

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 <https://www.rsa.com/en-us/company/rsa-trademarks>. 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 and 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.

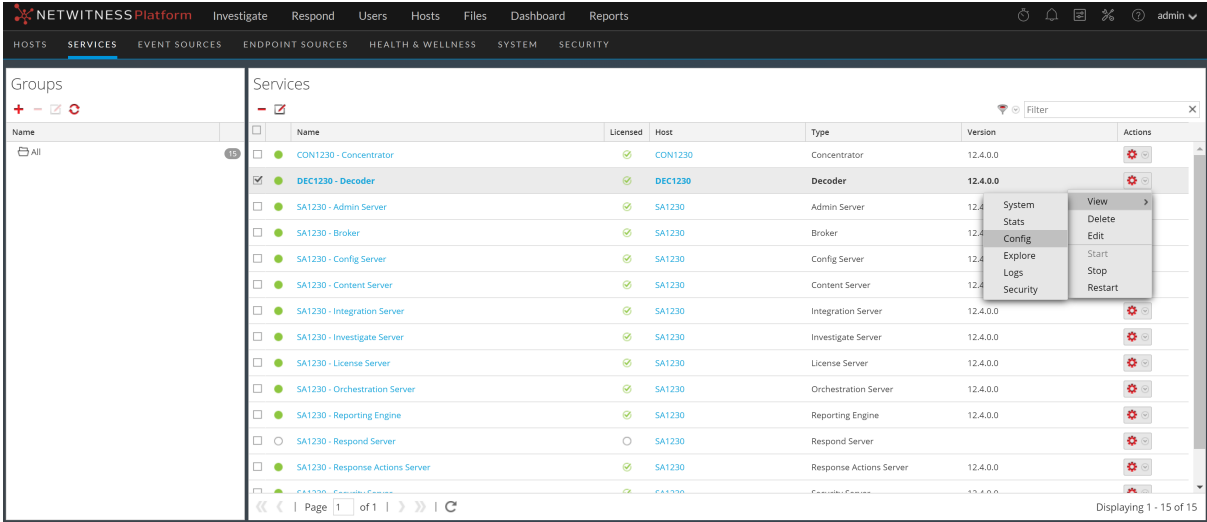
- [Task 1. Map Network Adapter in Decoder for Broadcom ETM Integration](#)
- [Task 2. Create and Publish Policy for Broadcom ETM Integration](#)
- [Task 3. Configure Broadcom ETM Integration from Policy Details View](#)
- [Task 4. Verify Broadcom ETM Events Received at Decoder](#)
- [Task 5. Verify Events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

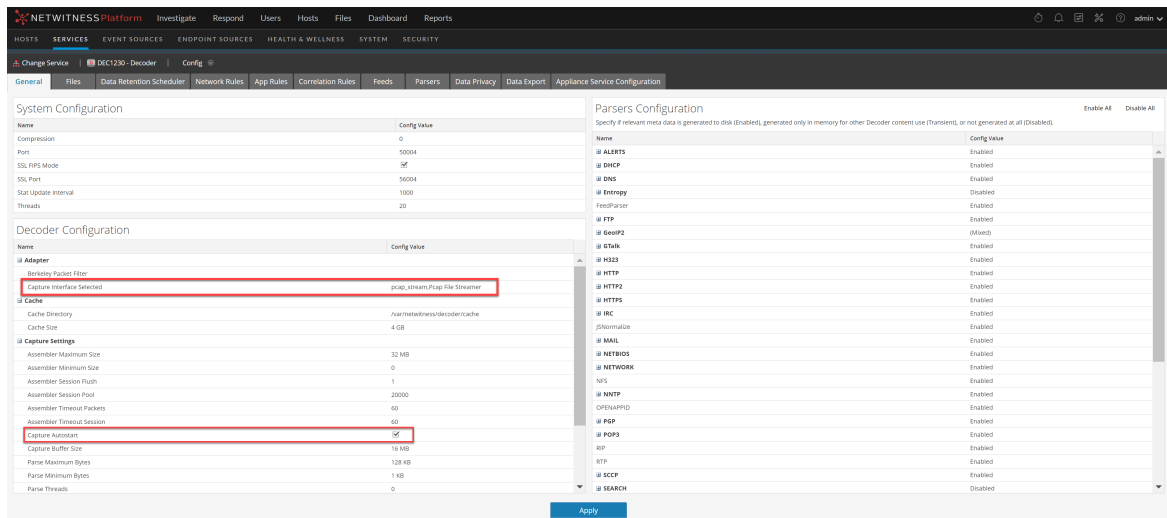
To Map the Network Adapter in Decoder for Broadcom ETM Integration

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



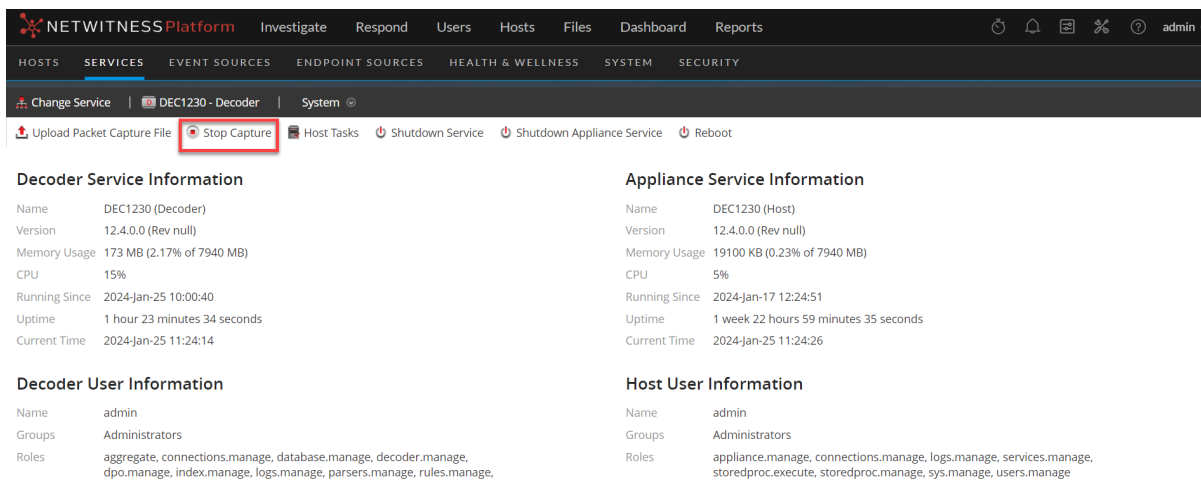
The Configure view for the Decoder service is displayed with the **General** tab open.

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.



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.



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

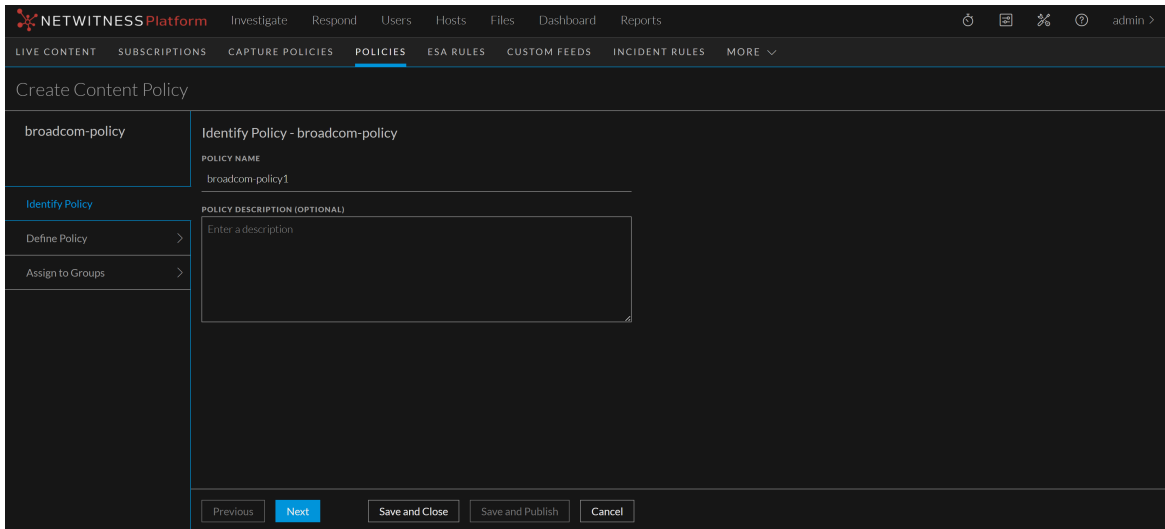
- Ensure that the **Broadcom ETM Integration** plugin is available at the SASE Integration Plugin tab.
- Ensure that the group with one or more decoder services is created.

Supported Hosts

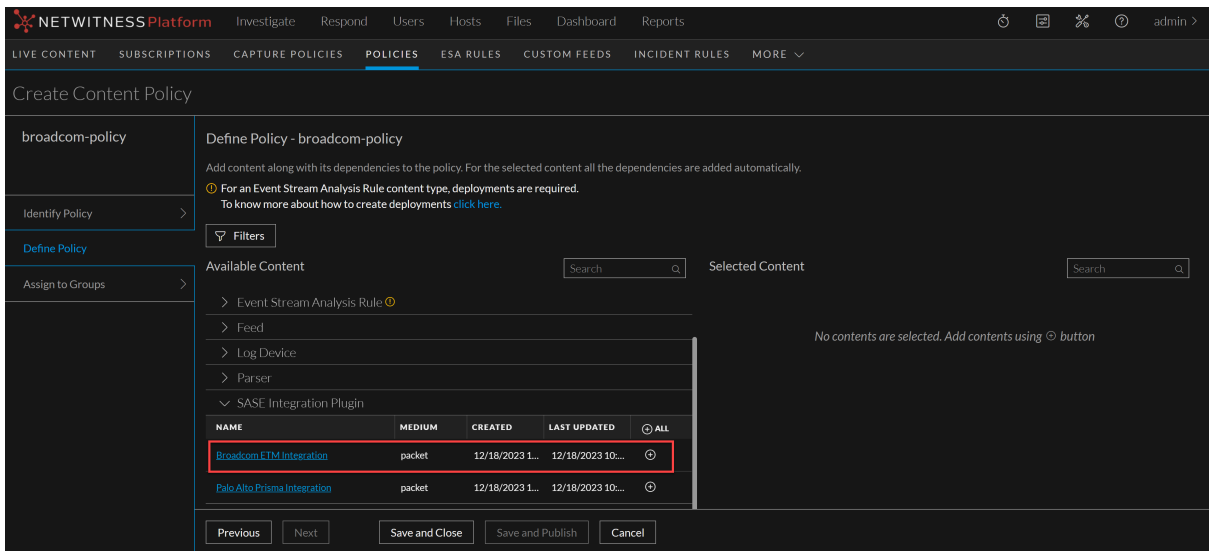
- Packet Decoder
- Packet Hybrid

To create and publish policy for Broadcom ETM Integration

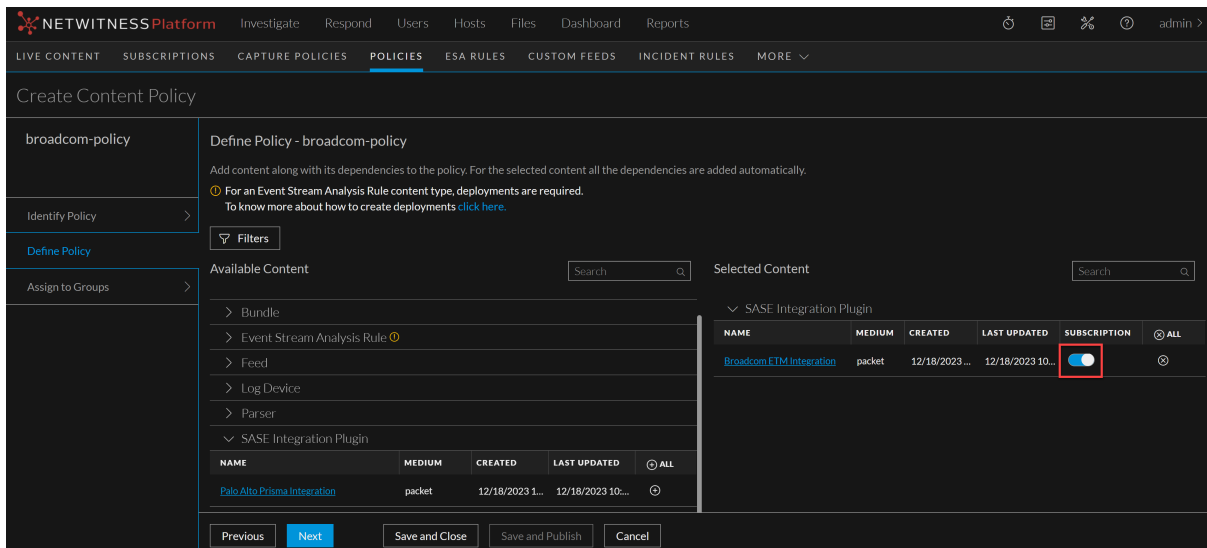
1. Go to  (Configure) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**.
The available policies are displayed.
4. Click + **Create New** to add a new policy.
5. In the **New Policy** panel, do the following:
 - a. Enter a unique policy name.
 - b. (Optional) Enter a description for the policy.



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 **⊕ ALL**.



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

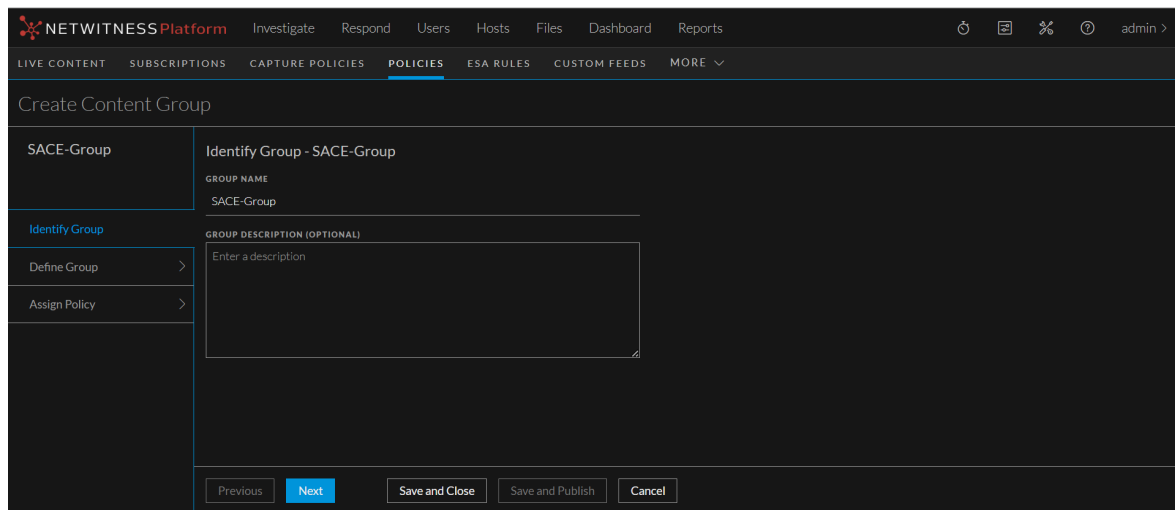


9. Click **Next**.

10. If there are no unassigned groups available, click  to save the policy and redirect you to the **Create New Group** screen.

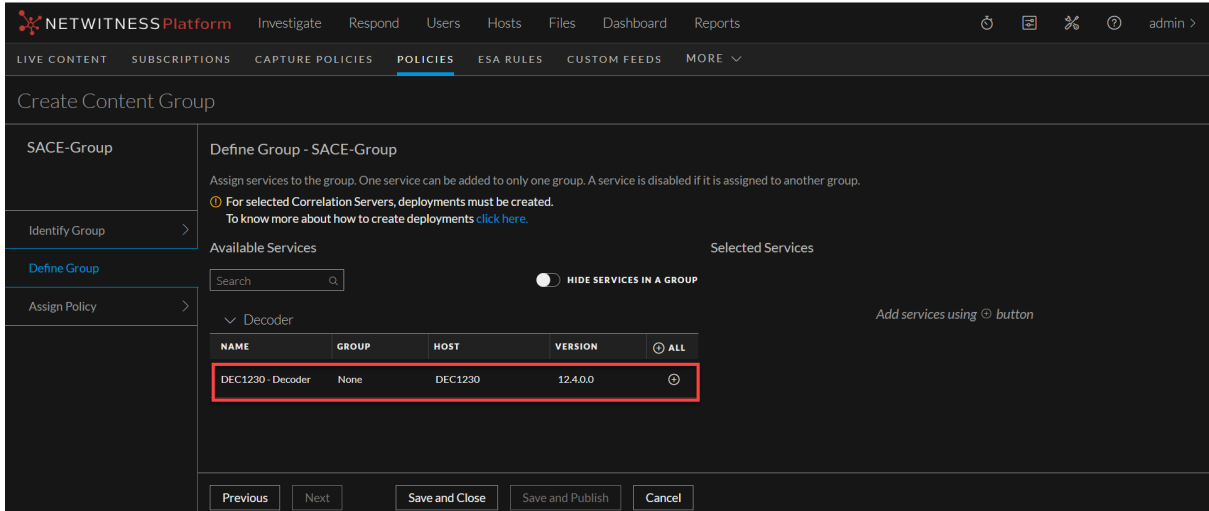
11. In the New Group panel, do the following:

- Enter the name of the group.
- (Optional) Enter the description for the group.



12. Click **Next**.

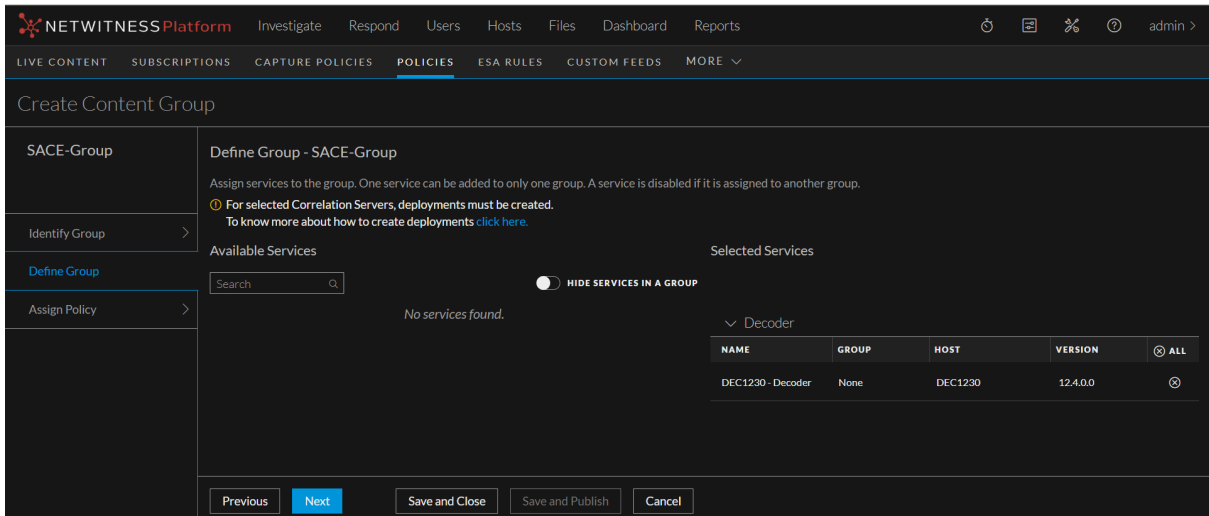
13. In the **Define Group**, click + to assign services to the group.



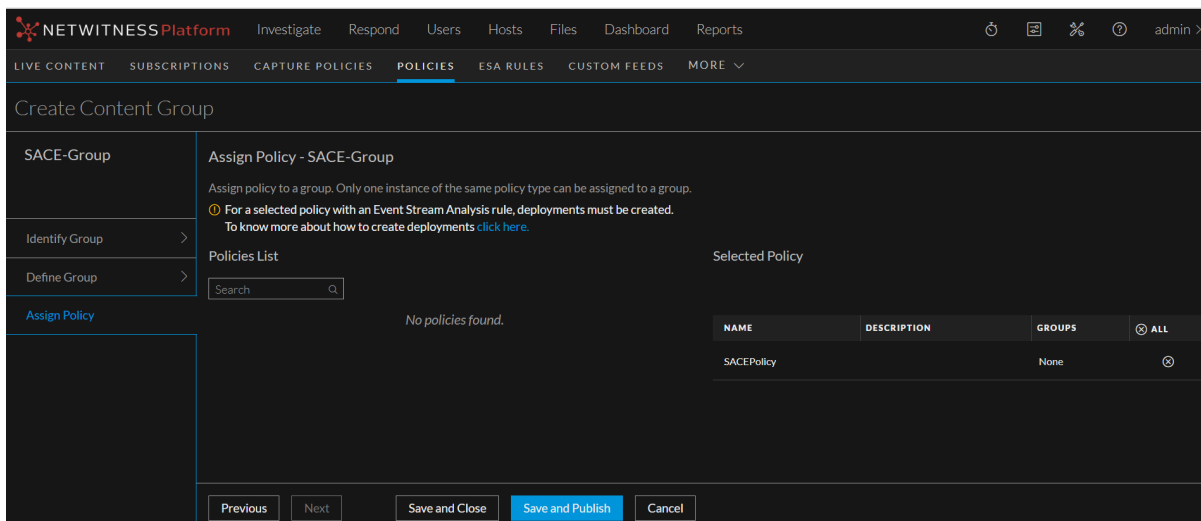
Note:

- 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.

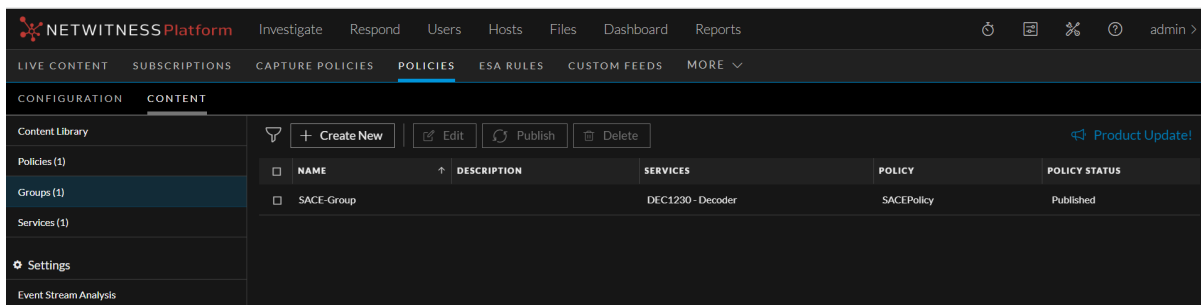
14. Click Next.



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



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



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 [Task 3. Configure Broadcom ETM Integration from Policy Details View](#)

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.

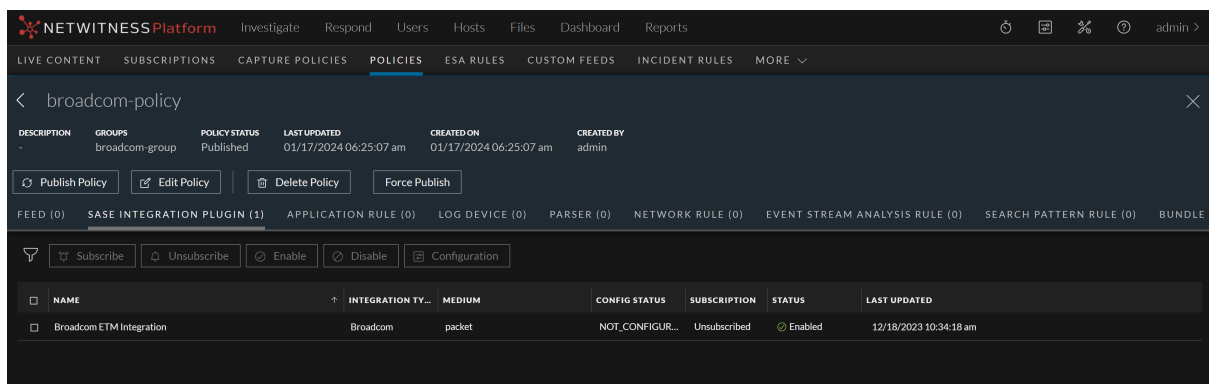
Prerequisites

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.



IMPORTANT: The **Configuration** button will be disabled when the policy status is **Unpublished**, **Failed**, or **N/A**. For more information, see [Filter Policies](#).

6. Select the **Broadcom ETM Integration** type and click  **Configuration**.
The Configuration dialog is displayed.

The screenshot shows a configuration window titled "Configuration" with a close button (X) in the top right corner. The main heading is "Broadcom ETM Integration". Below the heading is a descriptive text: "Configure the Broadcom ETM SASE integration type to send network data to NetWitness." There are two input fields: "REQUEST URL*" and "AUTH TOKEN*", both with asterisks indicating they are required. The "REQUEST URL*" field contains the text "https:" followed by a blurred area and "ig". Below the input fields is a "Test connection" button. At the bottom right of the dialog are "Cancel" and "Next" buttons.

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 SERVERS	DECODER
tool1_name	gusdm.kafka...	decoder - De...
tool2_name	gusdm.kafka...	decoder - De...
tool3_name	gusdm.kafka...	decoder - De...

Cancel
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**.

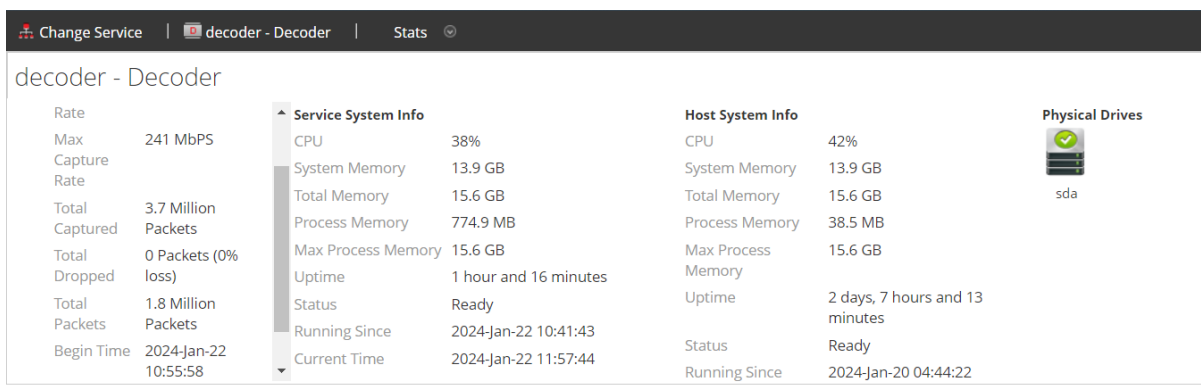
To verify if the configuration was completed successfully, ensure that the **Config Status** column displays **Configured** for the Broadcom ETM Integration.


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.






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

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  > **View** > **Config**.
The Services Config View of the Concentrator is displayed.
5. Select the **Sources** tab.
6. Click  and select Available Services.
The Available Services dialog is displayed.


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

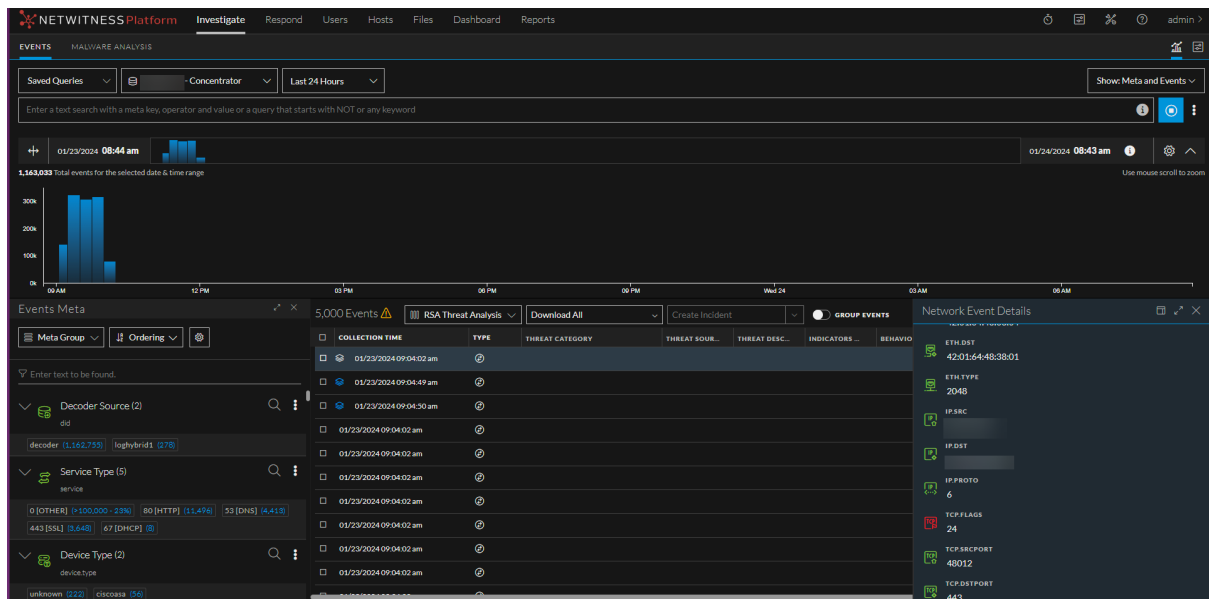
The service authentication dialog box is displayed.

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.



The screenshot displays the NetWitness Platform interface in the 'Investigate' section, specifically the 'Events' view. The top navigation bar includes 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. The main area shows a search bar and a bar chart indicating 1,163,033 total events for the selected date and time range. Below the chart is a table of events with columns for 'COLLECTION TIME', 'TYPE', 'THREAT CATEGORY', 'THREAT SOUR...', 'THREAT DESC...', 'INDICATORS', and 'BEHAVIO'. The 'Events Meta' panel on the left shows filters for 'Decoder Source (2)', 'Service Type (5)', and 'Device Type (2)'. The 'Network Event Details' panel on the right shows fields like 'ETHL.DST', 'ETHL.TYPE', 'IP.SRC', 'IP.DST', 'IP.PROTO', 'TCP.FLAGS', 'TCP.SRCPORT', and 'TCP.DSTPORT'.