NetWitness® Platform

Version 12.4.0.0

Centralized Content Management

NETWITNESS

Platform

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

License Agreement

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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/.

April, 2024

Contents

About Policy-based Centralized Content Management (CCM)

Legacy content management involves deploying and managing content in multiple places in the UI.

- **Live Content UI**: Located under the Configuration interface, this allows a “push” deployment of Live content to one or more services, but does not provide any management of content once it is deployed
- **Service Config UI**: Located under **Admin > Services > View Config**, this UI enables you to view, edit or delete content on individual services.

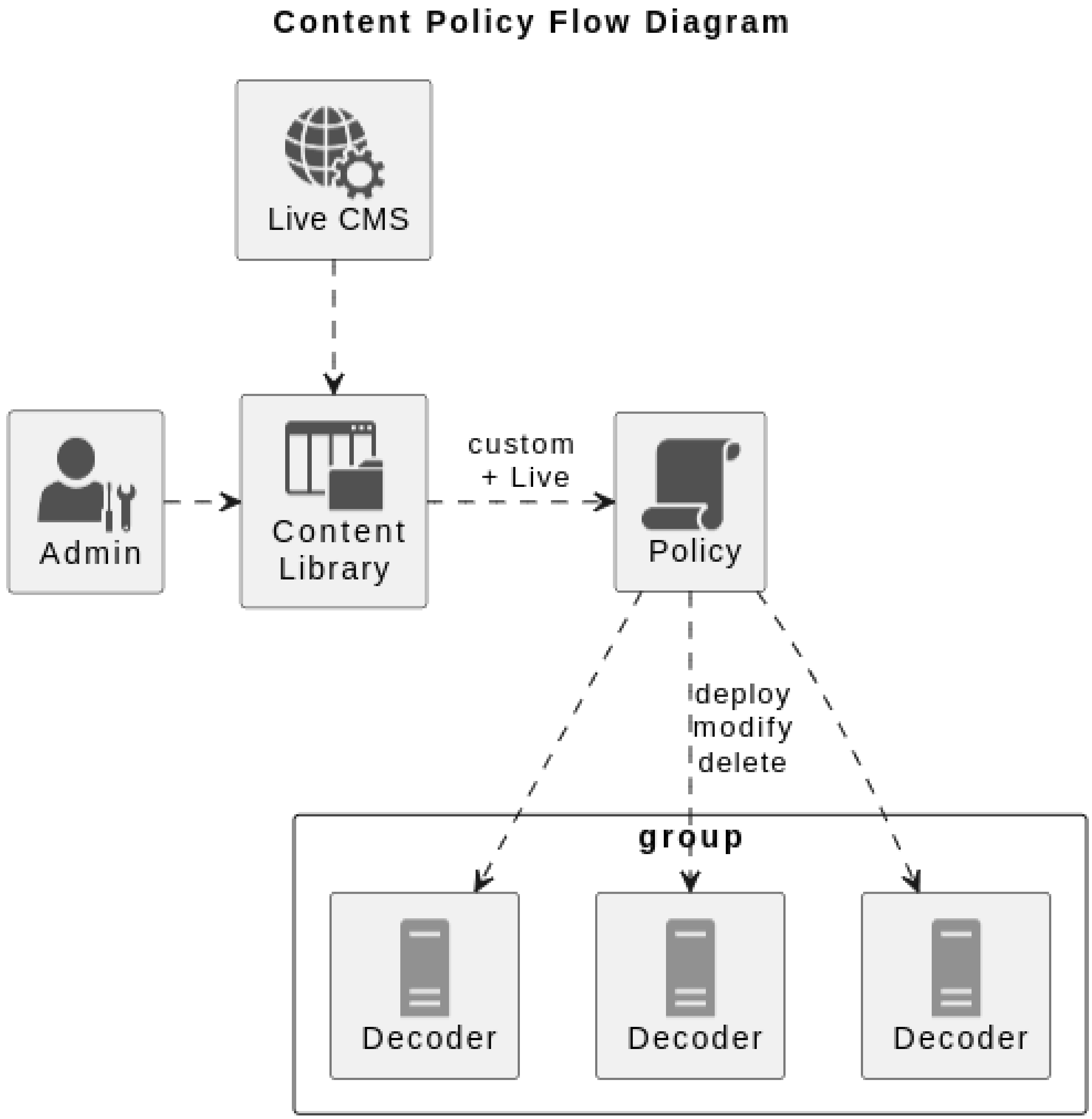
Policy-based Centralized Content Management (CCM) is a unified approach to find, deploy, and manage content through the entire life cycle based on policies that can be assigned to groups of devices. It is a single location to view, modify and manage the content deployed across all services in the environment.

This approach consists of three elements:

- Groups: A collection of NetWitness services (such as Decoders, Log Decoders, and Correlation Servers etc.) to assign and manage content.
- Content Policies: A container of content and subscription settings used to assign and manage content within a Group.
- Content Library: A local repository of content which resides on the Admin Server and is used to assign content to policies. This includes both Live and Custom content.

The Content Library contains Live content (synchronized with the Live CMS) and any custom content you create or import. To deploy, remove or manage content on your services, content is assigned from the Content Library to a Content Policy. Once that content policy is assigned to a group and Published, the content changes are put into effect on the services within the group.

Workflow



Benefits

Benefits of Policy-based Centralized Content Management:

- Add or remove content without repeating the process on each service.
- Add content from RSA Live or add your custom content into a single content repository. You can add content from this repository to a policy.
- Add a new service to an existing group to automatically deploy all necessary content.
- One-click management of subscriptions and automatic updates
- Provides highly responsive and updated UI for browsing RSA Live content that can help you with the following:
  - View Live content along with your content policies and click ⊕ to add content from Live.
  - Seamlessly view Live content along with your custom content.
- Create and upload content to the Content Library easily by:
  - Importing log parsers as a zip file instead of converting to ".envision" format.
  - Cloning existing Application Rules and Network Rules.
- Switch services between legacy Content Management UI and the new Centralized Content Management via Groups and Policies using the "toggle" feature. This can prevent content being mistakenly added or modified outside of a Policy, causing an out-of-sync issue.
- Create, modify and publish policies and manage custom content in the Content Library even without an internet connection.
- Find content, policies or groups of interest easily by using the **Filtering** capability of the UI.
- Receives meta key and operator suggestions while creating Application Rule and Network Rule conditions. This eases the creation of error-free rules.
- Manage ESA content and handle multiple deployments seamlessly using Policy.
- Seamlessly view ESA Live content along with your own custom content.
- Add and manage ESA Correlation servers as part of groups.
- Manage all the data sources for the ESA Correlation servers from the **Settings** > **Event Stream Analysis** > **Data Sources** page seamlessly.

IMPORTANT: It is recommended not to use the Centralized Content Management and Service Config page or Live Content page simultaneously for managing the content. Using the Service Config UI to add or modify content can cause the content to become out-of-sync with the Content Policy.

Note: If Policy-based Centralized Content Management is enabled for a service, then the Policy-based Centralized Content Management enabled services will be disabled in Live content UI and user will not be able to manage content of these services from Service Config page as Service Config page becomes read only and no actions except 'export' can be performed from Service Config page.

Enable or Disable CCM for All or Individual Decoder Services

You can choose to use CCM to manage content for selected services or for all services.

When CCM is Enabled:

- The service config page is read-only. Only **Export** button is enabled in service config page to export content.
- Content cannot be deployed to CCM enabled services through the Live Content UI.
- Content for all CCM enabled services can be managed through the Content Policies and the Content Library.
- Content subscription from CCM overrides content subscription from **(CONFIGURE) > Subscriptions** page.

When CCM is Disabled:

- Content can be deployed from Live Content UI.
- The content of the service can be managed from service config page. Any changes made through the Service Config page does not reflect in the content policy.
- The service is disabled in the Policy or Group page of CCM and the policy status changes to **Partial**. The policy can be published with a disabled service. However, the policy state always remains **Partial**. Publishing a policy will affect only the services that are enabled for CCM.

  > **Note:** When a service, which is part of a group, is added back to CCM, the policy status changes to “Unpublished”.

Enable or Disable CCM for All Decoder Services

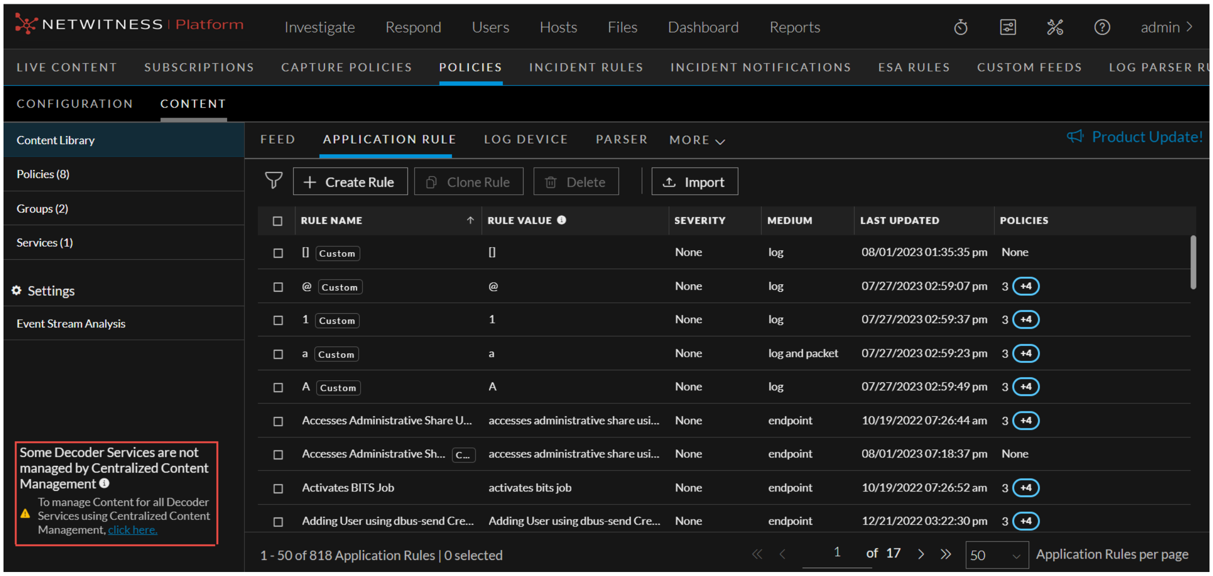
From 12.2 version onwards, a CCM toggle is introduced to enable or disable CCM for all 12.0+ Decoder Services. The toggle is available on the UI.

To enable or disable CCM for all Decoder Services on the UI

Scenario 1: Some Decoder Services are Managed by CCM

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. Click either **Content Library**, **Policies**, **Groups** or **Services**.

   The respective screens are displayed. On these screens, on the left bottom corner, the message on managing the content is displayed.



□	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
□	[] Custom	[]	None	log	08/01/2023 01:35:35 pm	None
□	@ Custom	@	None	log	07/27/2023 02:59:07 pm	3 +4
□	1 Custom	1	None	log	07/27/2023 02:59:37 pm	3 +4
□	a Custom	a	None	log and packet	07/27/2023 02:59:23 pm	3 +4
□	A Custom	A	None	log	07/27/2023 02:59:49 pm	3 +4
□	Accesses Administrative Share U...	accesses administrative share usi...	None	endpoint	10/19/2022 07:26:44 am	3 +4
□	Accesses Administrative Sh... C...	accesses administrative share usi...	None	endpoint	08/01/2023 07:18:37 pm	None
□	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
□	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

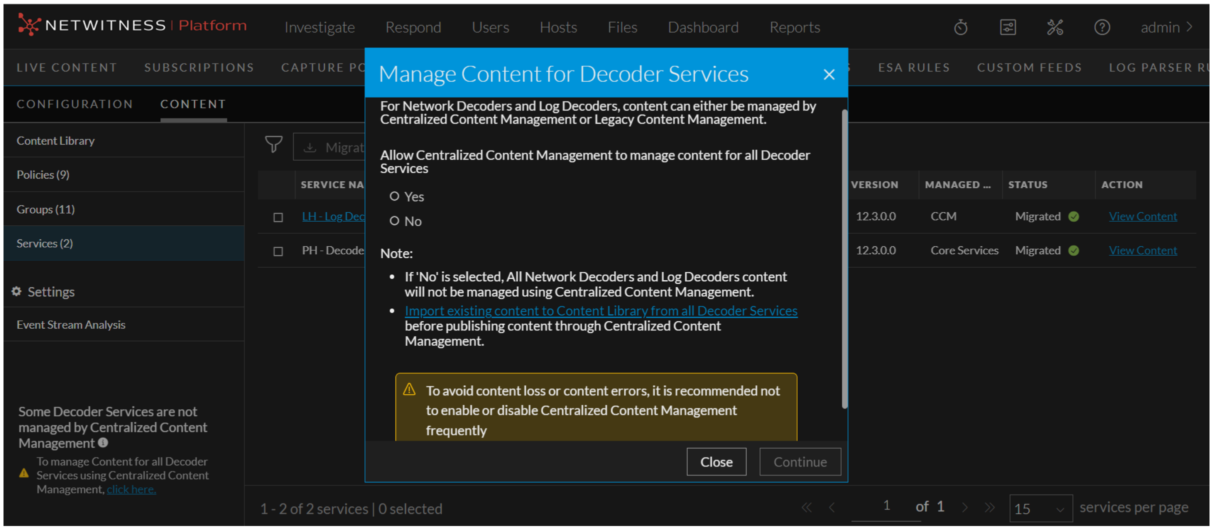
1 - 50 of 818 Application Rules | 0 selected   1 of 17   50 Application Rules per page

Some Decoder Services are not managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

4. If the NetWitness platform consists of only few Decoders managed by CCM, then the message "Some Decoder Services are managed by Centralized Content Management" is diplayed. In such a case, you can choose to either manage all the Decoder Services by CCM or not to manage any Decoder Services by CCM by clicking **click here**.

   The **Manage Content for Decoder Services** pop-up window is displayed.



□	SERVICE NA	VERSION	MANAGED ...	STATUS	ACTION
□	LH - Log Dec	12.3.0.0	CCM	Migrated	View Content
□	PH - Decode	12.3.0.0	Core Services	Migrated	View Content

1 - 2 of 2 services | 0 selected   1 of 1   15 services per page

Some Decoder Services are not managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Manage Content for Decoder Services

For Network Decoders and Log Decoders, content can either be managed by Centralized Content Management or Legacy Content Management.

Allow Centralized Content Management to manage content for all Decoder Services

○ Yes
○ No

Note:

- If 'No' is selected, All Network Decoders and Log Decoders content will not be managed using Centralized Content Management.
- Import existing content to Content Library from all Decoder Services before publishing content through Centralized Content Management.

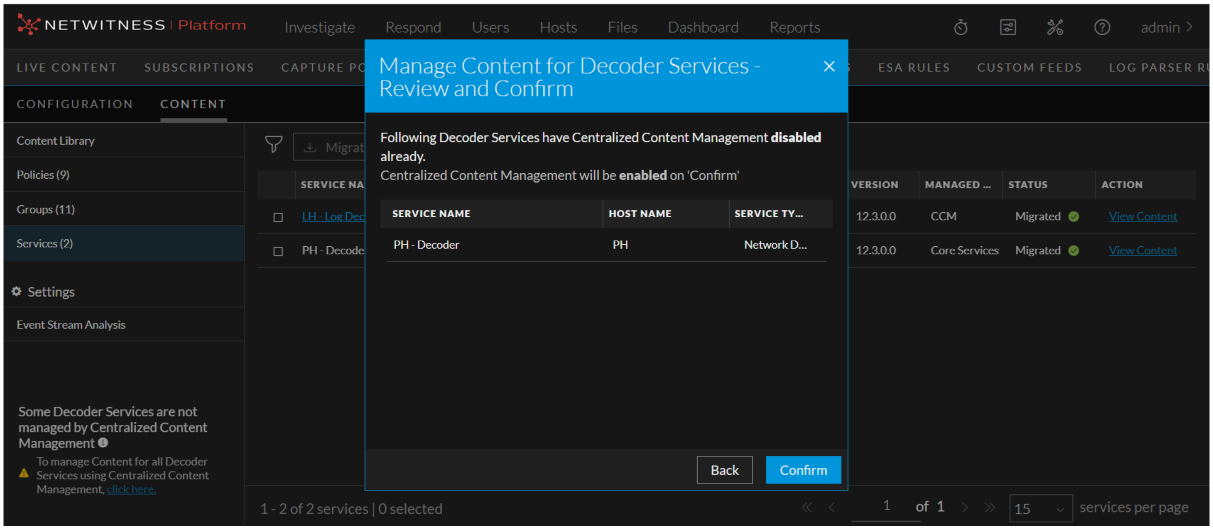
To avoid content loss or content errors, it is recommended not to enable or disable Centralized Content Management frequently

Close   Continue

5. On the **Manage Content for Decoder Services** pop-up window, click **Yes** for **Allow Centralized Content Management to manage content for all Decoder Services** to enable CCM for all Decoder Services. Click **No** to disable CCM for all Decoder Services.

   Note: Read the notes on the pop-up window before clicking on **Continue**.

6. Click **Continue**. The **Manage Content for Decoder Services - Review and Confirm** screen is displayed.



Manage Content for Decoder Services - Review and Confirm

Following Decoder Services have Centralized Content Management **disabled** already.
Centralized Content Management will be **enabled** on 'Confirm'

SERVICE NAME	HOST NAME	SERVICE TY...
PH - Decoder	PH	Network D...

SERVICE NA	VERSION	MANAGED ...	STATUS	ACTION
LH - Log Dec	12.3.0.0	CCM	Migrated	View Content
PH - Decode	12.3.0.0	Core Services	Migrated	View Content

Some Decoder Services are not managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 2 of 2 services | 0 selected   1 of 1   15 services per page

7. Click **Confirm** to review and confirm the services which will be enabled or disabled based on the selected option. Else, click **Back** to go back to the previous screen.

8. The success message is displayed on the screen.

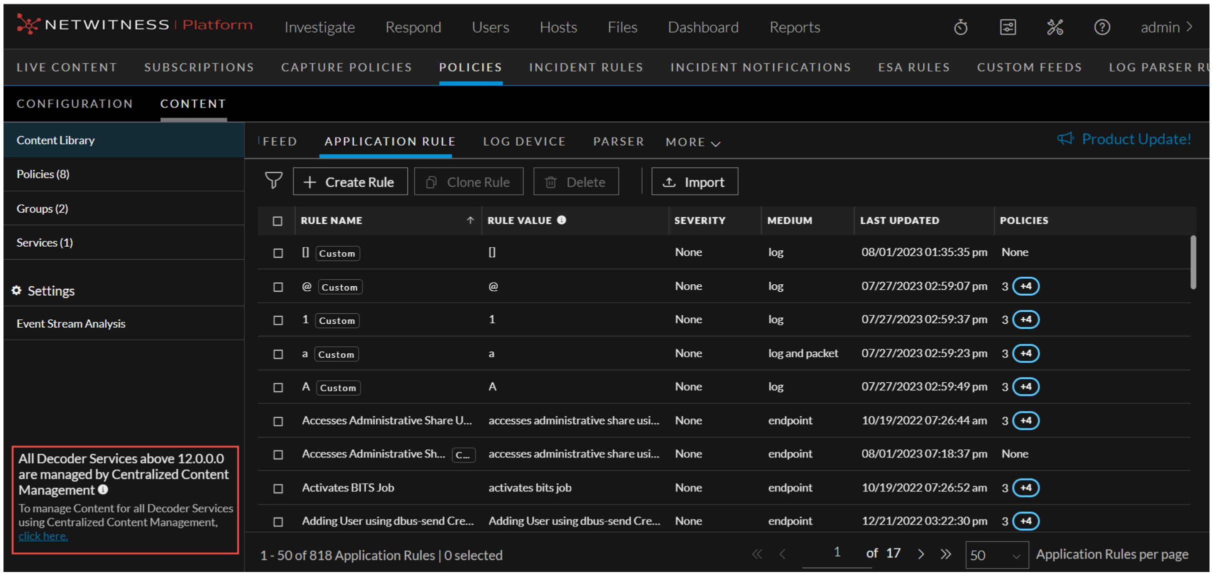
Scenario 2: All Decoder Services are Managed by CCM

1. Go to **(CONFIGURE)** > **Policies**.

2. In the policies panel, click **Content**.

3. Click either **Content Library**, **Policies**, **Groups** or **Services**.

4. The respective screens are displayed. On these screens, on the left bottom corner, the message on managing the content is displayed.



□	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
□	[] Custom	[]	None	log	08/01/2023 01:35:35 pm	None
□	@ Custom	@	None	log	07/27/2023 02:59:07 pm	3 +4
□	1 Custom	1	None	log	07/27/2023 02:59:37 pm	3 +4
□	a Custom	a	None	log and packet	07/27/2023 02:59:23 pm	3 +4
□	A Custom	A	None	log	07/27/2023 02:59:49 pm	3 +4
□	Accesses Administrative Share U...	accesses administrative share usi...	None	endpoint	10/19/2022 07:26:44 am	3 +4
□	Accesses Administrative Sh... C...	accesses administrative share usi...	None	endpoint	08/01/2023 07:18:37 pm	None
□	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
□	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

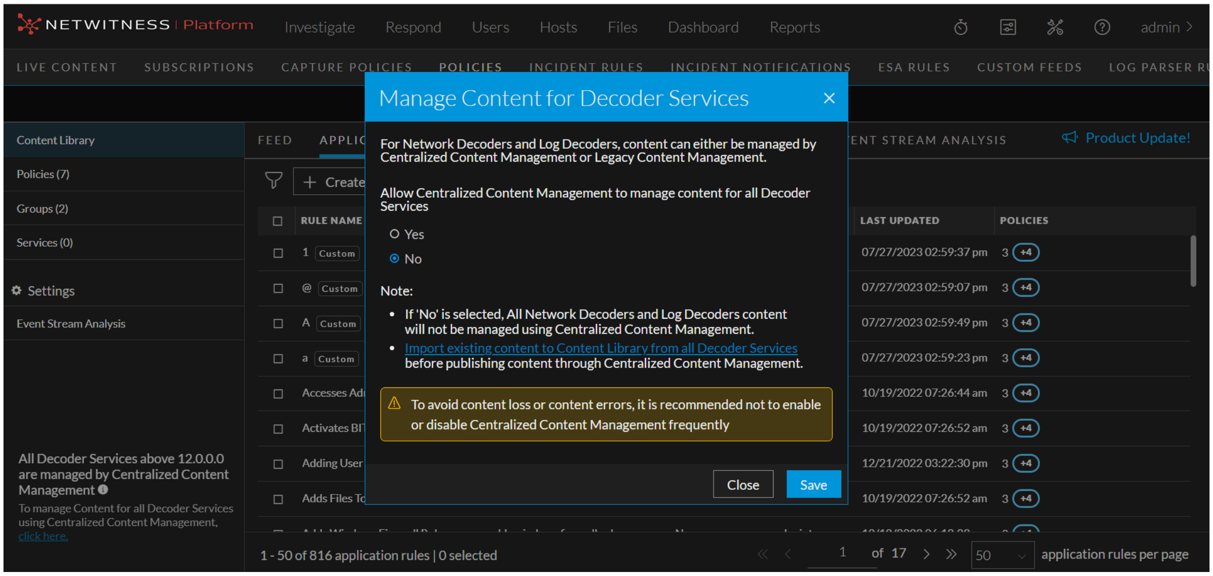
All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 50 of 818 Application Rules | 0 selected   1 of 17   50 Application Rules per page

5. 5. If the NetWitness platform consists of all Decoders managed by CCM, then the message "All Decoder Services above 12.0.0.0 are managed by Centralized Content Management" is displayed. In such a case, you can choose to not manage any Decoder Services by CCM by clicking **click here**.

6. The **Manage Content for Decoder Services** pop-up window is displayed.



Manage Content for Decoder Services

For Network Decoders and Log Decoders, content can either be managed by Centralized Content Management or Legacy Content Management.

Allow Centralized Content Management to manage content for all Decoder Services

○ Yes

● No

Note:

- If 'No' is selected, All Network Decoders and Log Decoders content will not be managed using Centralized Content Management.
- Import existing content to Content Library from all Decoder Services before publishing content through Centralized Content Management.

⚠ To avoid content loss or content errors, it is recommended not to enable or disable Centralized Content Management frequently

Close Save

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 50 of 816 application rules | 0 selected

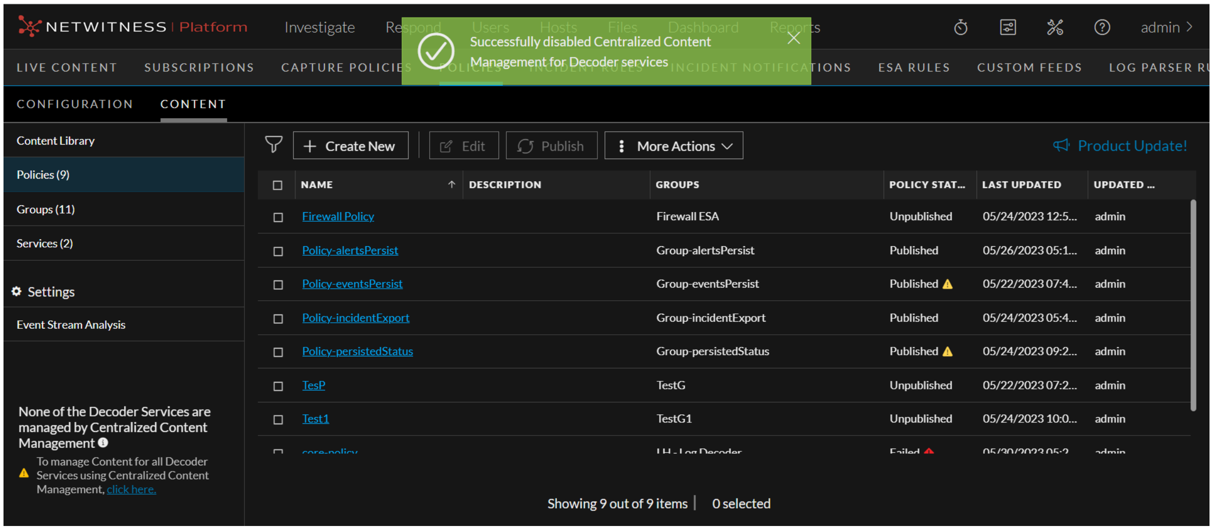
1 of 17 50 application rules per page

7. On the **Manage Content for Decoder Services** pop-up window, click **No** for **Allow Centralized Content Management to manage content for all Decoder Services** to disable CCM for all Decoder Services.

Note:
- The **Yes** option is selected by default.
- Read the notes on the pop-up window before clicking on **Save**.

8. Click **Save**. The success message is displayed on the screen.

Note: The **Save** option is enabled only when you select **No**.



Successfully disabled Centralized Content Management for Decoder services

NAME	DESCRIPTION	GROUPS	POLICY STAT...	LAST UPDATED	UPDATED ...
Firewall Policy		Firewall ESA	Unpublished	05/24/2023 12:5...	admin
Policy-alertsPersist		Group-alertsPersist	Published	05/26/2023 05:1...	admin
Policy-eventsPersist		Group-eventsPersist	Published ⚠	05/22/2023 07:4...	admin
Policy-incidentExport		Group-incidentExport	Published	05/24/2023 05:4...	admin
Policy-persistedStatus		Group-persistedStatus	Published ⚠	05/24/2023 09:2...	admin
TesP		TestG	Unpublished	05/22/2023 07:2...	admin
Test1		TestG1	Unpublished	05/24/2023 10:0...	admin
core-policy		LH - Log Decoder	Failed ⚠	05/30/2023 05:2	admin

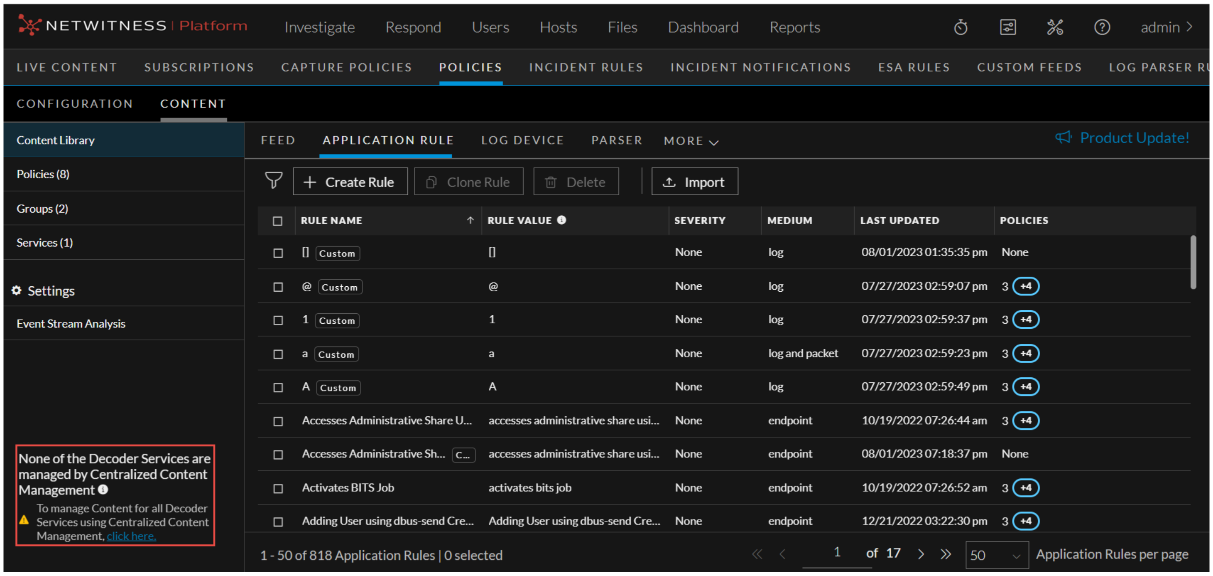
None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 9 out of 9 items | 0 selected

Scenario 3: None of the Decoder Services are Managed by CCM

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Click either **Content Library**, **Policies**, **Groups** or **Services**.
4. The respective screens are displayed. On these screens, on the left bottom corner, the message on managing the content is displayed.



None of the Decoder Services are managed by Centralized Content Management

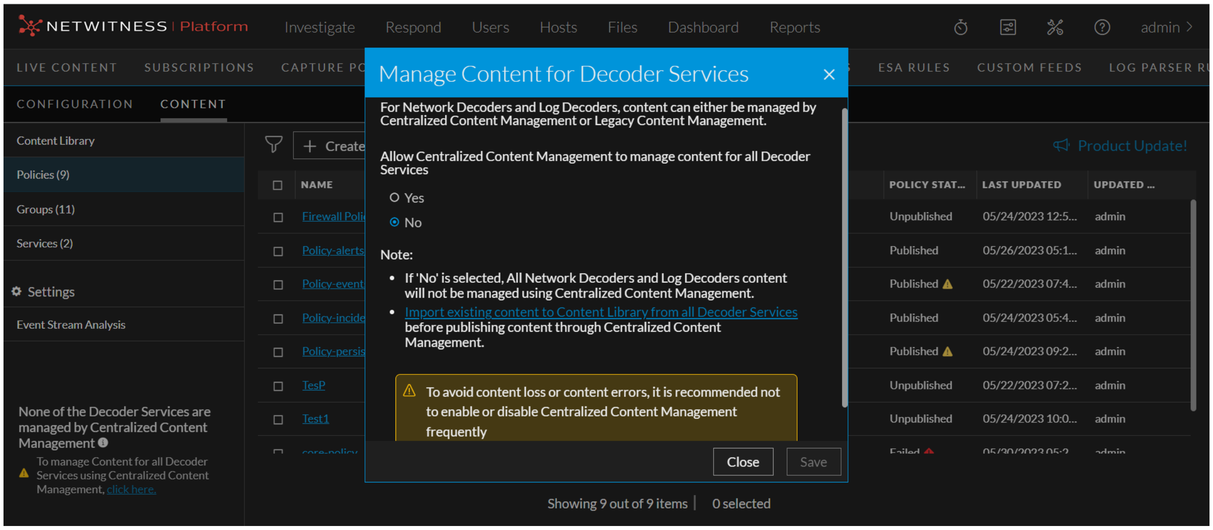
To manage Content for all Decoder Services using Centralized Content Management, click here.

☐	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
☐	[] Custom	[]	None	log	08/01/2023 01:35:35 pm	None
☐	@ Custom	@	None	log	07/27/2023 02:59:07 pm	3 +4
☐	1 Custom	1	None	log	07/27/2023 02:59:37 pm	3 +4
☐	a Custom	a	None	log and packet	07/27/2023 02:59:23 pm	3 +4
☐	A Custom	A	None	log	07/27/2023 02:59:49 pm	3 +4
☐	Accesses Administrative Share U...	accesses administrative share usi...	None	endpoint	10/19/2022 07:26:44 am	3 +4
☐	Accesses Administrative Sh... C...	accesses administrative share usi...	None	endpoint	08/01/2023 07:18:37 pm	None
☐	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
☐	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

1 - 50 of 818 Application Rules | 0 selected

1 of 17 | 50 Application Rules per page

5. If the NetWitness platform does not consist of any Decoders managed by CCM, then the message "None of the Decoder Services are managed by Centralized Content Management" is displayed. In such a case, you can choose to manage all Decoder Services by CCM by clicking **click here**.
6. The **Manage Content for Decoder Services** pop-up window is displayed.



None of the Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Manage Content for Decoder Services

For Network Decoders and Log Decoders, content can either be managed by Centralized Content Management or Legacy Content Management.

Allow Centralized Content Management to manage content for all Decoder Services

○ Yes

● No

Note:

- If 'No' is selected, All Network Decoders and Log Decoders content will not be managed using Centralized Content Management.
- Import existing content to Content Library from all Decoder Services before publishing content through Centralized Content Management.

To avoid content loss or content errors, it is recommended not to enable or disable Centralized Content Management frequently

Close Save

Showing 9 out of 9 items | 0 selected

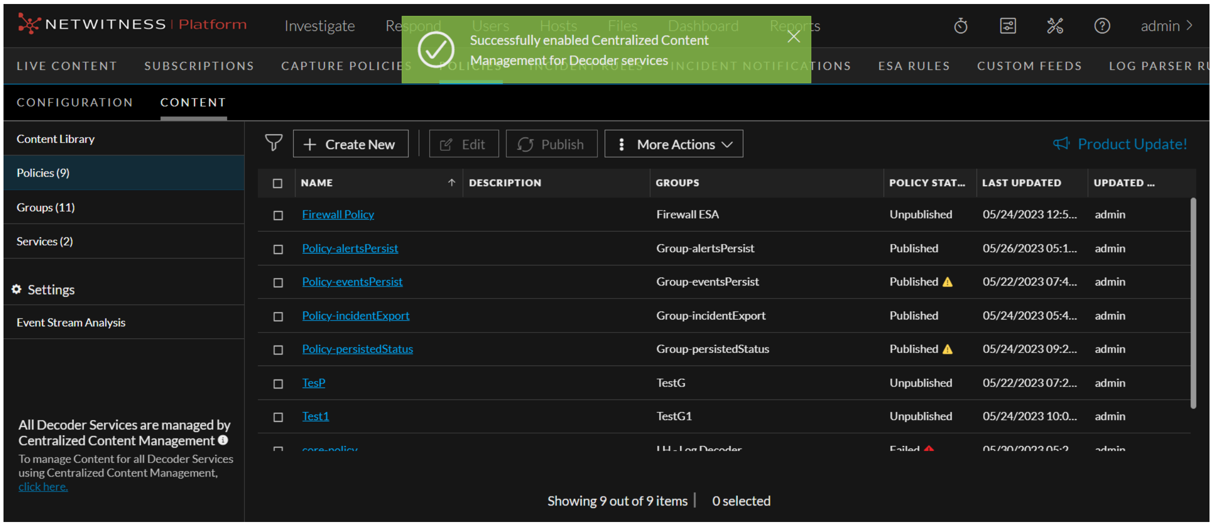
7. On the **Manage Content for Decoder Services** pop-up window, click **Yes** for **Allow Centralized Content Management to manage content for all Decoder Services** to enable CCM for all Decoder Services.

> **Note:**
> - The **No** option is selected by default.
> - Read the notes on the pop-up window before clicking on **Save**.

8. Click **Save**. The success message is displayed on the screen.

9.

> **Note:** The **Save** option is enabled only when you select **Yes**.



Successfully enabled Centralized Content Management for Decoder services

□	NAME	DESCRIPTION	GROUPS	POLICY STAT...	LAST UPDATED	UPDATED ...
□	Firewall Policy		Firewall ESA	Unpublished	05/24/2023 12:5...	admin
□	Policy-alertsPersist		Group-alertsPersist	Published	05/26/2023 05:1...	admin
□	Policy-eventsPersist		Group-eventsPersist	Published ⚠	05/22/2023 07:4...	admin
□	Policy-incidentExport		Group-incidentExport	Published	05/24/2023 05:4...	admin
□	Policy-persistedStatus		Group-persistedStatus	Published ⚠	05/24/2023 09:2...	admin
□	TesP		TestG	Unpublished	05/22/2023 07:2...	admin
□	Test1		TestG1	Unpublished	05/24/2023 10:0...	admin
□	core-policy		LH - Log Decoder	Failed ▲	05/30/2023 05:2	admin

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 9 out of 9 items | 0 selected

Enable or Disable CCM for Individual Decoder Services

To enable or disable CCM for individual Decoder services, see Enable or Disable CCM for Individual Decoder Services *topic under* Manage Services*.*

Manage Content Library

This section contains:

Migrate Content from Core Services to Content Library

The customers who want to use Centralized Content Management, and if their content is already deployed, a migration process is required.

The following types of content can be migrated from Core Services:

- Application Rule
- Network Rule
- Log Device
- Live Feeds
- LUA Parser

Note:
- When the user upgrades a Decoder or Log Decoder from 11.x, 12.0 or 12.1 version to 12.1.1 or later version, a back up of all the content is created automatically. Backup file will be available on Core Services' host under the following path:
For Log Decoder - `/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar`
For Network Decoder - `/var/netwitness/decoder/decoder_backupcontent_ccm.tar`
- When migrating content from two Decoders that have two different types of Custom or Live Base Parser associated with same Custom or Live Base Parser, both the Custom Parsers are added to Content Library. Th association inside the Policy will be with the most recently migrated Custom Parser.
- Within a migrated Policy, a Custom Parser will have only one Custom or Live Base Parser associated with it.
- Migrated content version will be in the Policy, if as part of migration, the Policy is auto created. If you remove this content, you cannot add the old version of the content back.

For steps on how to migrate content from Core Services to Content Library, see Migrate Content from Service under Manage Services.

Import Content to Content Library

Before the custom content can be used in policies, it must be imported to the Content Library.

To export Application Rules or Network Rules from Legacy UI

1. Go to **(Admin)** > **Services**.
2. Go to Config view of the service where application rule or network rule is deployed.
3. Click either the **Application Rule** or the **Network Rule** tab.

   Note: The **Network Rule** tab is only available for **Network Decoder** services.

4. Select the content to migrate.
5. Click **Export** to export the selected content or click **All** to export all the content.

   The following table lists the supported file types and file extensions for Application Rules and Network Rules:

Content	Supported File Types	Supported File Extensions
Application Rules	**.NWR**	NA
Network Rules	**.NWR**	NA

To export Feeds, LUA Parsers, or Log Devices

The content file locations are as given below:

- Feeds content file location: /etc/netwitness/ng/feeds
- Lua Parsers content file location: /etc/netwitness/ng/parsers
- Log Devices content file location: /etc/netwitness/ng/envision/etc/devices

You can upload the files which are copied locally from these locations and import these files to Content Library.

The following table lists the supported file types and file extensions for Log Devices, LUA Parsers and Feeds:

Content	Supported File Types	Supported File Extensions
Feeds	**.zip**	**.feed** and **.token**
Log Devices	**.envision**, **.zip**, **.xml** **Note:** - The zip file should have a root folder. The root folder should contain the 'N' folders for 'N' number of content. The 'N' folder names should be the content names. The 'N' folders, will contain the respective xml files. - You can upload a maximum of 10 xml files at once. - You can upload base parsers as well as custom parser at once. - If you are importing a file which has both base and custom content, the base and custom content files are separated after importing them. - - The custom log parser naming convention should be '<base>msg-custom.xml'. - The base content name in Content Library will be the display name mentioned in the xml file. - The custom content name in Content Library will be the 'displayname-custom'. - While importing extension of a Base Parser, when multiple flavours of a Base Parser are present in Content Library, the extension is associated to the first Base Parser that is found.	NA
LUA Parsers	**.zip**	**.luax**, **.lua** and **.flextoken**

Note: Any imported content will be treated as custom content. If imported content has the same name as existing Live content, then it must be renamed upon import. Custom content with the same name can be overwritten.

To create .envision files

1. Keep all the Log Devices in a root folder in your local drive. For example, "logDevices".
2. From the command prompt, run the python script specified in the NetWitness Community portal with input argument as the path of the above folder.

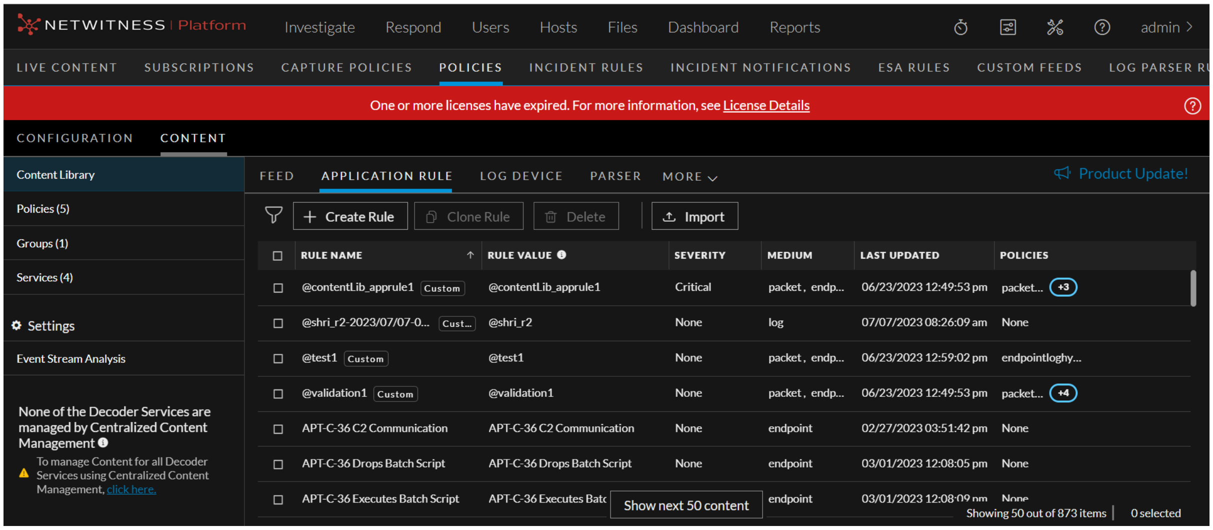
   Note: The command to run the python script is "python3 pythonscriptname.py inputArg".
3. Once you run the script, a new zip named "nw_content_logDevices.zip" is created. This zip file will contain all the envision files.

IMPORTANT: All actions except 'Export' are disabled for Application Rules, Network Rules, Feeds, LUA Parsers and Log Devices from Service Config page for all core services if the service is managed by Policy-based Centralized Content Management.

To import content to Content Library

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Depending upon the type of content to be imported, click the following tabs:
   - **Application Rule**
   - **Network Rule**
   - **Parser**
   - **Feeds**
   - **Log Devices**

   Note: The name of the application rule or network rule to be imported should not be same as existing rule name.



One or more licenses have expired. For more information, see License Details

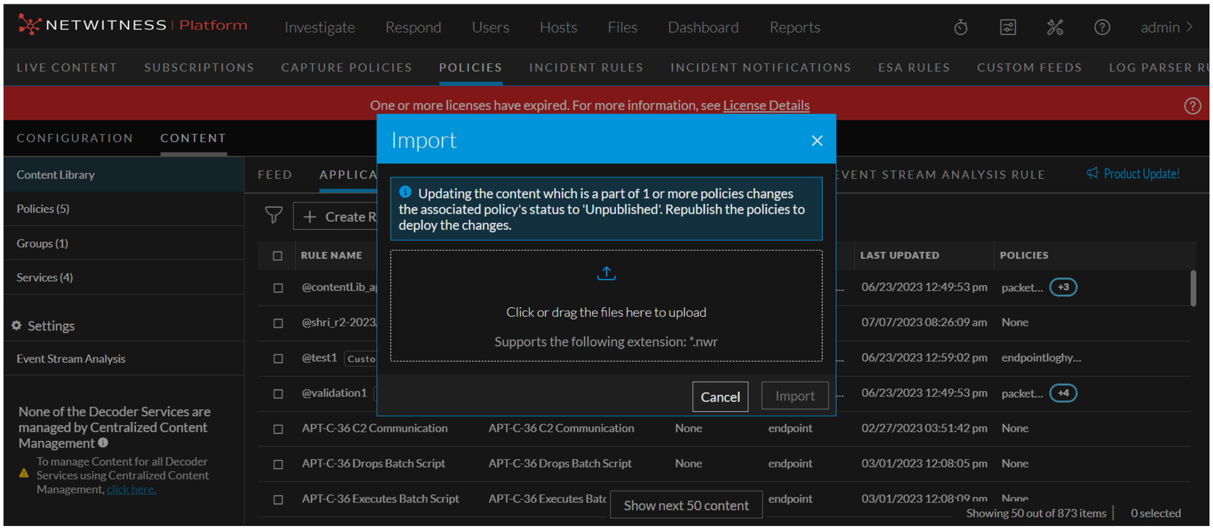
None of the Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

□	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
□	@contentLib_apprule1 Custom	@contentLib_apprule1	Critical	packet , endp...	06/23/2023 12:49:53 pm	packet... +3
□	@shri_r2-2023/07/07-0... Cust...	@shri_r2	None	log	07/07/2023 08:26:09 am	None
□	@test1 Custom	@test1	None	packet , endp...	06/23/2023 12:59:02 pm	endpointloghy...
□	@validation1 Custom	@validation1	None	packet , endp...	06/23/2023 12:49:53 pm	packet... +4
□	APT-C-36 C2 Communication	APT-C-36 C2 Communication	None	endpoint	02/27/2023 03:51:42 pm	None
□	APT-C-36 Drops Batch Script	APT-C-36 Drops Batch Script	None	endpoint	03/01/2023 12:08:05 pm	None
□	APT-C-36 Executes Batch Script	APT-C-36 Executes Batc		endpoint	03/01/2023 12:08:09 pm	None

Showing 50 out of 873 items | 0 selected

5. In the respective content panel, click **Import**.



One or more licenses have expired. For more information, see License Details

Import

Updating the content which is a part of 1 or more policies changes the associated policy's status to 'Unpublished'. Republish the policies to deploy the changes.

Click or drag the files here to upload

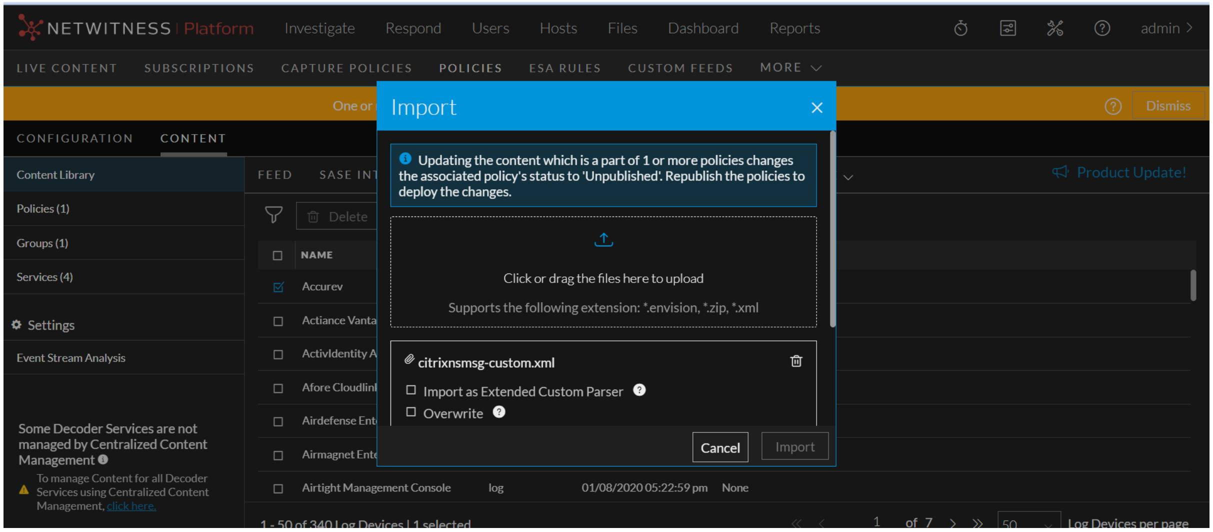
Supports the following extension: *.nwr

None of the Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

RULE NAME					LAST UPDATED	POLICIES
@contentLib_a					06/23/2023 12:49:53 pm	packet... +3
@shri_r2-2023					07/07/2023 08:26:09 am	None
@test1 Custo					06/23/2023 12:59:02 pm	endpointloghy...
@validation1					06/23/2023 12:49:53 pm	packet... +4
APT-C-36 C2 Communication	APT-C-36 C2 Communication	None	endpoint		02/27/2023 03:51:42 pm	None
APT-C-36 Drops Batch Script	APT-C-36 Drops Batch Script	None	endpoint		03/01/2023 12:08:05 pm	None
APT-C-36 Executes Batch Script	APT-C-36 Executes Batc		endpoint		03/01/2023 12:08:09 pm	None

Showing 50 out of 873 items | 0 selected



One or

Import

Updating the content which is a part of 1 or more policies changes the associated policy's status to 'Unpublished'. Republish the policies to deploy the changes.

Click or drag the files here to upload

Supports the following extension: *.envision, *.zip, *.xml

citrixnsmsg-custom.xml

□ Import as Extended Custom Parser

□ Overwrite

Some Decoder Services are not managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

NAME				
☑ Accurev				
□ Actiance Vanta				
□ ActivIdentity A				
□ Afore Cloudlin				
□ Airdefense Ent				
□ Airmagnet Ente				
□ Airtight Management Console	log	01/08/2020 05:22:59 pm	None	

1 - 50 of 340 Log Devices | 1 selected   1 of 7   50   Log Devices per page

6. In the **Import** panel, click or drag the file to upload.
7. While importing a Log Device parser, if you want to import a standalone XML as an extended parser, select **Import as Extended Custom Parser**. If this option is not selected, then the XML will be imported as a standalone parser.
8. Click **Overwrite** to overwrite content. This is applicable only in case of overriding an already imported content.

> **Note:** You cannot overwrite the content if the content name is same as the rule name of the existing content of the same type from live server. However, you can overwrite the content if the content name is same as the custom content rule name.

9. Select the medium types.
10. Click **Import** to complete the import process.

Create an Application Rule

This topic describes the steps to create an application rule. When you create a custom application rule, NetWitness allows you to tag MITRE ATT&CK Tactics and Techniques and for each rule.

> **IMPORTANT:** Both MITRE ATT&CK® and ATT&CK® are registered trademarks of the MITRE Corporation. © 2024 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

To create a new Application Rule

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.

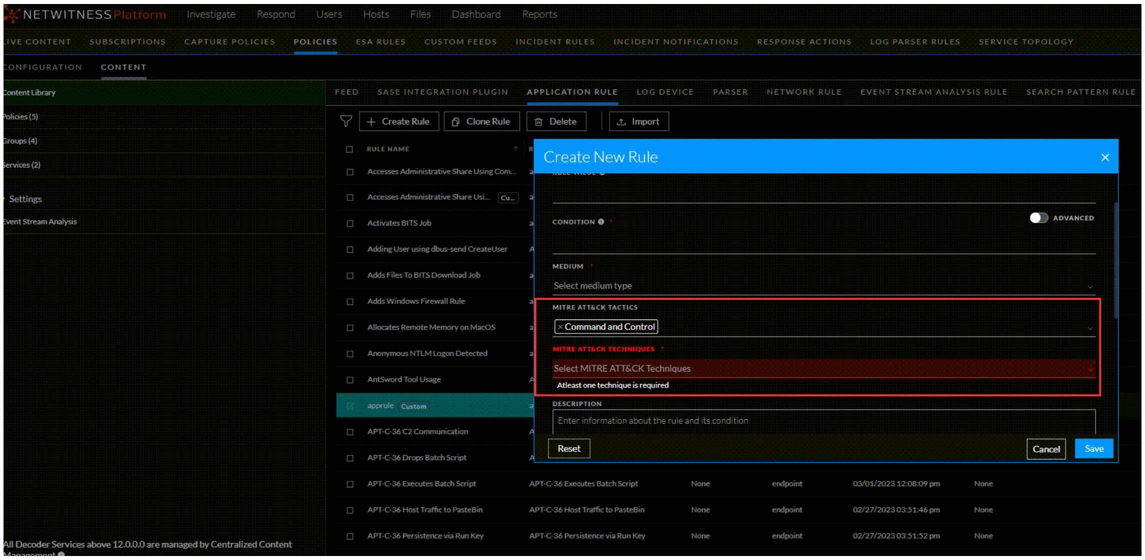
   The available rules are displayed.
4. In the application rule panel, click **+ Create Rule** to add an application rule.
5. In the **CreateNew Rule** panel, do the following:
   - Enter a unique rule name. If the name of that application rule is the same as an existing rule, an error message is displayed.
   - Enter the rule value. This is the value written to the alert meta. While creating a new rule, the rule value is defaulted with the rule name. However, you can modify the same.
   - Enter the condition for the rule. You can apply two types of conditions for the rule.
     - Normal mode:
       - It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on).
       - The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators.
     - Advanced: You can customize the conditions as a free form text.
   - Select the medium to be applied for the rule.
   - Enter the description for the rule.
   - Select the session data to be applied for the rule.
   - Select the session options to be applied for the rule. The options are listed below:
     - **Flag Session with rule name in meta key**: Select the meta value for the alert from the drop-down menu. This is mandatory.
     - **Forward**: This option enables the performance of syslog forwarding when the log matches the rule.
     - **Transient**: This option prevents the created alert metadata from being written to the disk.

- **Notify**: This option enables you to choose the **Severity** levels for the application rule and utilize the option to trigger alert generation.
  - Low
  - Medium
  - High
  - Critical

> **Note:** Severity is selected by default as Low.

- **MITRE ATT&CK TACTICS**: Lets you select MITRE ATT&CK TACTICS from the list.

> **Note:** Ensure that you apply at least one MITRE ATT&CK TACTIC for the rule.



Create New Rule

MEDIUM *: Select medium type

MITRE ATT&CK TACTICS: Command and Control

MITRE ATT&CK TECHNIQUES *: Select MITRE ATT&CK Techniques

Atleast one technique is required

DESCRIPTION: Enter information about the rule and its condition

Accesses Administrative Share Using Com...
Accesses Administrative Share Usi... Cu...
Activates BITS Job
Adding User using dbus-send CreateUser
Adds Files To BITS Download Job
Adds Windows Firewall Rule
Allocates Remote Memory on MacOS
Anonymous NTLM Logon Detected
AntSword Tool Usage
apprule Custom
APT-C-36 C2 Communication
APT-C-36 Drops Batch Script

APT-C-36 Executes Batch Script	APT-C-36 Executes Batch Script	None	endpoint	03/01/2023 12:08:09 pm	None
APT-C-36 Host Traffic to PasteBin	APT-C-36 Host Traffic to PasteBin	None	endpoint	02/27/2023 03:51:46 pm	None
APT-C-36 Persistence via Run Key	APT-C-36 Persistence via Run Key	None	endpoint	02/27/2023 03:51:52 pm	None

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

- **MITRE ATT&CK TECHNIQUES**: Lets you select MITRE ATT&CK TECHNIQUES from the list.
- **DESCRIPTION**: Provide a description for the rule.

- Click **Save** to save the new application rule.
- Click **Reset** to reset the fields.
- Click **Cancel** to cancel the operation.

Clone Application Rule

This topic describes the steps to clone an application rule.

To clone an Application Rule

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.

3. In the left panel, click **Content Library**.
4. The list of application rules is displayed. From the available list of rules, select the rule to be cloned.
5. Click **Clone Rule**.
6. In the **Clone Rule** panel, do the following:
   - Enter a unique rule name. If the name of that application rule is same as an existing rule, an error message is displayed.
   - Enter the rule value.

     > **Note:** You can clone existing rules to generate cloned rules with different rule names but with same rule value.

   - Enter the condition for the rule.
   - Select the medium to be applied for the rule.
   - Select the MITRE ATT&CK TACTICS for the rule.
   - Select the MITRE ATT&CK TECHNIQUES for the rule.
   - Enter the description for the rule.
   - Select the session data to be applied for the rule.
   - Select the session options to be applied for the rule.
   - Select a meta value from the Flag session with rule name in meta key drop-down menu. This is a mandatory field.
   - Click **Clone** to clone the rule.
   - Click **Cancel** to cancel the operation.

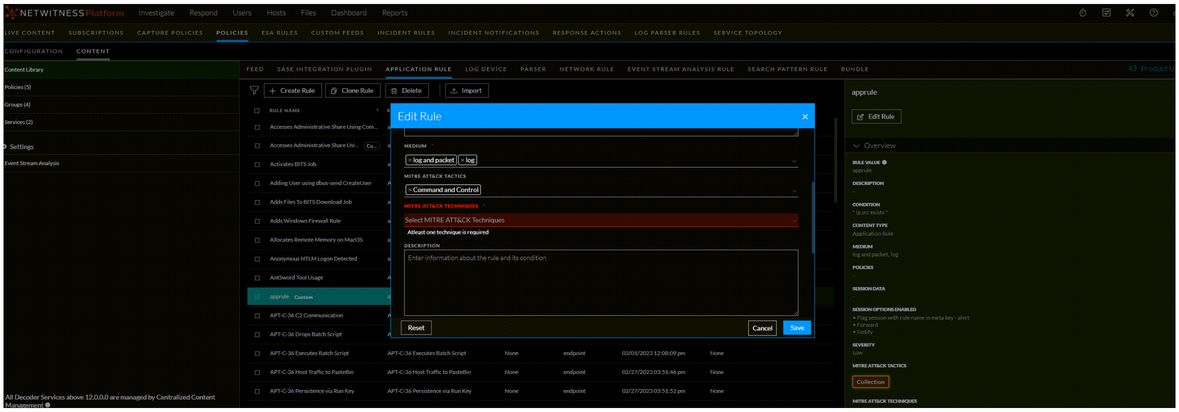
Edit Application Rule

When you edit the application rule, follow these guidelines:

- You can only edit the custom rules.
- The rule name and rule value cannot be edited if the custom rule is assigned to a policy.
- If the custom rule assigned to a policy is edited, then the customer must republish the policy for the changes to take effect in the service.
- The rule value cannot be edited. The rule value can be same for different rule names.
- While editing the rule name, if the name of that application rule is same as an existing rule, an error message is displayed.
- Let’s you to tag MITRE ATT&CK Tactics for each rule.
- Let’s you select the MITRE ATT&CK Techniques for the rule.

To edit an Application Rule

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Select an application rule to edit.
5. Click **Edit Rule** to edit the application rule.
6. In the **Edit Rule** panel, do the following:
   - Enter a unique rule name. If the name of that application rule is the same as an existing rule, an error message is displayed.
   - Enter the rule value. This is the value written to the alert meta.
   - Enter the condition for the rule. You can apply two types of conditions for the rule.
     - Normal mode:
       - It gives suggestions for supported metas (ip, host and so on) and operators ("=", "Not Equal To", "Contains", "Exists" and so on).
       - The entered condition will be enclosed in a 'Pill'. When you enter multiple conditions, the conditions are automatically joined by an 'AND' operator. On clicking the 'AND' operator, you can toggle between 'AND' and 'OR' operators.
     - Advanced: You can customize the conditions as a free form text.
   - Select the medium to be applied for the rule.
   - Select the MITRE ATT&CK TACTICS for the rule. The MITRE ATT&CK Tactics are listed. You can select an appropriate MITRE ATT&CK Tactic.



Edit Rule

MEDIUM *: × log and packet × log

MITRE ATT&CK TACTICS: × Command and Control

MITRE ATT&CK TECHNIQUES *: Select MITRE ATT&CK Techniques

Atleast one technique is required

DESCRIPTION: Enter information about the rule and its condition

APT-C-36 Executes Batch Script	APT-C-36 Executes Batch Script	None	endpoint	03/01/2023 12:08:09 pm	None
APT-C-36 Host Traffic to PasteBin	APT-C-36 Host Traffic to PasteBin	None	endpoint	02/27/2023 03:51:46 pm	None
APT-C-36 Persistence via Run Key	APT-C-36 Persistence via Run Key	None	endpoint	02/27/2023 03:51:52 pm	None

RULE VALUE: apprule

DESCRIPTION: -

CONDITION: " ip.src exists "

CONTENT TYPE: Application Rule

MEDIUM: log and packet, log

POLICIES: -

SESSION DATA: -

SESSION OPTIONS ENABLED:
- Flag session with rule name in meta key - alert
- Forward
- Notify

SEVERITY: Low

MITRE ATT&CK TACTICS: Collection

MITRE ATT&CK TECHNIQUES

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

   - Select the MITRE ATT&CK TECHNIQUES for the rule. The MITRE ATT&CK Techniques are listed. You can select an appropriate MITRE ATT&CK Technique.
   - Enter the description for the rule.
   - Select the session data to be applied for the rule.

- Select the session options to be applied for the rule.The options are listed below:
  - **Flag Session with rule name in meta key**: Select the meta value for the alert from the drop-down menu. This is mandatory.
  - **Forward**: This option enables the performance of syslog forwarding when the log matches the rule.
  - **Transient**: This option prevents the created alert metadata from being written to the disk.
  - **Notify**: This option enables you to choose the **Severity** levels for the application rule and utilize the option to trigger alert generation.
    - Low
    - Medium
    - High
    - Critical

  Note: Severity is selected by default as Low.
- Click **Save** to save the application rule details.
- Click **Reset** to reset the fields.
- Click **Cancel** to cancel the operation.

Delete Application Rule

When you delete the application rule, follow these guidelines:

- You can delete only the custom application rules.
- You cannot delete the application rule if it is associated to a policy. You should first disassociate the application rule from the policy and then delete it.

To delete an Application Rule

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Select an application rule to delete.
5. Click **Delete** to permanently delete the selected application rule.

View Application Rule Details

This topic describes the steps to view the application rule details.

To view Application Rule details

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.

   The list of application rules is displayed.
4. Click a row to view details about the selected application rule in the right panel.

   The various details of the application rule are displayed.

Create a Network Rule

This topic describes the steps to create a network rule.

To create a Network Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click the **Network Rule** tab.
5. In the network rule panel, click **+ Create Rule** to add a network rule.
6. In the **New Create Rule** panel, do the following:
   - Enter a unique rule name. If the name of that network rule is the same as an existing rule, an error message is displayed.
   - Enter the rule value. This is the value written to the alert meta. While creating a new rule, the rule value is defaulted with the rule name. However, you can modify the same.
   - Enter the condition for the rule. You can apply two types of conditions for the rule.
     - Normal mode:
       - It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on).
       - The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators.
     - Advanced: You can customize the conditions as a free form text.

     Note: The medium is selected as **Packet** by default, and it cannot be modified.
   - Enter the description for the rule.
   - Select the session data to be applied for the rule.
   - Select the session options to be applied for the rule.

- Click **Cancel** to cancel the operation.
- Click **Reset** to reset the data.
- Click **Save** to save the new network rule.

Clone Network Rule

This topic describes the steps to clone an application rule.

To clone an Application Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **Network Rule** tab.
5. The list of application rules is displayed. From the available list of rules, select the rule to be cloned.
6. Click **Clone Rule**.
7. In the **Clone Rule** panel, do the following:
   - Enter a unique rule name. If the name of that network rule is same as an existing rule, an error message is displayed.
   - Enter the rule value.

     Note: You can clone existing rules to generate cloned rules with different rule names but with same rule value.

   - Enter the condition for the rule.

     Note: The medium is selected as **Packet** by default, and it cannot be modified.

   - Enter the description for the rule.
   - Select the session data to be applied for the rule.
   - Select the session options to be applied for the rule.
   - Click **Clone** to clone the rule.
   - Click **Cancel** to cancel the operation.

Edit Network Rule

When you edit the network rule, follow these guidelines:

- You can only edit the custom rules.
- The rule name and rule value cannot be edited if the custom rule is assigned to a policy.

- If the custom rule assigned to a policy is edited, then you must republish the policy for the changes to take effect in the service.
- The rule value cannot be edited. The rule value can be same for different rule names.
- While editing the rule name, if the name of that network rule is same as an existing rule, an error message is displayed.

To edit a Network Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click the **Network Rule** tab.
5. Select the network rule to edit.
6. Click **Edit Rule** to edit the network rule.
7. In the **Edit Rule** panel, do the following:
   - Enter a unique rule name. If the name of that network rule is the same as an existing rule, an error message is displayed.
   - Enter the rule value. This is the value written to the alert meta.
   - Enter the condition for the rule. You can apply two types of conditions for the rule.
     - Normal mode:
       - It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on).
       - The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators.
     - Advanced: You can customize the conditions as a free form text.

     Note: The medium is selected as **Packet** by default, and it cannot be modified.
   - Enter the description for the rule.
   - Select the session data to be applied for the rule.
   - Select the session options to be applied for the rule.
   - Click **Cancel** to cancel the operation.
   - Click **Reset** to reset the data.
   - Click **Save** to save the new network rule.

Delete Network Rule

When you delete the network rule, follow these guidelines:

- You can delete only the custom network rules.
- You cannot delete the network rule if it is associated to a policy. You should first disassociate the network rule from the policy and then delete it.

To delete a Network Rule

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **Network Rule** tab.
5. Select a network rule to delete.
6. Click **Delete** to permanently delete the selected network rule.

View Network Rule Details

This topic describes the steps to view the network rule details.

To view Network Rule details

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click the **Network Rule** tab.
5. The list of network rules is displayed.
6. Click a row to view details about the selected network rule in the right panel.

   The various details of the network rule are displayed.

Create an ESA Rule

This topic describes the steps to create an ESA rule.

To create an ESA Rule

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
   The available rules are displayed.
4. Click **Event Stream Analysis Rule**.
5. In the ESA rule panel, click **+ Create Rule** to add an ESA rule.

You can select the **Advanced EPL** option or **Rule Builder** option from the dropdown as per your requirement. It navigates to **ESA Rules** > **Rules** view.

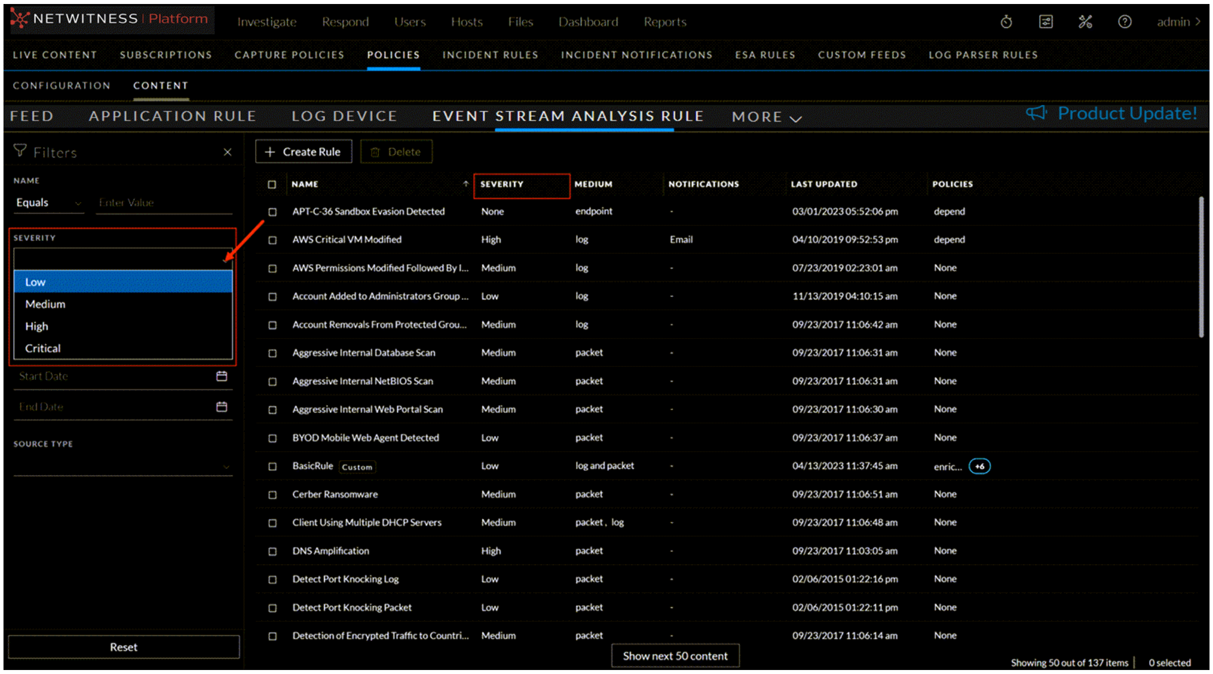
See the section Add a Rule Builder Rule for more information on creating rules in Rule Builder.

See the section Add an Advanced EPL for more information on creating Advanced EPL.

> **Note:** Analysts must have appropriate permissions to view the ESA rules under (**CONFIGURE**) > **ESA Rules** and (**CONFIGURE**) > **Policies** pages. For more information, see the **Source-server** section in the "Role Permissions" topic in the *System Security and User Management Guide*.

From 12.3 and later, **Severity** and **Notifications** list views are added to the **Event Stream Analysis Rule** section.

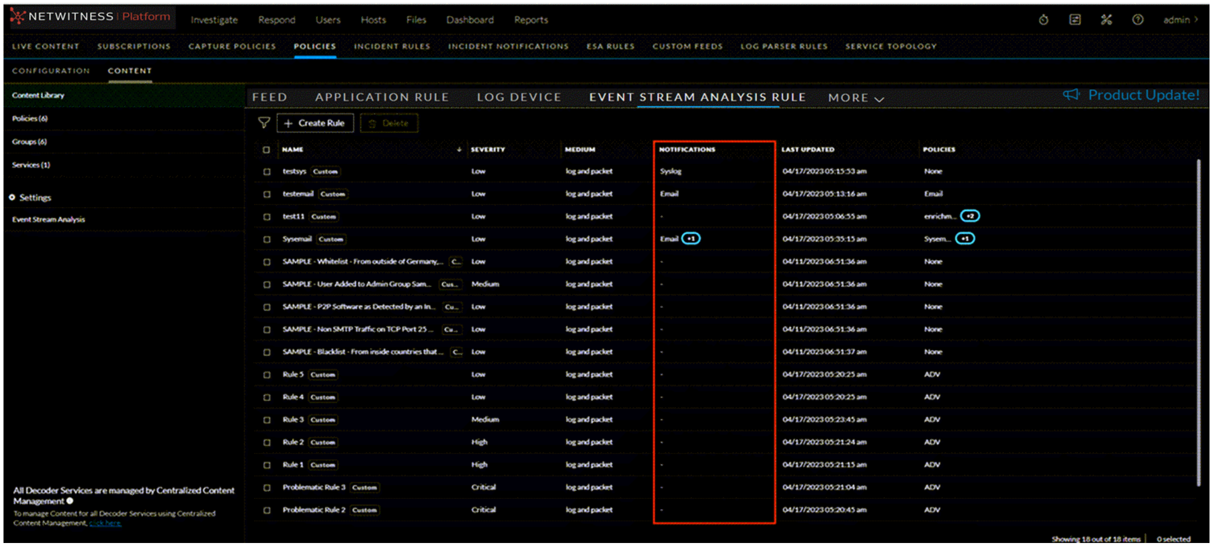
The Severity list consists of None, Low, Medium, High, and Critical. You can also view rules filtering these options except for None. For more information on filtering these options, see Filter Content Rules.



NAME	SEVERITY	MEDIUM	NOTIFICATIONS	LAST UPDATED	POLICIES
APT-C-36 Sandbox Evasion Detected	None	endpoint	-	03/01/2023 05:52:06 pm	depend
AWS Critical VM Modified	High	log	Email	04/10/2019 09:52:53 pm	depend
AWS Permissions Modified Followed By I...	Medium	log	-	07/23/2019 02:23:01 am	None
Account Added to Administrators Group ...	Low	log	-	11/13/2019 04:10:15 am	None
Account Removals From Protected Grou...	Medium	log	-	09/23/2017 11:06:42 am	None
Aggressive Internal Database Scan	Medium	packet	-	09/23/2017 11:06:31 am	None
Aggressive Internal NetBIOS Scan	Medium	packet	-	09/23/2017 11:06:31 am	None
Aggressive Internal Web Portal Scan	Medium	packet	-	09/23/2017 11:06:30 am	None
BYOD Mobile Web Agent Detected	Low	packet	-	09/23/2017 11:06:37 am	None
BasicRule Custom	Low	log and packet	-	04/13/2023 11:37:45 am	enric... +6
Cerber Ransomware	Medium	packet	-	09/23/2017 11:06:51 am	None
Client Using Multiple DHCP Servers	Medium	packet , log	-	09/23/2017 11:06:48 am	None
DNS Amplification	High	packet	-	09/23/2017 11:03:05 am	None
Detect Port Knocking Log	Low	packet	-	02/06/2015 01:22:16 pm	None
Detect Port Knocking Packet	Low	packet	-	02/06/2015 01:22:11 pm	None
Detection of Encrypted Traffic to Countri...	Medium	packet	-	09/23/2017 11:06:14 am	None

Showing 50 out of 137 items | 0 selected

Rules with syslog and email notifications can be viewed on the **Notifications** list of the **Event Stream Analysis Rule** section.



□	NAME	SEVERITY	MEDIUM	NOTIFICATIONS	LAST UPDATED	POLICIES
□	testsys Custom	Low	log and packet	Syslog	04/17/2023 05:15:53 am	None
□	testemail Custom	Low	log and packet	Email	04/17/2023 05:13:16 am	Email
□	test11 Custom	Low	log and packet	-	04/17/2023 05:06:55 am	enrichm... +2
□	Sysemail Custom	Low	log and packet	Email +1	04/17/2023 05:35:15 am	Sysem... +1
□	SAMPLE - Whitelist - From outside of Germany,... C...	Low	log and packet	-	04/11/2023 06:51:36 am	None
□	SAMPLE - User Added to Admin Group Sam... Cus...	Medium	log and packet	-	04/11/2023 06:51:36 am	None
□	SAMPLE - P2P Software as Detected by an In... Cu...	Low	log and packet	-	04/11/2023 06:51:36 am	None
□	SAMPLE - Non SMTP Traffic on TCP Port 25 ... Cu...	Low	log and packet	-	04/11/2023 06:51:36 am	None
□	SAMPLE - Blacklist - From inside countries that ... C...	Low	log and packet	-	04/11/2023 06:51:37 am	None
□	Rule 5 Custom	Low	log and packet	-	04/17/2023 05:20:25 am	ADV
□	Rule 4 Custom	Low	log and packet	-	04/17/2023 05:20:25 am	ADV
□	Rule 3 Custom	Medium	log and packet	-	04/17/2023 05:23:45 am	ADV
□	Rule 2 Custom	High	log and packet	-	04/17/2023 05:21:24 am	ADV
□	Rule 1 Custom	High	log and packet	-	04/17/2023 05:21:15 am	ADV
□	Problematic Rule 3 Custom	Critical	log and packet	-	04/17/2023 05:21:04 am	ADV
□	Problematic Rule 2 Custom	Critical	log and packet	-	04/17/2023 05:20:45 am	ADV

Showing 18 out of 18 items | 0 selected

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Edit an ESA Rule

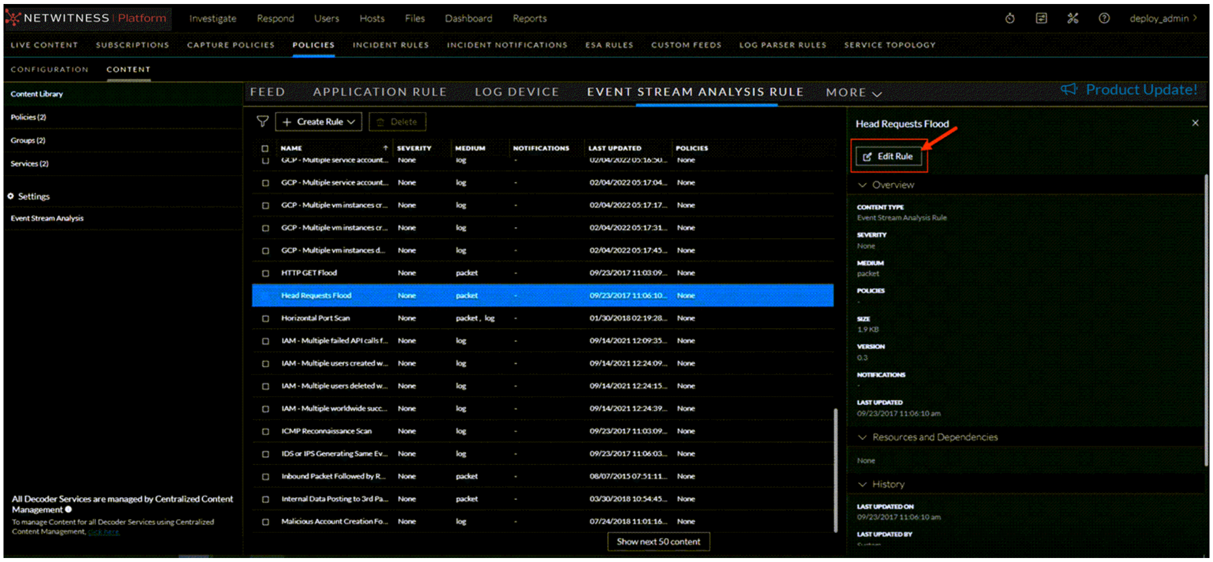
This topic provides instructions to edit an Event Stream Analysis (ESA) rule. When you edit a rule, ESA applies the updated criteria going forward. No changes are made to previously generated alerts.

To edit an ESA Rule

1. Go to (**CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.

   The available rules are displayed.
4. Click **Event Stream Analysis Rule**.
5. In the ESA rule panel, select the rule that needs to be edited.

   The overview panel opens, showing the Edit Rule tab on top.
6. Click the **Edit Rule** tab.



NAME	SEVERITY	MEDIUM	NOTIFICATIONS	LAST UPDATED	POLICIES
GCP - Multiple service account...	None	log	-	02/04/2022 05:16:50...	None
GCP - Multiple service account...	None	log	-	02/04/2022 05:17:04...	None
GCP - Multiple vm instances cr...	None	log	-	02/04/2022 05:17:17...	None
GCP - Multiple vm instances cr...	None	log	-	02/04/2022 05:17:31...	None
GCP - Multiple vm instances d...	None	log	-	02/04/2022 05:17:45...	None
HTTP GET Flood	None	packet	-	09/23/2017 11:03:09...	None
Head Requests Flood	None	packet	-	09/23/2017 11:06:10...	None
Horizontal Port Scan	None	packet , log	-	01/30/2018 02:19:28...	None
IAM - Multiple failed API calls f...	None	log	-	09/14/2021 12:09:35...	None
IAM - Multiple users created w...	None	log	-	09/14/2021 12:24:09...	None
IAM - Multiple users deleted w...	None	log	-	09/14/2021 12:24:15...	None
IAM - Multiple worldwide succ...	None	log	-	09/14/2021 12:24:39...	None
ICMP Reconnaissance Scan	None	log	-	09/23/2017 11:03:09...	None
IDS or IPS Generating Same Ev...	None	log	-	09/23/2017 11:06:03...	None
Inbound Packet Followed by R...	None	packet	-	08/07/2015 07:51:11...	None
Internal Data Posting to 3rd Pa...	None	packet	-	03/30/2018 10:54:45...	None
Malicious Account Creation Fo...	None	log	-	07/24/2018 11:01:16...	None

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Head Requests Flood

CONTENT TYPE: Event Stream Analysis Rule
SEVERITY: None
MEDIUM: packet
POLICIES: -
SIZE: 1.9 KB
VERSION: 0.3
NOTIFICATIONS: -
LAST UPDATED: 09/23/2017 11:06:10 am

Resources and Dependencies: None

LAST UPDATED ON: 09/23/2017 11:06:10 am
LAST UPDATED BY

It navigates to **ESA Rules** > **Rules** view.

For more information on editing an ESA rule, see Edit, Duplicate or Delete a Rule.

Configure MITRE ATT&CK Details for an ESA Rule

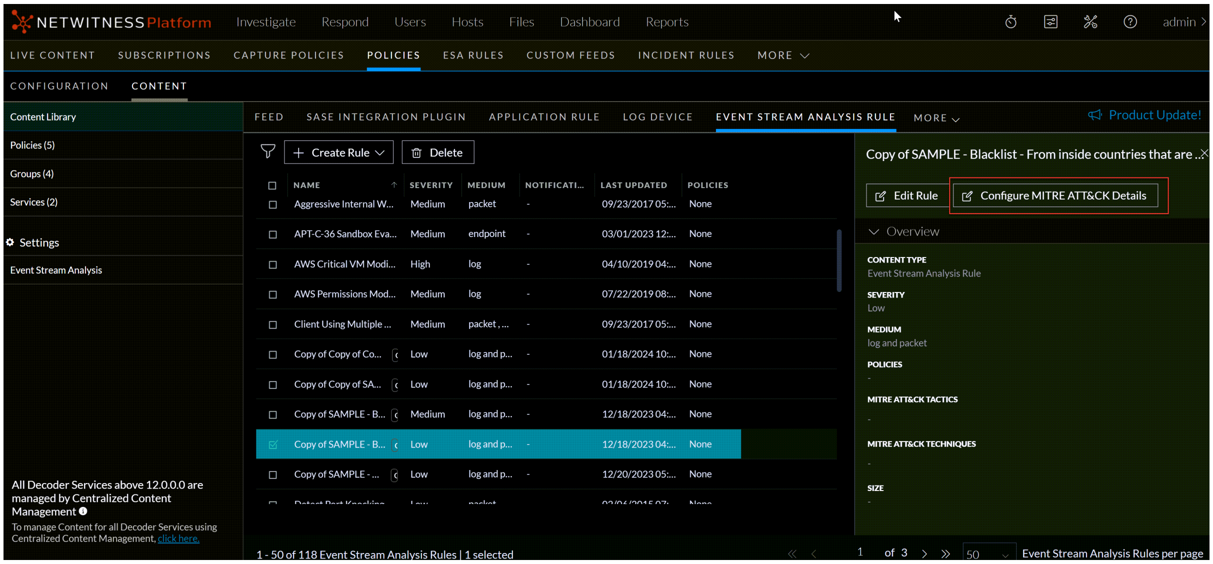
You can tag MITRE ATT&CK Tactics and Techniques for an ESA rule. MITRE framework provides insight into tactics, techniques, or sub-techniques used by advanced attackers or advanced persistent threats (APTs). When you tag an ESA rule with MITRE ATT&CK Tactics and Techniques, analysts can easily identify incidents, alerts, and events that are associated with MITRE techniques and tactics.

To configure MITRE ATT&CK details for an ESA Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the **policies** panel, click **Content**.
3. In the left panel, click **Content Library**.

   The available rules are displayed.
4. Click **Event Stream Analysis Rule**.
5. In the ESA rule panel, select the rule that needs to be edited.

   The overview panel opens, showing the Edit Rule tab on top.
6. Click the **Configure MITRE ATT&CK Details** option.



All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

□	NAME	SEVERITY	MEDIUM	NOTIFICATI...	LAST UPDATED	POLICIES
□	Aggressive Internal W...	Medium	packet	-	09/23/2017 05:...	None
□	APT-C-36 Sandbox Eva...	Medium	endpoint	-	03/01/2023 12:...	None
□	AWS Critical VM Modi...	High	log	-	04/10/2019 04:...	None
□	AWS Permissions Mod...	Medium	log	-	07/22/2019 08:...	None
□	Client Using Multiple ...	Medium	packet , ...	-	09/23/2017 05:...	None
□	Copy of Copy of Co...	Low	log and p...	-	01/18/2024 10:...	None
□	Copy of Copy of SA...	Low	log and p...	-	01/18/2024 10:...	None
□	Copy of SAMPLE - B...	Medium	log and p...	-	12/18/2023 04:...	None
☑	Copy of SAMPLE - B...	Low	log and p...	-	12/18/2023 04:...	None
□	Copy of SAMPLE - ...	Low	log and p...	-	12/20/2023 05:...	None

1 - 50 of 118 Event Stream Analysis Rules | 1 selected

1 of 3 | 50 Event Stream Analysis Rules per page

Copy of SAMPLE - Blacklist - From inside countries that are ..

CONTENT TYPE
Event Stream Analysis Rule

SEVERITY
Low

MEDIUM
log and packet

POLICIES
-

MITRE ATT&CK TACTICS
-

MITRE ATT&CK TECHNIQUES
-

SIZE
-

7. In the **Configure MITRE ATT&CK Details** window, select the **MITRE ATT&CK Tactics**. You can apply multiple MITRE Tactics for an ESA rule.
8. Select the **MITRE ATT&CK Techniques**. You can apply multiple MITRE Techniques for an ESA rule.

   For more information on MITRE ATT&CK framework, see About MITRE ATT&CK Tactics and Techniques .

Delete an ESA Rule

You can delete one or more ESA rules. Once the ESA rule is deleted, the ESA rule will be removed from the available list.

To delete an ESA Rule

1. Go to (**CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.

   The available rules are displayed.
4. Click **Event Stream Analysis Rule**.

   The available ESA rules are displayed.

   Note: Only Custom ESA rules that are not assigned to a policy will be available for deletion.
5. Select one or more custom ESA rules and click **Delete**.

   A confirmation pop-up is displayed.
6. Click **Delete**.

About MITRE ATT&CK Tactics and Techniques

NetWitness allows you to tag an application rule with MITRE ATT&CK Tactics and Techniques. MITRE framework provides insight into tactics, techniques, or sub-techniques used by advanced attackers or advanced persistent threats (APTs). NetWitness uses the MITRE ATT&CK framework to detect and analyze different types of threats.

When you tag an application rule with MITRE ATT&CK Tactics and Techniques, analysts can look into the various techniques and tactics associated with the Incidents, alerts, and events.

You do not have to search the MITRE pages to understand techniques or tactics and learn about their implications. You can view all the MITRE details in the **ATT&CK Explorer**. The additional details about MITRE ATT&CK Tactics and Techniques help you to understand how an attack or event is detected in their NetWitness system and then make informed decisions.

NetWitness Platform enables analysts to conduct further analysis with levels of granularity in techniques.

The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior. It reflects the various phases of an adversary's attack lifecycle and the platforms they are known to target.

For more information on the MITRE ATT&CK framework, go tohttps://attack.mitre.org/resources/faq/

For more information, see “Use MITRE ATT&CK Framework” chapter in the NetWitness Respond User Guide for 12.4 .

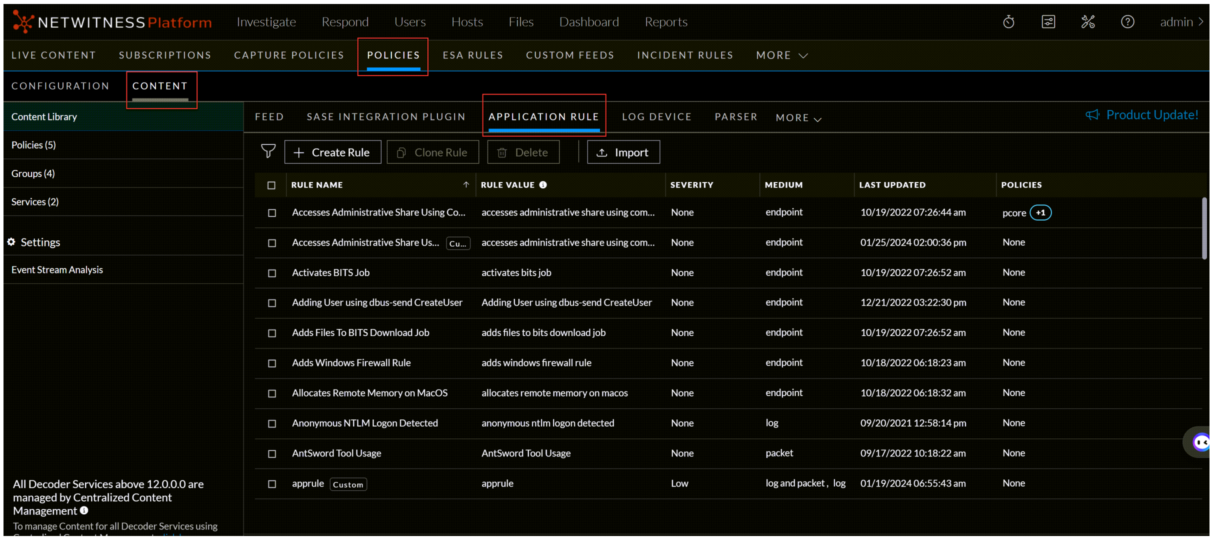
View MITRE ATT&CK Tactics and Techniques in Application and ESA rules

NetWitness allows you to tag application rules and ESA rules with MITRE ATT&CK Tactics and Techniques. When you tag MITRE ATT&CK Tactics and Techniques, you can view the details of the tactics and techniques used by advanced attackers or advanced persistent threats (APTs). You do not have to search the MITRE pages to understand techniques or tactics and learn about their implications. You can view all the MITRE details in the ATT&CK explorer. The additional details about MITRE ATT&CK Tactics and Techniques help you to understand how an attack or event is detected in their NetWitness system and then make informed decisions.

IMPORTANT: Both MITRE ATT&CK® and ATT&CK® are registered trademarks of the MITRE Corporation. © 2024 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

To view MITRE ATT&CK Tactics and Techniques in application and ESA rules

1. Go to **(CONFIGURE)** > **Policies**.
2. In the **Policies** panel, click **Content** tab.
3. Click **APPLICATION RULE**. The Application Rules are listed.

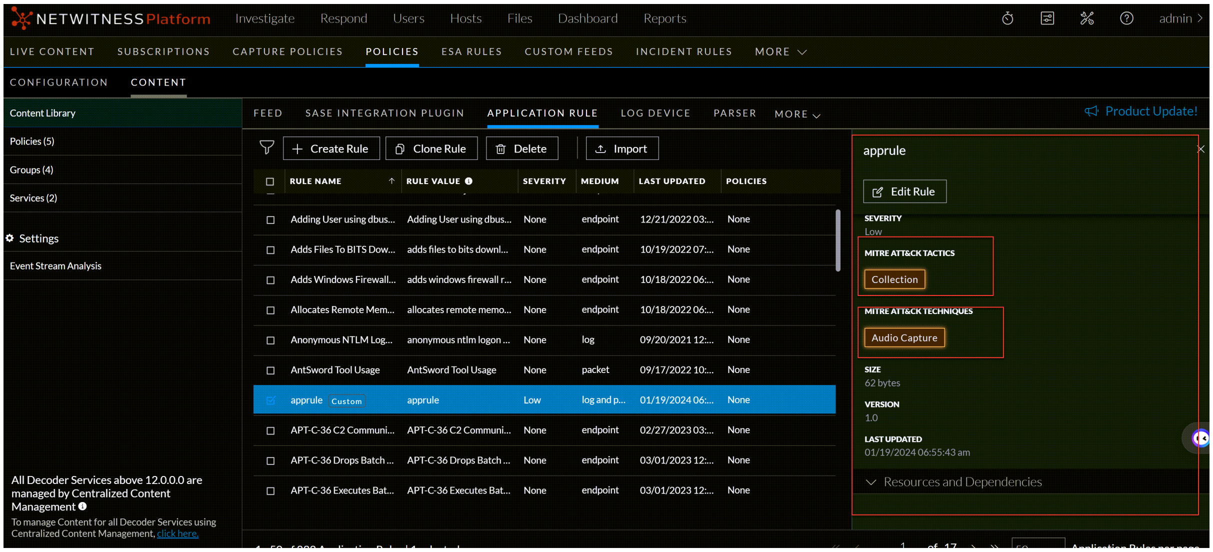


RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
Accesses Administrative Share Using Co...	accesses administrative share using com...	None	endpoint	10/19/2022 07:26:44 am	pcore +1
Accesses Administrative Share Us... Cu...	accesses administrative share using com...	None	endpoint	01/25/2024 02:00:36 pm	None
Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	None
Adding User using dbus-send CreateUser	Adding User using dbus-send CreateUser	None	endpoint	12/21/2022 03:22:30 pm	None
Adds Files To BITS Download Job	adds files to bits download job	None	endpoint	10/19/2022 07:26:52 am	None
Adds Windows Firewall Rule	adds windows firewall rule	None	endpoint	10/18/2022 06:18:23 am	None
Allocates Remote Memory on MacOS	allocates remote memory on macos	None	endpoint	10/18/2022 06:18:32 am	None
Anonymous NTLM Logon Detected	anonymous ntlm logon detected	None	log	09/20/2021 12:58:14 pm	None
AntSword Tool Usage	AntSword Tool Usage	None	packet	09/17/2022 10:18:22 am	None
apprule Custom	apprule	Low	log and packet , log	01/19/2024 06:55:43 am	None

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using

4. Click a rule that you want to view the MITRE ATT&CK Tactics and Techniques. The rule panel appears on the left side.



RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
Adding User using dbus...	Adding User using dbus...	None	endpoint	12/21/2022 03:...	None
Adds Files To BITS Dow...	adds files to bits downl...	None	endpoint	10/19/2022 07:...	None
Adds Windows Firewall...	adds windows firewall r...	None	endpoint	10/18/2022 06:...	None
Allocates Remote Mem...	allocates remote memo...	None	endpoint	10/18/2022 06:...	None
Anonymous NTLM Log...	anonymous ntlm logon ...	None	log	09/20/2021 12:...	None
AntSword Tool Usage	AntSword Tool Usage	None	packet	09/17/2022 10:...	None
apprule Custom	apprule	Low	log and p...	01/19/2024 06:...	None
APT-C-36 C2 Communi...	APT-C-36 C2 Communi...	None	endpoint	02/27/2023 03:...	None
APT-C-36 Drops Batch ...	APT-C-36 Drops Batch ...	None	endpoint	03/01/2023 12:...	None
APT-C-36 Executes Bat...	APT-C-36 Executes Bat...	None	endpoint	03/01/2023 12:...	None

apprule

SEVERITY
Low

MITRE ATT&CK TACTICS
Collection

MITRE ATT&CK TECHNIQUES
Audio Capture

SIZE
62 bytes

VERSION
1.0

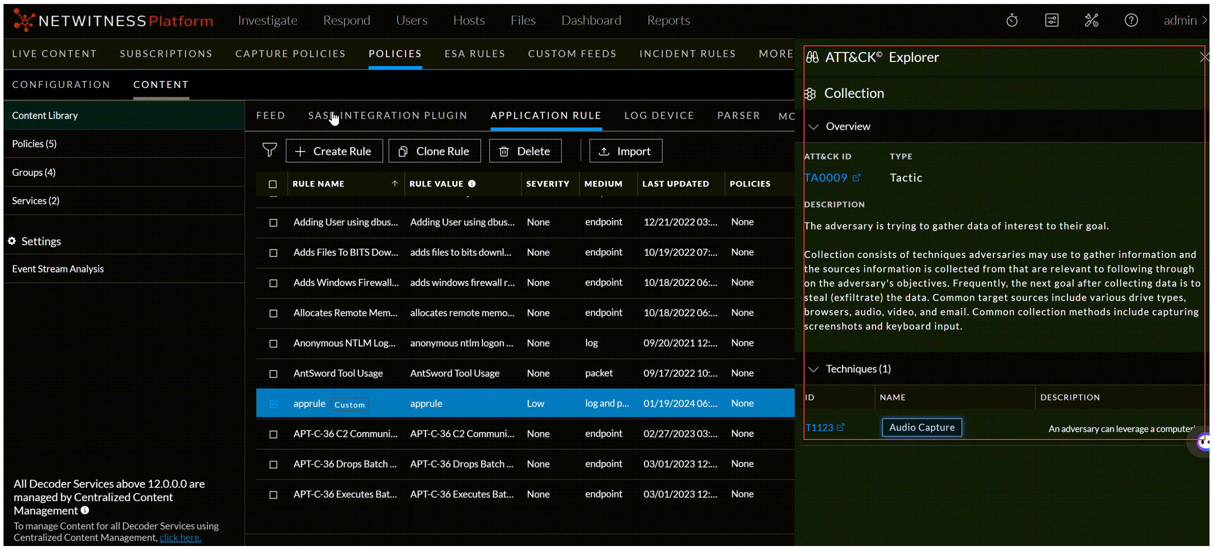
LAST UPDATED
01/19/2024 06:55:43 am

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

5. In the left panel, scroll down and view the MITRE ATT&CK TACTICS and TECHNIQUES categories.

6. Click a MITRE ATT&CK TACTICS or TECHNIQUES. The ATT&CK Explorer panel appears with details on tactics and techniques.



☐	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
☐	Adding User using dbus...	Adding User using dbus...	None	endpoint	12/21/2022 03:...	None
☐	Adds Files To BITS Dow...	adds files to bits downl...	None	endpoint	10/19/2022 07:...	None
☐	Adds Windows Firewall...	adds windows firewall r...	None	endpoint	10/18/2022 06:...	None
☐	Allocates Remote Mem...	allocates remote memo...	None	endpoint	10/18/2022 06:...	None
☐	Anonymous NTLM Log...	anonymous ntlm logon ...	None	log	09/20/2021 12:...	None
☐	AntSword Tool Usage	AntSword Tool Usage	None	packet	09/17/2022 10:...	None
☑	apprule Custom	apprule	Low	log and p...	01/19/2024 06:...	None
☐	APT-C-36 C2 Communi...	APT-C-36 C2 Communi...	None	endpoint	02/27/2023 03:...	None
☐	APT-C-36 Drops Batch ...	APT-C-36 Drops Batch ...	None	endpoint	03/01/2023 12:...	None
☐	APT-C-36 Executes Bat...	APT-C-36 Executes Bat...	None	endpoint	03/01/2023 12:...	None

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

ATT&CK© Explorer

Collection

Overview

ATT&CK ID	TYPE
TA0009	Tactic

DESCRIPTION

The adversary is trying to gather data of interest to their goal.

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

Techniques (1)

ID	NAME	DESCRIPTION
T1123	Audio Capture	An adversary can leverage a computer'

You can view the following details:

Fields	Description
MITRE ATT&CK Tactics	Displays the type of tactics associated with the Incident. For example, **Credential Access**. The tactic **Credential Access** tries to steal account names and passwords. For more information, see https://attack.mitre.org/tactics/enterprise/.
ATT&CK ID	Displays the ATT&CK ID associated with the Tactics. You can click the ATT&CK ID and go to the MITRE page and view the details. Analysts can benefit by visiting the MITRE page directly to get additional details about the Tactics. For example: **TA0006**. The Tactics ID **TA0006** is associated with the Tactic **Credential Access**.
TYPE	Displays the Technique associated with the Tactics.
TACTIC	Displays the Tactics that you tagged. You can tag multiple Tactics with a rule.
DESCRIPTION	Displays the detailed information about the Tactic associated with the particular incident.
Techniques	Displays the ID, Name, and the Description of the various Techniques and Sub – Techniques associated with the Tactics. **Note:** Techniques are how the adversary tries to achieve a tactical goal by performing an action. Sub – Techniques describe the adversarial behavior at a lower level than a technique. For more information, see • https://attack.mitre.org/resources/faq/#faq-0-0-header. • https://attack.mitre.org/techniques/enterprise/.

Fields	Description
Mitigations	Displays the ID, Name, and Description of the Mitigations used to prevent a technique or sub-technique from successfully executing. For example, The Mitigation name Account Use Policies associated with the ID M1036 helps configure features related to account use, like login attempt lockouts and specific login times. For more information, see https://attack.mitre.org/mitigations/enterprise/.
Procedure Examples	Displays the ID, Name, and Description of the procedures that the adversary uses for techniques or sub-techniques. For example, Lazarus Group with the ID G0032 is a North Korean state-sponsored cyber threat group that was responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. For more information, see https://attack.mitre.org/resources/faq/#faq-0-2-header and https://attack.mitre.org/groups/G0032/.

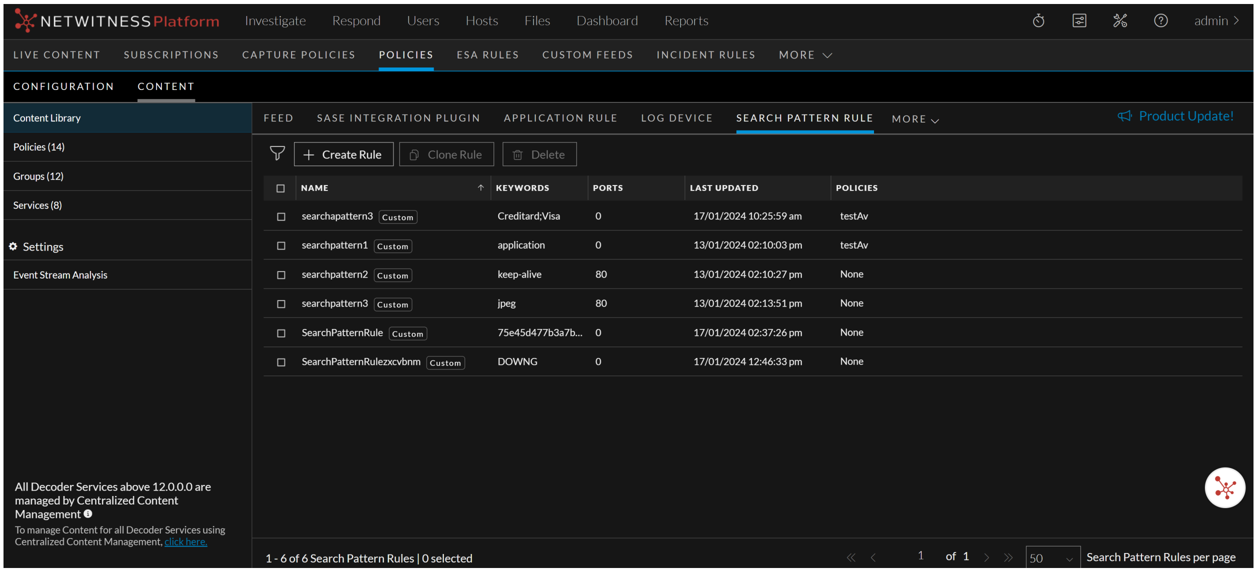
For more information, see “Use MITRE ATT&CK Framework” chapter in the NetWitness Respond User Guide for 12.4 .

Manage Search Pattern Rules

From NetWitness Platform version 12.4 or later, administrators and analysts can create search pattern rules from the **Configure** > **Policies** > **Content Library** page to find sensitive data on their networks. These rules use keywords to identify patterns and they are matched based on an exact keyword string. Once a pattern is applied to a matched policy with services (Decoders), it searches for that pattern in the network traffic. Upon successful detection of a match, two important metadata will be generated (**found** and **match**).

- **found**: If a match (a keyword) is identified in a stream, the name of the search pattern rule will be added as the found metadata.
- **match**: If a keyword is detected as a match, the specific keyword that is identified will be added as a match meta.

Analysts can use this metadata to investigate further and determine if the sensitive data is being used maliciously. Additionally, analysts can gain real-time visibility into their network traffic, proactively monitoring it for potential threats.



□	NAME	KEYWORDS	PORTS	LAST UPDATED	POLICIES
□	searchapattern3 Custom	Creditard;Visa	0	17/01/2024 10:25:59 am	testAv
□	searchpattern1 Custom	application	0	13/01/2024 02:10:03 pm	testAv
□	searchpattern2 Custom	keep-alive	80	13/01/2024 02:10:27 pm	None
□	searchpattern3 Custom	jpeg	80	13/01/2024 02:13:51 pm	None
□	SearchPatternRule Custom	75e45d477b3a7b...	0	17/01/2024 02:37:26 pm	None
□	SearchPatternRulezxcvbnm Custom	DOWNG	0	17/01/2024 12:46:33 pm	None

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 6 of 6 Search Pattern Rules | 0 selected

1 of 1

Here is an example of search pattern that can be used to find sensitive data in networks:

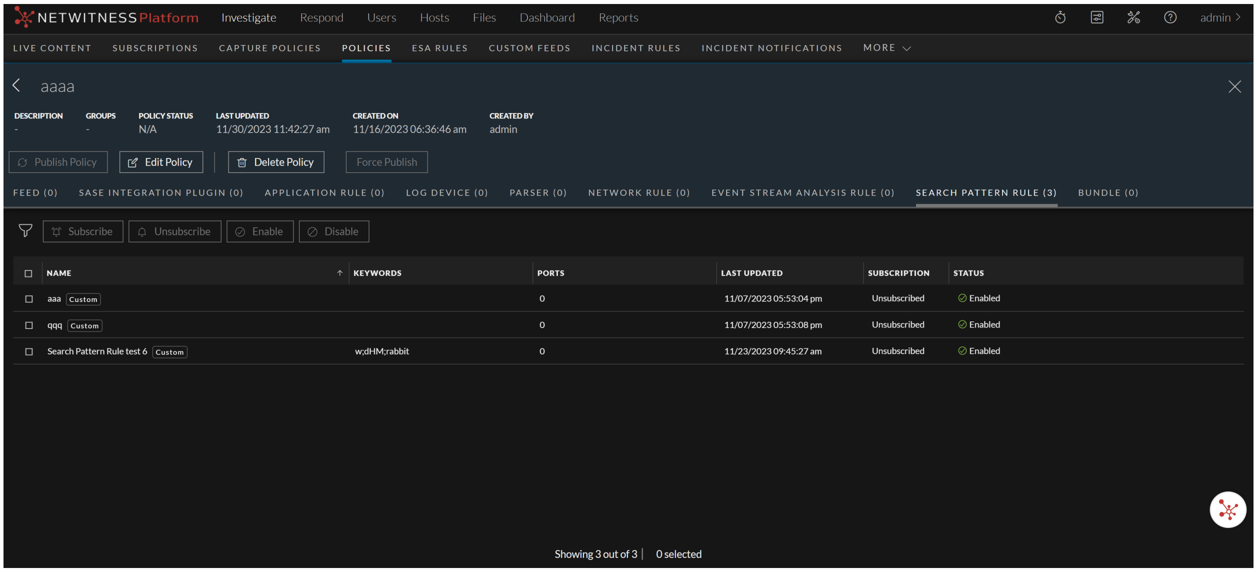
Keywords: Keywords are words or phrases that are often associated with sensitive data. For example, the keyword **credit card** could be used to find network traffic that contains credit card numbers.

IMPORTANT: The custom search patterns you created using the **search.ini** file in version 12.3.1 or earlier will not be migrated to the new **search.xml** file format used in version 12.4 and later. As a result, those custom search patterns will not be available from the **Content Library** > **More** > **Search Pattern Rule** tab after you upgrade to version 12.4 or later.

For example, in an environment, if you have four Decoders with CCM enabled and published to the policy. However, only three of these decoders have the search parser enabled, while one decoder doesn't have it enabled. As a result, only the three decoders with enabled search parser will generate **found** and **match** meta keys.

In addition, administrators can perform other operations on the search pattern rule, such as editing, cloning, deleting, and filtering a rule.

Note: You can also view the search pattern rules inside a **Policy Details** view and allows you to enable or disable those rules. For more information, see Manage Policies.



aaaa

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	-	N/A	11/30/2023 11:42:27 am	11/16/2023 06:36:46 am	admin

□	NAME	KEYWORDS	PORTS	LAST UPDATED	SUBSCRIPTION	STATUS
□	aaa Custom		0	11/07/2023 05:53:04 pm	Unsubscribed	✓ Enabled
□	qqq Custom		0	11/07/2023 05:53:08 pm	Unsubscribed	✓ Enabled
□	Search Pattern Rule test 6 Custom	w;dHM;rabbit	0	11/23/2023 09:45:27 am	Unsubscribed	✓ Enabled

Showing 3 out of 3 | 0 selected

You must create a policy with the **Search Pattern Rule** type and associate the policy with the group having a Decoder service, and then publish the policy.

For more information on adding the search pattern rule content to a policy, see Create and Publish Policies.

For more information on groups, see Manage Groups.

You can perform following operations for Search Pattern Rule:

- View Search Pattern Rule Details
- Create a Search Pattern Rule
- Edit a Search Pattern Rule
- Clone a Search Pattern Rule
- Delete a Search Pattern Rule
- Filter Search Pattern Rules
- Filter Search Pattern Rules from Policy Details View

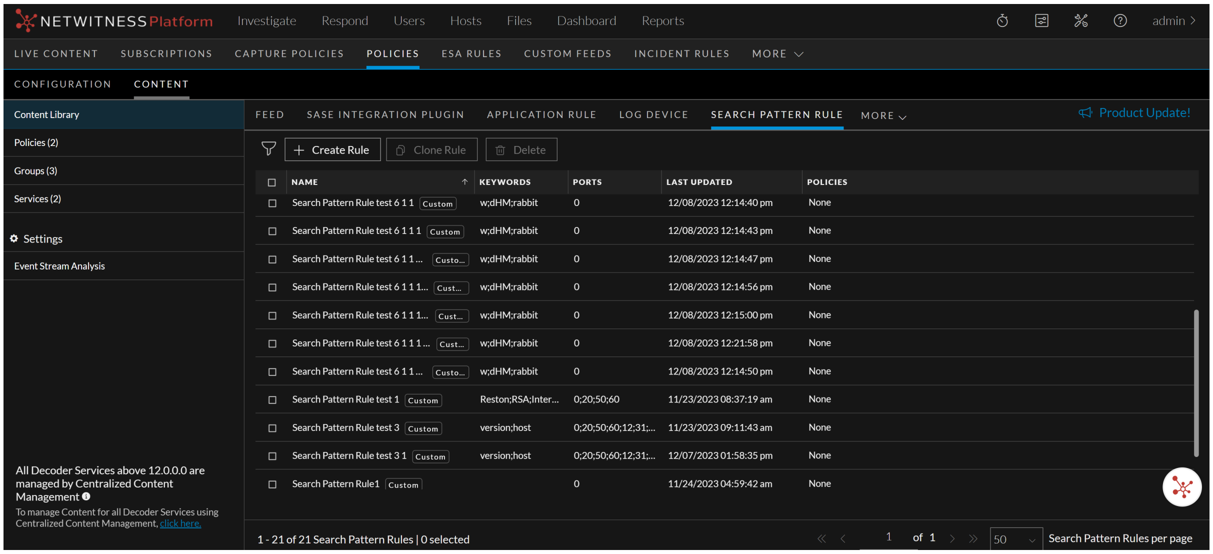
View Search Pattern Rule Details

This topic describes the steps to view the search pattern rule details.

To view the Search Pattern Rule details

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **More** > **Search Pattern Rule**.

The Search Pattern Rule tab is displayed.



☐	NAME	KEYWORDS	PORTS	LAST UPDATED	POLICIES
☐	Search Pattern Rule test 6 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14:40 pm	None
☐	Search Pattern Rule test 6 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14:43 pm	None
☐	Search Pattern Rule test 6 1 1 ... Custo...	w;dHM;rabbit	0	12/08/2023 12:14:47 pm	None
☐	Search Pattern Rule test 6 1 1 1... Cust...	w;dHM;rabbit	0	12/08/2023 12:14:56 pm	None
☐	Search Pattern Rule test 6 1 1 1... Cust...	w;dHM;rabbit	0	12/08/2023 12:15:00 pm	None
☐	Search Pattern Rule test 6 1 1 1 ... Cust...	w;dHM;rabbit	0	12/08/2023 12:21:58 pm	None
☐	Search Pattern Rule test 6 1 1 ... Custo...	w;dHM;rabbit	0	12/08/2023 12:14:50 pm	None
☐	Search Pattern Rule test 1 Custom	Reston;RSA;Inter...	0;20;50;60	11/23/2023 08:37:19 am	None
☐	Search Pattern Rule test 3 Custom	version;host	0;20;50;60;12;31;...	11/23/2023 09:11:43 am	None
☐	Search Pattern Rule test 3 1 Custom	version;host	0;20;50;60;12;31;...	12/07/2023 01:58:35 pm	None
☐	Search Pattern Rule1 Custom		0	11/24/2023 04:59:42 am	None

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

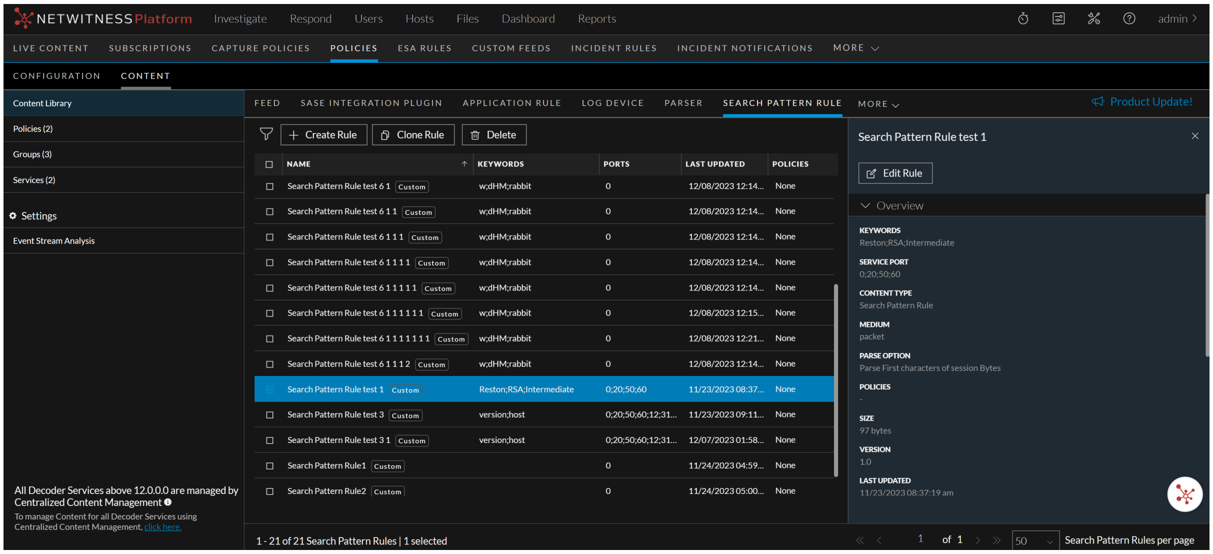
To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 21 of 21 Search Pattern Rules | 0 selected

1 of 1 50 Search Pattern Rules per page

5. Click a row to view details about the selected search pattern rule in the right panel.

   The various details of the search pattern rule are displayed.



☐	NAME	KEYWORDS	PORTS	LAST UPDATED	POLICIES
☐	Search Pattern Rule test 6 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14...	None
☐	Search Pattern Rule test 6 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14...	None
☐	Search Pattern Rule test 6 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14...	None
☐	Search Pattern Rule test 6 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14...	None
☐	Search Pattern Rule test 6 1 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14...	None
☐	Search Pattern Rule test 6 1 1 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:15...	None
☐	Search Pattern Rule test 6 1 1 1 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:21...	None
☐	Search Pattern Rule test 6 1 1 1 2 Custom	w;dHM;rabbit	0	12/08/2023 12:14...	None
☑	Search Pattern Rule test 1 Custom	Reston;RSA;Intermediate	0;20;50;60	11/23/2023 08:37...	None
☐	Search Pattern Rule test 3 Custom	version;host	0;20;50;60;12;31...	11/23/2023 09:11...	None
☐	Search Pattern Rule test 3 1 Custom	version;host	0;20;50;60;12;31...	12/07/2023 01:58...	None
☐	Search Pattern Rule1 Custom		0	11/24/2023 04:59...	None
☐	Search Pattern Rule2 Custom		0	11/24/2023 05:00...	None

Search Pattern Rule test 1

KEYWORDS
Reston;RSA;Intermediate

SERVICE PORT
0;20;50;60

CONTENT TYPE
Search Pattern Rule

MEDIUM
packet

PARSE OPTION
Parse First characters of session Bytes

POLICIES
-

SIZE
97 bytes

VERSION
1.0

LAST UPDATED
11/23/2023 08:37:19 am

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 21 of 21 Search Pattern Rules | 1 selected

1 of 1 50 Search Pattern Rules per page

Create a Search Pattern Rule

This topic describes the steps to create the search pattern rules.

Prerequisites

- By default, only administrators are allowed to create search patterns. To enable access for analysts, they must contact their administrators.

- To generate the meta keys **found** and **match**, you need to enable the **Search Parser** (found and match), which is disabled by default. To do this, navigate to **(Admin)**> **Services** > select **Decoder** service > > **Config** > **General** > under **Parser Configuration** section, enable the **Search Parser**.

Note: Creating a generic search pattern rule will cause performance issues.

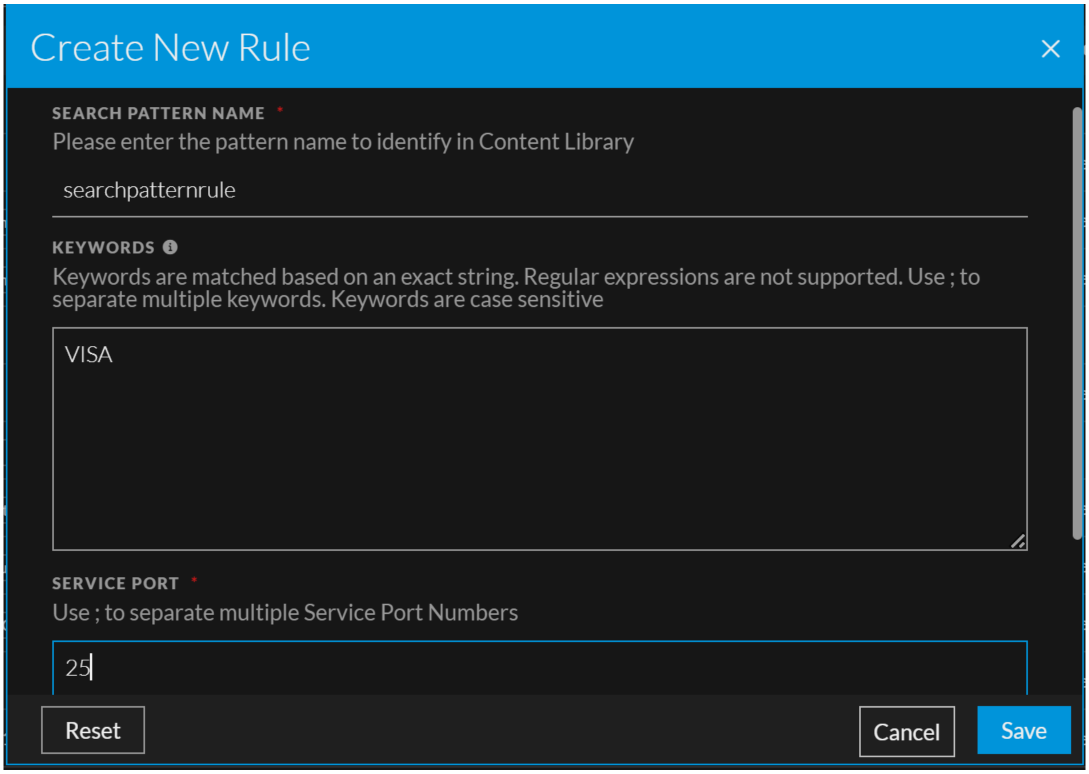
Note: An administrator must enable **source-server.centralpolicy.manage** permission on the source server and **rules.manage** permission on the core devices to allow analysts to create the search pattern rules. For more information, see the "Role Permissions" topic in the *System Security and User Management Guide*.

To create a Search Pattern Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **More** > **Search Pattern Rule**.

   The Search Pattern Rule tab is displayed.
5. Click + **Create Rule**.

   The Create New Rule dialog is displayed.



Create New Rule

SEARCH PATTERN NAME *
Please enter the pattern name to identify in Content Library

searchpatternrule

KEYWORDS
Keywords are matched based on an exact string. Regular expressions are not supported. Use ; to separate multiple keywords. Keywords are case sensitive

VISA

SERVICE PORT *
Use ; to separate multiple Service Port Numbers

25

6. Enter the pattern name to identify them. The name must be unique and can contain a maximum of 256 characters. Use only letters, and numbers.

   Note: Search Pattern names cannot contain spaces.

7. Enter one or more keywords in the **Keywords** text box. Keywords are matched based on an exact string only. Regular expressions (Regex) are not supported.

   Use semicolons (;) to separate multiple keywords. For example, **CreditCard**;**VISA**;**US**. Keywords are case-sensitive. You can enter one or more keywords to improve the chances of detecting an exact string match.

   Note: Non-ASCII characters (for example, é, €, ★ , etc.) are not supported. Enter only ASCII characters when creating a search pattern.

8. Enter one or more port numbers in the **Service Port** field. Use semicolons (;) to separate multiple port numbers. For example, **20**;**21**;**23**.

   Note: The port numbers must be between **1** and **65535**.

9. Click **Save** to create the search pattern rule.

10. Click **Reset** to reset the fields.

Edit a Search Pattern Rule

When you edit the search pattern rule, follow these guidelines:

- The search pattern rule name cannot be edited if the rule is assigned to a policy.
- If the rule assigned to a policy is edited, then the administrator must republish the policy for the changes to take effect in the service.
- While editing the rule name, if the name of that search pattern rule is the same as an existing rule, an error message is displayed.

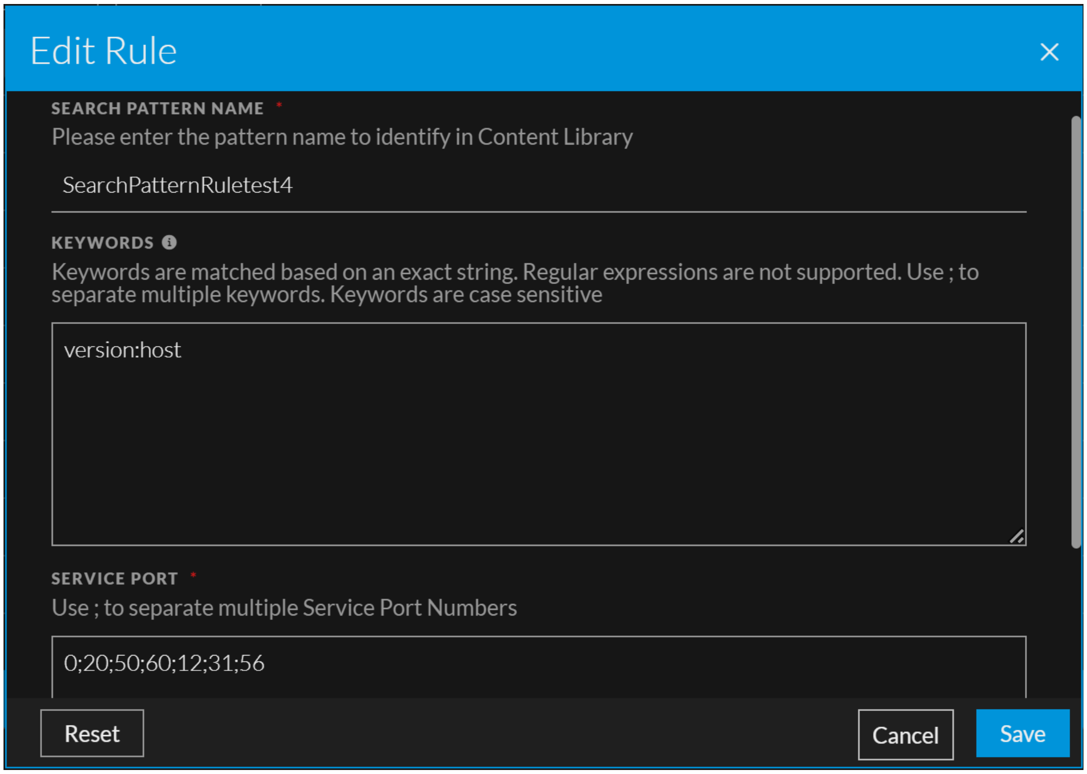
To edit a Search Pattern Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **More** > **Search Pattern Rule**.

   The Search Pattern Rule tab is displayed.

5. Click a row of the search pattern rule to be modified.
6. Click **Edit Rule** to modify the search pattern rule.

   The Edit Rule dialog is displayed.



Edit Rule

SEARCH PATTERN NAME *

Please enter the pattern name to identify in Content Library

SearchPatternRuletest4

KEYWORDS

Keywords are matched based on an exact string. Regular expressions are not supported. Use ; to separate multiple keywords. Keywords are case sensitive

version:host

SERVICE PORT *

Use ; to separate multiple Service Port Numbers

0;20;50;60;12;31;56

7. In the **Edit Rule** panel, do the following:

   a. Enter a unique rule name. The name must be unique and can contain a maximum of 256 characters. Use only letters, and numbers.

      Note: Search Pattern names cannot contain spaces. If the name of that search pattern rule is the same as an existing rule, an error message is displayed.

   b. Enter one or more keywords in the **Keywords** field. Keywords are matched based on an exact string only. Regular expressions (Regex) are not supported.

      Use semicolons (;) to separate multiple keywords. For example, **CreditCard**;**VISA**;**US**. Keywords are case-sensitive. You can enter one or more keywords to improve the chances of detecting an exact string match.

   c. Enter one or more port numbers in the **Service Port** field. Use semicolons (;) to separate multiple port numbers. For example, **20**;**21**;**23**,

      Note: The port numbers must be between **1** and **65535**.

   d. Click **Save** to save the search pattern rule details.

   e. Click **Reset** to reset the fields.

   f. Click **Cancel** to cancel the operation.

Clone a Search Pattern Rule

This topic describes the steps to clone a Search Pattern rule.

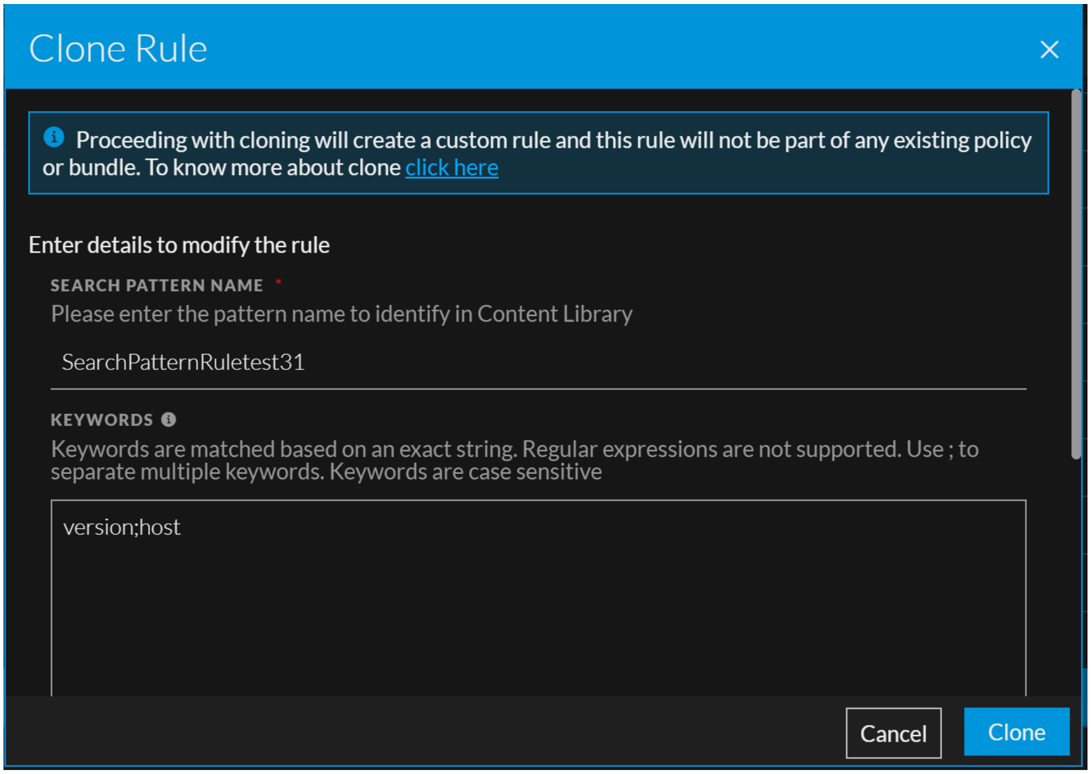
Note:
• Cloning will create a search pattern rule and will not be associated with any existing policy.
• You can clone existing search pattern rules to generate new ones with different rule names but with the same parameters.
• You can clone only one search pattern rule at a time.

To Clone a Search Pattern Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **More** > **Search Pattern Rule**.

   The Search Pattern Rule tab is displayed.
5. Select a search pattern rule and click **Clone Rule**.

   The Clone Rule dialog is displayed.



Clone Rule

Proceeding with cloning will create a custom rule and this rule will not be part of any existing policy or bundle. To know more about clone click here

Enter details to modify the rule

SEARCH PATTERN NAME *
Please enter the pattern name to identify in Content Library
SearchPatternRuletest31

KEYWORDS
Keywords are matched based on an exact string. Regular expressions are not supported. Use ; to separate multiple keywords. Keywords are case sensitive
version;host

6. In the **Clone Rule** panel, do the following:

   a. Enter a unique name for the search pattern rule clone. The name can contain a maximum of 256 characters. Use only letters, and numbers.

   Note: Rule names are always appended with a number. For example, if the rule has the name **SearchPatternRuletest3**, its name will be changed to **SearchPatternRuletest31** after the cloning.

b. Enter one or more keywords in the **Keywords** text box. Keywords are matched based on an exact string only. Regular expressions (Regex) are not supported.

   Use semicolons (;) to separate multiple keywords. For example, **CreditCard**;**VISA**;**US**. Keywords are case-sensitive. You can enter one or more keywords to improve the chances of detecting an exact string match.

c. Enter one or more port numbers in the **Service Port** field. Use semicolons (;) to separate multiple port numbers. For example, **20**;**21**;**23**,

   > **Note:** The port numbers must be between **1** and **65535**.

d. Click **Clone** to clone the search pattern rule details.

e. Click **Cancel** to cancel the operation.

Delete a Search Pattern Rule

When you delete the search pattern rule, follow these guidelines:

- You cannot delete the search pattern rule if it is associated with a policy. You should first disassociate the search pattern rule from the policy and then delete it.
- If you select a search pattern rule that is associated with a policy and another that is not associated with a policy, the delete button will be disabled.

To delete a Search Pattern Rule

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.
4. Click **More** > **Search Pattern Rule**.

   The Search Pattern Rule tab is displayed.
5. Select one or more search pattern rules and click **Delete**.

   A confirmation pop-up is displayed.
6. Click **Delete** to permanently delete the selected search pattern rules.

Filter Search Pattern Rules

The Filters panel allows you to filter the list of search pattern rules under the content library based on the name, keywords, ports, last updated date, and source type.

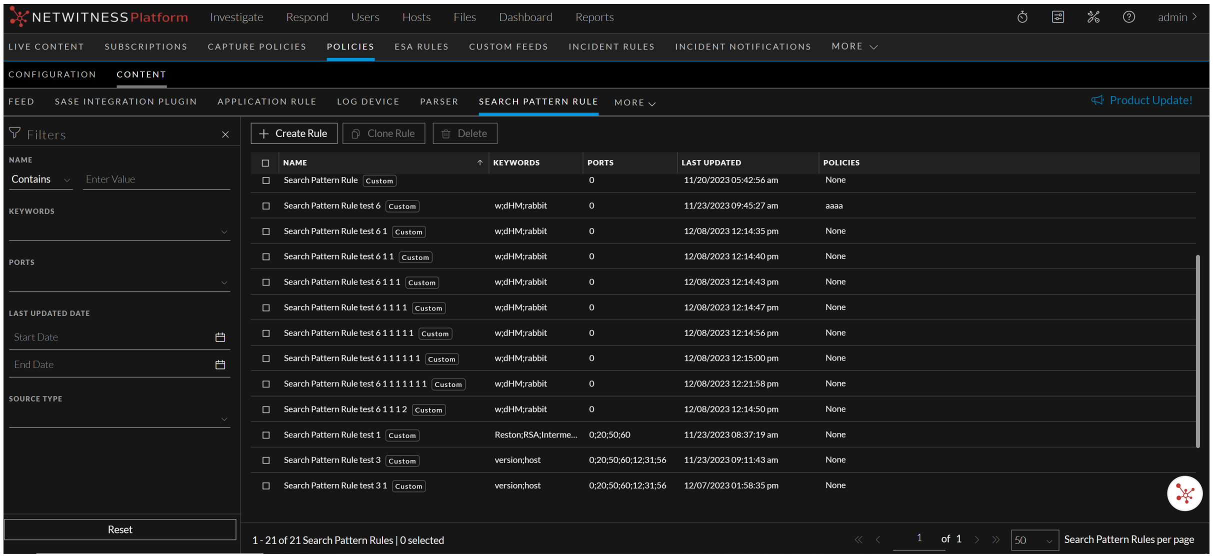
To filter the search pattern rules

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Content Library**.

4. Click **More** > **Search Pattern Rule**.

   The Search Pattern Rule tab is displayed.

5. By default, the filters panel is hidden. Click the ⏷ (Filters) icon in the toolbar to expand the filters panel.



□	NAME	KEYWORDS	PORTS	LAST UPDATED	POLICIES
□	Search Pattern Rule Custom		0	11/20/2023 05:42:56 am	None
□	Search Pattern Rule test 6 Custom	w;dHM;rabbit	0	11/23/2023 09:45:27 am	aaaa
□	Search Pattern Rule test 6 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14:35 pm	None
□	Search Pattern Rule test 6 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14:40 pm	None
□	Search Pattern Rule test 6 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14:43 pm	None
□	Search Pattern Rule test 6 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14:47 pm	None
□	Search Pattern Rule test 6 1 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:14:56 pm	None
□	Search Pattern Rule test 6 1 1 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:15:00 pm	None
□	Search Pattern Rule test 6 1 1 1 1 1 1 1 Custom	w;dHM;rabbit	0	12/08/2023 12:21:58 pm	None
□	Search Pattern Rule test 6 1 1 1 2 Custom	w;dHM;rabbit	0	12/08/2023 12:14:50 pm	None
□	Search Pattern Rule test 1 Custom	Reston;RSA;Interme...	0;20;50;60	11/23/2023 08:37:19 am	None
□	Search Pattern Rule test 3 Custom	version;host	0;20;50;60;12;31;56	11/23/2023 09:11:43 am	None
□	Search Pattern Rule test 3 1 Custom	version;host	0;20;50;60;12;31;56	12/07/2023 01:58:35 pm	None

1 - 21 of 21 Search Pattern Rules | 0 selected

1 of 1 50 Search Pattern Rules per page

6. To search by name:

   - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the search pattern rule. Type one character, and a list of search pattern rules that contain that character is displayed, as you continue to type, the list is filtered to match.

   - Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular rule will be displayed.

7. To search by keywords, select one or more keywords that are listed in the **Keywords** drop-down list. The filter is an AND operator when searching for multiple keywords, such as **Visa** and **MasterCard**. In this case, the filter results will display all matches that contain both Visa and MasterCard.

8. To search by ports, select one or more port numbers that are listed in the **Ports** drop-down list. The filter is an AND operator when searching for multiple port numbers, such as **25** and **34**. In this case, the filter results will display all matches that contain both 25 and 34.

9. To filter by date range, under the **Last Update Date**, select the start date and end date from the date fields.

   For example, to filter search pattern rules that were updated between May 1 and May 31, you select May 1 as the start date and May 31 as the end date. You must enter dates in mm/dd/yyyy format, or you can click and pick dates from a calendar.

10. To filter by source type, select one or more sources from the **Source Type** drop-down list. The options are listed below:

    - **Custom**

    - **Live**

11. To hide, click the ✕ icon at the top-right of the panel.

The search pattern rules are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.

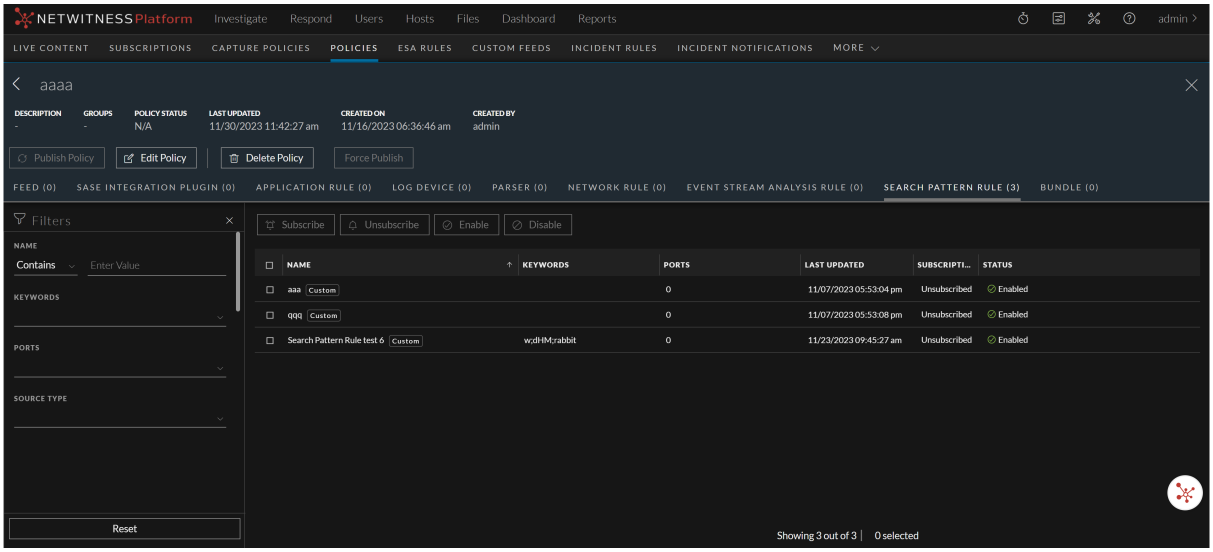
Filter Search Pattern Rules from Policy Details View

The Filters panel allows you to filter the list of displayed search pattern rules in the policy details view based on the name, keywords, ports, source type, enabled/disabled status, subscription status, resource-created date, and last updated date.

To filter the search pattern rules

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Do one of the following:
   - Click a policy name.
   - Click a row to view details about the selected policy and click **View Details**.

   The policy details view is displayed.
5. Click the **Search Pattern Rule** tab.
6. By default, the filters panel is hidden. Click the (Filters) icon in the toolbar to expand the filters panel.



aaaa

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	-	N/A	11/30/2023 11:42:27 am	11/16/2023 06:36:46 am	admin

NAME
Contains Enter Value

KEYWORDS

PORTS

SOURCE TYPE

☐	NAME	KEYWORDS	PORTS	LAST UPDATED	SUBSCRIPTI...	STATUS
☐	aaa Custom		0	11/07/2023 05:53:04 pm	Unsubscribed	✓ Enabled
☐	qqq Custom		0	11/07/2023 05:53:08 pm	Unsubscribed	✓ Enabled
☐	Search Pattern Rule test 6 Custom	w;dHM;rabbit	0	11/23/2023 09:45:27 am	Unsubscribed	✓ Enabled

Showing 3 out of 3 | 0 selected

7. To search by name:
   - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the search pattern rule. Type one character, and a list of search pattern rules that contain that character is displayed, as you continue to type, the list is filtered to match.
   - Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular rule will be displayed.

8. To search by keywords, select one or more keywords that are listed in the **Keywords** drop-down list. The filter is an AND operator when searching for multiple keywords, such as **Visa** and **MasterCard**. In this case, the filter results will display all matches that contain both Visa and MasterCard.
9. To search by ports, select one or more port numbers that are listed in the **Ports** drop-down list. The filter is an AND operator when searching for multiple port numbers, such as **25** and **34**. In this case, the filter results will display all matches that contain both 25 and 34.
10. To filter by source type, select one or more sources from the **Source Type** drop-down list. The options are listed below:
    - **Custom**
    - **Live**
11. To filter by enabled/disabled status, select one or more statuses from the **Enabled/Disabled Status** drop-down list. The options are listed below:
    - **Enabled**
    - **Disabled**
12. To filter by subscription status, select one or more statuses from the **Subscription** drop-down list. The options are listed below:
    - **Subscribed**
    - **Unsubscribed**
13. To filter by a resource created date range, under the **Resource Created Date**, select the start date and end date from the date fields.

    For example, to filter contents that were created between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.
14. To filter by date range, under the **Last Update Date**, select the start date and end date from the date fields.

    For example, to filter search pattern rules that were updated between May 1 and May 31, you select May 1 as the start date and May 31 as the end date. You must enter dates in mm/dd/yyyy format, or you can click and pick dates from a calendar.
15. To hide, click the ☒ icon at the top-right of the panel.

    The search pattern rules are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.

Filter Content Rules

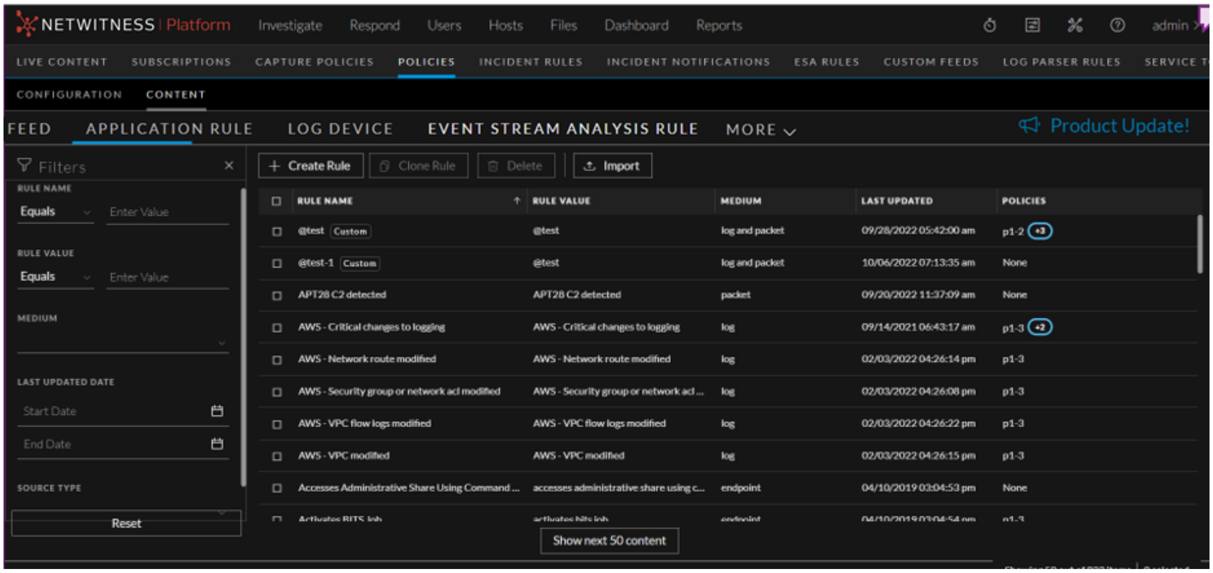
The Filters panel allows you to filter the list of displayed contents under the content library based on the name, medium, date range, and source type.

This applies to the following content rule types:

- Feed
- Application Rule
- Log Device
- Lua Parser
- Network Rule
- Event Steam Analysis Rule
- Search Pattern Rule
- Bundle

To filter the content rules

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Content Library**.
4. By default, the filters panel is hidden, click the (Filters) icon in the toolbar to expand the filters panel.



☐	RULE NAME	RULE VALUE	MEDIUM	LAST UPDATED	POLICIES
☐	@test Custom	@test	log and packet	09/28/2022 05:42:00 am	p1-2 +3
☐	@test-1 Custom	@test	log and packet	10/06/2022 07:13:35 am	None
☐	APT28 C2 detected	APT28 C2 detected	packet	09/20/2022 11:37:09 am	None
☐	AWS - Critical changes to logging	AWS - Critical changes to logging	log	09/14/2021 06:43:17 am	p1-3 +2
☐	AWS - Network route modified	AWS - Network route modified	log	02/03/2022 04:26:14 pm	p1-3
☐	AWS - Security group or network acl modified	AWS - Security group or network acl ...	log	02/03/2022 04:26:08 pm	p1-3
☐	AWS - VPC flow logs modified	AWS - VPC flow logs modified	log	02/03/2022 04:26:22 pm	p1-3
☐	AWS - VPC modified	AWS - VPC modified	log	02/03/2022 04:26:15 pm	p1-3
☐	Accesses Administrative Share Using Command ...	accesses administrative share using c...	endpoint	04/10/2019 03:04:53 pm	None
☐	Activates BITS Job	activates bits job	endpoint	04/10/2019 03:04:54 pm	p1-3

5. To search by rule name:
   - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the rule. Type one character and a list of rules that contain that character is displayed, as you continue to type the list is filtered to match.
   - Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular content type will be displayed.

6. To filter by rule value:

   - Set the filter option to **Contains** operator from the drop-down list and start typing the rule value. Type one character and a list of rules that contain the rule value with that character is displayed, as you continue to type the list is filtered to match.

   - Set the filter option to **Equals** operator from the drop-down list and enter the full rule value. The particular content type will be displayed.

7. To filter by medium, select one or more mediums from the **Medium** drop-down list. The options are listed below:

   - **endpoint**

   - **log**

   - **log and packet**

   - **packet**

8. To filter by date range, under the **Last Update date**, select the start date and end date from the date fields.

   For example, to filter policies that were updated between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.

9. To filter by source type, select one or more sources from the **Source Type** drop-down list. The options are listed below:

   - **Custom**

   - **Live**

10. To hide, click the ☒ icon at the top-right of the panel.

    The contents are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.

Manage Groups

This section contains:

- Create a Group
- View a Group
- Delete a Group
- Edit a Group
- Filter Groups

Create a Group

You can create a group with one or more services and assign one policy to it. Groups may be created without any assigned policy; however, a policy must be assigned to a group and Published in order for any content changes to take effect.

To create a Group

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Groups**.
4. In the tool bar, click **+ Create New**.
5. In the **New Group** panel, do the following:
   - Enter the name of the group.
   - Enter the description for the group.
6. Click **Next**.
7. 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.
   > - ESA Services are not disabled when assigned to a group, as the ESA services can be assigned to more than one group.

8. Click **Next**.
9. In the **Assign Policies**, click + to assign policies to a group. You can assign only one policy to any particular group.

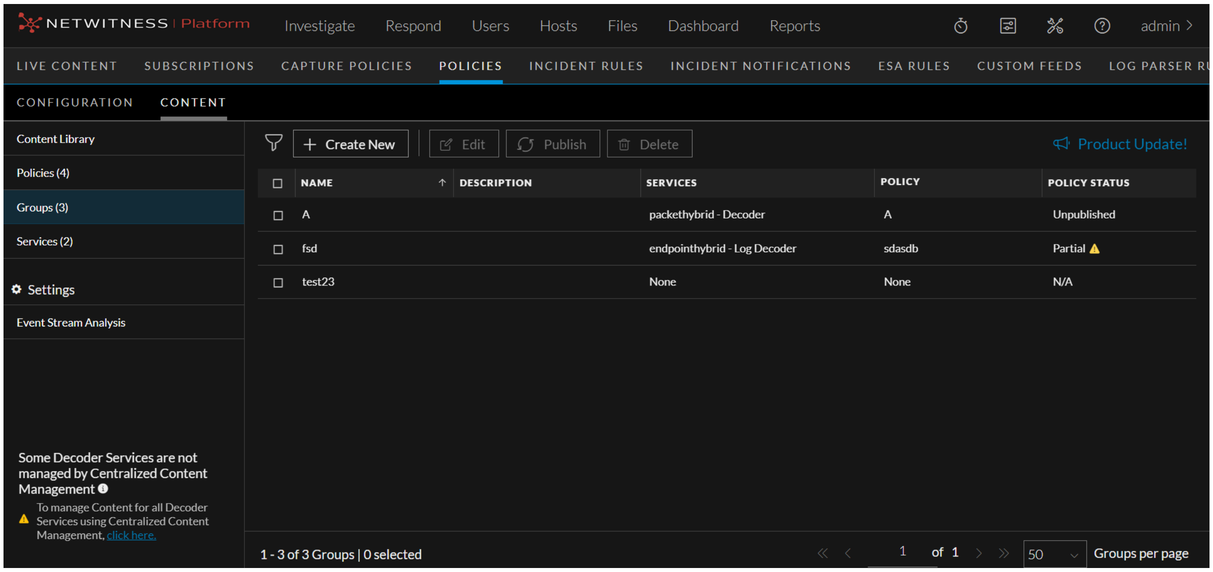
10. Do any one of the following:
    - Click **Save and Publish** to save and publish the settings.
    - Click **Save and Close** to save the settings.

View a Group

This topic describes the steps to view the properties of Group.

To view the properties of the selected Group

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Groups**. The available groups are displayed. By default, 50 groups are displayed per page. To go to the next page, click >. To go to the last page, click >>.



□	NAME	DESCRIPTION	SERVICES	POLICY	POLICY STATUS
□	A		packethybrid - Decoder	A	Unpublished
□	fsd		endpointhybrid - Log Decoder	sdasdb	Partial ⚠
□	test23		None	None	N/A

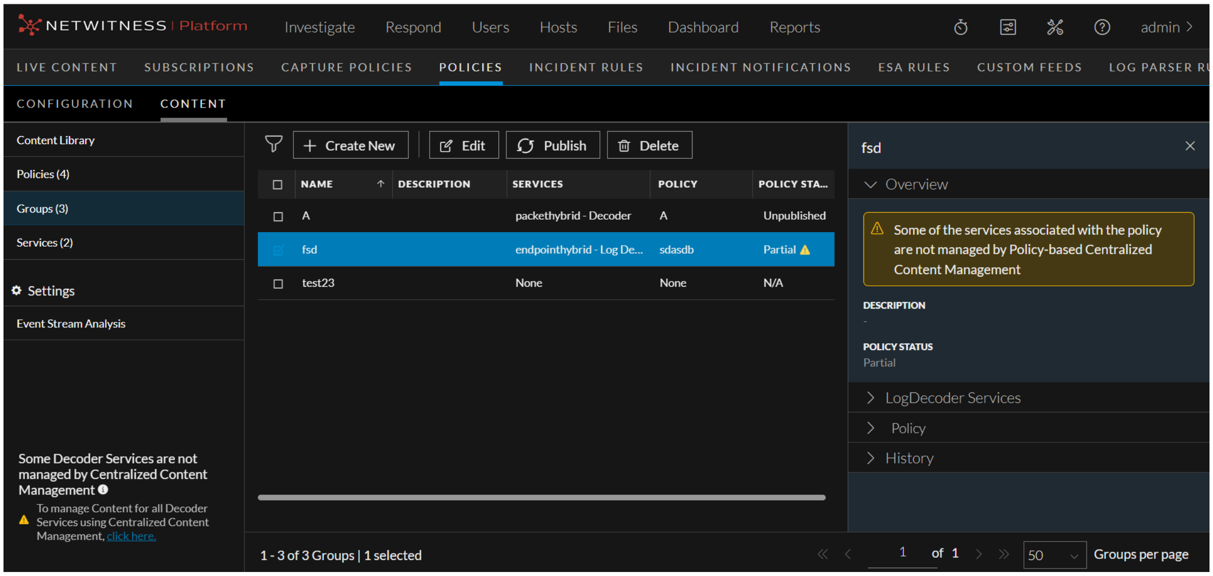
Some Decoder Services are not managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 3 of 3 Groups | 0 selected

1 of 1 50 Groups per page

4. Click a row to view details about the selected group in the right panel.



☐	NAME	DESCRIPTION	SERVICES	POLICY	POLICY STA...
☐	A		packethybrid - Decoder	A	Unpublished
☑	fsd		endpointhybrid - Log De...	sdasdb	Partial ⚠
☐	test23		None	None	N/A

1 - 3 of 3 Groups | 1 selected

Some Decoder Services are not managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

fsd

Overview

⚠ Some of the services associated with the policy are not managed by Policy-based Centralized Content Management

DESCRIPTION
-

POLICY STATUS
Partial

Caution:

- An icon ⚠ is displayed in the Groups View indicating policy status unpublished, if any services are part of the selected group and do not have any deployment then some of the associated correlation services require ESA deployments.
- An icon ❗ is displayed in the Groups View, indicating that the policy status failed for multiple reasons. Please see the groups overview section in the UI to find the failure reason and the workaround.

Delete a Group

You can delete one or more groups. Once the group is deleted, all services will be removed from the group and all the policy content will be deleted from the services.

To delete a Group

1. Go to ☰ **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Groups**. The available groups are displayed.
4. Select one or more Groups and click **Delete**.

   The Delete Groups dialog is displayed.
5. To delete the deployed content from the services upon deleting the group, select the option **Delete deployed content from the services on group removal**. For ESA service, the content will be deleted upon deleting the group.
6. Click **Delete** to permanently delete the selected group.

   The confirmation message is displayed.

> **Note:**
> - For a group with multiple services, even if we fail to delete a particular service under the group, the other services will get deleted. The service which is not deleted will be in **Failed** state.
> - The group status changes to **Failed** if group deletion fails for any particular reason.

Edit a Group

You can edit the properties of the group at any point in time. The status of the updated group is unpublished if you change the service or policies in a group. If you just change the group name and description, then the status remains published (if it is already published).

To edit the selected Group

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Group**. The available groups are displayed.
4. Select a group to edit and click **Edit**.
5. Make the required changes in the group.
6. Do any one of the following:
   - Click **Save and Publish** to save and publish the policy.

     > **Note:**
     > - While removing a service from the group, you can opt to either delete the content of the service and remove the service or just remove the service from the group. While removing a service that has Log Device content, you can delete the Custom Parser and disable the Base Log Device Parser from the service.
     > - While removing the group from the policy, the ESA content will be deleted by default.

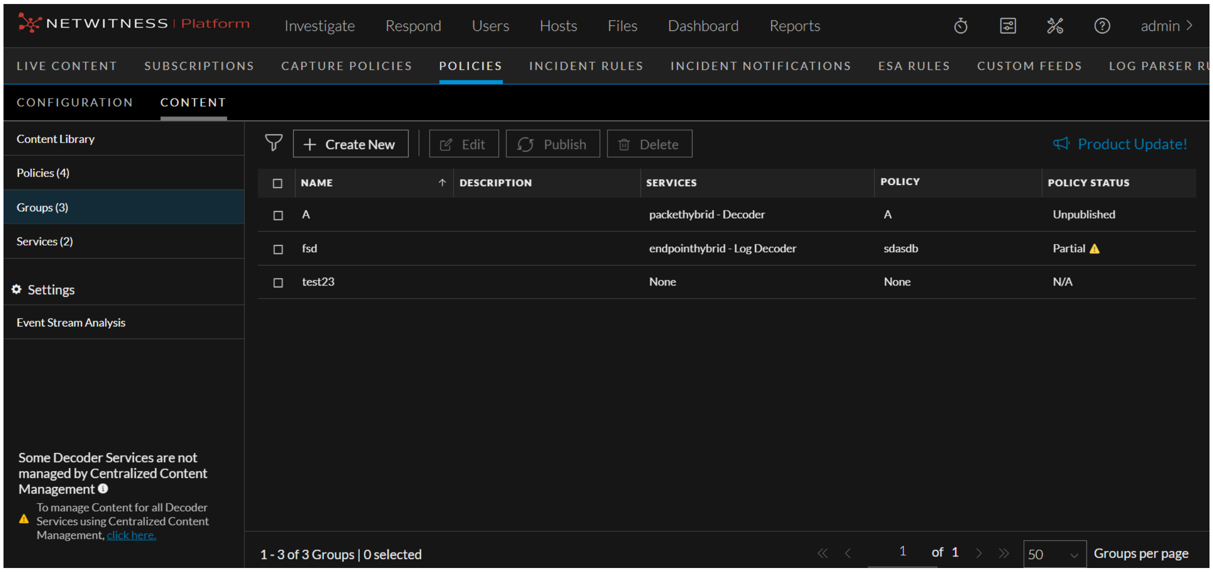
   - The policy will be listed under the Unpublished category.
   - Click **Save and Close** to save the settings and return to the Policies view.

Filter Groups

The Filters Panel for content group allows you to filter the list of displayed groups, based on the group name, policy status, services and policies.

To filter the Groups

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Groups**. The available groups are displayed.



☐	NAME	DESCRIPTION	SERVICES	POLICY	POLICY STATUS
☐	A		packethybrid - Decoder	A	Unpublished
☐	fsd		endpointhybrid - Log Decoder	sdasdb	Partial ⚠
☐	test23		None	None	N/A

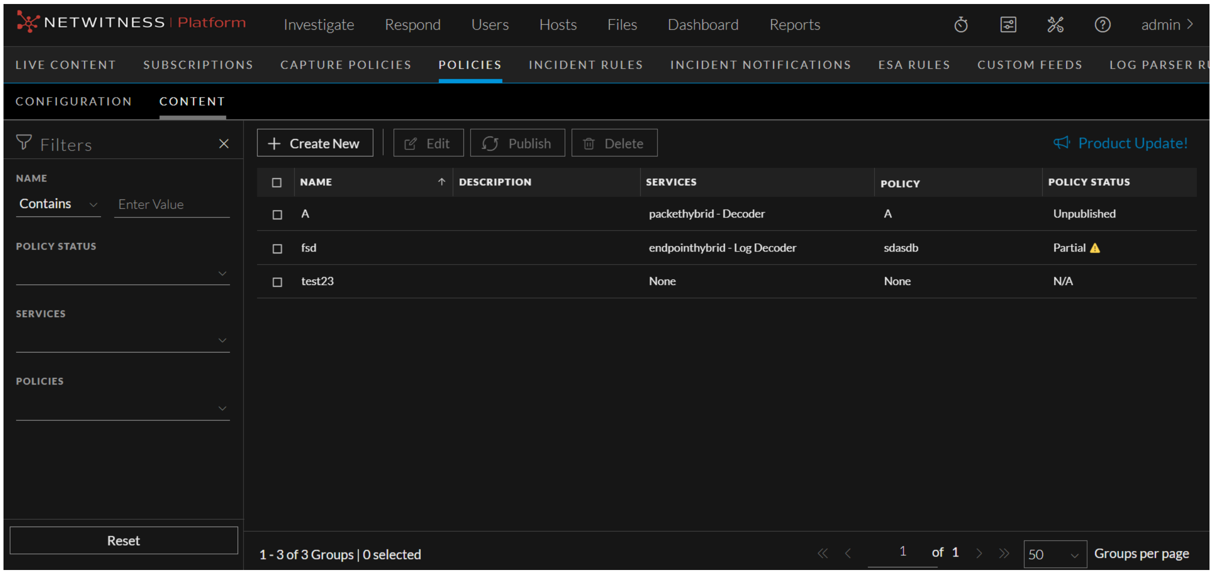
Some Decoder Services are not managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 3 of 3 Groups | 0 selected

1 of 1 | 50 | Groups per page

4. To filter the groups, click ▽. The filter panel is displayed.



☐	NAME	DESCRIPTION	SERVICES	POLICY	POLICY STATUS
☐	A		packethybrid - Decoder	A	Unpublished
☐	fsd		endpointhybrid - Log Decoder	sdasdb	Partial ⚠
☐	test23		None	None	N/A

1 - 3 of 3 Groups | 0 selected

1 of 1 | 50 | Groups per page

5. On the filter panel, do the following:

   a. Select the **Name** drop-down value as either **Equals** or **Contains**. To search the group name using the **Contains** operator, set the filter option to **Contains** operator from the drop-down list and start typing the name of the group. Type one character and a list of group that contain that character is displayed, as you continue to type, the list is filtered to match. To search the group name using the **Equals** operator, set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular group name will be displayed.

   b. Select the **Policy Status** from the drop-down list. The various drop-down values are:

      i. **Published**: Groups that are published to use.

      ii. **Unpublished**: Groups that are saved but not published.

      iii. **Failed**: Groups that are failed to publish.

    iv. **N/A**: Groups for which publication status is not applicable.
    v. **Partial**: Groups that are partially published.

c. Select the **Services** from the drop-down list.

d. Select the **Policies** from the drop-down list.

e. To reset the fields, click **Reset**.

Manage Policies

This section contains:

Create and Publish Policies

You can create a policy and assign it to one or more groups.

To create a Policy

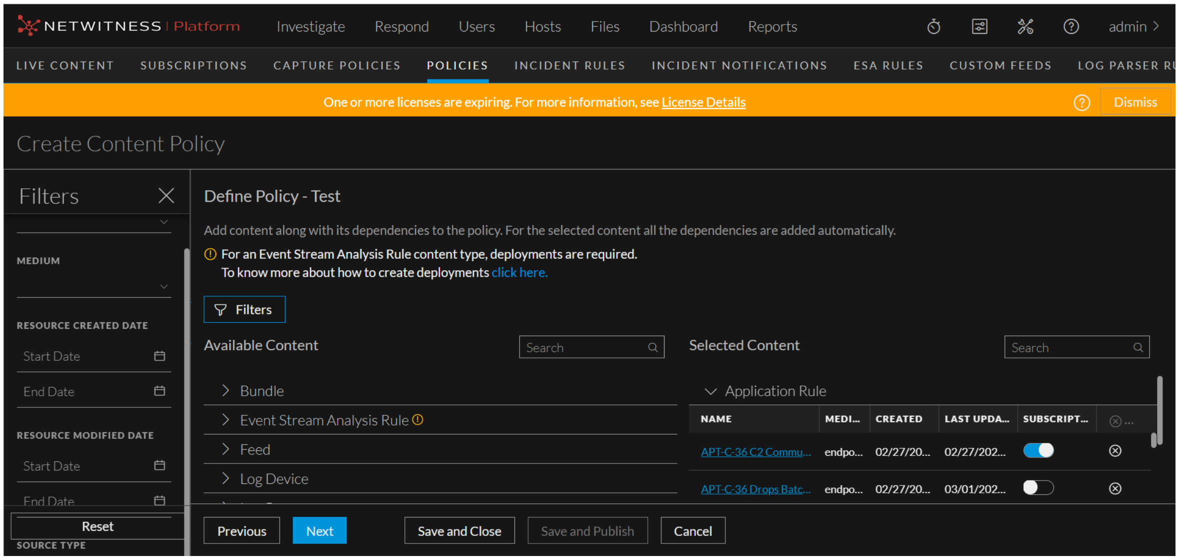
1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**.

   The available policies are displayed.
4. Click **+ Create New** to add a new policy.
5. In the **New Policy** panel, do the following:
   - Enter a unique policy name.
   - Enter a description for the policy.
6. Click **Next**.
7. In the **Available Content**, select the content type and click + to add the content to the policy. To add all content based on the resource type, click ⊕ ALL. After you add the content, you can enable subscription (if required) by clicking subscribed toggle. Once the content is subscribed the updates are pushed automatically. To conveniently search the available content, type the initial content text in

the **Search** box available under the **Available Content** .To conveniently search the selected content, type the initial content text in the **Search** box available under the **Selected Content** .

8. To filter both available and selected content, do the following:

   - Click the icon. The filter panel window is displayed.



One or more licenses are expiring. For more information, see License Details

Define Policy - Test

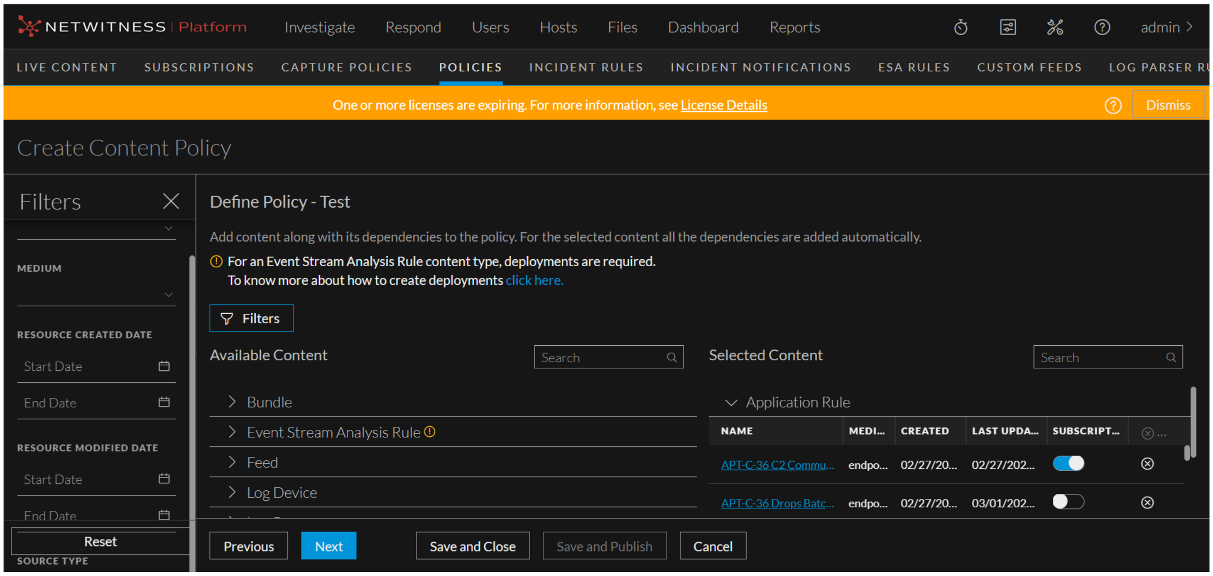
Add content along with its dependencies to the policy. For the selected content all the dependencies are added automatically.

For an Event Stream Analysis Rule content type, deployments are required.
To know more about how to create deployments click here.

NAME	MEDI...	CREATED	LAST UPDA...	SUBSCRIPT...
APT-C-36 C2 Commu...	endpo...	02/27/20...	02/27/202...	●
APT-C-36 Drops Batc...	endpo...	02/27/20...	03/01/202...	○

   - Select the **Resource Types** from the available drop-down values.
   - Select the **Medium** from the available drop-down values.
   - Select the **Resource Created Date** and **Resource Modified Date**.
   - To reset the fields, click **Reset**.

> **Note:** Subscription is not allowed for custom content.



One or more licenses are expiring. For more information, see License Details

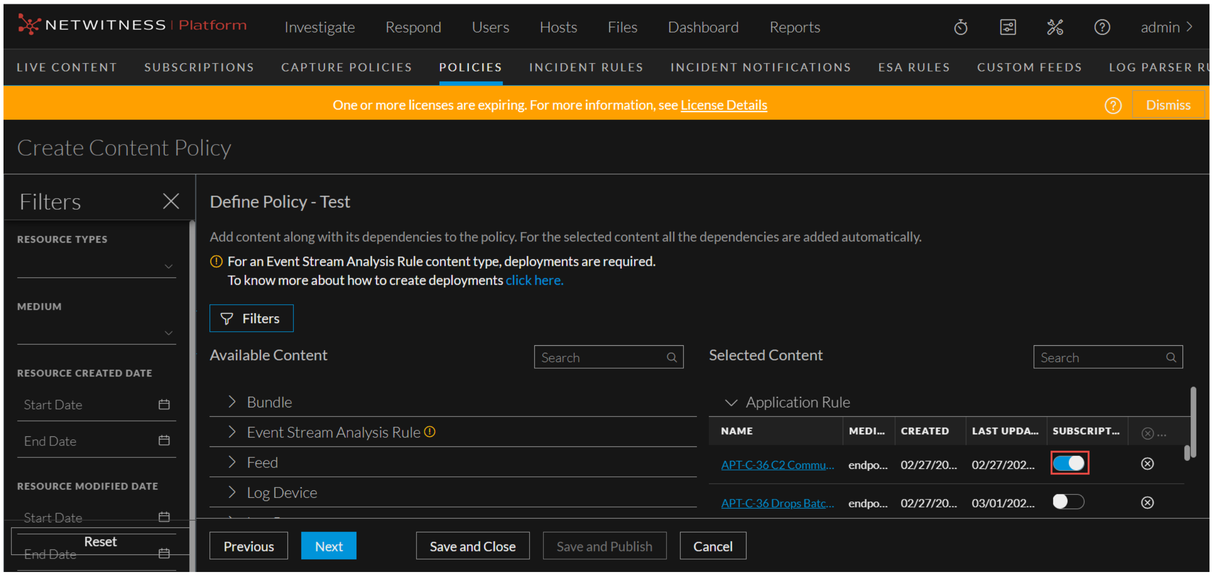
Define Policy - Test

Add content along with its dependencies to the policy. For the selected content all the dependencies are added automatically.

For an Event Stream Analysis Rule content type, deployments are required.
To know more about how to create deployments click here.

NAME	MEDI...	CREATED	LAST UPDA...	SUBSCRIPT...
APT-C-36 C2 Commu...	endpo...	02/27/20...	02/27/202...	●
APT-C-36 Drops Batc...	endpo...	02/27/20...	03/01/202...	○

9. **Note:**
- All the dependencies are added automatically for the selected content. You can click on the content name highlighted in blue and look for details such as content description, content type, resources and dependencies and so on. You can also add and subscribe the resource from the details view.



One or more licenses are expiring. For more information, see License Details

Create Content Policy

Define Policy - Test

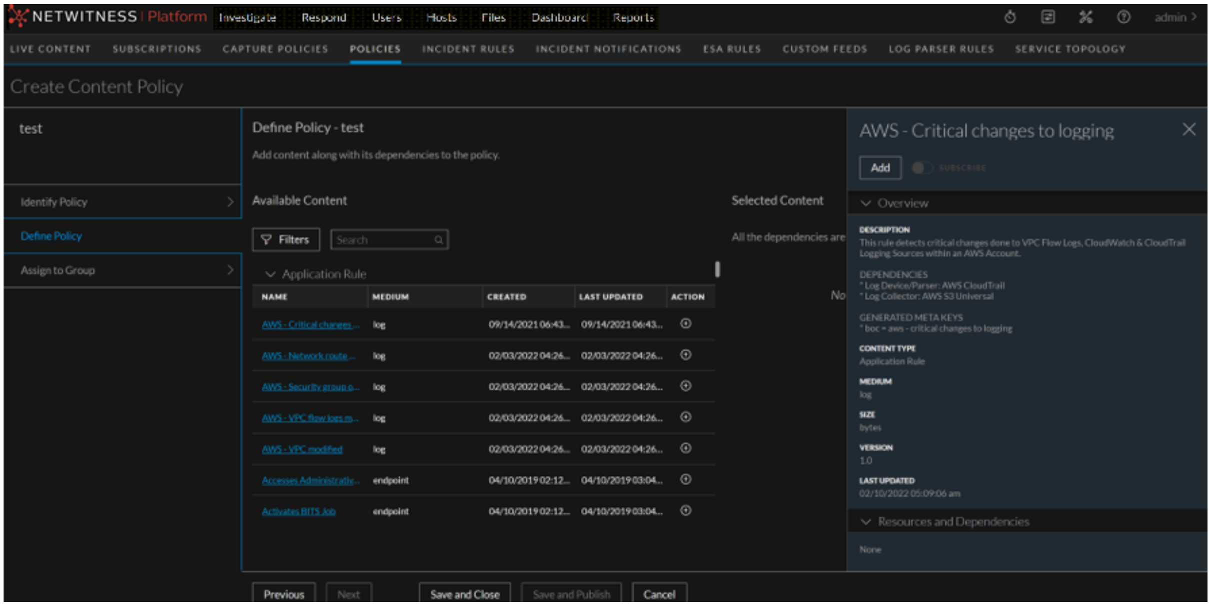
Add content along with its dependencies to the policy. For the selected content all the dependencies are added automatically.

For an Event Stream Analysis Rule content type, deployments are required.
To know more about how to create deployments click here.

Available Content

Selected Content

NAME	MEDI...	CREATED	LAST UPDA...	SUBSCRIPT...
APT-C-36 C2 Commu...	endpo...	02/27/20...	02/27/202...	●
APT-C-36 Drops Batc...	endpo...	02/27/20...	03/01/202...	○



Create Content Policy

Define Policy - test

Add content along with its dependencies to the policy.

Available Content

Selected Content

All the dependencies are

No

NAME	MEDIUM	CREATED	LAST UPDATED	ACTION
AWS - Critical changes ...	log	09/14/2021 06:43...	09/14/2021 06:43...	⊕
AWS - Network route ...	log	02/03/2022 04:26...	02/03/2022 04:26...	⊕
AWS - Security group o...	log	02/03/2022 04:26...	02/03/2022 04:26...	⊕
AWS - VPC flow logs m...	log	02/03/2022 04:26...	02/03/2022 04:26...	⊕
AWS - VPC modified	log	02/03/2022 04:26...	02/03/2022 04:26...	⊕
Accesses Administrativ...	endpoint	04/10/2019 02:12...	04/10/2019 03:04...	⊕
Activates BITS Job	endpoint	04/10/2019 02:12...	04/10/2019 03:04...	⊕

AWS - Critical changes to logging

DESCRIPTION
This rule detects critical changes done to VPC Flow Logs, CloudWatch & CloudTrail Logging Sources within an AWS Account.

DEPENDENCIES
* Log Device/Parser: AWS CloudTrail
* Log Collector: AWS S3 Universal

GENERATED META KEYS
* boc = aws - critical changes to logging

CONTENT TYPE
Application Rule

MEDIUM
log

SIZE
bytes

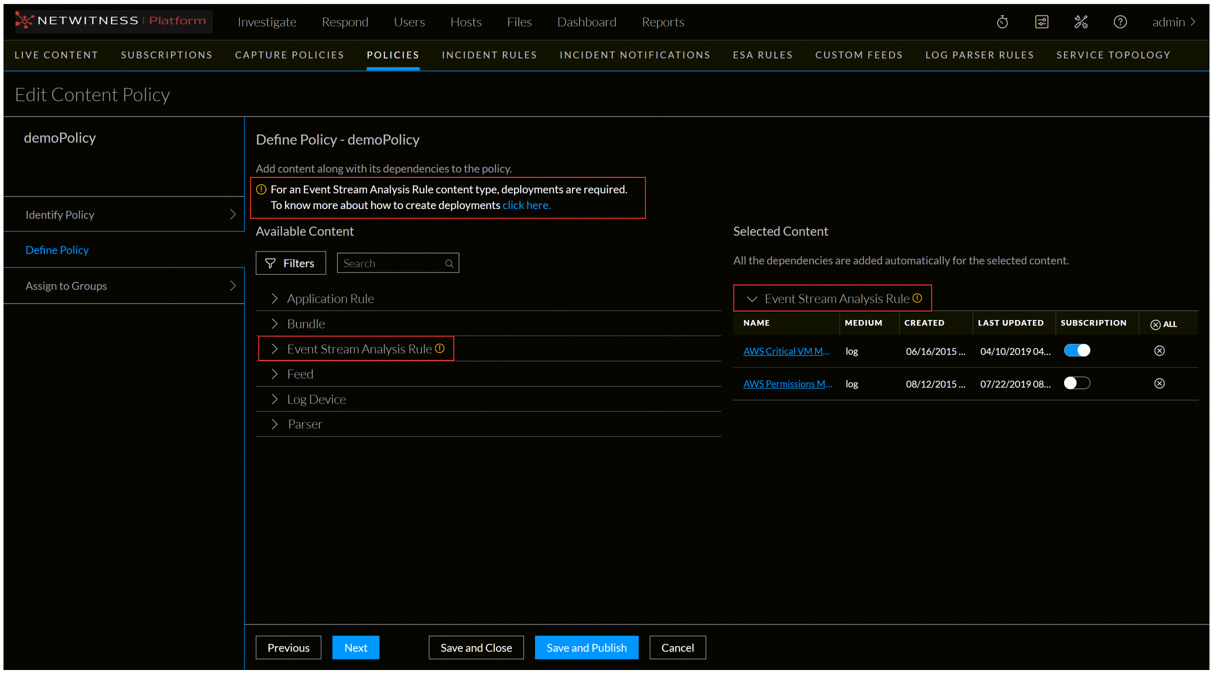
VERSION
1.0

LAST UPDATED
02/10/2022 05:09:06 am

None

A caution icon ⓘ is displayed to create a deployment on three scenarios.

- To implement the **Event Stream Analysis Rule** content type, you must have a deployment.



Edit Content Policy

demoPolicy

Define Policy - demoPolicy

Add content along with its dependencies to the policy.

For an Event Stream Analysis Rule content type, deployments are required.
To know more about how to create deployments click here.

Available Content

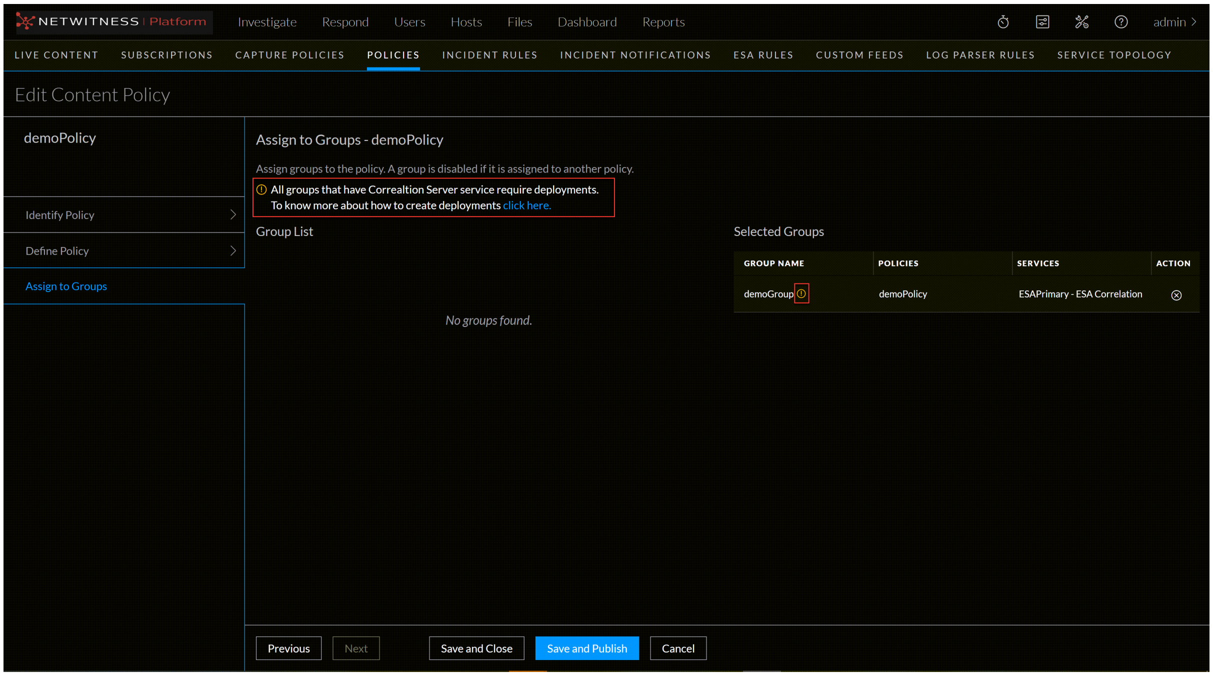
Selected Content

All the dependencies are added automatically for the selected content.

Event Stream Analysis Rule

NAME	MEDIUM	CREATED	LAST UPDATED	SUBSCRIPTION	⊗ ALL
AWS Critical VM M...	log	06/16/2015 ...	04/10/2019 04...	●	⊗
AWS Permissions M...	log	08/12/2015 ...	07/22/2019 08...	○	⊗

- All groups that have correlation server service must have a deployment.



Edit Content Policy

demoPolicy

Assign to Groups - demoPolicy

Assign groups to the policy. A group is disabled if it is assigned to another policy.

All groups that have Correaltion Server service require deployments.
To know more about how to create deployments click here.

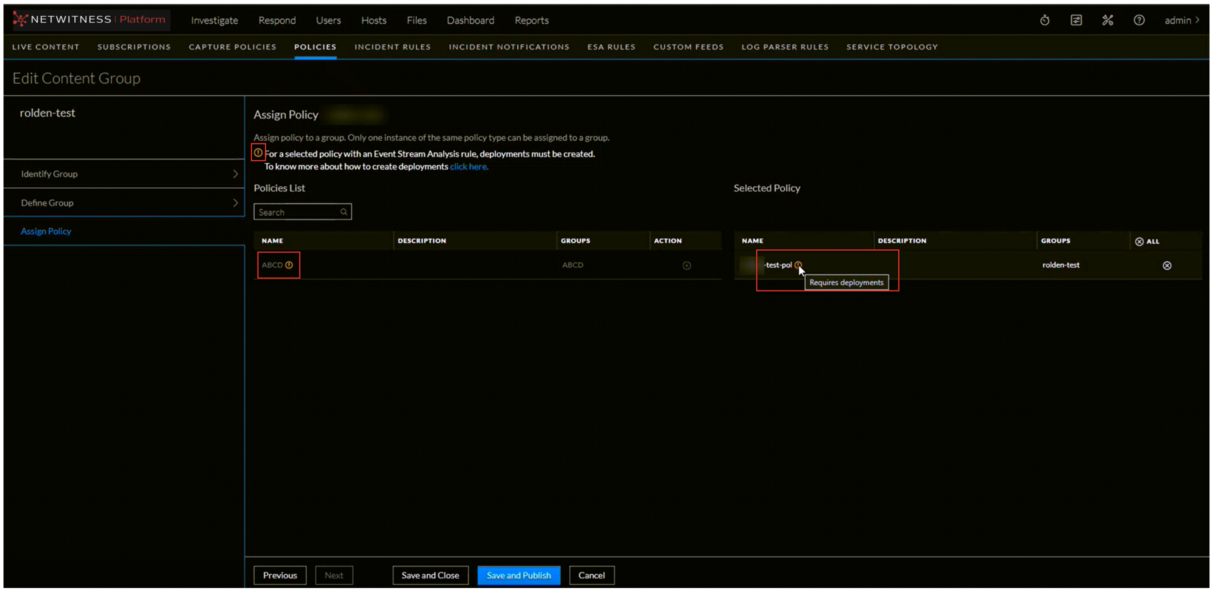
Group List

No groups found.

Selected Groups

GROUP NAME	POLICIES	SERVICES	ACTION
demoGroup	demoPolicy	ESAPrimary - ESA Correlation	⊗

- For any selected policy with an ESA rule, deployment are must be created.



Edit Content Group

rolden-test

Assign Policy

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

NAME	DESCRIPTION	GROUPS	ACTION
ABCD		ABCD	⊕

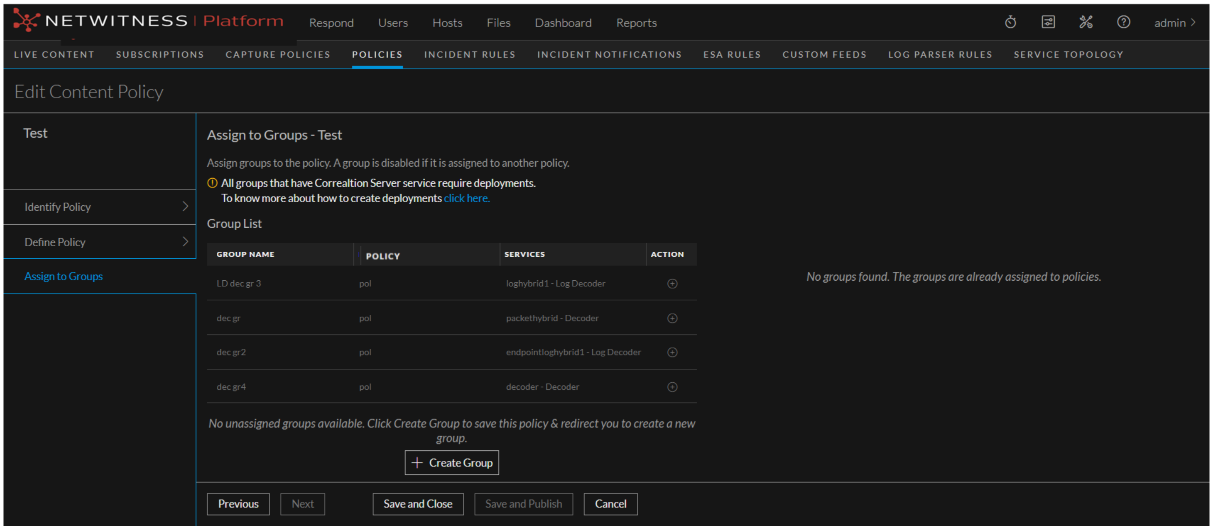
Selected Policy

NAME	DESCRIPTION	GROUPS	⊗ ALL
-test-pol		rolden-test	⊗

To create and manage deployments, refer to Manage Deployments feature.

10. In the Group List, click + to assign groups to the policy.

Note: A group is disabled if another policy of the same type is already assigned to this group.



Edit Content Policy

Test

Assign to Groups - Test

Assign groups to the policy. A group is disabled if it is assigned to another policy.

All groups that have Correaltion Server service require deployments.
To know more about how to create deployments click here.

Group List

GROUP NAME	POLICY	SERVICES	ACTION
LD dec gr 3	pol	loghybrid1 - Log Decoder	⊕
dec gr	pol	packethybrid - Decoder	⊕
dec gr2	pol	endpointloghybrid1 - Log Decoder	⊕
dec gr4	pol	decoder - Decoder	⊕

No unassigned groups available. Click Create Group to save this policy & redirect you to create a new group.

No groups found. The groups are already assigned to policies.

11. If there are no unassigned groups available, click + Create Group to save the policy and redirect you to **Create New Group** screen. For more information on creating a new group, see Create a Group feature.

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

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

13. Click **Cancel** to cancel the publish content dialog.

14. Click **Save and Close** to save the settings.

IMPORTANT:
- From 12.3 version onwards, contents of services are not wiped out while publishing the first policy.
- The endpoint risk scoring requires certain application rules. Refer Endpoint Risk Scoring Rules to view the list of these application rules.

Clone a Policy

When you clone a policy, all the content from the old policy is copied to the new policy. The cloned policy can be assigned to a new group. You can clone only one policy at a time.

To clone a Policy

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Select a policy to clone and in the More actions drop-down list in the tool bar, click **Clone**.

   The policy is cloned successfully.

Delete a Policy

Deleting a policy removes all content from the associated group.

To delete a Policy

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Select one or more policies and in the More actions drop-down list in the tool bar, click **Delete**.

   The **Delete Policies** dialog is displayed.
5. To delete the deployed content from the group’s services upon deleting the policy, select the option **Delete deployed content from the group's services on policy removal**. For ESA service, the content will be deleted upon deleting the policy.
6. Click **Delete** to permanently delete the selected policy.

   Deletion will take immediate effect and the policy will no longer be available in any group.

Note:
- While deleting a policy that has Log Device content, you can delete the Custom Parser and disable the Base Log Device Parser from the service.
- The services associated with this policy still require a restart if the restart is pending.
- You can also delete a policy from **Policy Details** screen. For more information on deleting a policy from **Policy Details** screen, refer View a Policy feature.
- The policy status changes to **Failed** if policy deletion fails for any particular reason.

Edit a Policy

You can edit the content and settings of the policies. Once the policy is edited, the changes in the policy are reflected upon saving the policy. The changes are applied to the service once published. After saving and before publishing, the publication status of the changed policy is set to **Unpublished** if any settings are changed.

To edit a Policy

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Select a policy to edit and click **Edit**.
5. Make the required changes in policy.
6. Do any one of the following:
    - Click **Save and Publish** to save and publish the policy. The policy will be listed under the Unpublished category.

      Note:
      - While removing a service from the group, you can opt to either delete the content of the service and remove the service or just remove the service from the group. While removing a service that has Log Device content, you can delete the Custom Parser and disable the Base Log Device Parser from the service.
      - While removing the group from the policy, the ESA content will be deleted by default.

    - Click **Save and Close** to save the settings and return to the Policies view.

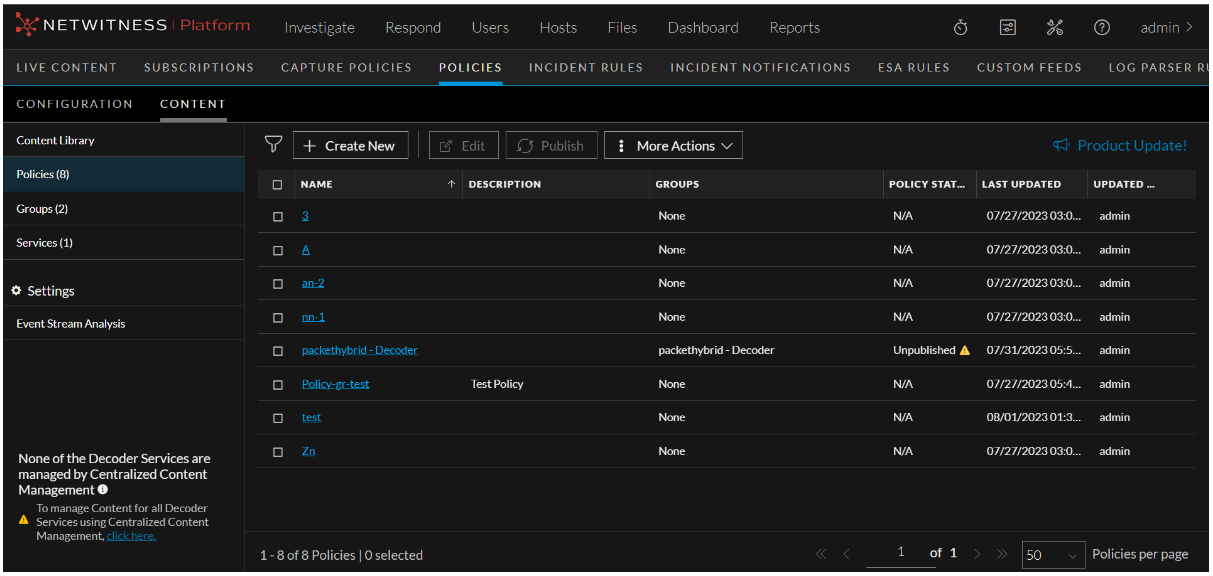
Note: You can also edit a policy from **Policy Details** screen. For more information on editing a policy from **Policy Details** screen, see View a Policy feature.

View a Policy

This topic describes the steps to view the properties of a Policy.

To view properties of the selected Policy

1. Go to ☰ **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed. By default, 50 policies are displayed per page. To go to the next page, click ›. To go to the last page, click ».



□	NAME	DESCRIPTION	GROUPS	POLICY STAT...	LAST UPDATED	UPDATED ...
□	3		None	N/A	07/27/2023 03:0...	admin
□	A		None	N/A	07/27/2023 03:0...	admin
□	an-2		None	N/A	07/27/2023 03:0...	admin
□	nn-1		None	N/A	07/27/2023 03:0...	admin
□	packethybrid - Decoder		packethybrid - Decoder	Unpublished ⚠	07/31/2023 05:5...	admin
□	Policy-gr-test	Test Policy	None	N/A	07/27/2023 05:4...	admin
□	test		None	N/A	08/01/2023 01:3...	admin
□	Zn		None	N/A	07/27/2023 03:0...	admin

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

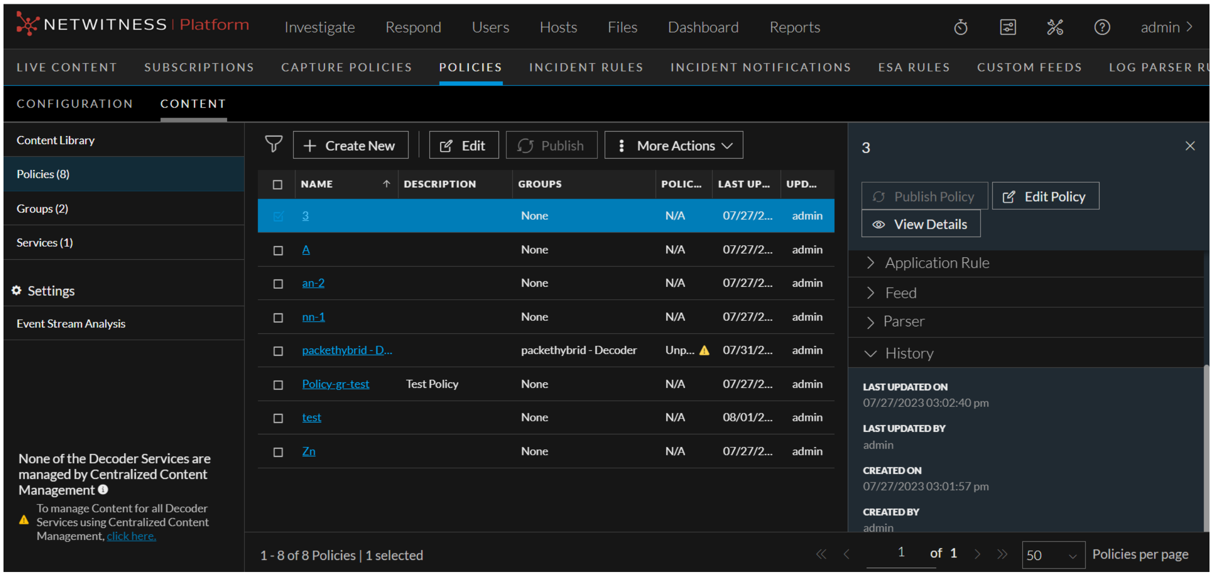
1 - 8 of 8 Policies | 0 selected

1 of 1 50 Policies per page

Caution:

- An icon ⚠ is displayed in the Policy View indicating policy status unpublished, if any services are part of the selected policy and do not have any deployment then some of the associated correlation services require ESA deployments.
- An icon ❗ is displayed in the Policy View, indicating that the policy status failed for multiple reasons. Please see the policy overview section in the UI to find the failure reason and the workaround.

4. From the policy listing page, you can perform the following actions:
   - Select a policy and click **Edit** to edit the policy. For more information on editing a policy, seeEdit a Policy feature.
   - Select the policy and click **Publish** to publish the policy if the policy is unpublished.
   - Select the policy and click **More Actions** > **Assign to Groups** to assign policy to available group.
   - Select the policy and click **More Actions** > **Clone** to clone the policy. For more information on cloning a policy, seeEdit a PolicyClone a Policy feature.
   - Select the policy and click **More Actions** > **Delete** to delete the policy. For more information on deleting a policy, see Delete a Policy feature.
   - Select the policy and click **More Actions** > **Force Publish** to force publish the policy. This action allows you republish all the content irrespective of the policy status.
5. Click a row to view details about the selected policy on the side panel.



□	NAME	DESCRIPTION	GROUPS	POLIC...	LAST UP...	UPD...
□	3		None	N/A	07/27/2...	admin
□	A		None	N/A	07/27/2...	admin
□	an-2		None	N/A	07/27/2...	admin
□	nn-1		None	N/A	07/27/2...	admin
□	packethybrid - D...		packethybrid - Decoder	Unp... ⚠	07/31/2...	admin
□	Policy-gr-test	Test Policy	None	N/A	07/27/2...	admin
□	test		None	N/A	08/01/2...	admin
□	Zn		None	N/A	07/27/2...	admin

1 - 8 of 8 Policies | 1 selected

1 of 1

LAST UPDATED ON
07/27/2023 03:02:40 pm

LAST UPDATED BY
admin

CREATED ON
07/27/2023 03:01:57 pm

CREATED BY
admin

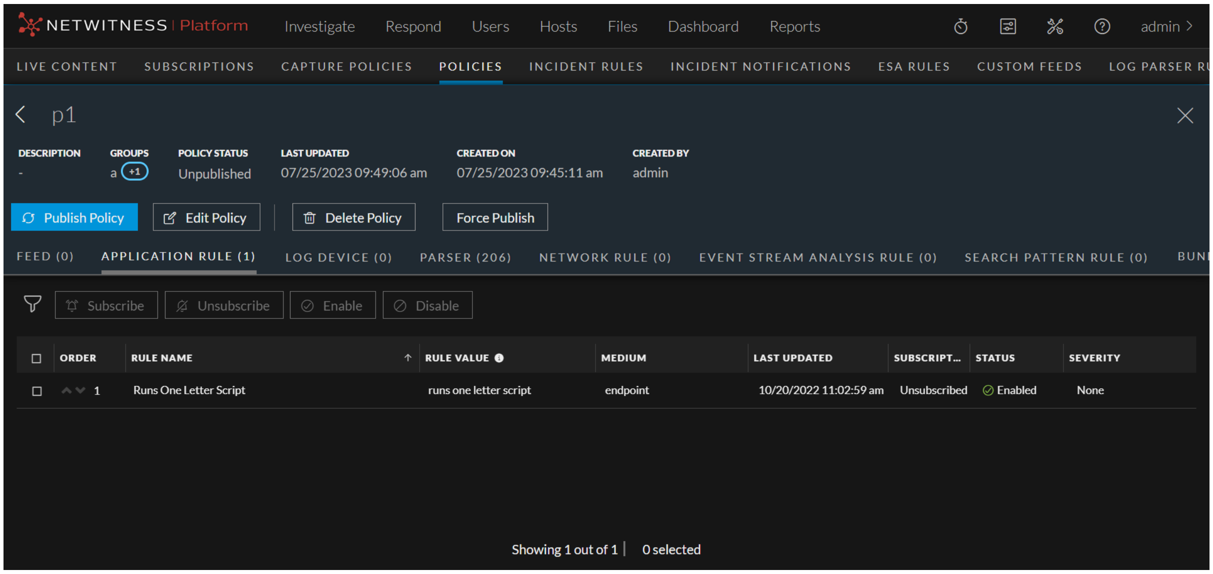
None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

6. To change the order of application rule assigned to the policy, do the following:
   1. To move the application rule or network down the order, click ⌄ in the **Order** column.
   2. To move the application rule up the order, click ⌃ in the **Order** column.
   3. You can also manually enter the order number in the **Order** column.
7. To change the order of network rule assigned to the policy, do the following:
   1. Click **Network Rules** tab.
   2. To move the network rule or network down the order, click ⌄ in the **Order** column.
   3. To move the network rule up the order, click ⌃ in the **Order** column.
   4. You can also manually enter the order number in the **Order** column.

IMPORTANT: It is recommended not to order application rules or network rules deployed on the service from Service Config page if the service is part of Centralized Content Management.

8. Click the policy to view the details on the policy in a new page.



p1

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	a +1	Unpublished	07/25/2023 09:49:06 am	07/25/2023 09:45:11 am	admin

□	ORDER	RULE NAME	RULE VALUE	MEDIUM	LAST UPDATED	SUBSCRIPT...	STATUS	SEVERITY
□	1	Runs One Letter Script	runs one letter script	endpoint	10/20/2022 11:02:59 am	Unsubscribed	✓ Enabled	None

Showing 1 out of 1 | 0 selected

9. From the policy details page, you can perform the following actions:
   - To edit the policy, click **Edit Policy**. For more information on editing a policy, see Edit a Policy feature.
   - To delete the policy, click **Delete Policy**. For more information on deleting a policy, see Delete a Policy feature.
   - To publish the policy, click **Publish Policy**. For more information on creating and publishing a policy, see Create and Publish Policies feature.
   - To force publish a policy, click **Force Publish**. This action allows you republish all the content irrespective of the policy status.
   - To filter the content, click . For more information on filtering policy content details, see Filter Policy Content Details feature.
   - To enable or disable subscription, click **Subscribe** or **Unsubscribe** respectively.

   > **Note:**
   > - Subscription is not allowed for custom content.
   > - The **Subscribe** and **Unsubscribe** button is disabled if any one of the content selected is custom.

Enable Content for a Policy

This topic describes the steps to enable the content for a Policy.

To enable content

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.

4. Click the policy name to view the policy details.
5. In the **Application Rule**, **Network Rule**, **Feed**, **Log Device**, **Search Pattern Rule** or **LUA Parser** panel, click the row to select the content to be enabled. You can either select all content or select any specific content to be enabled.
6. Click **Enable**.

If a Custom Log Device has a Base Parser as its dependency, then:

- The enable or disable status of the Custom Log Device will be same as that of the enable or disable status of Base Parser.
- You will not be able to enable or disable the Custom Parser.

Disable Content for a Policy

This topic describes the steps to disable the content for a Policy.

To disable content

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.
4. Click the policy name to view the policy details.
5. In the **Application Rule**, **Network Rule**, **Feed**, **Log Device**, **Search Pattern Rule** or **LUA Parser** panel, click the row to select the content to be disabled. You can either select all content or select any specific content to be disabled.
6. Click **Disable**.

If a Custom Log Device has a Base Parser as its dependency, then:

- The enable or disable status of the Custom Log Device will be same as that of the enable or disable status of Base Parser.
- You will not be able to enable or disable the Custom Parser.

Subscribe Content for a Policy

This topic describes the steps to subscribe content for a Policy.

To subscribe content

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.
4. Click the policy name to view the policy details.

5. In the **Application Rule**, **Network Rule**, **Feed**, **Log Device**, **LUA Parser**, **Event Stream Analysis Rule**, or **Bundles** panel, click the row to select the content to be subscribed. You can either select all content or select any specific content to be subscribed.
6. Click **Subscribe**.

Unsubscribe Content for a Policy

This topic describes the steps to unsubscribe the content for a Policy.

To unsubscribe content

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.
4. Click the policy name to view the policy details.
5. In the **Application Rule**, **Network Rule**, **Feed**, **Log Device**, **LUA Parser**, **Event Stream Analysis Rule,** or **Bundles** panel, click the row to select the content to be unsubscribed. You can either select all content or select any specific content to be unsubscribed.
6. Click **Unsubscribe**.

Filter Policies

The Filters Panel allows you to filter the list of displayed policies, based on the policy status and service type:

- **Decoder**
- **Log Decoder**
- **Concentrator**

Additionally, you can filter based on publication status or service status:

- **Published**: Policies that are published to use.
- **Unpublished**: Policies that are saved but not published.
- **Failed**: Policies that are failed to publish.
- **N/A**: Policies for which publication status is not applicable.

The **Filters** panel can be hidden or displayed:

- To display if hidden, click the icon in the toolbar.
- To hide, click the × icon at the top-right of the panel.

Filter Policy Content Details

The Filters panel allows you to filter the list of displayed content in the policy details view based on the name, medium, source type, enabled/disabled status, subscription status, severity, resource created date, and last updated date.

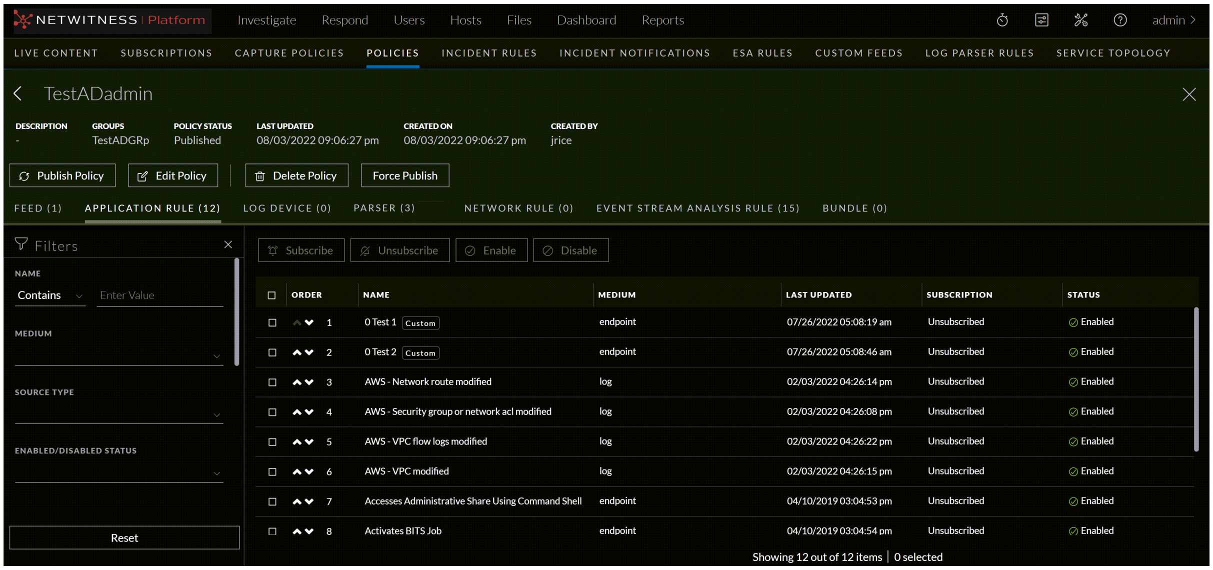
This applies to the following content types:

- Feed
- Application Rule
- Log Device
- Lua Parser
- Network Rule
- Event Steam Analysis Rule
- Search Pattern Rule
- Bundle

To filter policy content details

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Do one of the following:
   - Click a policy name.
   - Click a row to view details about the selected policy and click **View Details**.

   The policy details view is displayed.



TestADadmin

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	TestADGRp	Published	08/03/2022 09:06:27 pm	08/03/2022 09:06:27 pm	jrice

NAME: Contains | Enter Value

MEDIUM

SOURCE TYPE

ENABLED/DISABLED STATUS

☐	ORDER	NAME	MEDIUM	LAST UPDATED	SUBSCRIPTION	STATUS
☐	1	0 Test 1 Custom	endpoint	07/26/2022 05:08:19 am	Unsubscribed	✓ Enabled
☐	2	0 Test 2 Custom	endpoint	07/26/2022 05:08:46 am	Unsubscribed	✓ Enabled
☐	3	AWS - Network route modified	log	02/03/2022 04:26:14 pm	Unsubscribed	✓ Enabled
☐	4	AWS - Security group or network acl modified	log	02/03/2022 04:26:08 pm	Unsubscribed	✓ Enabled
☐	5	AWS - VPC flow logs modified	log	02/03/2022 04:26:22 pm	Unsubscribed	✓ Enabled
☐	6	AWS - VPC modified	log	02/03/2022 04:26:15 pm	Unsubscribed	✓ Enabled
☐	7	Accesses Administrative Share Using Command Shell	endpoint	04/10/2019 03:04:53 pm	Unsubscribed	✓ Enabled
☐	8	Activates BITS Job	endpoint	04/10/2019 03:04:54 pm	Unsubscribed	✓ Enabled

Showing 12 out of 12 items | 0 selected

5. By default, the filters panel is hidden, click the (Filters) icon in the toolbar to expand the filters panel.
6. To search by name:
   - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the content rules. Type one character and a list of content rules that contain that character is displayed, as you continue to type the list is filtered to match.
   - Set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular content type will be displayed.
7. To filter by medium, select one or more mediums from the **Medium** drop-down list. The options are listed below:
   - **endpoint**
   - **log**
   - **log and packet**
   - **packet**
8. To filter by source type, select one or more sources from the **Source Type** drop-down list. The options are listed below:
   - **Custom**
   - **Live**
9. To filter by enabled/disabled status, select one or more statuses from the **Enabled/Disabled Status** drop-down list. The options are listed below:
   - **Enabled**
   - **Disabled**

   Note: Enabled/Disabled Status filtering is not applicable to Event Stream Analysis Rule content.

10. To filter by subscription status, select one or more statuses from the **Subscription** drop-down list. The options are listed below:
    - **Subscribed**
    - **Unsubscribed**
11. To filter by severity of the content, under the **Severity** field, select the drop-down values as either **Low**, **Medium**, **High** or **Critical**.

    Note: This field is applicable only for the content type 'Application Rule'.
12. To filter by a resource created date range, under the **Resource Created Date**, select the start date and end date from the date fields.

    For example, to filter contents that were created between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.
13. To filter by date range, under the **Last Update date**, select the start date and end date from the date fields.

    For example, to filter contents that were updated between July 1 and July 30, you select July 1 as the start date and July 30 as the end date. You must enter dates in **mm/dd/yyyy** format or you click and pick dates from a calendar.
14. To hide, click the ✕ icon at the top-right of the panel.

    The contents are displayed in the right panel according to the filter you selected. Click **Reset** to clear the existing filter results.

Merge Policy with ESA Content

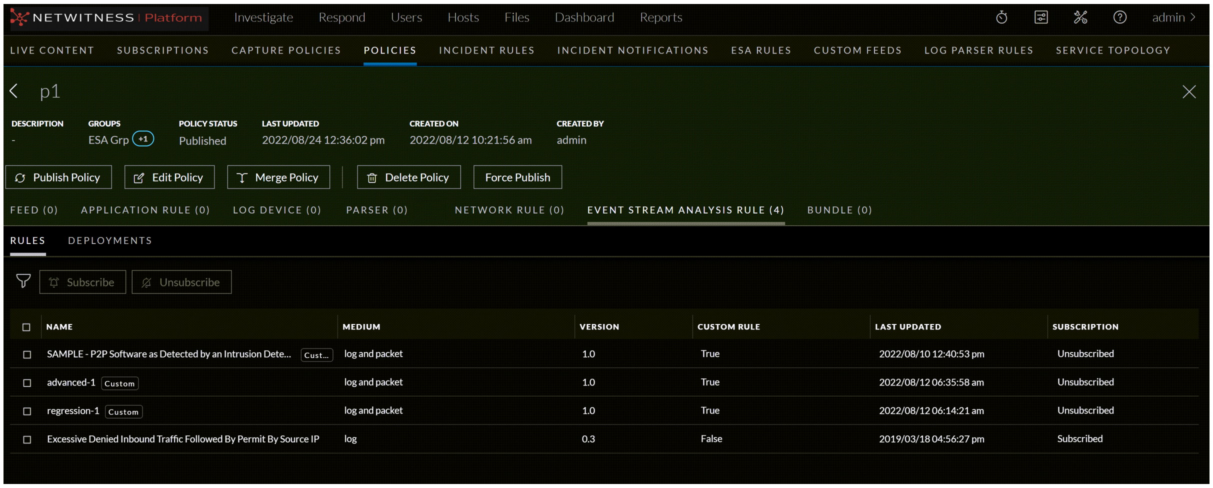
From the 12.1 version, the ESA content is managed through the **(CONFIGURE)** > **Policies** page. After you upgrade to the 12.1 version, all the existing ESA deployments will be migrated to the policies and groups view. The **Merge Policy** button will be available only for the policy having ESA content and can only be merged with a policy with no ESA content.

Note: On merging a policy with another policy, the original policy gets deleted, and the other policy gets updated with the original policy content.

To merge Policy with an ESA Content

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. Select a policy having ESA content to merge with another policy.

   The selected policy with ESA content view is displayed.



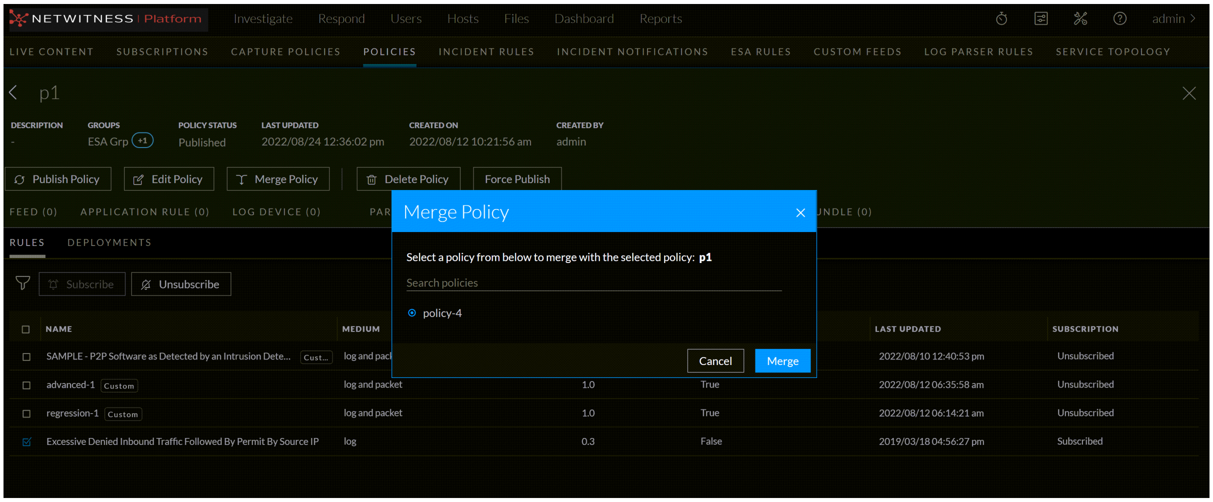
p1

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	ESA Grp +1	Published	2022/08/24 12:36:02 pm	2022/08/12 10:21:56 am	admin

□	NAME	MEDIUM	VERSION	CUSTOM RULE	LAST UPDATED	SUBSCRIPTION
□	SAMPLE - P2P Software as Detected by an Intrusion Dete... Cust...	log and packet	1.0	True	2022/08/10 12:40:53 pm	Unsubscribed
□	advanced-1 Custom	log and packet	1.0	True	2022/08/12 06:35:58 am	Unsubscribed
□	regression-1 Custom	log and packet	1.0	True	2022/08/12 06:14:21 am	Unsubscribed
□	Excessive Denied Inbound Traffic Followed By Permit By Source IP	log	0.3	False	2019/03/18 04:56:27 pm	Subscribed

4. Click **Merge Policy**.

   The Merge Policy dialog is displayed.



p1

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	ESA Grp +1	Published	2022/08/24 12:36:02 pm	2022/08/12 10:21:56 am	admin

Select a policy from below to merge with the selected policy: **p1**

Search policies

● policy-4

□	NAME	MEDIUM			LAST UPDATED	SUBSCRIPTION
□	SAMPLE - P2P Software as Detected by an Intrusion Dete... Cust...	log and pack			2022/08/10 12:40:53 pm	Unsubscribed
□	advanced-1 Custom	log and packet	1.0	True	2022/08/12 06:35:58 am	Unsubscribed
□	regression-1 Custom	log and packet	1.0	True	2022/08/12 06:14:21 am	Unsubscribed
☑	Excessive Denied Inbound Traffic Followed By Permit By Source IP	log	0.3	False	2019/03/18 04:56:27 pm	Subscribed

5. Select a policy from the list or search for the name and Click **Merge**.

   A confirmation pop-up is displayed.

6. Click **Confirm**.

Manage Services

A service performs a unique function, such as collecting logs or archiving data. Each service runs on a dedicated port and is modeled as a plug-in to enable or disable, according to the function of the host.

This sections contains:

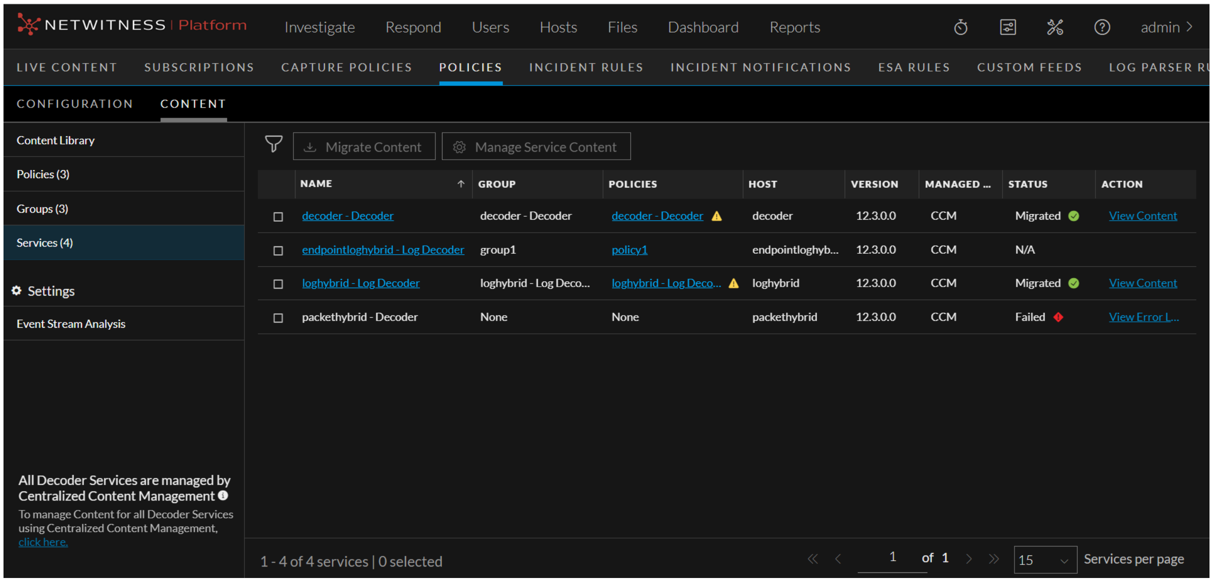
- Migrate Content from Service
- View a Service
- Enable or Disable CCM for Individual Decoder Services

View a Service

This topic describes the steps to view the details of a service.

To view details of the selected Service

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Services**. The list of services are displayed. By default, 15 services are displayed per page. To go to the next page, click ›. To go to the last page, click ».



	NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
□	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ♦	View Error L...

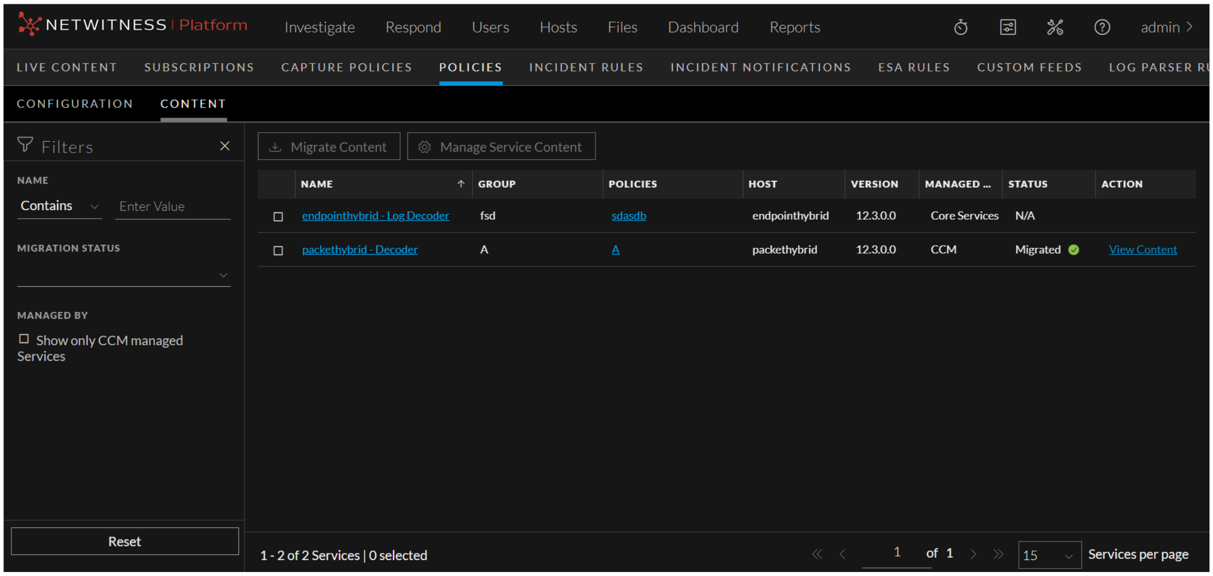
All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 0 selected

1 of 1 15 Services per page

4. To filter the services, click ▽. The **Filters** panel is displayed.



	NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	endpointhybrid - Log Decoder	fsd	sdasdb	endpointhybrid	12.3.0.0	Core Services	N/A	
□	packethybrid - Decoder	A	A	packethybrid	12.3.0.0	CCM	Migrated ✓	View Content

1 - 2 of 2 Services | 0 selected

1 of 1

15

5. On the **Filters** panel, do the following:

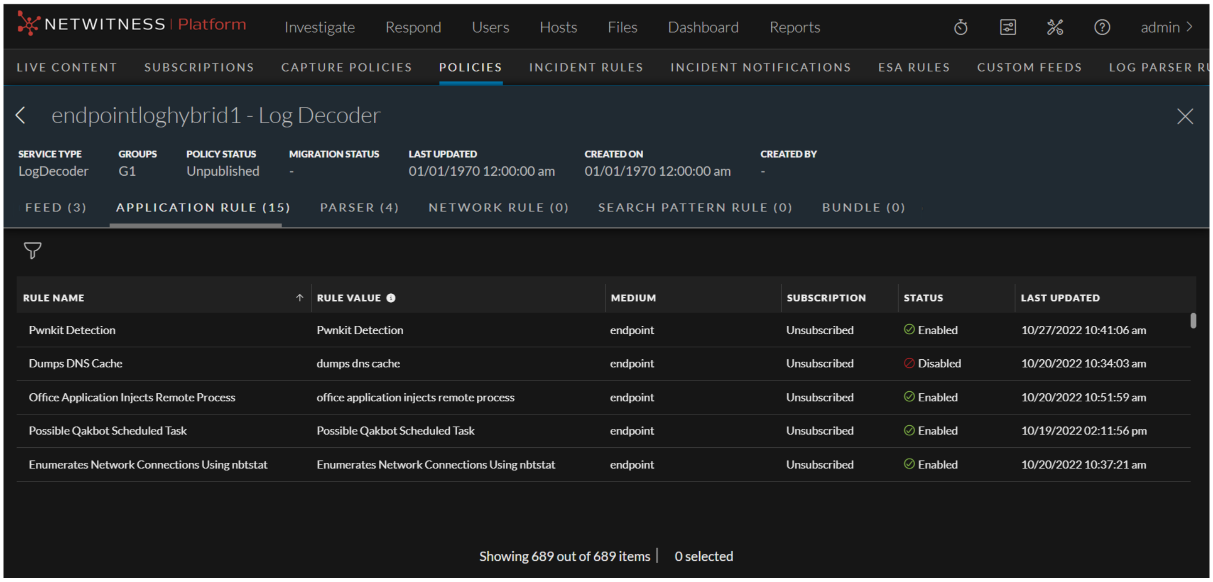
   i. Select the **Name** drop-down value as either **Equals** or **Contains**. To search the service name using the **Contains** operator, set the filter option to **Contains** operator from the drop-down list and start typing the name of the service. Type one character and a list of service that contain that character is displayed, as you continue to type, the list is filtered to match. To search the service name using the **Equals** operator, set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular service name will be displayed.

   ii. Select the **Migration Status** drop-down value.

   iii. Select **Show only CCM Managed Services** check-box under the **Managed By** field to display only the CCM managed services.

   iv. To reset the fields, click **Reset**.

6. Click the service to view the details of the service. The different details of the service are displayed. These details include the contents which will be deployed to the services from CCM policies.



endpointloghybrid1 - Log Decoder

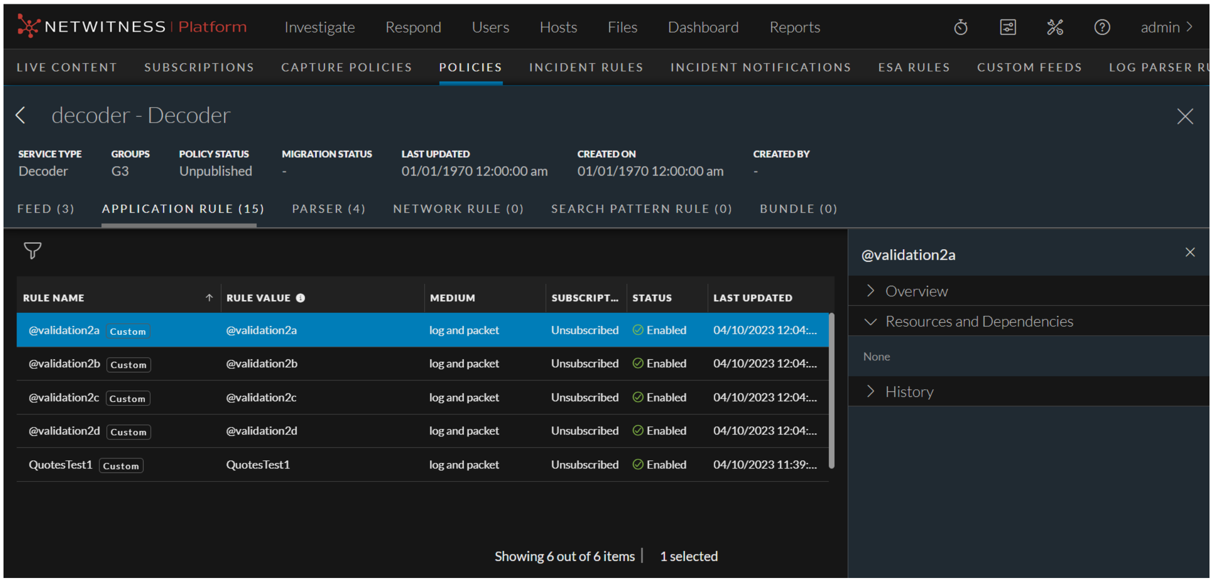
SERVICE TYPE	GROUPS	POLICY STATUS	MIGRATION STATUS	LAST UPDATED	CREATED ON	CREATED BY
LogDecoder	G1	Unpublished	-	01/01/1970 12:00:00 am	01/01/1970 12:00:00 am	-

RULE NAME	RULE VALUE	MEDIUM	SUBSCRIPTION	STATUS	LAST UPDATED
Pwnkit Detection	Pwnkit Detection	endpoint	Unsubscribed	Enabled	10/27/2022 10:41:06 am
Dumps DNS Cache	dumps dns cache	endpoint	Unsubscribed	Disabled	10/20/2022 10:34:03 am
Office Application Injects Remote Process	office application injects remote process	endpoint	Unsubscribed	Enabled	10/20/2022 10:51:59 am
Possible Qakbot Scheduled Task	Possible Qakbot Scheduled Task	endpoint	Unsubscribed	Enabled	10/19/2022 02:11:56 pm
Enumerates Network Connections Using nbtstat	Enumerates Network Connections Using nbtstat	endpoint	Unsubscribed	Enabled	10/20/2022 10:37:21 am

Showing 689 out of 689 items | 0 selected

7. To filter the content based on various parameters, click ▽.

8. Click the content to view the details of the content on the right side panel. The complete content details such as **Overview**, **Resources and Dependencies**, and **History** are displayed.



decoder - Decoder

SERVICE TYPE	GROUPS	POLICY STATUS	MIGRATION STATUS	LAST UPDATED	CREATED ON	CREATED BY
Decoder	G3	Unpublished	-	01/01/1970 12:00:00 am	01/01/1970 12:00:00 am	-

RULE NAME	RULE VALUE	MEDIUM	SUBSCRIPT...	STATUS	LAST UPDATED
@validation2a Custom	@validation2a	log and packet	Unsubscribed	Enabled	04/10/2023 12:04:...
@validation2b Custom	@validation2b	log and packet	Unsubscribed	Enabled	04/10/2023 12:04:...
@validation2c Custom	@validation2c	log and packet	Unsubscribed	Enabled	04/10/2023 12:04:...
@validation2d Custom	@validation2d	log and packet	Unsubscribed	Enabled	04/10/2023 12:04:...
QuotesTest1 Custom	QuotesTest1	log and packet	Unsubscribed	Enabled	04/10/2023 11:39:...

Showing 6 out of 6 items | 1 selected

@validation2a

Overview

Resources and Dependencies

None

History

9. To view the details of the policy for the migrated service, click the policy name present under the **Policies** column in the **Service List** page.

   For more details on the policy details, see View a Policy feature.

10. To view the details of the migrated content for the service, click the **View Content** hyperlink present under the **Action** column in the **Service List** page.

11. To view the details of the logs for failed migration, click the **View Error Log** hyperlink present under the **Action** column in the **Service List** page.

For more details on the migrating content from service, viewing migrated content and viewing error logs, see Migrate Content from Service feature.

Migrate Content from Service

This option allows you to migrate the contents of 12.3 and above version services.

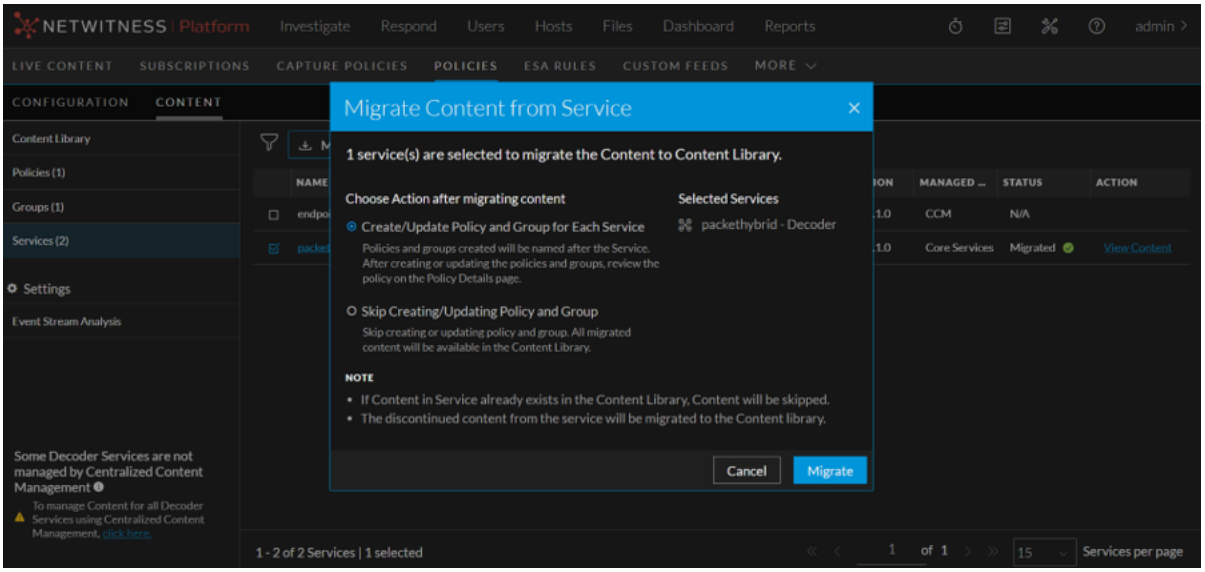
To migrate Content from Service

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Services**. The list of services are displayed.
4. Select the services from which you want to migrate the content.

   > **Note:** By default, you can select up to 5 services for migration. This also includes the services which are under migration. However, you can modify this number from **Admin -> Source Server -> Explore -> Central/Content -> Migration**.

5. Click **Migrate Content**.

   The **Migrate Content from Service** pop-up window is displayed.



Migrate Content from Service

1 service(s) are selected to migrate the Content to Content Library.

Choose Action after migrating content

● Create/Update Policy and Group for Each Service

Policies and groups created will be named after the Service. After creating or updating the policies and groups, review the policy on the Policy Details page.

○ Skip Creating/Updating Policy and Group

Skip creating or updating policy and group. All migrated content will be available in the Content Library.

Selected Services

packethybrid - Decoder

NOTE

- If Content in Service already exists in the Content Library, Content will be skipped.
- The discontinued content from the service will be migrated to the Content library.

Cancel Migrate

Some Decoder Services are not managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 2 of 2 Services | 1 selected

1 of 1 15 Services per page

6. On the **Migrate Content from Service** pop-up window, choose action and click **Migrate**.
   - If you select **Create/Update Policy and Group for Each Service**, policy and group will be created or updated for each service selected for migration. Once the migration process is complete, the policy and group will be listed under the respective listing pages. The policy and group which is created or updated for the service will be in 'Unpublished' state and it can be published only after it is reviewed. In the **Policy Listing** page, the **Publish** button for such a policy will be disabled until the policy is reviewed. The policy can be published only after reviewing it either from **Policy Details** page or **Edit Policy** Page. When the policy or group gets updated with the

new content, the order of the new content will be given priority.

- If you select **Skip Creating/Updating a Policy and Group**, only the content will be migrated. All the migrated content will be available in Content Library.

> **Note:**
> - If the service is assigned to a group which is not attached to any policy, then the **Create/Update Policy and Group for Each Service** is disabled.
> - When migrating content from two Decoders that have two different types of Custom or Live Base Parser associated with same Custom or Live Base Parser, both the Custom Parsers are added to Content Library. The association inside the Policy will be with the most recently migrated Custom Parser.
> - Within a migrated Policy, a Custom Parser will have only one Custom or Live Base Parser associated with it.
> - Migrated content version will be in the Policy, if as part of migration, the Policy is auto created. If you remove this content, you cannot add the old version of the content back.

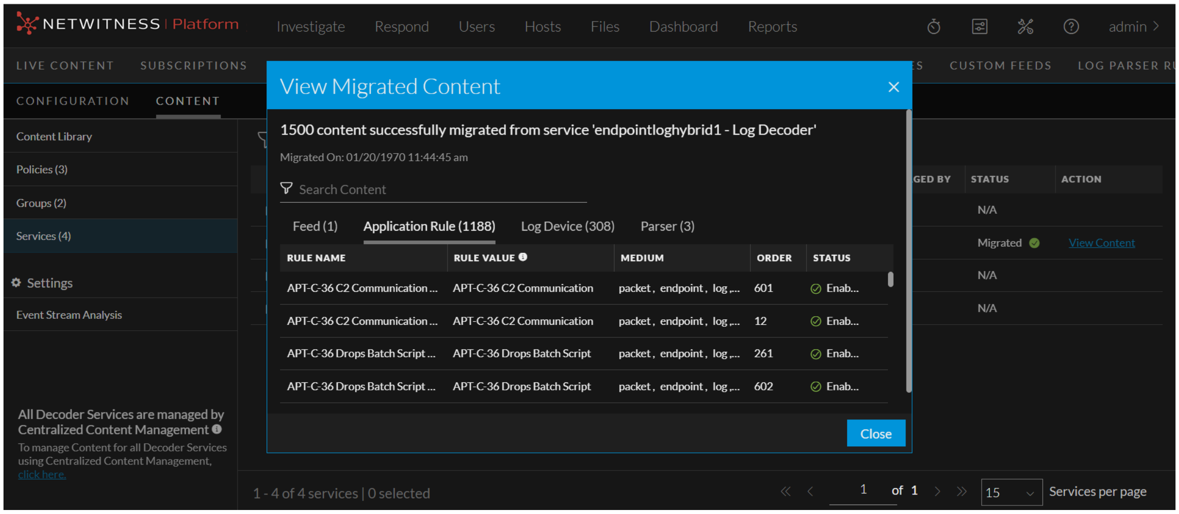
> **Note:** If a service migration fails to update a policy:
> - You can edit the existing policy and add only the required content.
> - Remove the service that is part of a group and remigrate the content. This will only create a policy if the content number is less than 8000.

7. The migration initiation message is displayed on the screen. The **Status** column displays the following values based on the status of migration:
   - Queued
   - Initializing
   - Analyzing Content
   - Migrating Content
   - Migrated
   - Failed

> **Note:**
> - The service can also be remigrated if it is already migrated and assigned to groups and policies.
> - During parallel migration, if the selected services are updating common policies or using policies that are already being updated, you will receive a warning message on the screen. In such a scenario, it is recommended to update the policies through migration one service at a time to ensure that the last migrated service influences the policy in terms of order and version.

8. To view the migrated content details, do the following:
   - Click the **View Content** hyperlink present under the **Action** column. The hyperlink is available only after the migration process is complete.

     The **View Migrated Content** pop-up window is displayed with the different tabs such as **Feed**, **Application Rule**, **Network Rule**, **Log Device** and **LUA Parser**.



View Migrated Content

1500 content successfully migrated from service 'endpointloghybrid1 - Log Decoder'

Migrated On: 01/20/1970 11:44:45 am

Search Content

Feed (1) | Application Rule (1188) | Log Device (308) | Parser (3)

RULE NAME	RULE VALUE	MEDIUM	ORDER	STATUS
APT-C-36 C2 Communication ...	APT-C-36 C2 Communication	packet , endpoint , log ,...	601	✓ Enab...
APT-C-36 C2 Communication ...	APT-C-36 C2 Communication	packet , endpoint , log ,...	12	✓ Enab...
APT-C-36 Drops Batch Script ...	APT-C-36 Drops Batch Script	packet , endpoint , log ,...	261	✓ Enab...
APT-C-36 Drops Batch Script ...	APT-C-36 Drops Batch Script	packet , endpoint , log ,...	602	✓ Enab...

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 0 selected

1 of 1

Note:
- **Network Rules** tab is not applicable for Log Decoders.
- **Log Device** tab is not applicable for Decoders.

IMPORTANT: During the process of migration, if a Decoder that is being migrated contains multiple application rules and/or network rules with the exact same rule name and rule condition, only one of those rules will be retained in the service. The remaining rules will be considered duplicates and removed. Therefore, post migration, none of the migrated services will have multiple rules with the same rule name and the same rule value.

- Click ⛛ to search the migrated content based on various parameters.

Note:
- For Application Rule and Network Rule, the search is based on **Rule Name** and **Rule Value**.
- For Feeds, Log Device and LUA Parser, the search is based on the **Name**.

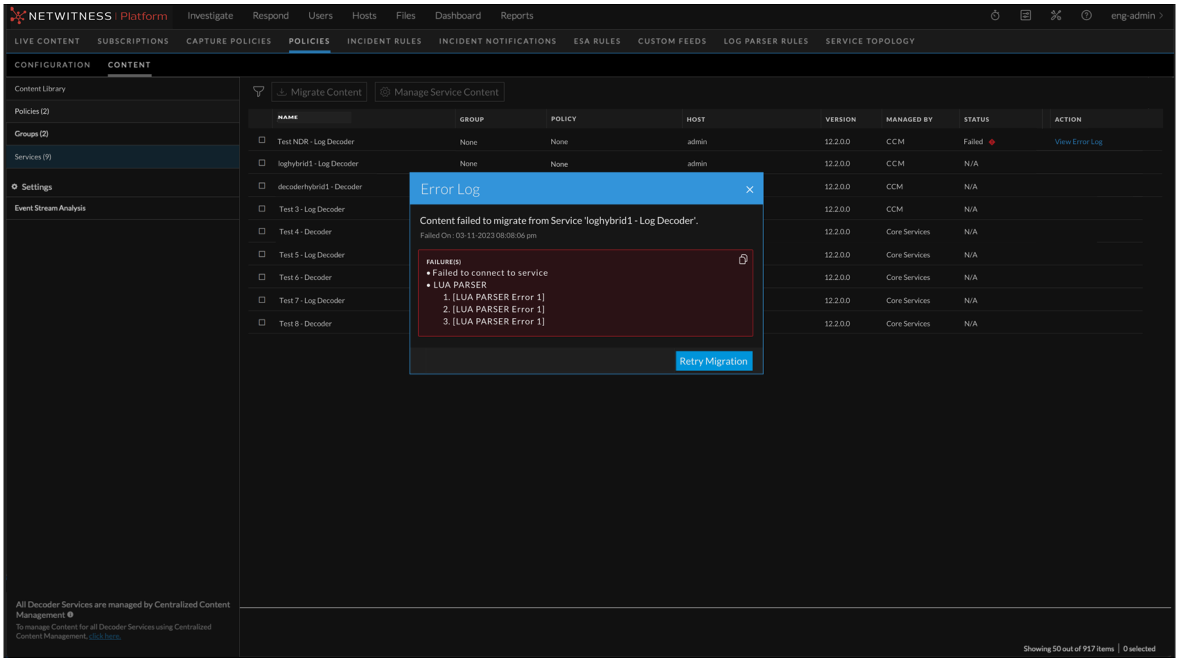
- Click each tab to view the content details. The **Application Rule** and **Network Rule** tabs will have details such as **Rule Name**, **Rule Value**, **Medium**, **Order** and **Status**. The **Log Device**, **Feeds** and **LUA Parser** tabs will have details such as **Name**, **Medium** and **Status**.

9. To view the error log details in case of failed migration, do the following:

   - Click the **View Error Log** hyperlink present under the **Action** column. The hyperlink is available only if the migration process has failed due to some reason.

     The **Error Log** pop-up window is displayed with the details of error.

     The following screen is displayed if no content is migrated to Content Library.



	NAME	GROUP	POLICY	HOST	VERSION	MANAGED BY	STATUS	ACTION
□	Test NDR - Log Decoder	None	None	admin	12.2.0.0	CCM	Failed ◆	View Error Log
□	loghybrid1 - Log Decoder	None	None	admin	12.2.0.0	CCM	N/A	
□	decoderhybrid1 - Decoder				12.2.0.0	CCM	N/A	
□	Test 3 - Log Decoder				12.2.0.0	CCM	N/A	
□	Test 4 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 5 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 6 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 7 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 8 - Decoder				12.2.0.0	Core Services	N/A	

Error Log ×

Content failed to migrate from Service 'loghybrid1 - Log Decoder'.

Failed On : 03-11-2023 08:08:06 pm

```
FAILURE(S)
• Failed to connect to service
• LUA PARSER
    1. [LUA PARSER Error 1]
    2. [LUA PARSER Error 1]
    3. [LUA PARSER Error 1]
```

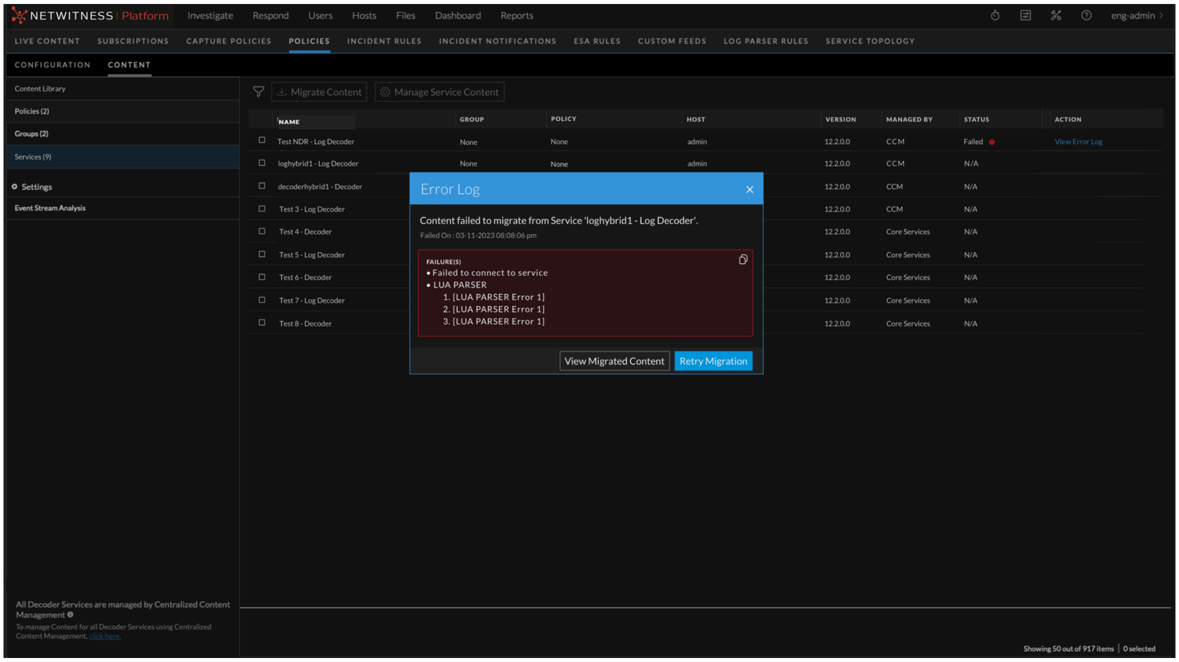
All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 50 out of 917 items | 0 selected

Note: You should manually migrate the content in case of failed automated migration.

The following screen is displayed if some content is migrated is Content Library.



	NAME	GROUP	POLICY	HOST	VERSION	MANAGED BY	STATUS	ACTION
□	Test NDR - Log Decoder	None	None	admin	12.2.0.0	CCM	Failed ◆	View Error Log
□	loghybrid1 - Log Decoder	None	None	admin	12.2.0.0	CCM	N/A	
□	decoderhybrid1 - Decoder				12.2.0.0	CCM	N/A	
□	Test 3 - Log Decoder				12.2.0.0	CCM	N/A	
□	Test 4 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 5 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 6 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 7 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 8 - Decoder				12.2.0.0	Core Services	N/A	

Error Log ×

Content failed to migrate from Service 'loghybrid1 - Log Decoder'.

Failed On : 03-11-2023 08:08:06 pm

```
FAILURE(S)
• Failed to connect to service
• LUA PARSER
    1. [LUA PARSER Error 1]
    2. [LUA PARSER Error 1]
    3. [LUA PARSER Error 1]
```

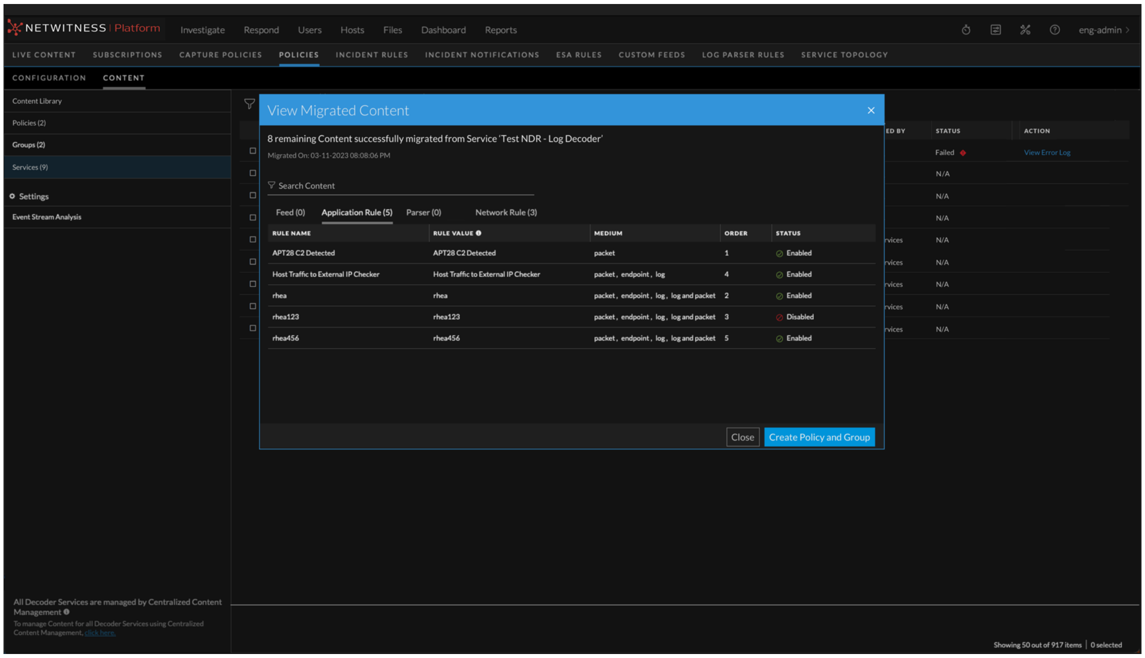
All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 50 out of 917 items | 0 selected

- To copy the error logs, click ⧉.
- To retry migration, click **Retry Migration**.
- In case of partial migration, to view the content that have been migrated successfully, do the following:

- Click **View Migrated Content**. The **View Migrated Content** pop-up window is displayed with the details of migrated content.



View Migrated Content

8 remaining Content successfully migrated from Service 'Test NDR - Log Decoder'

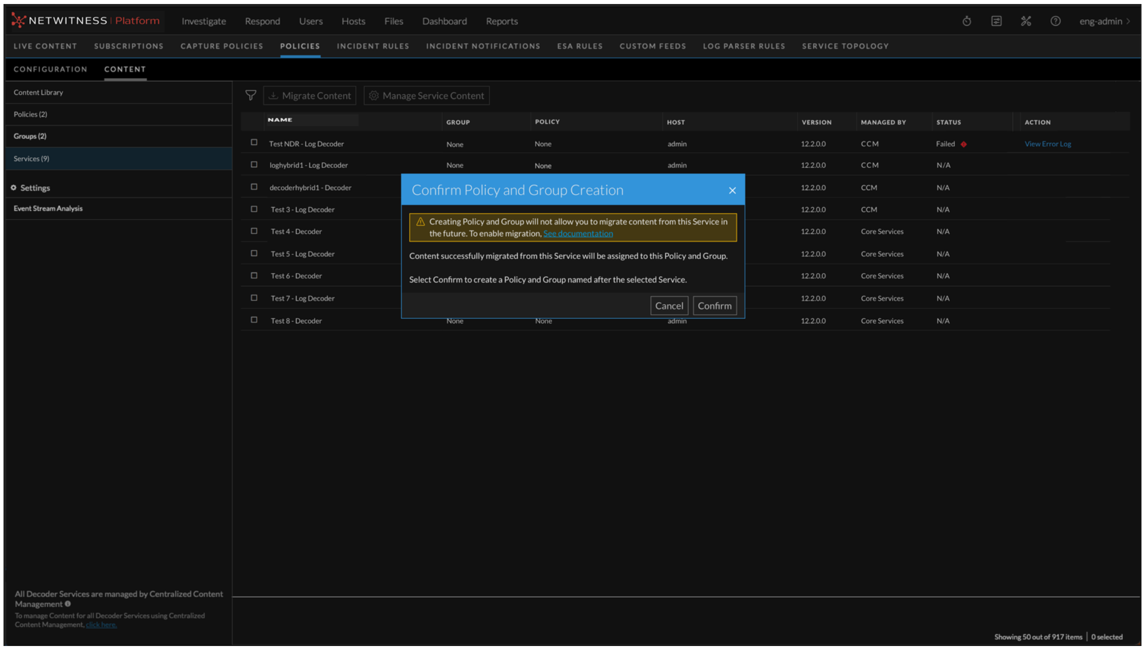
Migrated On: 03-11-2023 08:08:06 PM

Feed (0) | Application Rule (5) | Parser (0) | Network Rule (3)

RULE NAME	RULE VALUE	MEDIUM	ORDER	STATUS
APT28 C2 Detected	APT28 C2 Detected	packet	1	Enabled
Host Traffic to External IP Checker	Host Traffic to External IP Checker	packet, endpoint, log	4	Enabled
rhea	rhea	packet, endpoint, log, log and packet	2	Enabled
rhea123	rhea123	packet, endpoint, log, log and packet	3	Disabled
rhea456	rhea456	packet, endpoint, log, log and packet	5	Enabled

- To create policy and group for the service which is partially migrated, click **Create Policy and Group**.

  The **Confirm Policy and Group Creation** pop-up window is displayed.



Confirm Policy and Group Creation

Creating Policy and Group will not allow you to migrate content from this Service in the future. To enable migration, See documentation

Content successfully migrated from this Service will be assigned to this Policy and Group.

Select Confirm to create a Policy and Group named after the selected Service.

Best Practice Recommendation: Before creating policy and group for partially migrated service, it is recommended to retry migration.

- To confirm creation of policy and group, click **Confirm**. The policy and group will be listed under the **Policy Listing** and **Group Listing** pages.
- To go back to the **Service List** page, click **Cancel**.
- If you do not want to create policy and group for partially migrated service, click **Close in View Migrated Content** pop-up window.

10. To cancel the migration, click **Cancel** in the **Migrate Content from Service** pop-up window.

Note: Migrated Live contents will be categorized as Custom contents, if:
- You have modified the Live content manually before migrating it.
- The migrated Live content is an older version of the content.

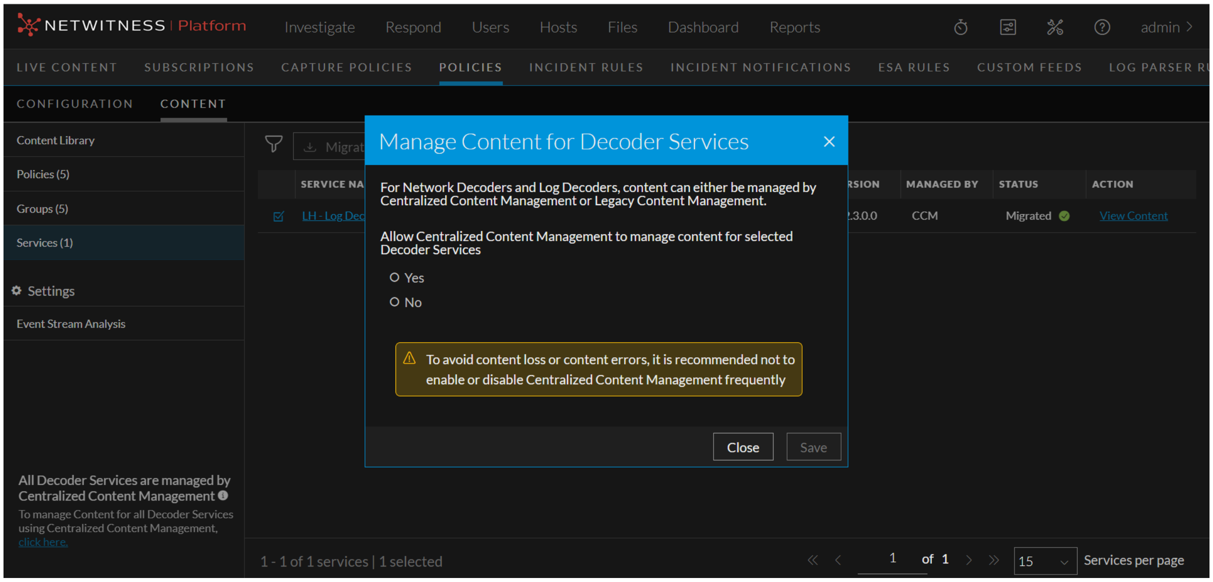
Enable or Disable CCM for Individual Decoder Services

This topic describes the steps to enable or disable CCM for individual Decoder Services.

To enable or disable CCM for individual Decoder Service

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Services**. The list of services are displayed.
4. Select the service(s) for which you want to enable or disable CCM and click **Manage Service Content**.

   The **Manage Content for Decoder Services** pop-up window is displayed.



Manage Content for Decoder Services

For Network Decoders and Log Decoders, content can either be managed by Centralized Content Management or Legacy Content Management.

Allow Centralized Content Management to manage content for selected Decoder Services

○ Yes

○ No

To avoid content loss or content errors, it is recommended not to enable or disable Centralized Content Management frequently

Close Save

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 1 of 1 services | 1 selected

1 of 1 | 15 Services per page

5. In the pop-up window, select **Yes** for **Allow Centralized Content Management to Manage Content for Selected Decoder Services** to enable CCM for the selected service. Select **No** to disable CCM for the selected service.
6. Click **Save** to save the changes.

Manage ESA Datasources

This section contains:

- View an ESA Datasource
- Add an ESA Datasource
- Edit an ESA Datasource
- Delete an ESA Datasource

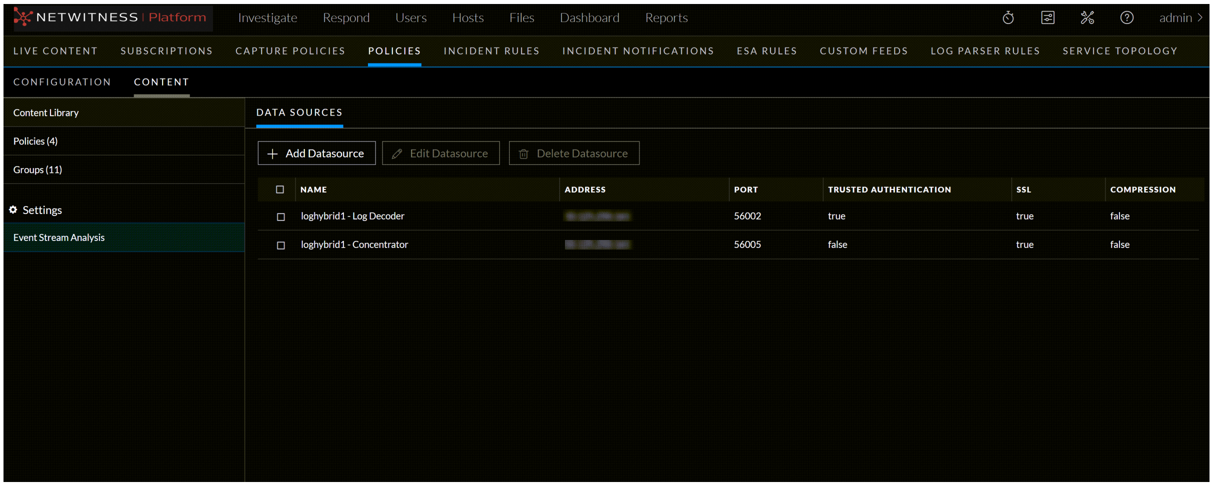
View an ESA Datasource

This topic describes the steps to view the ESA datsources available.

To view an ESA Datasource

1. Go to ☰ **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.

   The available datasources are displayed.



□	NAME	ADDRESS	PORT	TRUSTED AUTHENTICATION	SSL	COMPRESSION
□	loghybrid1 - Log Decoder	[redacted]	56002	true	true	false
□	loghybrid1 - Concentrator	[redacted]	56005	false	true	false

Add an ESA Datasource

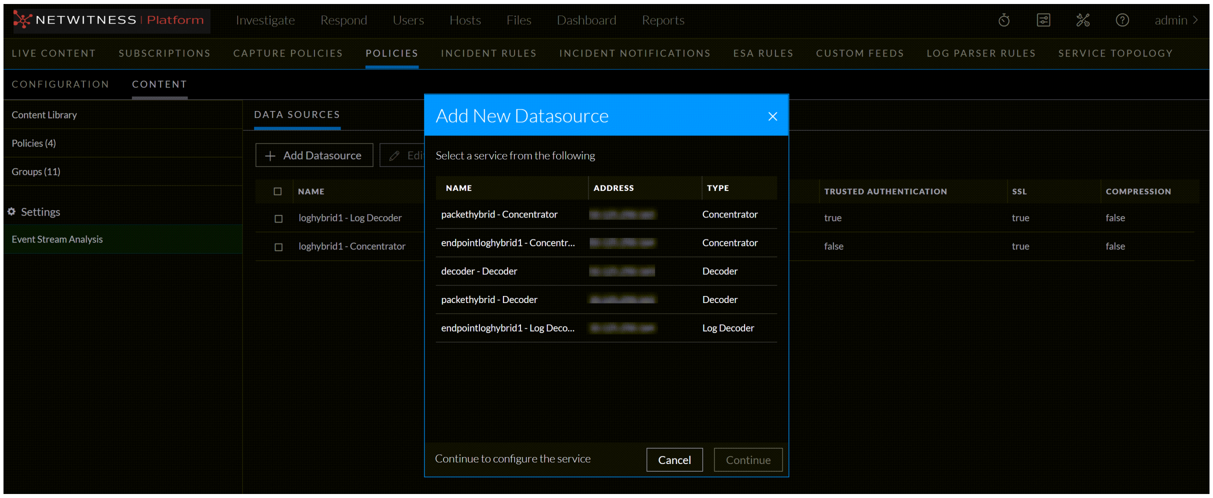
You can add one or more ESA data sources, such as Concentrators, to use for your selected ESA Service. This enables you to specify different data sources for each deployment.

To add an ESA Datasource

1. Go to ☰ **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.

3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.
4. Click + **Add Datasource**.

   The Add New Datasource dialog is displayed.



□	NAME	TRUSTED AUTHENTICATION	SSL	COMPRESSION
□	loghybrid1 - Log Decoder	true	true	false
□	loghybrid1 - Concentrator	false	true	false

Add New Datasource ×

Select a service from the following

NAME	ADDRESS	TYPE
packethybrid - Concentrator	[redacted]	Concentrator
endpointloghybrid1 - Concentr...	[redacted]	Concentrator
decoder - Decoder	[redacted]	Decoder
packethybrid - Decoder	[redacted]	Decoder
endpointloghybrid1 - Log Deco...	[redacted]	Log Decoder

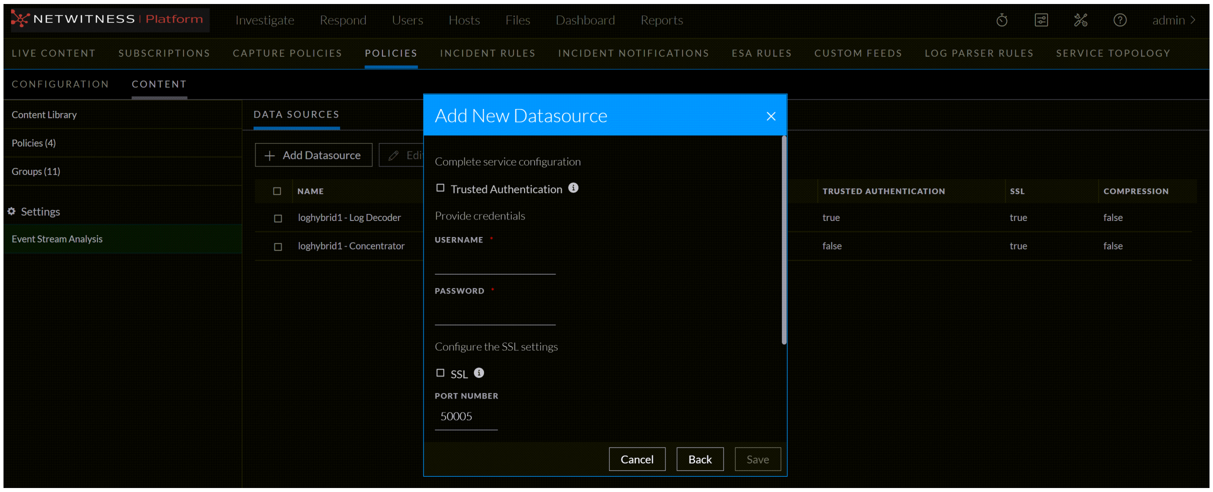
Continue to configure the service

Cancel Continue

Note: You can add a Log Decoder as a data source for ESA. But, it is better to add a Concentrator to take advantage of undivided aggregation as the Decoder may have other processes aggregating from it.

5. Select a service and click **Continue**.

Note: You can add only one service at a time.



□	NAME	TRUSTED AUTHENTICATION	SSL	COMPRESSION
□	loghybrid1 - Log Decoder	true	true	false
□	loghybrid1 - Concentrator	false	true	false

Add New Datasource ×

Complete service configuration

□ Trusted Authentication

Provide credentials

USERNAME *

PASSWORD *

Configure the SSL settings

□ SSL

PORT NUMBER

50005

Cancel Back Save

6. Do one of the following:
   - Select the **Trusted Authentication** checkbox.
   - Enter your credentials (username and password) for the datasource.

> **Note:**
> - If you select **Trusted Authentication** instead of username and password. This option will enable the use of SSL by default. However, you can still configure the compression settings.
> - If you choose to enter your username and password. You can configure both SSL and compression settings.

7. To enable the SSL settings, select the **SSL** checkbox. You can set your desired port number.

   > **IMPORTANT:** Ensure that you turn on SSL only if necessary, in order to avoid performance impact on the SSL protocol.

8. (Optional) You have the option to adjust the Compression Level for Concentrators on ESA. To enable compression, select the **Compression** checkbox. You can set the **Compression Level** for a Concentrator from 0-9:

   - Compression Level = **0** (If compression is enabled, it allows Core Services to control the amount of compression.)
   - Compression Level = **1** (It uses the lowest amount of compression and has the highest performance.)
   - Compression Level = **9** (It uses the highest amount of compression and has the worst performance.)

   Somewhere in the middle between 1 and 9 is usually the best setting, which is what you get when you select a compression level of 0. For more detailed information, see the *Core Database Tuning Guide*.

   > **Note:** When you set the compression level for a Concentrator on ESA, it sets the same compression level for that Concentrator for ESA Correlation Rules.

9. Click **Test Configuration** to make sure that it can communicate with the ESA service.
10. Click **Save**.

    After you configure your data sources and they appear in the Available Configured Data Sources dialog, you can use them for your deployment.

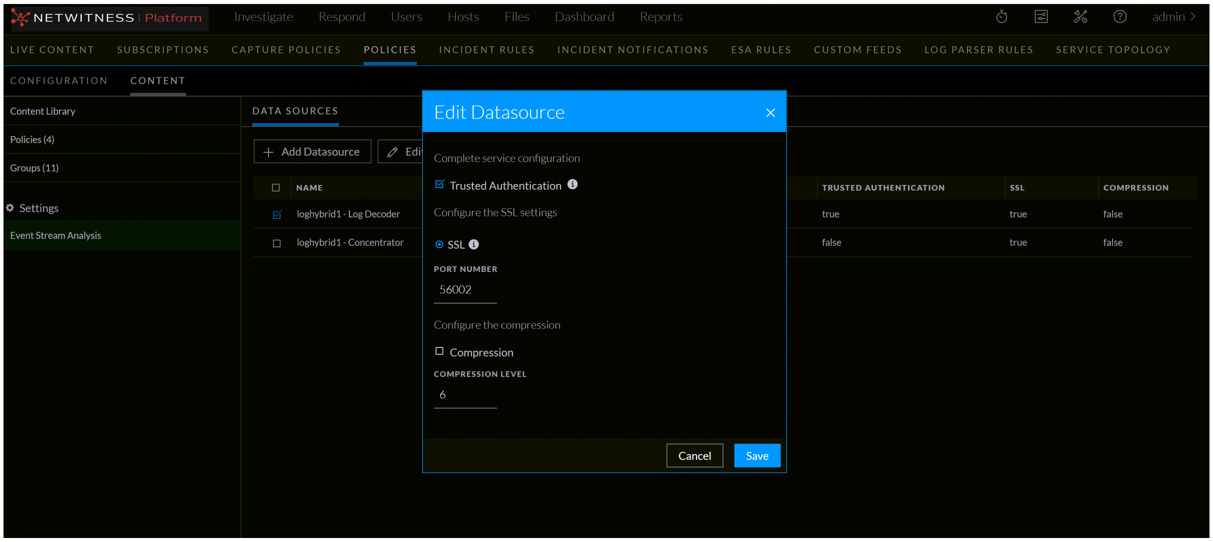
Edit an ESA Datasource

You can edit the properties of the datasource at any point in time. You can edit the user credentials, SSL, port, and compression value of the datasource. When a data source password changes, it is important to change the password on the data source so that ESA can continue to communicate with the data source.

To edit an ESA Datasource

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.
4. Select a datasource and click **Edit Datasource**.

The Edit Datasource dialog is displayed.



☐	NAME	TRUSTED AUTHENTICATION	SSL	COMPRESSION
☑	loghybrid1 - Log Decoder	true	true	false
☐	loghybrid1 - Concentrator	false	true	false

Edit Datasource

Complete service configuration

☑ Trusted Authentication

Configure the SSL settings

● SSL

PORT NUMBER

56002

Configure the compression

☐ Compression

COMPRESSION LEVEL

6

5. Make the required changes in the datasource.
6. Click **Save**.

Delete an ESA Datasource

You can delete one or more ESA datasources. Once the datasource is deleted, the service will be removed from the available configured list.

To delete an ESA Datasource

1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. Under **Settings**, click **Event Stream Analysis** > **Data Sources**.
4. Select a datasource and click **Delete Datasource**.

   A confirmation pop-up is displayed.
5. Click **Delete Datasource**.

Manage Deployments

The ESA deployment consists of a policy with ESA rules, ESA services, and data sources. The ESA service scans your network for suspicious activity whenever you deploy policies. An ESA rule detects a different event every time, such as when a user account is created and deleted within 24 hours.

In addition, you can perform other steps on your deployment, such as changing a data source, editing or deleting a rule from the deployment through policy, renaming or deleting the deployment, or showing updates to the deployment, see Additional ESA Correlation Rules Procedures

In 12.1 and later versions, you must create a policy with the ESA rule content type and associate the policy with the group having a correlation service to create a deployment.

For more information on policies, see Policies

For more information about groups, see Groups

Note: With the unified ESA Deployments tab, you can manage deployments from a single view across all policies within Policy-based Centralized Content Management (CCM).

You can do the following:

- View a Deployment
- Create a Deployment
- Edit a Deployment
- Start a Deployment
- Fast Deployment
- Deployment Stats
- Remove a Deployment
- Stop a Deployment
- Migrate ESA Deployments to Policies and Groups

View a Deployment

In the ESA deployment view, you can view a list of all the deployments associated with the policies and the actions you can perform with them. It helps you manage and set-up deployments within CCM to create, edit, deploy, remove, and stop deployments. NetWitness Platform provides two methods to manage deployments.

You can view deployments in the following ways:

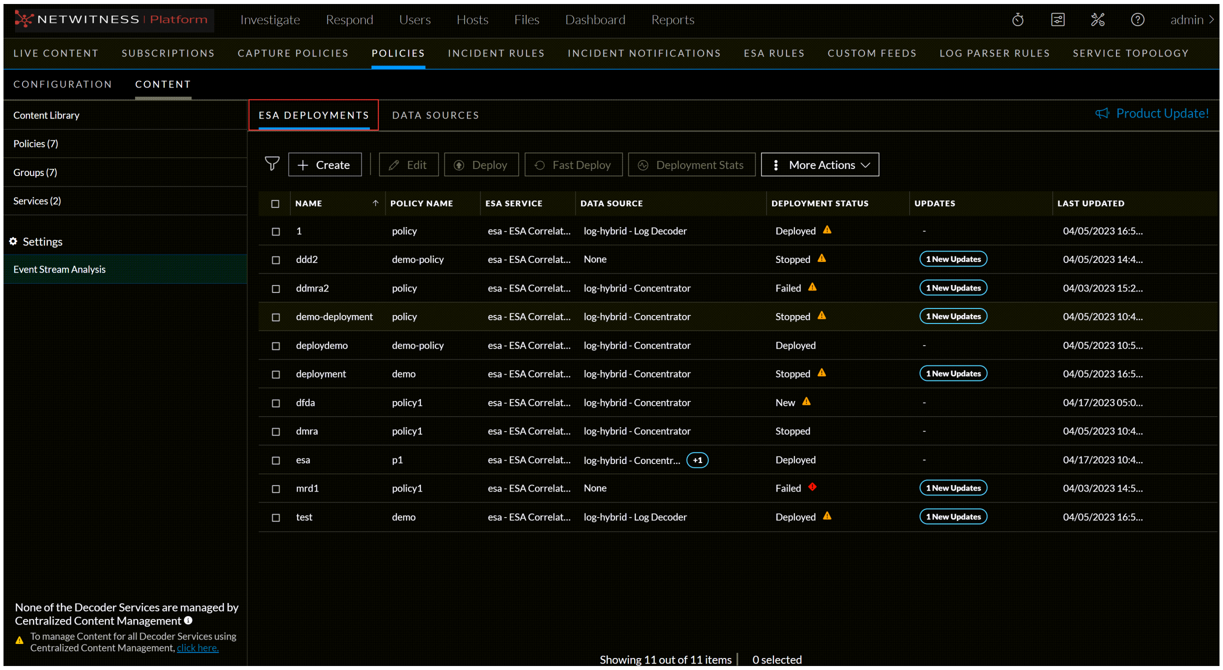
- Using the **ESA Deployments** tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can create, edit, remove, and pause deployments.

- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and create, edit, remove and pause a deployment.

To view all deployments using the ESA Deployments tab

1. Go to (CONFIGURE) > **Policies** > **Content**.
2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

The available deployments are displayed.



□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
□	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	-	04/05/2023 16:5...
□	ddd2	demo-policy	esa - ESA Correlat...	None	Stopped ⚠	1 New Updates	04/05/2023 14:4...
□	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
□	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
□	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
□	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 16:5...
□	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	New ⚠	-	04/17/2023 05:0...
□	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped	-	04/05/2023 10:4...
□	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
□	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
□	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

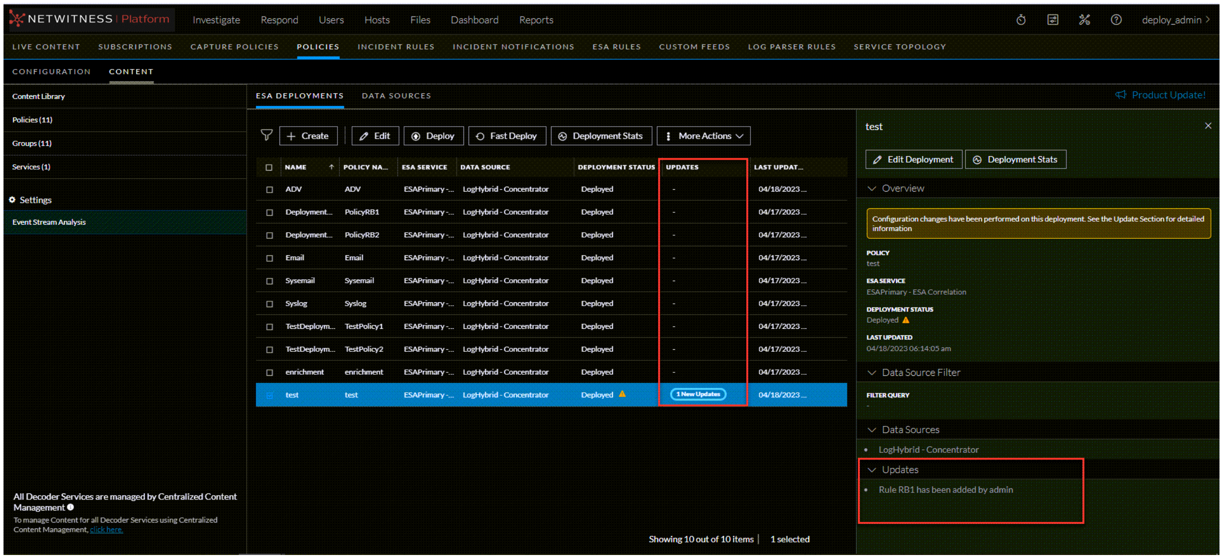
None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 11 out of 11 items | 0 selected

Note: Any changes made, like add / edit / delete to **rules**, **notifications**, and **enrichments** on the **ESA Rules** page for deployments, are displayed in the **Updates** section of the **ESA Deployments** view.

IMPORTANT: Any changes required for rule configurations must be made on the **ESA Rules** page only.



□	NAME	POLICY NA...	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDAT...
□	ADV	ADV	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/18/2023 ...
□	Deployment...	PolicyRB1	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
□	Deployment...	PolicyRB2	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
□	Email	Email	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
□	Sysemail	Sysemail	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
□	Syslog	Syslog	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
□	TestDeploym...	TestPolicy1	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
□	TestDeploym...	TestPolicy2	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
□	enrichment	enrichment	ESAPrimary -...	LogHybrid - Concentrator	Deployed	-	04/17/2023 ...
☑	test	test	ESAPrimary -...	LogHybrid - Concentrator	Deployed ⚠	1 New Updates	04/18/2023 ...

Showing 10 out of 10 items | 1 selected

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

test

Edit Deployment | Deployment Stats

Overview

Configuration changes have been performed on this deployment. See the Update Section for detailed information

POLICY
test

ESA SERVICE
ESAPrimary - ESA Correlation

DEPLOYMENT STATUS
Deployed ⚠

LAST UPDATED
04/18/2023 06:14:05 am

Data Source Filter

FILTER QUERY
-

Data Sources

- LogHybrid - Concentrator

Updates

- Rule RB1 has been added by admin

To view a deployment from a selected policy

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.

The available policies are displayed.

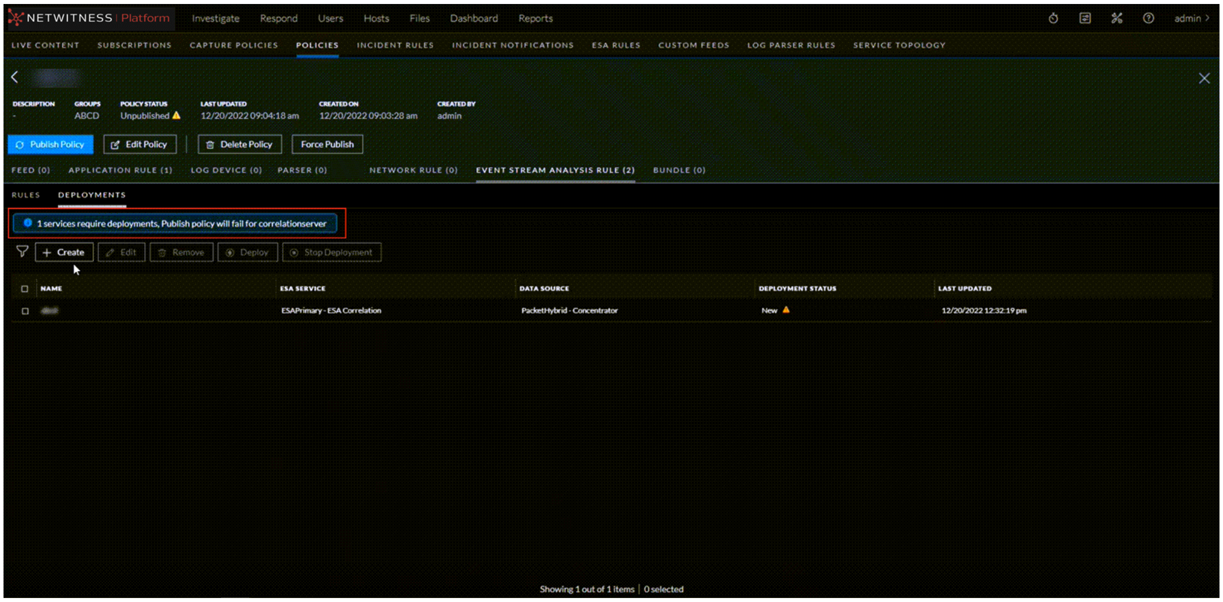
3. Click a Policy.

The selected policy view is displayed, and the Application Rule is default selected.

4. Click **Event Stream Analysis Rule** > **Deployments**.

The available deployments for the selected policy are displayed.

Caution: An icon ❗ is displayed in the deployments view indicating services require deployments, publish policy will fail for correlation servers. You may need to create deployments for such services if required.



[redacted]

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	ABCD	Unpublished ⚠	12/20/2022 09:04:18 am	12/20/2022 09:03:28 am	admin

1 services require deployments, Publish policy will fail for correlationserver

□	NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
□	[redacted]	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	New ⚠	12/20/2022 12:32:19 pm

Showing 1 out of 1 items | 0 selected

Create a Deployment

When you create a deployment, you need to select a policy, ESA service, and data sources. An ESA rule deployment consists of an ESA service, one or more data sources, and a set of ESA rules. When you deploy rules, the ESA service runs them to detect suspicious or undesirable activity in your network. Each ESA rule detects a different event, such as when a user account is created and deleted within one hour.

For more information on data sources, see Data Source

In 12.1 and later versions, you must create a policy with the ESA rule content type and associate the policy with the group having a correlation service to create a deployment.

For more information on policies, see Policies

You can create deployments in the following ways:

- Using the ESA Deployments tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can create deployments.

- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and create a deployment.

Prerequisites

- The group is assigned to a policy

- The Correlation server service is available in the groups assigned.

- A minimum of one ESA rule is added to the policy.
- ESA data source must be configured.

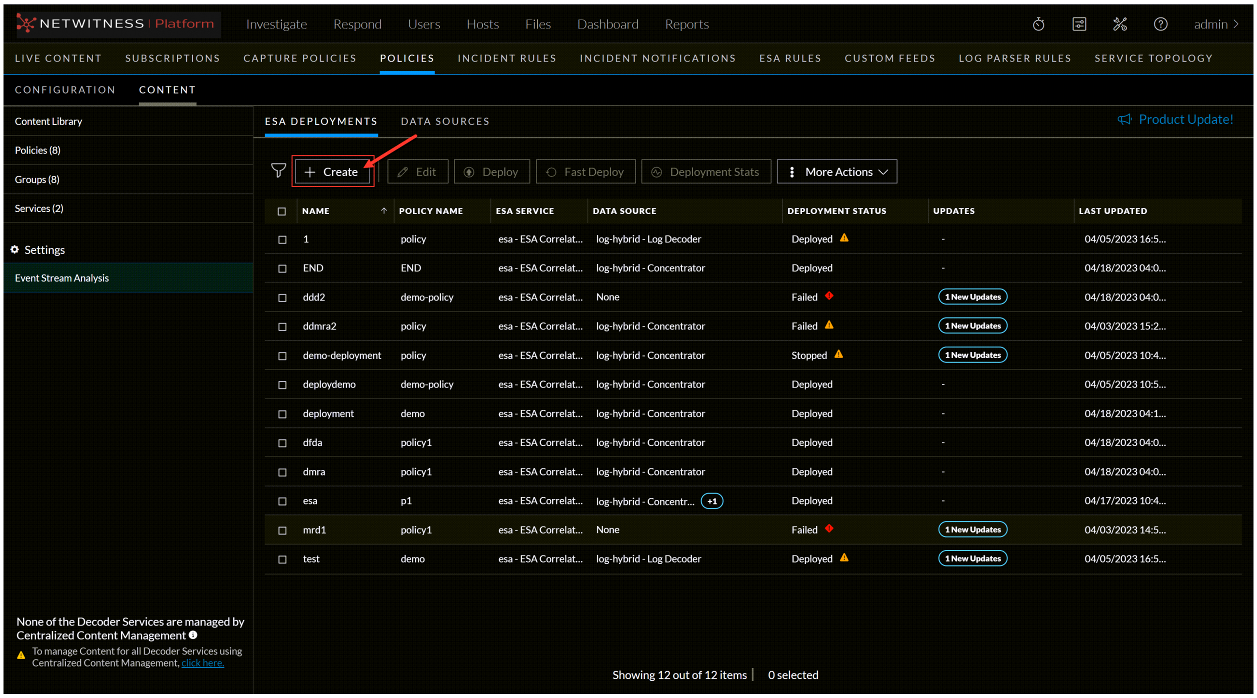
  For more information about groups, see Groups

To create a deployment using the ESA Deployments tab

1. Go to ⚙ **(CONFIGURE)** > **Policies** > **Content**.
2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

The available deployments are displayed.

3. Click + **Create**



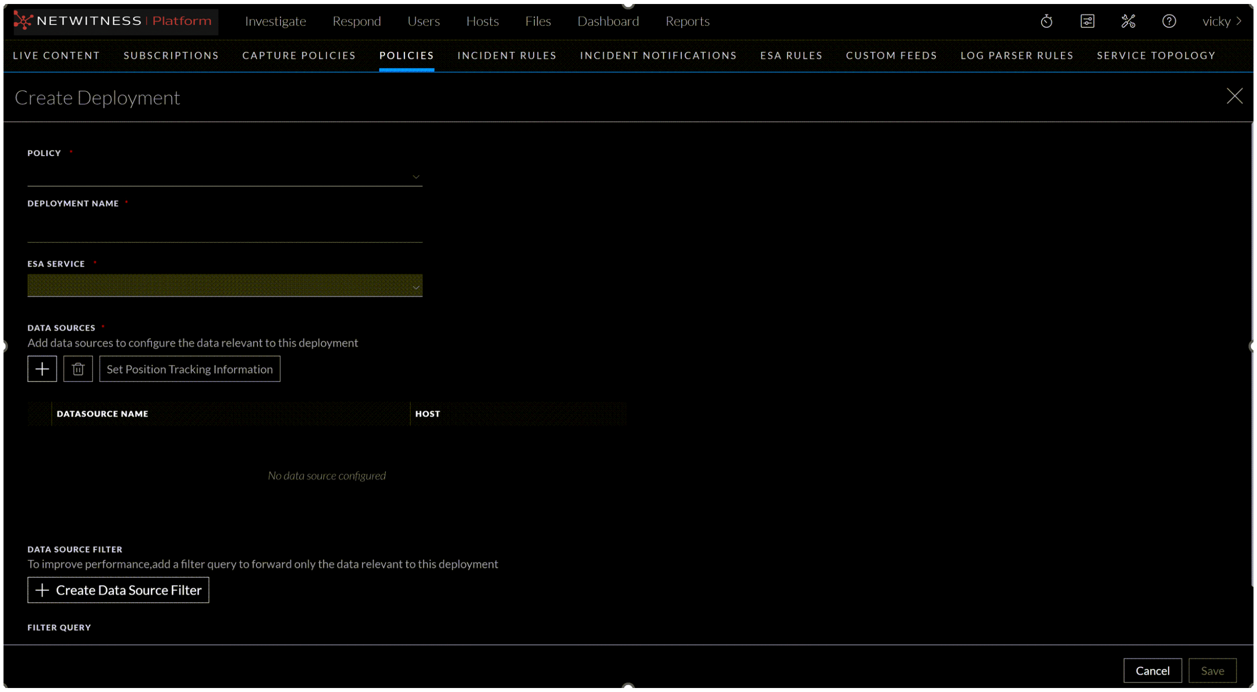
□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
□	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	-	04/05/2023 16:5...
□	END	END	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
□	ddd2	demo-policy	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/18/2023 04:0...
□	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
□	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
□	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
□	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:1...
□	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
□	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
□	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
□	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
□	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

Showing 12 out of 12 items | 0 selected

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

The Create Deployment dialog is displayed.



Add data sources to configure the data relevant to this deployment

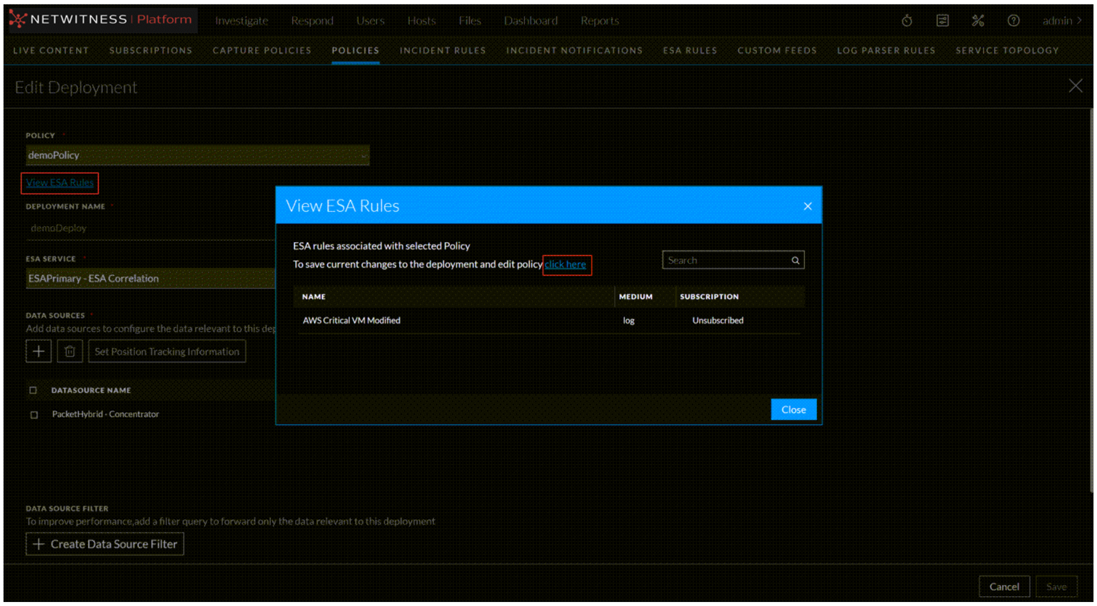
No data source configured

To improve performance,add a filter query to forward only the data relevant to this deployment

4. Select an eligible policy from the policy list.

> **Note:** All the policies that meet the criteria mentioned above are listed in the policy drop-down. It is required to select a policy to proceed further.

If required, you can click on View ESA Rules to search for rules associated with selected policy.



POLICY * demoPolicy

DEPLOYMENT NAME * demoDeploy

ESA SERVICE * ESAPrimary - ESA Correlation

DATA SOURCES *
Add data sources to configure the data relevant to this dep

□ PacketHybrid - Concentrator

To improve performance,add a filter query to forward only the data relevant to this deployment

ESA rules associated with selected Policy
To save current changes to the deployment and edit policy click here

NAME	MEDIUM	SUBSCRIPTION
AWS Critical VM Modified	log	Unsubscribed

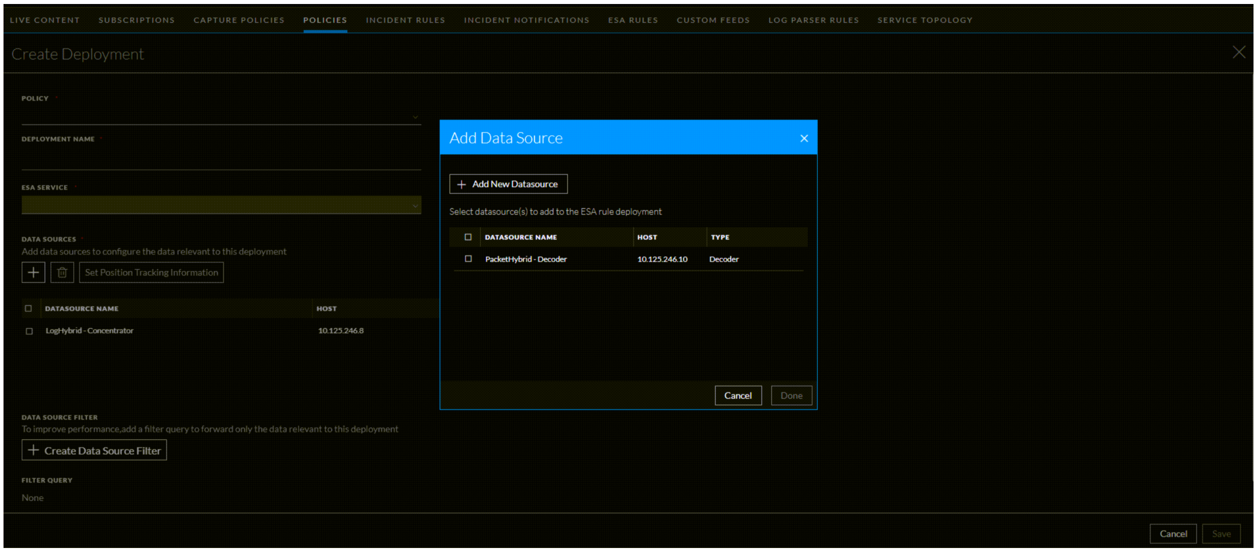
5. Enter a name for the deployment.

6. Select a service from the **ESA Service** drop-down list.

> **Note:** Once the deployment is saved, the selected policy, name and ESA service cannot be modified.

7. Under **Data Sources**, click + to add a data source.

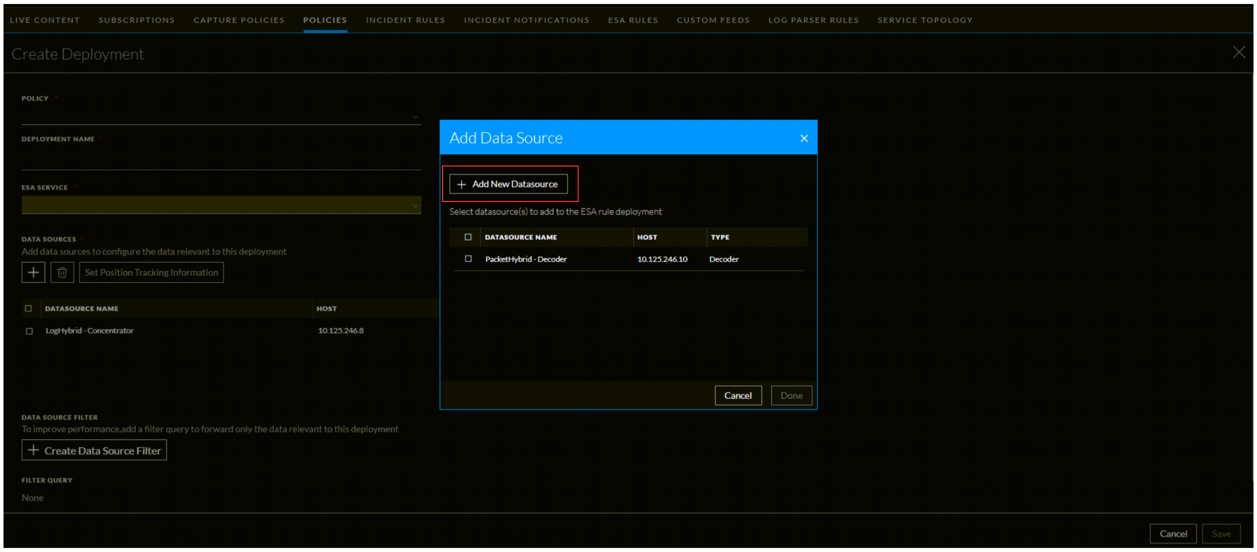
   The **Add Data Source** dialog is displayed.



□	DATASOURCE NAME	HOST
□	LogHybrid - Concentrator	10.125.246.8

□	DATASOURCE NAME	HOST	TYPE
□	PacketHybrid - Decoder	10.125.246.10	Decoder

If required, you can add a new data source by selecting **+ Add New Datasource** tab in the dialog-box.



□	DATASOURCE NAME	HOST
□	LogHybrid - Concentrator	10.125.246.8

□	DATASOURCE NAME	HOST	TYPE
□	PacketHybrid - Decoder	10.125.246.10	Decoder

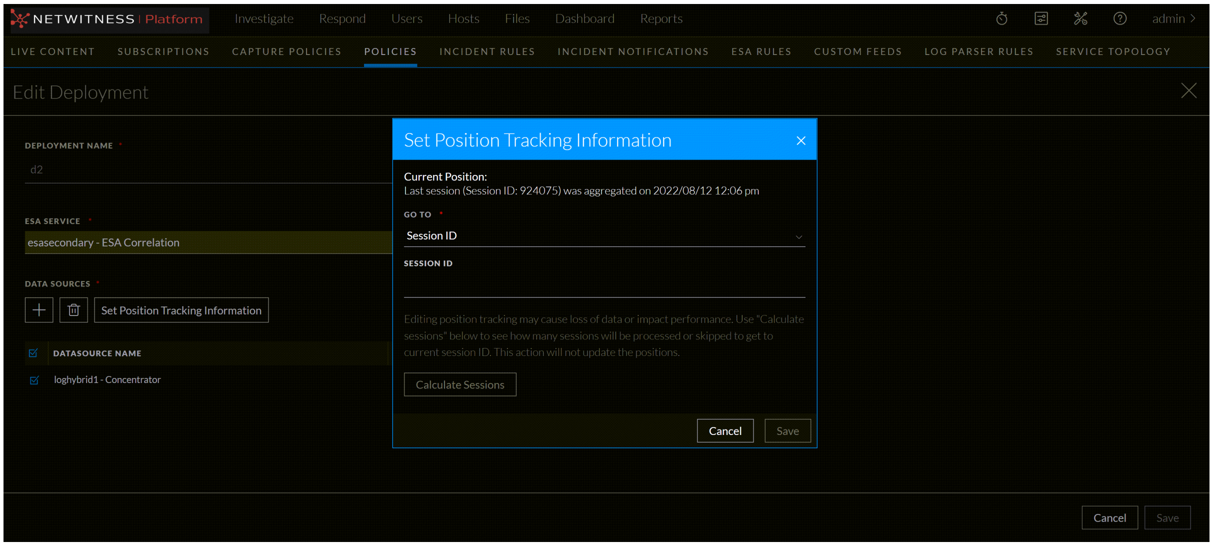
IMPORTANT: If the data sources are not listed, you can add the required datasource. For more information, see the topic Add an ESA Datasource.

8. Select one or more data sources and click Done.

9. To delete the data source, select the data source and click 🗑.

10. (Optional) Select the required data source and click **Set Position Tracking Information** to process specific or ignore certain sessions.

    The Set Position Tracking Information dialog is displayed.



Edit Deployment

DEPLOYMENT NAME *
d2

ESA SERVICE *
esasecondary - ESA Correlation

DATA SOURCES *

☑	DATASOURCE NAME
☑	loghybrid1 - Concentrator

Set Position Tracking Information

Current Position:
Last session (Session ID: 924075) was aggregated on 2022/08/12 12:06 pm

GO TO *
Session ID

SESSION ID

Editing position tracking may cause loss of data or impact performance. Use "Calculate sessions" below to see how many sessions will be processed or skipped to get to current session ID. This action will not update the positions.

a. In the Position Tracking Information dialog, perform the following:

   i. If you want to set the position tracking information based on date and time stamp:

      In the **Go To** drop-down menu, select **Date and Time** and enter the date and time.

   ii. If you want to set the position tracking information, based on the session ID:

      In the **Go To** drop-down menu, select **Session ID** and enter the session ID in the **Session ID** field.

      The ESA Correlation service starts processing the events from the session ID that you entered.

b. Click **Calculate Sessions** to calculate the number of sessions that will be processed to the existing position of the data source, if any.

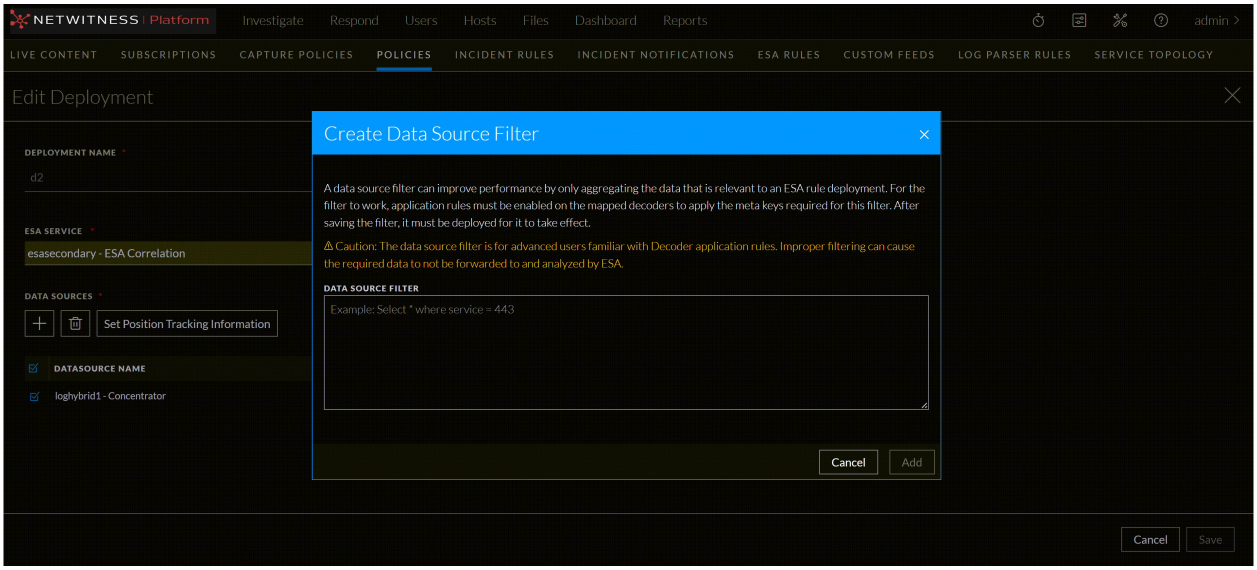
c. To save the edited position tracking data source, click **Save**.

   For more information on Position Tracking Information, see Position Tracking Information.

11. (Optional) To filter out specific session data coming into ESA, under Data Source Filter, click + **Create Data Source Filter**.

Caution: The data source filter is for advanced users familiar with Decoder application rules. Improper filtering can cause the required data not to be forwarded to and analyzed by ESA.

The **Create Data Source Filter** dialog is displayed.



Edit Deployment

DEPLOYMENT NAME *: d2

ESA SERVICE *: esasecondary - ESA Correlation

DATA SOURCES *

☑ DATASOURCE NAME

☑ loghybrid1 - Concentrator

Create Data Source Filter

A data source filter can improve performance by only aggregating the data that is relevant to an ESA rule deployment. For the filter to work, application rules must be enabled on the mapped decoders to apply the meta keys required for this filter. After saving the filter, it must be deployed for it to take effect.

⚠ Caution: The data source filter is for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

DATA SOURCE FILTER: Example: Select * where service = 443

a. Specify the filter query in the below format as shown in the following example:

Select *where service = 443

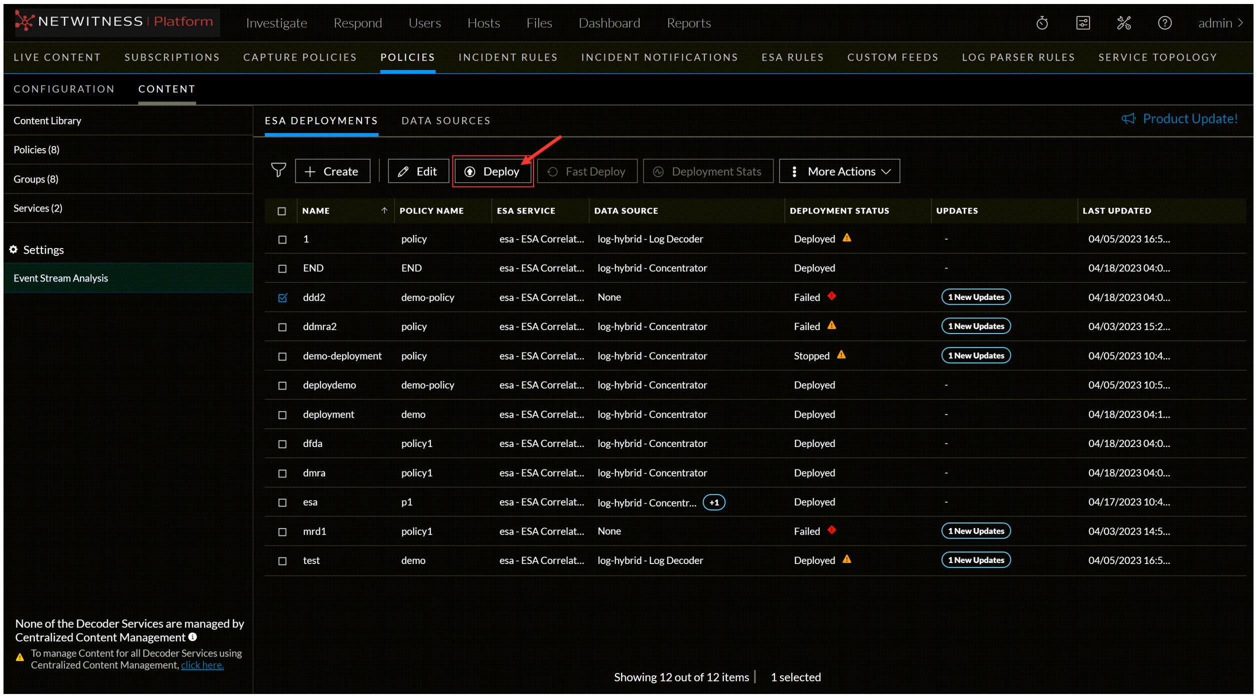
Based on the query processed, it will filter out only HTTPS logs-related sessions and will be forwarded to the ESA.

b. Click **Add**.

c. If you want to delete the existing data sources filter, click **Clear Data Source Filter**, and **Save** to remove it permanently.

12. To save the deployment, click **Save**.

13. Select the created deployment and click **Deploy**.



□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
□	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	-	04/05/2023 16:5...
□	END	END	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☑	ddd2	demo-policy	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/18/2023 04:0...
□	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
□	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
□	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
□	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:1...
□	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
□	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
□	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
□	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
□	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 12 out of 12 items | 1 selected

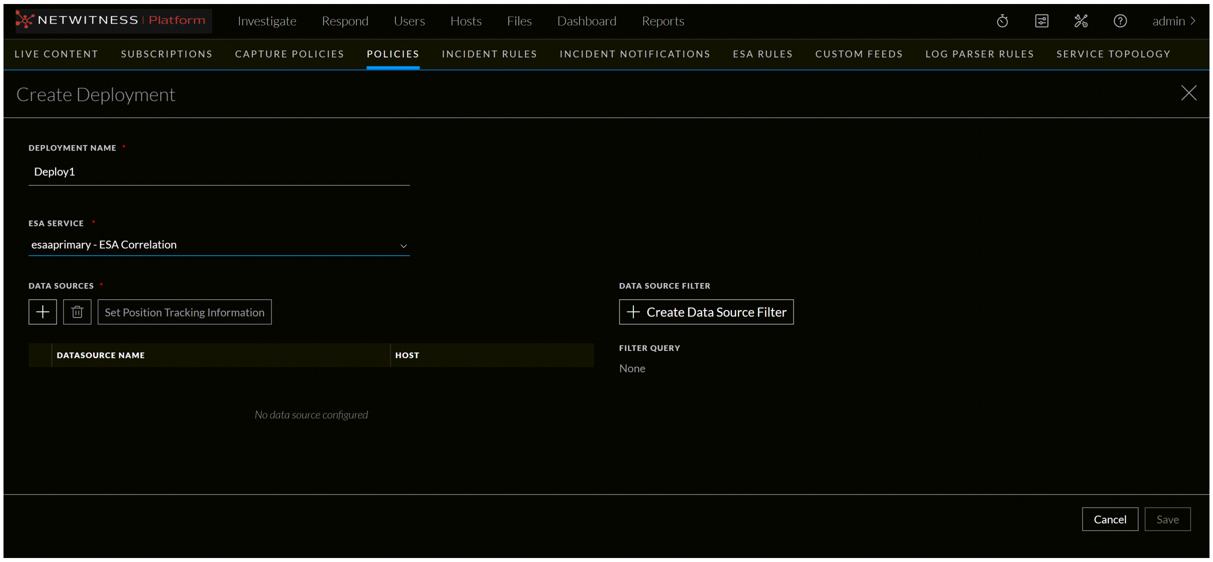
To create a deployment from a selected policy

1. Go to **(CONFIGURE)** > **Policies**.
2. In the policies panel, click **Content**.
   The available policies are displayed.
3. Click a Policy.

   The selected policy view is displayed and by default **Application Rule** is selected.
4. Click **Event Stream Analysis Rule** > **Deployments**.

   The available deployments for the selected policy are displayed.
5. Click + **Create Deployment**.

   The Create Deployment dialog is displayed.



Create Deployment

DEPLOYMENT NAME *
Deploy1

ESA SERVICE *
esaaprimary - ESA Correlation

DATA SOURCES *

No data source configured

DATA SOURCE FILTER

FILTER QUERY
None

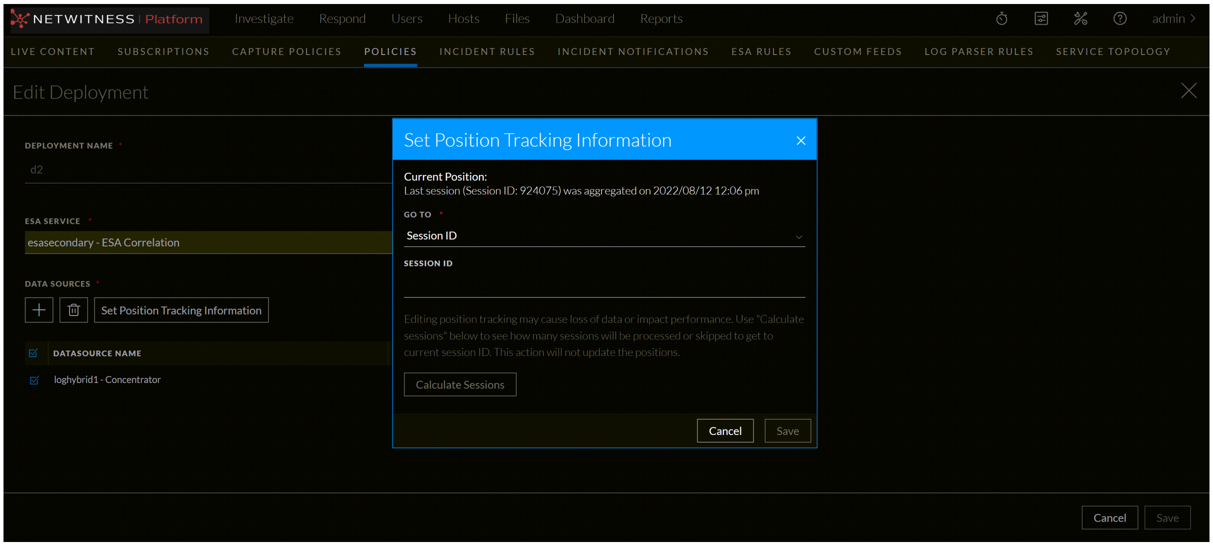
6. Enter a name for the deployment.

   Note: The policy is preselected as the user creates the deployment from the policy details view.
7. Select a service from the **ESA Service** drop-down list.
8. Under **Data Sources**, click + to add a data source.

   The Add Data Source dialog is displayed.
9. Select one or more data sources and click **Done**.

   IMPORTANT: If the data sources are not listed, you can add the required datasource. For more information, see the topic Add an ESA Datasource.
10. To delete the data source, select the data source and click .
11. (Optional) the required data source and click **Set Position Tracking Information** to reprocess specific sessions or ignore certain sessions.

    The Set Position Tracking Information dialog is displayed.



DEPLOYMENT NAME *
d2

ESA SERVICE *
esasecondary - ESA Correlation

DATA SOURCES *

☑	DATASOURCE NAME
☑	loghybrid1 - Concentrator

Current Position:
Last session (Session ID: 924075) was aggregated on 2022/08/12 12:06 pm

GO TO *
Session ID

SESSION ID

Editing position tracking may cause loss of data or impact performance. Use "Calculate sessions" below to see how many sessions will be processed or skipped to get to current session ID. This action will not update the positions.

a. In the Position Tracking Information dialog, perform the following:

   i. If you want to set the position tracking information based on date and time stamp:

      In the **Go To** drop-down menu, select **Date and Time** and enter the date and time.

   ii. If you want to set the position tracking information, based on the session ID:

      In the **Go To** drop-down menu, select **Session ID** and enter the session ID in the **Session ID** field.

      The ESA Correlation service starts processing the events from the session ID that you entered.

b. Click **Calculate Sessions** to calculate the number of sessions that will be processed with respect to the existing position of the data source, if any.

c. To save the edited position tracking data source, click **Save**.

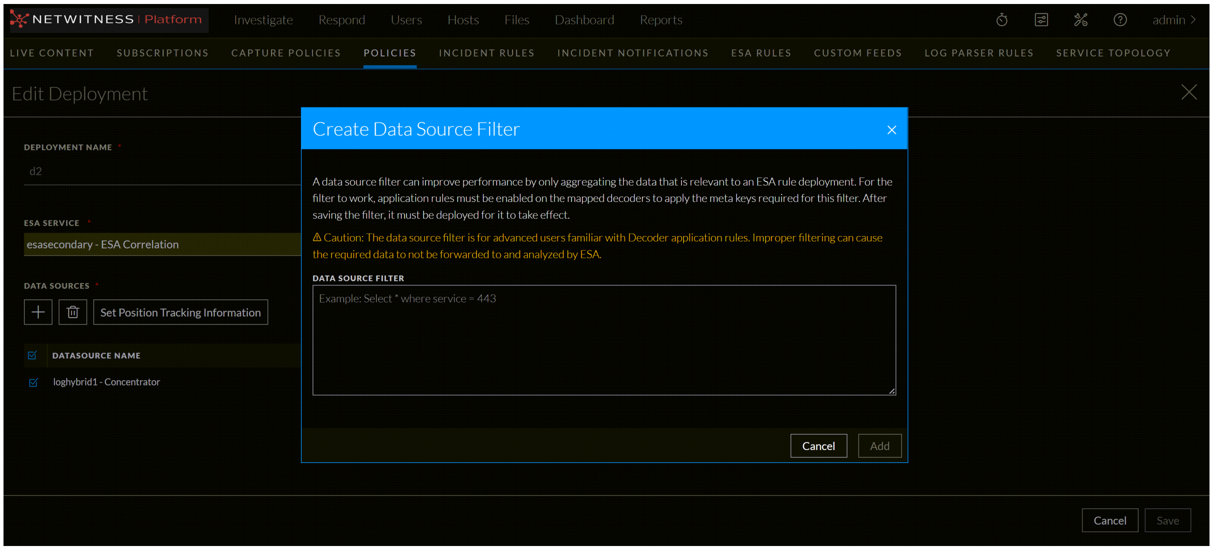
d. The tracking position information will be deployed to the ESA Correlation service, only when the deployment is successfully completed.

   For more information on Position Tracking Information, see Position Tracking Information.

12. (Optional) To filter out certain session data coming into ESA, under Data Source Filter, click + **Create Data Source Filter**.

> **Caution:** The data source filter is for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

The Create Data Source Filter dialog is displayed.



Edit Deployment

DEPLOYMENT NAME *
d2

ESA SERVICE *
esasecondary - ESA Correlation

DATA SOURCES *

☑	DATASOURCE NAME
☑	loghybrid1 - Concentrator

Create Data Source Filter

A data source filter can improve performance by only aggregating the data that is relevant to an ESA rule deployment. For the filter to work, application rules must be enabled on the mapped decoders to apply the meta keys required for this filter. After saving the filter, it must be deployed for it to take effect.

⚠ Caution: The data source filter is for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

DATA SOURCE FILTER
Example: Select * where service = 443

a. Specify the filter query in the below format as shown in the following example:

   Select *where service = 443

   Based on the query processed, it will filter out only HTTPS logs related sessions and will be forwarded to the ESA.

b. Click **Add**.

c. If you want to delete the existing data sources filter, click **Clear Data Source Filter** and click **Save** to remove it permanently.

13. To save deployment, click **Save**.

14. Select the created deployment and click **Deploy**.

Edit a Deployment

You can edit a deployment to change the data source, create a data source filter, and view ESA rules that are associated with this deployment. A data source filter can improve performance by only aggregating the data that is relevant to an ESA rule deployment. For the filter to work, application rules must be enabled on the mapped decoders to apply the meta keys required for this filter. After saving the filter, it must be deployed for it to take effect.

However, you cannot change the deployment name, or ESA service that are associated with the deployment.

You can edit deployments in the following ways:

- Using the ESA Deployments tab. The **ESA Deployments** tab provides a consolidated view of all the available deployments within CCM. You can edit deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and edit a deployment.

To edit a deployment from the ESA Deployments tab

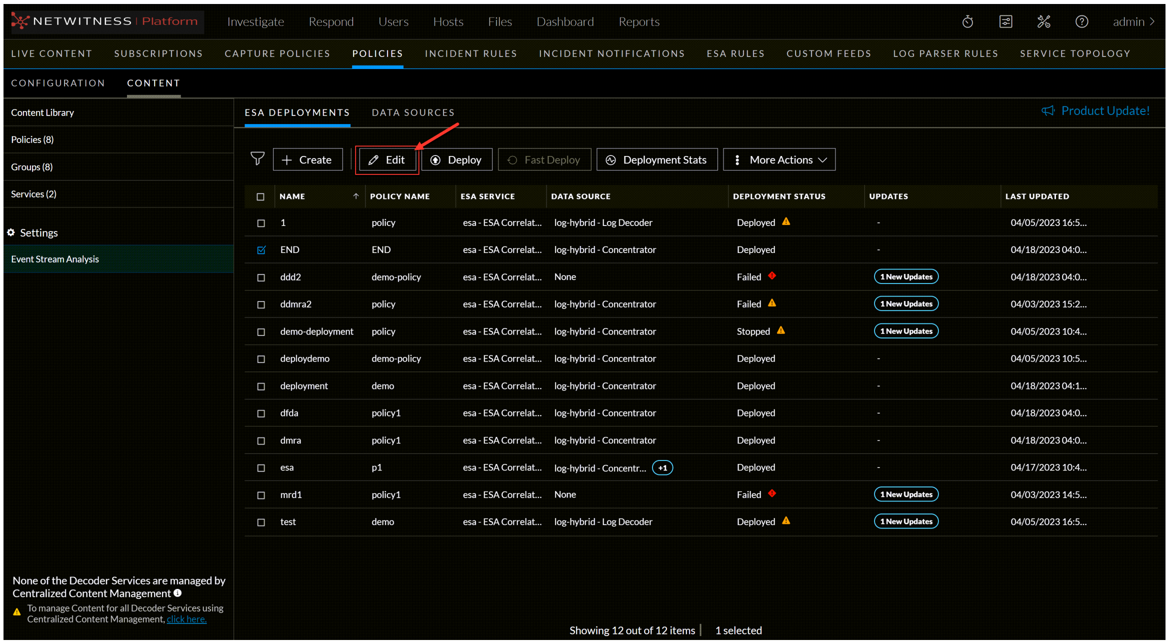
1. Go to **(CONFIGURE)** > **Policies** > **Content**.

2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

The available deployments are displayed.

3. Select a deployment and click **Edit** or **Edit Deployment**.

   a. When you select the checkbox and click **Edit**.



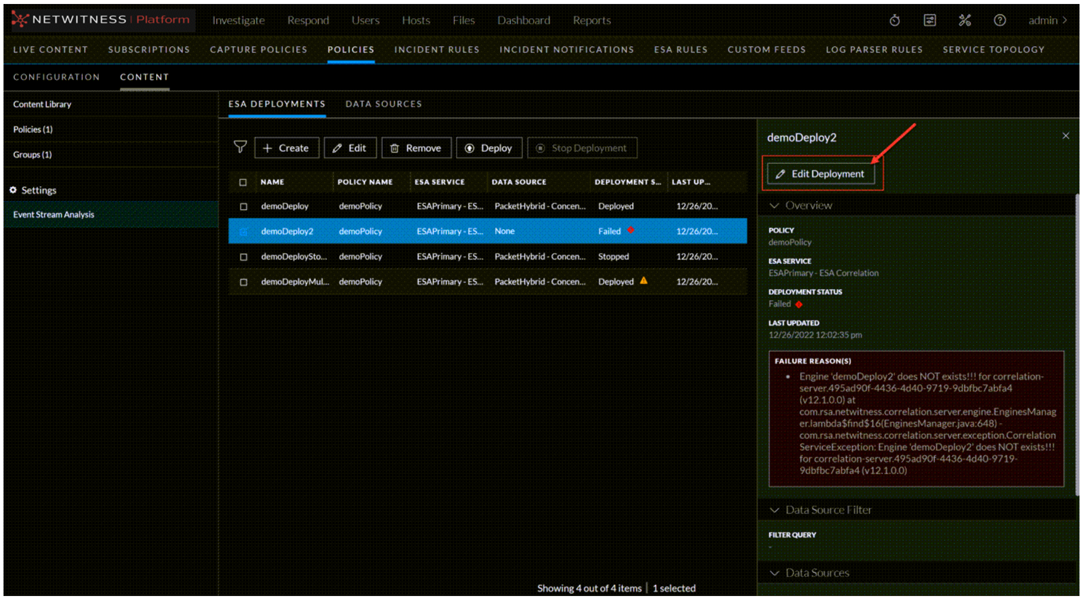
☐	NAME ↑	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
☐	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	-	04/05/2023 16:5...
☑	END	END	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	ddd2	demo-policy	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/18/2023 04:0...
☐	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
☐	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
☐	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
☐	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:1...
☐	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
☐	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
☐	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 12 out of 12 items | 1 selected

   b. When you select or click a row of the deployment, a right panel is displayed to click **Edit Deployment**.



☐	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT S...	LAST UP...
☐	demoDeploy	demoPolicy	ESAPrimary - ES...	PacketHybrid - Concen...	Deployed	12/26/20...
☑	demoDeploy2	demoPolicy	ESAPrimary - ES...	None	Failed ◆	12/26/20...
☐	demoDeploySto...	demoPolicy	ESAPrimary - ES...	PacketHybrid - Concen...	Stopped	12/26/20...
☐	demoDeployMul...	demoPolicy	ESAPrimary - ES...	PacketHybrid - Concen...	Deployed ⚠	12/26/20...

Showing 4 out of 4 items | 1 selected

demoDeploy2

POLICY
demoPolicy

ESA SERVICE
ESAPrimary - ESA Correlation

DEPLOYMENT STATUS
Failed ◆

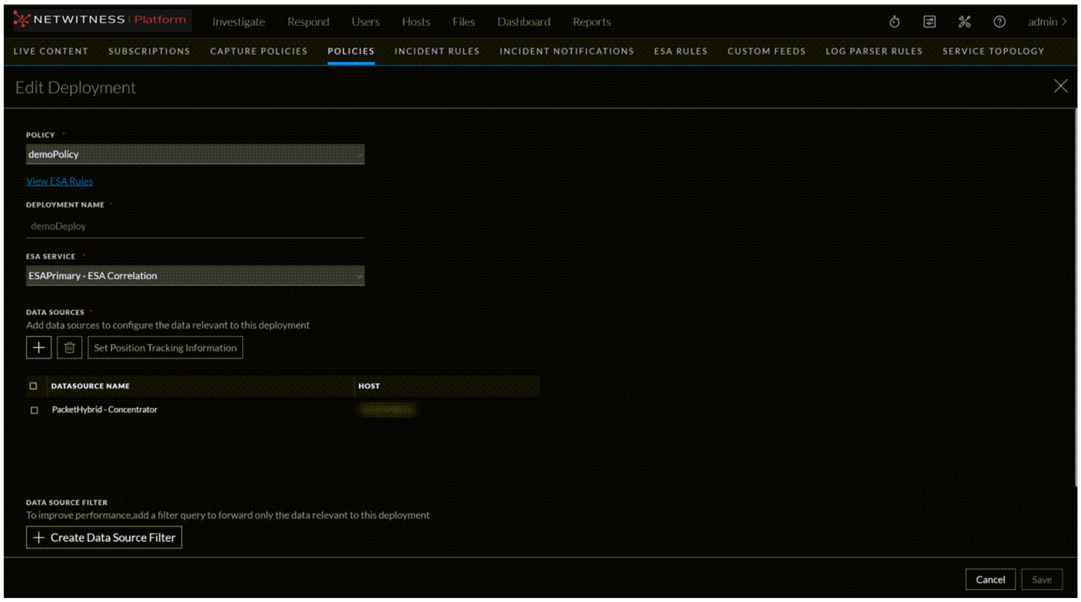
LAST UPDATED
12/26/2022 12:02:35 pm

FAILURE REASON(S)

- Engine 'demoDeploy2' does NOT exists!!! for correlation-server.495ad90f-4436-4d40-9719-9dbfbc7abfa4 (v12.1.0.0) at com.rsa.netwitness.correlation.server.engine.EnginesManager.lambda$find$16(EnginesManager.java:648) - com.rsa.netwitness.correlation.server.exception.CorrelationServiceException: Engine 'demoDeploy2' does NOT exists!!! for correlation-server.495ad90f-4436-4d40-9719-9dbfbc7abfa4 (v12.1.0.0)

FILTER QUERY
-

The **Edit Deployment** dialog is displayed.



Edit Deployment

POLICY * demoPolicy

View ESA Rules

DEPLOYMENT NAME * demoDeploy

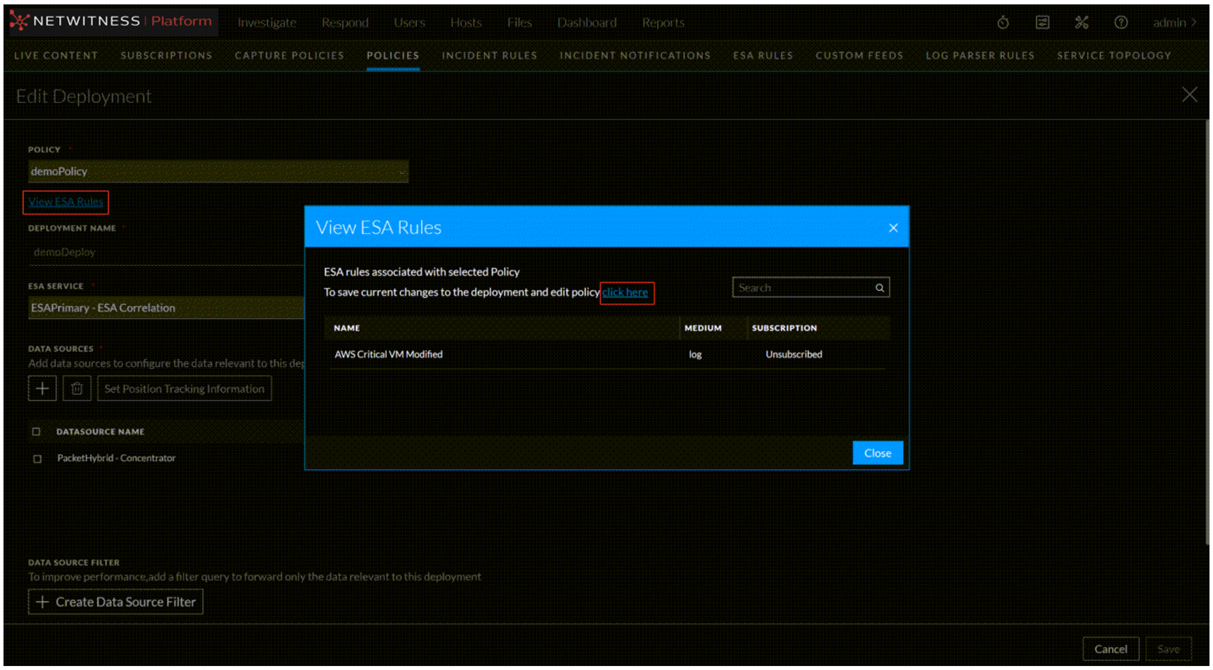
ESA SERVICE * ESAPrimary - ESA Correlation

DATA SOURCES *
Add data sources to configure the data relevant to this deployment

□	DATASOURCE NAME	HOST
□	PacketHybrid - Concentrator	[redacted]

DATA SOURCE FILTER
To improve performance,add a filter query to forward only the data relevant to this deployment

4. (Optional) you can click on **View ESA Rules** to search for rules associated with selected policy. To save current changes to the deployment and modify the policy, select **click here** and navigate to the **Edit Content Policy** page.



View ESA Rules

ESA rules associated with selected Policy
To save current changes to the deployment and edit policy click here

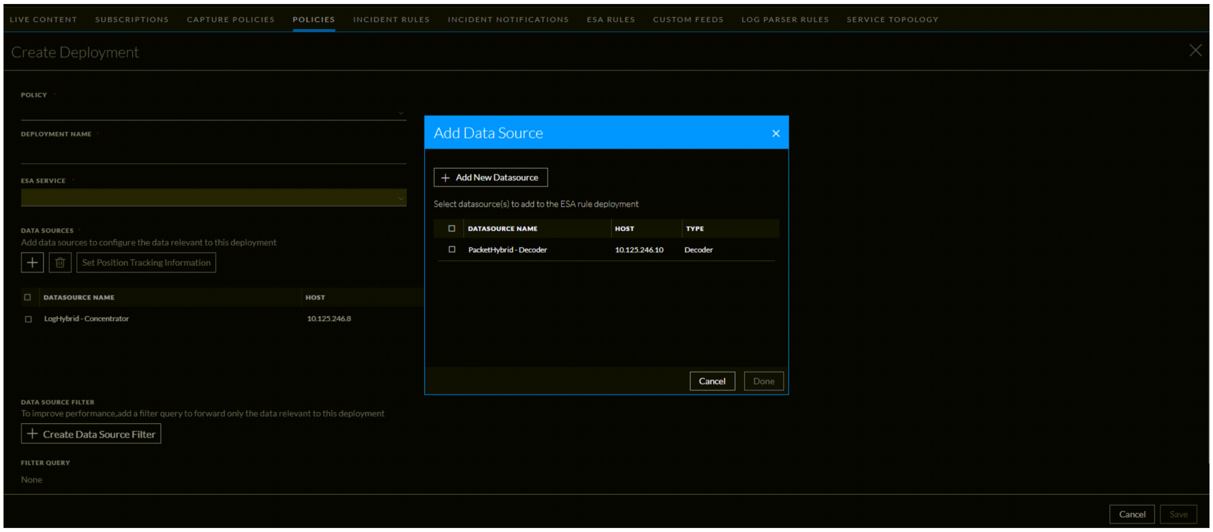
NAME	MEDIUM	SUBSCRIPTION
AWS Critical VM Modified	log	Unsubscribed

5. Make the required changes in the deployment.

   Policy, deployment name, and ESA service are pre-populated and cannot be modified.

6. Under **Data Sources**, click + to add a data source.

   The **Add Data Source** dialog is displayed.



Create Deployment

POLICY *

DEPLOYMENT NAME *

ESA SERVICE *

DATA SOURCES *
Add data sources to configure the data relevant to this deployment

□	DATASOURCE NAME	HOST
□	LogHybrid - Concentrator	10.125.246.8

DATA SOURCE FILTER
To improve performance,add a filter query to forward only the data relevant to this deployment

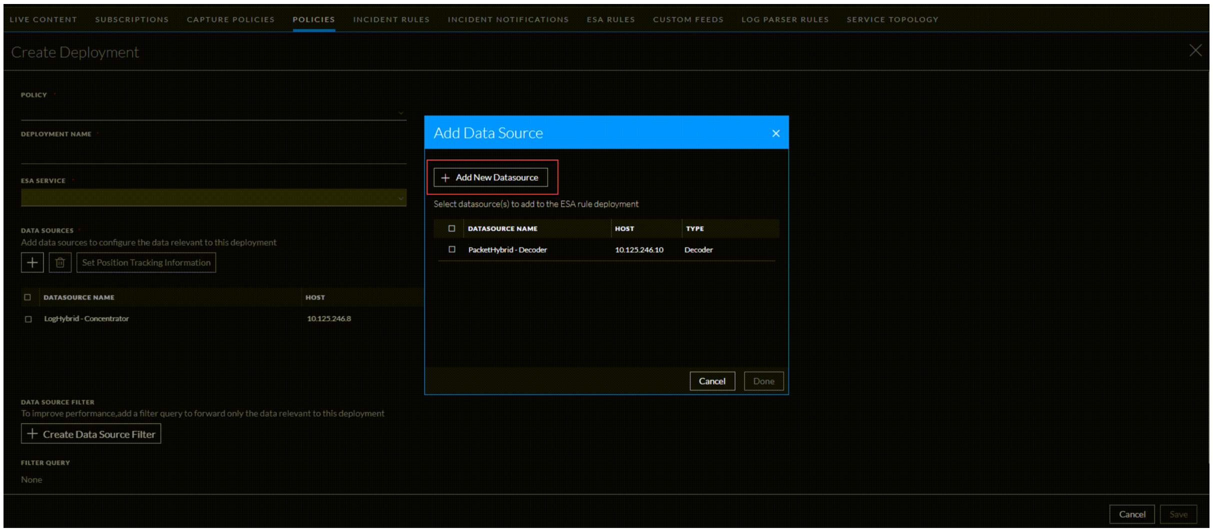
FILTER QUERY
None

Add Data Source

Select datasource(s) to add to the ESA rule deployment

□	DATASOURCE NAME	HOST	TYPE
□	PacketHybrid - Decoder	10.125.246.10	Decoder

7. If required, you can add a new data source by selecting **+ Add New Datasource** tab in the dialog-box.



Create Deployment

POLICY *

DEPLOYMENT NAME *

ESA SERVICE *

DATA SOURCES *
Add data sources to configure the data relevant to this deployment

□	DATASOURCE NAME	HOST
□	LogHybrid - Concentrator	10.125.246.8

DATA SOURCE FILTER
To improve performance,add a filter query to forward only the data relevant to this deployment

FILTER QUERY
None

Add Data Source

Select datasource(s) to add to the ESA rule deployment

□	DATASOURCE NAME	HOST	TYPE
□	PacketHybrid - Decoder	10.125.246.10	Decoder

IMPORTANT: If the data sources are not listed, you can add the required datasource. For more information, see the topic Add an ESA Datasource.

8. Click **Save**.

9. Select the deployment and click **Deploy**.

To edit a deployment from a selected policy

1. Go to ⚙ **(CONFIGURE)** > **Policies**.

2. In the policies panel, click **Content**.
   The available policies are displayed.

3. Click a Policy.

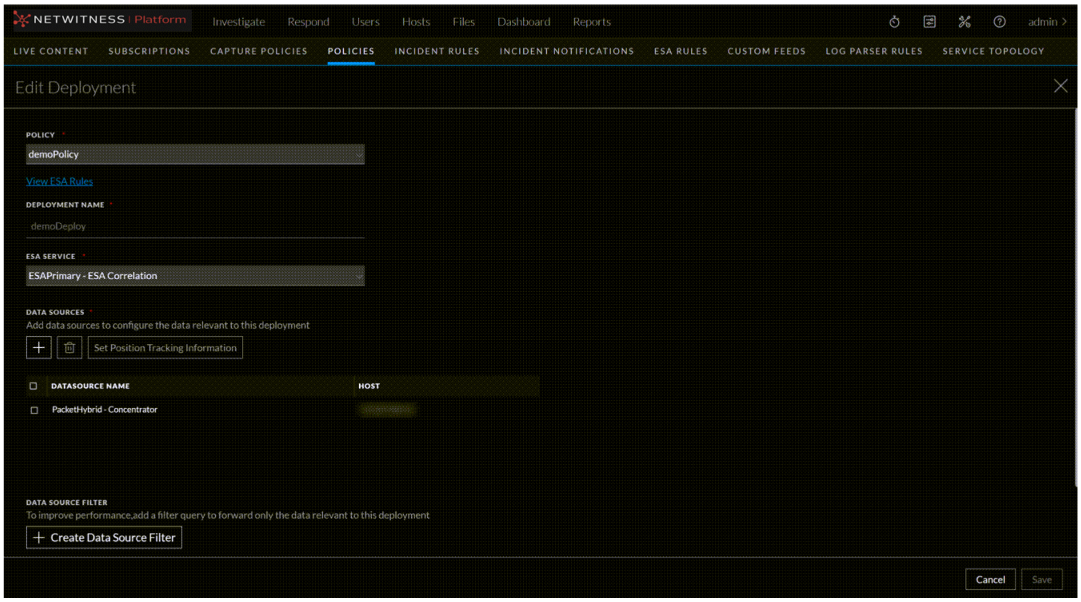
   The selected policy view is displayed and by default **Application Rule** is selected.

4. Click **Event Stream Analysis Rule** > **Deployments**.

   The available deployments for the selected policy are displayed.

5. Select a deployment to edit and click **Edit Deployment**.

   The **Edit Deployment** dialog is displayed.



Edit Deployment

POLICY *
demoPolicy

DEPLOYMENT NAME *
demoDeploy

ESA SERVICE *
ESAPrimary - ESA Correlation

DATA SOURCES *
Add data sources to configure the data relevant to this deployment

□	DATASOURCE NAME	HOST
□	PacketHybrid - Concentrator	[redacted]

DATA SOURCE FILTER
To improve performance,add a filter query to forward only the data relevant to this deployment

6. Make the required changes in the deployment.

7. Click **Save**.

8. Select the deployment and click **Deploy**.

   Note: You can deploy the changes either by performing a **Deploy** action on selected deployment or by publishing the policy. Publishing a policy with deployment in stopped state, will not deploy the deployment.

Start a Deployment

The deployment includes ESA services with policy and associated ESA rules. When you initiate deployment, the correlation services start processing sessions from the configured data sources for matching events for the selected ESA rules in the policy.

For more information about ESA services and rules, see Alerting with ESA Correlation Rules

You can start deployments in the following ways:

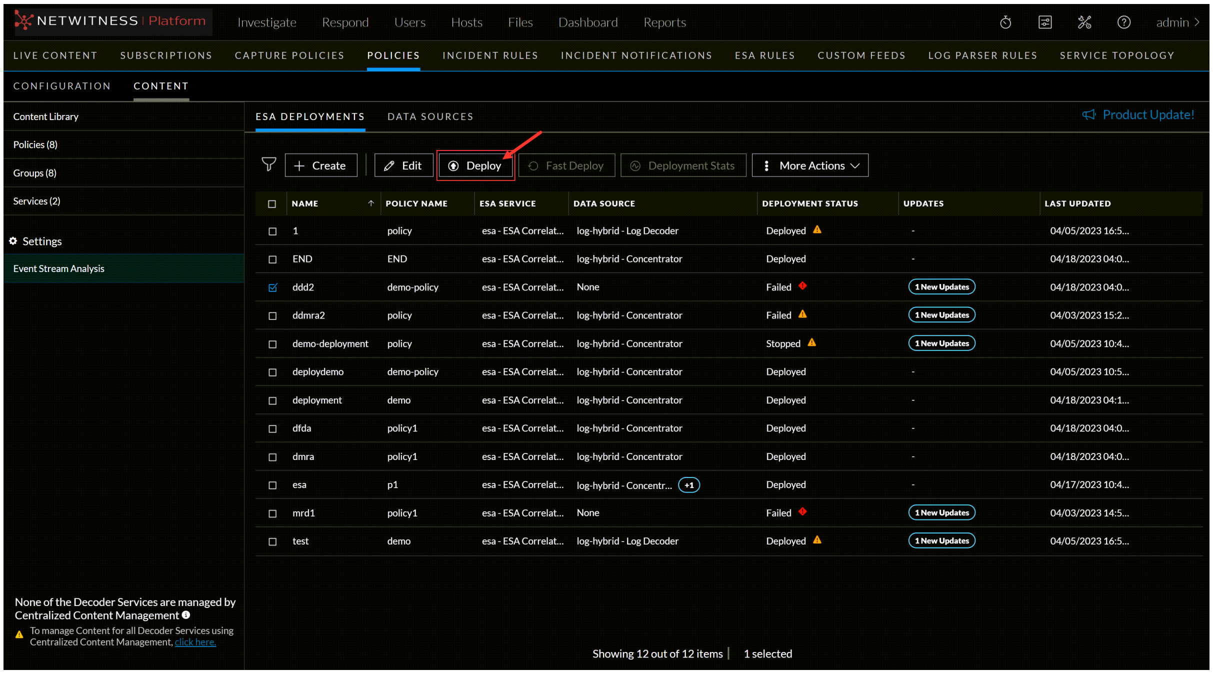
- Using the ESA Deployments tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can initiate deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and initiate a deployment.

To initiate a deployment, with the ESA Deployments tab

1. Go to (**CONFIGURE**) > **Policies** > **Content**.
2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

The available deployments are displayed.

3. Select a deployment and click **Deploy**.



☐	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
☐	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	-	04/05/2023 16:5...
☐	END	END	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☑	ddd2	demo-policy	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/18/2023 04:0...
☐	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
☐	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
☐	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
☐	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:1...
☐	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
☐	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
☐	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 12 out of 12 items | 1 selected

To start a deployment with selected policy

1. Go to (**CONFIGURE**) > **Policies**.
2. In the policies panel, click **Content**.
   The available policies are displayed.
3. Click a Policy.

   The selected policy view is displayed and by default **Application Rule** is selected.
4. Click **Event Stream Analysis Rule** > **Deployments**.

   The available deployments for the selected policy are displayed.
5. Select the deployment to deploy and click **Deploy**.

> **Note:** You can deploy the changes either by performing a Deploy action on selected deployment or by publishing the policy. Publishing a policy with deployment in stopped state, will not deploy the deployment.

Fast Deployment

The **Fast Deploy** option is a feature that allows a user to quickly load the latest rule that runs entirely on the Esper Engine without redeploying the entire engine.

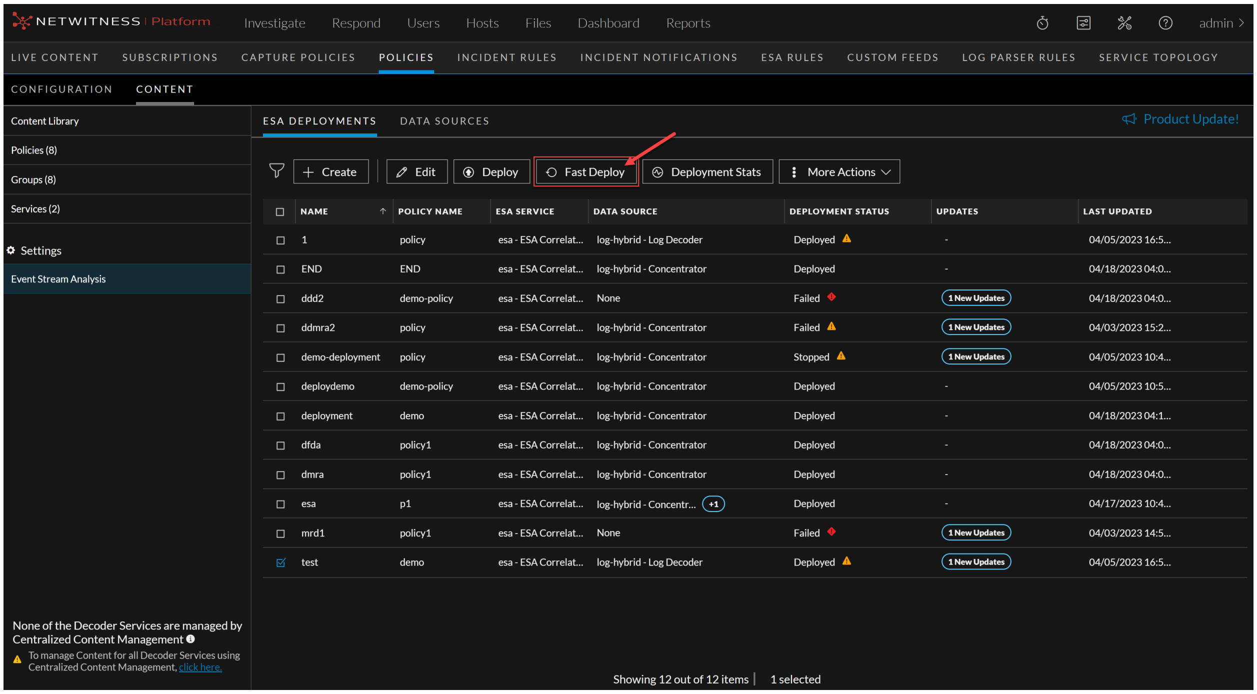
To do fast deployment

1. Go to ▣ **(CONFIGURE)** > **Policies** > **Content**.
2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

The available deployments are displayed.

You can use the **Fast Deploy** option when there has been a change to an ESA rule, i.e., a rule has been added, modified, or deleted. If any other changes have been made, such as adding a data source, then the **Fast Deploy** option will not be available.

3. Select the deployments that are updated and need to be deployed.
4. Click **Fast Deploy**.



☐	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
☐	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	-	04/05/2023 16:5...
☐	END	END	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	ddd2	demo-policy	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/18/2023 04:0...
☐	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
☐	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
☐	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
☐	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:1...
☐	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☐	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
☐	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
☑	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

Showing 12 out of 12 items | 1 selected

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Deployment Stats

When an ESA deployment is deployed, you can view details about how the deployment is performing, such as statistics on the engine, rule, and alert. You can also view information on which rules are enabled or disabled and change their status.

This topic describes how to view an ESA Correlation service's deployment statistics (stats). This procedure is useful when determining a rule's effectiveness or troubleshooting an ESA rule deployment.

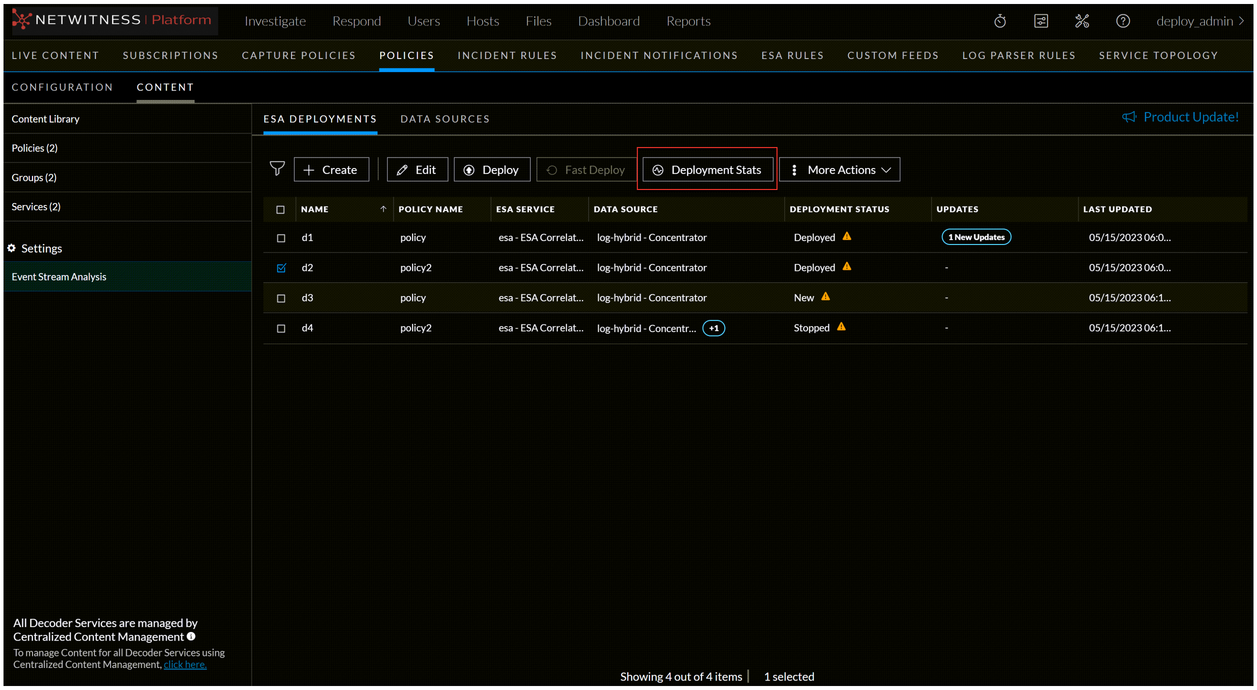
> **Caution:** When you modify and re-deploy an ESA rule deployment, all the stats are removed from that deployment. The generated alerts are not removed from NetWitness.

To view a Deployment Stats

1. Go to (CONFIGURE) > **Policies** > **Content**.
2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

The available deployments are displayed.

3. Select a deployment you want to see the stats.
4. Click on the **Deployment Stats** tab.



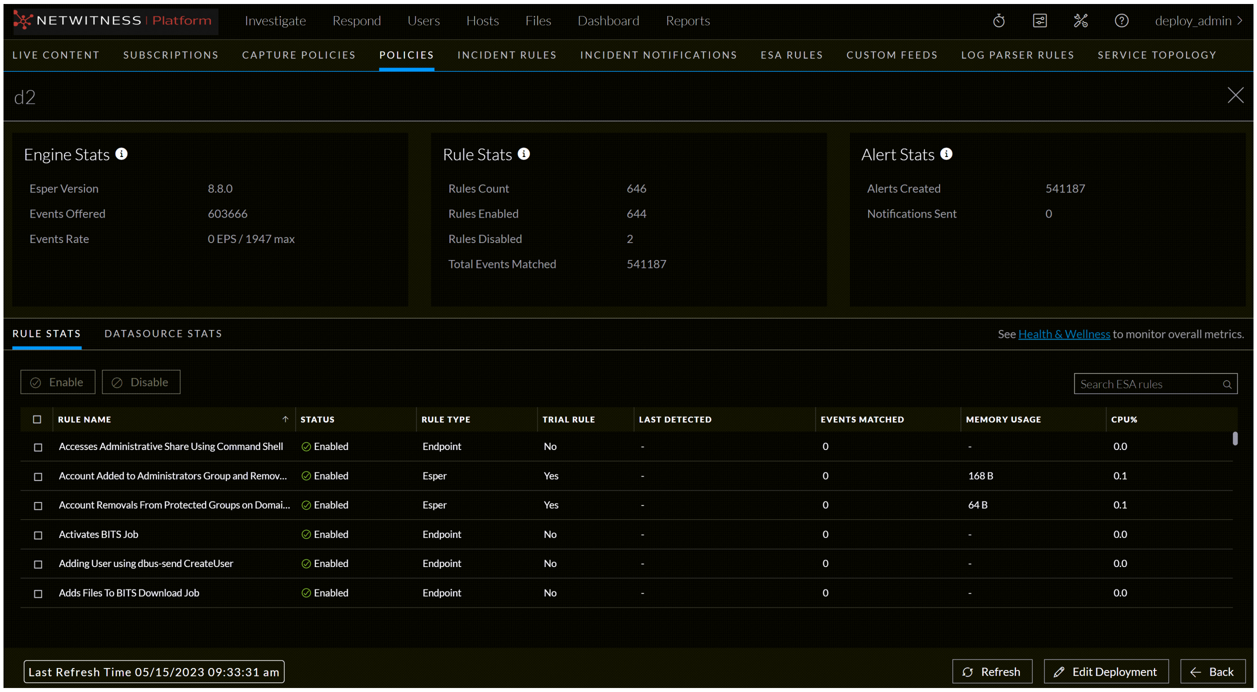
□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	UPDATES	LAST UPDATED
□	d1	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed ⚠	1 New Updates	05/15/2023 06:0...
☑	d2	policy2	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed ⚠	-	05/15/2023 06:0...
□	d3	policy	esa - ESA Correlat...	log-hybrid - Concentrator	New ⚠	-	05/15/2023 06:1...
□	d4	policy2	esa - ESA Correlat...	log-hybrid - Concentr... +1	Stopped ⚠	-	05/15/2023 06:1...

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 4 out of 4 items | 1 selected

The deployment stats for the selected service are displayed.



d2

Engine Stats

Esper Version	8.8.0
Events Offered	603666
Events Rate	0 EPS / 1947 max

Rule Stats

Rules Count	646
Rules Enabled	644
Rules Disabled	2
Total Events Matched	541187

Alert Stats

Alerts Created	541187
Notifications Sent	0

See Health & Wellness to monitor overall metrics.

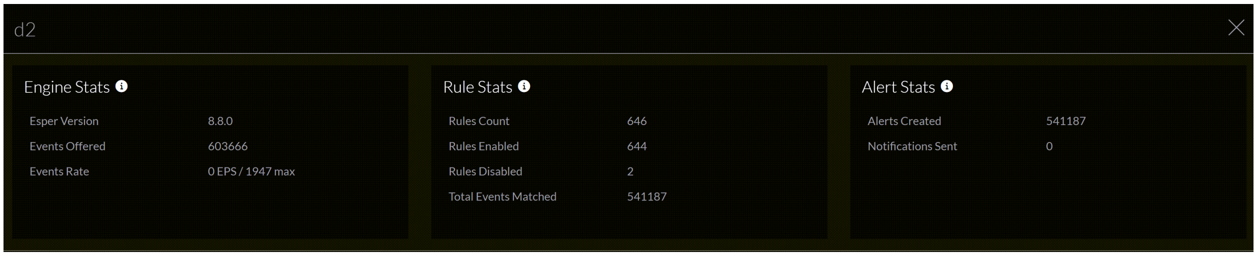
□	RULE NAME	STATUS	RULE TYPE	TRIAL RULE	LAST DETECTED	EVENTS MATCHED	MEMORY USAGE	CPU%
□	Accesses Administrative Share Using Command Shell	Enabled	Endpoint	No	-	0	-	0.0
□	Account Added to Administrators Group and Remov...	Enabled	Esper	Yes	-	0	168 B	0.1
□	Account Removals From Protected Groups on Domai...	Enabled	Esper	Yes	-	0	64 B	0.1
□	Activates BITS Job	Enabled	Endpoint	No	-	0	-	0.0
□	Adding User using dbus-send CreateUser	Enabled	Endpoint	No	-	0	-	0.0
□	Adds Files To BITS Download Job	Enabled	Endpoint	No	-	0	-	0.0

Last Refresh Time 05/15/2023 09:33:31 am

Review the following sections of selected Deployment Stats. For a complete description of each statistic in each section, see the Deployment Stats Information.

- **Engine Stats**
- **Rule Stats**
- **Alert Stats**

The following figure shows the Deployment Stats panel.



d2

Engine Stats

Esper Version	8.8.0
Events Offered	603666
Events Rate	0 EPS / 1947 max

Rule Stats

Rules Count	646
Rules Enabled	644
Rules Disabled	2
Total Events Matched	541187

Alert Stats

Alerts Created	541187
Notifications Sent	0

5. Review the list of details about the rules deployed on the ESA.

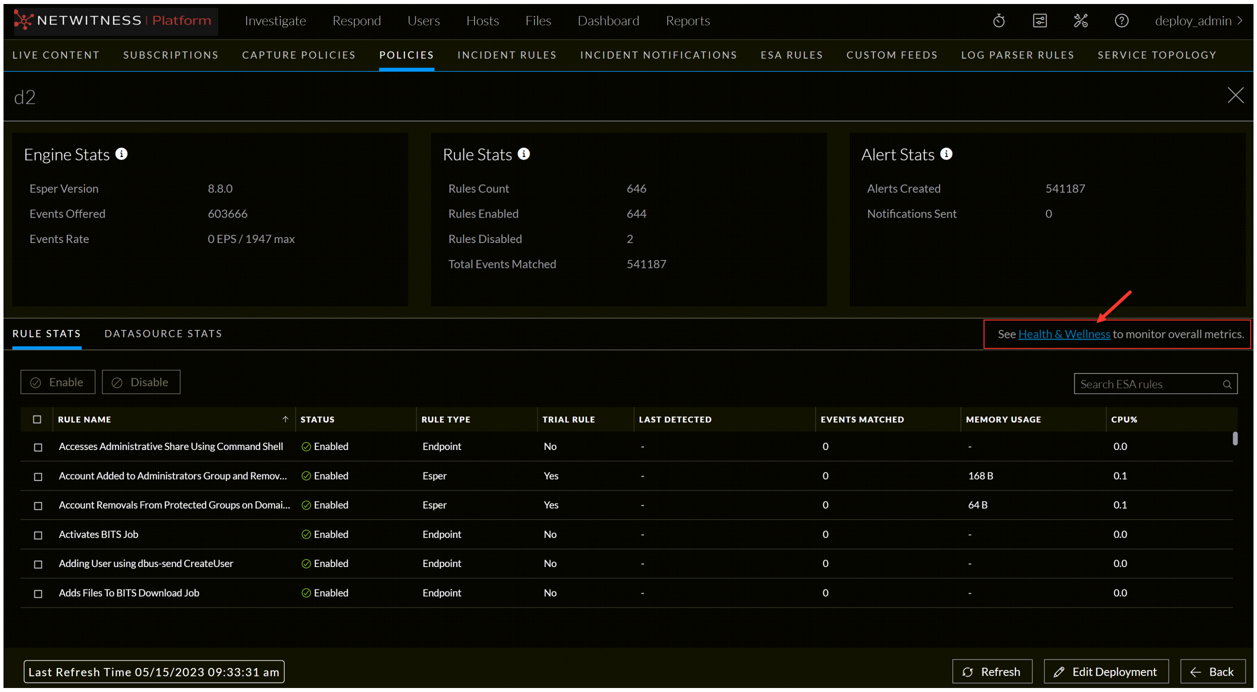
- If the rule is enabled or disabled
- Rule name
- Rule type
- Rule trial mode
- Last detected
- Events matched
- Rule memory usage

- Deployment CPU percentage used by the rule.

  For a complete description of each column in each section, see Deployment Stats Information.

Check Health and Wellness

To monitor your ESA Correlation service's overall memory usage and health, click **Health & Wellness**.



Engine Stats

Esper Version	8.8.0
Events Offered	603666
Events Rate	0 EPS / 1947 max

Rule Stats

Rules Count	646
Rules Enabled	644
Rules Disabled	2
Total Events Matched	541187

Alert Stats

Alerts Created	541187
Notifications Sent	0

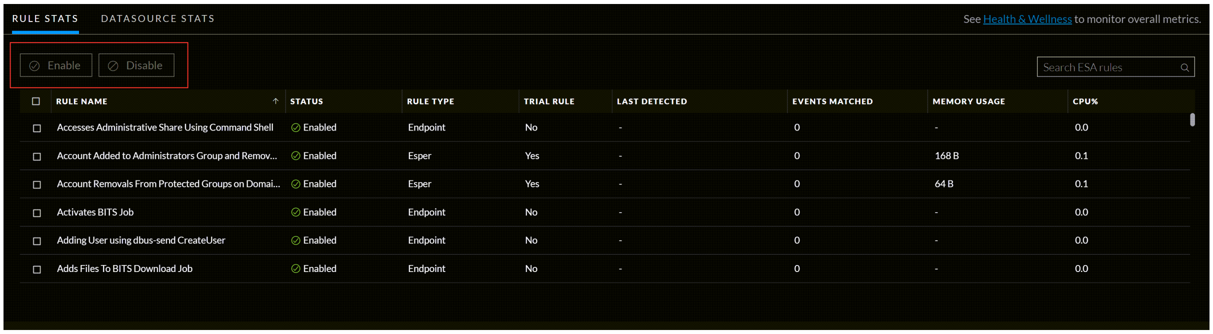
See Health & Wellness to monitor overall metrics.

□	RULE NAME	STATUS	RULE TYPE	TRIAL RULE	LAST DETECTED	EVENTS MATCHED	MEMORY USAGE	CPU%
□	Accesses Administrative Share Using Command Shell	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Account Added to Administrators Group and Remov...	✓ Enabled	Esper	Yes	-	0	168 B	0.1
□	Account Removals From Protected Groups on Domai...	✓ Enabled	Esper	Yes	-	0	64 B	0.1
□	Activates BITS Job	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adding User using dbus-send CreateUser	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adds Files To BITS Download Job	✓ Enabled	Endpoint	No	-	0	-	0.0

Last Refresh Time 05/15/2023 09:33:31 am

To Enable or Disable Rules

1. Select a rule from the **Rule Stats** panel grid.
2. Click **Enable** to enable the rule or click **Disable** to disable the rule.



See Health & Wellness to monitor overall metrics.

□	RULE NAME	STATUS	RULE TYPE	TRIAL RULE	LAST DETECTED	EVENTS MATCHED	MEMORY USAGE	CPU%
□	Accesses Administrative Share Using Command Shell	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Account Added to Administrators Group and Remov...	✓ Enabled	Esper	Yes	-	0	168 B	0.1
□	Account Removals From Protected Groups on Domai...	✓ Enabled	Esper	Yes	-	0	64 B	0.1
□	Activates BITS Job	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adding User using dbus-send CreateUser	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adds Files To BITS Download Job	✓ Enabled	Endpoint	No	-	0	-	0.0

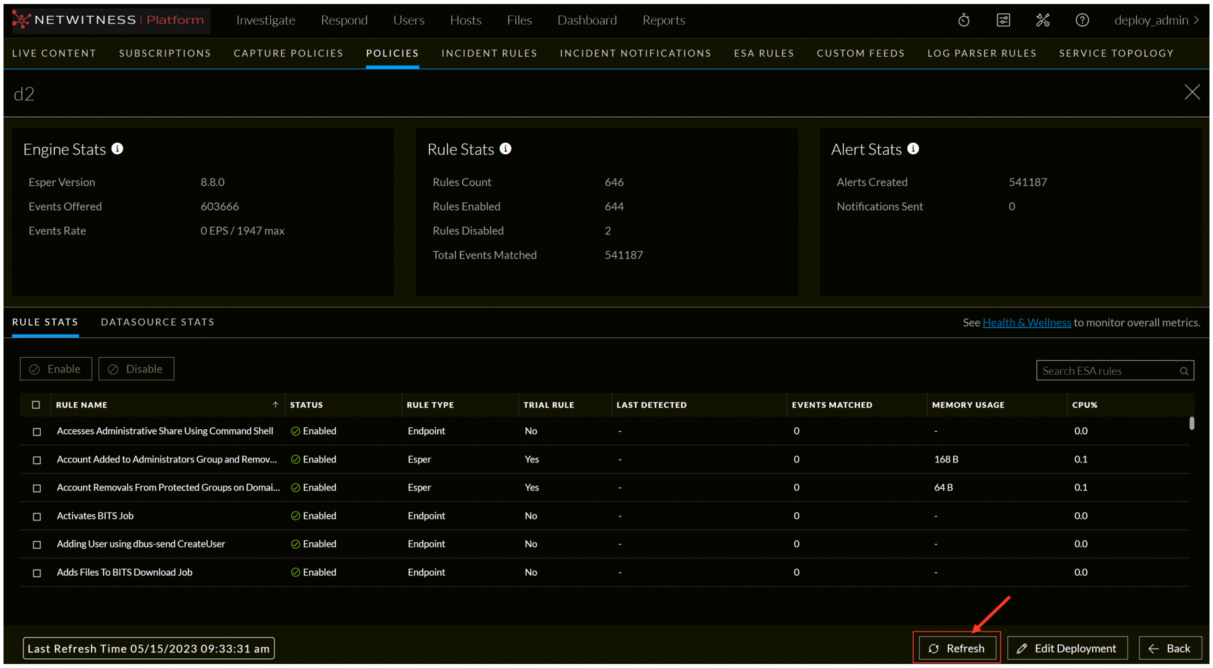
To Refresh the Statistics

The Services tab does not update statistics automatically unless you enable or disable a rule.

1. Click the **Refresh** tab in the bottom right corner to refresh the information.

   The Services tab is refreshed to show the changes which take effect immediately.

2. View the updated information.



Engine Stats

Esper Version	8.8.0
Events Offered	603666
Events Rate	0 EPS / 1947 max

Rule Stats

Rules Count	646
Rules Enabled	644
Rules Disabled	2
Total Events Matched	541187

Alert Stats

Alerts Created	541187
Notifications Sent	0

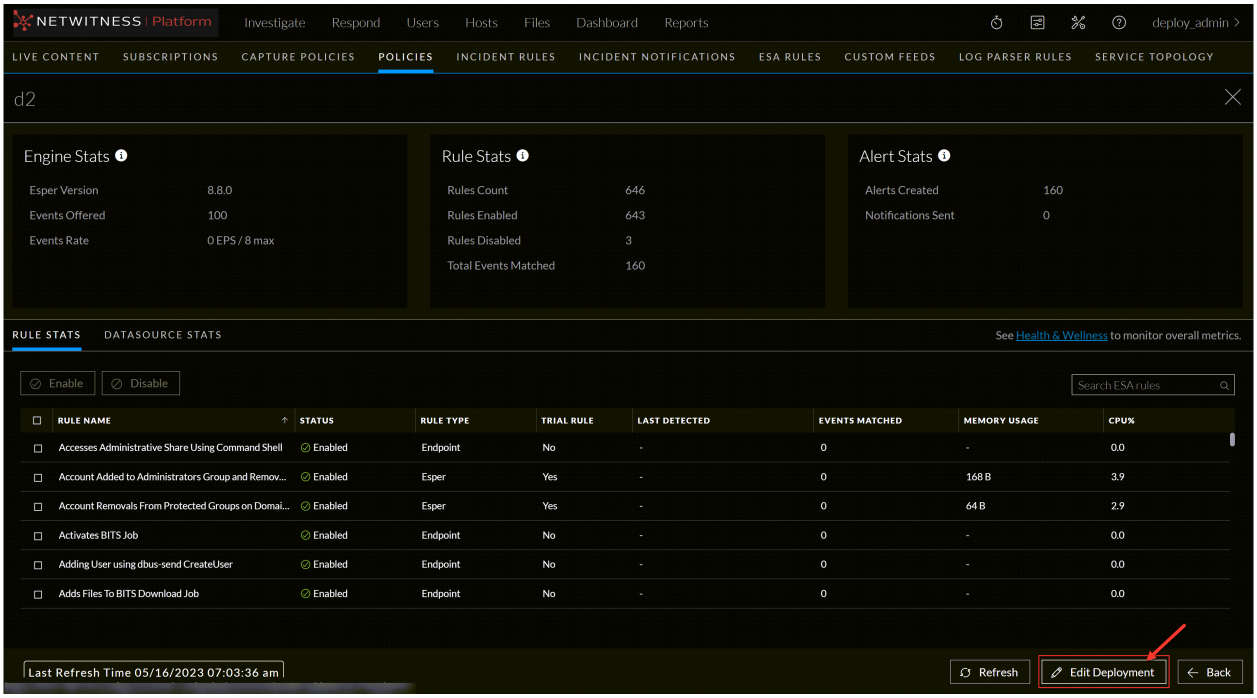
See Health & Wellness to monitor overall metrics.

□	RULE NAME	STATUS	RULE TYPE	TRIAL RULE	LAST DETECTED	EVENTS MATCHED	MEMORY USAGE	CPU%
□	Accesses Administrative Share Using Command Shell	Enabled	Endpoint	No	-	0	-	0.0
□	Account Added to Administrators Group and Remov...	Enabled	Esper	Yes	-	0	168 B	0.1
□	Account Removals From Protected Groups on Domai...	Enabled	Esper	Yes	-	0	64 B	0.1
□	Activates BITS Job	Enabled	Endpoint	No	-	0	-	0.0
□	Adding User using dbus-send CreateUser	Enabled	Endpoint	No	-	0	-	0.0
□	Adds Files To BITS Download Job	Enabled	Endpoint	No	-	0	-	0.0

Last Refresh Time 05/15/2023 09:33:31 am

Edit the Deployment

To edit the deployment, Click the **Edit Deployment** tab in the bottom right corner of the page.



Engine Stats

Esper Version	8.8.0
Events Offered	100
Events Rate	0 EPS / 8 max

Rule Stats

Rules Count	646
Rules Enabled	643
Rules Disabled	3
Total Events Matched	160

Alert Stats

Alerts Created	160
Notifications Sent	0

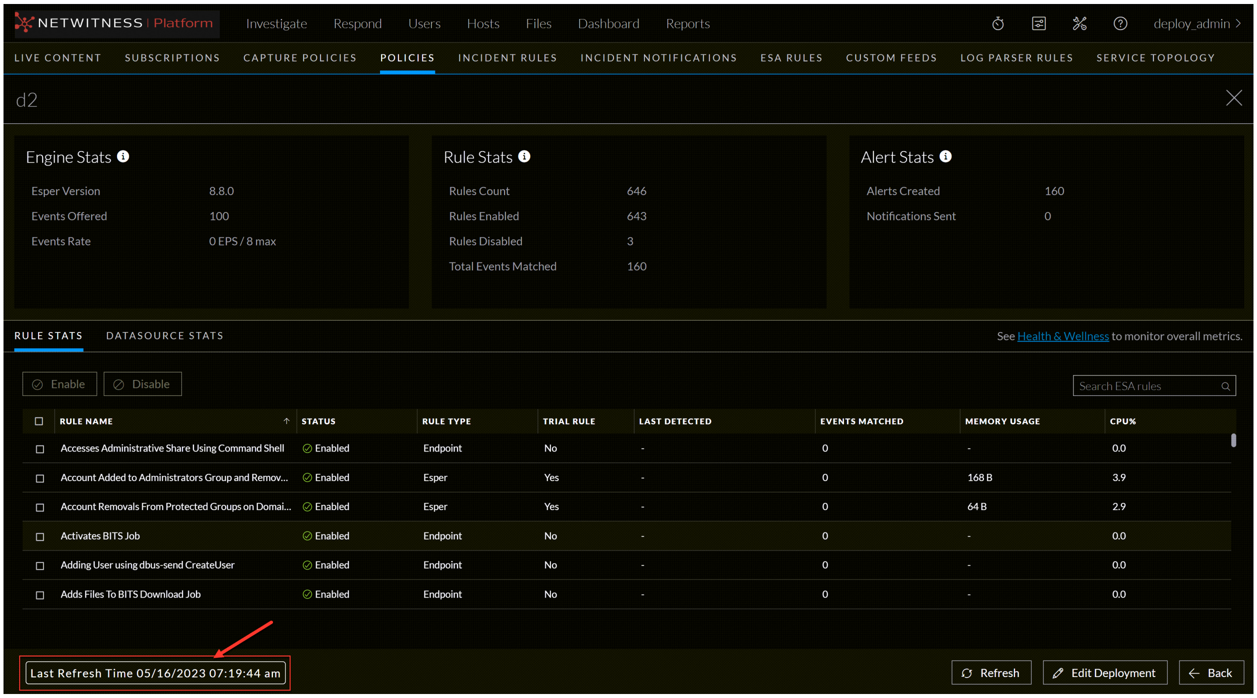
See Health & Wellness to monitor overall metrics.

□	RULE NAME	STATUS	RULE TYPE	TRIAL RULE	LAST DETECTED	EVENTS MATCHED	MEMORY USAGE	CPU%
□	Accesses Administrative Share Using Command Shell	Enabled	Endpoint	No	-	0	-	0.0
□	Account Added to Administrators Group and Remov...	Enabled	Esper	Yes	-	0	168 B	3.9
□	Account Removals From Protected Groups on Domai...	Enabled	Esper	Yes	-	0	64 B	2.9
□	Activates BITS Job	Enabled	Endpoint	No	-	0	-	0.0
□	Adding User using dbus-send CreateUser	Enabled	Endpoint	No	-	0	-	0.0
□	Adds Files To BITS Download Job	Enabled	Endpoint	No	-	0	-	0.0

Last Refresh Time 05/16/2023 07:03:36 am

Last Refresh Time

This information indicates the last time when the deployment stats page was refreshed.



Engine Stats

Esper Version	8.8.0
Events Offered	100
Events Rate	0 EPS / 8 max

Rule Stats

Rules Count	646
Rules Enabled	643
Rules Disabled	3
Total Events Matched	160

Alert Stats

Alerts Created	160
Notifications Sent	0

See Health & Wellness to monitor overall metrics.

□	RULE NAME	STATUS	RULE TYPE	TRIAL RULE	LAST DETECTED	EVENTS MATCHED	MEMORY USAGE	CPU%
□	Accesses Administrative Share Using Command Shell	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Account Added to Administrators Group and Remov...	✓ Enabled	Esper	Yes	-	0	168 B	3.9
□	Account Removals From Protected Groups on Domai...	✓ Enabled	Esper	Yes	-	0	64 B	2.9
□	Activates BITS Job	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adding User using dbus-send CreateUser	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adds Files To BITS Download Job	✓ Enabled	Endpoint	No	-	0	-	0.0

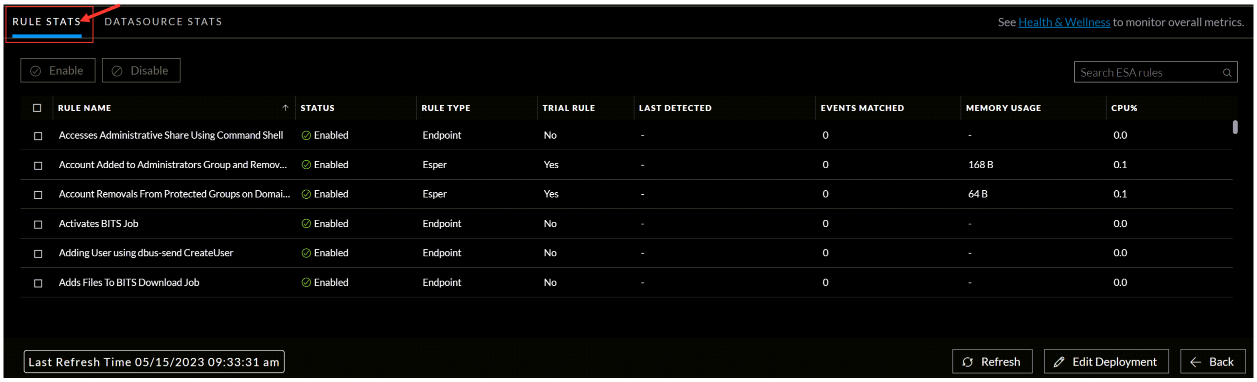
Last Refresh Time 05/16/2023 07:19:44 am

Sections	Parameter	Description
Engine Stats	Esper Version	Esper version running on the ESA service
	Events Offered	Number of events processed by the ESA service since the last service started.
	Events Rate	The rate that the ESA service processes current events / The maximum rate that the ESA service processed events.

Sections	Parameter	Description
Rule Stats	Rules Enabled	The number of rules enabled.
	Rules Disabled	The number of rules disabled.
	Rules Count	The number of rules inside a deployment.
	Total Events Matched	Total number of events matched to all rules on the ESA service.
Alert Stats	Notifications	The total number of notifications sent by email, SNMP, syslog, or script for the deployment. (ESA SNMP notifications are not supported in NetWitness Platform version 11.3 and later.)
	Alerts Created	The total number of alerts sent to Respond for the deployment.

The Rule Stats panel details:

The Rules Stats provides details on the rules that are deployed on the ESA service. The following figure shows the **Rule Stats** panel.



See Health & Wellness to monitor overall metrics.

□	RULE NAME	STATUS	RULE TYPE	TRIAL RULE	LAST DETECTED	EVENTS MATCHED	MEMORY USAGE	CPU%
□	Accesses Administrative Share Using Command Shell	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Account Added to Administrators Group and Remov...	✓ Enabled	Esper	Yes	-	0	168 B	0.1
□	Account Removals From Protected Groups on Domai...	✓ Enabled	Esper	Yes	-	0	64 B	0.1
□	Activates BITS Job	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adding User using dbus-send CreateUser	✓ Enabled	Endpoint	No	-	0	-	0.0
□	Adds Files To BITS Download Job	✓ Enabled	Endpoint	No	-	0	-	0.0

Last Refresh Time 05/15/2023 09:33:31 am

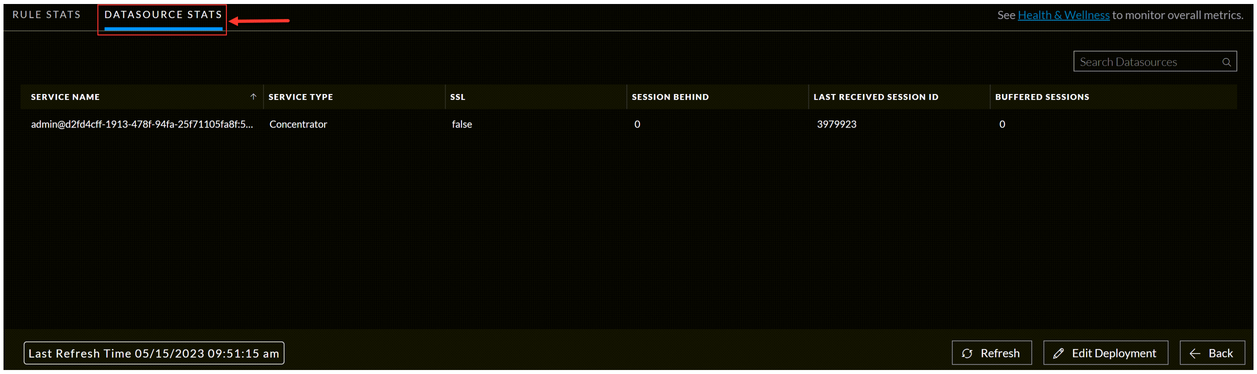
The table below lists the various parameters in the Rules Stats view and their description.

Parameters	Description
✓ Enabled	Enables a rule that was disabled.
⊘ Disabled	Disables a rule that was enabled.
Health & Wellness link	Enables you to monitor overall memory usage and health of your ESA Correlation service.
Status	Indicates whether the rule is enabled or disabled. A green circle icon ✓ Enabled indicates that the rule is enabled. A white circle icon ⊘ Disabled indicates that the rule is disabled. **Note:** If a rule has an error on deployment, it shows up as **'Failed'**. Hover over the Failed icon to view the error message in the tooltip.
Rule Name	Name of the ESA rule.

Parameters	Description
Rule Type	**Endpoint** indicates a rule from the Endpoint Risk Scoring Bundle and **Esper** indicates Esper-specific rules, such as Rule Builder and Advanced EPL rules.
Trial Rule	Indicates if the rule is running in trial rule mode.
Last Detected	The last time alert was triggered for the rule.
Events Matched	The total number of events that matched the rule.
Memory Usage	The total amount of memory used by the rule. **Note:** The Endpoint Risk Scoring Rules Bundle rules do not show memory usage.

Parameters	Description
CPU %	The percentage of the deployment CPU used by the rule. For example, a deployment with 1 rule shows 100% CPU usage for that rule and a deployment with two equally CPU heavy rules show 50% each. **Note:** The Endpoint Risk Scoring Rules Bundle rules do not show CPU usage.

The Data Source Stats panel details:



RULE STATS
DATASOURCE STATS
See Health & Wellness to monitor overall metrics.
Search Datasources
Last Refresh Time 05/15/2023 09:51:15 am
Refresh
Edit Deployment
Back

SERVICE NAME	SERVICE TYPE	SSL	SESSION BEHIND	LAST RECEIVED SESSION ID	BUFFERED SESSIONS
admin@d2fd4cff-1913-478f-94fa-25f71105fa8f:5...	Concentrator	false	0	3979923	0

Parameters	Description
Service Name	Identity of the service.
Service Type	Type of the service.

Parameters	Description
SSL	Data Source connected to ESA deployment over an SSL connection using SSL port (For example, for the concentrator, it is 56005).
Session Behind	Difference between the last latest session id on the concentrator and the currently processed session id on ESA.
Last Received Session ID	The latest session id received by the deployment from the data source.
Buffered Sessions	Number of sessions in the ESA buffer to be consumed by the Esper engine.

Remove a Deployment

You can delete one or more deployments when those deployments are not required. Once the deployment is deleted, all the configurations associated with the deployment will be permanently deleted from the correlation server. The alert process will be stopped for the deleted deployment.

You can remove deployments in the following ways:

- Using the **ESA Deployments** tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can remove deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and remove a deployment.

To remove a deployment from the ESA Deployments tab

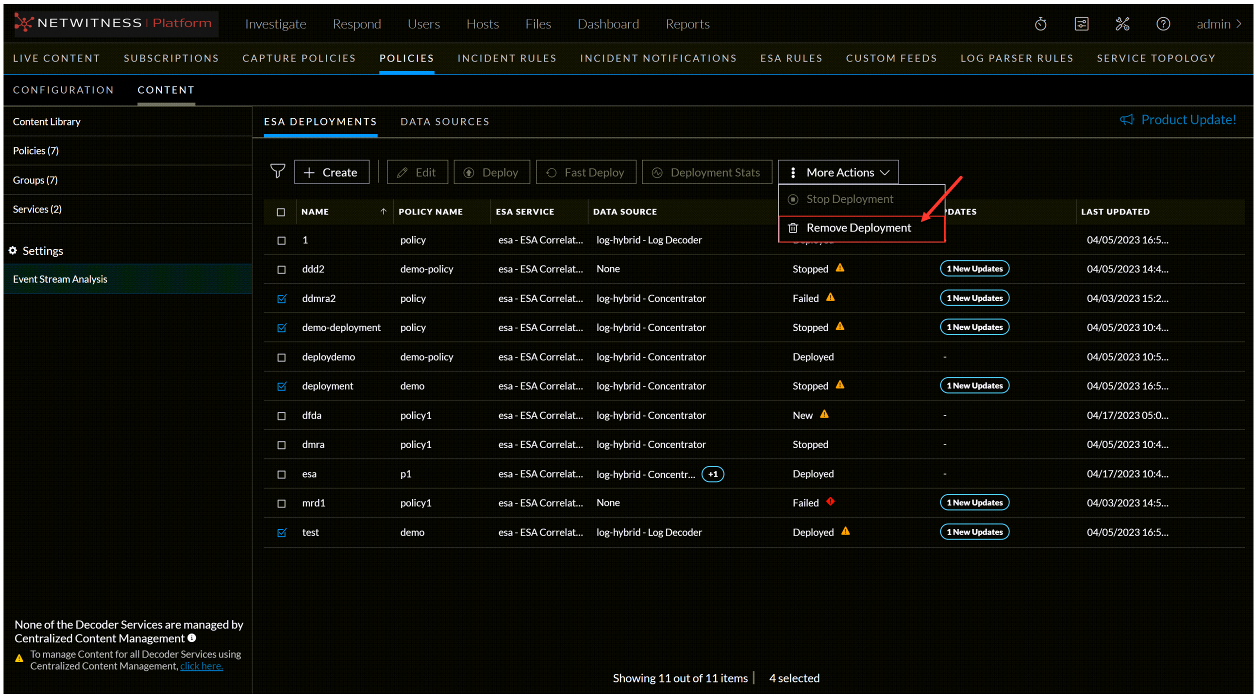
1. Go to ⚙ **(CONFIGURE)** > **Policies** > **Content**.
2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

The available deployments are displayed.

3. Select the deployment that needs to be removed and click **Remove**.

   A confirmation pop-up is displayed to confirm.

4. Click **Remove**.



☐	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE		DATES	LAST UPDATED
☐	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder			04/05/2023 16:5...
☐	ddd2	demo-policy	esa - ESA Correlat...	None	Stopped ⚠	1 New Updates	04/05/2023 14:4...
☑	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
☑	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
☐	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
☑	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 16:5...
☐	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	New ⚠	-	04/17/2023 05:0...
☐	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped	-	04/05/2023 10:4...
☐	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
☐	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
☑	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

None of the Decoder Services are managed by Centralized Content Management ℹ

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 11 out of 11 items | 4 selected

To remove a deployment from a selected policy

1. Go to ⚙ **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
   The available policies are displayed.
3. Click a Policy.

   The selected policy view is displayed and by default **Application Rule** is selected.

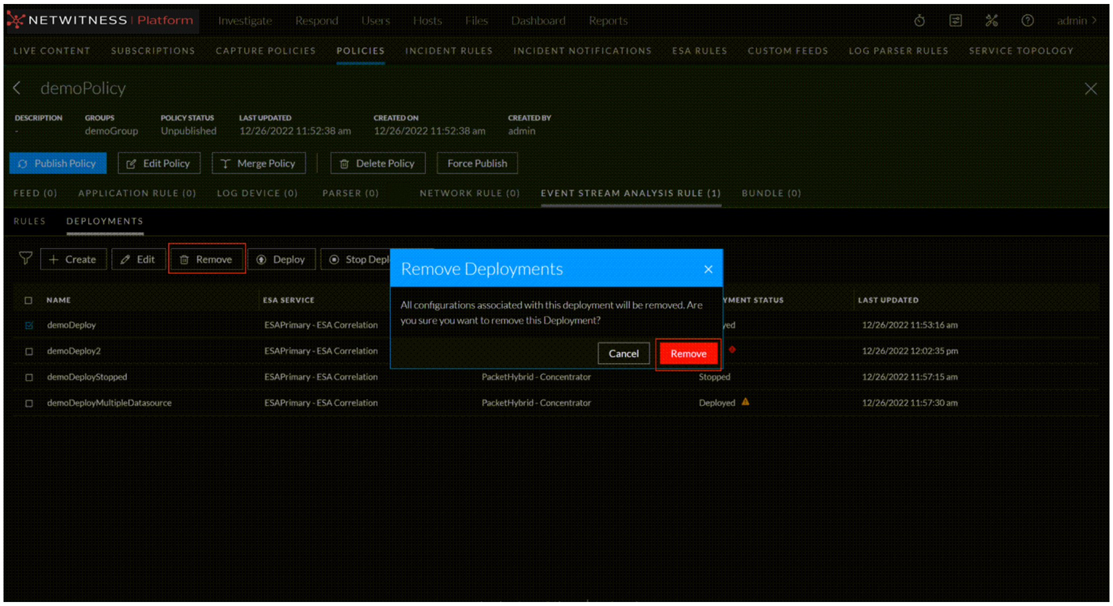
4. Click **Event Stream Analysis Rule** > **Deployments**.

   The available deployments for the selected policy are displayed.

5. Select the deployment that needs to be removed and click **Remove Deployment**.

   A confirmation pop-up is displayed to confirm if you want to remove it.

6. Click **Remove**.



DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	demoGroup	Unpublished	12/26/2022 11:52:38 am	12/26/2022 11:52:38 am	admin

☐	NAME	ESA SERVICE		YMENT STATUS	LAST UPDATED
☑	demoDeploy	ESAPrimary - ESA Correlation		yed	12/26/2022 11:53:16 am
☐	demoDeploy2	ESAPrimary - ESA Correlation		◆	12/26/2022 12:02:35 pm
☐	demoDeployStopped	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Stopped	12/26/2022 11:57:15 am
☐	demoDeployMultipleDatasource	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed ⚠	12/26/2022 11:57:30 am

Remove Deployments

All configurations associated with this deployment will be removed. Are you sure you want to remove this Deployment?

Note: It is required to have at least one deployment associated with the correlation service present in the group associated with the policy.

Stop a Deployment

You can stop a deployment to temporarily pause an ESA deployment. This will stop processing the event stream analysis alerts corresponding to the deployed policy.

To delete a deployment completely, see Remove a Deployment

To initiate a deployment again, see Start a Deployment

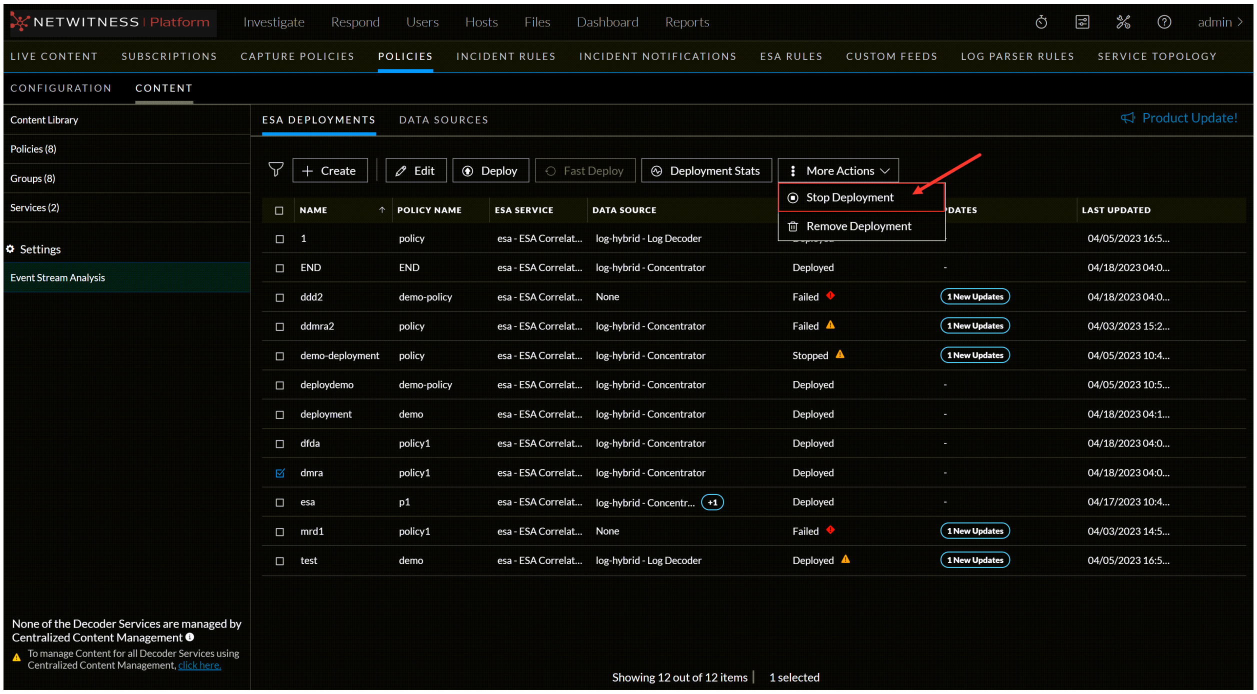
You can stop deployments in the following ways:

- Using the ESA Deployments tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can stop deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and stop a deployment.

To stop a deployment from the ESA Deployments tab

1. Go to **(CONFIGURE)** > **Policies** > **Content**.
2. Under **Settings**, click **Event Stream Analysis** > **ESA Deployments**.

   The available deployments are displayed.
3. Select the deployment that must be stopped temporarily and click **Stop Deployment**.



□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE		DATES	LAST UPDATED
□	1	policy	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed		04/05/2023 16:5...
□	END	END	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
□	ddd2	demo-policy	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/18/2023 04:0...
□	ddmra2	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Failed ⚠	1 New Updates	04/03/2023 15:2...
□	demo-deployment	policy	esa - ESA Correlat...	log-hybrid - Concentrator	Stopped ⚠	1 New Updates	04/05/2023 10:4...
□	deploydemo	demo-policy	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/05/2023 10:5...
□	deployment	demo	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:1...
□	dfda	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
☑	dmra	policy1	esa - ESA Correlat...	log-hybrid - Concentrator	Deployed	-	04/18/2023 04:0...
□	esa	p1	esa - ESA Correlat...	log-hybrid - Concentr... +1	Deployed	-	04/17/2023 10:4...
□	mrd1	policy1	esa - ESA Correlat...	None	Failed ◆	1 New Updates	04/03/2023 14:5...
□	test	demo	esa - ESA Correlat...	log-hybrid - Log Decoder	Deployed ⚠	1 New Updates	04/05/2023 16:5...

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 12 out of 12 items | 1 selected

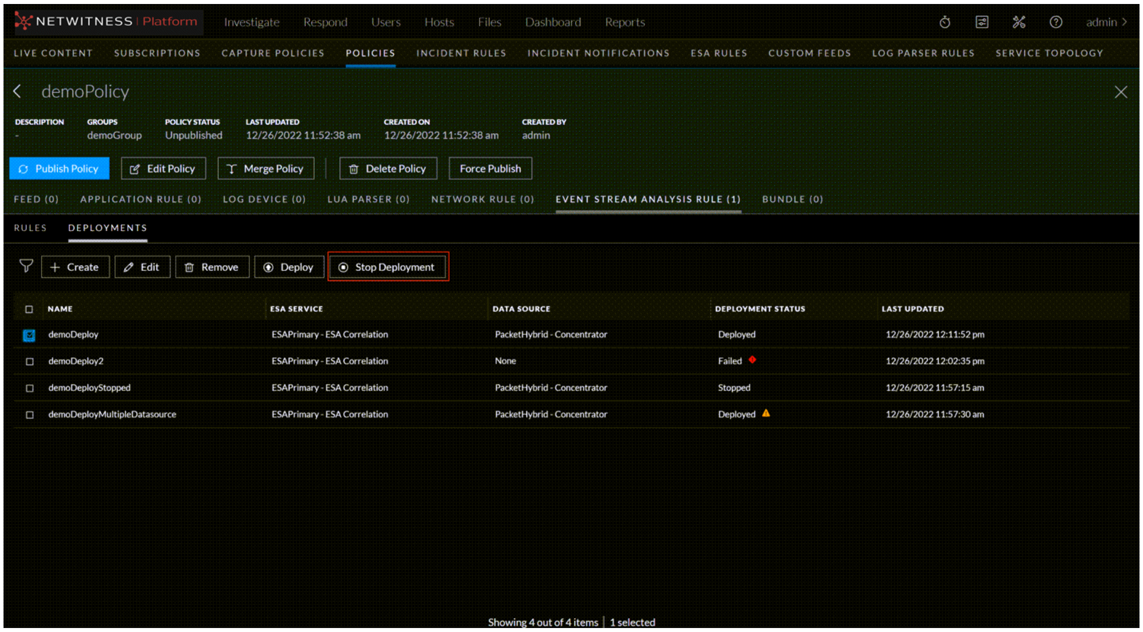
To stop a deployment from a selected policy

1. Go to (CONFIGURE) > **Policies**.
2. In the policies panel, click **Content**.
   The available policies are displayed
3. Click a Policy.

   The selected policy view is displayed and by default **Application Rule** is selected.
4. Click **Event Stream Analysis Rule** > **Deployments**.

   The available deployments for the selected policy are displayed.
5. Select the deployment that needs to be stopped temporally and click **Stop Deployment**.

Note: Publishing the policy will not deploy the stopped deployments.



demoPolicy

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	demoGroup	Unpublished	12/26/2022 11:52:38 am	12/26/2022 11:52:38 am	admin

☐	NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
☑	demoDeploy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed	12/26/2022 12:11:52 pm
☐	demoDeploy2	ESAPrimary - ESA Correlation	None	Failed ◆	12/26/2022 12:02:35 pm
☐	demoDeployStopped	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Stopped	12/26/2022 11:57:15 am
☐	demoDeployMultipleDatasource	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed ⚠	12/26/2022 11:57:30 am

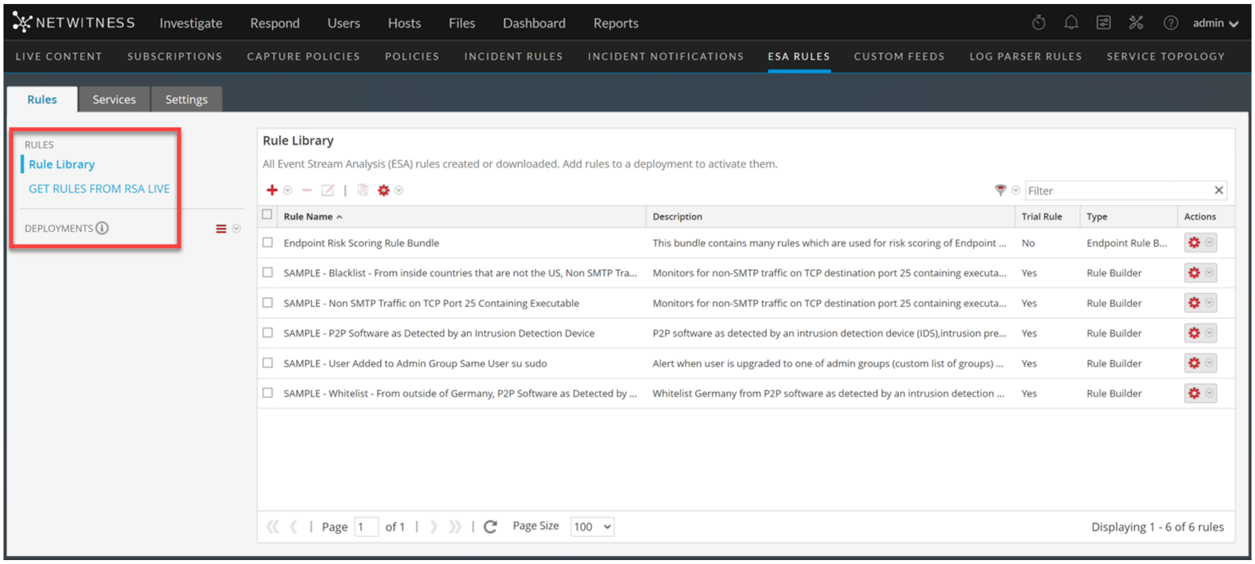
Showing 4 out of 4 items | 1 selected

Migrate ESA Deployments to Policies and Groups

From version 12.1 and later, on successful upgrade of the Admin Server, the ESA deployments are managed by the policies and groups page. The deployments are not available on **(CONFIGURE)** > **ESA Rules** page.

12.0 and Earlier version

ESA Rules page in the 12.0 version.



Rule Library

All Event Stream Analysis (ESA) rules created or downloaded. Add rules to a deployment to activate them.

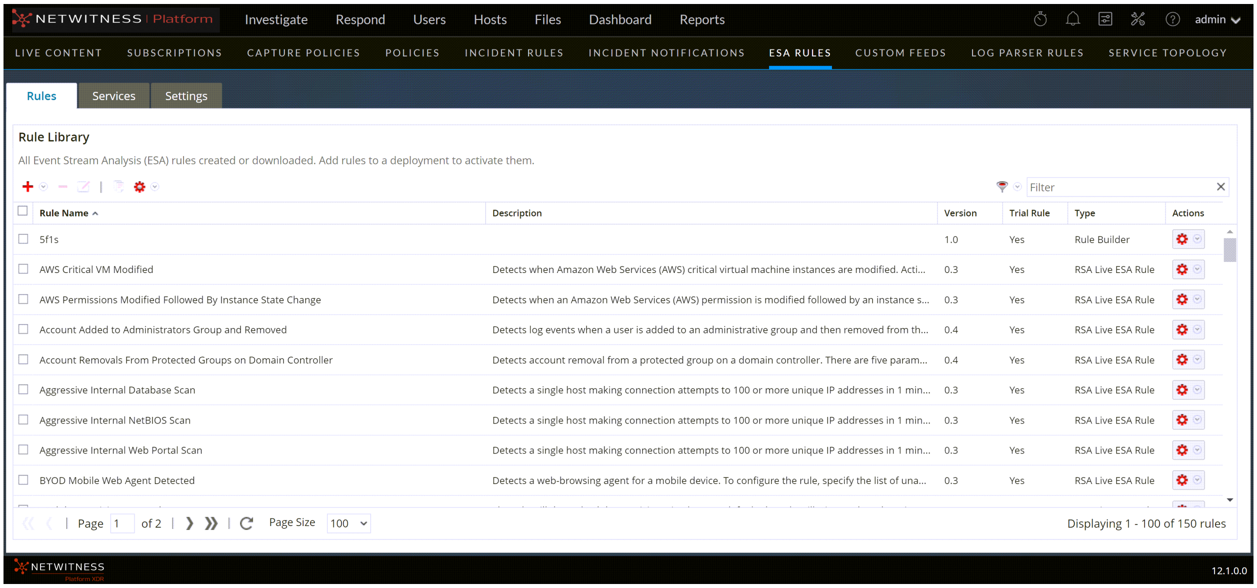
☐	Rule Name	Description	Trial Rule	Type	Actions
☐	Endpoint Risk Scoring Rule Bundle	This bundle contains many rules which are used for risk scoring of Endpoint ...	No	Endpoint Rule B...	
☐	SAMPLE - Blacklist - From inside countries that are not the US, Non SMTP Tra...	Monitors for non-SMTP traffic on TCP destination port 25 containing executa...	Yes	Rule Builder	
☐	SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Executable	Monitors for non-SMTP traffic on TCP destination port 25 containing executa...	Yes	Rule Builder	
☐	SAMPLE - P2P Software as Detected by an Intrusion Detection Device	P2P software as detected by an intrusion detection device (IDS),intrusion pre...	Yes	Rule Builder	
☐	SAMPLE - User Added to Admin Group Same User su sudo	Alert when user is upgraded to one of admin groups (custom list of groups) ...	Yes	Rule Builder	
☐	SAMPLE - Whitelist - From outside of Germany, P2P Software as Detected by ...	Whitelist Germany from P2P software as detected by an intrusion detection ...	Yes	Rule Builder	

Page 1 of 1 | Page Size 100 | Displaying 1 - 6 of 6 rules

12.1 version

Updated ESA Rules page in 12.1 version, where only rule libraries are available.

Note: The ESA deployments, after upgrading the Admin Server to 12.1 are not available to view or modify until the Correlation servers are also upgraded to the 12.1 version. However, the events are consumed, and ESA alerts are processed by the Correlation server.



Rule Library

All Event Stream Analysis (ESA) rules created or downloaded. Add rules to a deployment to activate them.

Rule Name	Description	Version	Trial Rule	Type	Actions
5f1s		1.0	Yes	Rule Builder	
AWS Critical VM Modified	Detects when Amazon Web Services (AWS) critical virtual machine instances are modified. Acti...	0.3	Yes	RSA Live ESA Rule	
AWS Permissions Modified Followed By Instance State Change	Detects when an Amazon Web Services (AWS) permission is modified followed by an instance s...	0.3	Yes	RSA Live ESA Rule	
Account Added to Administrators Group and Removed	Detects log events when a user is added to an administrative group and then removed from th...	0.4	Yes	RSA Live ESA Rule	
Account Removals From Protected Groups on Domain Controller	Detects account removal from a protected group on a domain controller. There are five param...	0.4	Yes	RSA Live ESA Rule	
Aggressive Internal Database Scan	Detects a single host making connection attempts to 100 or more unique IP addresses in 1 min...	0.3	Yes	RSA Live ESA Rule	
Aggressive Internal NetBIOS Scan	Detects a single host making connection attempts to 100 or more unique IP addresses in 1 min...	0.3	Yes	RSA Live ESA Rule	
Aggressive Internal Web Portal Scan	Detects a single host making connection attempts to 100 or more unique IP addresses in 1 min...	0.3	Yes	RSA Live ESA Rule	
BYOD Mobile Web Agent Detected	Detects a web-browsing agent for a mobile device. To configure the rule, specify the list of una...	0.3	Yes	RSA Live ESA Rule	

Page 1 of 2 | Page Size 100 | Displaying 1 - 100 of 150 rules

All the deployments are automatically migrated to policies and groups:

- Each deployment is converted into a policy and a group.
- Once the ESA Correlation server is upgraded to the 12.1 version, you can access these deployments as groups and policies.

IMPORTANT: If there is any need to import ESA Rules and Enrichments. NetWitness recommends importing those missing rules and enrichments before the upgrade.

The following table provides the information on different deployment states for Policy and Groups:

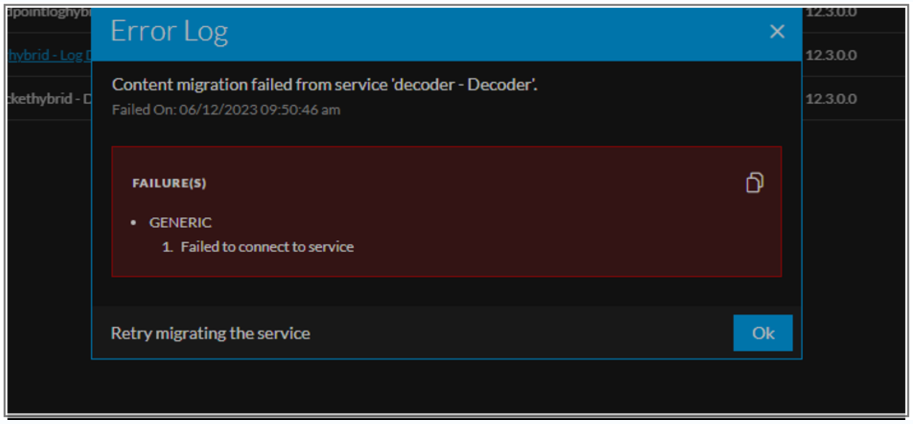
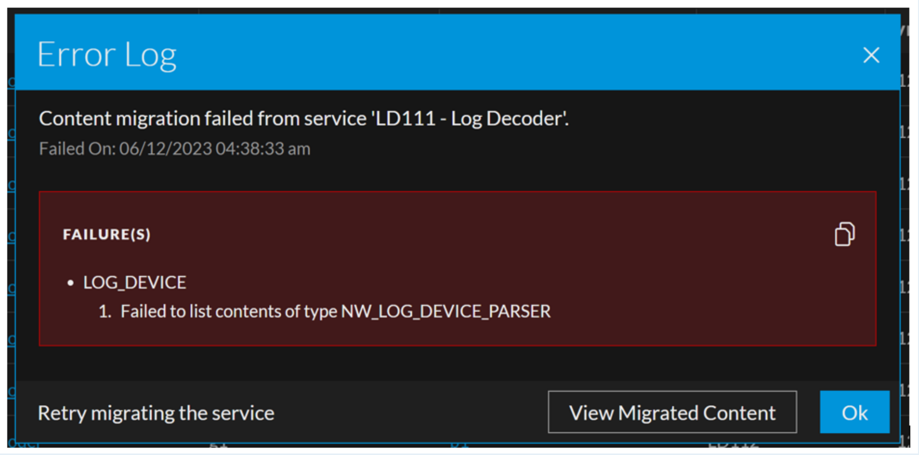
SlNo	Pre-upgrade Deployment State	Post-upgrade Deployment State		
		Creates Policy	Creates Group	The policy will be Published
1	Healthy deployment	Yes	Yes	Yes
2	Deployment with errors	Yes	Yes	Yes
3	Deployment with only rules	Yes	No	No
4	Deployment with no rules	No	No	No

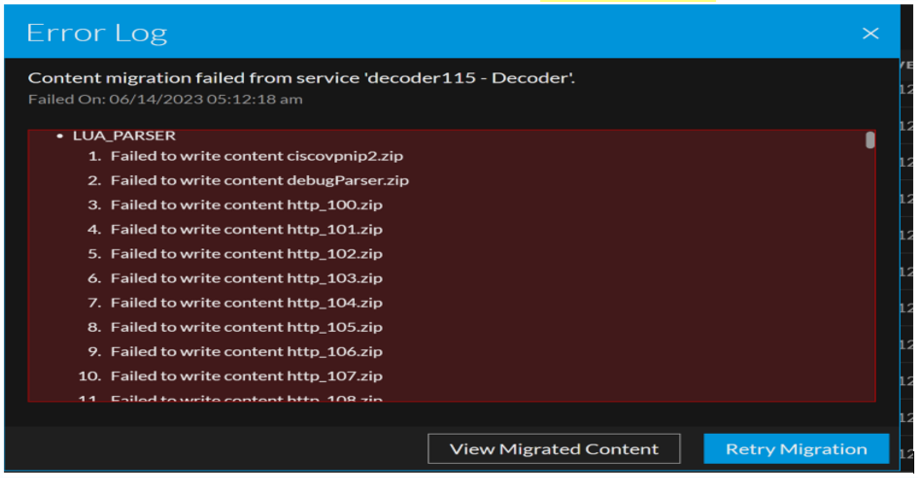
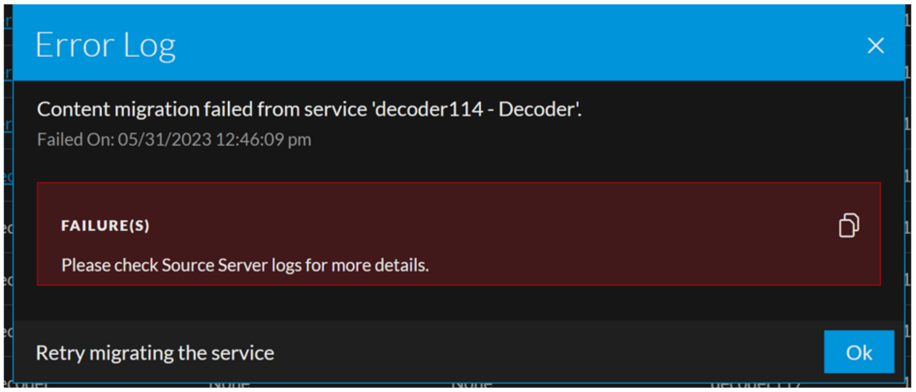
Healthy deployment contains no errors, and the required resources such as ESA Server, Data source, and ESA rule are added.

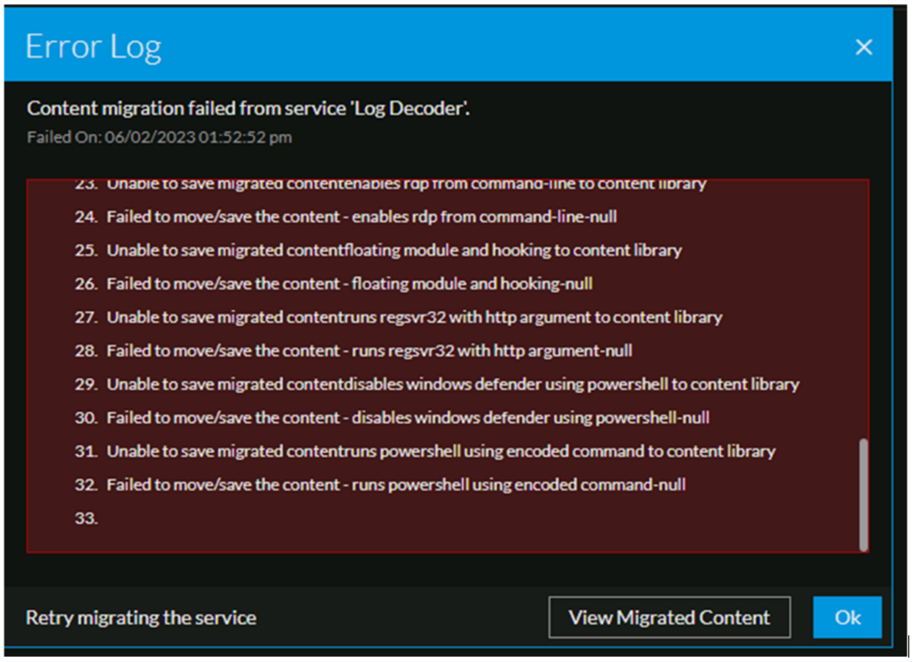
Note: NetWitness recommends that all the deployments maintain an error-free state and also remove any unnecessary or unused ESA deployments.

Troubleshooting

This topic provides information about possible issues that NetWitness users may encounter when using Centralized Content Management (CCM) in NetWitness. You can look up explanations of issues and their solutions.

Problem	Solution
Failed to connect to service	Generally this error occurs when service is offline. If the service status is offline, then restart service and retry migration. If the service status is online, then retry migration.  Error Log Content migration failed from service 'decoder - Decoder'. Failed On: 06/12/2023 09:50:46 am FAILURE(S) • GENERIC 1. Failed to connect to service Retry migrating the service
Failed to list content of type LOG_DEVICE_ PARSER	This is a temporary failure. Retrying migration resolves this issue.  Error Log Content migration failed from service 'LD111 - Log Decoder'. Failed On: 06/12/2023 04:38:33 am FAILURE(S) • LOG_DEVICE 1. Failed to list contents of type NW_LOG_DEVICE_PARSER Retry migrating the service

Problem	Solution
Failed to write content	This is a temporary failure. Retrying migration resolves this issue.  Error Log Content migration failed from service 'decoder115 - Decoder'. Failed On: 06/14/2023 05:12:18 am - LUA_PARSER 1. Failed to write content ciscovpnip2.zip 2. Failed to write content debugParser.zip 3. Failed to write content http_100.zip 4. Failed to write content http_101.zip 5. Failed to write content http_102.zip 6. Failed to write content http_103.zip 7. Failed to write content http_104.zip 8. Failed to write content http_105.zip 9. Failed to write content http_106.zip 10. Failed to write content http_107.zip 11. Failed to write content http_108.zip
Please check source server logs for more details.	This error occurs when source server goes offline during migration. Hence, restart source server and retry migration.  Error Log Content migration failed from service 'decoder114 - Decoder'. Failed On: 05/31/2023 12:46:09 pm FAILURE(S) Please check Source Server logs for more details. Retry migrating the service

Problem	Solution
Failed to move/save the content	This error may occur for various reasons and needs more investigation. Hence, please raise a CE ticket and share mongo dump and source server log with ticket.  Content migration failed from service 'Log Decoder'. Failed On: 06/02/2023 01:52:52 pm 23. Unable to save migrated contentenables rdp from command-line to content library 24. Failed to move/save the content - enables rdp from command-line-null 25. Unable to save migrated contentfloating module and hooking to content library 26. Failed to move/save the content - floating module and hooking-null 27. Unable to save migrated contentruns regsvr32 with http argument to content library 28. Failed to move/save the content - runs regsvr32 with http argument-null 29. Unable to save migrated contentdisables windows defender using powershell to content library 30. Failed to move/save the content - disables windows defender using powershell-null 31. Unable to save migrated contentruns powershell using encoded command to content library 32. Failed to move/save the content - runs powershell using encoded command-null 33.

References

This section is a collection of references, which describe the user interface and more detailed information about how Policy-based Centralized Content Management works in NetWitness. The topics are presented in alphabetical order.

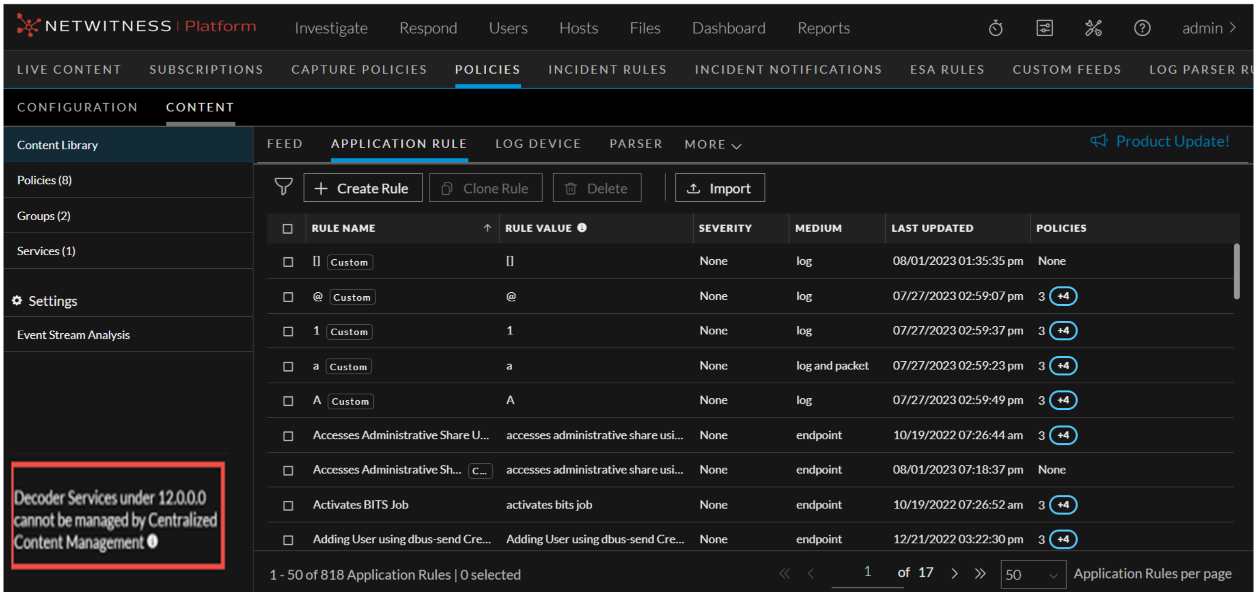
- Content Library Tab
- Data Sources Tab
- Deployments Tab
- Groups Tab
- Policies Tab
- Services Tab

Content Library Tab

The (CONFIGURE) > **Policies** view contains two tabs: **Configuration** and **Content**.

The **CONTENT** tab has **Content Library**, **Policies**, **Groups** and **Services** on the left panel.

Below is an example of the Content > Content Library tab:

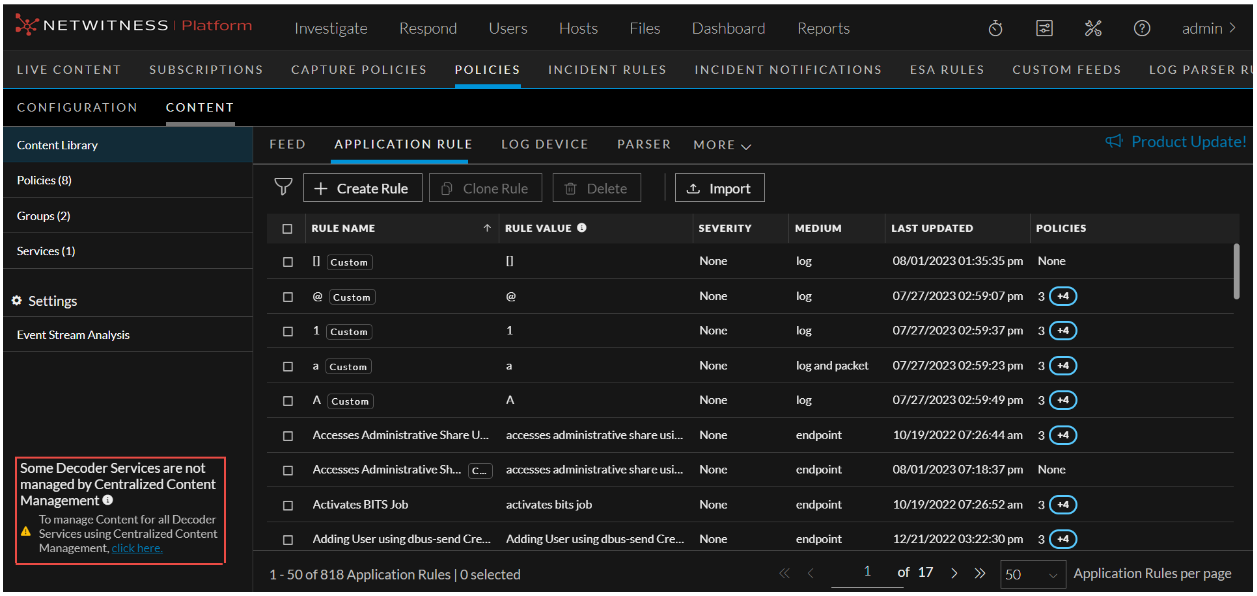


Decoder Services under 12.0.0.0 cannot be managed by Centralized Content Management

☐	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
☐	[] Custom	[]	None	log	08/01/2023 01:35:35 pm	None
☐	@ Custom	@	None	log	07/27/2023 02:59:07 pm	3 +4
☐	1 Custom	1	None	log	07/27/2023 02:59:37 pm	3 +4
☐	a Custom	a	None	log and packet	07/27/2023 02:59:23 pm	3 +4
☐	A Custom	A	None	log	07/27/2023 02:59:49 pm	3 +4
☐	Accesses Administrative Share U...	accesses administrative share usi...	None	endpoint	10/19/2022 07:26:44 am	3 +4
☐	Accesses Administrative Sh... C...	accesses administrative share usi...	None	endpoint	08/01/2023 07:18:37 pm	None
☐	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
☐	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

1 - 50 of 818 Application Rules | 0 selected

1 of 17 50 Application Rules per page

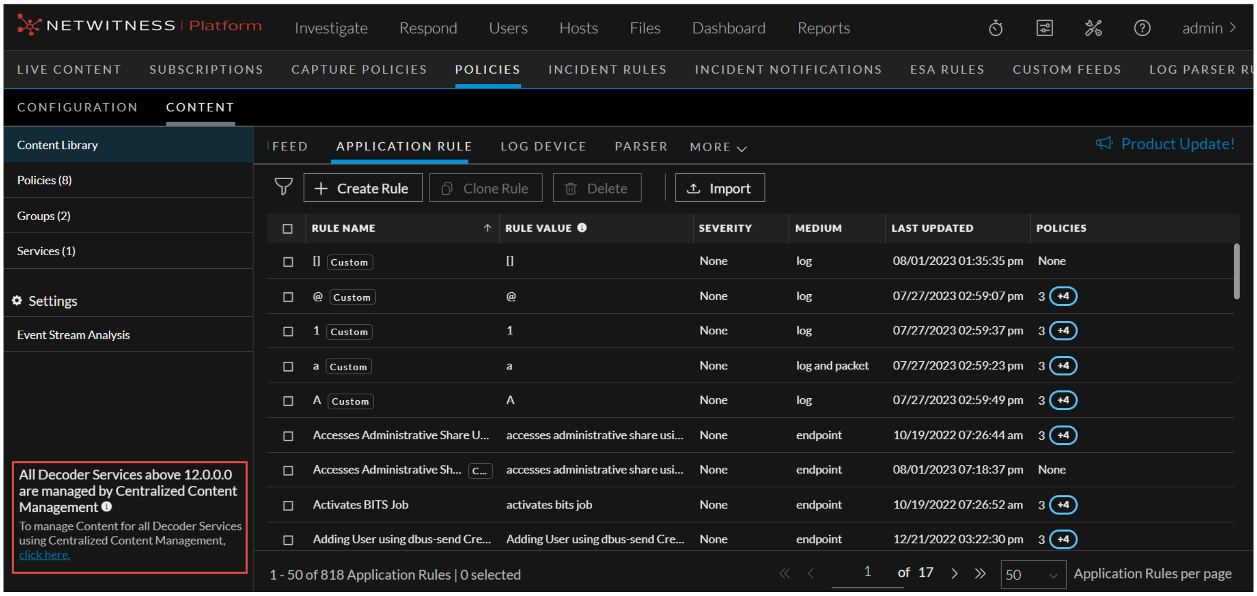


□	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
□	[] Custom	[]	None	log	08/01/2023 01:35:35 pm	None
□	@ Custom	@	None	log	07/27/2023 02:59:07 pm	3 +4
□	1 Custom	1	None	log	07/27/2023 02:59:37 pm	3 +4
□	a Custom	a	None	log and packet	07/27/2023 02:59:23 pm	3 +4
□	A Custom	A	None	log	07/27/2023 02:59:49 pm	3 +4
□	Accesses Administrative Share U...	accesses administrative share usi...	None	endpoint	10/19/2022 07:26:44 am	3 +4
□	Accesses Administrative Sh... C...	accesses administrative share usi...	None	endpoint	08/01/2023 07:18:37 pm	None
□	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
□	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

1 - 50 of 818 Application Rules | 0 selected   1 of 17   50   Application Rules per page

Some Decoder Services are not managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

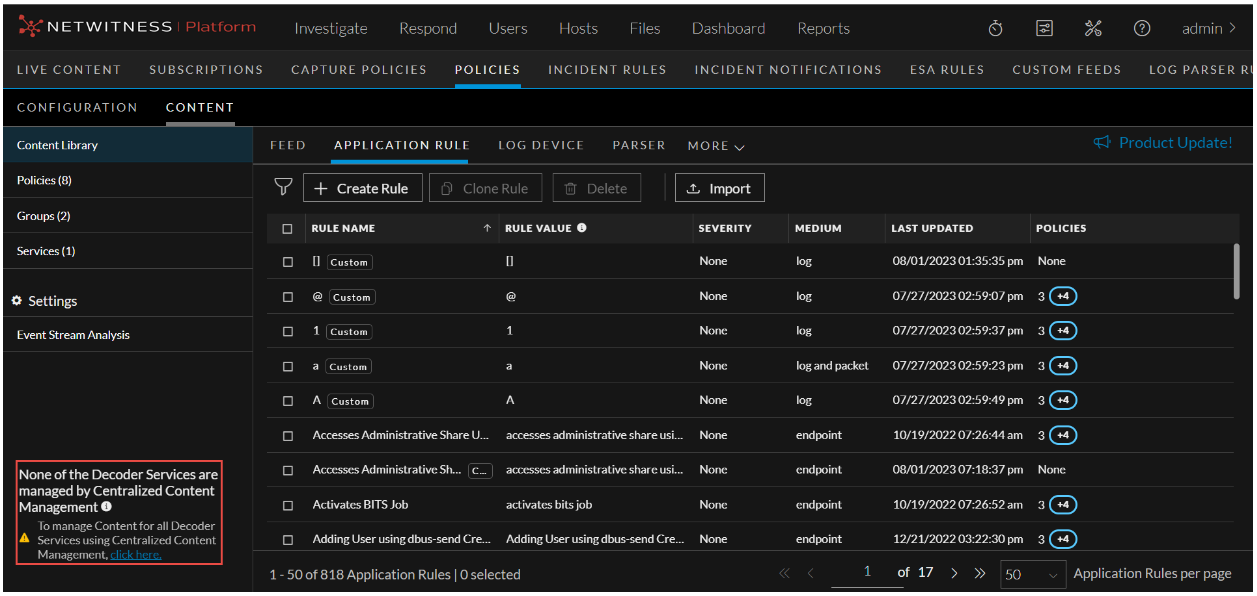


□	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
□	[] Custom	[]	None	log	08/01/2023 01:35:35 pm	None
□	@ Custom	@	None	log	07/27/2023 02:59:07 pm	3 +4
□	1 Custom	1	None	log	07/27/2023 02:59:37 pm	3 +4
□	a Custom	a	None	log and packet	07/27/2023 02:59:23 pm	3 +4
□	A Custom	A	None	log	07/27/2023 02:59:49 pm	3 +4
□	Accesses Administrative Share U...	accesses administrative share usi...	None	endpoint	10/19/2022 07:26:44 am	3 +4
□	Accesses Administrative Sh... C...	accesses administrative share usi...	None	endpoint	08/01/2023 07:18:37 pm	None
□	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
□	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

1 - 50 of 818 Application Rules | 0 selected   1 of 17   50   Application Rules per page

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.



None of the Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

□	RULE NAME	RULE VALUE	SEVERITY	MEDIUM	LAST UPDATED	POLICIES
□	[] Custom	[]	None	log	08/01/2023 01:35:35 pm	None
□	@ Custom	@	None	log	07/27/2023 02:59:07 pm	3 +4
□	1 Custom	1	None	log	07/27/2023 02:59:37 pm	3 +4
□	a Custom	a	None	log and packet	07/27/2023 02:59:23 pm	3 +4
□	A Custom	A	None	log	07/27/2023 02:59:49 pm	3 +4
□	Accesses Administrative Share U...	accesses administrative share usi...	None	endpoint	10/19/2022 07:26:44 am	3 +4
□	Accesses Administrative Sh... C...	accesses administrative share usi...	None	endpoint	08/01/2023 07:18:37 pm	None
□	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
□	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

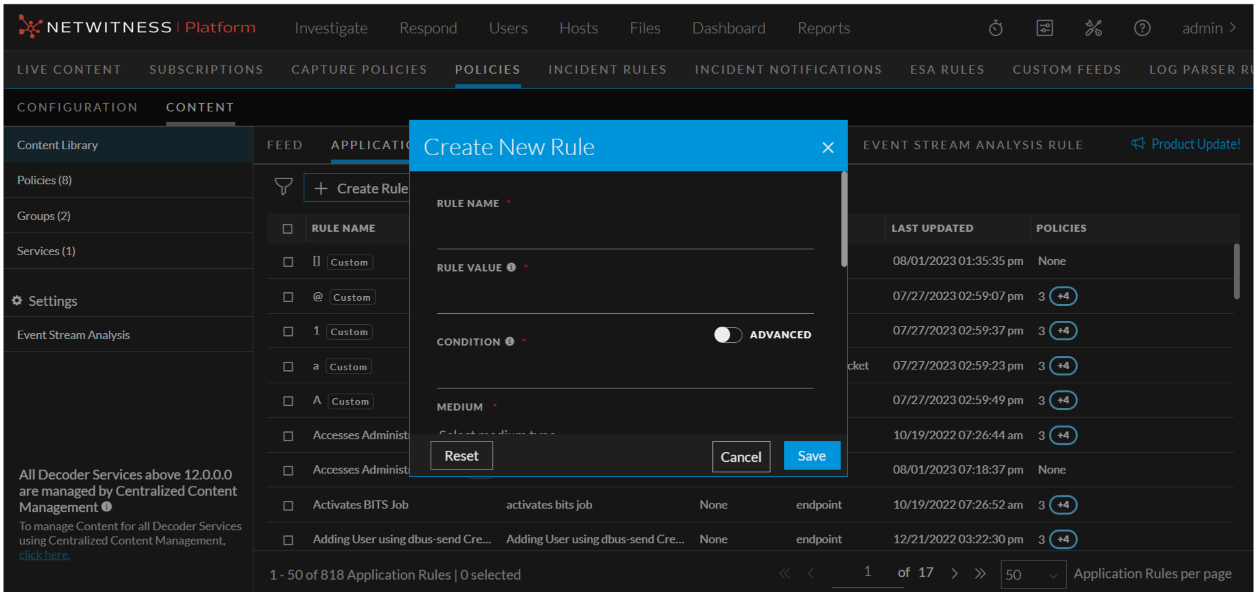
1 - 50 of 818 Application Rules | 0 selected   « ‹ 1 of 17 › » 50 Application Rules per page

The following table describes the Content Library tab:

1	By default, 50 contents are displayed per page. To go to the next page, click ›. To go to the last page, click ».
2	Toolbar - Create Rule - Lets you create a rule. - Clone Rule - Lets you clone an application rule or network rule. For more information, see Clone Application Rule or Clone Network Rule. - Delete - Lets you delete an application rule or network rule. For more information, see Delete Application Rule or Delete Network Rule. - Import - Lets you import an application rule or network rule. For more information, see Import Content to Content Library.
3	Rule List Pane - Rule Name - Name of the rule. - Rule Value - The rule value. - Medium - Medium through which the rule is created. - Last Updated - Displays the time when the rule is updated. - Policies - Policies to which the rule is applied. You can also sort on any column. If you mouse over a column header, a sort icon is displayed: . Click the ↑ icon to sort by the selected column.

Create New Rule dialog:

Below is an example of the Create New Rule dialog:



RULE NAME				LAST UPDATED	POLICIES
[] Custom				08/01/2023 01:35:35 pm	None
@ Custom				07/27/2023 02:59:07 pm	3 +4
1 Custom				07/27/2023 02:59:37 pm	3 +4
a Custom			cket	07/27/2023 02:59:23 pm	3 +4
A Custom				07/27/2023 02:59:49 pm	3 +4
Accesses Administ				10/19/2022 07:26:44 am	3 +4
Accesses Administ				08/01/2023 07:18:37 pm	None
Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

1 - 50 of 818 Application Rules | 0 selected

1 of 17 · 50 Application Rules per page

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

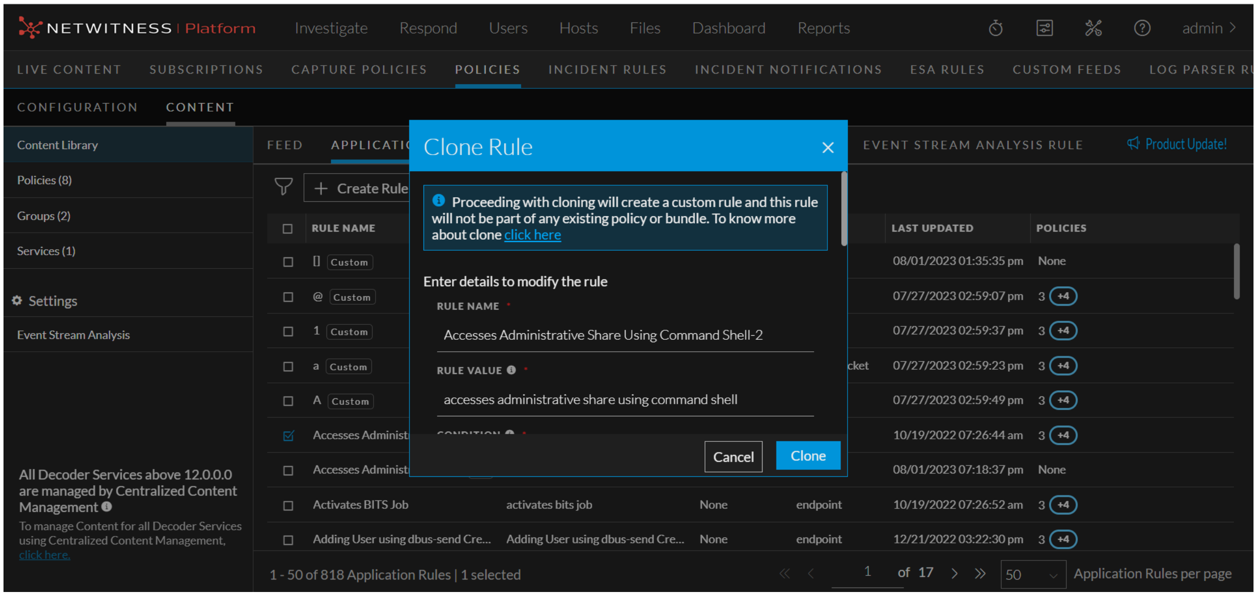
The table describes the information and options in the Create New Rule dialog:

Field	Description
Rule Name	Name of the new rule. The name should be unique.
Rule Value	The rule value. While creating a new rule, the rule value is defaulted with the rule name. However, you can modify the same.
Condition	Condition for the new rule. You can apply two types of conditions for the rule. **Normal mode:** It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on). The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators. **Advanced:** You can customize the conditions as a free form text.
Medium	Medium through which the rule is created. For a network rule, the value of medium is selected as **Packet** as default and you cannot edit it.
MITRE ATT&CK Tactics	Tactics associated with the rule. For example: **Credential Access**. For more information on MITRE ATT&CK Tactics, see **Use MITRE ATT&CK Framework** topic in the NetWitness Respond User Guide for 12.4
MITRE ATT&CK Techniques	Techniques associated with the rule. For example: **OS Credential Dumping**. For more information on MITRE ATT&CK Techniques, see **Use MITRE ATT&CK Framework** topic in the NetWitness Respond User Guide for 12.4

Description	The description of the new rule.
Session Data	Session data for the new rule. Indicates if the rule processing should stop, keep, filter or truncate when the session data is running.
Session Options	Session options for the new rule. Indicates if the session options should be alert, forward or transient.
Flag session with rule name in meta key	Conditions for which the alert should be turned on.
Save	Saves the settings and closes the Create New Rule dialog.
Cancel	Cancels the operations.

Clone Rule dialog:

Below is an example of the Clone Rule dialog.



Clone Rule

Proceeding with cloning will create a custom rule and this rule will not be part of any existing policy or bundle. To know more about clone click here

Enter details to modify the rule

RULE NAME *

Accesses Administrative Share Using Command Shell-2

RULE VALUE *

accesses administrative share using command shell

CONDITION *

	RULE NAME				LAST UPDATED	POLICIES
□	[] Custom				08/01/2023 01:35:35 pm	None
□	@ Custom				07/27/2023 02:59:07 pm	3 +4
□	1 Custom				07/27/2023 02:59:37 pm	3 +4
□	a Custom			cket	07/27/2023 02:59:23 pm	3 +4
□	A Custom				07/27/2023 02:59:49 pm	3 +4
☑	Accesses Administ				10/19/2022 07:26:44 am	3 +4
□	Accesses Administ				08/01/2023 07:18:37 pm	None
□	Activates BITS Job	activates bits job	None	endpoint	10/19/2022 07:26:52 am	3 +4
□	Adding User using dbus-send Cre...	Adding User using dbus-send Cre...	None	endpoint	12/21/2022 03:22:30 pm	3 +4

1 - 50 of 818 Application Rules | 1 selected

1 of 17 50 Application Rules per page

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

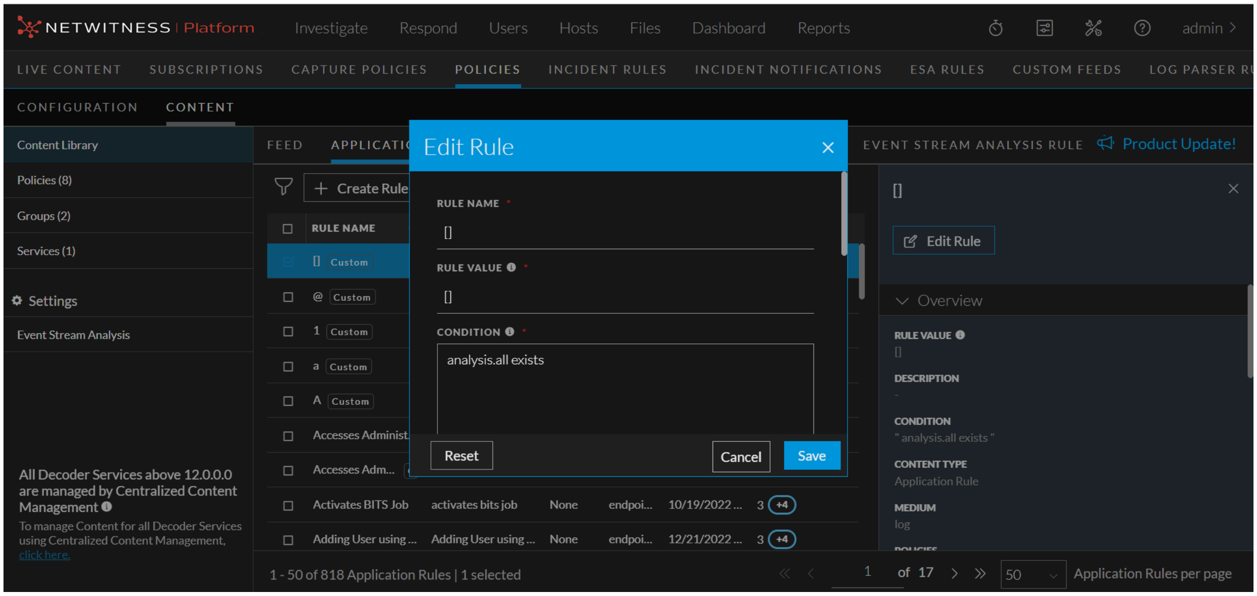
The table describes the information and options in the Clone Rule dialog:

Field	Description
Rule Name	Name of the cloned rule. The name should be unique.
Rule Value	The rule value written to the alert meta.

Condition	Condition for the new rule. You can apply two types of conditions for the rule. **Normal mode:** It gives suggestions for supported metas (ip, host and so on) and operators ("=", "Not Equal To", "Contains", "Exists" and so on). The entered condition will be enclosed in a 'Pill'. When you enter multiple conditions, the conditions are automatically joined by an 'AND' operator. On clicking the 'AND' operator, you can toggle between 'AND' and 'OR' operators. **Advanced:** You can customize the conditions as a free form text.
Medium	Medium through which the rule is created. For a network rule, the value of medium is selected as **Packet** as default and you cannot edit it.
MITRE ATT&CK Tactics	Tactics associated with the rule. For example: **Credential Access**. For more information on MITRE ATT&CK Tactics, see **Use MITRE ATT&CK Framework** topic in the NetWitness Respond User Guide for 12.4
MITRE ATT&CK Techniques	Techniques associated with the rule. For example: **OS Credential Dumping**. For more information on MITRE ATT&CK Techniques, see **Use MITRE ATT&CK Framework** topic in the NetWitness Respond User Guide for 12.4
Description	The description of the new rule.
Session Data	Session data for the new rule. Indicates if the rule processing should stop, keep, filter or truncate when the session data is running.
Session Options	Session options for the new rule. Indicates if the session options should be alert, forward or transient.
Flag session with rule name in meta key	Conditions for which the alert should be turned on.
Clone	Clones the rule and closes the Cone Rule dialog.
Cancel	Cancels the operation.

Edit Rule dialog:

Below is an example of the Edit Rule dialog:



Edit Rule

RULE NAME *
[]

RULE VALUE *
[]

CONDITION *
analysis.all exists

RULE NAME						
[] Custom						
@ Custom						
1 Custom						
a Custom						
A Custom						
Accesses Administ...						
Accesses Adm...						
Activates BITS Job	activates bits job	None	endpoi...	10/19/2022 ...	3	+4
Adding User using ...	Adding User using ...	None	endpoi...	12/21/2022 ...	3	+4

1 - 50 of 818 Application Rules | 1 selected   1 of 17   50 Application Rules per page

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management
To manage Content for all Decoder Services using Centralized Content Management, click here.

[]
Edit Rule
RULE VALUE
[]
DESCRIPTION
-
CONDITION
" analysis.all exists "
CONTENT TYPE
Application Rule
MEDIUM
log
POLICIES

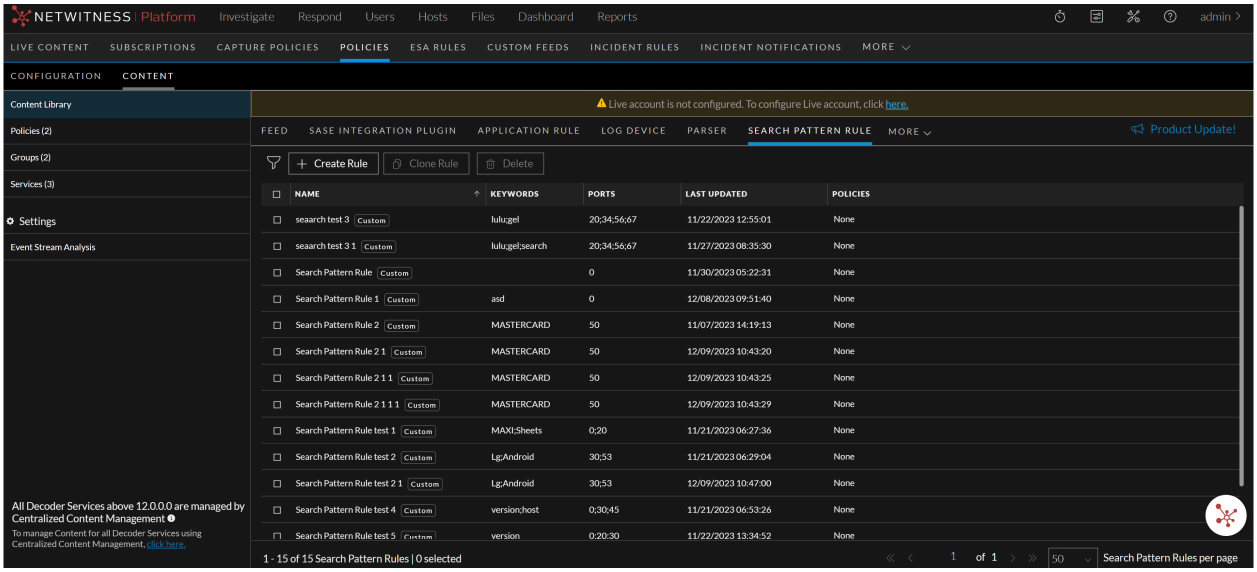
The table describes the information and options in the Edit Rule dialog:

Field	Description
Rule Name	Name of the new rule. The name should be unique.
Rule Value	The rule value.
Condition	Condition for the new rule. You can apply two types of conditions for the rule. **Normal mode:** It gives suggestions for supported metas (ip, host and so on) and operators (“=”, “Not Equal To”, “Contains”, “Exists” and so on). The entered condition will be enclosed in a ‘Pill’. When you enter multiple conditions, the conditions are automatically joined by an ‘AND’ operator. On clicking the ‘AND’ operator, you can toggle between ‘AND’ and ‘OR’ operators. **Advanced:** You can customize the conditions as a free form text.
Medium	Medium through which the rule is created. For a network rule, the value of medium is selected as **Packet** as default and you cannot edit it.
MITRE ATT&CK Tactics	Tactics associated with the rule. For example: **Credential Access**. For more information on MITRE ATT&CK Tactics, see **Use MITRE ATT&CK Framework** topic in the NetWitness Respond User Guide for 12.4
MITRE ATT&CK Techniques	Techniques associated with the rule. For example: **OS Credential Dumping**. For more information on MITRE ATT&CK Techniques, see **Use MITRE ATT&CK Framework** topic in the NetWitness Respond User Guide for 12.4

Description	The description of the new rule.
Session Data	Session data for the new rule. Indicates if the rule processing should stop, keep, filter or truncate when the session data is running.
Session Options	Session options for the new rule. Indicates if the session options should be alert, forward or transient.
Flag session with rule name in meta key	Conditions for which the alert should be turned on.
Save	Saves the settings and closes the Edit Rule dialog.
Reset	Reset the fields.
Cancel	Cancels the operation.

Search Pattern Rule tab

Following is an example of the **Content** > **Content Library** > **More** > **Search Pattern Rule** tab:



Live account is not configured. To configure Live account, click here.

☐	NAME	KEYWORDS	PORTS	LAST UPDATED	POLICIES
☐	seaarch test 3 Custom	lulu;gel	20;34;56;67	11/22/2023 12:55:01	None
☐	seaarch test 3 1 Custom	lulu;gel;search	20;34;56;67	11/27/2023 08:35:30	None
☐	Search Pattern Rule Custom		0	11/30/2023 05:22:31	None
☐	Search Pattern Rule 1 Custom	asd	0	12/08/2023 09:51:40	None
☐	Search Pattern Rule 2 Custom	MASTERCARD	50	11/07/2023 14:19:13	None
☐	Search Pattern Rule 2 1 Custom	MASTERCARD	50	12/09/2023 10:43:20	None
☐	Search Pattern Rule 2 1 1 Custom	MASTERCARD	50	12/09/2023 10:43:25	None
☐	Search Pattern Rule 2 1 1 1 Custom	MASTERCARD	50	12/09/2023 10:43:29	None
☐	Search Pattern Rule test 1 Custom	MAXI;Sheets	0;20	11/21/2023 06:27:36	None
☐	Search Pattern Rule test 2 Custom	Lg;Android	30;53	11/21/2023 06:29:04	None
☐	Search Pattern Rule test 2 1 Custom	Lg;Android	30;53	12/09/2023 10:47:00	None
☐	Search Pattern Rule test 4 Custom	version;host	0;30;45	11/21/2023 06:53:26	None
☐	Search Pattern Rule test 5 Custom	version	0:20:30	11/22/2023 13:34:52	None

1 - 15 of 15 Search Pattern Rules | 0 selected

All Decoder Services above 12.0.0.0 are managed by Centralized Content Management

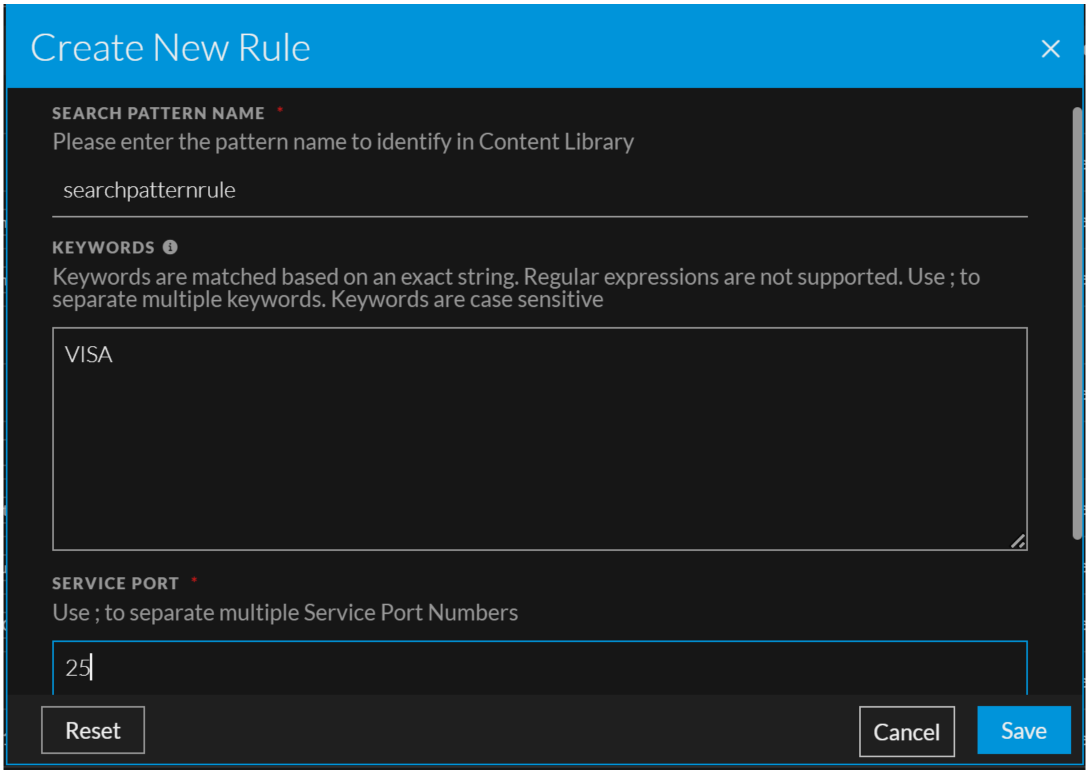
To manage Content for all Decoder Services using Centralized Content Management, click here.

1	Toolbar • **Create Rule** - Allows you to create a search pattern rule. • **Clone Rule** - Allows you to clone a search pattern rule. For more information, see Manage Search Pattern Rules • **Delete** - Allows you to delete a search pattern rule. For more information, see Manage Search Pattern Rules

2	Rule List Pane • **Name** - Name of the search pattern rule. • **Keywords** - Displays the keywords associated for each search pattern rule. • **Ports** - Displays the ports associated for each search pattern rule. • **Last Updated** - Displays the time when the rule is updated. • **Policies** - Policies to which the rule is applied. You can also sort on any column. If you mouse over a column header, a sort icon is displayed: . Click the ↑ icon to sort by the selected column.

Create New Rule dialog for Search Pattern Rule:

Below is an example of the Create New Rule dialog for Search Pattern Rule:



Create New Rule

SEARCH PATTERN NAME *
Please enter the pattern name to identify in Content Library

searchpatternrule

KEYWORDS
Keywords are matched based on an exact string. Regular expressions are not supported. Use ; to separate multiple keywords. Keywords are case sensitive

VISA

SERVICE PORT *
Use ; to separate multiple Service Port Numbers

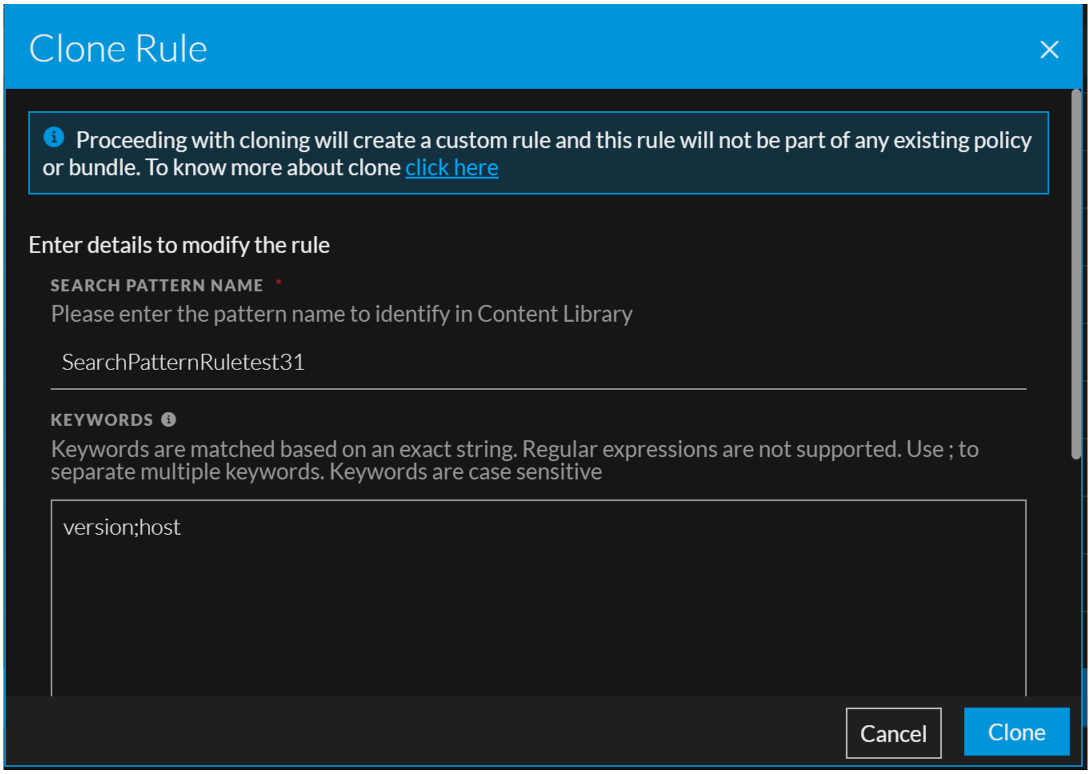
25

Field	Description
Search Pattern Name	Name of the new rule. The name should be unique.
Keywords	Allows you to add one or more keywords. Keywords are matched based on an exact string only. Regular expressions (Regex) are not supported. Use semicolons (;) to separate multiple keywords. For example, **CreditCard**;**VISA**;**US**.

Field	Description
Service Port	Allows you to add one or more ports. Use semicolons (;) to separate multiple port numbers.For example, **20**;**21**;**23**. The port numbers must be between **1** and 65535.
Save	Saves the settings and closes the Create New Rule dialog.
Cancel	Cancels the operations.
Reset	Reset the fields.

Clone Rule dialog for Search Pattern Rule:

Below is an example of the Clone Rule dialog.



Clone Rule

Proceeding with cloning will create a custom rule and this rule will not be part of any existing policy or bundle. To know more about clone click here

Enter details to modify the rule

SEARCH PATTERN NAME *
Please enter the pattern name to identify in Content Library

SearchPatternRuletest31

KEYWORDS
Keywords are matched based on an exact string. Regular expressions are not supported. Use ; to separate multiple keywords. Keywords are case sensitive

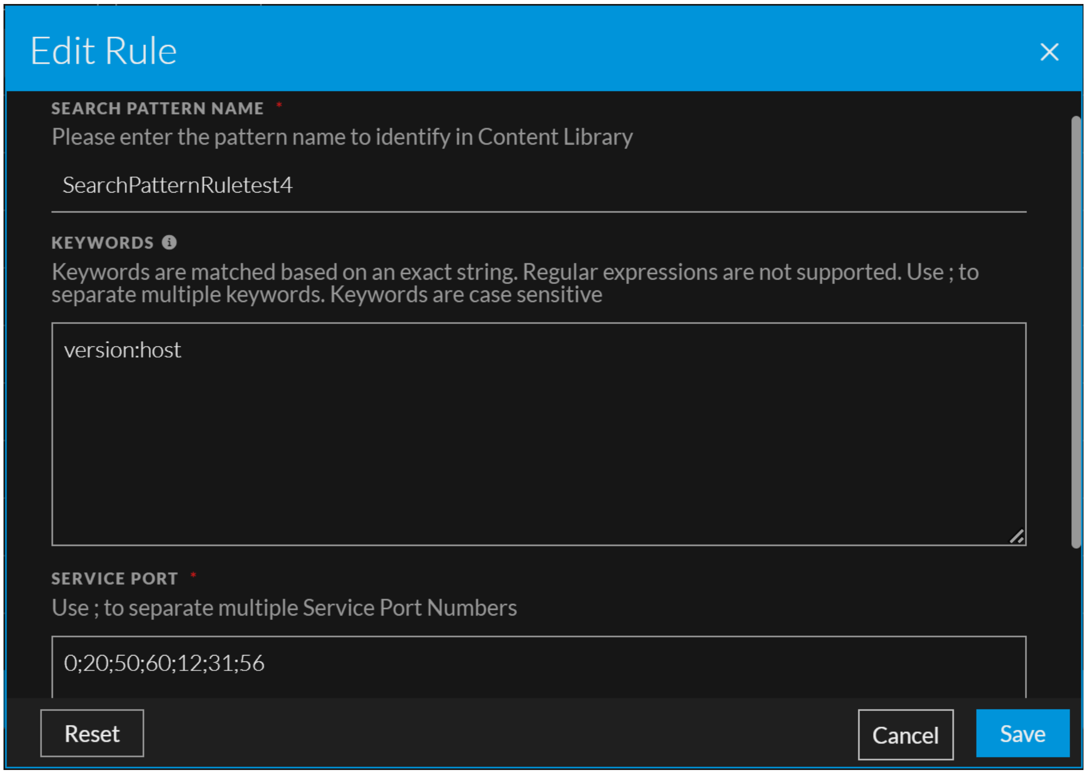
version;host

Field	Description
Search Pattern Name	Name of the new rule. The name should be unique.
Keywords	Allows you to add one or more keywords. Keywords are matched based on an exact string only. Regular expressions (Regex) are not supported. Use semicolons (;) to separate multiple keywords. For example, **CreditCard**;**VISA**;**US**.
Service Port	Allows you to add one or more ports. Use semicolons (;) to separate multiple port numbers.For example, **20**;**21**;**23**. The port numbers must be between **1** and **65535**.

Field	Description
Clone	Clones the rule and closes the Cone Rule dialog.
Cancel	Cancels the operations.

Edit Rule dialog for Search Pattern Rule:

Below is an example of the Edit Rule dialog.



SEARCH PATTERN NAME *
Please enter the pattern name to identify in Content Library
SearchPatternRuletest4

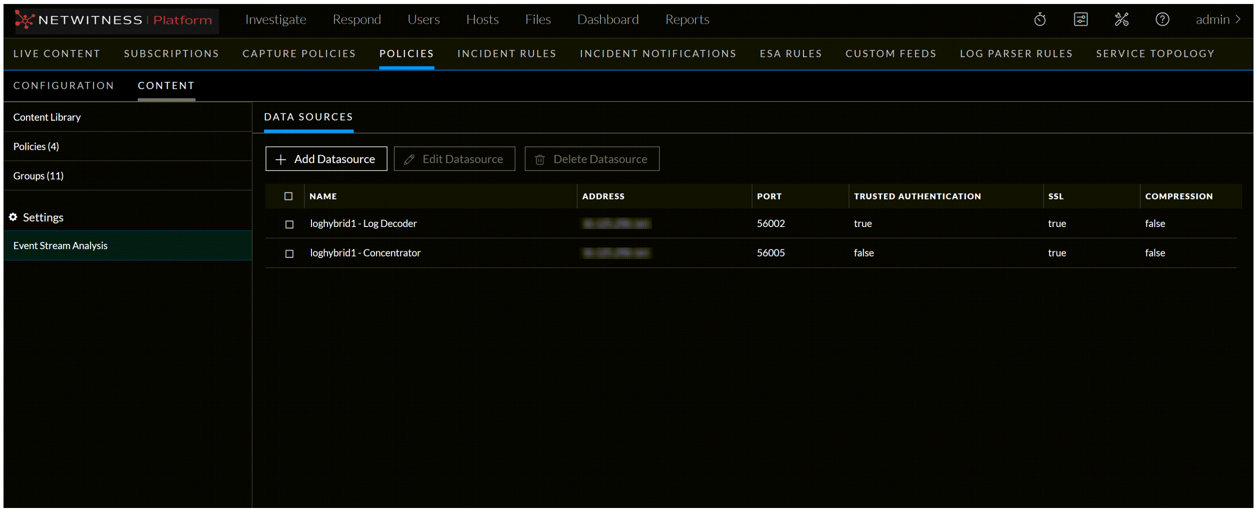
KEYWORDS
Keywords are matched based on an exact string. Regular expressions are not supported. Use ; to separate multiple keywords. Keywords are case sensitive
version:host

SERVICE PORT *
Use ; to separate multiple Service Port Numbers
0;20;50;60;12;31;56

Field	Description
Search Pattern Name	Name of the new rule. The name should be unique.
Keywords	Allows you to add one or more keywords. Keywords are matched based on an exact string only. Regular expressions (Regex) are not supported. Use semicolons (;) to separate multiple keywords. For example, **CreditCard**;**VISA**;**US**.
Service Port	Allows you to add one or more ports. Use semicolons (;) to separate multiple port numbers.For example, **20**;**21**;**23**. The port numbers must be between **1** and **65535**.
Save	Saves the settings and closes the Edit Rule dialog.
Cancel	Cancels the operations.
Reset	Reset the fields.

Data Sources Tab

Below is an example of the **Content** > **Settings** > **Event Stream Analysis** > **Data Sources** tab:

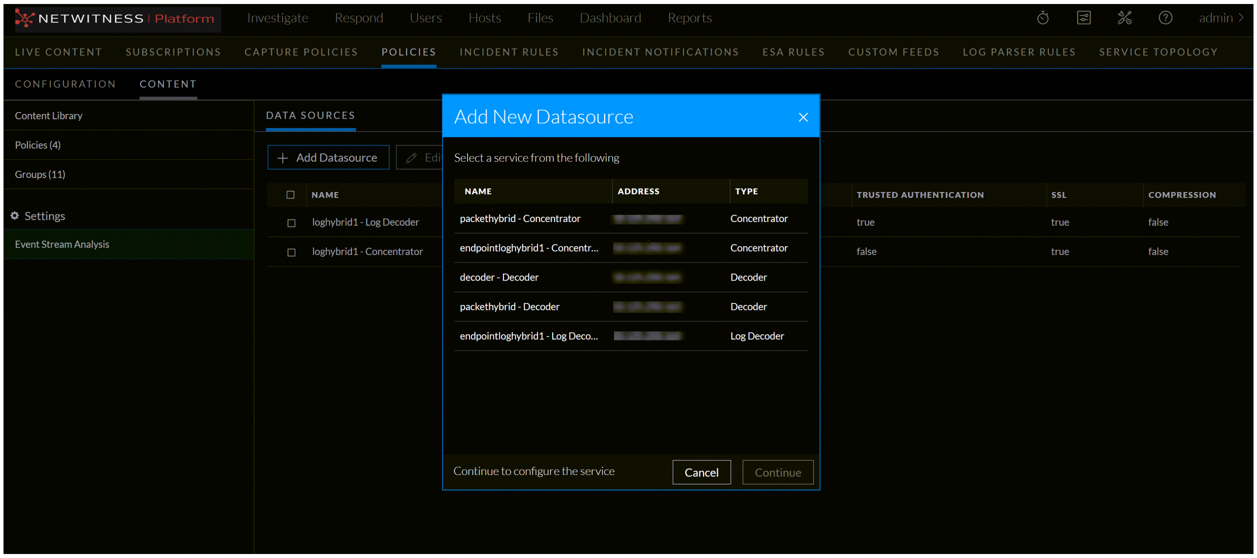


□	NAME	ADDRESS	PORT	TRUSTED AUTHENTICATION	SSL	COMPRESSION
□	loghybrid1 - Log Decoder	[redacted]	56002	true	true	false
□	loghybrid1 - Concentrator	[redacted]	56005	false	true	false

The following table describes the Data Sources tab.

1	Toolbar • Add Datasource- Lets you to add a new Datasource. For more information, see Add an ESA Datasource. • Edit - Datasource - Lets you edit the Datasource. For more information, see Edit an ESA Datasource. • Delete Datasource - Deletes the selected Datasource.
2	Data Sources List Pane • Name - Shows the name of the data sources used by the selected ESA service. Data sources can be Concentrators or Decoders. • Address - IP address of the datasource where the ESA service is installed. • Port - Shows the port number used for authentication. • Trusted Authentication - Indicates that it uses Trusted Authentication for communication with ESA Service. • SSL - Indicates that it uses SSL for Authentication. • Compression - Enables you to adjust the Compression Level on different datasources for ESA.

Below is an example of the **Add New Datasource** dialog:



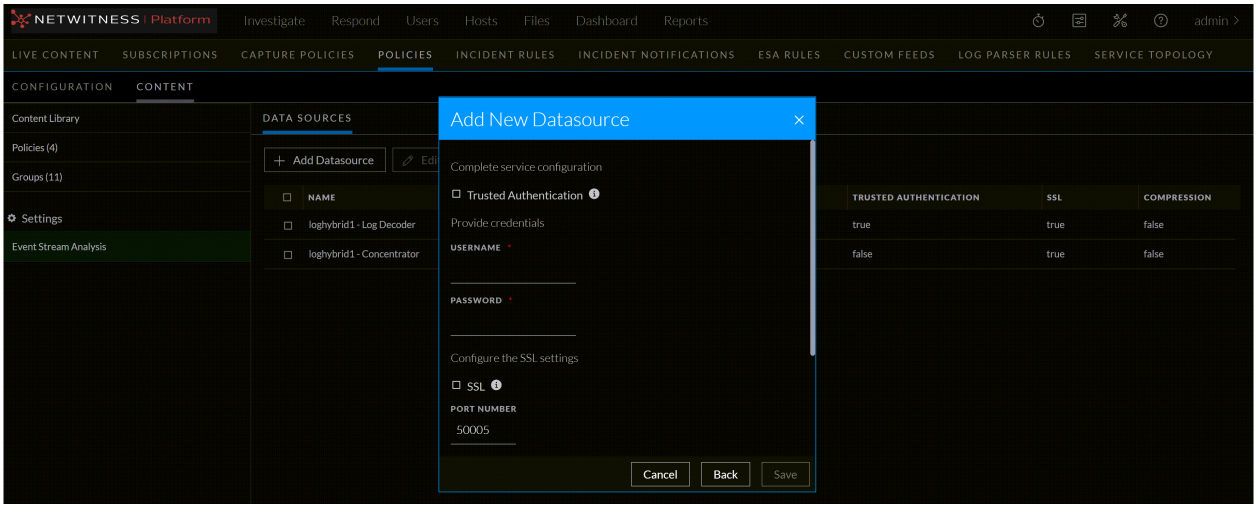
Add New Datasource

Select a service from the following

NAME	ADDRESS	TYPE
packethybrid - Concentrator	[redacted]	Concentrator
endpointloghybrid1 - Concentr...	[redacted]	Concentrator
decoder - Decoder	[redacted]	Decoder
packethybrid - Decoder	[redacted]	Decoder
endpointloghybrid1 - Log Deco...	[redacted]	Log Decoder

Continue to configure the service

☐	NAME	TRUSTED AUTHENTICATION	SSL	COMPRESSION
☐	loghybrid1 - Log Decoder	true	true	false
☐	loghybrid1 - Concentrator	false	true	false



Add New Datasource

Complete service configuration

☐ Trusted Authentication

Provide credentials

USERNAME *

PASSWORD *

Configure the SSL settings

☐ SSL

PORT NUMBER
50005

☐	NAME	TRUSTED AUTHENTICATION	SSL	COMPRESSION
☐	loghybrid1 - Log Decoder	true	true	false
☐	loghybrid1 - Concentrator	false	true	false

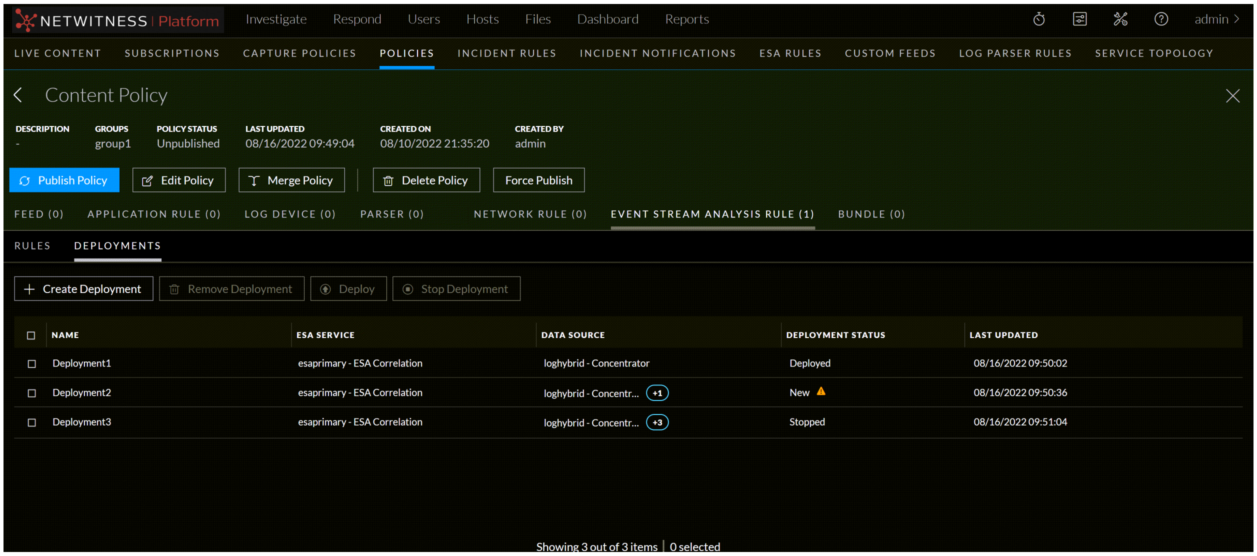
The table describes the information and options in the **Add New Datasource** dialog.

Field	Description
Trusted Authentication	This option will enable the use of SSL by default for authentication.
Username	The username used to sign in to your account for authenticating the datasource.
Password	The password for authenticating the datasource.
SSL	This will enable the use of SSL for authentication.
Port Number	This will enable the use of the port number for authentication.
Compression	This option enables you to adjust the Compression Level on different datasources for ESA.
Compression Level	Enables you to set different compression level. Compression Level: **0**, **1**, and **9**. For more information, see Add an ESA Datasource.

Field	Description
Test Configuration	Validates the provided configuration.
Save	Saves the settings and closes the Add New Datasource dialog.
Cancel	Cancels the operations.

Deployments Tab

Below is an example of the **Content** > **Policies** > select a policy > **Event Stream Analysis Rule** > **Deployments** tab:



Content Policy

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	group1	Unpublished	08/16/2022 09:49:04	08/10/2022 21:35:20	admin

□	NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
□	Deployment1	esaprimary - ESA Correlation	loghybrid - Concentrator	Deployed	08/16/2022 09:50:02
□	Deployment2	esaprimary - ESA Correlation	loghybrid - Concentr... +1	New ⚠	08/16/2022 09:50:36
□	Deployment3	esaprimary - ESA Correlation	loghybrid - Concentr... +3	Stopped	08/16/2022 09:51:04

Showing 3 out of 3 items | 0 selected

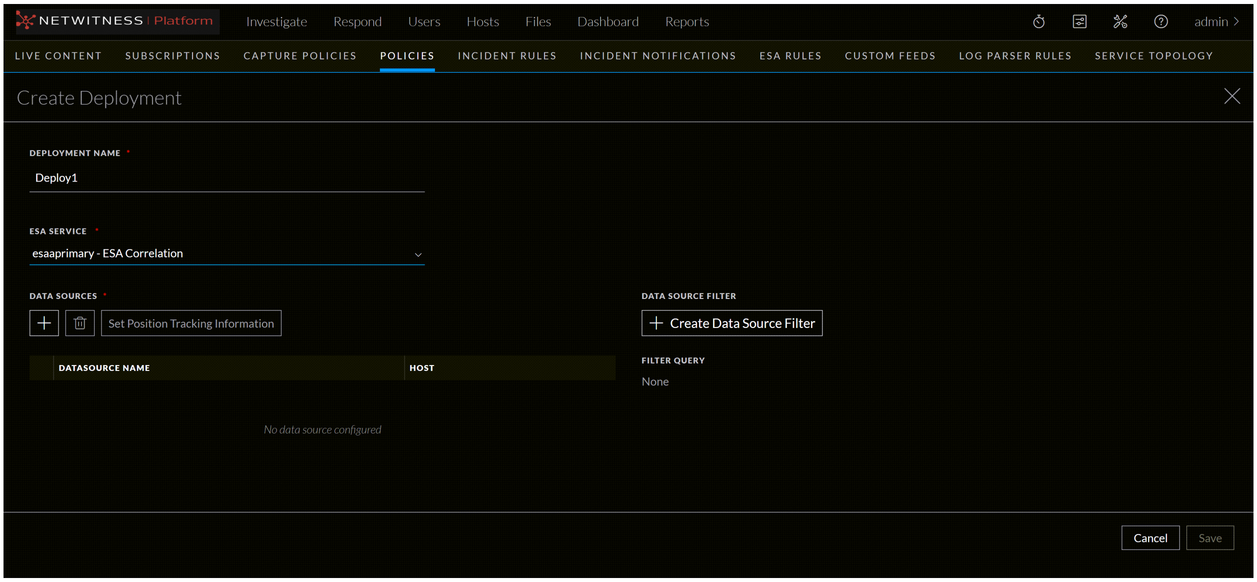
The following table describes the Deployments tab.

1	Toolbar • Create Deployment - Lets you to Add a new Deployment. For more information, see Create a Deployment. • Remove Deployment - Lets you to remove the Deployment.For more information, see Remove a Deployment. • Deploy - Lets you to deploy the Deployment. • Stop Deployment - Lets you to stop the selected Deployment.

2	Deployment List Pane • Name - Name of the content. • ESA Service - Displays the ESA service selected. • Data Source - Displays the Datasource added for ESA deployment. • Deployment Status - Status of the deployment. The values are: Deploying, Deployed, New, Stopping, Stopped, and Failed. • Last Updated - Displays the time when the deployment is updated.

Create Deployment dialog:

Below is an example of the Create Deployment dialog:



Create Deployment

DEPLOYMENT NAME *
Deploy1

ESA SERVICE *
esaaprimary - ESA Correlation

DATA SOURCES *

DATASOURCE NAME	HOST

No data source configured

DATA SOURCE FILTER

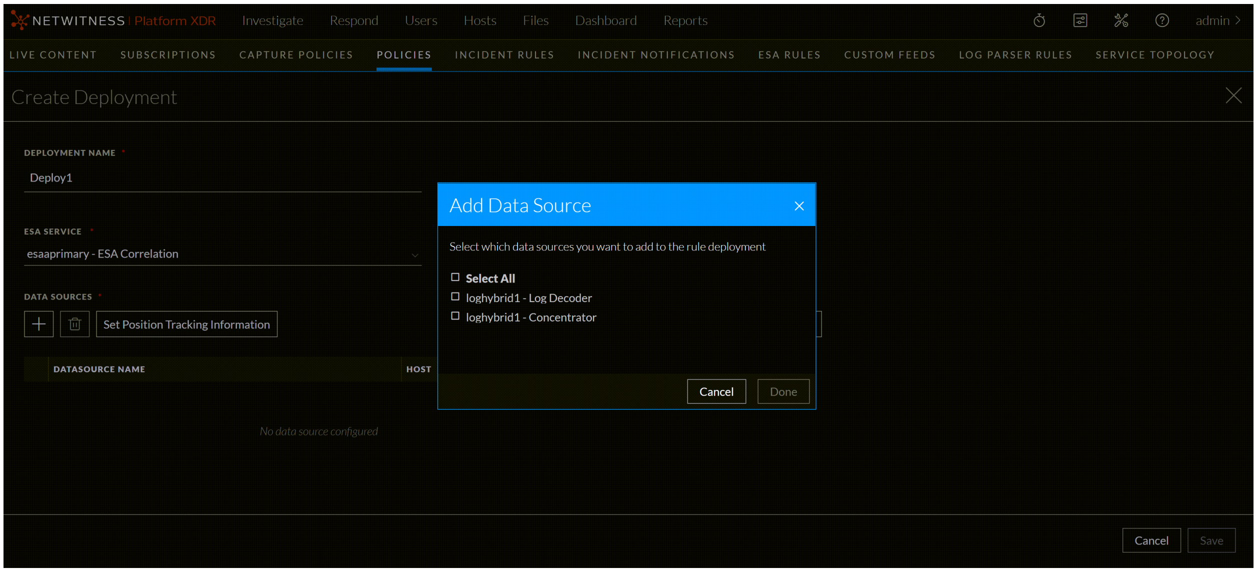
FILTER QUERY
None

The table describes the information and options in the **Create Deployment** dialog.

Field	Description
Deployment Name	Name of the deployment. The name must be unique.
ESA Service	Displays the list of ESA services from the drop-down list. • esaprimary – ESA Correlation • esasecondary – ESA Correlation
+	Adds a Datasource from the available list. At least one Datasource is required to set the position tracking information for ESA.
🗑	Deletes the datasource that you are currently editing.

Field	Description
Set Position Tracking Information	Adds a position tracking information on different datasources for ESA. Position Tracking Information enables you to visualize the progress of the sessions that ESA has processed, and provides information on the session IDs and the time/date when the events were processed. For more information, see Position Tracking Information.
Create Data Source Filter	Enables you to create the datasource filter to get the required results.
Save	Saves the settings and closes the Create Deployment dialog.
Cancel	Cancels the operations.

Below is an example of **Add Data Source** Dialog.



Create Deployment

DEPLOYMENT NAME *
Deploy1

ESA SERVICE *
esaaprimary - ESA Correlation

DATA SOURCES *

No data source configured

Add Data Source

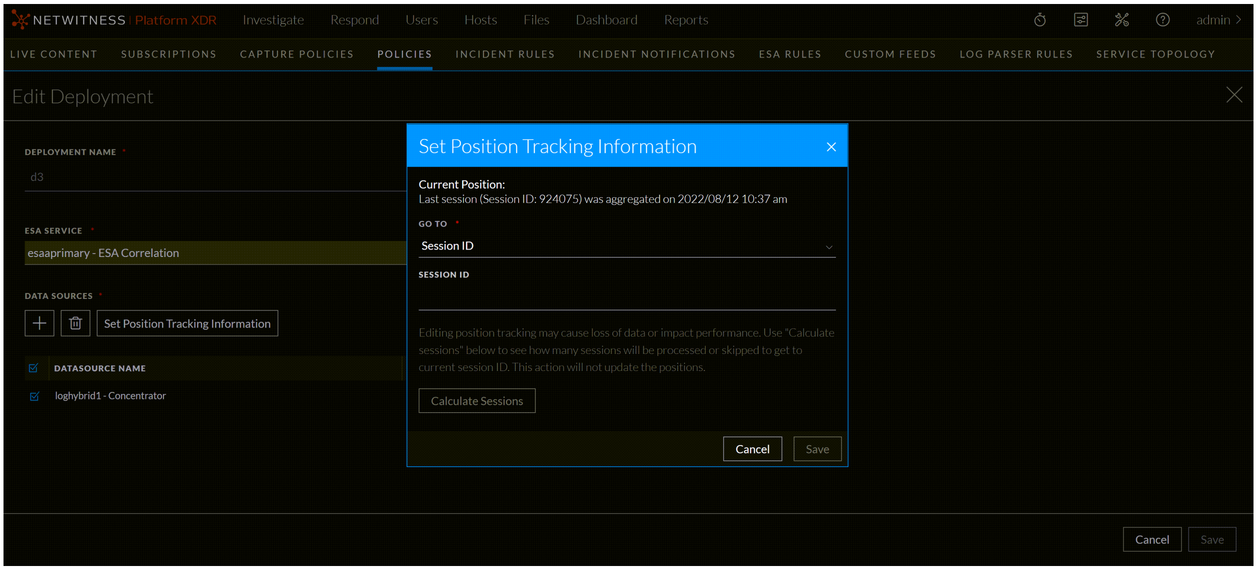
Select which data sources you want to add to the rule deployment

□ Select All
□ loghybrid1 - Log Decoder
□ loghybrid1 - Concentrator

The table describes the information and options in the **Add Data Source** dialog.

Field	Description
Select Datasource / Select All	Allows you to select one or more datasources.
Done	Adds the datasource and closes the Add Data Source dialog.
Cancel	Cancels the operations.

Below is an example of **Set Position Tracking Information** dialog.



Edit Deployment

DEPLOYMENT NAME *
d3

ESA SERVICE *
esaaprimary - ESA Correlation

DATA SOURCES *

☑	DATASOURCE NAME
☑	loghybrid1 - Concentrator

Set Position Tracking Information

Current Position:
Last session (Session ID: 924075) was aggregated on 2022/08/12 10:37 am

GO TO *
Session ID

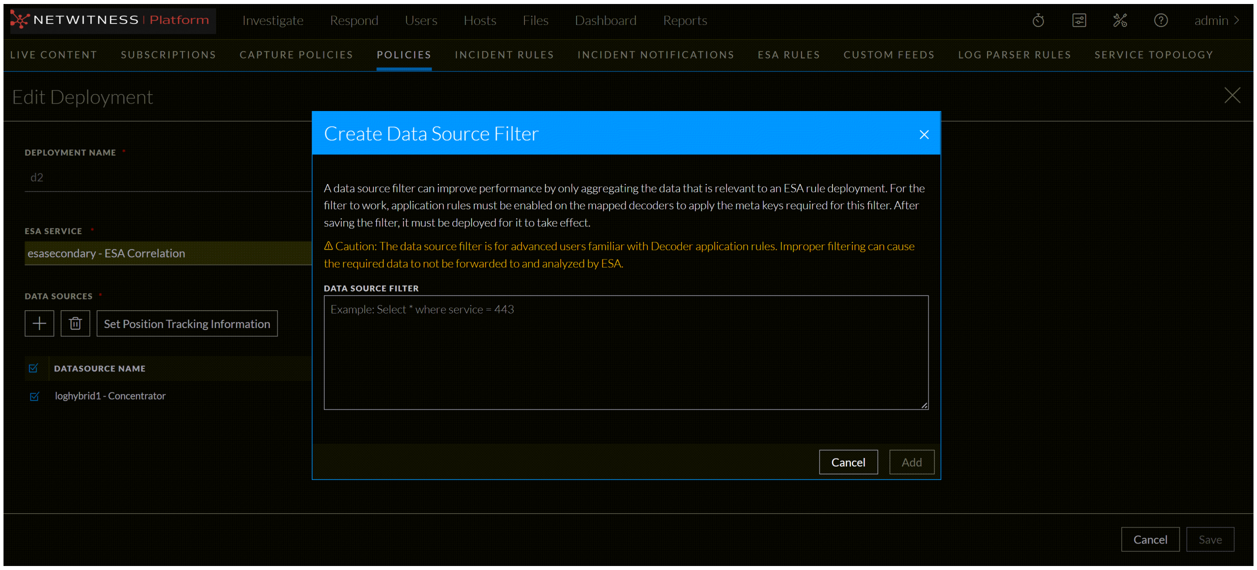
SESSION ID

Editing position tracking may cause loss of data or impact performance. Use "Calculate sessions" below to see how many sessions will be processed or skipped to get to current session ID. This action will not update the positions.

The table describes the information and options in the **Set Position Tracking Information** dialog.

Field	Description
Go To	This option will enable the use of Session ID and data and time for ESA Correlation Service for the events.
Session ID	The ESA Correlation service starts processing the events from the session ID that you entered.
Date and Time	The ESA Correlation service starts processing the events from the date and time that you entered.
Calculate Sessions	This will calculate the number of sessions that will be processed with respect to the existing position of the data source.
Save	Saves the settings and closes the Set Position Tracking Information dialog.
Cancel	Cancels the operations.

Below is an example of **Create Data Source Filter** Dialog



Edit Deployment

DEPLOYMENT NAME *
d2

ESA SERVICE *
esasecondary - ESA Correlation

DATA SOURCES *

☑	DATASOURCE NAME
☑	loghybrid1 - Concentrator

Create Data Source Filter

A data source filter can improve performance by only aggregating the data that is relevant to an ESA rule deployment. For the filter to work, application rules must be enabled on the mapped decoders to apply the meta keys required for this filter. After saving the filter, it must be deployed for it to take effect.

⚠ Caution: The data source filter is for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

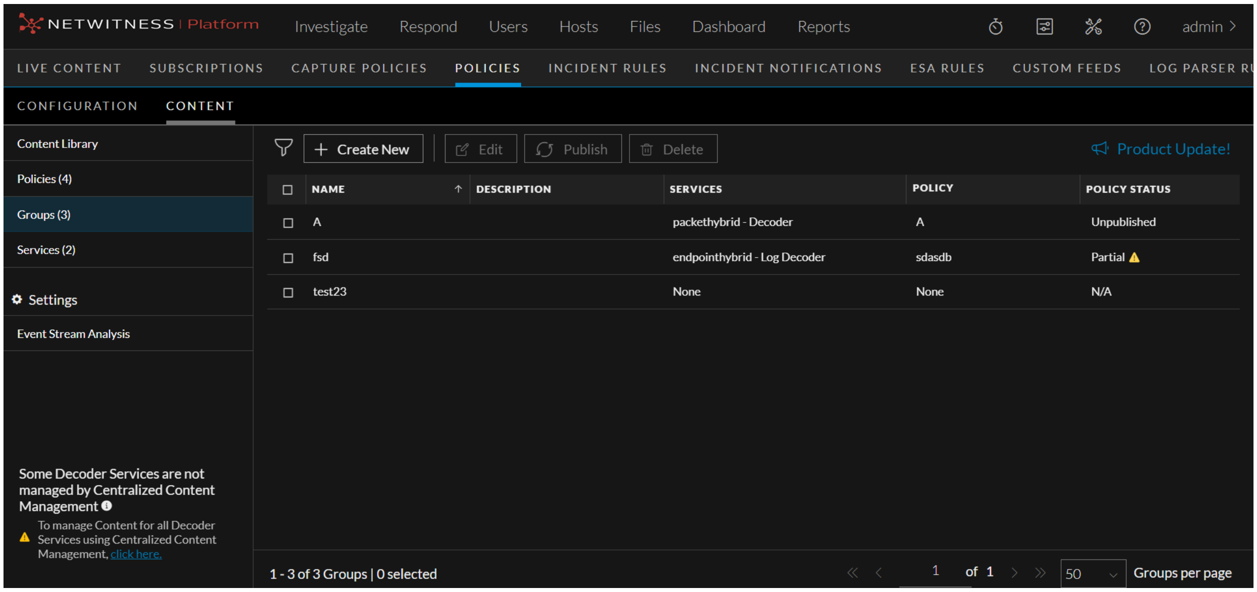
DATA SOURCE FILTER
Example: Select * where service = 443

The table describes the information and options in the **Create Data Source Filter** dialog.

Field	Description
Data Source Filter	Enables you to enter the data source filter. For example, you can type **Select *where service = 443** to filter based on the query processed, it will filter out only HTTPS logs related sessions and will be forwarded to the ESA.
Add	Adds the configurations and closes the Create Data Source Filter dialog.
Cancel	Cancels the operations.

Groups Tab

Below is an example of the Content > Groups tab:



□	NAME	DESCRIPTION	SERVICES	POLICY	POLICY STATUS
□	A		packethybrid - Decoder	A	Unpublished
□	fsd		endpointhybrid - Log Decoder	sdasdb	Partial ⚠
□	test23		None	None	N/A

Some Decoder Services are not managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

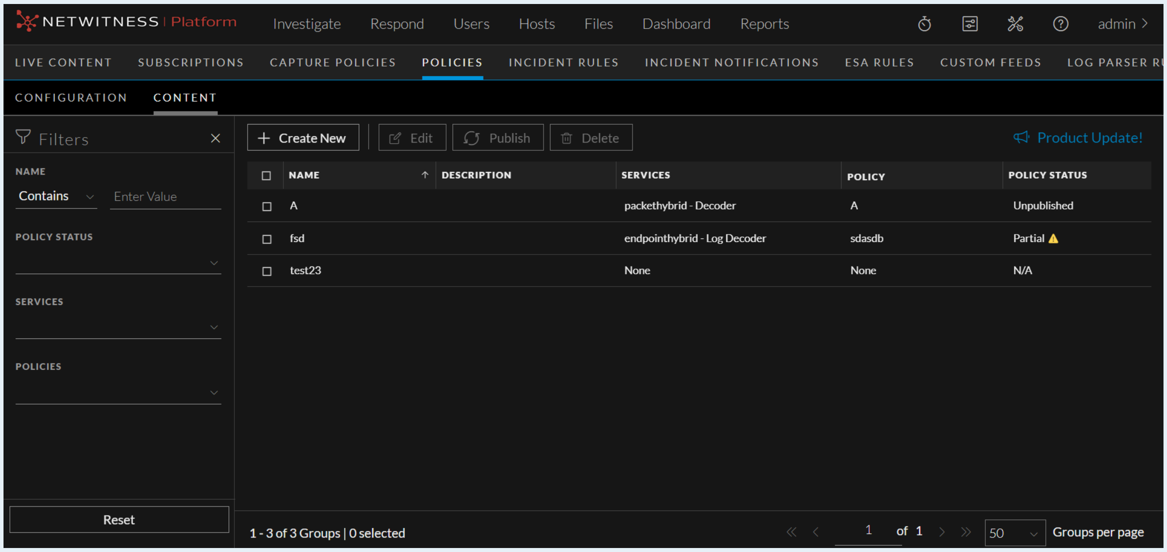
1 - 3 of 3 Groups | 0 selected

« ‹ 1 of 1 › » 50 Groups per page

The following table describes the Groups tab.

1	By default, 50 groups are displayed per page. To go to the next page, click ›. To go to the last page, click ».

2 - Filter the groups based on various parameters.



NAME: Contains | Enter Value

POLICY STATUS

SERVICES

POLICIES

□	NAME	DESCRIPTION	SERVICES	POLICY	POLICY STATUS
□	A		packethybrid - Decoder	A	Unpublished
□	fsd		endpointhybrid - Log Decoder	sdasdb	Partial ⚠
□	test23		None	None	N/A

1 - 3 of 3 Groups | 0 selected

1 of 1 | 50 Groups per page

Filter Panel:

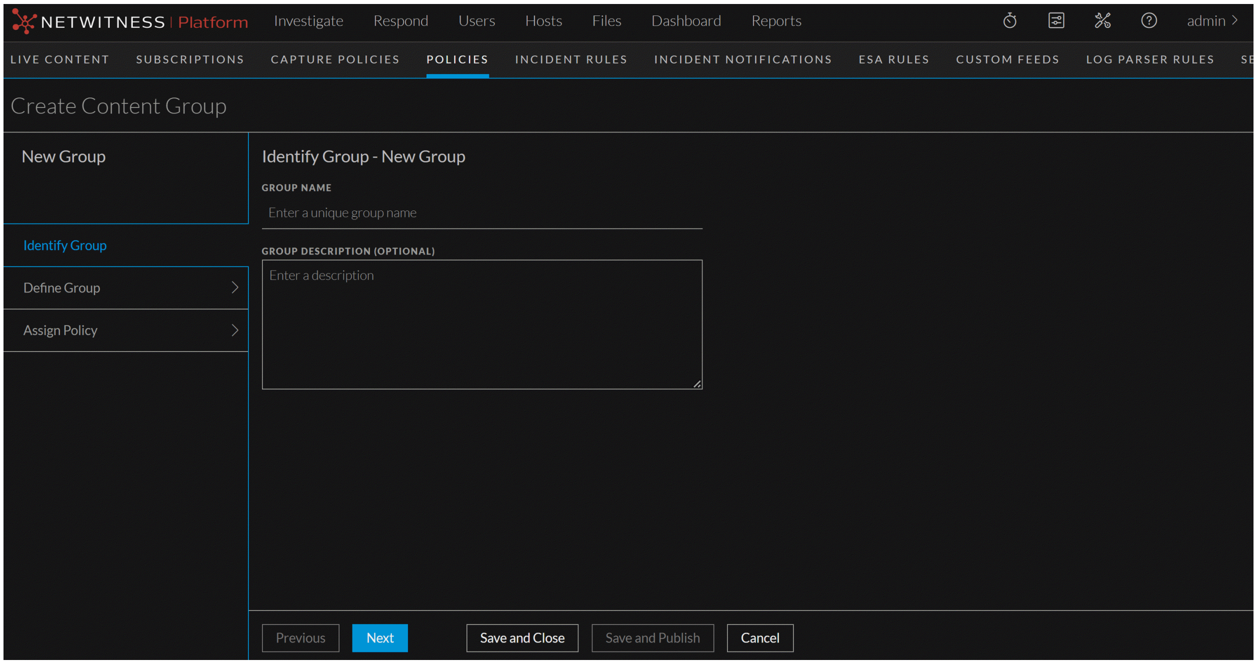
- Name - Select the **Name** drop-down value as either **Equals** or **Contains**. To search the group name using the **Contains** operator, set the filter option to **Contains** operator from the drop-down list and start typing the name of the group. Type one character and a list of group that contain that character is displayed, as you continue to type, the list is filtered to match. To search the group name using the **Equals** operator, set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular group name will be displayed.
- Policy Status - Select the **Policy Status** from the drop-down list. The various drop-down values are:
  - **Published**: Groups that are published to use.
  - **Unpublished**: Groups that are saved but not published.
  - **Failed**: Groups that are failed to publish.
  - **N/A**: Groups for which publication status is not applicable.
  - **Partial**: Groups that are partially published.
- Services - The service type to which the group is attached.
- Policies – The policies to which the group is attached.

3 Toolbar

- Create New - Lets you create a new group. For more information, see Create a group.
- Edit - Lets you edit the group. For more information, see Managing Groups.
- Publish - Publishes selected groups.
- Delete - Deletes the selected group.

4	Group List Pane • Name - Name of the group. • Description - Description of the group. • Services - Displays the service to the which the group is applied. • Policies - Displays the policy to which the group is applied. • Policy Status - Status of the policy. The values are: Published, Unpublished, Failed, N/A. You can also sort on any column. If you mouse over a column header, a sort icon is displayed: ↑. Click ↑ to sort by the selected column.
5	Groups Details Panel Displays the properties of the selected group.

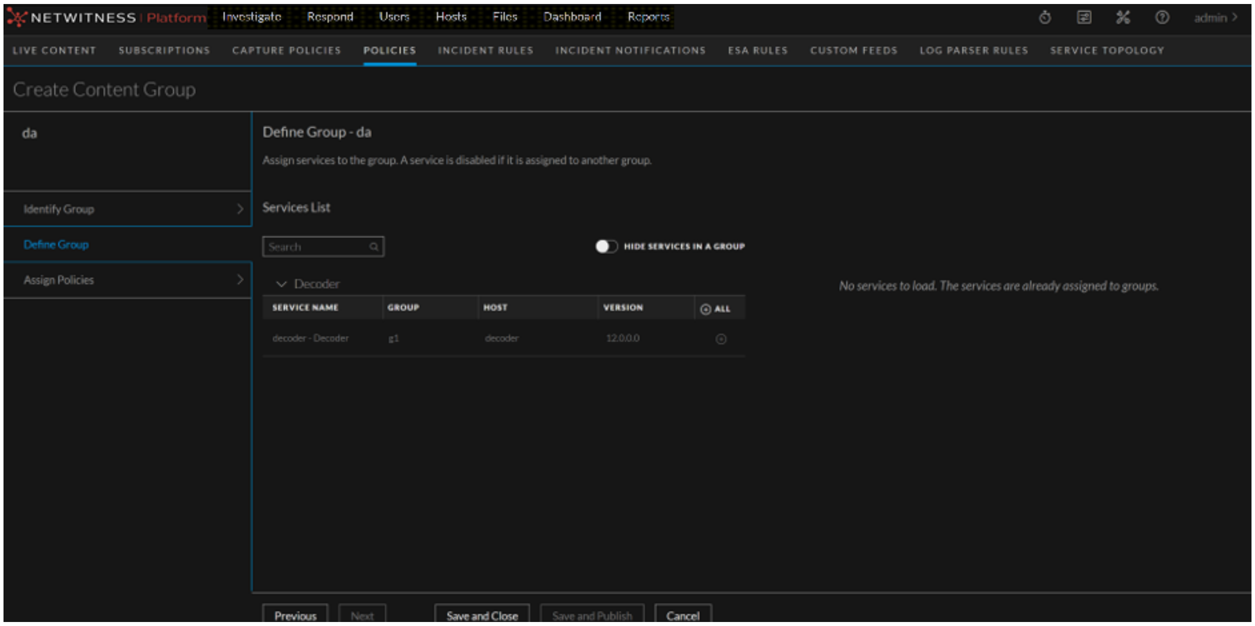
Below is an example of the Create group dialog:



The table describes the information and options in the Create Group dialog:

Field	Description
Group Name	Name of the group. The name should be unique.
Group Description (Optional)	Description of the group. Description should not exceed 8000 characters.
Save and Close	Saves the settings and closes the Create Group dialog.

Below is an example of the define group dialog:



Create Content Group

da

Define Group - da

Assign services to the group. A service is disabled if it is assigned to another group.

Services List

Decoder

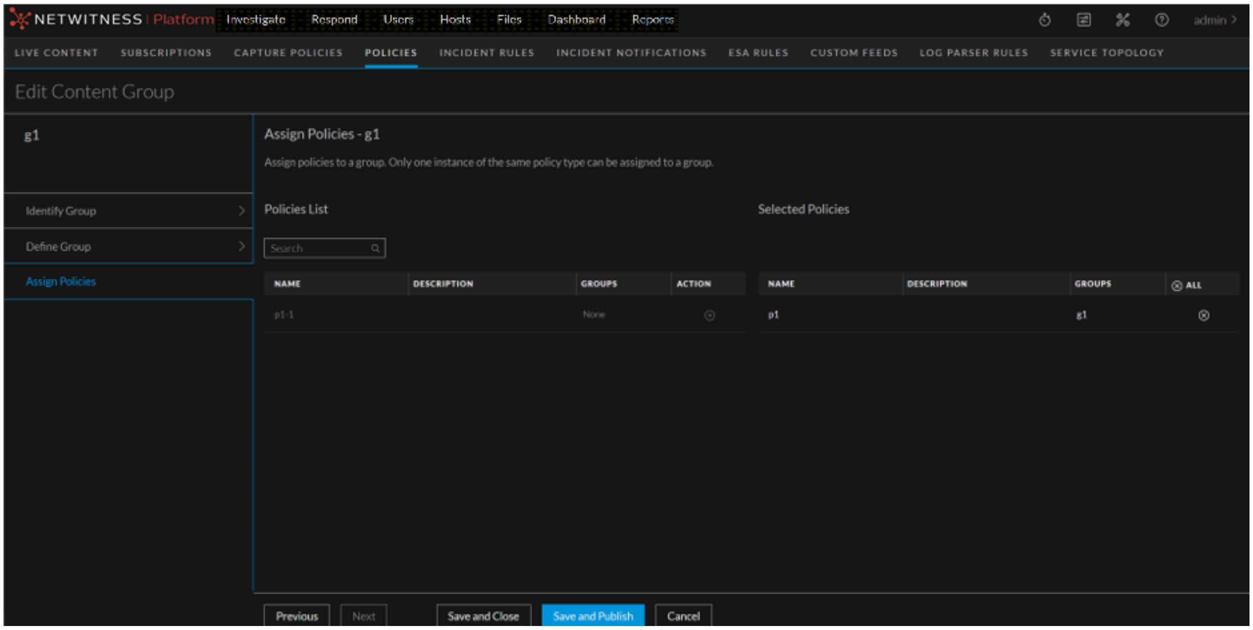
SERVICE NAME	GROUP	HOST	VERSION	ALL
decoder - Decoder	g1	decoder	12.0.0.0	

No services to load. The services are already assigned to groups.

The table describes the information and options in the Define Group dialog:

Field	Description
Services List	Displays the list of services. The following describes services list: Service name – Name of the service. • Group - Name of the group. • Host - Host name of the service. • Version - Service version. • All - Lets you to add services to the group. You can either click to add all services or click ⊕ to add specific service.
Hide Services in a Group	Displays the services that is not assigned to any group. By default, this option is disabled.
Selected Services	Displays the list of selected services for the group.
Save and Close	Saves the setting and closed the create group dialog.
Save and Publish	Saves and publishes the created group. **Note:** This option is disabled if you have not: - Assigned services. - Assigned policies.

Below is an example of Assign policy dialog:



Edit Content Group

g1

Assign Policies - g1

Assign policies to a group. Only one instance of the same policy type can be assigned to a group.

Policies List

NAME	DESCRIPTION	GROUPS	ACTION
p1-1		None	⊕

Selected Policies

NAME	DESCRIPTION	GROUPS	⊗ ALL
p1		g1	⊗

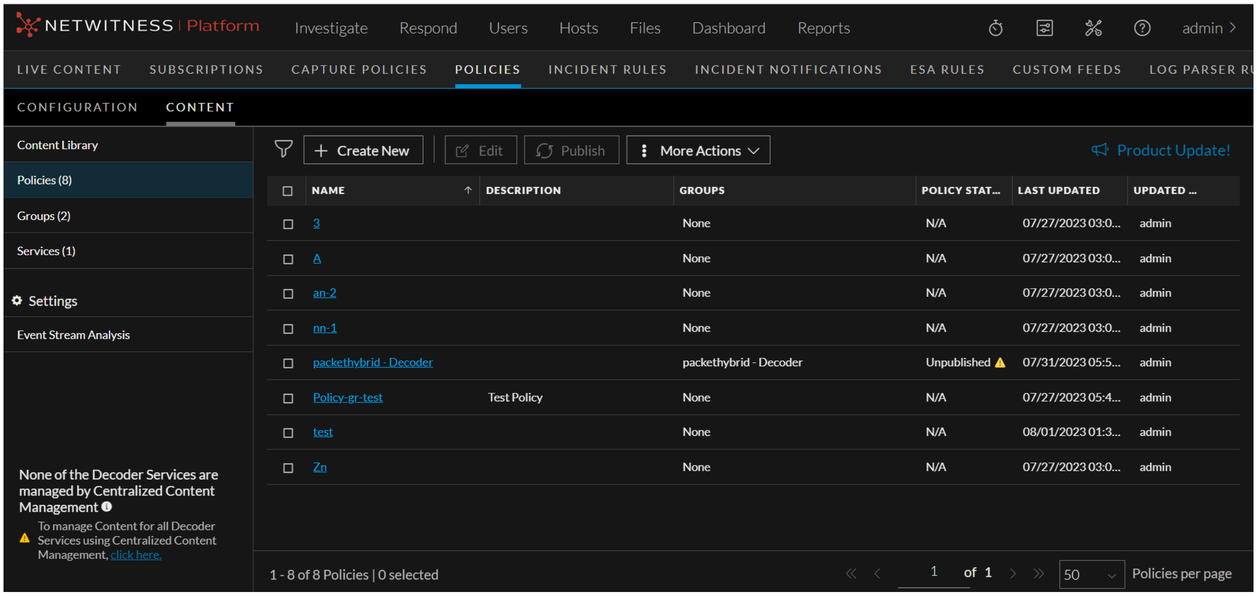
The following table describes assign policy dialog:

Field	Description
Policies List	Displays the list of policies associated with the group. The following describes policies list: • Name - Name of the policy. • Description - Description of the policy. • Groups - Groups associated with the policy. • Action - Click to add policies to the group.
Selected Policies	Displays the list of selected policies for the group.
Save and Close	Saves the setting and closed the create group dialog.
Save and Publish	Saves and publishes the created group. **Note:** This option is disabled if you have not: - Assigned services. - Assigned policies.

Policies Tab

The (CONFIGURE) > **Policies** view contains two tabs: **Configuration** and **Content**.

Below is an example of the **Content** > **Policies** tab:



□	NAME	DESCRIPTION	GROUPS	POLICY STAT...	LAST UPDATED	UPDATED ...
□	3		None	N/A	07/27/2023 03:0...	admin
□	A		None	N/A	07/27/2023 03:0...	admin
□	an-2		None	N/A	07/27/2023 03:0...	admin
□	nn-1		None	N/A	07/27/2023 03:0...	admin
□	packethybrid - Decoder		packethybrid - Decoder	Unpublished ⚠	07/31/2023 05:5...	admin
□	Policy-gr-test	Test Policy	None	N/A	07/27/2023 05:4...	admin
□	test		None	N/A	08/01/2023 01:3...	admin
□	Zn		None	N/A	07/27/2023 03:0...	admin

1 - 8 of 8 Policies | 0 selected « ‹ 1 of 1 › » 50 Policies per page

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

The following table describes the Policies tab.

1	By default, 50 policies are displayed per page. To go to the next page, click ›. To go to the last page, click ».

2 Toolbar:

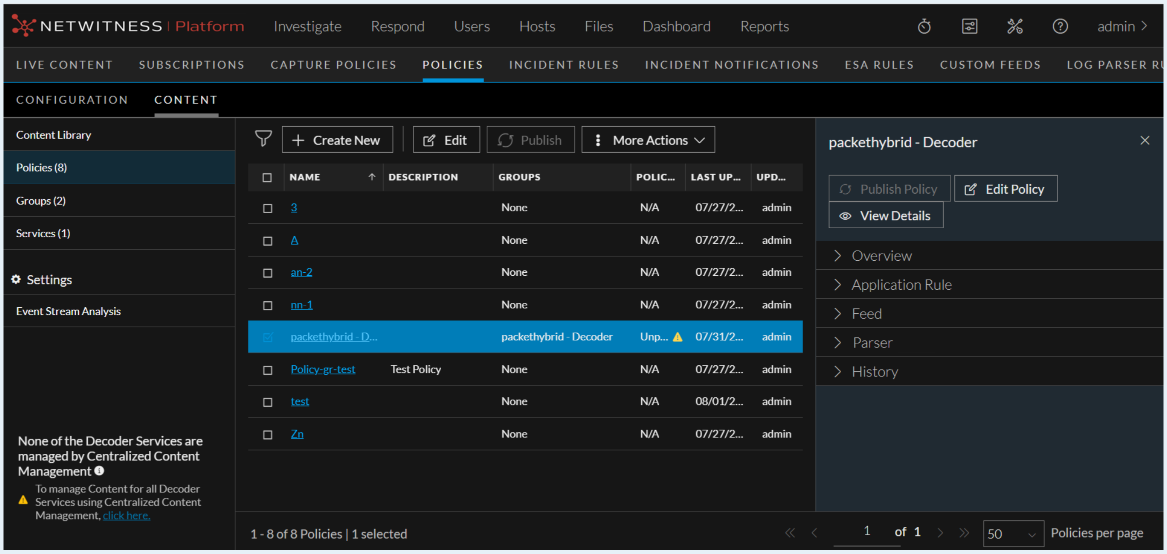
- Create New - Lets you create a new policy. For more information, see Create a policy.
- Edit - Lets you edit the policy. For more information, see Edit a Policy.
- Publish - Publishes selected policy or policies.
- More Actions:
    - Assign to Group --Lets you assign policy to a group.
    - Clone - Lets you clone a policy.
    - Revert to - Lets you view the previous policy versions and revert policy to any previous version.

      Note:
      - The current version of the policy is disabled.
      - This option is disabled either if no policy is selected or multiple policies are selected.
    - ✎ - Lets you name a policy version when you revert the policy.
    - Delete - Deletes the selected group or groups permanently.
    - Force Publish - Lets you republish all the content irrespective of the policy status. This option allows you to re-push all content or configurations to all services in the group. Some of the scenarios where you might want to force publish the policy are:
        - There was a service that was down or did not successfully receive content when it was first pushed out.
        - Some content may have been modified or removed locally on a service (outside of CCM control) and you want to re-apply the content from the policy.

3 Policy List Pane:

- Name - Name of the policy.
- Description - Description of the policy.
- Groups - Lists the group to which this policy is applied.
- Policy Status - Status of the policy. The values are: Published, Unpublished, Failed, N/A.
- Last Updated - Displays the time when the policy is updated.
- Updated By - The user who updated the policy. You can also sort on any column. If you mouse over a column header, a sort icon is displayed: . Click the ↑ icon to sort by the selected column.

4 Policy List - Side Pane:



☐	NAME	DESCRIPTION	GROUPS	POLIC...	LAST UP...	UPD...
☐	3		None	N/A	07/27/2...	admin
☐	A		None	N/A	07/27/2...	admin
☐	an-2		None	N/A	07/27/2...	admin
☐	nn-1		None	N/A	07/27/2...	admin
☑	packethybrid - D...		packethybrid - Decoder	Unp... ⚠	07/31/2...	admin
☐	Policy-gr-test	Test Policy	None	N/A	07/27/2...	admin
☐	test		None	N/A	08/01/2...	admin
☐	Zn		None	N/A	07/27/2...	admin

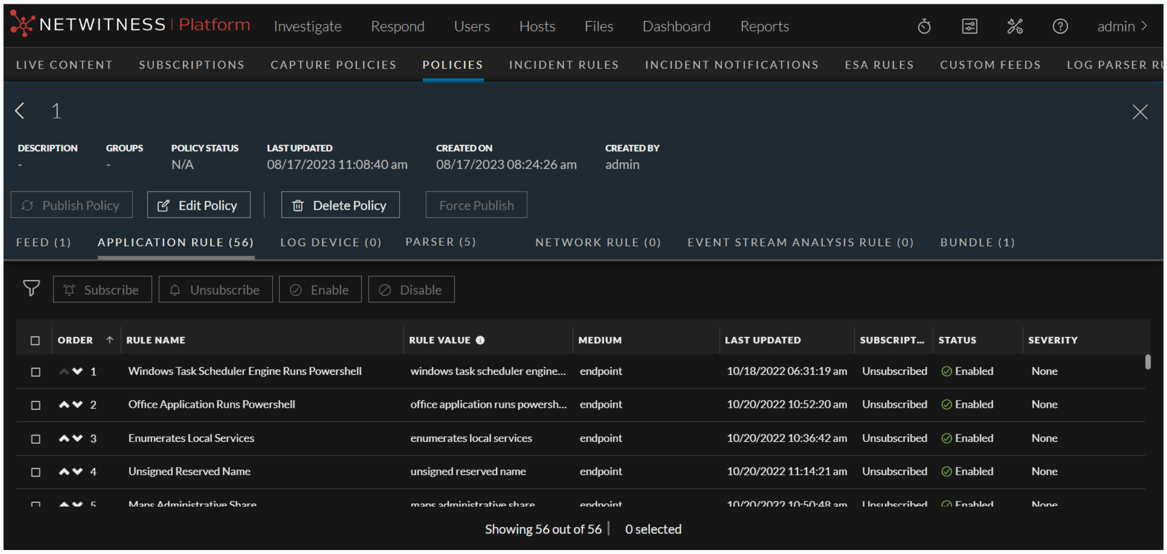
1 - 8 of 8 Policies | 1 selected

None of the Decoder Services are managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

- Publish Policy - Lets you publish all the unpublished and/or failed content. For more information, see Create a policy.
- Edit Policy - Lets you edit the policy. For more information, see Edit a Policy.
- View Details - Lets you view the complete policy details.
- Expand the sections **Overview**, **Application Rule**, **Bundle**, **Feed**, **Lua Parse**r and **History** to view the details of the policy.
- The table contains details such as **Policy Version**, **Version Name** and **Published By**.

5 Policy Details Panel:

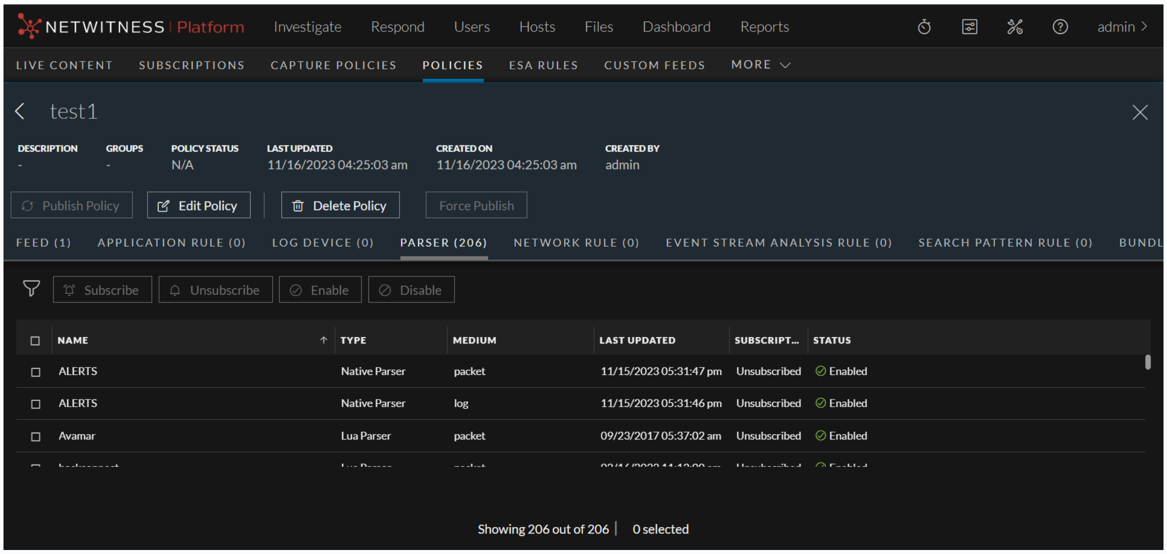


1

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	-	N/A	08/17/2023 11:08:40 am	08/17/2023 08:24:26 am	admin

□	ORDER ↑	RULE NAME	RULE VALUE	MEDIUM	LAST UPDATED	SUBSCRIPT...	STATUS	SEVERITY
□	1	Windows Task Scheduler Engine Runs Powershell	windows task scheduler engine...	endpoint	10/18/2022 06:31:19 am	Unsubscribed	✓ Enabled	None
□	2	Office Application Runs Powershell	office application runs powersh...	endpoint	10/20/2022 10:52:20 am	Unsubscribed	✓ Enabled	None
□	3	Enumerates Local Services	enumerates local services	endpoint	10/20/2022 10:36:42 am	Unsubscribed	✓ Enabled	None
□	4	Unsigned Reserved Name	unsigned reserved name	endpoint	10/20/2022 11:14:21 am	Unsubscribed	✓ Enabled	None
□	5	Maps Administrative Share	maps administrative share	endpoint	10/20/2022 10:50:48 am	Unsubscribed	✓ Enabled	None

Showing 56 out of 56 | 0 selected



test1

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
-	-	N/A	11/16/2023 04:25:03 am	11/16/2023 04:25:03 am	admin

□	NAME ↑	TYPE	MEDIUM	LAST UPDATED	SUBSCRIPT...	STATUS
□	ALERTS	Native Parser	packet	11/15/2023 05:31:47 pm	Unsubscribed	✓ Enabled
□	ALERTS	Native Parser	log	11/15/2023 05:31:46 pm	Unsubscribed	✓ Enabled
□	Avamar	Lua Parser	packet	09/23/2017 05:37:02 am	Unsubscribed	✓ Enabled

Showing 206 out of 206 | 0 selected

Displays the properties of the selected policy.

Toolbar:

- Publish Policy - Lets you publish all the unpublished and/or failed content. For more information, see Create a policy.
- Edit Policy - Lets you edit the policy. For more information, see Edit a Policy.
- Delete Policy - Deletes the selected policy or policies permanently.
- Force Publish - Lets you republish all the content irrespective of the policy status.

Policy Details Pane:

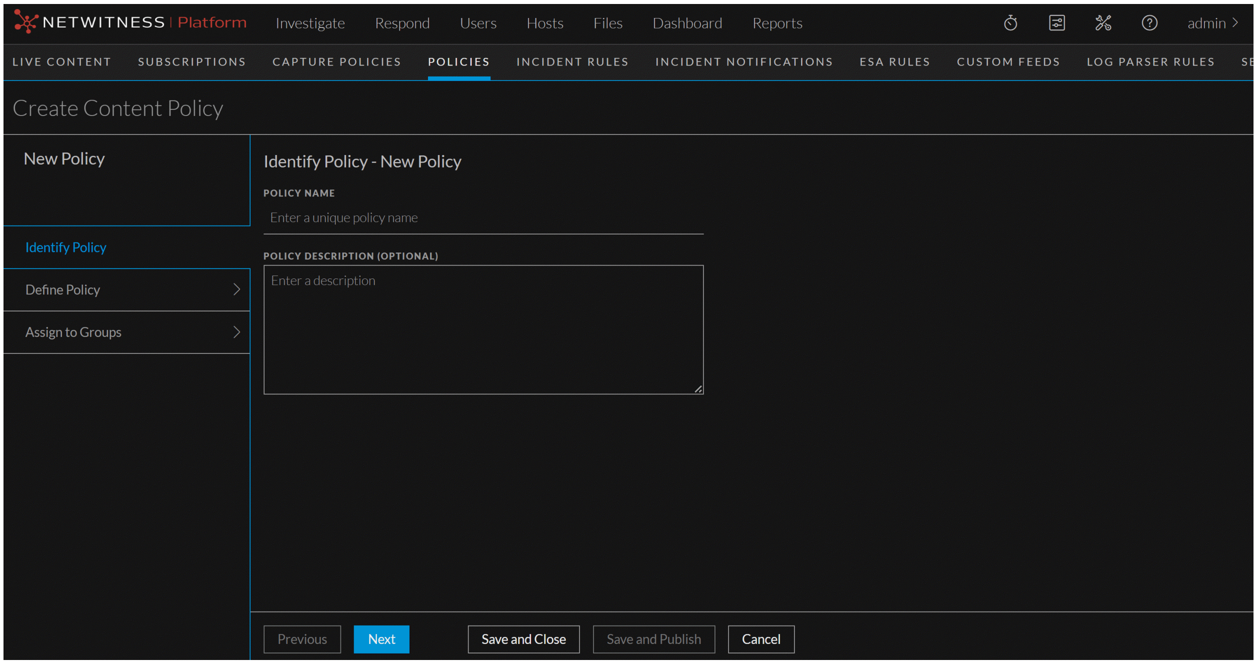
- Order - Order of the content. Click ↑ to sort and display the content in the ascending order.

Click ↓ to sort and display the content in descending order. This field is applicable only for **Application Rule** and **Network Rule** tabs.

- Rule Name - Name of the rule. The rule name will be unique. This field is applicable only for **Application Rule** and **Network Rule** tabs.
- Rule Value - The rule value. It is the value written to the alert meta. The rule value can be duplicate. You can clone existing rules with different rule names, but with same rule value. This field is applicable only for **Application Rule** and **Network Rule** tabs.
- Name - The content name. This field is applicable only for **Feed**, **Log Device** and **Parser** tabs.
- Type - The type of parser. For example, **Lua Parser** or **Native Parser**. This field is applicable only for **Parser** tab.
- Medium - Meta data source medium.
- Severity - The severity of content. For example, **Low**, **Medium**, **High** or **Critical**. This field is applicable only for **Application Rule** and **Event Stream Analysis Rule** tabs.
- Last Updated - Displays the time when the content is last updated.
- Subscription - Indicates if the content is subscribed or unsubscribed.
- Status - The status of resource.
- ▽ - Filter the list of displayed content in the policy details view based on the name, medium, source type, enabled/disabled status, subscription status, severity, resource created date, and last updated date. Following are the fields available in the filter panel:
    - Name - If you set the filter option to **Contains** operator from the drop-down list and start typing the name of the content rules, a list of content rules that contain that character is displayed, as you continue to type the list is filtered to match. If you set the filter option to **Equals** operator from the drop-down list and enter the full name, the particular content type will be displayed.
    - Medium - Select one or more mediums from the drop-down list. The available options are 'endpoint', 'log', 'log and packet' and 'packet'.
    - Source Type - Select one or more sources from the drop-down list. The available options are 'Custom' and 'Live'.
    - Enabled/Disabled Status - Select one or more statuses from the drop-down list. The available options are 'Enabled' and 'Disabled'. This field is not applicable for Event Stream Analysis Rule content type.
    - Subscription - Select one or more statuses from the drop-down list. The available options are 'Subscribed' and 'Unsubscribed'.
    - Severity - Select the severity from the drop-down list. The available options are 'Low', 'Medium', 'High' and 'Critical'. This field is applicable only for Application Rule and ESA content type.
    - Resource Created Date - Select the resource created date range.
    - Last Update Date - Select the last update date range.
- Subscribe - Lets you subscribe for the content if it is unsubscribed.

- Unsubscribe - Lets you unsubscribe for the content if it is subscribed.
- Enable - Lets you enable the content for the policy.
- Disable - Lets you disable the content from the policy.
- ⌄ - Move the content down the order.
- ⌃ - Move the content up the order.

Below is an example of the Create Content Policy dialog.



Create Content Policy

Identify Policy - New Policy

POLICY NAME

Enter a unique policy name

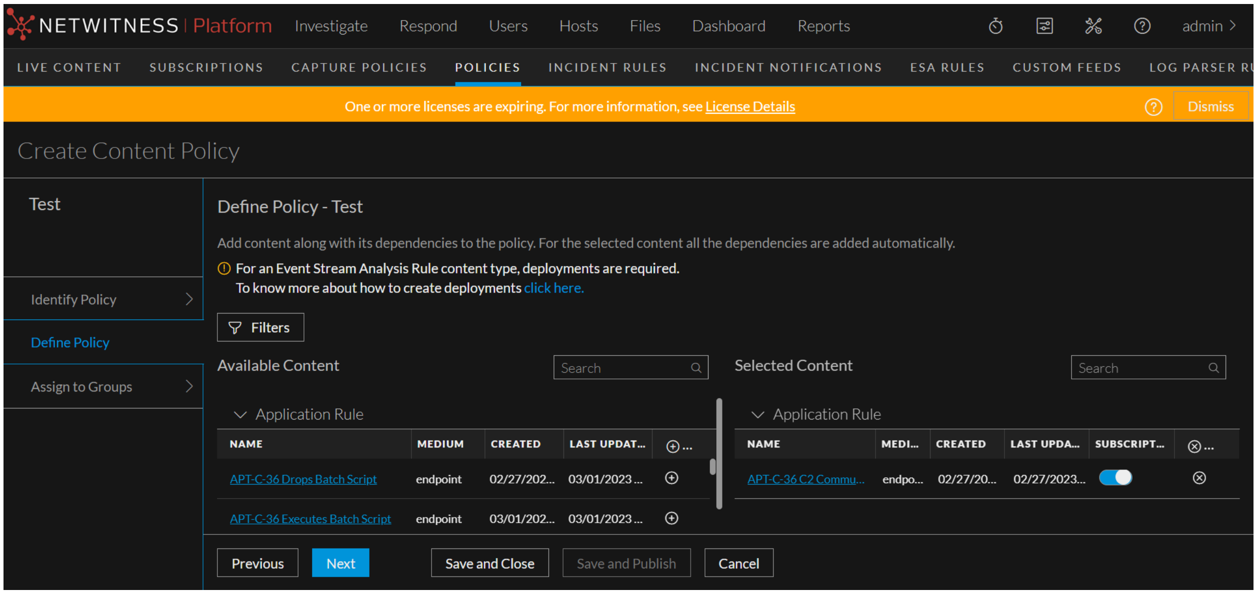
POLICY DESCRIPTION (OPTIONAL)

Enter a description

The table describes the information and options in the Create Policy dialog:

Field	Description
Policy Name	Name of the policy. The name should be unique.
Policy Description (Optional)	Description of the policy. Description should not exceed 8000 characters.

Define Policy Settings:



One or more licenses are expiring. For more information, see License Details

Create Content Policy

Test

Define Policy - Test

Add content along with its dependencies to the policy. For the selected content all the dependencies are added automatically.

ⓘ For an Event Stream Analysis Rule content type, deployments are required.
To know more about how to create deployments click here.

Available Content

Application Rule

NAME	MEDIUM	CREATED	LAST UPDAT...	⊕ ...
APT-C-36 Drops Batch Script	endpoint	02/27/202...	03/01/2023 ...	⊕
APT-C-36 Executes Batch Script	endpoint	03/01/202...	03/01/2023 ...	⊕

Selected Content

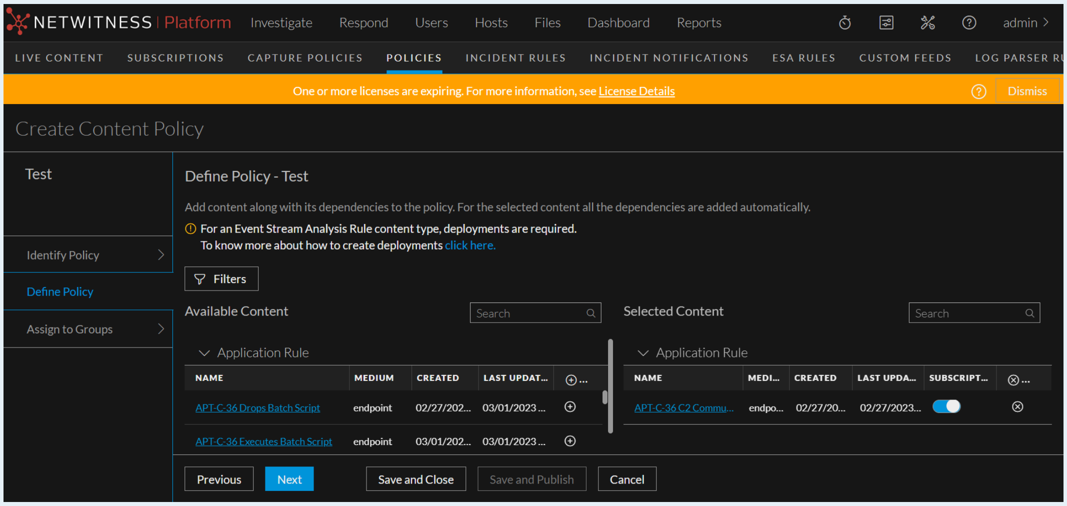
Application Rule

NAME	MEDI...	CREATED	LAST UPDA...	SUBSCRIPT...	⊗ ...
APT-C-36 C2 Commu...	endpo...	02/27/20...	02/27/2023...	●	⊗

Field	Description

Available Content

Displays the available content resources in your deployment. Click > expand the resource type.



One or more licenses are expiring. For more information, see License Details

Create Content Policy

Define Policy - Test

Add content along with its dependencies to the policy. For the selected content all the dependencies are added automatically.

For an Event Stream Analysis Rule content type, deployments are required.
To know more about how to create deployments click here.

Available Content

Application Rule

NAME	MEDIUM	CREATED	LAST UPDAT...	⊕ ...
APT-C-36 Drops Batch Script	endpoint	02/27/202...	03/01/2023 ...	⊕
APT-C-36 Executes Batch Script	endpoint	03/01/202...	03/01/2023 ...	⊕

Selected Content

Application Rule

NAME	MEDI...	CREATED	LAST UPDA...	SUBSCRIPT...	⊗ ...
APT-C-36 C2 Commu...	endpo...	02/27/20...	02/27/2023...	●	⊗

The following describes resource type:

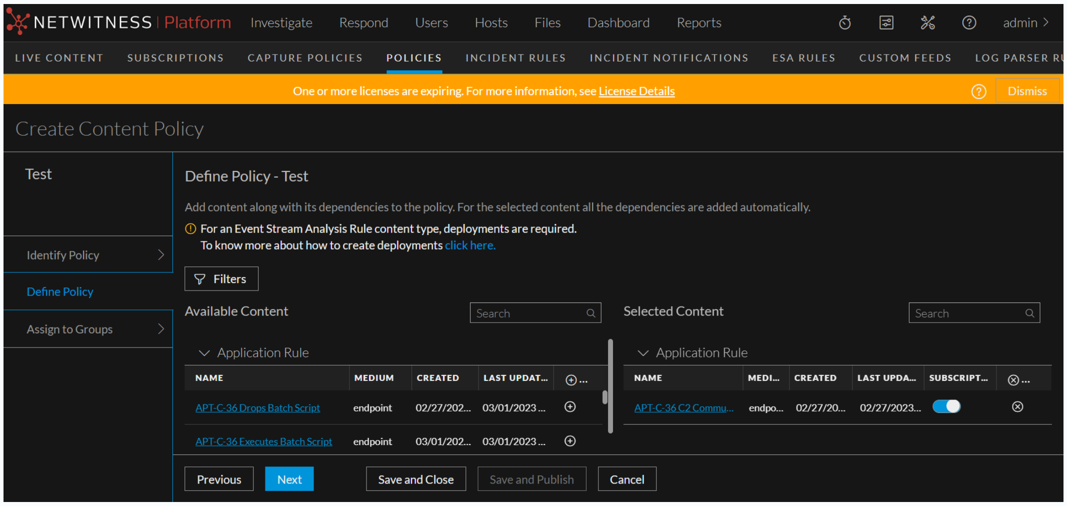
- Name - Name of the resource.
- Medium - Meta data source medium. Available values for medium are as follows:
  - **Endpoint**: applied to content that uses meta derived from endpoint agent and endpoint server data
  - **Log**: applied to content that uses meta derived from log data
  - **Packet**: applied to content that uses meta derived from network packets
  - **Log and packet**: applied to content that correlates meta derived across log and packet data
- Created - Displays the time when the resource is created
- Last Updated - Displays the time when the resource is updated last.
- Action- Click + to add the resource and its dependencies to your deployment.
- ⊕ ALL - Click to add all content based on the resource type.
- ▽ - Filter the available content based on the following parameters:
  - **Resource Types -** The resource or the content type.
  - **Medium** - Meta data source medium. Available values for medium are as follows:
    - **Endpoint**: Applied to content that uses meta derived from endpoint agent and endpoint server data
    - **Log**: Applied to content that uses meta derived from log data
    - **Packet**: Applied to content that uses meta derived from network packets
    - **Log and packet**: Applied to content that correlates meta derived across log and packet data

  - **Resource Created Date** - The date on which the content was created.
  - **Resource Modified Date** - The date on which the content was modified.
  - **Reset** - Reset the fields.
- **Search** - Conveniently search the available content.

Selected Content

Lists the selected resource.

Additionally, you can subscribe the content. Once the content is subscribed, the content resources are updated automatically in case of any changes.



One or more licenses are expiring. For more information, see License Details

Create Content Policy

Test

Define Policy - Test

Add content along with its dependencies to the policy. For the selected content all the dependencies are added automatically.

For an Event Stream Analysis Rule content type, deployments are required.
To know more about how to create deployments click here.

Available Content

Application Rule

NAME	MEDIUM	CREATED	LAST UPDAT...	⊕ ...
APT-C-36 Drops Batch Script	endpoint	02/27/202...	03/01/2023 ...	⊕
APT-C-36 Executes Batch Script	endpoint	03/01/202...	03/01/2023 ...	⊕

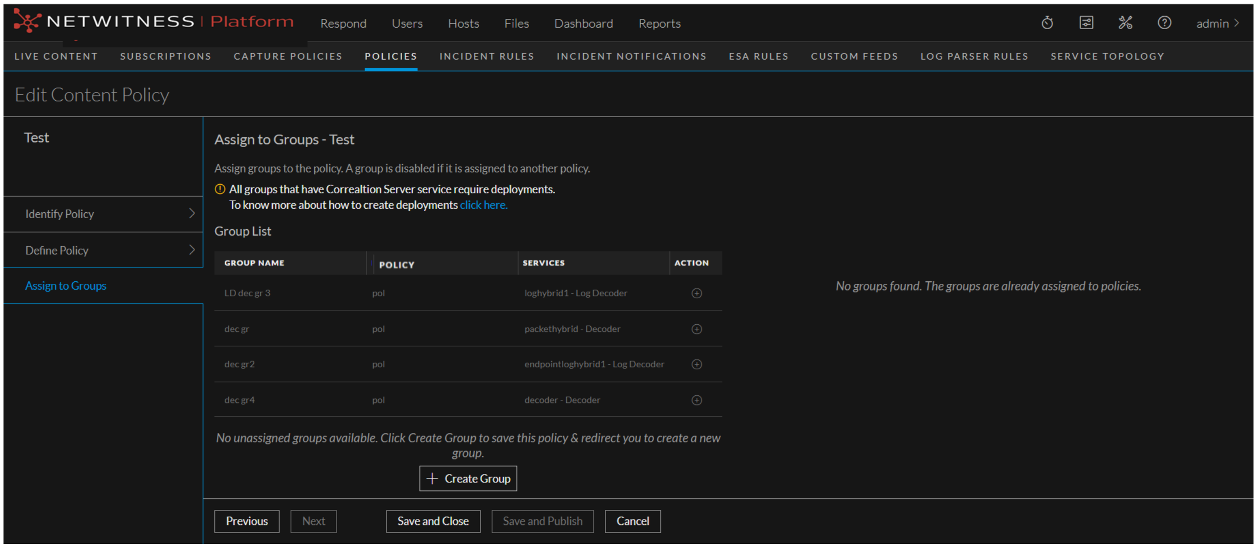
Selected Content

Application Rule

NAME	MEDI...	CREATED	LAST UPDA...	SUBSCRIPT...	⊗ ...
APT-C-36 C2 Commu...	endpo...	02/27/20...	02/27/2023...	●	⊗

- ▽ - Filter the selected content based on the following parameters:
  - **Resource Types** - The resource or the content type.
  - **Medium** - Meta data source medium. Available values for medium are as follows:
    - **Endpoint**: Applied to content that uses meta derived from endpoint agent and endpoint server data
    - **Log**: Applied to content that uses meta derived from log data
    - **Packet**: Applied to content that uses meta derived from network packets
    - **Log and packet**: Applied to content that correlates meta derived across log and packet data
  - **Resource Created Date** - The date on which the content was created.
  - **Resource Modified Date** - The date on which the content was modified.
  - **Reset** - Reset the fields.
- **Search** - Conveniently search the selected content.

Assign to Group:



Assign to Groups - Test

Assign groups to the policy. A group is disabled if it is assigned to another policy.

ⓘ All groups that have Correaltion Server service require deployments.
To know more about how to create deployments click here.

Group List

GROUP NAME	POLICY	SERVICES	ACTION
LD dec gr 3	pol	loghybrid1 - Log Decoder	⊕
dec gr	pol	packethybrid - Decoder	⊕
dec gr2	pol	endpointloghybrid1 - Log Decoder	⊕
dec gr4	pol	decoder - Decoder	⊕

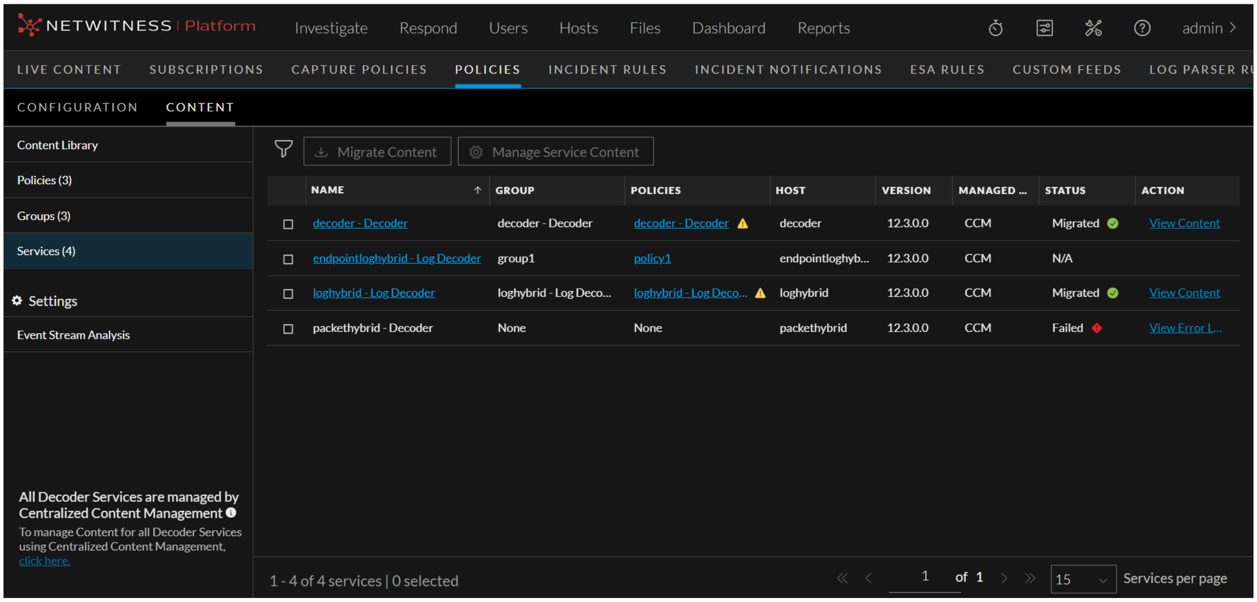
No unassigned groups available. Click Create Group to save this policy & redirect you to create a new group.

No groups found. The groups are already assigned to policies.

Group List	Displays the list of groups associated with the policy. A group is disabled if it is already assigned to another policy. • Group Name • Policies • Services • Action
+ Create Grou	Click to create new group.
Selected Group	Lists the selected groups. Click ⊕ to add groups.
Save and Close	Saves the settings and closes the Create Policy dialog.
Save and Publish	Saves and publishes the created policy. **Note:** This option is disabled if: - Policy settings are not customized. - Policy is not assigned to groups.

Services Tab

The (CONFIGURE) > **Policies** view contains two tabs: **Configuration** and **Content**. The **CONTENT** tab has **Content Library**, **Policies**, **Groups** and **Services** on the left panel. Below is an example of the Content > Services tab:



	NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	decoder - Decoder	decoder - Decoder	decoder - Decoder ⚠	decoder	12.3.0.0	CCM	Migrated ✓	View Content
□	endpointloghybrid - Log Decoder	group1	policy1	endpointloghyb...	12.3.0.0	CCM	N/A	
□	loghybrid - Log Decoder	loghybrid - Log Deco...	loghybrid - Log Deco... ⚠	loghybrid	12.3.0.0	CCM	Migrated ✓	View Content
□	packethybrid - Decoder	None	None	packethybrid	12.3.0.0	CCM	Failed ◆	View Error L...

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 4 of 4 services | 0 selected

1 of 1

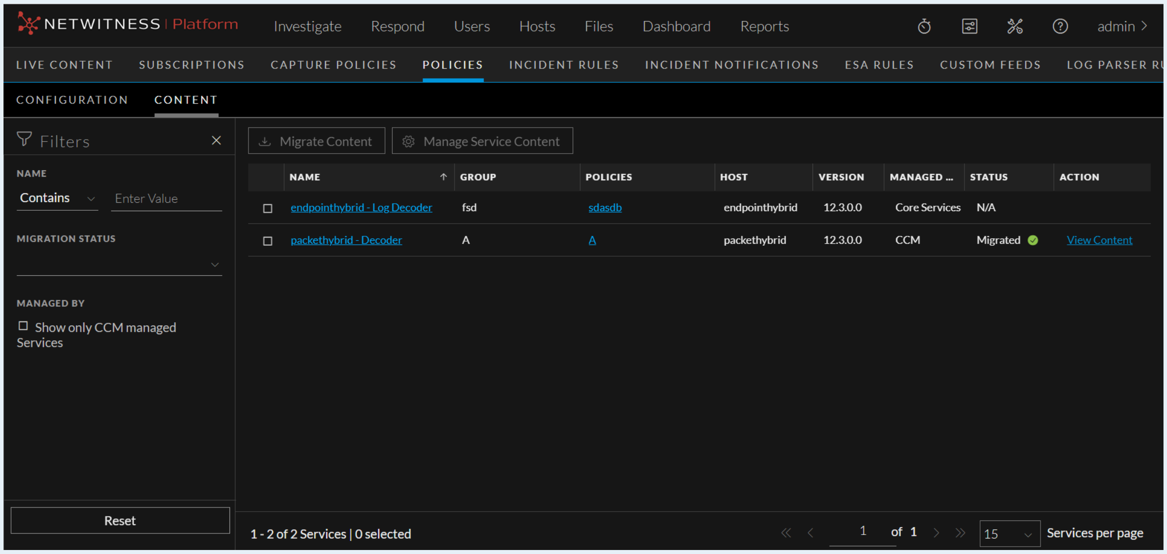
15

By default, 15 services are displayed per page. To go to the next page, click ›. To go to the last page, click ».

1 Toolbar

- Migrate Content - Lets you migrate content from service. For more information, see Migrate Content from Service.
- Manage Service Content - Lets you enable or disable CCM for individual service(s). For more information, see Enable or Disable CCM for Individual Decoder Services.

2 - Filter services based on various parameters.



	NAME	GROUP	POLICIES	HOST	VERSION	MANAGED ...	STATUS	ACTION
□	endpointhybrid - Log Decoder	fsd	sdasdb	endpointhybrid	12.3.0.0	Core Services	N/A	
□	packethybrid - Decoder	A	A	packethybrid	12.3.0.0	CCM	Migrated ✓	View Content

1 - 2 of 2 Services | 0 selected

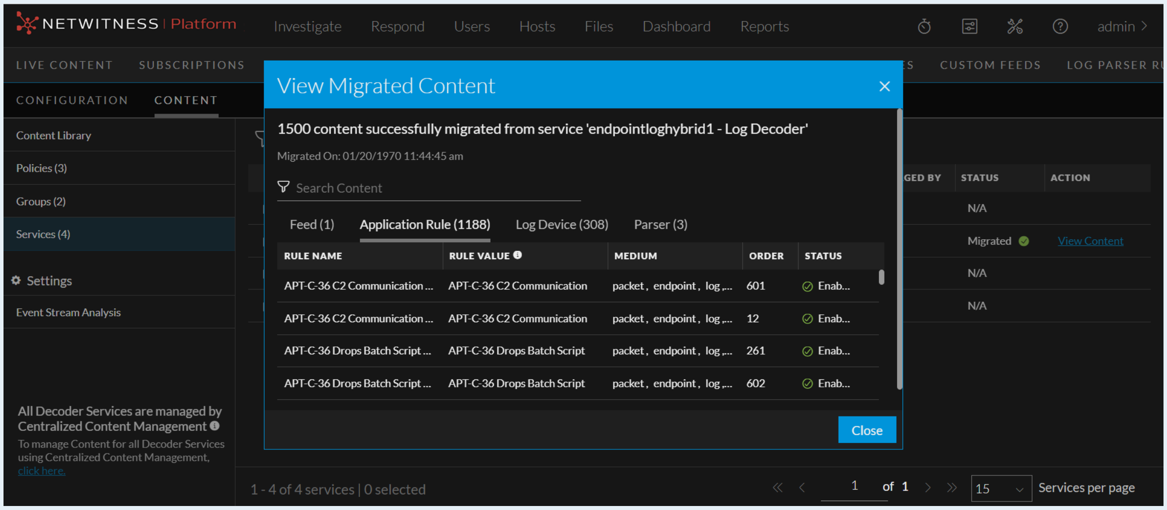
Filter Panel:

- Name - Select the **Name** drop-down value as either **Equals** or **Contains**. To search the service name using the **Contains** operator, set the filter option to **Contains** operator from the drop-down list and start typing the name of the service. Type one character and a list of service that contain that character is displayed, as you continue to type, the list is filtered to match. To search the service name using the **Equals** operator, set the filter option to **Equals** operator from the drop-down list and enter the full name. The particular service name will be displayed.
- Migration Status - The **Migration Status** drop-down value. The drop-down values are 'Migrated', 'Migrating', 'Failed' and 'NA'.
- Managed By - Select the **Show only CCM Managed Services** to display only the CCM managed services.
- Reset - Reset the fields.

3 Services List Pane:

- Name - Name of the service.
- Group - The group to which service belongs.
- Policies - The policy to which the service is assigned. Click the policy name to view the details of the policy.
- Host - The service host name .
- Version - The service version number.
- Managed By - Indicates if the service is managed by CCM or Core Services.
- Status - Displays the migration status of the service. The column displays the following values based on the status of migration:
    - Queued
    - Initializing
    - Analyzing Content
    - Migrating Content
    - Migrated
    - Failed
- Action - Displays the action on the migrated content. The following actions are available:
    - View Content - If the **Status** is 'Migrated'.
    - View Error Log - If the **Status** is 'Failed'.

4 View Content - Click the hyperlink under the **Action** column to view the migrated content details in the **View Migrated Content** Pop-up window.



1500 content successfully migrated from service 'endpointloghybrid1 - Log Decoder'

Migrated On: 01/20/1970 11:44:45 am

RULE NAME	RULE VALUE	MEDIUM	ORDER	STATUS
APT-C-36 C2 Communication ...	APT-C-36 C2 Communication	packet , endpoint , log ,...	601	Enab...
APT-C-36 C2 Communication ...	APT-C-36 C2 Communication	packet , endpoint , log ,...	12	Enab...
APT-C-36 Drops Batch Script ...	APT-C-36 Drops Batch Script	packet , endpoint , log ,...	261	Enab...
APT-C-36 Drops Batch Script ...	APT-C-36 Drops Batch Script	packet , endpoint , log ,...	602	Enab...

All Decoder Services are managed by Centralized Content Management
To manage Content for all Decoder Services using Centralized Content Management, click here.

Available Tabs in the **View Migrated Content** Pop-up Window:

- Feed
- Application Rule
- Network Rule
- Log Device
- LUA Parser

Note:
- **Network Rules** tab is not applicable or Log Decoders.
- **Log Device** tab is not applicable for Decoders.

IMPORTANT: During the process of migration, if a Decoder that is being migrated contains multiple application rules and/or network rules with the exact same rule name and rule condition, only one of those rules will be retained in the service. The remaining rules will be considered duplicates and removed. Therefore, post migration, none of the migrated services will have multiple rules with the same rule name and the same rule value.

- Search the migrated content based on various parameters.

Note:
- For Application Rule and Network Rule, the search is based on **Rule Name** and **Rule Value**.
- For Feeds, Log Device and LUA Parser, the search is based on the **Name**.

Content Details for Feeds, Log Device and LUA Parser:

- Name - The content name.
- Medium - Meta data source medium.
- Status - The status of resource. For example, Enabled or Disabled.

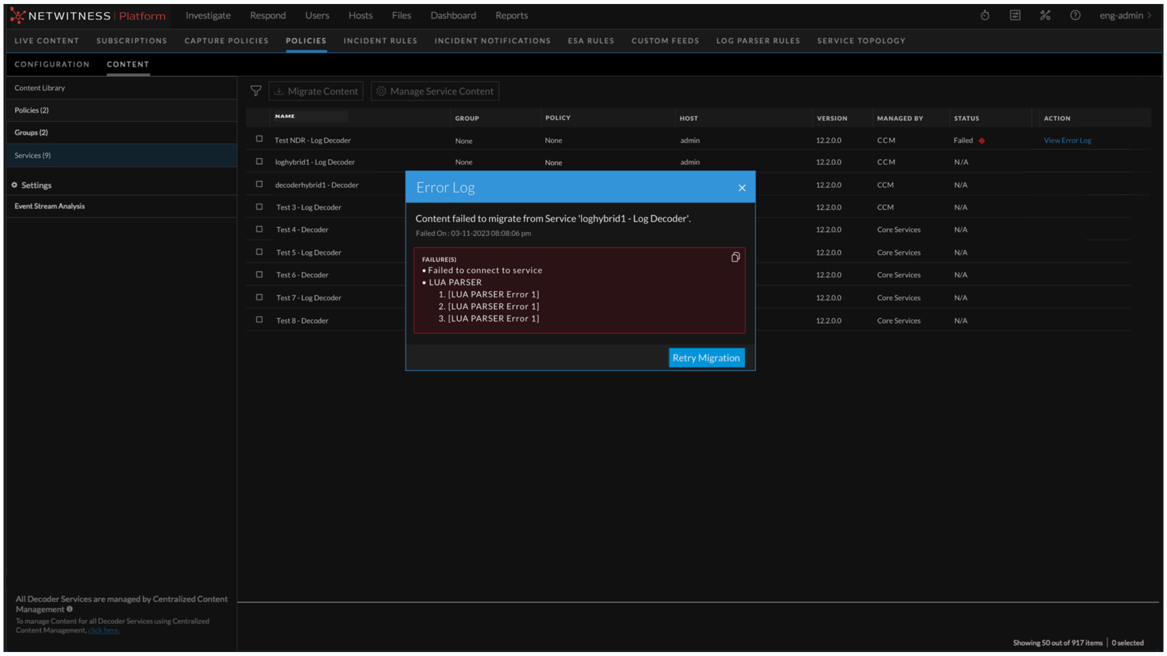
Content Details for Application Rule and Network Rule:

- Rule Name - Name of the rule. The rule name will be unique.
- Rule Value - The rule value. It is the value written to the alert meta. The rule value can be duplicate. You can clone existing rules with different rule names, but with same rule value.
- Medium - Meta data source medium.
- Order - The order of rule.
- Status - The status of resource. The status of resource. For example, Enabled or Disabled.

Available button in the **View Migrated Content** Pop-up Window:

- Close - Close the pop-up window and return to **Service List** page.

5 View Error Log - Click the hyperlink under the **Action** column to view the log details in case the migration is failed.



	NAME	GROUP	POLICY	HOST	VERSION	MANAGED BY	STATUS	ACTION
□	Test NDR - Log Decoder	None	None	admin	12.2.0.0	CCM	Failed ◆	View Error Log
□	loghybrid1 - Log Decoder	None	None	admin	12.2.0.0	CCM	N/A	
□	decoderhybrid1 - Decoder				12.2.0.0	CCM	N/A	
□	Test 3 - Log Decoder				12.2.0.0	CCM	N/A	
□	Test 4 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 5 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 6 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 7 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 8 - Decoder				12.2.0.0	Core Services	N/A	

Error Log

Content failed to migrate from Service 'loghybrid1 - Log Decoder'.

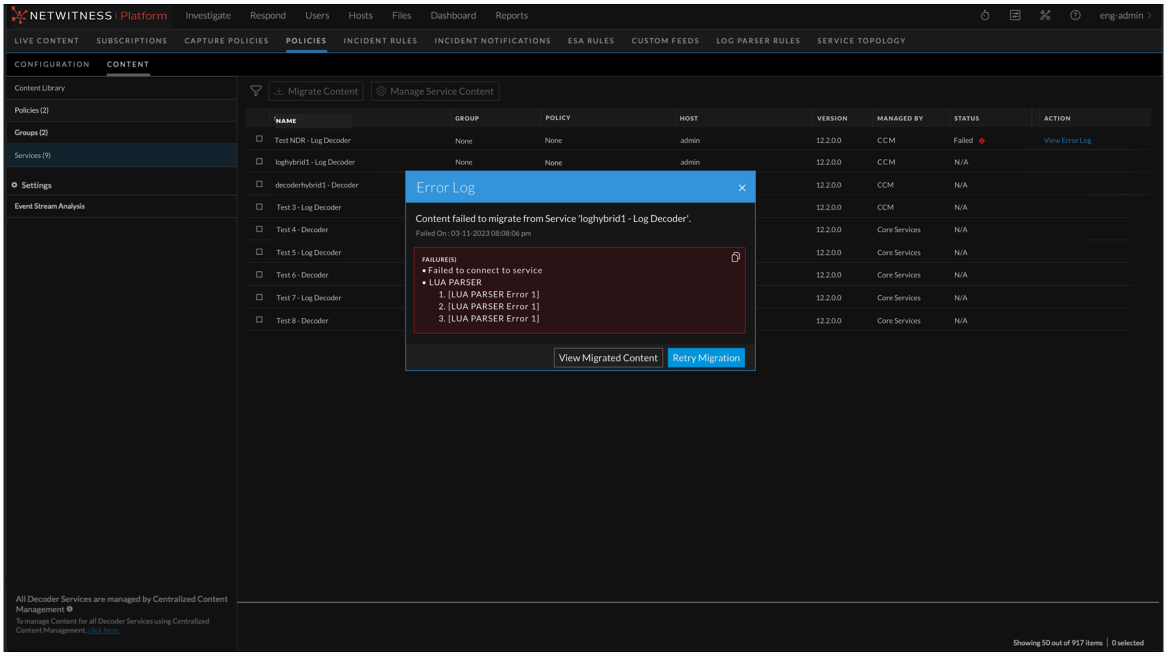
Failed On : 03-11-2023 08:08:06 pm

```
FAILURE(S)
• Failed to connect to service
• LUA PARSER
    1. [LUA PARSER Error 1]
    2. [LUA PARSER Error 1]
    3. [LUA PARSER Error 1]
```

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 50 out of 917 items | 0 selected



	NAME	GROUP	POLICY	HOST	VERSION	MANAGED BY	STATUS	ACTION
□	Test NDR - Log Decoder	None	None	admin	12.2.0.0	CCM	Failed ◆	View Error Log
□	loghybrid1 - Log Decoder	None	None	admin	12.2.0.0	CCM	N/A	
□	decoderhybrid1 - Decoder				12.2.0.0	CCM	N/A	
□	Test 3 - Log Decoder				12.2.0.0	CCM	N/A	
□	Test 4 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 5 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 6 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 7 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 8 - Decoder				12.2.0.0	Core Services	N/A	

Error Log

Content failed to migrate from Service 'loghybrid1 - Log Decoder'.

Failed On : 03-11-2023 08:08:06 pm

```
FAILURE(S)
• Failed to connect to service
• LUA PARSER
    1. [LUA PARSER Error 1]
    2. [LUA PARSER Error 1]
    3. [LUA PARSER Error 1]
```

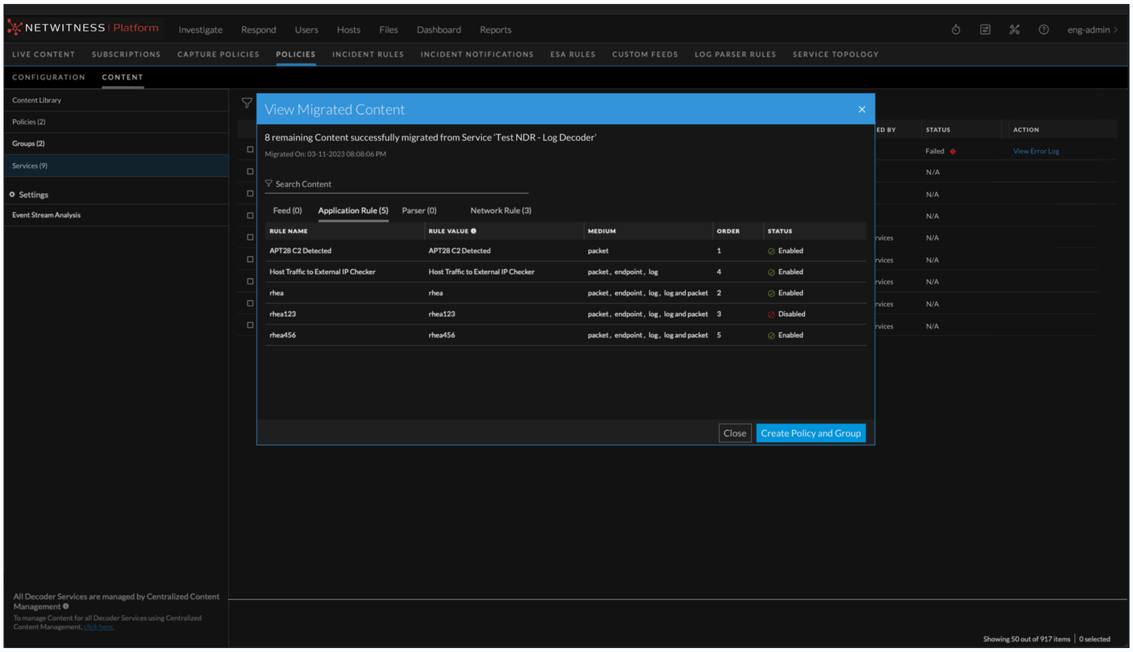
All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 50 out of 917 items | 0 selected

Available buttons and Icons in the **Error Log** Pop-up Window:

- ⧉ - Copy the error logs.
- View Migrated Content - Click to View the content that have been migrated successfully. This button is present only in case of partial migration.



View Migrated Content

8 remaining Content successfully migrated from Service 'Test NDR - Log Decoder'

Migrated On: 03-11-2023 08:08:06 PM

RULE NAME	RULE VALUE	MEDIUM	ORDER	STATUS
APT28 C2 Detected	APT28 C2 Detected	packet	1	✓ Enabled
Host Traffic to External IP Checker	Host Traffic to External IP Checker	packet, endpoint, log	4	✓ Enabled
rhea	rhea	packet, endpoint, log, log and packet	2	✓ Enabled
rhea123	rhea123	packet, endpoint, log, log and packet	3	⊘ Disabled
rhea456	rhea456	packet, endpoint, log, log and packet	5	✓ Enabled

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

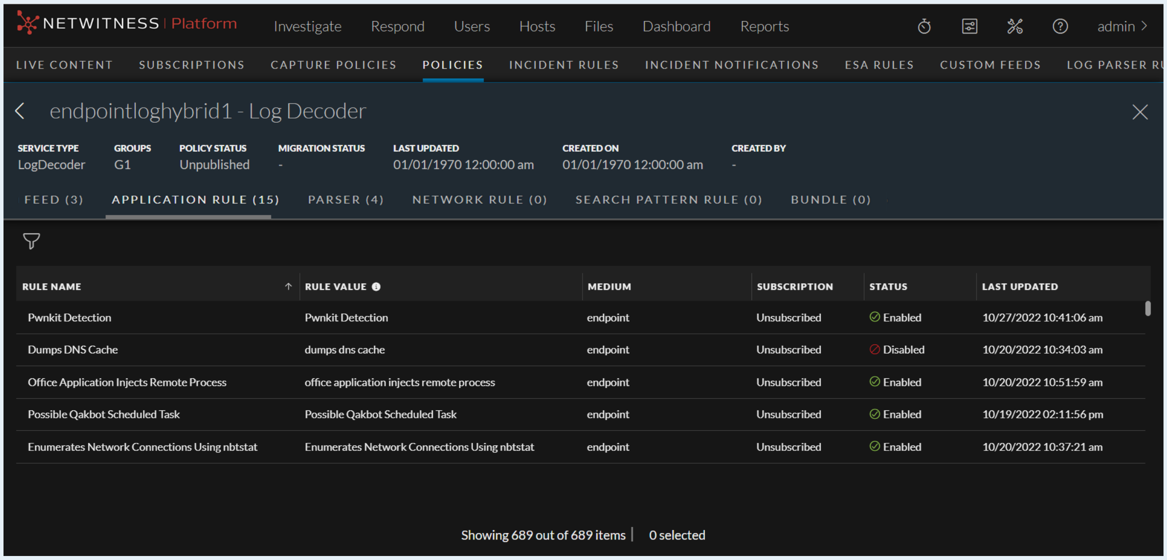
Showing 50 out of 917 items | 0 selected

Available buttons and Icons in the **View Migrated Content** Pop-up Window:

- ○ Close - Closes the pop-up window.
- ○ Create Policy and Group - Creates policy and group for the partially migrated service.

- Retry migration - Retry migration.

6 Service Details Panel:



endpointloghybrid1 - Log Decoder

SERVICE TYPE	GROUPS	POLICY STATUS	MIGRATION STATUS	LAST UPDATED	CREATED ON	CREATED BY
LogDecoder	G1	Unpublished	-	01/01/1970 12:00:00 am	01/01/1970 12:00:00 am	-

RULE NAME ↑	RULE VALUE	MEDIUM	SUBSCRIPTION	STATUS	LAST UPDATED
Pwnkit Detection	Pwnkit Detection	endpoint	Unsubscribed	✓ Enabled	10/27/2022 10:41:06 am
Dumps DNS Cache	dumps dns cache	endpoint	Unsubscribed	⊘ Disabled	10/20/2022 10:34:03 am
Office Application Injects Remote Process	office application injects remote process	endpoint	Unsubscribed	✓ Enabled	10/20/2022 10:51:59 am
Possible Qakbot Scheduled Task	Possible Qakbot Scheduled Task	endpoint	Unsubscribed	✓ Enabled	10/19/2022 02:11:56 pm
Enumerates Network Connections Using nbtstat	Enumerates Network Connections Using nbtstat	endpoint	Unsubscribed	✓ Enabled	10/20/2022 10:37:21 am

Showing 689 out of 689 items | 0 selected

Displays the properties of the selected service.

Toolbar:

- Service Type - The type of service. For example, LogDecoder.
- Groups - The groups associated with the service.
- Policy Status -Indicates if the policy associated with the service is published or unpublished.
- Migration Status - The migration status of the service content.
- Last Updated - The date and time stamp on which the service was last updated.
- Created On - The date and time stamp on which the service was created.
- Created By - The user ID of the user who has created the service.

Available Content Tabs:

- Feed
- Application Rule
- Log Device. This tab is not applicable for service type 'Packet Decoder'.
- LUA Parser
- Network Rule. This tab is not applicable for service type 'LogDecoder'.
- Bundle

Service Details Pane for Feeds, Log Device, LUA Parser and Bundle:

- Name - The content name.
- Medium - Meta data source medium.
- Last Updated - Displays the time when the content is last updated.

- Subscription - Indicates if the content is subscribed or unsubscribed.
- Status - The status of resource.

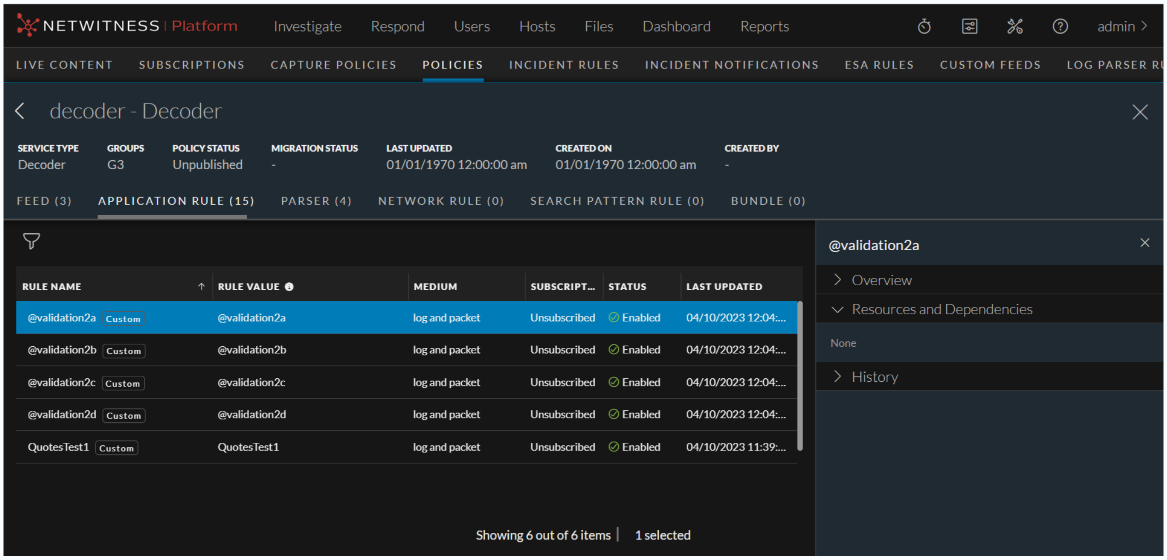
Service Details Pane for Application Rule and Network Rule:

- Rule Name - Name of the rule. The rule name will be unique.
- Rule Value - The rule value. It is the value written to the alert meta. The rule value can be duplicate. You can clone existing rules with different rule names, but with same rule value.
- Medium - Meta data source medium.
- Last Updated - Displays the time when the content is last updated.
- Subscription - Indicates if the content is subscribed or unsubscribed.
- Status - The status of resource.

⏷ - Filter the content based on various parameters.

7 Service Details Right Panel:

Displays the complete content details such as **Overview**, **Resources and Dependencies** and **History**.



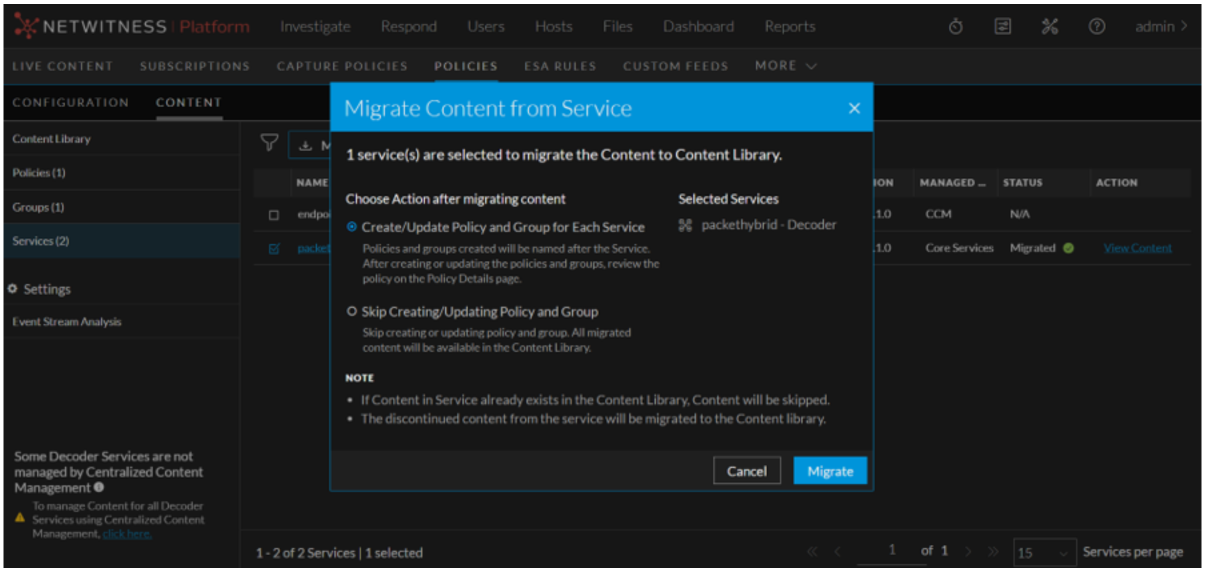
SERVICE TYPE	GROUPS	POLICY STATUS	MIGRATION STATUS	LAST UPDATED	CREATED ON	CREATED BY
Decoder	G3	Unpublished	-	01/01/1970 12:00:00 am	01/01/1970 12:00:00 am	-

RULE NAME	RULE VALUE	MEDIUM	SUBSCRIPT...	STATUS	LAST UPDATED
@validation2a Custom	@validation2a	log and packet	Unsubscribed	✓ Enabled	04/10/2023 12:04:...
@validation2b Custom	@validation2b	log and packet	Unsubscribed	✓ Enabled	04/10/2023 12:04:...
@validation2c Custom	@validation2c	log and packet	Unsubscribed	✓ Enabled	04/10/2023 12:04:...
@validation2d Custom	@validation2d	log and packet	Unsubscribed	✓ Enabled	04/10/2023 12:04:...
QuotesTest1 Custom	QuotesTest1	log and packet	Unsubscribed	✓ Enabled	04/10/2023 11:39:...

Showing 6 out of 6 items | 1 selected

Migrate Content from Service dialog:

Below is an example of the Migrate Content from Service dialog:



Migrate Content from Service

1 service(s) are selected to migrate the Content to Content Library.

Choose Action after migrating content

● Create/Update Policy and Group for Each Service

Policies and groups created will be named after the Service. After creating or updating the policies and groups, review the policy on the Policy Details page.

○ Skip Creating/Updating Policy and Group

Skip creating or updating policy and group. All migrated content will be available in the Content Library.

Selected Services

packethybrid - Decoder

NOTE

- If Content in Service already exists in the Content Library, Content will be skipped.
- The discontinued content from the service will be migrated to the Content library.

	NAME	...ION	MANAGED ...	STATUS	ACTION
□	endpo...	...1.0	CCM	N/A	
☑	packet...	...1.0	Core Services	Migrated ●	View Content

Some Decoder Services are not managed by Centralized Content Management

⚠ To manage Content for all Decoder Services using Centralized Content Management, click here.

1 - 2 of 2 Services | 1 selected

1 of 1 15 Services per page

Note:
- If you select **Create/Update Policy and Group for Each Service**, policy and group will be the created or updated for each service selected for migration. Once the migration process is complete, the policy and group will be listed under the respective pages.
- The policy and group which is created or updated for the service will be in 'Unpublished' state and it can be published only after it is reviewed. In the **Policy Listing** page, the **Publish** button for such a policy will be disabled. The policy can be published only after reviewing it either from **Policy Details** page or **Edit Policy** Page. When the policy or group gets updated with the new content, the order of the new content will be given priority.
- If you select **Skip Creating/Updating Policy and Group**, only the content will be migrated. All the migrated content will be available in Content Library.

For more details on publishing a policy, refer Create and Publish Policies feature.

For more details on editing a policy, refer Edit a Policy feature.

For more details on policy details, refer View a Policy feature.

For more details on editing a group, refer Edit a Group feature.

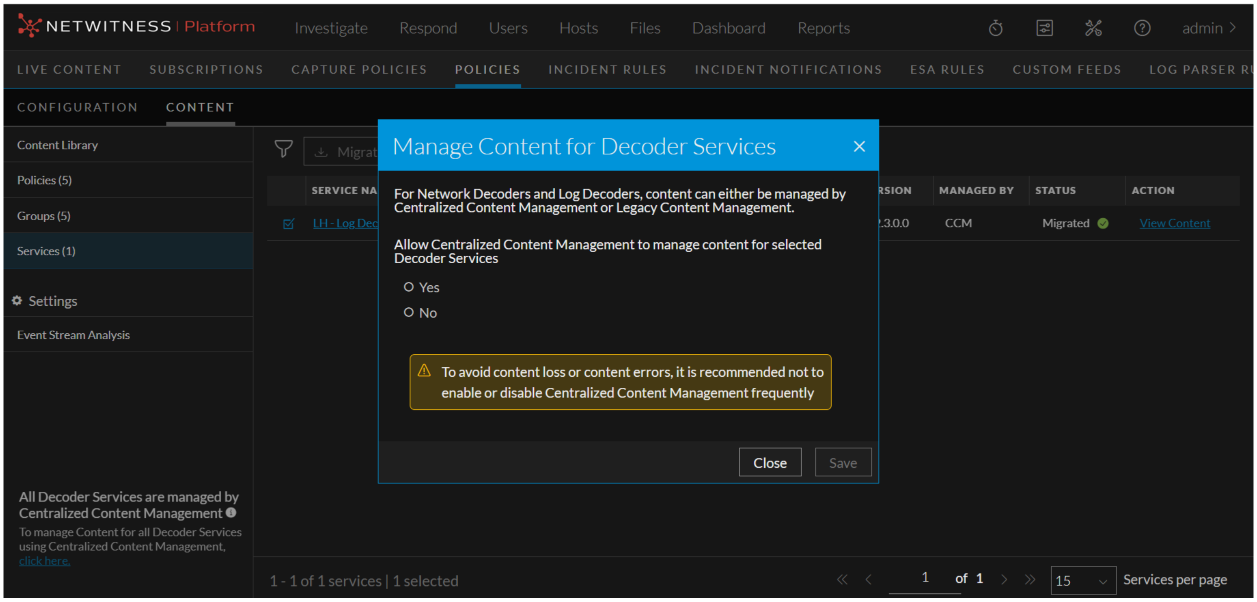
For more details on group details, refer View a Group feature.

The table describes the information and options in the Migrate Content from Service dialog:

Field	Description
Migrate	Initiate the migration of content for the selected service.
Cancel	Cancels the operation.

Manage Content for Decoder Services dialog:

Below is an example of the Manage Content for Decoder Services dialog:



All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Manage Content for Decoder Services

For Network Decoders and Log Decoders, content can either be managed by Centralized Content Management or Legacy Content Management.

Allow Centralized Content Management to manage content for selected Decoder Services

○ Yes

○ No

⚠ To avoid content loss or content errors, it is recommended not to enable or disable Centralized Content Management frequently

1 - 1 of 1 services | 1 selected

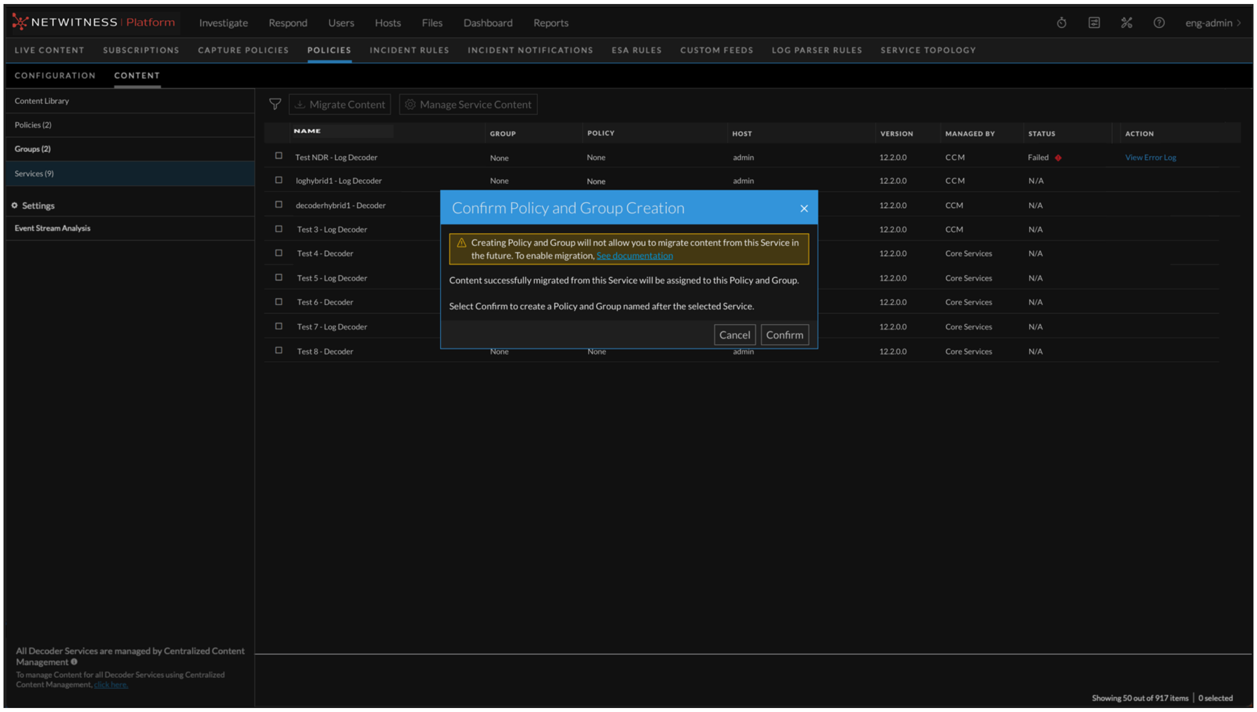
1 of 1

The table describes the information and options in the Manage Content for Decoder Services dialog:

Field	Description
Allow Centralized Content Management to Manage Content for Selected Decoder Services	Select **Yes** to enable CCM for selected service(s). Select **No** to disable CCM for selected service(s).
Save	Save the changes.
Close	Close the **Manage Content for Decoder Services** pop-up window.

Confirm Policy and Group Creation dialog:

Below is an example of the Confirm Policy and Group Creation dialog:



	NAME	GROUP	POLICY	HOST	VERSION	MANAGED BY	STATUS	ACTION
□	Test NDR - Log Decoder	None	None	admin	12.2.0.0	CCM	Failed ◆	View Error Log
□	loghybrid1 - Log Decoder	None	None	admin	12.2.0.0	CCM	N/A	
□	decoderhybrid1 - Decoder				12.2.0.0	CCM	N/A	
□	Test 3 - Log Decoder				12.2.0.0	CCM	N/A	
□	Test 4 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 5 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 6 - Decoder				12.2.0.0	Core Services	N/A	
□	Test 7 - Log Decoder				12.2.0.0	Core Services	N/A	
□	Test 8 - Decoder	None	None	admin	12.2.0.0	Core Services	N/A	

Confirm Policy and Group Creation

⚠ Creating Policy and Group will not allow you to migrate content from this Service in the future. To enable migration, See documentation

Content successfully migrated from this Service will be assigned to this Policy and Group.

Select Confirm to create a Policy and Group named after the selected Service.

All Decoder Services are managed by Centralized Content Management

To manage Content for all Decoder Services using Centralized Content Management, click here.

Showing 50 out of 917 items | 0 selected

The table describes the information and options in the Confirm Policy and Group Creation dialog dialog:

Field	Description
Cancel	Close the pop-up window and cancel the policy and group creation for the partially migrated service.
Confirm	Creates the policy and group for the partially migrated service. The policy and group will be listed under the Policy Listing and Group Listing pages.

Appendix A: Endpoint Risk Scoring Rules

Endpoint risk scoring requires the following content:

- "accesses administrative share using command shell"
- "activates bits job"
- "adds files to bits download job"
- "adds firewall rule"
- "allocates remote memory"
- "antivirus disabled"
- "archiving software reads multiple documents"
- "autorun debian package mismatch"
- "autorun file path not part of debian package"
- "autorun file path not part of rpm"
- "autorun key contains non-printable characters"
- "autorun"
- "autorun rpm mismatch"
- "autorun unsigned active setup"
- "autorun unsigned appinit_dlls"
- "autorun unsigned bho"
- "autorun unsigned bootexecute registry startup method"
- "autorun unsigned explorer registry startup method"
- "autorun unsigned hidden"
- "autorun unsigned hidden only executable in directory"
- "autorun unsigned ie toolbar"
- "autorun unsigned in appdatalocal directory"
- "autorun unsigned in appdataroaming directory"
- "autorun unsigned in programdata directory"
- "autorun unsigned in temp directory"
- "autorun unsigned logontype registry startup method"

- "autorun unsigned lsa provider"
- "autorun unsigned servicedll"
- "autorun unsigned winlogon helper dll"
- "autorun unsigned winsock lsp"
- "bad certificate warning disabled"
- "blacklisted file"
- "browser runs command prompt"
- "browser runs mshta"
- "browser runs powershell"
- "builds script incrementally"
- "clears application event log"
- "clears event logs using powershell"
- "clears security event log"
- "clears setup event log"
- "clears system event log"
- "combines binaries using command prompt"
- "command line usage of archiving software"
- "command line writes script files"
- "command prompt obfuscation"
- "command prompt obfuscation using value extraction"
- "command shell runs rundll32"
- "completes bits download job"
- "configures image hijacking"
- "configures port redirection"
- "copies binary over administrative share"
- "created in last month"
- "creates browser extension"
- "creates domain user account"
- "creates executable in startup directory"
- "creates local driver service"

- "creates local service"
- "creates local task"
- "creates local user account"
- "creates password-protected archive"
- "creates recursive archive"
- "creates remote process using wmi command-line tool"
- "creates remote service"
- "creates remote task"
- "creates run key"
- "creates shadow volume for logical drive"
- "creates suspicious service running command prompt"
- "debian package hash mismatch in important system directory"
- "debian package hash mismatch"
- "deletes backup catalog"
- "deletes firewall rule"
- "deletes shadow volume copies"
- "deletes shadow volume copies using powershell"
- "deletes usn change journal"
- "disables event logging service"
- "disables firewall"
- "disables safe mode"
- "disables security service"
- "disables startup repair"
- "disables uac"
- "disables uac remote restrictions"
- "disables windows audit policy"
- "disables windows defender using powershell"
- "downloads binary using certutil"
- "drops credential dumping tools"
- "dumps dns cache"

- "dyld inserted"
- "enables cleartext credential storage"
- "enables login bypass"
- "enables rdp from command-line"
- "enables safe mode"
- "enumerates arp table"
- "enumerates available systems on network"
- "enumerates domain account policy"
- "enumerates domain administrators"
- "enumerates domain computers"
- "enumerates domain controllers"
- "enumerates domain groups"
- "enumerates domain users"
- "enumerates enterprise administrators"
- "enumerates exchange domain servers"
- "enumerates exchange servers"
- "enumerates ip configuration"
- "enumerates local account policy"
- "enumerates local administrators"
- "enumerates local administrators on domain controller"
- "enumerates local groups"
- "enumerates local services"
- "enumerates local users"
- "enumerates logical disk"
- "enumerates mapped resources"
- "enumerates network connections"
- "enumerates primary domain controller"
- "enumerates processes on local system"
- "enumerates processes on remote system"
- "enumerates remote netbios name table"

- "enumerates remote resources"
- "enumerates route table"
- "enumerates services hosted in processes"
- "enumerates system info"
- "enumerates trusted domains"
- "evades scanning within windows defender"
- "evasive powershell used over network"
- "event viewer executes uncommon binary"
- "execute dll through rundll32"
- "exports sensitive registry hive"
- "extracts password-protected archive"
- "file encrypted"
- "file hidden"
- "file path not part of debian package in important system directory"
- "file path not part of debian package"
- "file path not part of rpm in important system directory"
- "file path not part of rpm"
- "file vault disabled"
- "floating module and hooking"
- "floating module in browser process"
- "floating module in os process"
- "floating module"
- "gatekeeper disabled"
- "gets current user as system"
- "gets current username and group information"
- "gets current username"
- "gets hostname"
- "gets remote time"
- "gina replacement"
- "graylisted file"

- "hidden and hooking"
- "hidden in appdata"
- "hidden plist and autorun"
- "hidden running as root"
- "hooks audio output function"
- "hooks authentication function"
- "hooks crypto function"
- "hooks dnsquery function"
- "hooks gui function"
- "hooks network http function"
- "hooks network io function"
- "hooks ntldr function"
- "hooks registry access function"
- "hooks registry enumeration function"
- "http daemon runs command prompt"
- "http daemon runs powershell"
- "http daemon runs reconnaissance tool"
- "http daemon writes executable"
- "ie dep disabled"
- "ie enhanced security disabled"
- "in appdata directory"
- "in hidden directory"
- "in recycle bin directory"
- "in root of appdatalocal directory"
- "in root of appdataroaming directory"
- "in root of logical drive"
- "in root of program directory"
- "in root of users directory"
- "installs root certificate"
- "in system volume information directory"

- "in temporary directory"
- "in uncommon directory"
- "invalid signature"
- "kext signature validation disabled"
- "lateral movement with credentials using net utility"
- "ld preload"
- "library preferences directory"
- "lists anti-spyware products"
- "lists antivirus products"
- "lists firewall products"
- "login bypass configured"
- "lua disabled"
- "mac firewall disabled"
- "malicious file by reputation service"
- "maps administrative share"
- "maps ipc$ share"
- "misleading file extension"
- "modifies file associations"
- "modifies image file execution for persistence"
- "modifies registry using command-line registry tool"
- "modifies run key"
- "modifies shell-open-command file association"
- "modifies startup folder location"
- "modifies winlogon dll for persistence"
- "modifies winlogon registry settings"
- "mshta runs command prompt"
- "mshta runs powershell"
- "mshta runs scripting engine"
- "mshta writes executable"
- "network access"

- "no antivirus notification disabled"
- "no firewall notification disabled"
- "non-microsoft modifies bad certificate warning setting"
- "non-microsoft modifies firewall policy"
- "non-microsoft modifies internet zone setting"
- "non-microsoft modifies lua setting"
- "non-microsoft modifies registry editor setting"
- "non-microsoft modifies security center config"
- "non-microsoft modifies services imagepath"
- "non-microsoft modifies task manager setting"
- "non-microsoft modifies windows system policy"
- "non-microsoft modifies zone crossing warning setting"
- "no uac notification disabled"
- "no windows update notification disabled"
- "office application crashed"
- "office application injects remote process"
- "office application runs bits"
- "office application runs command prompt"
- "office application runs powershell"
- "office application runs scripted ftp"
- "office application runs scripting engine"
- "office application runs task scheduler"
- "office application runs wmi scripting engine"
- "office application writes executable"
- "opens browser process"
- "opens os process"
- "opens process"
- "opswat reported infected"
- "opswat reported suspicious"
- "os process runs command shell"

- "packed and autorun"
- "packed and network access"
- "packed"
- "performs scripted file transfer"
- "possible login bypass"
- "possible mimikatz activity"
- "possible rdp session hijacking"
- "possibly configures uac bypass"
- "possibly renamed net.exe detected"
- "potential abuse of odbcconf"
- "potential outlook exploit"
- "powershell command using string manipulation"
- "powershell injects remote process"
- "powershell opens lsass process"
- "powershell runs command prompt"
- "powershell runs scripting engine"
- "process authorized in firewall"
- "process redirects to stdout or stderr"
- "process with matched yara rule"
- "process with opswat reported infected"
- "process with opswat reported suspicious"
- "psexesvc runs powershell"
- "psexesvc runs scripting engine"
- "psexesvc runs shell commands"
- "pubprn detection"
- "queries cached kerberos tickets"
- "queries processes on local system"
- "queries processes on remote system"
- "queries registry using command-line registry tool"
- "queries terminal sessions"

- "queries users logged on local system"
- "queries users logged on remote system"
- "record screen captures using psr tool"
- "registers always install elevated policy"
- "registers appcert dll"
- "registers appinit dll"
- "registers boot execute"
- "registers lsa authentication package"
- "registers lsa notification package"
- "registers lsa security package"
- "registers netsh helper dll"
- "registers port monitor dll"
- "registers shim database"
- "registers startup during safe mode boot"
- "registers time provider dll"
- "registry tools disabled"
- "regsvr32 creates windows task"
- "regsvr32 runs powershell"
- "regsvr32 runs rundll32"
- "regsvr32 writes executable"
- "remote directory traversal"
- "removes windows defender definitions"
- "rpm hash mismatch in important system directory"
- "rpm hash mismatch"
- "rpm ownership changed"
- "rpm permissions changed"
- "rundll32 creates windows task"
- "rundll32 runs powershell"
- "runkey persistence"
- "runs acl management tool"

- "runs active directory service query tool"
- "runs binary located in recycle bin directory"
- "runs binary located in root of logical drive"
- "runs binary located in root of program directory"
- "runs binary located in root of users directory"
- "runs binary located in system volume information directory"
- "runs blacklisted file"
- "runs certutil with decode arguments"
- "runs certutil with encode arguments"
- "runs certutil with hashfile arguments"
- "runs chained command shell"
- "runs chmod"
- "runs credential dumping tools"
- "runs curl"
- "runs ditto"
- "runs dns lookup tool for txt record"
- "runs dns lookup tool"
- "runs file attributes modification tool"
- "runs file transfer tool"
- "runs forfiles.exe"
- "runs graylisted file"
- "runs ifconfig"
- "runs kextload"
- "runs kextstat"
- "runs launchctl"
- "runs malicious file by reputation service"
- "runs mshta with http argument"
- "runs mshta with script argument"
- "runs msiexec with http argument"
- "runs netstat"

- "runs network configuration tool"
- "runs network connectivity tool"
- "runs one letter executable"
- "runs one letter script"
- "runs ping"
- "runs powershell bypassing execution policy"
- "runs powershell decoding base64 string"
- "runs powershell defining function"
- "runs powershell downloading content"
- "runs powershell invoke-mimikatz function"
- "runs powershell memory stream function"
- "runs powershell"
- "runs powershell shellexecute function"
- "runs powershell using encoded command"
- "runs powershell using environment variables"
- "runs powershell with hidden window"
- "runs powershell with http argument"
- "runs powershell with long arguments"
- "runs psexec on remote system and silently accepts user license"
- "runs psexec on remote system as system user"
- "runs ps"
- "runs registry tool"
- "runs regsvr32 com scriplets"
- "runs regsvr32 using one letter dll"
- "runs regsvr32 with http argument"
- "runs regsvr32 without arguments"
- "runs remote execution tool"
- "runs remote powershell command"
- "runs robocopy.exe"
- "runs rundll32 using one letter dll"

- "runs rundll32 with http argument"
- "runs rundll32 with javascript argument"
- "runs rundll32 without arguments"
- "runs scripting engine in batch mode using execution engine argument"
- "runs scripting engine"
- "runs service control tool"
- "runs shim database installer"
- "runs sh"
- "runs suspicious file by reputation service"
- "runs tar"
- "runs tasks management tool"
- "runs unzip"
- "runs waitfor.exe"
- "runs wmi command-line tool"
- "runs wmi scripting engine"
- "runs xcopy.exe"
- "safari fraud website warning disabled"
- "scripting addition in process"
- "scripting engine injects remote process"
- "scripting engine runs powershell"
- "scripting engine runs regsvr32"
- "scripting engine runs rundll32"
- "self signed"
- "services in programdata directory"
- "services runs command shell"
- "smartscreen filter disabled"
- "starts local service"
- "starts rdp service"
- "starts remote service"
- "stops diagtrack service"

- "stops error reporting service"
- "stops security service"
- "stops windows update service"
- "sudo no password prompt"
- "suspicious file by reputation service"
- "suspicious regsvr32.exe task"
- "system integrity protection disabled"
- "system restore disabled"
- "tampers with windows defender registry"
- "task manager disabled"
- "tasks in programdata directory"
- "terminates process"
- "transfers file using bits"
- "uac disabled"
- "unexpected csrss.exe parent"
- "unexpected explorer.exe destination location"
- "unexpected explorer.exe parent"
- "unexpected explorer.exe source location"
- "unexpected lsass.exe parent"
- "unexpected lsm.exe parent"
- "unexpected msdtc.exe parent"
- "unexpected os process destination location"
- "unexpected os process source location"
- "unexpected runtimebroker.exe parent"
- "unexpected services.exe parent"
- "unexpected smss.exe parent"
- "unexpected svchost arguments"
- "unexpected svchost.exe parent"
- "unexpected taskhostw.exe parent"
- "unexpected wininit.exe parent"

- "unexpected winlogon.exe parent"
- "unknown segment"
- "unsigned copies self"
- "unsigned creates remote thread and file hidden"
- "unsigned creates remote thread"
- "unsigned cron job"
- "unsigned deletes self"
- "unsigned kext"
- "unsigned library in suspicious daemon"
- "unsigned module in signed process"
- "unsigned reserved name"
- "unsigned runs python"
- "unsigned writes executable"
- "unsigned writes executable to appdatalocal directory"
- "unsigned writes executable to appdataroaming directory"
- "unsigned writes executable to library application support directory"
- "unsigned writes executable to library directory"
- "unsigned writes executable to library preferences directory"
- "unsigned writes executable to scripting additions directory"
- "unsigned writes executable to system directory"
- "unsigned writes executable to var directory"
- "unsigned writes executable to windows directory"
- "unsigned writes to autorun"
- "uses libnss"
- "uses libpcap"
- "uses mach injection"
- "uses mach override"
- "warning on post redirect disabled"
- "windows firewall disabled"
- "windows task runs powershell"

- "windows update disabled"
- "wmic remote node activity"
- "wmiprvse runs command shell"
- "wmiprvse runs powershell"
- "wmiprvse runs scripting engine"
- "writes blacklisted file"
- "writes executable to recycle bin directory"
- "writes executable to root of logical drive"
- "writes executable to root of program directory"
- "writes executable to root of users directory"
- "writes executable to system volume information directory"
- "writes graylisted file"
- "writes malicious file by reputation service"
- "writes suspicious file by reputation service"
- "yara rule matched"
- "executable in ads"
- "explorer public folder dll load"
- "powershell double base64"
- "outbound from windows directory"
- "outbound from unsigned temporary directory"
- "unsigned opens lsass"
- "outbound from unsigned appdata directory"
- "rdp launching loopback address"
- "autorun invalid signature windows directory"
- "command shell copy items"

Position Tracking Information

The ESA Correlation service continuously streams data from the data sources like decoders (log and network), and concentrators. ESA retrieves events from the data sources, and applies rules to generate alerts to detect malicious activities. When you deploy a data source, ESA starts processing information from the latest available session, by default. Position Tracking Information enables you to visualize the progress of the sessions that ESA has processed, and provides information on the session IDs and the date and time when the events were processed.

Set Position Tracking Information enables you to:

- Visualize the number of sessions that a particular ESA data source has already analyzed, review the number of sessions ESA would process after you edit the position tracking, and plan your work.
- Set the tracking position information based on:
  - Session ID
  - Date and Time (Collection Time)
- Set position tracking for multiple data sources before you deploy them.
- Calculate the number of sessions that the ESA Correlation Service is scheduled to process for a particular data source to either process, reprocess, or skip sessions with respect to the current position of the data source.

> **Note:** The Position tracking feature with the Date and Time option works based on the profile time settings in the NetWitness Platform UI. This time-zone based time from the UI is converted to UTC, and is sent to the core, to retrieve the corresponding session ID for that time stamp.
> Example: If the UI follows IST, the UI converts it to UTC and sends it to the core. The session ID is fetched for the specific UTC time stamp, and set to position tracking at deployment.

Use Case Scenario

This section provides information about how you can use position tracking information in a real-world scenario.

Case 1: If you have deployed a data source with a total of 400 sessions that ESA has already processed, and if you want to start processing the events from the beginning, perform the following steps to reprocess the sessions.

Edit the position Tracking Information

1. Select the deployment and click **Edit Deployment**.
2. Select the datasource and click **Set Position Tracking Information**.

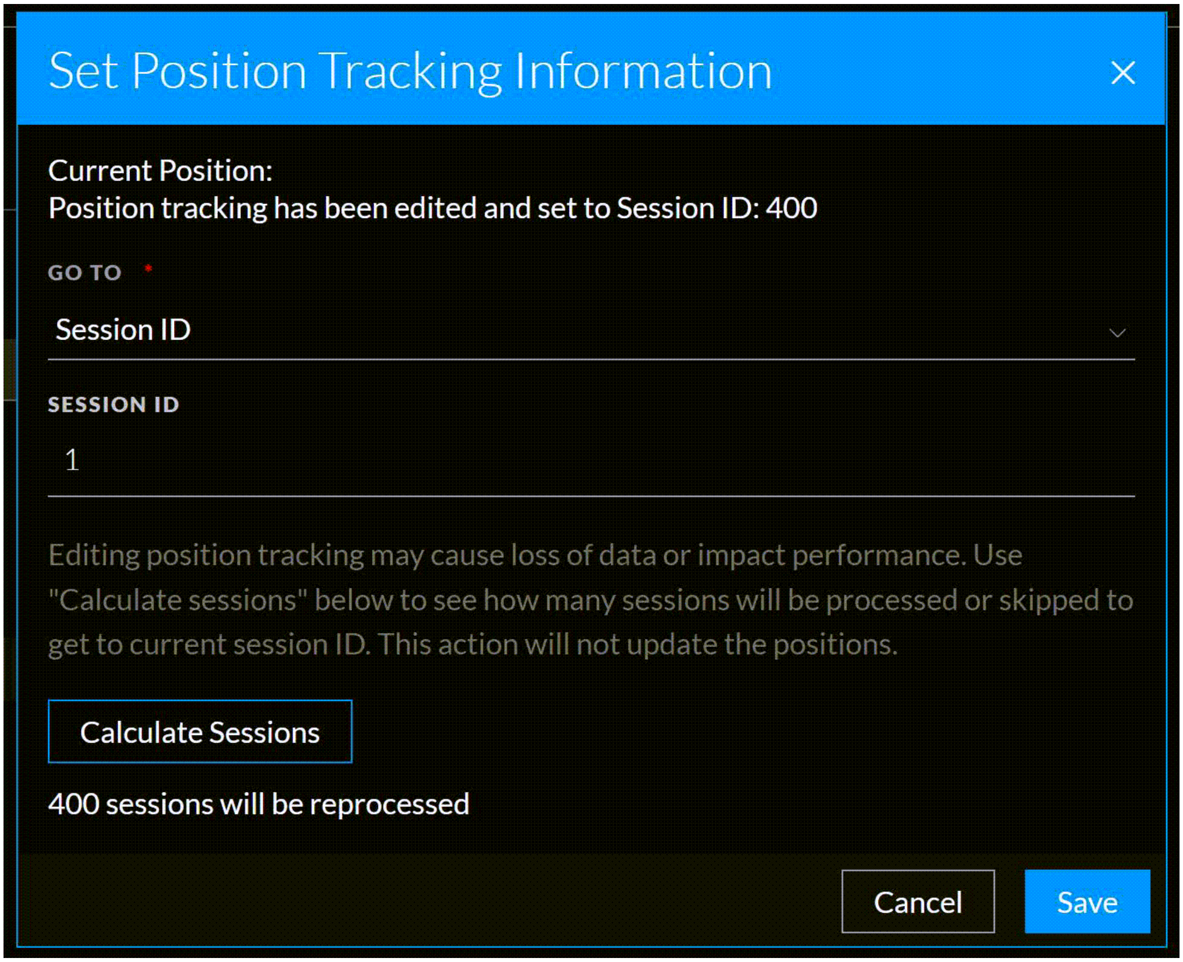
   The Set Position Tracking Information dialog is displayed.
3. In the **Go To** drop-down menu, select the **Session ID** and enter the session number as 1 in the **Session ID** text field.

You can also set the position tracking information based on date and time and the sessions will be calculated using data and time.

4. Click **Calculate Sessions**.
5. Click **Save** twice.
6. Select the Deployment and click **Deploy**.

   All the 400 sessions will be reprocessed.

   The following image shows the use case scenario.



Set Position Tracking Information

Current Position:
Position tracking has been edited and set to Session ID: 400

GO TO *: Session ID

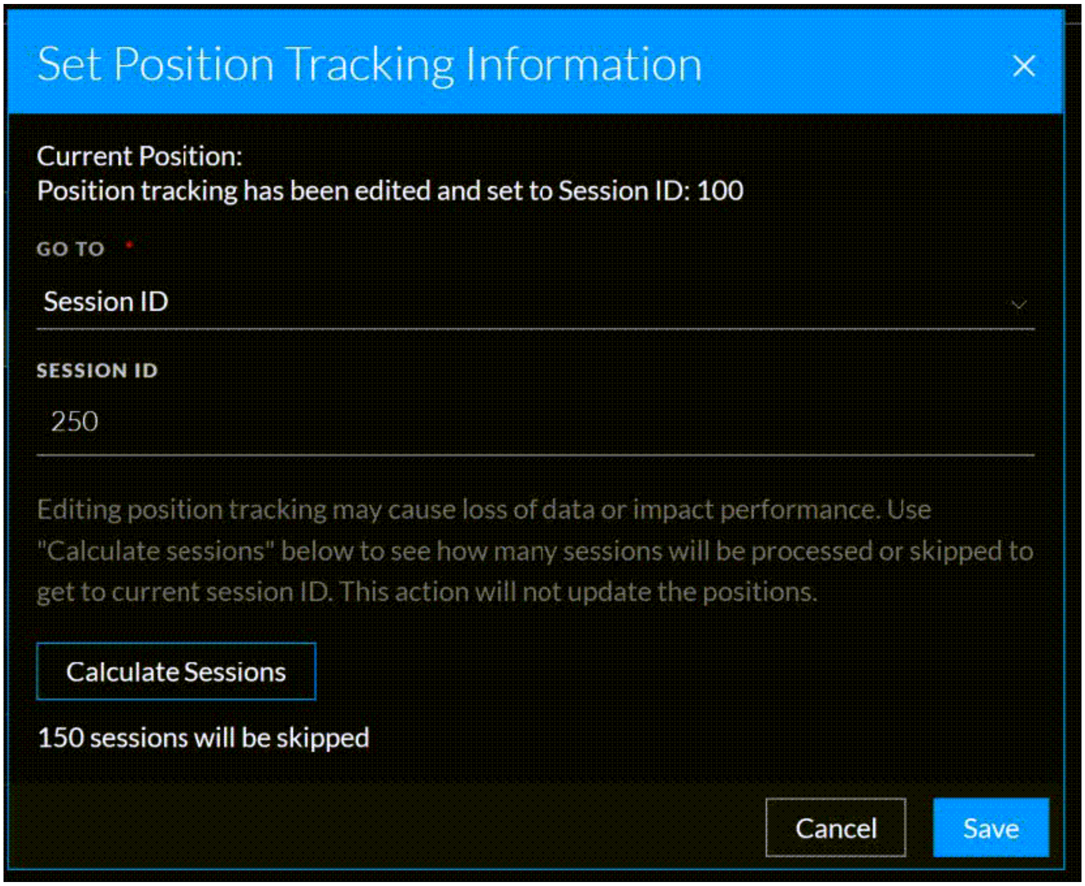
SESSION ID: 1

Editing position tracking may cause loss of data or impact performance. Use "Calculate sessions" below to see how many sessions will be processed or skipped to get to current session ID. This action will not update the positions.

400 sessions will be reprocessed

Case 2: If you have deployed a data source with a total of 700 sessions available and the current position of the data source is at 100 and if you set the sessions ID to 250. In this case, 150 sessions will be skipped. You can also set the sessions based on the date and time.

The following image shows the use case scenario.



Current Position:
Position tracking has been edited and set to Session ID: 100

GO TO *

Session ID

SESSION ID

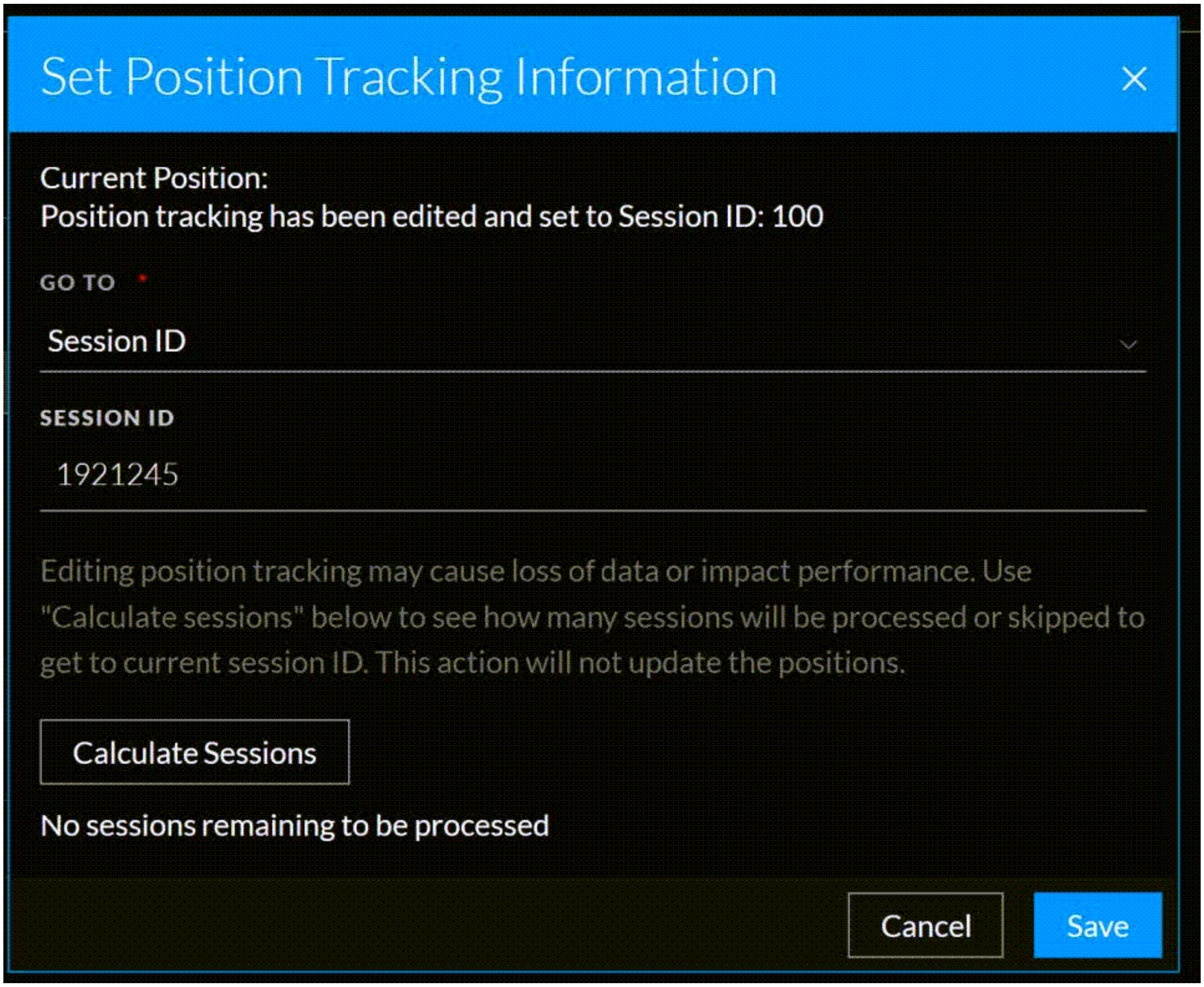
250

Editing position tracking may cause loss of data or impact performance. Use "Calculate sessions" below to see how many sessions will be processed or skipped to get to current session ID. This action will not update the positions.

150 sessions will be skipped

Case 3: If you have deployed a data source that has a total of 1921237 sessions available and if you set the session ID higher than the available sessions for the data source. In this case, no remaining sessions will be processed. You can also set the sessions based on date and time.

The following image shows the use case scenario.



Set Position Tracking Information

Current Position:
Position tracking has been edited and set to Session ID: 100

GO TO *

Session ID

SESSION ID

1921245

Editing position tracking may cause loss of data or impact performance. Use "Calculate sessions" below to see how many sessions will be processed or skipped to get to current session ID. This action will not update the positions.

Calculate Sessions

No sessions remaining to be processed

Note: Editing the tracking information is optional. If you add a new data source to an existing ESA deployment, and you do not edit the tracking information, ESA follows the default behavior to process events.