetWitness[®] Platform Version 12.4

Broadcom SASE Configuration Guide (Private Preview Mode)



Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <u>https://www.rsa.com/en-us/company/rsa-trademarks</u>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

March, 2024

Contents

Getting Started	4
About NetWitness SASE	4
Prerequisites	5
Deploy Broadcom ETM Integration using CCM	6
Task 1. Map Network Adapter in Decoder for Broadcom ETM Integration	6
Task 2. Create and Publish Policy for Broadcom ETM Integration	8
Task 3. Configure Broadcom ETM Integration from Policy Details View	12
Task 4. Verify Broadcom ETM Events Received at Decoder	15
Task 5. Verify Events Meta from Broadcom ETM in Investigate View	16

Getting Started

NetWitness SASE, combined with Broadcom (Private Preview Mode), provides unprecedented visibility into behavior and communication among devices and services in remote and distributed networks across on-premises, hybrid, and cloud deployments.

What NetWitness SASE does:

- Streamline searches and investigations: Log into a single user interface to perform index searches, pivot through metadata, and reconstruct network sessions to receive results quickly.
- Leverage retained data: Empower analysts to perform forensic examinations on a triggered detection and threat hunt for unknown threats against retained raw network communications.
- Correlate disparate data sets: Enrich the context of investigations by correlating data from the actual network traffic of remote users with other access by those same users for a complete end-to-end story of what transpired.
- **Minimize costs**: Optimize storage and reduce operating costs using new compression algorithms, selective retention, and the ability to split network decoder components to limit what must run in the cloud.

Note: In 12.4 release, NetWitness SASE integration with Symantec by Broadcom is in Private Preview Mode.

About NetWitness SASE

NetWitness supports SASE and critical hybrid use cases across on-premises and in the cloud by partnering with Broadcom on technical integrations. NetWitness SASE Integrations give organizations complete visibility into encrypted traffic, remote users, and cloud workloads. With NetWitness SASE integrations, customers can achieve SASE flexibility, inherent security advantages, and complete visibility into threat detection and response.

NetWitness SASE provides the following capabilities:

- Flexible, secure, real-time traffic monitoring: NetWitness SASE integrations capture all network traffic from remote users in near real-time, enabling immediate response to any potential threats. Regardless of the location of the data collected, the data is available in the detection engine, and analysts can easily find the anomalies. The customization opens available in NetWitness SASE reduce the risk of storing sensitive, personally identifiable information.
- Get scalable, high-performance cloud security: With NetWitness SASE integrations, enhance total visibility and threat detection capabilities across your enterprise using well-known on-premises mechanisms such as rules, parsers, feeds, and machine learning. Perform searches and investigations and swiftly receive results with a single user interface. The integration supports forensic examinations on triggered detections and facilitates threat hunting against retained network communications, empowering analysts to combat unknown threats effectively.

- Eliminate blind spots: NetWitness SASE integrations empower organizations to retain complete visibility into their cloud security stack, cost-effectively eliminating blind spots in their cloud traffic and maximizing the effectiveness of their security infrastructure investments. Organizations have the visibility and control they need over encrypted traffic to ensure compliance with their privacy, regulatory, and acceptable use policies, whether on-premises or in the cloud.
- Unparalleled network visibility to strengthen SASE security: The improved visibility provided by the integration allows organizations to close gaps in their zero trust security posture and enable better detection capabilities.

Prerequisites

Before proceeding, it is important to make sure the following:

- The NetWitness Platform (Admin Server and Packet Decoder Host) is on version 12.4 or later.
- You are connected to Live Services under the 🎉 (Admin) > System > Live Services page.
- The Decoder services are managed by Centralized Content Management (CCM). If CCM does not manage it, you can enable CCM for the particular decoder service. For more information, see the topic Enable or Disable CCM for Individual Decoder Services.
- You must have the Request URL and Auth Token from Broadcom for configuration.

Deploy Broadcom ETM Integration using CCM

This topic describes how to deploy the Broadcom ETM Integration for users using the Policy based CCM.

You must perform the following tasks to deploy the Broadcom ETM Integration on NetWitness Platform.

- Task 1. Map Network Adapter in Decoder for Broadcom ETM Integration
- Task 2. Create and Publish Policy for Broadcom ETM Integration
- Task 3. Configure Broadcom ETM Integration from Policy Details View
- Task 4. Verify Broadcom ETM Events Received at Decoder
- Task 5. Verify Events Meta from Broadcom ETM in Investigate View

Task 1. Map Network Adapter in Decoder for Broadcom ETM Integration

You must select a network adapter (pcap_stream,Pcap File Streamer) and enable Capture Autostart option through which the Decoder captures packets and processes the data.

To Map the Network Adapter in Decoder for Broadcom ETM Integration

- 1. Log in to the NetWitness Platform.
- 2. Go to (Admin) > Services.
- 3. Select the Packet Decoder service and click > View > Config.

* NETWITNESS Platform	n Invest	igate	Respond Users Hosts Files Dashboard Re	ports				0 A Z	% ?) admin ✔	
HOSTS SERVICES EVENT SO										
Groups		Servi	ces							
+ - 🗷 O		- 🗷						💎 😔 Filter	×	
Name			Name	Licensed	Host	Туре	Versio	on	Actions	
🗄 Ali	15		CON1230 - Concentrator	0	CON1230	Concentrator	12.4.0	0.0	٠	
		•	DEC1230 - Decoder	ø	DEC1230	Decoder	12.4.0	D.0	۰ ا	
		•	SA1230 - Admin Server	0	SA1230	Admin Server	12.4	System View	N >	
			SA1230 - Broker	0	SA1230	Broker	12.4	Config Ed	ete t	
			SA1230 - Config Server	0	SA1230	Config Server	12.4	Explore Sta	rt	
		•	SA1230 - Content Server SA1230 - Integration Server	SA1230 - Content Server	ଡ	SA1230	Content Server	12.4	Logs Sto Security Res	p tart
				SA1230 - Integration Server		SA1230	Integration Server	12.4.0	0.0	۰ د
		•	SA1230 - Investigate Server	0	SA1230	Investigate Server	12.4.0	0.0	♦ ⊙	
		•	SA1230 - License Server	0	SA1230	License Server	12.4.0	0.0	♦ ⊙	
		•	SA1230 - Orchestration Server	0	SA1230	Orchestration Server	12.4.0	0.0	♦ ⊙	
		•	SA1230 - Reporting Engine	0	SA1230	Reporting Engine	12.4.0	0.0	♦ ⊙	
		00	SA1230 - Respond Server	0	SA1230	Respond Server			♦ ⊙	
		•	SA1230 - Response Actions Server	0	SA1230	Response Actions Server	12.4.0	0.0	♦ ⊙	
		-	CA1000 Convide Conver	a	644000	Consider Consider	12.4.0		*	
		~ < <	Page 1 of 1))) C					D	isplaying 1 - 15 of 15	

The Configure view for the Decoder service is displayed with the General tab open.

- 4. Under the **Decoder Configuration** section, do the following:
 - a. Set the Capture Interface Selected to pcap_stream, Pcap File Streamer network adapter.
 - b. Enable the Capture Autostart option.

XNETWITNESSPlatform Investigate Respond Users Ho						
HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & 1						
A Change Service Config Config						
General Files Data Retention Scheduler Network Rules App Rules Co	rrelation Rules Feeds Parsers Data Privacy Data Export	Applance	Service Configuration			
System Configuration			Parsers Configuration		Enable All	Disable All
Neme	Config Value		Specify if relevant meta data is generated to disk (Enabled), generate	d only in memory for other Decoder content use (Transient), or not generated at all (Disabled).		
Compression	0		Name	Config Value		
Port	50004		# ALERTS	Enabled		-
SSL RPS Mode	R		3 DHCP	Enabled		
SSL Port	50004		I DNS	Enabled		
Stat Update Interval	1000		Intropy	Disabled		
Threads	20		FeedParser	Enabled		
			I FTP	Enabled		
Decoder Configuration			∃ GeoIP2	(Mixed)		
Name	Config Value		a GTalk	Enabled		
a Adapter		-	# H323	Enabled		
Berkeley Packet Filter			B HTTP	Enabled		
Capture Interface Selected	pcap_stream,Pcap File Streamer		B HTTP2	Enabled		
G Cache			I HTTPS	Enabled		
Cache Directory	/var/netwitness/decoder/cache		38 IRC	Enabled		
Cache Size	4 GB		jSNormalize	Enabled		
Capture Settings			3 MAIL	Enabled		
Assembler Maximum Size	32 MB		NETBIOS	Enabled		
Assembler Minimum Size	0		INITWORK INITWORK INITYORK INITYOR INITYO	Enabled		
Assembler Session Rush	1		NFS	Enabled		
Assembler Session Pool	20000		I NNTP	Enabled		
Assembler Timeout Packets	60		OPENAPPID	Enabled		
Assembler Timeout Session	60		I PGP	Enabled		
Capture Autostart	ĭ ≤		B POP3	Enabled		
Capture Buffer Size	16 MB		RIP	Enabled		
Parse Maximum Bytes	128 KB		RTP	Enabled		
Parse Minimum Bytes	1 103		3 SCCP	Enabled		
Parse Threads	0	*	B SEARCH	Disabled		*
		Ap	pby			

- 5. Click **Apply** to save the changes.
- 6. To restart the Decoder service, go to the **Services** view, select the Decoder service, and click *** Restart**.
- 7. A Confirmation dialog request is displayed. To restart the service, click Yes.
- 8. (Optional) Navigate to the System view of the Decoder service and check if the Decoder is capturing the data.

This option ensures the decoder has already started capturing the packets.

🔆 NETW	/ITNESSPlatform Investigate Respond Users Hosts Files	Dashboard	Reports			K		admin 🗸			
HOSTS SI	NOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY										
🛔 Change Serv	rice 🔤 DEC1230 - Decoder System ⊚										
1 Upload Pack	ket Capture File 💽 Stop Capture 🛢 Host Tasks 🖞 Shutdown Service 🖞 Shutdown Applianc	e Service 🖞 Re	boot								
Decoder S	Decoder Service Information Appliance Service Information										
Name	DEC1230 (Decoder)	Name	DEC1230 (Host)								
Version	12.4.0.0 (Rev null)	Version	12.4.0.0 (Rev null)								
Memory Usage	173 MB (2.17% of 7940 MB)	Memory Usage	19100 KB (0.23% of 7940 MB)								
CPU	15%	CPU	5%								
Running Since	2024-Jan-25 10:00:40	Running Since	2024-Jan-17 12:24:51								
Uptime	1 hour 23 minutes 34 seconds	Uptime	1 week 22 hours 59 minutes 35 seconds								
Current Time	2024-Jan-25 11:24:14	Current Time	2024-Jan-25 11:24:26								
Decoder I	Iser Information	Host User	Information								
L L L D U L L		Name									
Name	admin	Name	admin								
Groups	Groups Administrators Groups Administrators										
Roles	aggregate, connections.manage, database.manage, decoder.manage, dpo.manage, index.manage, logs.manage, parsers.manage, rules.manage,	Roles	appliance.manage, connections.manage, logs.mana storedproc.execute, storedproc.manage, sys.mana	age, servi ge, users.	ces.mana manage	ge,					

Task 2. Create and Publish Policy for Broadcom ETM

Integration

You must create a policy with Broadcom ETM Integration plugin type and assign it to one or more groups having a decoder service and publish the policy.

Prerequisites

- Ensure that the Broadcom ETM Integration plugin is available at the SASE Integration Plugin tab.
- Ensure that the group with one or more decoder services is created.

Supported Hosts

- Packet Decoder
- Packet Hybrid

To create and publish policy for Broadcom ETM Integration

- 1. Go to \blacksquare (Configure) > Policies.
- 2. In the policies panel, click Content.
- 3. Click Policies.

The available policies are displayed.

- 4. Click + Create New to add a new policy.
- 5. In the New Policy panel, do the following:
 - a. Enter a unique policy name.
 - b. (Optional) Enter a description for the policy.

* NETWITNESS Platfo	rm Investigate Respond Users Hosts Files Dashboard Reports	Ŏ	ş.	‰	0	admin >
LIVE CONTENT SUBSCRIPTIO	ons capture policies policies esa rules custom feeds incident rules more \checkmark					
Create Content Policy						
broadcom-policy	Identify Policy - broadcom-policy					
Identify Policy	POLICY DESCRIPTION (OPTIONAL)					
Define Policy >						
Assign to Groups						
	Previous Next Save and Close Save and Publish Cancel					

- 6. Click Next.
- 7. In the Available Content, select the plugin and click + to add the Broadcom ETM Integration plugin to the policy. To add all content based on the resource type, click OAL.

* NETWITNESS Platfo	rm Investigate Respond	Users Ho	osts Files	Dashboard	Reports				Q	1	K	1	admin >
LIVE CONTENT SUBSCRIPTIC	ONS CAPTURE POLICIES POL	ICIES ESA					more \sim						
Create Content Policy													
broadcom-policy Identify Policy Define Policy Assign to Groups	Define Policy - broadcom-pol Add content along with its dependenc O For an Event Stream Analysis Rule To know more about how to create V Filters Available Content	iCy ies to the policy. content type, de deployments cli	For the selecte ployments are i ck here.	d content all the de required. Search		re added auto Selected	omatically. d Content						
	Event Stream Analysis Rule* Feed Log Device Parser SASE Integration Plugin AAE Broadcom ETM Integration Palo Albo Prima Integration	MEDIUM packet	CREATED 12/18/2023 1 12/18/2023 1	LAST UPDATED 12/18/2023 10: 12/18/2023 10:) ALL () ()			No contents are selected. Add cor		sing ⊙ l			
	Previous Next	Save and Close		d Publish Ca	ncel								

8. Enable the subscription (if required) by clicking the subscribed toggle. Once the content is subscribed to, the updates are pushed automatically.

* NETWITNESS Platfo	rm Investigate Respond	Users Hosts File	es Dashboard Reports			ġ	3 % (🕽 admin >
LIVE CONTENT SUBSCRIPTIC	ONS CAPTURE POLICIES POL	ICIES ESA RULES						
Create Content Policy								
broadcom-policy	Define Policy - broadcom-poli Add content along with its dependenc	Cy ies to the policy. For the selec						
Identify Policy >	To know more about how to create	deployments click here.	re requirea.					
Define Policy								
Assign to Groups	Available Content			Selected Content				
				✓ SASE Integration F	Plugin			
		D		NAME	MEDIUM CREATER	LAST UPDA	ATED SUBSCRIPTIO	N 🛞 ALL
				Broadcom ETM Integration	packet 12/18/2	023 12/18/202	23 10 🤍	
	NAME	MEDIUM CREATED	LAST UPDATED 🕕 ALL					
		packet 12/18/2023	i 1 12/18/2023 10: 🕀					
	Previous Next	Save and Close Save a	and Publish Cancel					

- 9. Click Next.
- 10. If there are no unassigned groups available, click + Create Group to save the policy and redirect you to the Create New Group screen.
- 11. In the New Group panel, do the following:
 - Enter the name of the group.
 - (Optional) Enter the description for the group.

	i <mark>orm</mark> Investigate Respond Users Hosts Files Dashboard Reports	ġ	8	劣	0	admin >
LIVE CONTENT SUBSCRIPT	ions capture policies policies esa rules custom feeds MORE \sim					
Create Content Grou						
SACE-Group	Identify Group - SACE-Group group name SACE-Group					
Identify Group	GROUP DESCRIPTION (OPTIONAL)					
Define Group >						
Assign Policy >						
	Previous Next Save and Close Save and Publish Cancel					

- 12. Click Next.
- 13. In the **Define Group**, click + to assign services to the group.

* NETWITNESS Platf	form Investigate	Respond	Users Hosts	s Files [Dashboard	Reports		ġ	14	劣	?	admin >
LIVE CONTENT SUBSCRIPT		DLICIES POL	ICIES ESARU									
Create Content Grou	qL											
SACE-Group	Define Group - SA Assign services to the g ① For selected Correla To know more about	CE-Group roup. One service ation Servers, deplo thow to create dep	can be added to on oyments must be co oloyments click her	nly one group. A se reated. re.								
Identify Group >	Available Services					Selected Services						
Define Group	Search	م		HIDE SER	RVICES IN A GROU							
Assign Policy >	✓ Decoder						Add services using	g⊕ bu	itton			
	NAME	GROUP	ноѕт	VERSION	⊕ ALL							
	DEC1230 - Decoder	None	DEC1230	12.4.0.0	Ð							
	Previous Next	Sav	ve and Close		Cancel							

Note:

- A service is disabled if it is assigned to another group.A service is disabled if it is not managed by Policy-based Centralized Content Management.

14. Click Next.

* NETWITNESS Plate	i <mark>orm</mark> Investigate Respond Users Hosts Files Dashboard Re					K				
LIVE CONTENT SUBSCRIPT	IONS CAPTURE POLICIES POLICIES ESA RULES CUSTOM FEEDS MO									
Create Content Group										
SACE-Group	Define Group - SACE-Group Assign services to the group. One service can be added to only one group. A service is disabled if i Or serselected Correlation Servers, deployments must be created. To know more about how to create deployments click here.	t is assigned to another	group.							
, achtary Group	Available Services	Selected Services								
Define Group	Search Q HIDE SERVICES IN A GROUP									
Assign Policy >		∽ Decoder								
		NAME	GROUP	ноѕт		VERSION	⊗ ALL			
		DEC1230 - Decoder	None	DEC1230		12.4.0.0				
	Previous Next Save and Close Save and Publish Cancel									

15. In the Assign Policies, click + to assign policies to a group. You can assign only one policy to any particular group.

* NETWITNESS Plat	f <mark>orm</mark> Investigate Respond Users Hosts Files Dashboard Reports	ġ	ß	劣	② admin >						
LIVE CONTENT SUBSCRIPT	ions capture policies policies esa rules custom feeds MORE \vee										
Create Content Gro	Create Content Group										
SACE-Group	Assign Policy - SACE-Group Assign policy to a group. Only one instance of the same policy type can be assigned to a group. For a selected policy with an Event Stream Analysis rule, deployments must be created. To know more about how to create deployments click here. Policies List Selected Policy										
Define Group >											
Assign Policy	No policies found. NAME DESCRIPTION		GRO	UPS	⊗ ALL						
	SACEPoilcy		None	e							
	Previous Next Save and Close Save and Publish Cancel										

16. Click Save and Publish to save and publish the settings.

	Investigate Respo	nd Users Hosts Files	Dashboard Reports	Ŏ) 🖻 % (?) ad	dmin >
LIVE CONTENT SUBSCRIPTIONS		POLICIES ESA RULES CU				
CONFIGURATION CONTENT						
Content Library	√ + Create New	Edit 🗘 Publish	Delete			
Policies (1)		↑ DESCRIPTION	SERVICES	POLICY	POLICY STATUS	
Groups (1)	SACE-Group		DEC1230 - Decoder	SACEPolicy	Published	
Services (1)						
Settings						
Event Stream Analysis						

IMPORTANT: Ensure that you always publish the policy after adding the **Broadcom ETM Integration** plugin to deploy the plugin to the Decoder service.

Note: You can also publish a policy from the **Policy Details** screen. For more information on publishing a policy from the **Policy Details** screen, refer to the View a Policy topic.

For more information on Policies, see Manage Policies.

For more information on Groups, see Manage Groups.

Next steps, go to the policy details view and perform the Broadcom ETM Integration settings. For more information, see <u>Task 3. Configure Broadcom ETM Integration from Policy Details View</u>

Task 3. Configure Broadcom ETM Integration from Policy

Details View

Administrators can configure the Broadcom ETM Integration type to capture the network data from the decoder service within a policy, which sends the data to NetWitness. The data is then processed by NetWitness so that it can provide a comprehensive view of network traffic and malicious activity. Analysts can use this data to monitor network traffic, identify threats, and investigate any malicious behavior.

Prerequisites

Before you begin configuring the Broadcom ETM Integration, ensure that you have the following details:

- Ensure there is a policy created with the Broadcom ETM Integration plugin type, and the policy is associated with the group that has a Decoder service configured, and the policy is published.
- You must have the Request URL and Auth Token from Broadcom for configuration.

To Configure Broadcom ETM Integration

1. Go to 🖾 (Configure) > Policies.

- 2. In the policies panel, click Content.
- 3. In the left panel, click **Policies**.
- 4. Do one of the following:
 - a. Click the policy name containing the Broadcom ETM plugin type to view the policy details.
 - b. Click a row to view details about the selected policy and click View Details.
- 5. Click the SASE Integration Plugin tab.

×1	NETWITNESS Platform Investigate	Respond Users	Hosts Files Da	shboard Report	S			ġ	*	36	0	admin >
LIVE		CIES POLICIES										
<	K broadcom-policy											
DESCRI -	DESCRIPTION GROUPS POLICY STATUS LAST UPDATED CREATED ON CREATED BY - broadcom-group Published 01/17/2024 06:25:07 am 01/17/2024 06:25:07 am admin											
Ø P	O Publish Policy If Edit Policy Force Publish											
FEED	FEED (0) SASE INTEGRATION PLUGIN (1) APPLICATION RULE (0) LOG DEVICE (0) PARSER (0) NETWORK RULE (0) EVENT STREAM ANALYSIS RULE (0) SEARCH PATTERN RULE (0) BUNDLE											
∇ [1] Subscribe] \bigcirc Unsubscribe] \oslash Enable] \oslash Disable] \boxdot Configuration												
	NAME	↑ INTEGRATION TY	MEDIUM	CONFIG STATUS	SUBSCRIPTION	STATUS	LAST UPDATED					
	Broadcom ETM Integration	Broadcom	packet	NOT_CONFIGUR	Unsubscribed	Enabled	12/18/2023 10:34:18 am					

IMPORTANT: The **Configuration** button will be disabled when the policy status is **Unpublished**, **Failed**, or **N/A**. For more information, see <u>Filter Policies</u>.

6. Select the **Broadcom ETM Integration** type and click **Configuration**.

The Configuration dialog is displayed.

Configuration		×
Broadcom ETM Integration Configure the Broadcom ETM SASE integration type to send network data to NetWitness.		
REQUEST URL* https:	ìg	
AUTH TOKEN*		
Test connection		
	Cancel	Next

- 7. Enter the request URL in the Request URL field.
- 8. Enter the auth token in the Auth Token field.

Note:

• Broadcom provides you with a unique request URL and Auth token for your account.

• It is important to keep your auth (bearer) token and request url secure. Do not share it with other users or applications

- 9. Click **Test Connection** to determine if NetWitness connects to the Broadcom service and ensure the connection is successful.
- 10. Click Next to continue.

The screen to configure the targets is displayed.

Configuration ×							
Map the following available targets Map a target to a decoder to receive network traffic from Broadcom							
	AVAILABLE TARGE	BOOTSTRAP SERV	/ERS	DECODER			
	tool1_name	gusdm.kafka	deco	oder - De			
	tool2_name	gusdm.kafka	deco	oder - De			
	tool3_name	gusdm.kafka	decoder - De				
			Cance	l Back	Save And Publish		

- 11. To configure the available targets, do the following:
 - Select the available bootstrap servers from the drop-down list.
 - Select a decoder service from the drop-down list to map it to the target.

The Bootstrap server in a Kafka cluster consists of a Kafka host and a Kafka port. The decoder connects to the target (topic) using this Kafka host and Kafka port and fetches the data from the Kafka topic.

Note:

• A target (Kafka topic or tool name) can only have one decoder configured.

- You can assign the target to an undefined value if no decoders are available.
- 12. (Optional) To return to the previous screen, click Back.
- 13. Review the target configuration details and click Save And Publish.

To verify if the configuration was completed successfully, ensure that the **Config Status** column displays **Configured** for the Broadcom ETM Integration.

Task 4. Verify Broadcom ETM Events Received at Decoder

You can analyze the Broadcom ETM events that have been received by the Decoder and verify their accuracy.

To verify the Broadcom ETM Events Received at Decoder

- 1. Log in to the NetWitness Platform.
- 2. Go to **%** (Admin) > Services.
- 3. Select the Packet Decoder service and click > View > Stats.
- 4. Under the Key Stats section, check the values for Capture Rate, Max Capture Rate, and Total Captured packets for the decoder service.

📩 Change Service 🛛 🧕 decoder - Decoder 🔰 Stats 🐵								
decoder - Decoder								
Rate			Service System Info			Host System Info		Physical Drives
Max	241 MbPS		CPU	38%		CPU	42%	
Capture		÷	System Memory	13.9 GB		System Memory	13.9 GB	
Tatal	3.7 Million Packets		Total Memory	15.6 GB		Total Memory	15.6 GB	sda
Captured			Process Memory	774.9 MB		Process Memory	38.5 MB	
Total	0 Packets (0% loss)		Max Process Memory	15.6 GB		Max Process	15.6 GB	
Dropped			Uptime	1 hour and 16 minutes		Memory		
Total	1.8 Million		Status	Ready		Uptime	2 days, 7 hours and 13	
Packets	Packets	1	Running Since	2024-Jan-22 10:41:43		_	minutes	
Begin Time	2024-Jan-22		Current Time	2024-lan-22 11:57:44		Status	Ready	
	10:55:58					Running Since	2024-Jan-20 04:44:22	

Task 5. Verify Events Meta from Broadcom ETM in

Investigate View

To verify Broadcom ETM events, you must first aggregate the Decoder service into the Concentrator and then go to the **Investigate** > **Events** page to view the Broadcom ETM events.

- Add the Decoder Service in the Concentrator
- Verify from the Investigate > Events View

Add the Decoder Service in the Concentrator

- 1. Log in to the NetWitness Platform.
- 2. Go to **%** (Admin) > Services.
- 3. In the Services list, select the Concentrator service.
- 4. Click \diamond \diamond \diamond > View > Config.

The Services Config View of the Concentrator is displayed.

- 5. Select the **Sources** tab.
- Click + and select Available Services.
 The Available Services dialog is displayed.

7. Select the **Decoder** service and click **OK**.

The service authentication dialog box is displayed.

Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

- 8. Enter the Username and Password for the service.
- 9. Click OK.
- 10. Click Apply.

Verify from the Investigate > Events View

- 1. Go to **Investigate** > **Events**.
- 2. Select the Concentrator Service from the Services selection drop-down list.
- 3. Click 🔍 to load the Broadcom ETM events in the Events table.

NETWITNESS Platform Investigate Respond Users Hosts Files Dashboard Reports	👌 🖃 拨 🕐 admin >							
Stevel Queries V 😝 Concentrator V Last 24 Hours V								
Enter a text search with a meta key, operator and value or a query that starts with NOT or any keyword	() 💿 E							
++ 01232024 0844 am	01/24/2024 08:43 am 👔 🛞 ∧							
1.143.0133 Total events for the selected date & time range	Use mouse scroll to zoom							
<u>ด เกม</u> เว้าน อว่าน ออ่าน ออ่าน เจ้าน อง่าน เจ้าน	ам обам							
Events Meta 🕹 × 5,000 Events 🛆 🕅 RSA Threat Analysis 🗸 Download All 🔍 Create Incident 🗸 🕥 caour events	Network Event Details 🗇 🦨 🗙							
E Mela Group 🗸 🖟 Ordering 🗸 🚯 🛛 Collection time TYPE therat category therat sourt_ indicators_ eenang	ETH.DST							
□ 🖗 01/23/2024/0744023.am 🕐	-5% 42:01:64:48:38:01							
	ETH.TYPE 2048							
✓ G Decoder Source (2) Q i 0 00232024090450.9 m	IPSRC IPSRC							
ad 01/23/022409(4402am)								
eccore 1.162/33) logmaria 6/3	IF DST							
✓ g: Service Type (5) Q i □ 01/21/024079402am @	IP.PROTO							
0(0THER] (\$12000-23%) 80[HTTP] (\$1476] \$3[DNS] (4418)	6							
443[551] 11.448] 67 [DH/CP] (0) 0 01/23/3024/09/402.2m	24 CEFFAGS							
✓ _ Device Type (2) Q I □ 01/23/8024090402 am Ø	TCP.SRCPORT							
Control Contro Control Control Control Control Control Control Control Control C								
unknown (222) cistossa (56)	1443 deg							