NetWitness® Platform XDR

Version 12.1.1.0

Centralized Content Management

NETWITNESS

Platform XDR

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

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.

January, 2023

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.

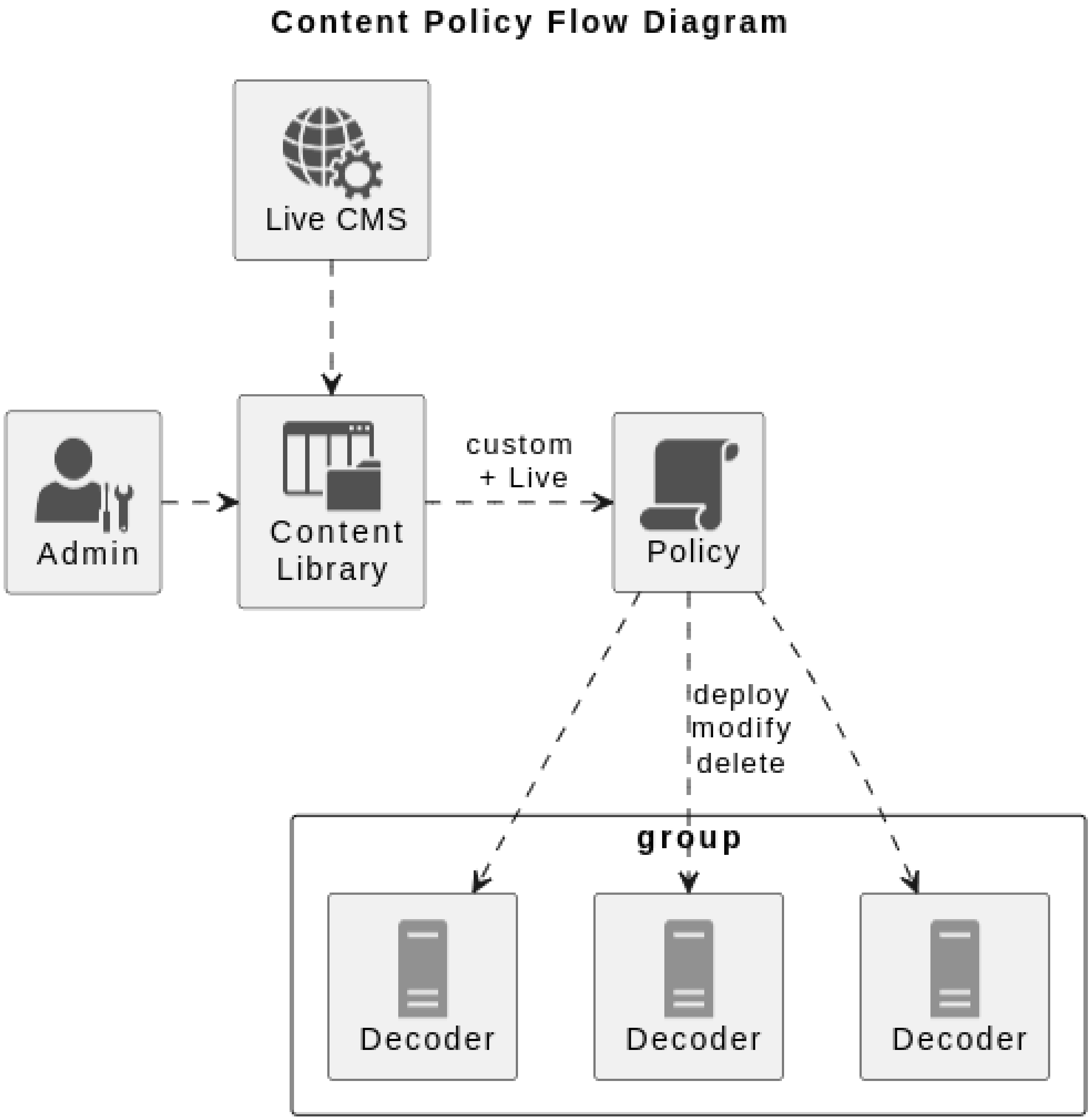
Policy-based Centralized Content Management (CCM) is a unified approach to find, deploy, and manage content through the entire life cycle based on policies that can be assigned to groups of devices. It is a single location to view, modify and manage the content deployed across all services in the environment.

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 Services

Prior to 12.1 version, content of the core services could be managed simultaneously either via Policy-based Central Content Management (CCM) or Service Config page/Live content UI. Managing content in this way could cause policies to go out of sync with the actual content of the services.

From 12.1 version, by default, CCM is enabled to manage all services.

From 12.1.1 version onwards, single CCM toggle is introduced to enable or disable CCM for all 12.0+ Decoders and Log Decoders.

The toggle button is available via backend of source-server. Through the backend server, you can disable or enable Policy-based Centralized Content Management (CCM) for an individual service.

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”.

How to Enable or Disable CCM for All Services

1. Connect through SSH to NW server node.
2. Run the following commands:
   a. `nw-shell`
   b. `connect --service source-server`
   c. `cd /rsa/central/service/`
   d. `cd set-all-managed-by-legacy`

e. `invoke true`

   Returns the message “Content of all Decoders & Log Decoders is centrally managed: No". This message indicates that the CCM is disabled for all Decoder services.

f. `invoke false`

   Returns the message “Content of all Decoders & Log Decoders is centrally managed: Yes". This message indicates that the CCM is enabled for all Decoder services.

How to Enable or Disable CCM for Individual Services

Follow these steps to enable or disable CCM for individual services:

1. Connect through SSH to NW server node.
2. Run the following commands:

   a. `nw-shell`

   b. `connect --service source-server`

   c. `cd /rsa/central/service/`

   d. `cd toggle-managed-by-legacy`

   e.
   ```
   invoke '<service_name>'
   example: invoke 'NWAPPLIANCE18845 - Log Decoder'
   ```

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.

Note:
- Existing Live content does not need to be exported or imported. All Live content will be available in the Content Library and will only need to be added to one or more policies and published as needed.
- When the user upgrades a Decoder or Log Decoder from 11.x, 12.0 or 12.1 version to 12.1.1 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`

This process includes the following steps:

- Make sure that the necessary Live content has been selected and applied to one or more Policies.

- Enable subscriptions for Live content as desired.
- Export any custom content, including Application Rules, Network Rules, Lua Parsers and Log Parsers.
- Import custom content into the Content Library.
- Apply custom content to one or more Policies.
- Create Groups to which Policies will be assigned.
- Publish Policies to their assigned Groups.

Warning: Initially, when a Policy is published to a Group , all the content which are not included in the policy will be removed from the services in that Group.

To migrate Application Rules or Network Rules

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.
6. Type a file name which contains exported content and import the content to Content Library.

   For details on importing content to content library, view Import Content to Content Library topic.

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 migrate 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.

For details on importing content to content library, view Import Content to Content Library topic.

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** **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.	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.

Import Content to Content Library

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

To view the list of supported file types and file extensions for different content types, refer Migrate Content from Core Services to Content Library topic.

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**
   - **LUA Parser**
   - **Feeds**
   - **Log Devices**

   Note: Log Devices content should be converted to .envision files before importing.

5. In the respective content panel, click **Import**.
6. In the **Import** panel, click or drag the file to upload.
7. Click **Overwrite** to overwrite content. This is applicable only in case of overriding an already imported content.

   Note: You can overwrite the content if the content name is the same as the custom content. However, overwriting is not supported if the content name is the same as existing content of the same type from the live server.

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

Create an Application Rule

This topic describes the steps to create an application rule.

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 **New Create 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.

     Note: This field is applicable only for 12.1.1 version.

- 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.
- Enter the meta value for the alert on. This is a mandatory field.
- Click **Save** to save the new application rule.

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. For 12.1 version, in the Clone Rule panel, do any of the following:
   - Enter the name for cloned rule and click **Clone** to clone the rule.
   - Click **Cancel** to cancel the operation.
7. For 12.1.1 version, in the Clone Rule panel, do any of 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.

     > **Note:** The rule value cannot be modified. 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.

- 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.
- Enter the meta value for the alert on. 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 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.

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.

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.

     > **Note:** This field is applicable only for 12.1.1 version.
   - 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. For 12.1 version, in the Clone Rule panel, do any of the following:
   - Enter the name for cloned rule and click **Clone** to clone the rule.
   - Click **Cancel** to cancel the operation.
8. For 12.1.1 version, in the Clone Rule panel, do any of 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.

     > **Note:** The rule value cannot be modified. 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 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.

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.

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.

   It navigates to **ESA Rules** > **Rules** view. For more information on creating new rules, see the section Add a Rule Builder Rule.

   > **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*.

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.

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

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**.

Filter Content Rules

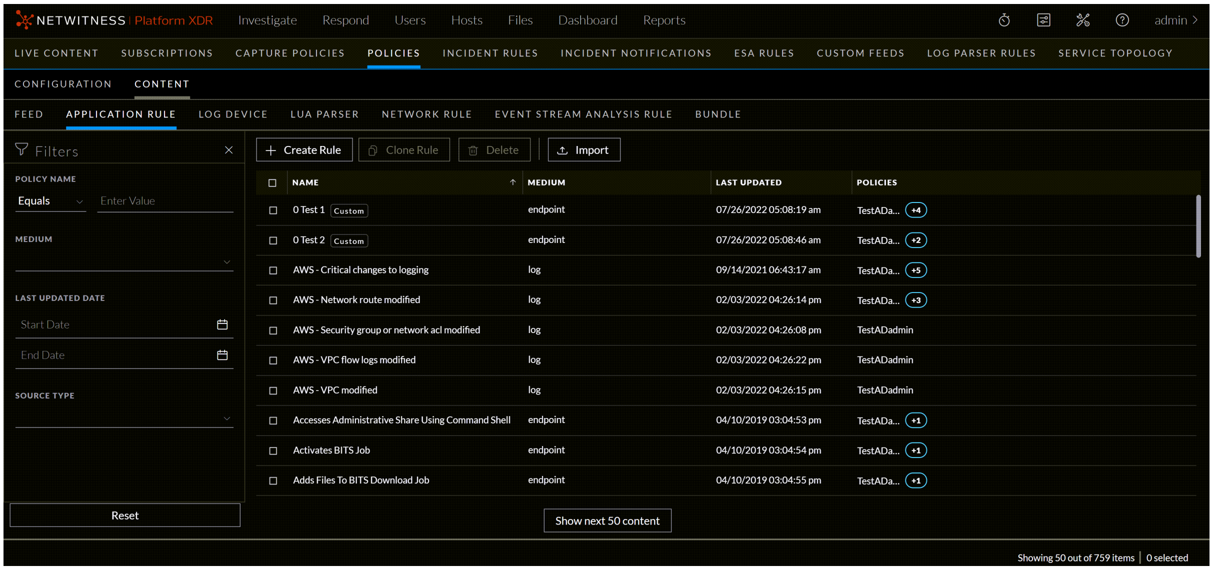
The Filters panel allows you to filter the list of displayed contents under the content library based on the name, medium, date range, and source type.

This applies to the following content rule types:

- Feed
- Application Rule
- Log Device
- Lua Parser
- Network Rule
- Event Steam Analysis Rule
- 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.



□	NAME	MEDIUM	LAST UPDATED	POLICIES
□	0 Test 1 Custom	endpoint	07/26/2022 05:08:19 am	TestADa... +4
□	0 Test 2 Custom	endpoint	07/26/2022 05:08:46 am	TestADa... +2
□	AWS - Critical changes to logging	log	09/14/2021 06:43:17 am	TestADa... +5
□	AWS - Network route modified	log	02/03/2022 04:26:14 pm	TestADa... +3
□	AWS - Security group or network acl modified	log	02/03/2022 04:26:08 pm	TestADadmin
□	AWS - VPC flow logs modified	log	02/03/2022 04:26:22 pm	TestADadmin
□	AWS - VPC modified	log	02/03/2022 04:26:15 pm	TestADadmin
□	Accesses Administrative Share Using Command Shell	endpoint	04/10/2019 03:04:53 pm	TestADa... +1
□	Activates BITS Job	endpoint	04/10/2019 03:04:54 pm	TestADa... +1
□	Adds Files To BITS Download Job	endpoint	04/10/2019 03:04:55 pm	TestADa... +1

Showing 50 out of 759 items | 0 selected

5. To search by policy name:
   - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the policy. Type one character and a list of policies 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 medium, select one or more mediums from the **Medium** drop-down list. The options are listed below:
   - **endpoint**
   - **log**
   - **log and packet**
   - **packet**
7. 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.
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 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.
        - To publish all the content, click **Publish All**.
        - To publish only the content that is not published on the service, click **Publish Changes**.
        - To cancel the publish content dialog, click **Cancel**.
    - Click **Save and Close** to save the settings.

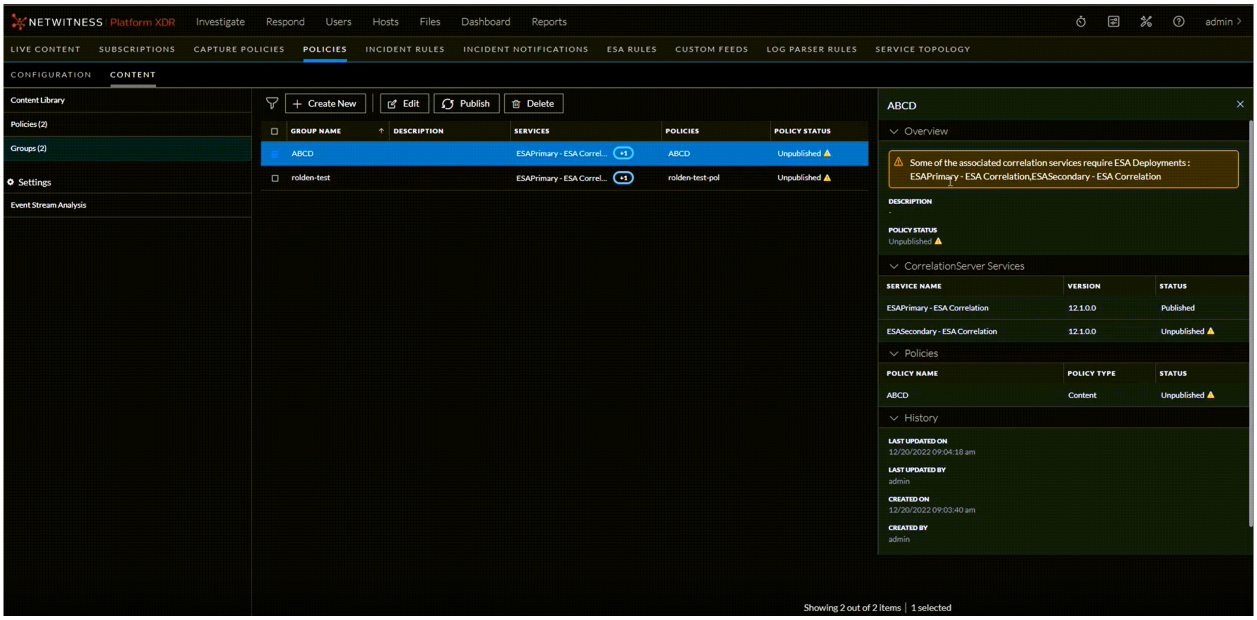
View a Group

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

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.



□	GROUP NAME	DESCRIPTION	SERVICES	POLICIES	POLICY STATUS
☑	ABCD		ESAPrimary - ESA Correl... +1	ABCD	Unpublished ⚠
□	rolden-test		ESAPrimary - ESA Correl... +1	rolden-test-pol	Unpublished ⚠

Showing 2 out of 2 items | 1 selected

ABCD

Overview

⚠ Some of the associated correlation services require ESA Deployments : ESAPrimary - ESA Correlation,ESASecondary - ESA Correlation

DESCRIPTION
-

POLICY STATUS
Unpublished ⚠

CorrelationServer Services

SERVICE NAME	VERSION	STATUS
ESAPrimary - ESA Correlation	12.1.0.0	Published
ESASecondary - ESA Correlation	12.1.0.0	Unpublished ⚠

Policies

POLICY NAME	POLICY TYPE	STATUS
ABCD	Content	Unpublished ⚠

History

LAST UPDATED ON
12/20/2022 09:04:18 am

LAST UPDATED BY
admin

CREATED ON
12/20/2022 09:03:40 am

CREATED BY
admin

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 the group from the policy, the ESA content will be deleted by default.

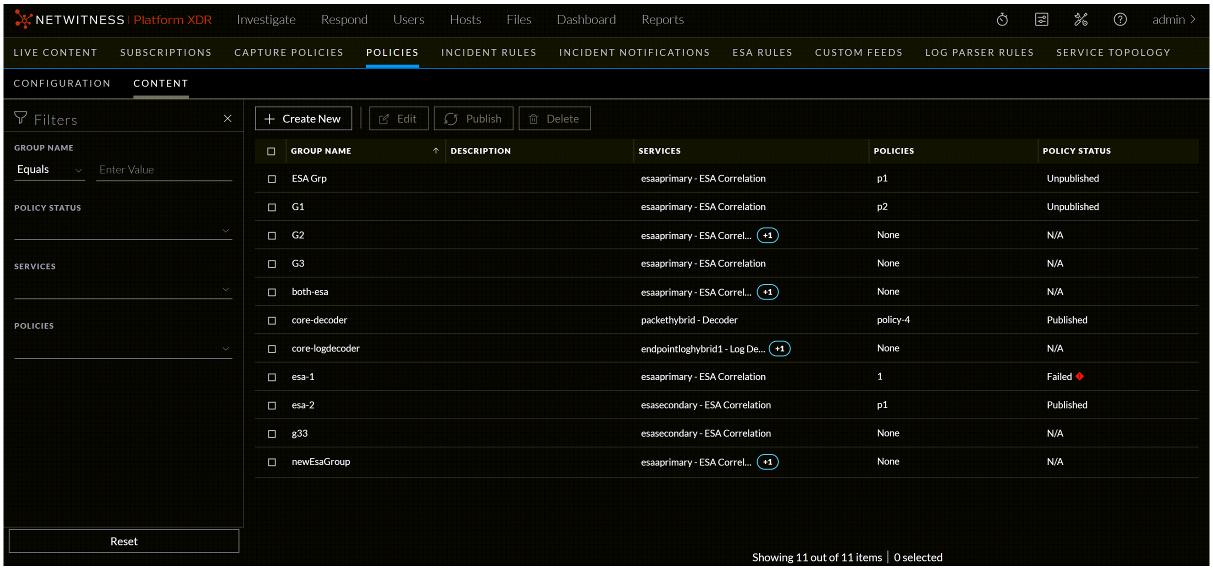
- The policy will be listed under the Unpublished category.
- Click **Save and Close** to save the settings and return to the Policies view.

Filter Groups

The Filters panel 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. Click **Groups**.
4. By default, the filters panel is hidden, click the (Filters) icon in the toolbar to expand the filters panel.



□	GROUP NAME	DESCRIPTION	SERVICES	POLICIES	POLICY STATUS
□	ESA Grp		esaaprimary - ESA Correlation	p1	Unpublished
□	G1		esaaprimary - ESA Correlation	p2	Unpublished
□	G2		esaaprimary - ESA Correl... +1	None	N/A
□	G3		esaaprimary - ESA Correlation	None	N/A
□	both-esa		esaaprimary - ESA Correl... +1	None	N/A
□	core-decoder		packethybrid - Decoder	policy-4	Published
□	core-logdecoder		endpointloghybrid1 - Log De... +1	None	N/A
□	esa-1		esaaprimary - ESA Correlation	1	Failed ◆
□	esa-2		esasecondary - ESA Correlation	p1	Published
□	g33		esasecondary - ESA Correlation	None	N/A
□	newEsaGroup		esaaprimary - ESA Correl... +1	None	N/A

Showing 11 out of 11 items | 0 selected

5. To search by group name:
   - 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 groups 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 group will be displayed.

6. To filter by policy status, select one or more statuses from the **Policy Status** drop-down list. The options are listed below:
   - **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.
7. To filter by services, select one or more services from the **Services** drop-down list. For example, Log Decoder.
8. To filter by policies, select one or more policies from the **Policies** drop-down list. You can also search for the name of the policies from this list.
9. To hide, click the ☒ icon at the top-right of the panel.

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

Manage Policies

Policies contain content and subscription settings used to assign and manage content within a Group.

IMPORTANT: The customers should note that, while publishing the first policy to a service, all previous content except custom feeds, will be deleted. Ensure that all custom content are migrated to Content Library before publishing the first policy.

This section contains:

- Create and Publish Policies
- Clone a Policy
- Delete a Policy
- Edit a Policy
- View a Policy
- Enable Content for a Policy
- Disable Content for a Policy
- Subscribe Content for a Policy
- Unsubscribe Content for a Policy
- Filter Policies
- Filter Policy Content Details
- Merge Policy with ESA Content

Create and Publish Policies

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

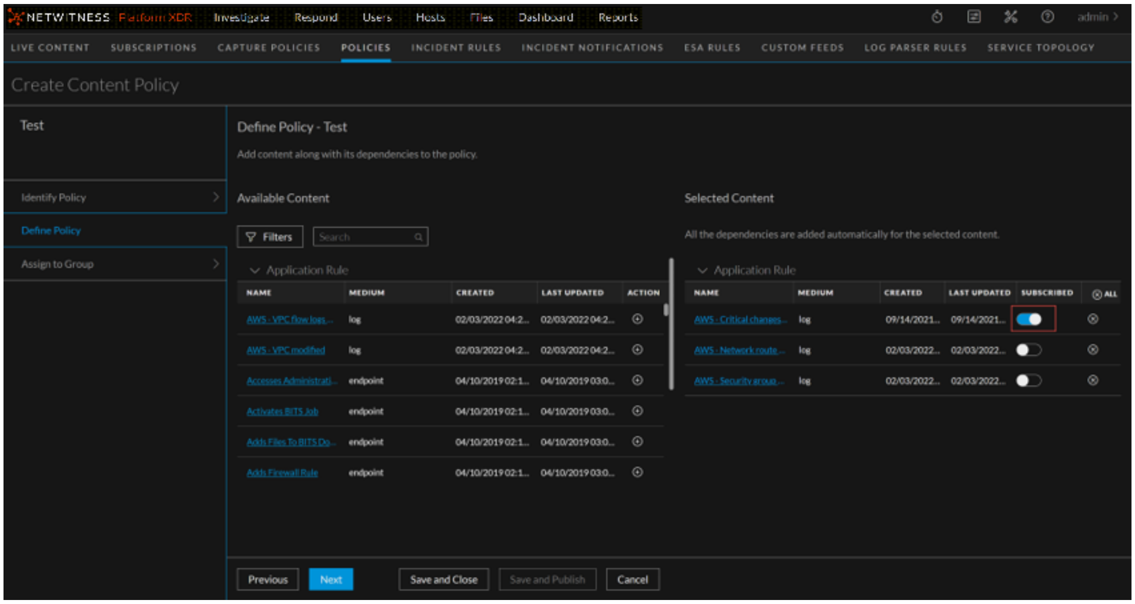
To create a Policy

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. 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.

Note: Subscription is not allowed for custom content.



Define Policy - Test

Add content along with its dependencies to the policy.

Available Content

Application Rule

NAME	MEDIUM	CREATED	LAST UPDATED	ACTION
AWS - VPC flow logs ...	log	02/03/2022 04:2...	02/03/2022 04:2...	⊕
AWS - VPC modified	log	02/03/2022 04:2...	02/03/2022 04:2...	⊕
Accesses Administrati...	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Activates BITS Job	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Adds Files To BITS Do...	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕
Adds Firewall Rule	endpoint	04/10/2019 02:1...	04/10/2019 03:0...	⊕

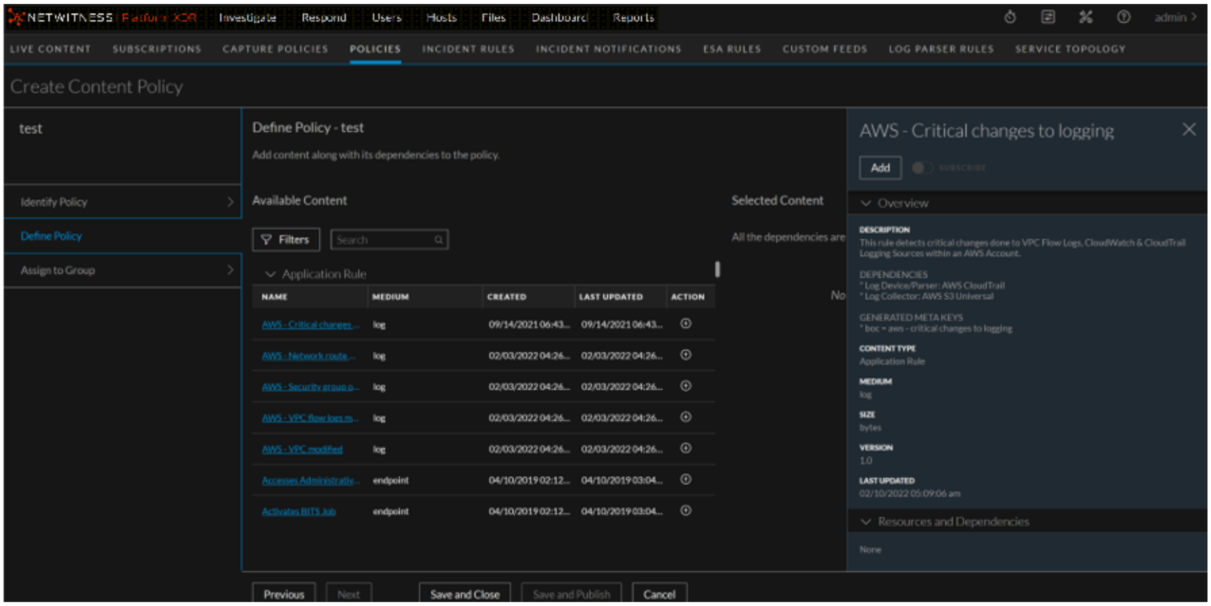
Selected Content

All the dependencies are added automatically for the selected content.

Application Rule

NAME	MEDIUM	CREATED	LAST UPDATED	SUBSCRIBED	⊗ ALL
AWS - Critical changes ...	log	09/14/2021...	09/14/2021...	●	⊗
AWS - Network route ...	log	02/03/2022...	02/03/2022...	○	⊗
AWS - Security group ...	log	02/03/2022...	02/03/2022...	○	⊗

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.



Define Policy - test

Add content along with its dependencies to the policy.

Available Content

Application Rule

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...	⊕

Selected Content

All the dependencies are

No

AWS - Critical changes to logging

Overview

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

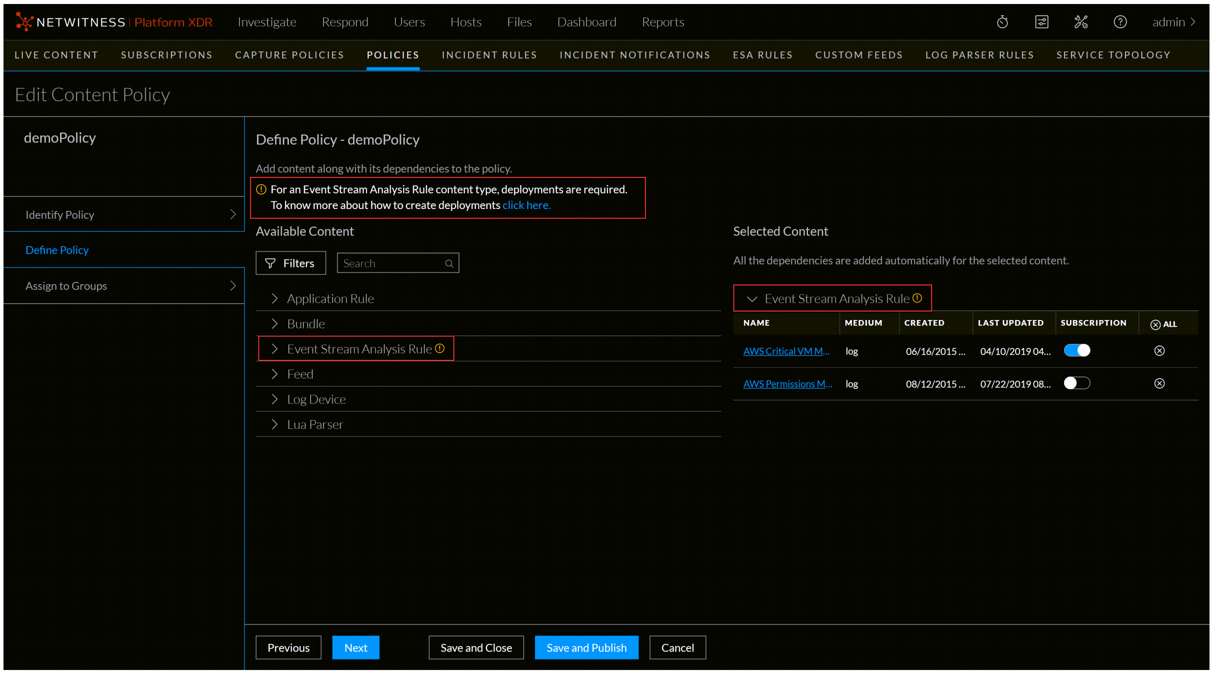
LAST UPDATED
02/10/2022 05:09:06 am

Resources and Dependencies

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.



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

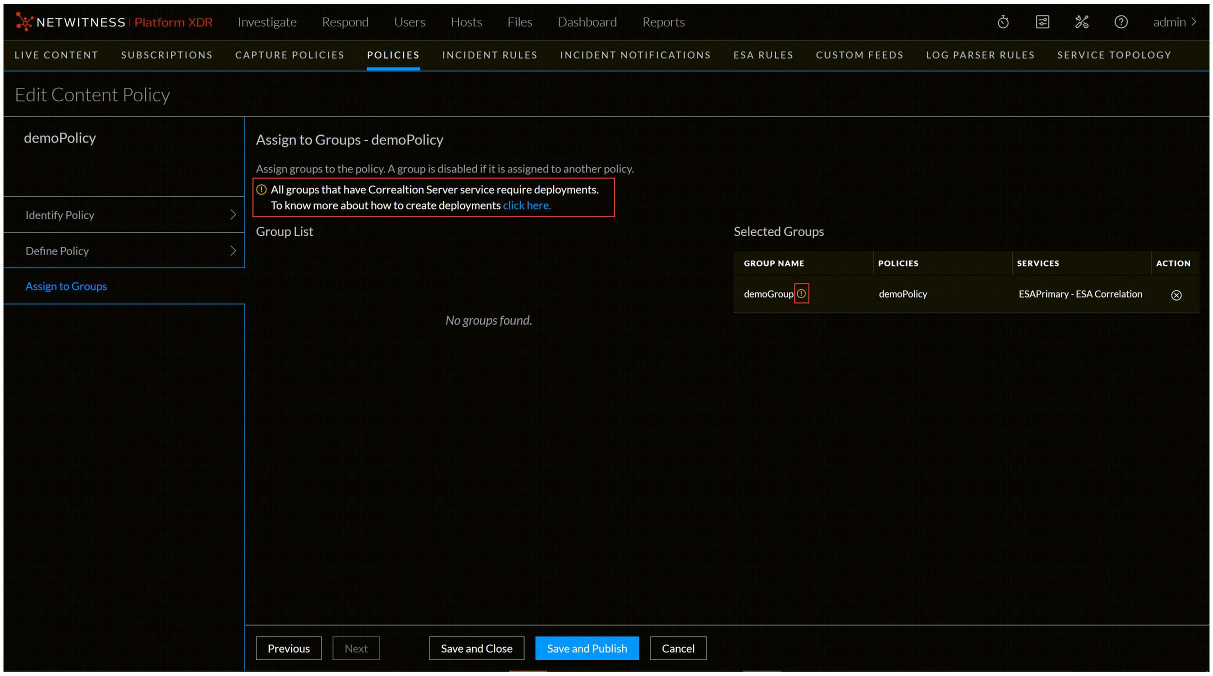
Selected Content

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.



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.

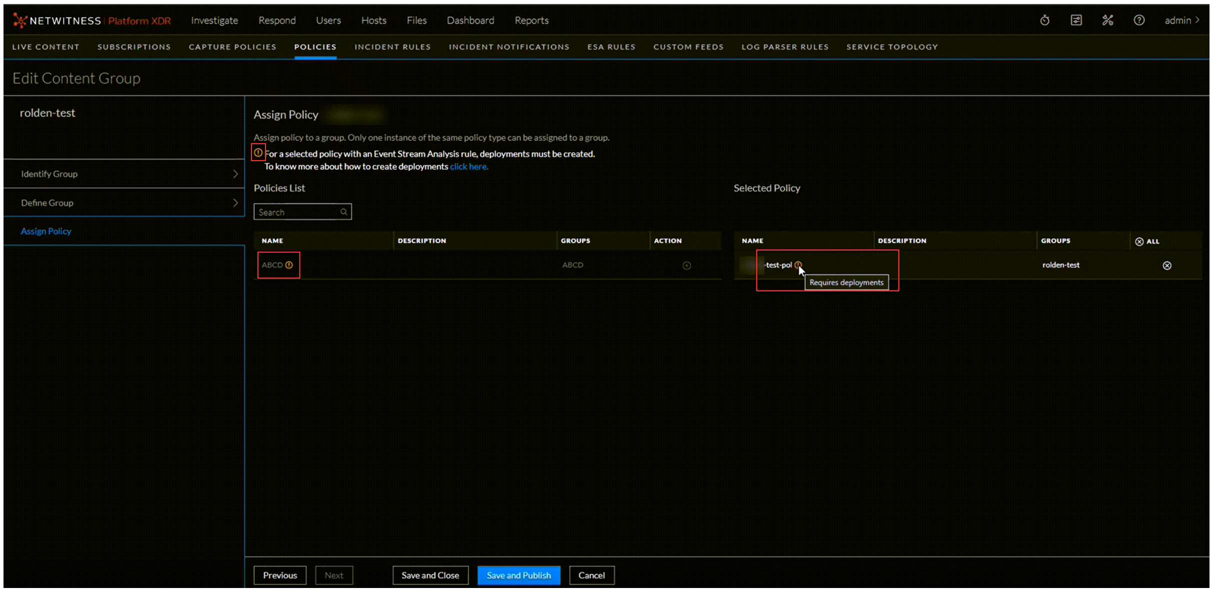
Group List

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 [redacted]

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
[redacted]-test-pol		rolden-test	⊗

Requires deployments

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

8. 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.

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

IMPORTANT: Once the publish is successful, you can view only the published content on the service while publishing the policy for the first time.

Note:
- While publishing the first policy to a service, all previous content except custom feeds, will be deleted. Ensure that all custom content are migrated to content library before publishing the first policy.
- 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.

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

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

IMPORTANT:
When first applying a Content Policy to manage content, the existing Live and custom content on the service (excluding Custom Feeds) will be removed and replaced with the Policy content. You should compare the existing service content with the policy before applying to ensure required content is added to the policy. 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:
   - 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 group from the policy, you can either delete the content of the service and remove the group or just remove the group from the policy.
      - 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.

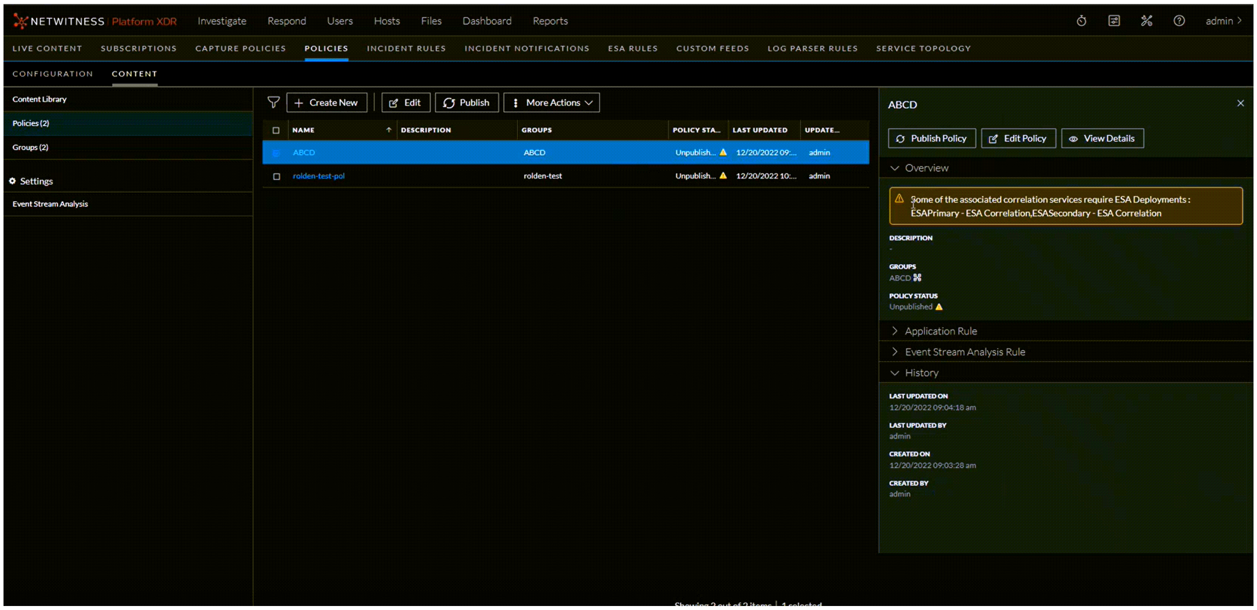
View a Policy

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.

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.



□	NAME	DESCRIPTION	GROUPS	POLICY STA...	LAST UPDATED	UPDATE...
●	ABCD		ABCD	Unpublish... ⚠	12/20/2022 09:...	admin
□	rolden-test-pol		rolden-test	Unpublish... ⚠	12/20/2022 10:...	admin

⚠ Some of the associated correlation services require ESA Deployments : ESAPrimary - ESA Correlation,ESASecondary - ESA Correlation

DESCRIPTION
-

GROUPS
ABCD

POLICY STATUS
Unpublished ⚠

LAST UPDATED ON
12/20/2022 09:04:18 am

LAST UPDATED BY
admin

CREATED ON
12/20/2022 09:03:28 am

CREATED BY
admin

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.
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. 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 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** 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**.

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** 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**.

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

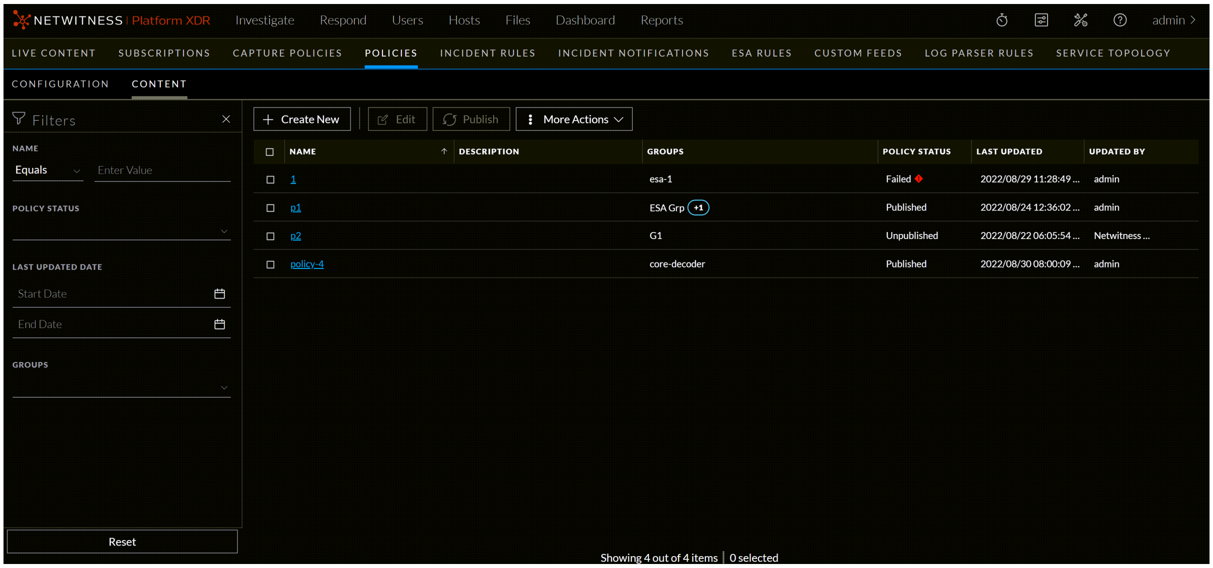
1. Go to **(CONFIGURE) > Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.
4. Click the policy name to view the policy details.
5. In the **Application Rule**, **Network Rule**, **Feed**, **Log Device**, **LUA Parser**, **Event Stream Analysis Rule** or **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 name, policy status, date range, and groups.

To filter the policies

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



□	NAME	DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	UPDATED BY
□	1		esa-1	Failed	2022/08/29 11:28:49 ...	admin
□	p1		ESA Grp +1	Published	2022/08/24 12:36:02 ...	admin
□	p2		G1	Unpublished	2022/08/22 06:05:54 ...	Netwitness ...
□	policy-4		core-decoder	Published	2022/08/30 08:00:09 ...	admin

Showing 4 out of 4 items | 0 selected

5. To search by name:
   - Set the filter option to **Contains** operator from the drop-down list and start typing the name of the policy. Type one character and a list of policies 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 policy will be displayed.
6. To filter by policy status, select one or more statuses from the **Policy Status** drop-down list. The options are listed below:
   - **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.

7. 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.

8. To filter by groups, select one or more groups from the **Groups** drop-down list. You can also search for the name of the groups from this list.

9. To hide, click the × icon at the top-right of the panel.

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

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, a resource created date, and last updated date.

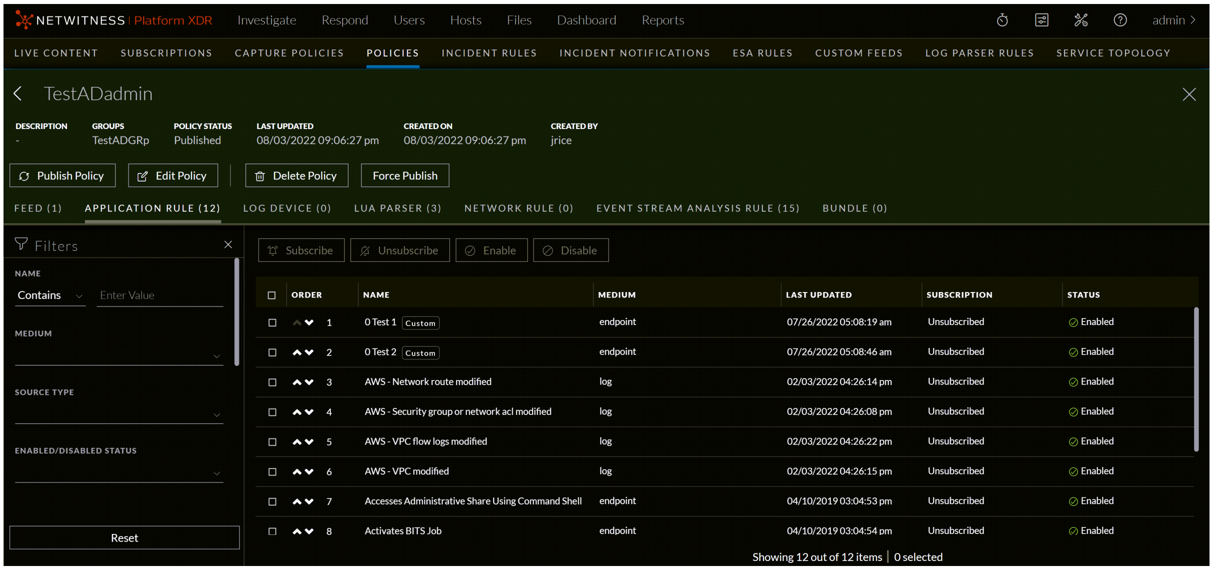
This applies to the following content types:

- Feed
- Application Rule
- Log Device
- Lua Parser
- Network Rule
- Event Steam Analysis Rule
- 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 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.
12. 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.
13. 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

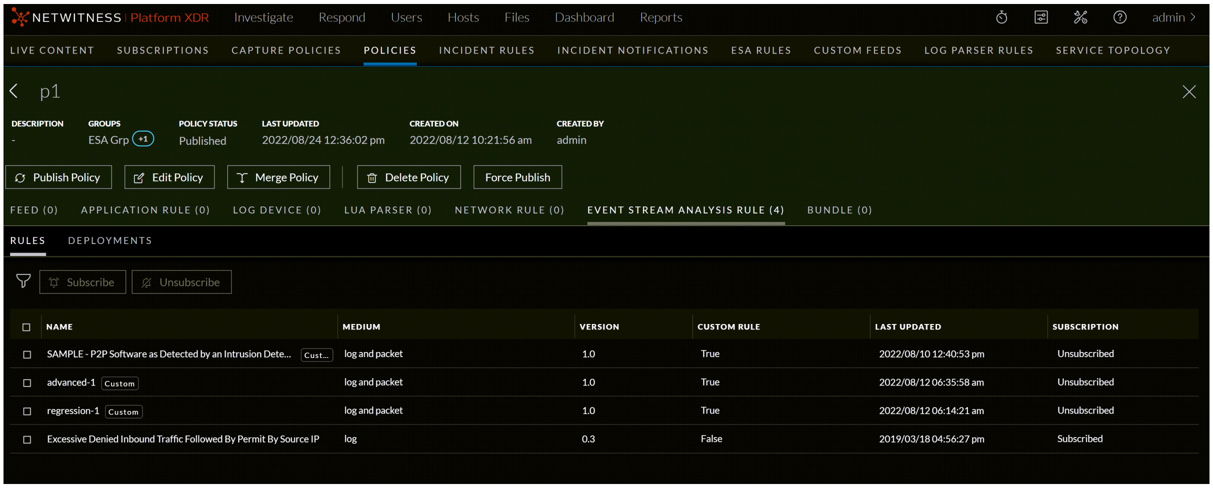
From the 12.1 version, the ESA content is managed through the **(CONFIGURE)** > **Policies** page. After you upgrade to the 12.1 version, all the existing ESA deployments will be migrated to the policies and groups view. The **Merge Policy** button will be available only for the policy having ESA content 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.



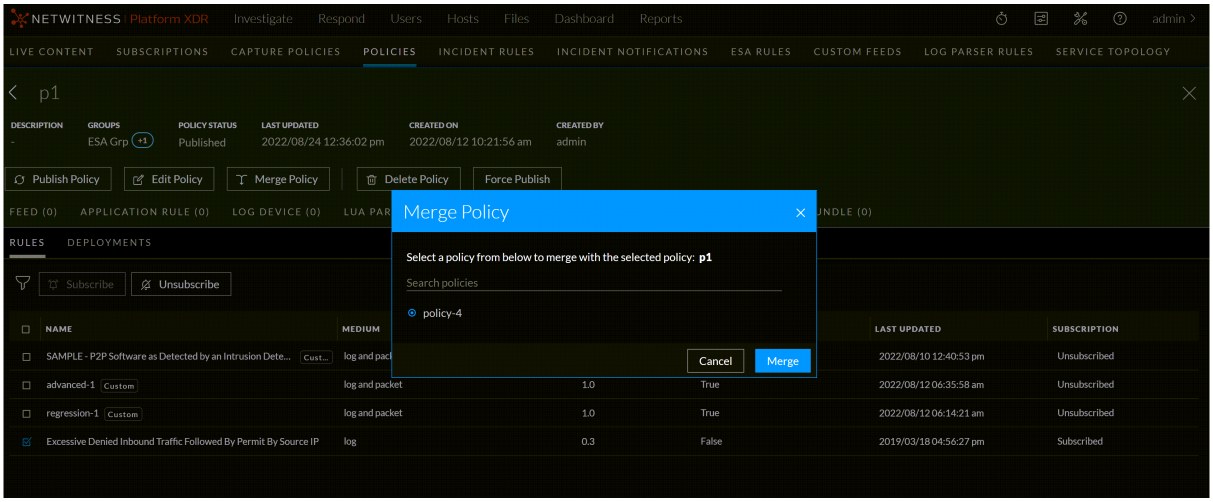
p1

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.



Merge Policy

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

Search policies

● policy-4

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 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 ESA Datasources

This section contains:

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

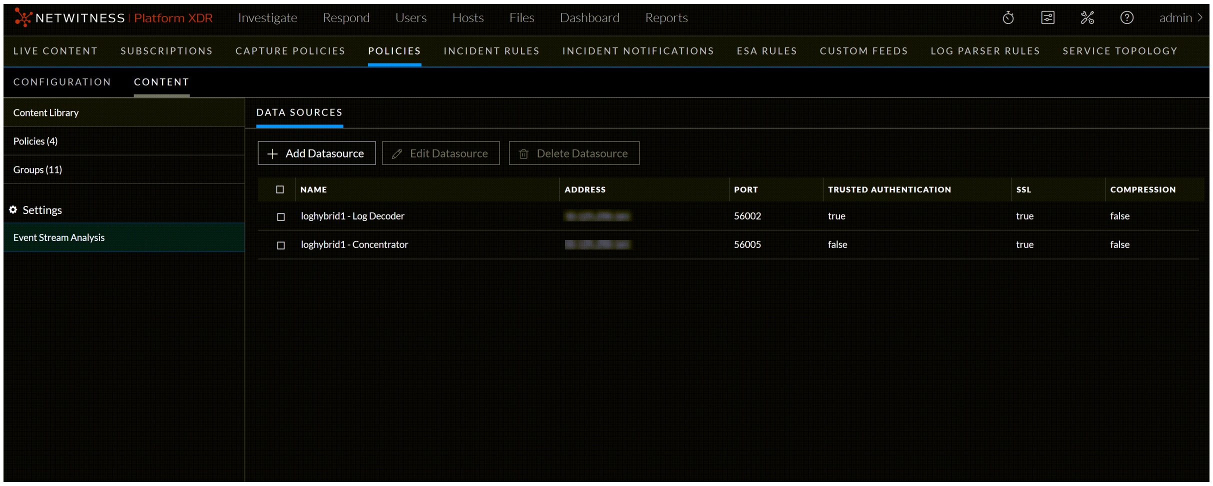
View an ESA Datasource

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.

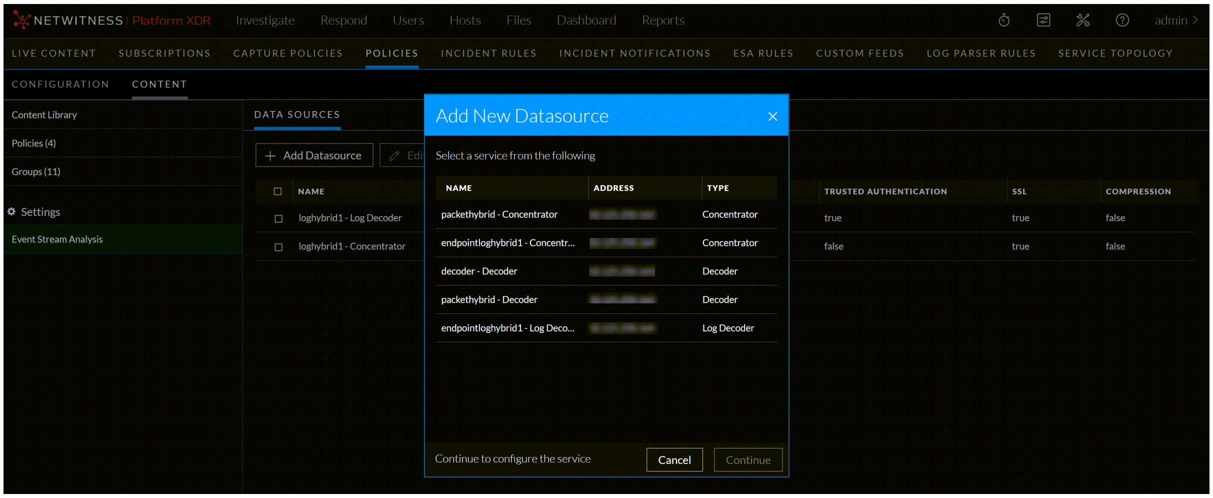
To add an ESA Datasource

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

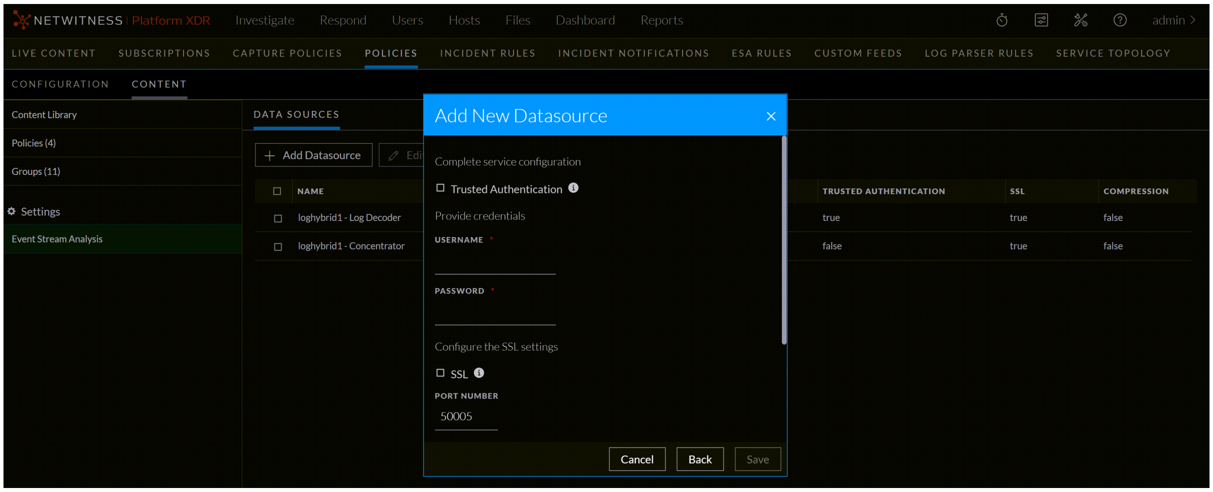
NAME	ADDRESS	TYPE
packethybrid - Concentrator	[redacted]	Concentrator
endpointloghybrid1 - Concentr...	[redacted]	Concentrator
decoder - Decoder	[redacted]	Decoder
packethybrid - Decoder	[redacted]	Decoder
endpointloghybrid1 - Log Deco...	[redacted]	Log Decoder

Continue to configure the service

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

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.

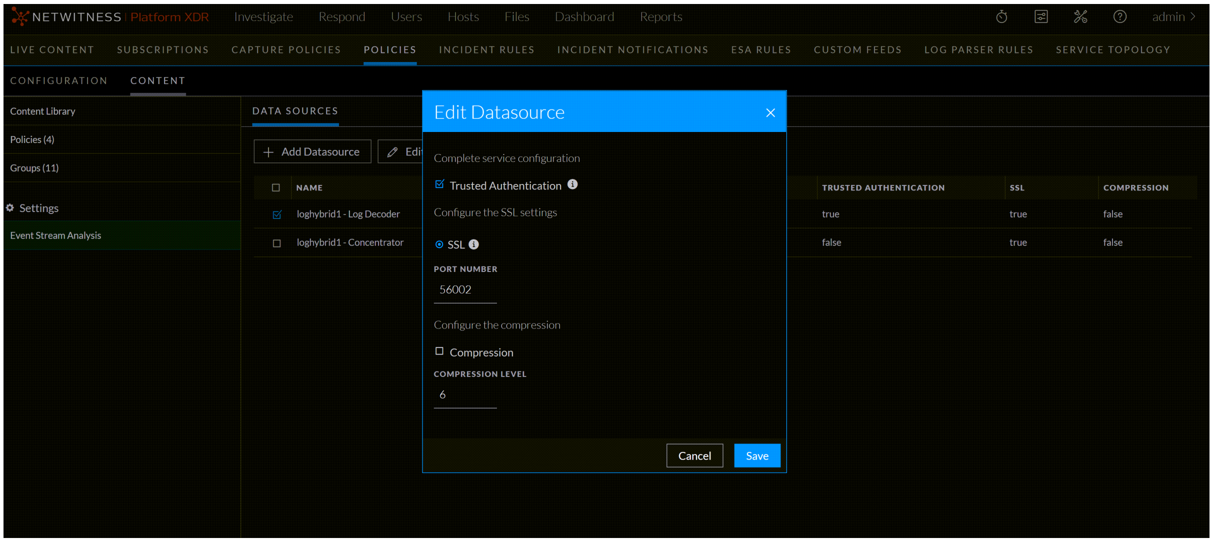
Edit an ESA Datasource

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
- 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 XDR provides two methods to manage deployments.

You can view deployments in the following ways:

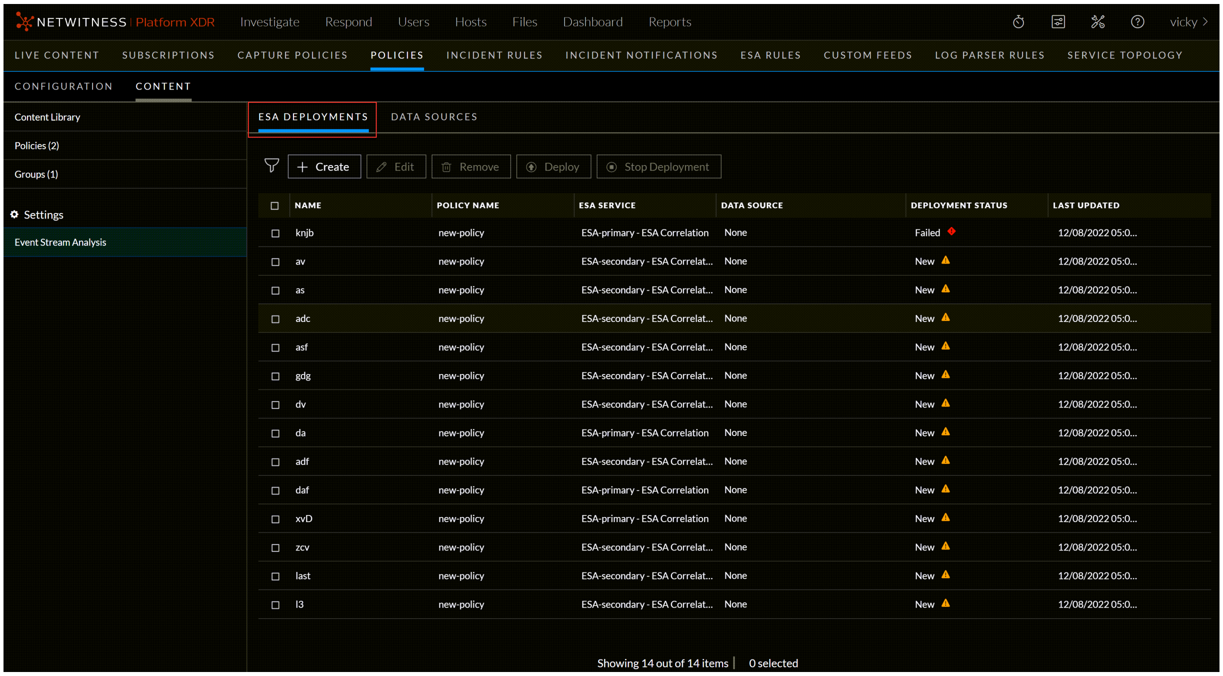
- Using the **ESA Deployments** tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can create, edit, remove, and pause deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and create, 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	LAST UPDATED
□	knjb	new-policy	ESA-primary - ESA Correlation	None	Failed ◆	12/08/2022 05:0...
□	av	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	as	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	adc	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	asf	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	gdg	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	dv	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	da	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
□	adf	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	daf	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
□	xvD	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
□	zcv	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	last	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	l3	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...

Showing 14 out of 14 items | 0 selected

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.

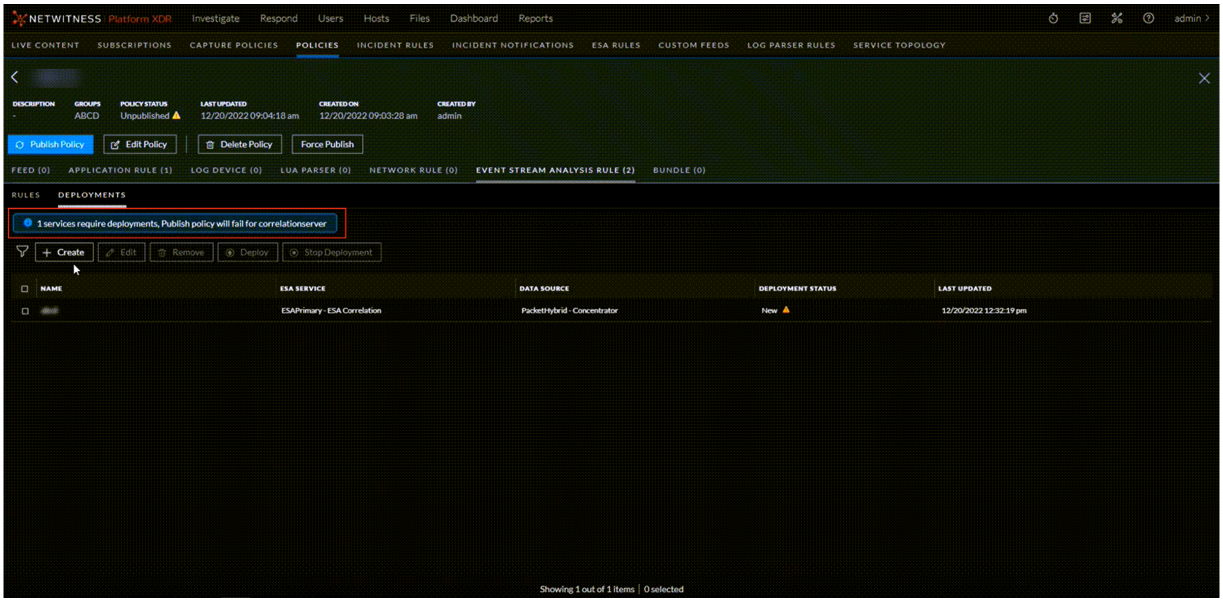
3. Click a Policy.

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.

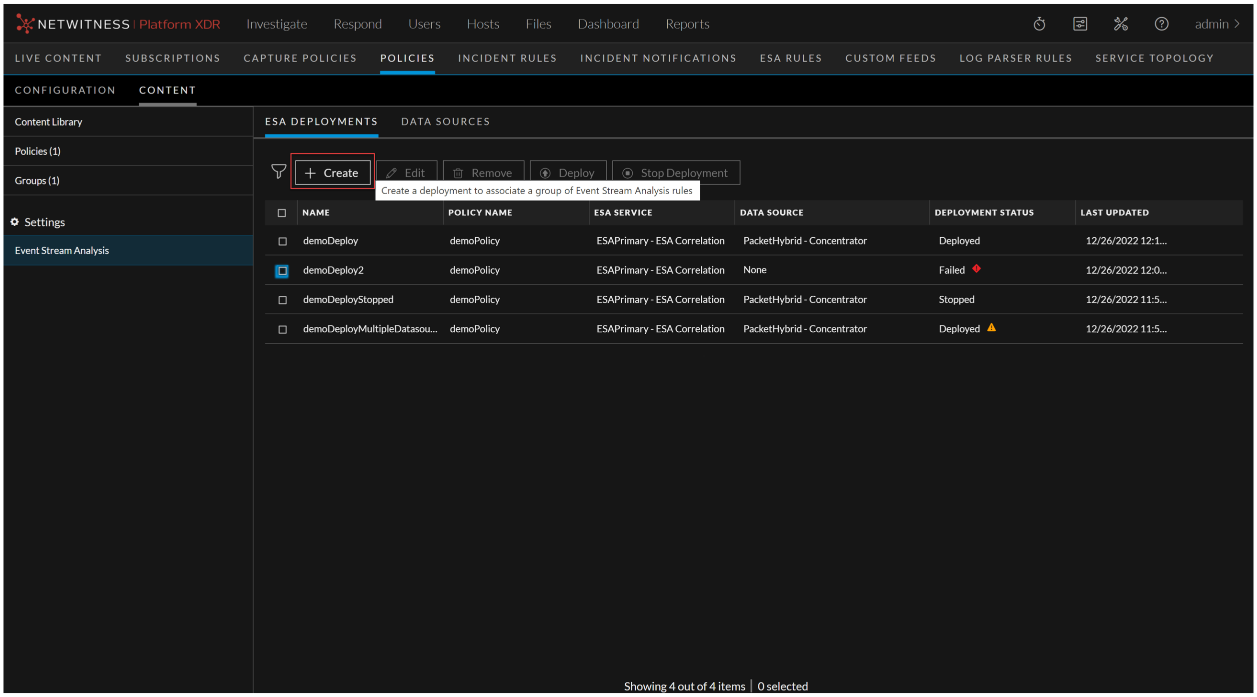
  For more information about groups, see Groups

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**

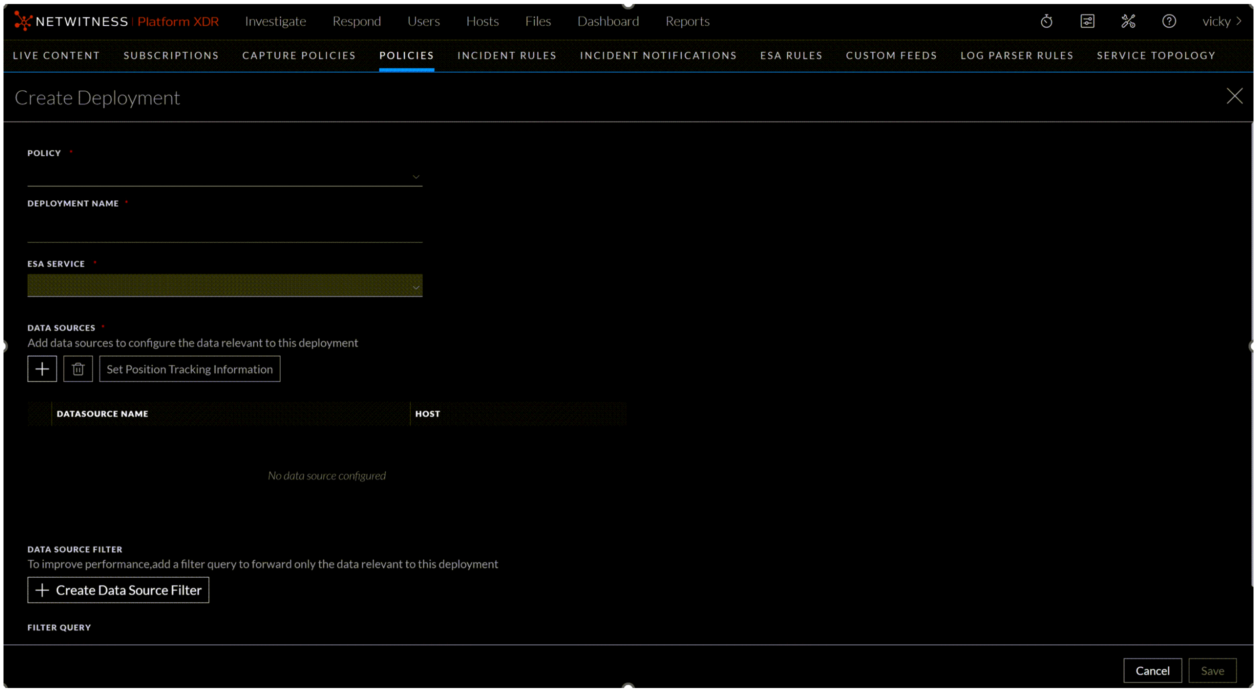


Create a deployment to associate a group of Event Stream Analysis rules

□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
□	demoDeploy	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed	12/26/2022 12:1...
□	demoDeploy2	demoPolicy	ESAPrimary - ESA Correlation	None	Failed ◆	12/26/2022 12:0...
□	demoDeployStopped	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Stopped	12/26/2022 11:5...
□	demoDeployMultipleDatasou...	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed ⚠	12/26/2022 11:5...

Showing 4 out of 4 items | 0 selected

The Create Deployment dialog is displayed.



Add data sources to configure the data relevant to this deployment

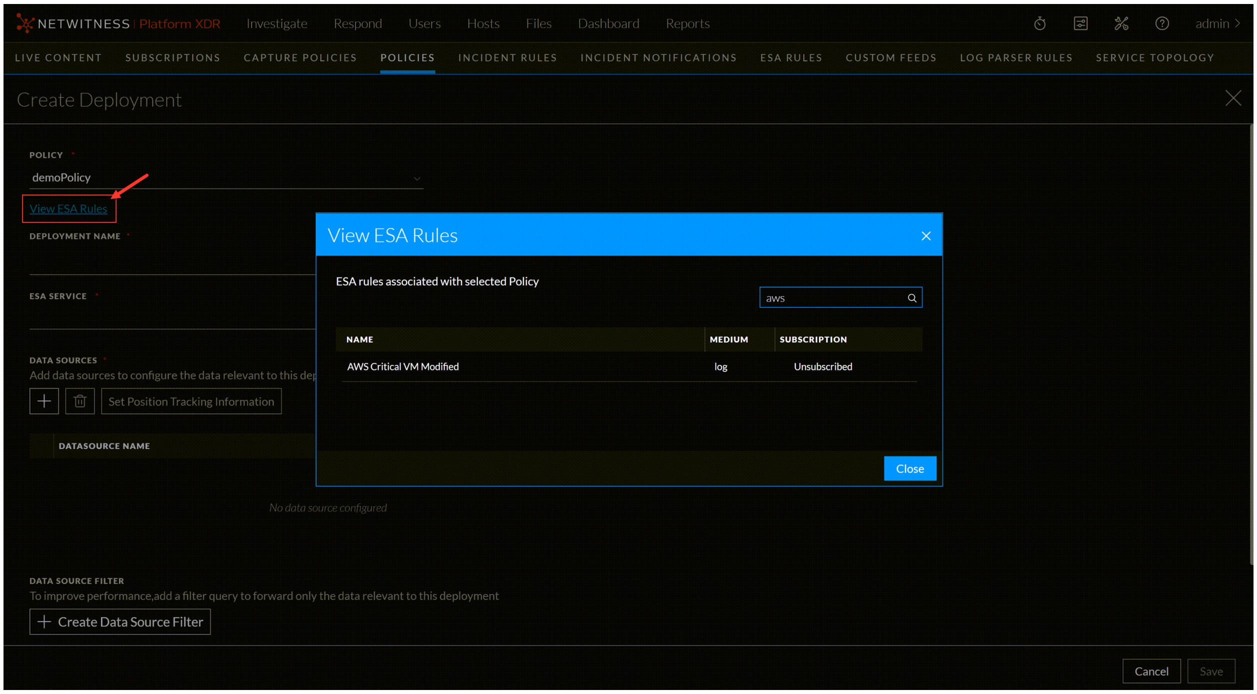
No data source configured

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

Add data sources to configure the data relevant to this dep

No data source configured

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

ESA rules associated with selected Policy

aws

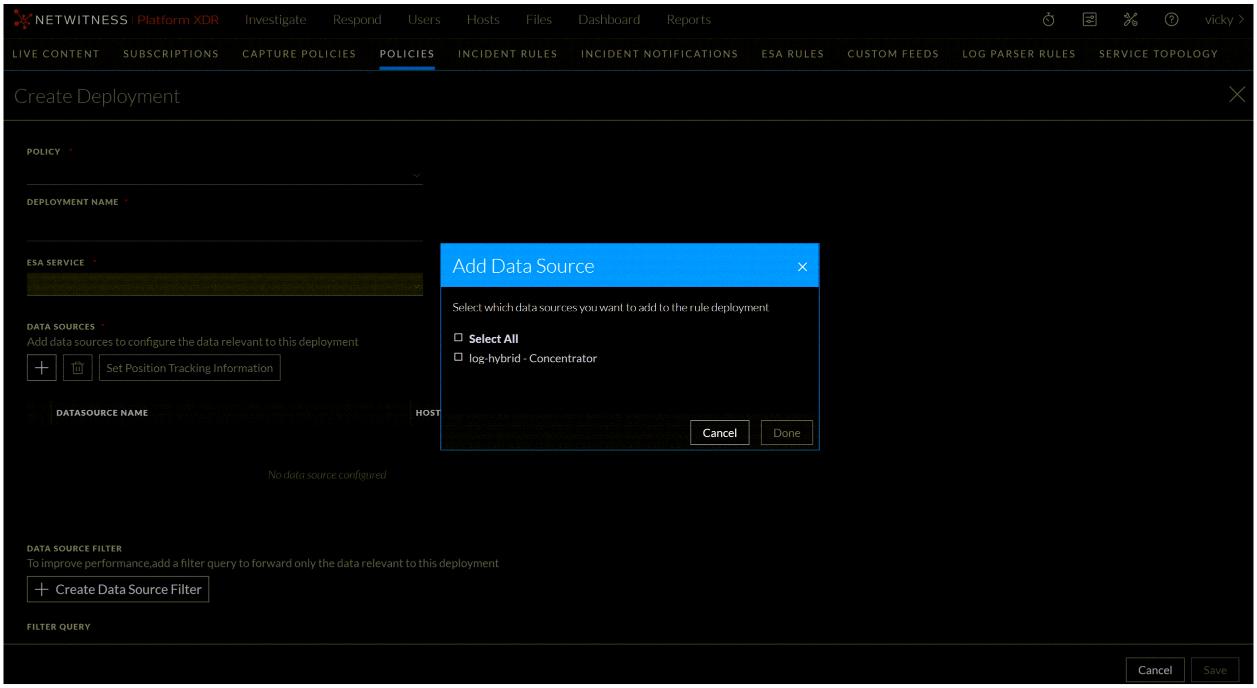
NAME	MEDIUM	SUBSCRIPTION
AWS Critical VM Modified	log	Unsubscribed

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.



Create Deployment

POLICY *

DEPLOYMENT NAME *

ESA SERVICE *

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

DATASOURCE NAME	HOST

No data source configured

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

FILTER QUERY

Add Data Source

Select which data sources you want to add to the rule deployment

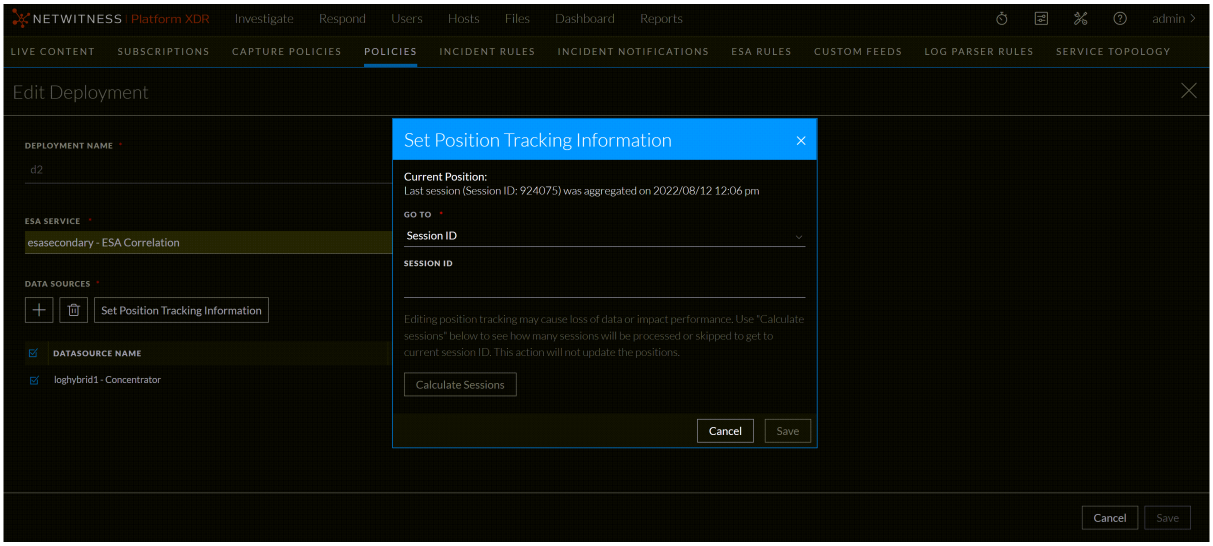
☐ **Select All**
☐ log-hybrid - Concentrator

8. 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.

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.

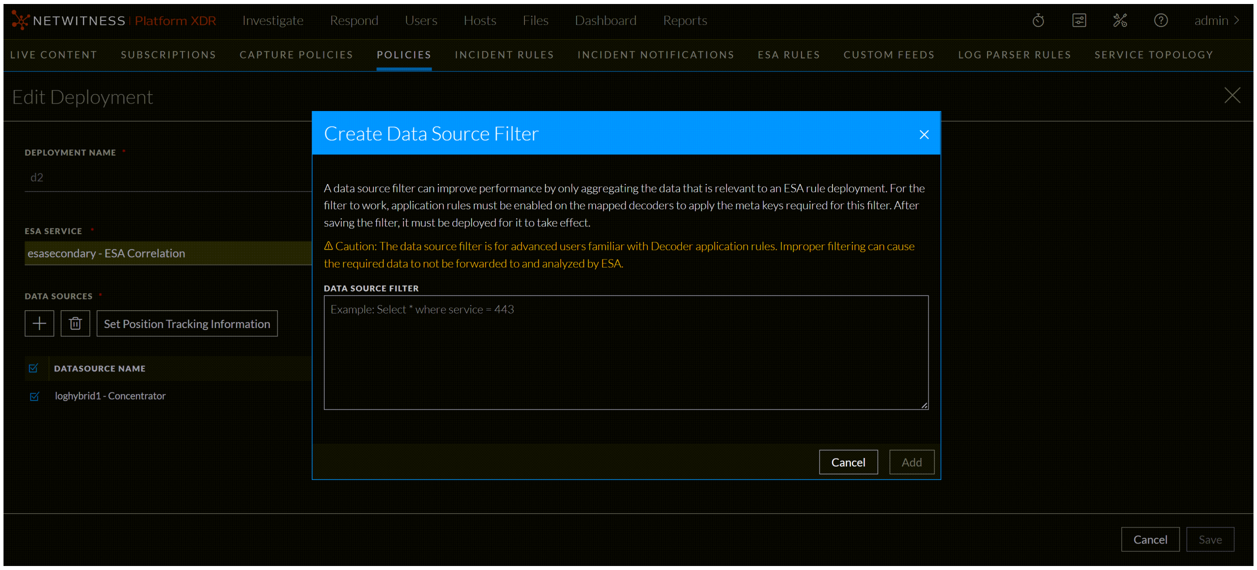
c. To save the edited position tracking data source, click **Save**.

   For more information on Position Tracking Information, see Appendix B: 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

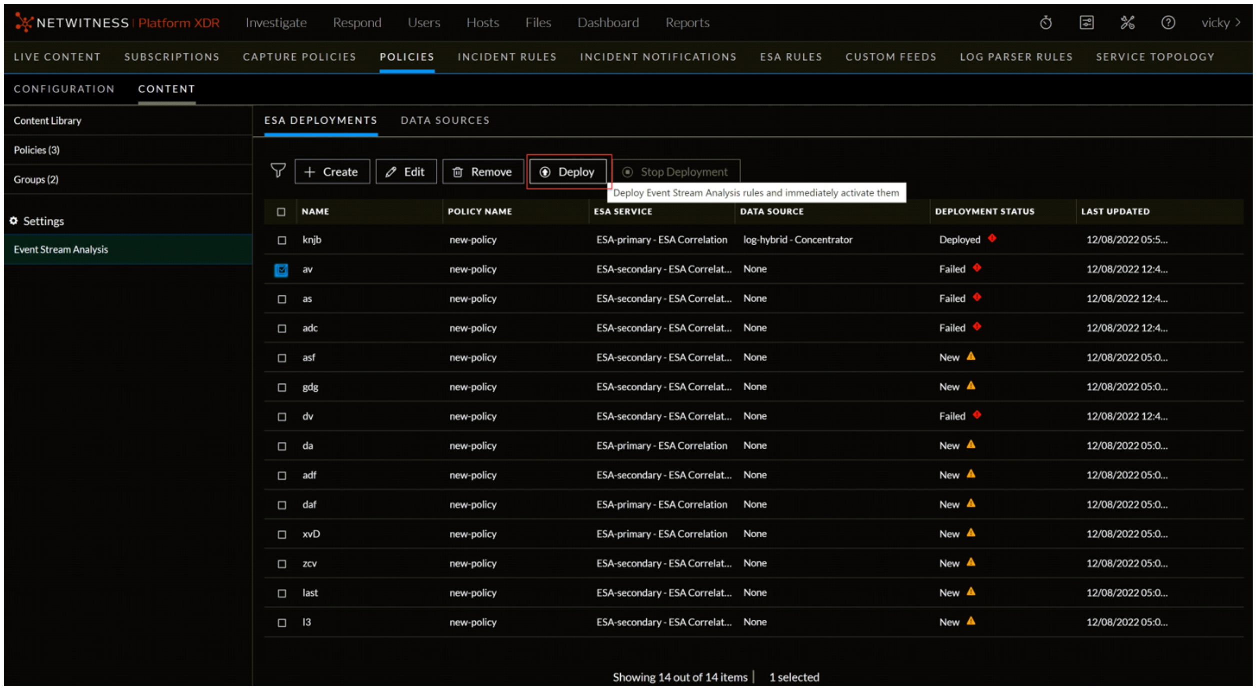
Based on the query processed, it will filter out only HTTPS logs-related sessions and will be forwarded to the ESA.

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	LAST UPDATED
□	knjb	new-policy	ESA-primary - ESA Correlation	log-hybrid - Concentrator	Deployed ◆	12/08/2022 05:5...
☑	av	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
□	as	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
□	adc	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
□	asf	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	gdg	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	dv	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
□	da	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
□	adf	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	daf	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
□	xvD	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
□	zcv	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	last	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
□	l3	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...

Showing 14 out of 14 items | 1 selected

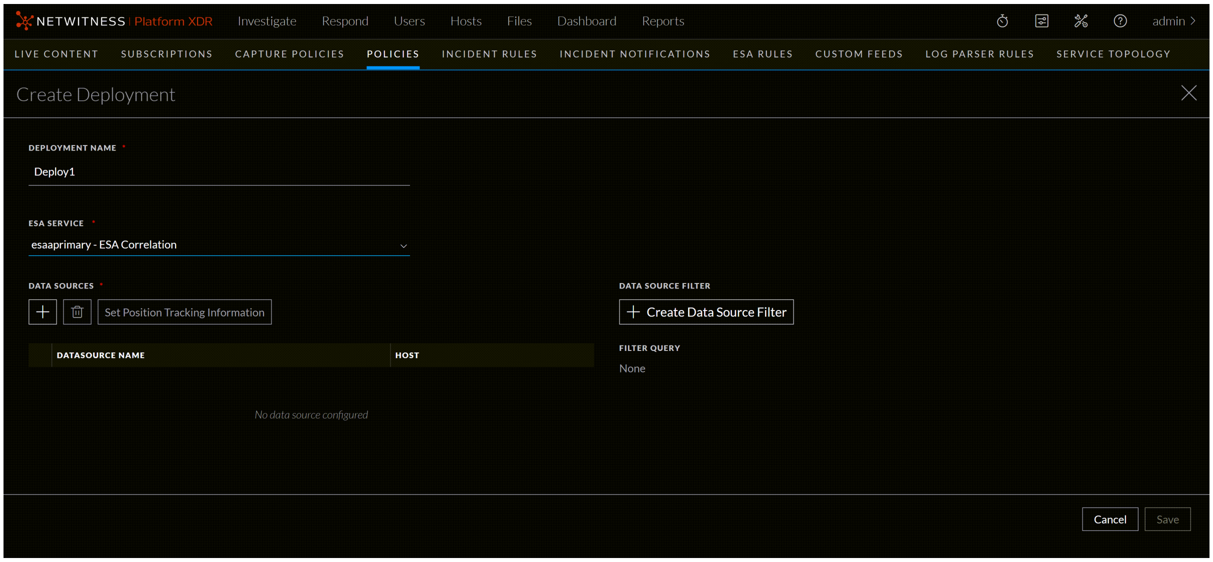
To create a deployment from a selected policy

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.



DEPLOYMENT NAME *: Deploy1

ESA SERVICE *: esaaprimary - ESA Correlation

DATA SOURCES *

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.

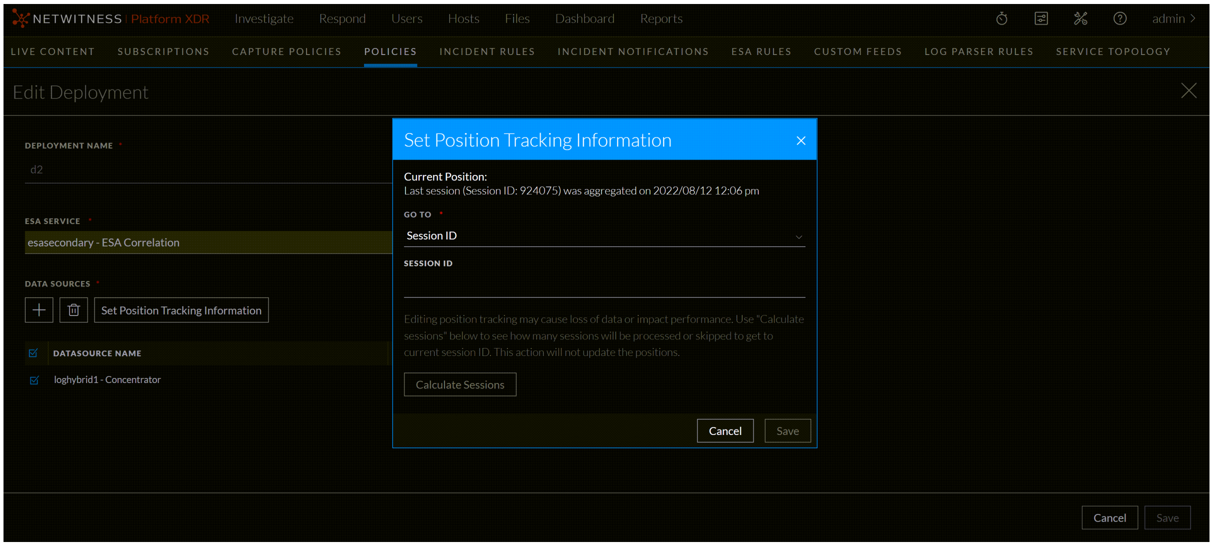
7. Select a service from the **ESA Service** drop-down list.
8. Under **Data Sources**, click + to add a data source.

   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.



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 with respect to the existing position of the data source, if any.

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

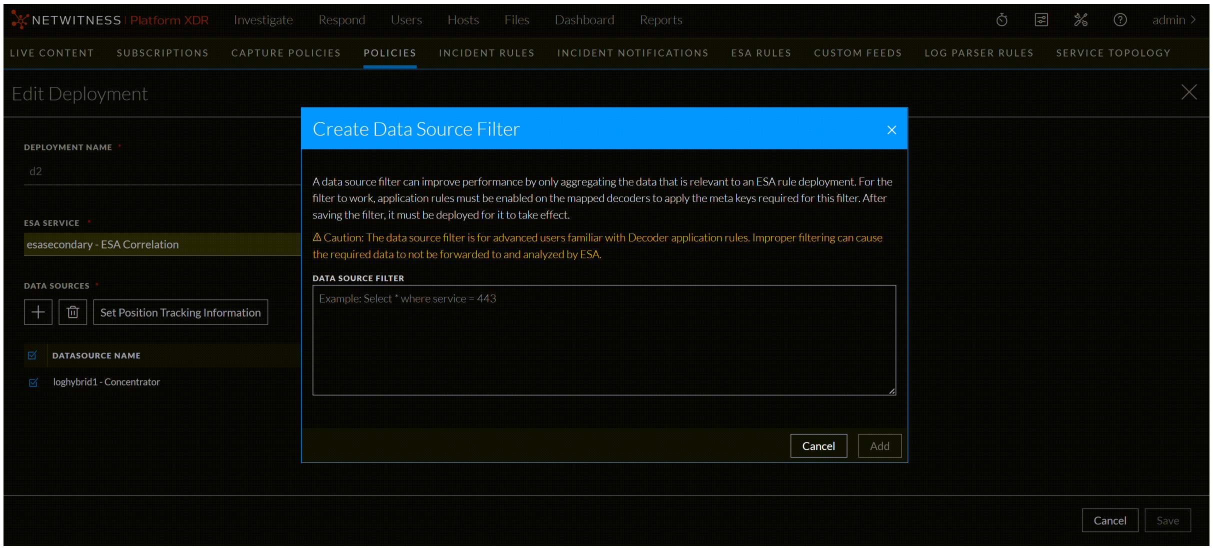
d. The tracking position information will be deployed to the ESA Correlation service, only when the deployment is successfully completed.

   For more information on Position Tracking Information, see Appendix B: 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.

NetWitness Platform XDR provides two methods to manage deployments.

You can edit deployments in the following ways:

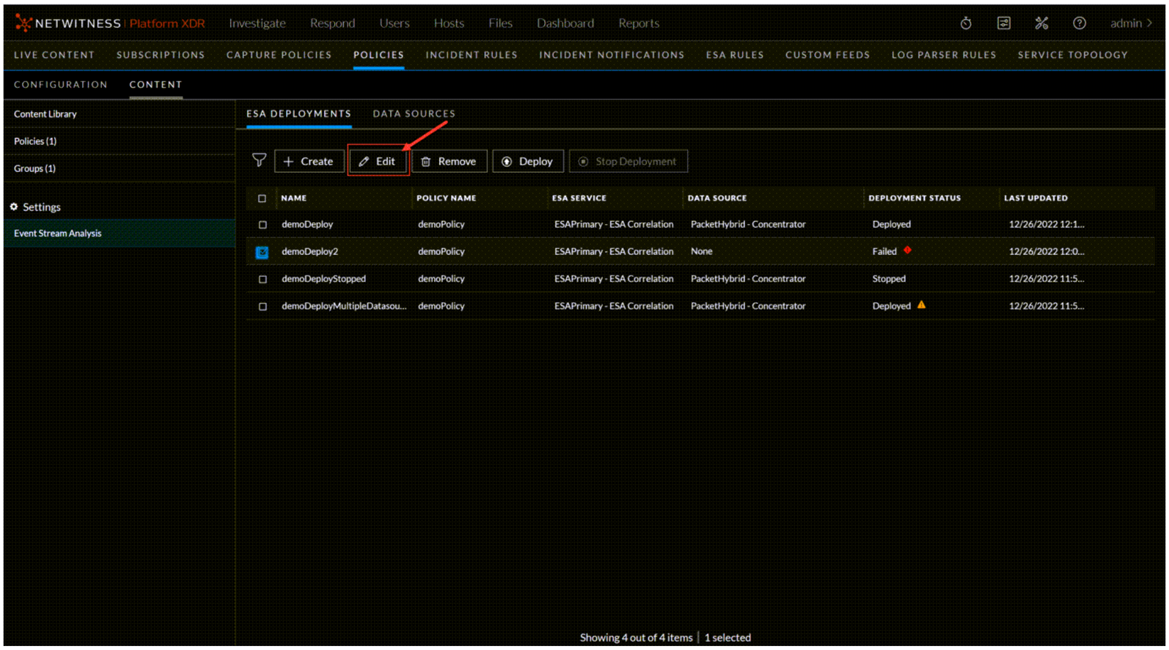
- Using the ESA Deployments tab. The **ESA Deployments** tab provides a consolidated view of all the available deployments within CCM. You can edit deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and edit a deployment.

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.

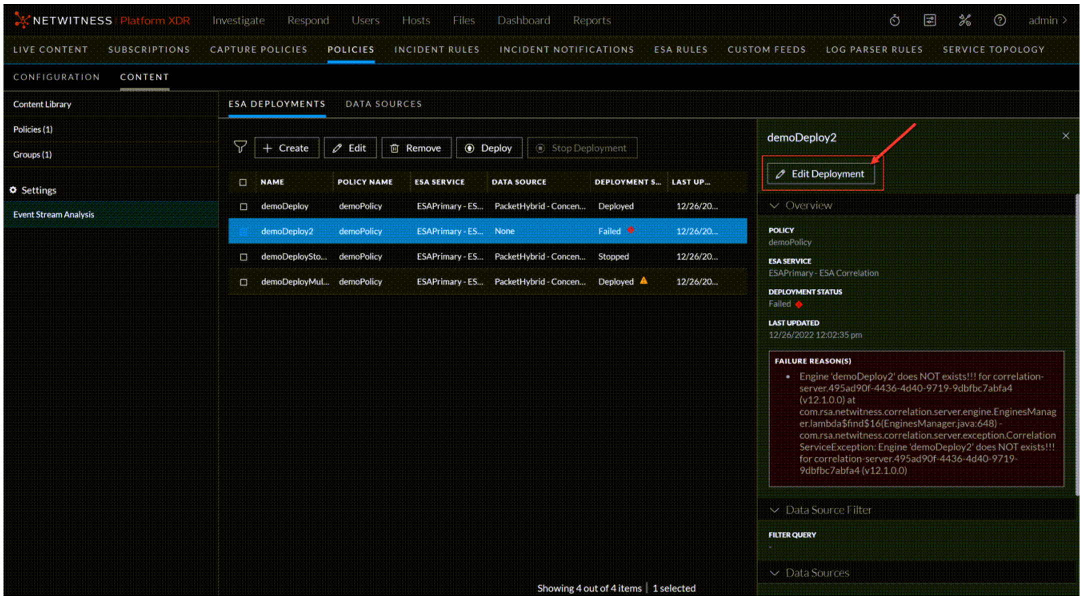
3. Select a deployment and click **Edit** or **Edit Deployment**.
   a. When you select the checkbox and click **Edit**.



□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
□	demoDeploy	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed	12/26/2022 12:1...
☑	demoDeploy2	demoPolicy	ESAPrimary - ESA Correlation	None	Failed ◆	12/26/2022 12:0...
□	demoDeployStopped	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Stopped	12/26/2022 11:5...
□	demoDeployMultipleDatasou...	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed ⚠	12/26/2022 11:5...

Showing 4 out of 4 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 ◆

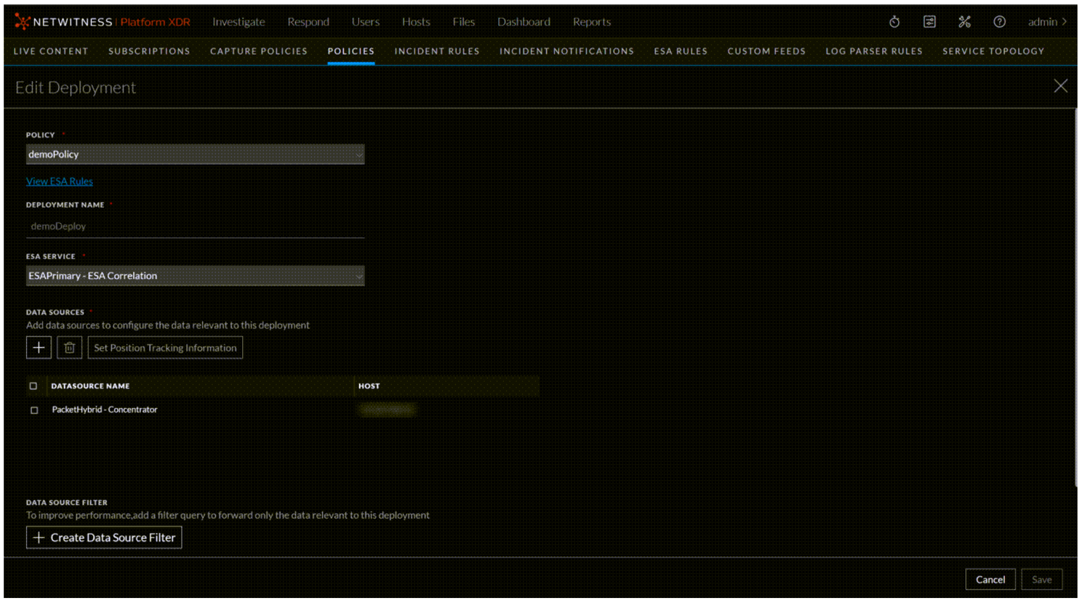
LAST UPDATED
12/26/2022 12:02:35 pm

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

DEPLOYMENT NAME *
demoDeploy

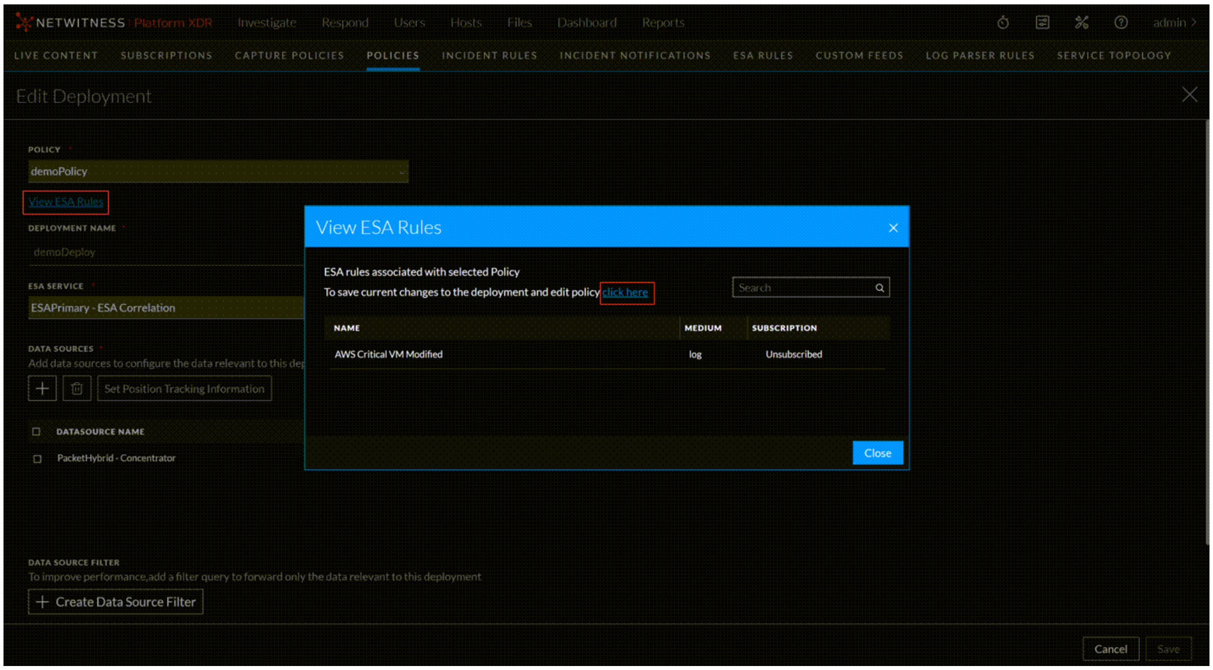
ESA SERVICE *
ESAPrimary - ESA Correlation

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.



Edit Deployment

POLICY *
demoPolicy

DEPLOYMENT NAME *
demoDeploy

ESA SERVICE *
ESAPrimary - ESA Correlation

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

□	DATASOURCE NAME
□	PacketHybrid - Concentrator

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

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. Click **Save**.

7. 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.

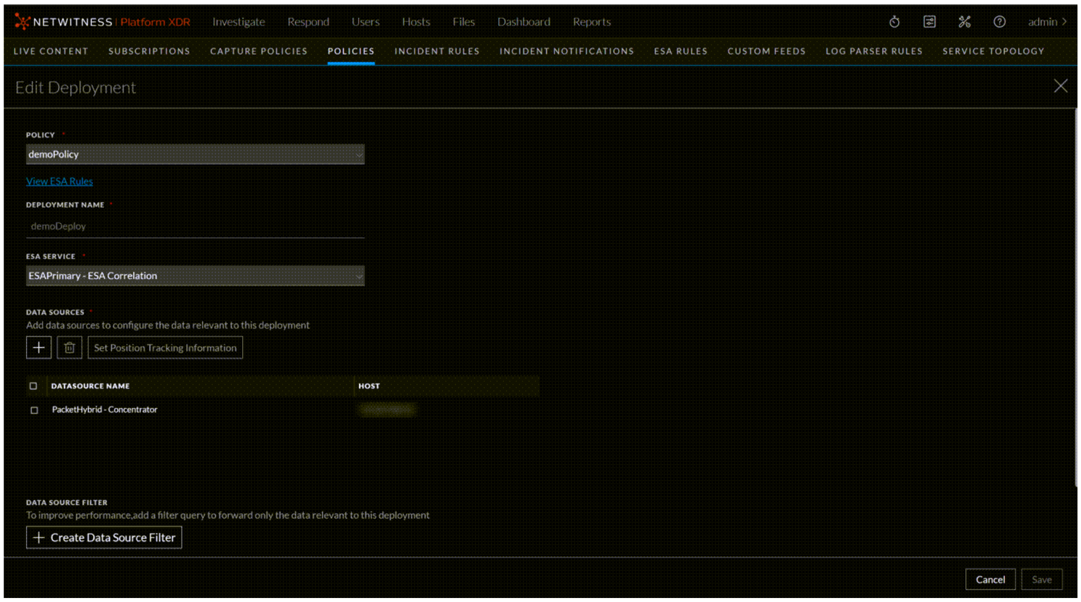
   The selected policy view is displayed and by default **Application Rule** is selected.

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:

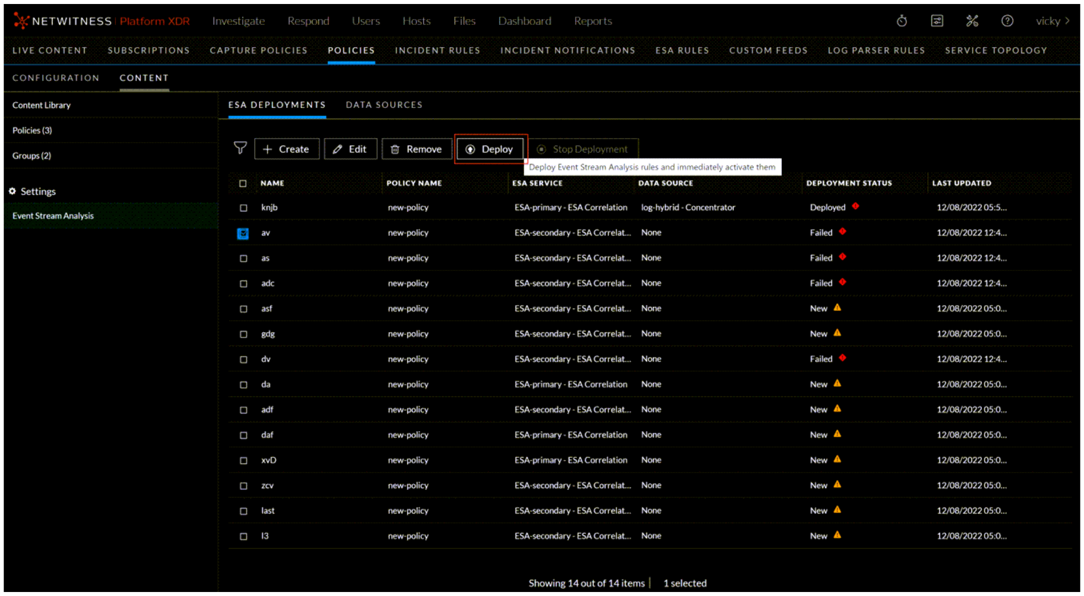
- Using the ESA Deployments tab. The ESA Deployments tab provides a consolidated view of all the available deployments within CCM. You can initiate deployments.
- Using a specific policy. In this method, you cannot view other deployments. You need to go to each policy and initiate a deployment.

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**.



Deploy Event Stream Analysis rules and immediately activate them

☐	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
☐	knjb	new-policy	ESA-primary - ESA Correlation	log-hybrid - Concentrator	Deployed ◆	12/08/2022 05:5...
☑	av	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
☐	as	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
☐	adc	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
☐	asf	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
☐	gdg	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
☐	dv	new-policy	ESA-secondary - ESA Correlat...	None	Failed ◆	12/08/2022 12:4...
☐	da	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
☐	adf	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
☐	daf	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
☐	xvD	new-policy	ESA-primary - ESA Correlation	None	New ⚠	12/08/2022 05:0...
☐	zcv	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
☐	last	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...
☐	l3	new-policy	ESA-secondary - ESA Correlat...	None	New ⚠	12/08/2022 05:0...

Showing 14 out of 14 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.

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.

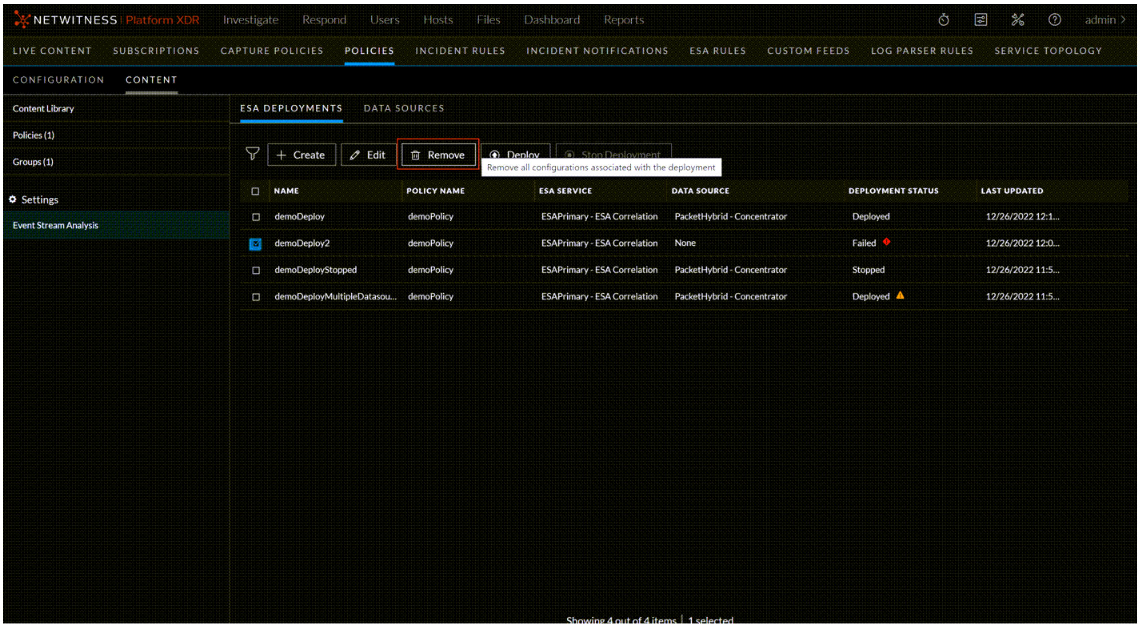
To remove a deployment from the ESA Deployments tab

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**.



Remove all configurations associated with the deployment

□	NAME	POLICY NAME	ESA SERVICE	DATA SOURCE	DEPLOYMENT STATUS	LAST UPDATED
□	demoDeploy	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed	12/26/2022 12:1...
☑	demoDeploy2	demoPolicy	ESAPrimary - ESA Correlation	None	Failed ◆	12/26/2022 12:0...
□	demoDeployStopped	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Stopped	12/26/2022 11:5...
□	demoDeployMultipleDatasou...	demoPolicy	ESAPrimary - ESA Correlation	PacketHybrid - Concentrator	Deployed ⚠	12/26/2022 11:5...

Showing 4 out of 4 items | 1 selected

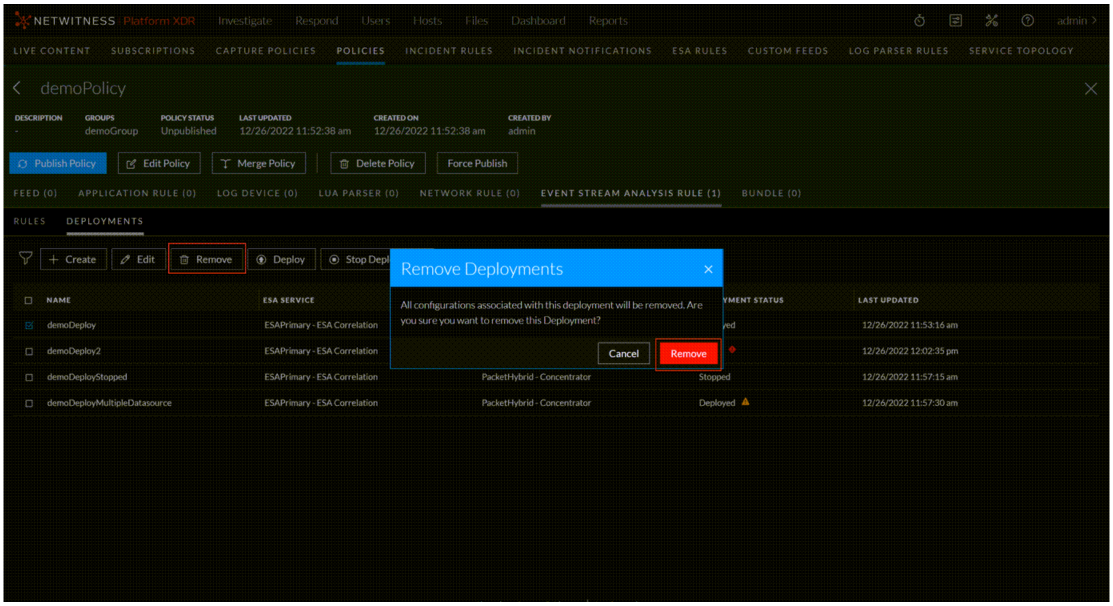
To remove a deployment from a selected policy

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

Remove Deployments

All configurations associated with this deployment will be removed. Are you sure you want to remove this Deployment?

Cancel | Remove

☐	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

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

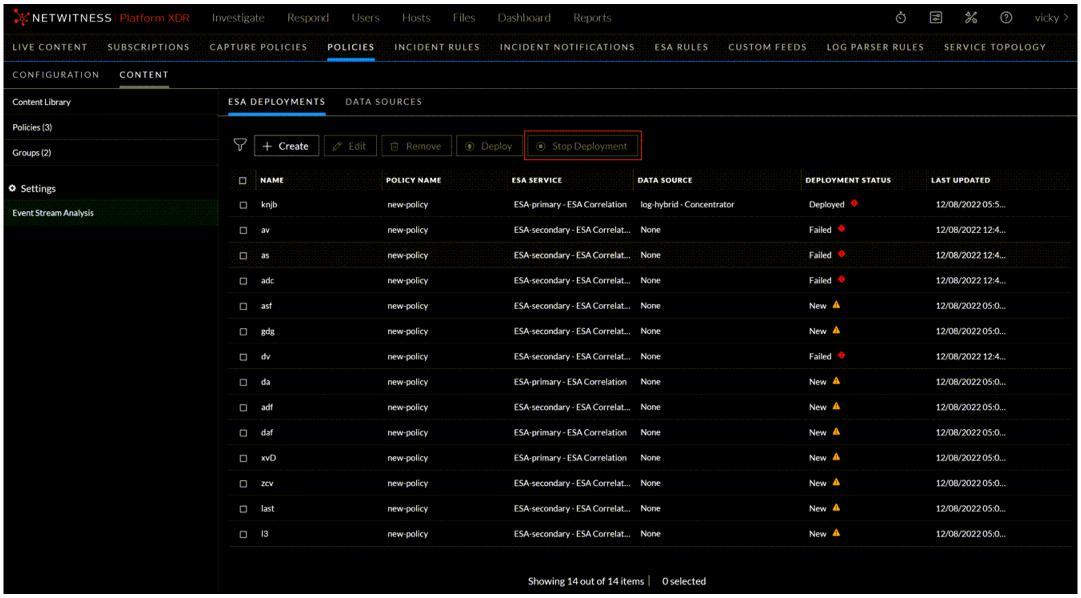
You can stop deployments in the following ways:

- 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	DEPLOYMENT STATUS	LAST UPDATED
knjb	new-policy	ESA-primary - ESA Correlation	log-hybrid - Concentrator	Deployed	12/08/2022 05:5...
av	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
as	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
adc	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
asf	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
gdg	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
dv	new-policy	ESA-secondary - ESA Correlat...	None	Failed	12/08/2022 12:4...
da	new-policy	ESA-primary - ESA Correlation	None	New	12/08/2022 05:0...
adf	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
daf	new-policy	ESA-primary - ESA Correlation	None	New	12/08/2022 05:0...
xvD	new-policy	ESA-primary - ESA Correlation	None	New	12/08/2022 05:0...
zcv	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
last	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...
l3	new-policy	ESA-secondary - ESA Correlat...	None	New	12/08/2022 05:0...

Showing 14 out of 14 items | 0 selected

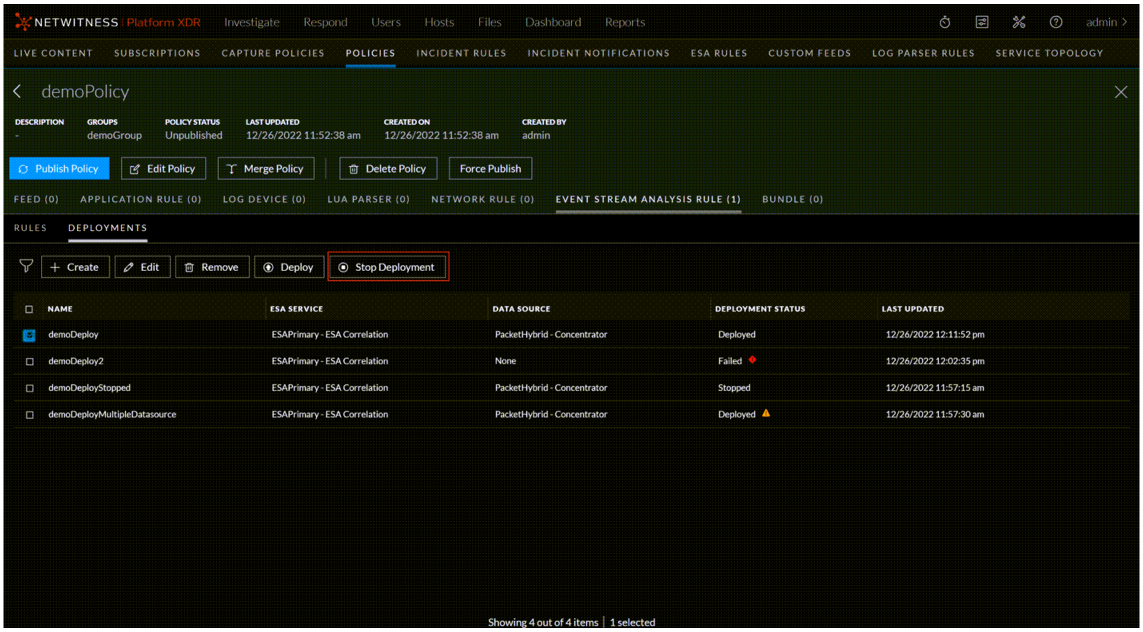
To stop a deployment from a selected policy

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

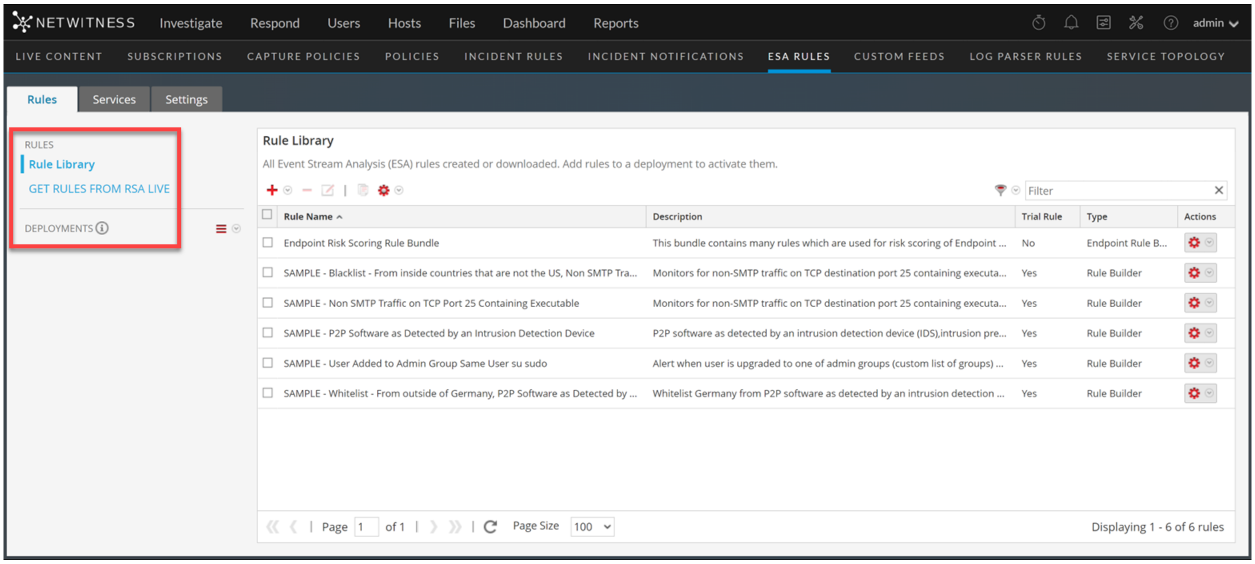
Showing 4 out of 4 items | 1 selected

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.

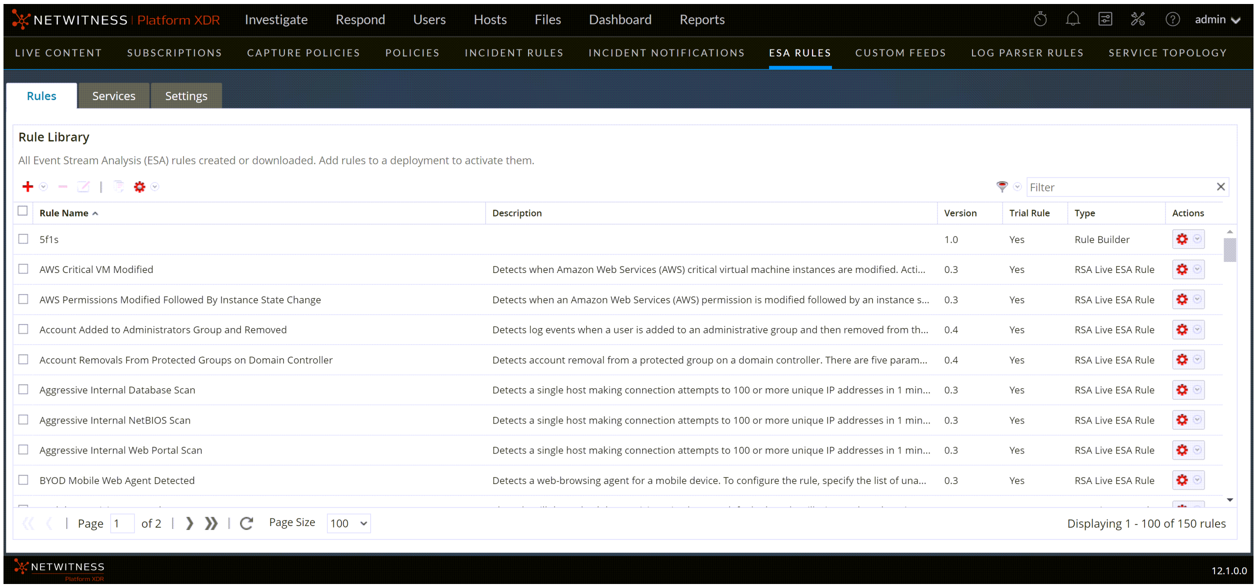
☐	Rule Name	Description	Trial Rule	Type	Actions
☐	Endpoint Risk Scoring Rule Bundle	This bundle contains many rules which are used for risk scoring of Endpoint ...	No	Endpoint Rule B...	
☐	SAMPLE - Blacklist - From inside countries that are not the US, Non SMTP Tra...	Monitors for non-SMTP traffic on 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	

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:

SINo	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.

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

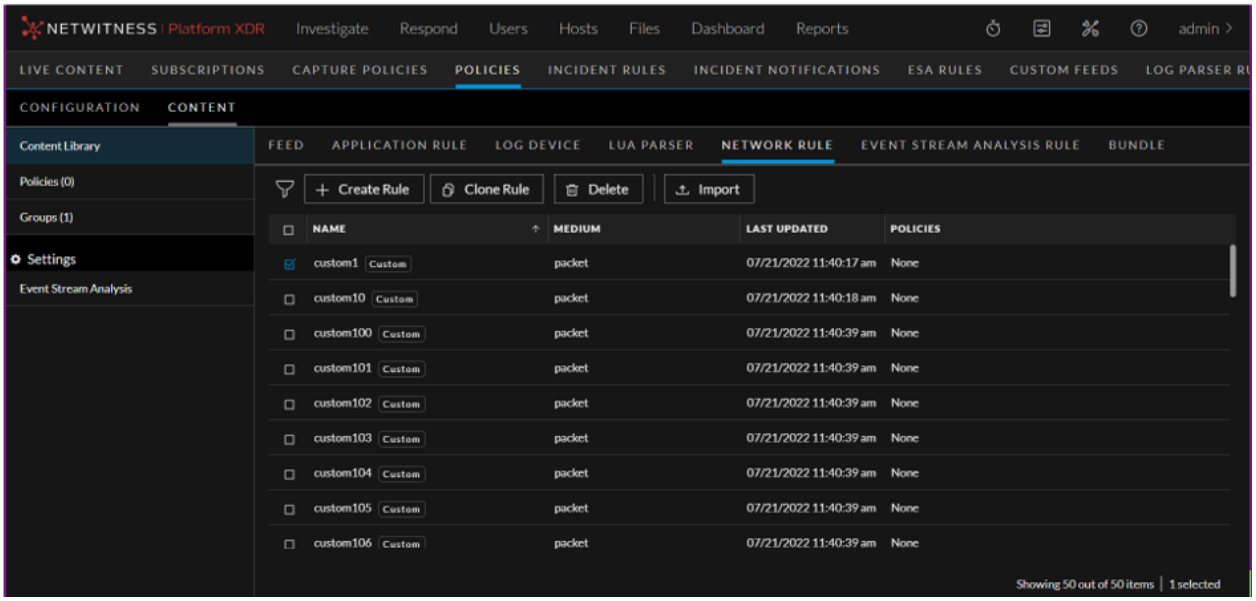
Content Library Tab

The (CONFIGURE) > **Policies** view contains two tabs: **Configuration** and **Content**.

The **CONTENT** tab has **Content Library**, **Policies** and **Groups** on the left panel.

Below is an example of the **Content** > **Content Library** tab:

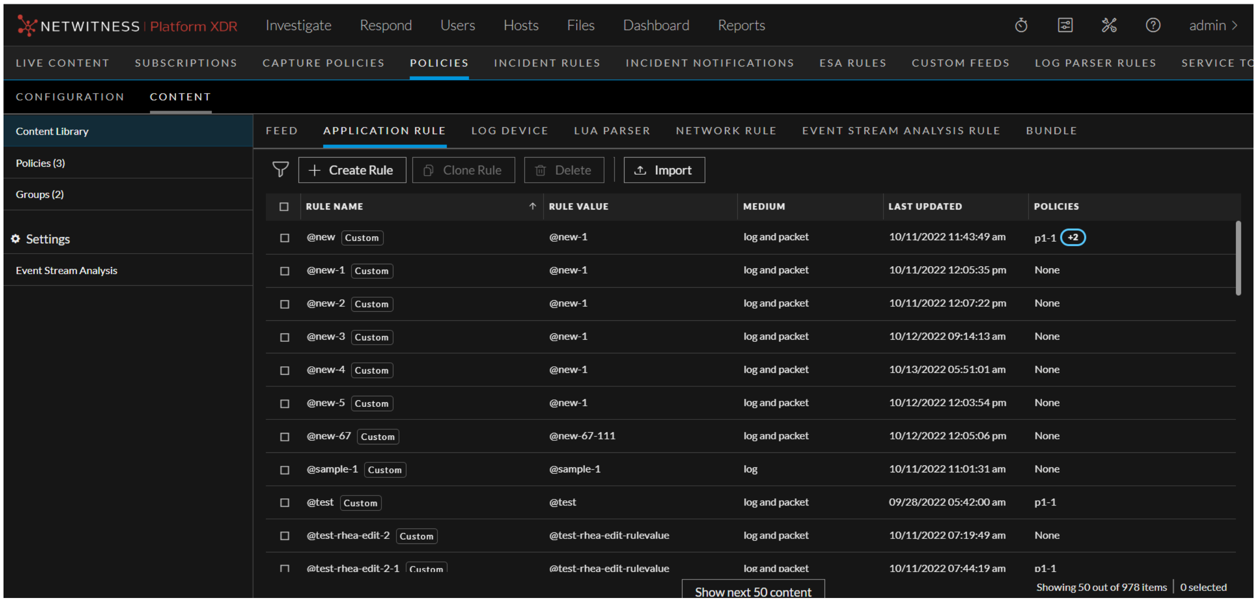
12.1 Version:



□	NAME	MEDIUM	LAST UPDATED	POLICIES
☑	custom1 Custom	packet	07/21/2022 11:40:17 am	None
□	custom10 Custom	packet	07/21/2022 11:40:18 am	None
□	custom100 Custom	packet	07/21/2022 11:40:39 am	None
□	custom101 Custom	packet	07/21/2022 11:40:39 am	None
□	custom102 Custom	packet	07/21/2022 11:40:39 am	None
□	custom103 Custom	packet	07/21/2022 11:40:39 am	None
□	custom104 Custom	packet	07/21/2022 11:40:39 am	None
□	custom105 Custom	packet	07/21/2022 11:40:39 am	None
□	custom106 Custom	packet	07/21/2022 11:40:39 am	None

Showing 50 out of 50 items | 1 selected

12.1.1 Version:



□	RULE NAME	RULE VALUE	MEDIUM	LAST UPDATED	POLICIES
□	@new Custom	@new-1	log and packet	10/11/2022 11:43:49 am	p1-1 +2
□	@new-1 Custom	@new-1	log and packet	10/11/2022 12:05:35 pm	None
□	@new-2 Custom	@new-1	log and packet	10/11/2022 12:07:22 pm	None
□	@new-3 Custom	@new-1	log and packet	10/12/2022 09:14:13 am	None
□	@new-4 Custom	@new-1	log and packet	10/13/2022 05:51:01 am	None
□	@new-5 Custom	@new-1	log and packet	10/12/2022 12:03:54 pm	None
□	@new-67 Custom	@new-67-111	log and packet	10/12/2022 12:05:06 pm	None
□	@sample-1 Custom	@sample-1	log	10/11/2022 11:01:31 am	None
□	@test Custom	@test	log and packet	09/28/2022 05:42:00 am	p1-1
□	@test-rhea-edit-2 Custom	@test-rhea-edit-rulevalue	log and packet	10/11/2022 07:19:49 am	None
□	@test-rhea-edit-2-1 Custom	@test-rhea-edit-rulevalue	log and packet	10/11/2022 07:44:19 am	p1-1

Showing 50 out of 978 items | 0 selected

1 Toolbar

- Create Rule - Lets you create a rule.
- Clone Rue - 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.

2 Rule List Pane for 12.1 Version:

- Name - Name of the rule.
- 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.

Rule List Pane for 12.1.1 Version:

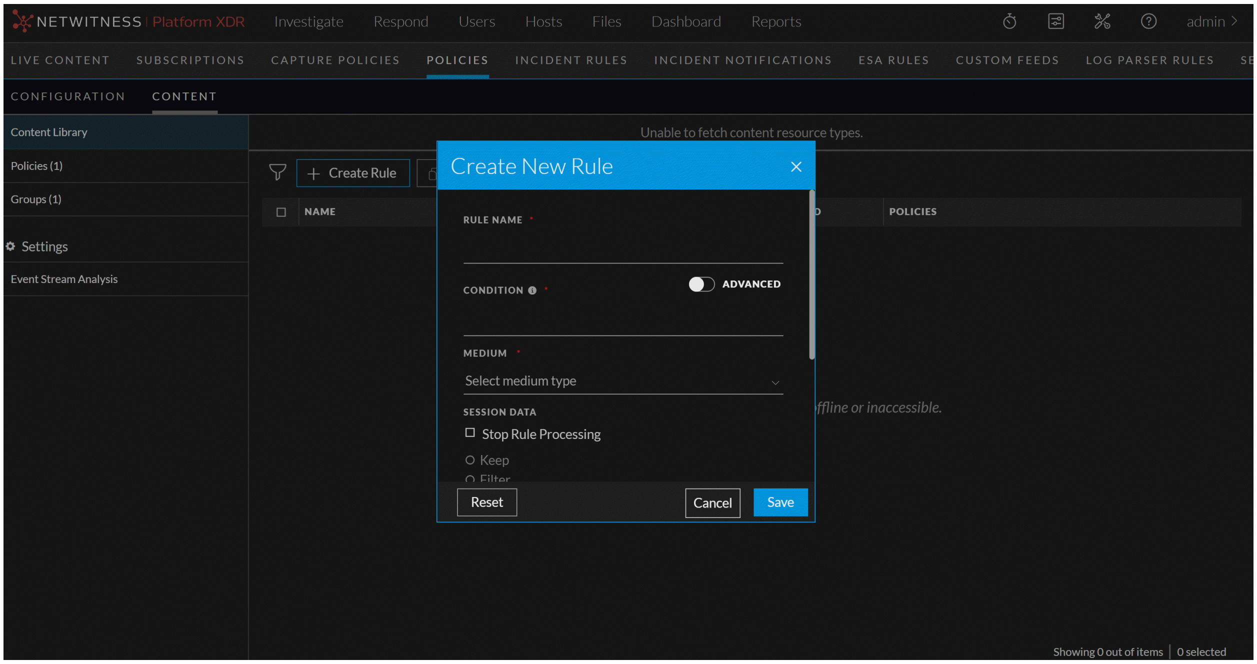
- Rule Name - Name of the rule.
- Rule Value - The rule value.
- Medium - Medium through which the rule is created.
- Last Updated - Displays the time when the rule is updated.
- Policies - Policies to which the rule is applied.

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 for 12.1 version:



Unable to fetch content resource types.

Create New Rule

RULE NAME *

CONDITION * ADVANCED

MEDIUM *

Select medium type

SESSION DATA

□ Stop Rule Processing

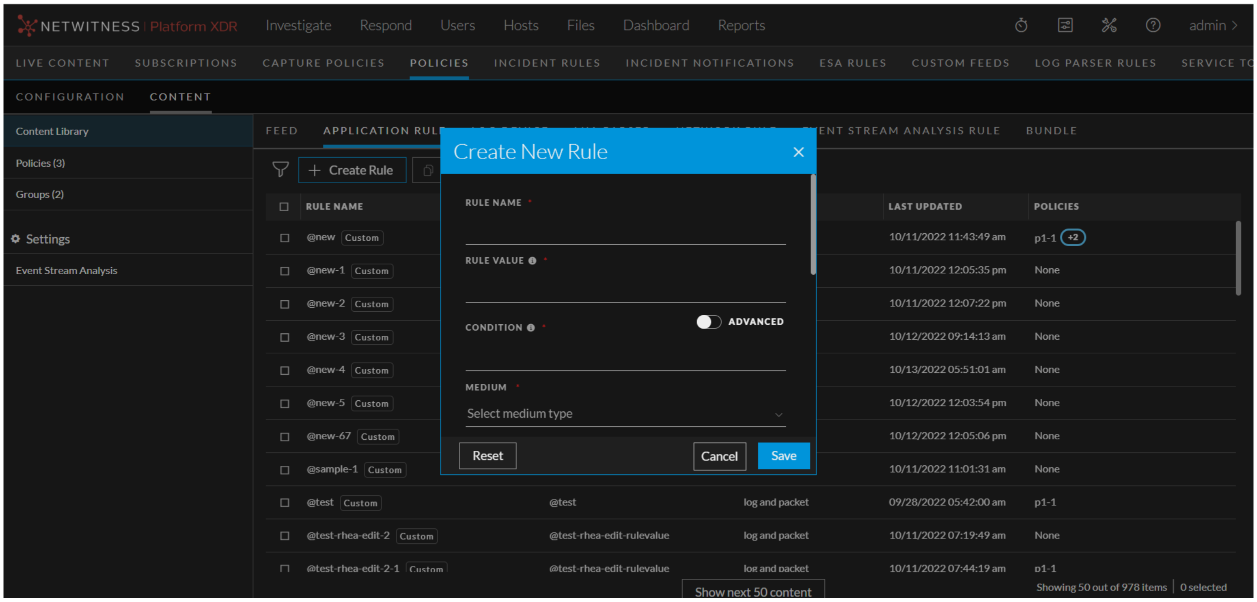
○ Keep

○ Filter

ffline or inaccessible.

Showing 0 out of items | 0 selected

Below is an example of the Create new rule dialog for 12.1.1 version:



RULE NAME			LAST UPDATED	POLICIES
@new Custom			10/11/2022 11:43:49 am	p1-1 +2
@new-1 Custom			10/11/2022 12:05:35 pm	None
@new-2 Custom			10/11/2022 12:07:22 pm	None
@new-3 Custom			10/12/2022 09:14:13 am	None
@new-4 Custom			10/13/2022 05:51:01 am	None
@new-5 Custom			10/12/2022 12:03:54 pm	None
@new-67 Custom			10/12/2022 12:05:06 pm	None
@sample-1 Custom			10/11/2022 11:01:31 am	None
@test Custom	@test	log and packet	09/28/2022 05:42:00 am	p1-1
@test-rhea-edit-2 Custom	@test-rhea-edit-rulevalue	log and packet	10/11/2022 07:19:49 am	None
@test-rhea-edit-2-1 Custom	@test-rhea-edit-rulevalue	log and packet	10/11/2022 07:44:19 am	p1-1

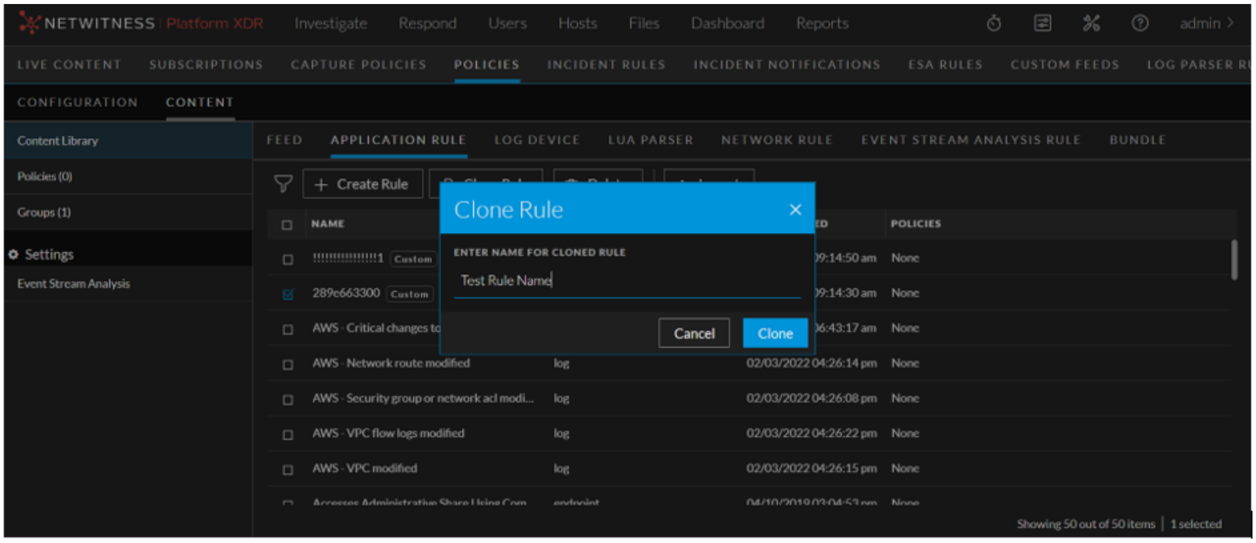
The table describes the information and options in the Create New Rule dialog:

Field	Description
Rule Name	Name of the new rule. The name should be unique.
Rule Value	The rule value written to the alert meta. The rule value cannot be modified while cloning the rule. **Note:** This field is applicable only for 12.1.1 version.
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 the user cannot edit it.
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.
Alert On	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 for 12.1 version.



Clone Rule

ENTER NAME FOR CLONED RULE

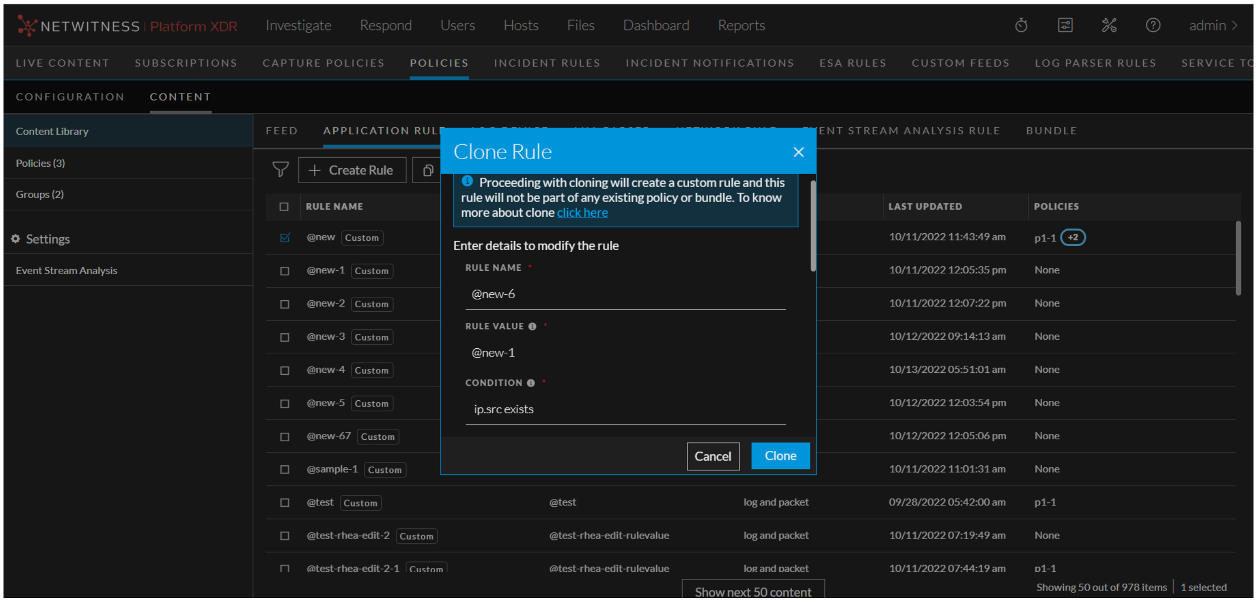
Test Rule Name

Cancel Clone

The table describes the information and options in the Clone Rule dialog for 12.1 version:

Field	Description
Enter Name for Cloned Rule	Name of the cloned rule. The name should be unique.
Clone	Clones the rule and closes the Cone Rule dialog.
Cancel	Cancels the operation.

Below is an example of the Clone rule dialog for 12.1.1 version.



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 *

@new-6

RULE VALUE *

@new-1

CONDITION *

ip.src exists

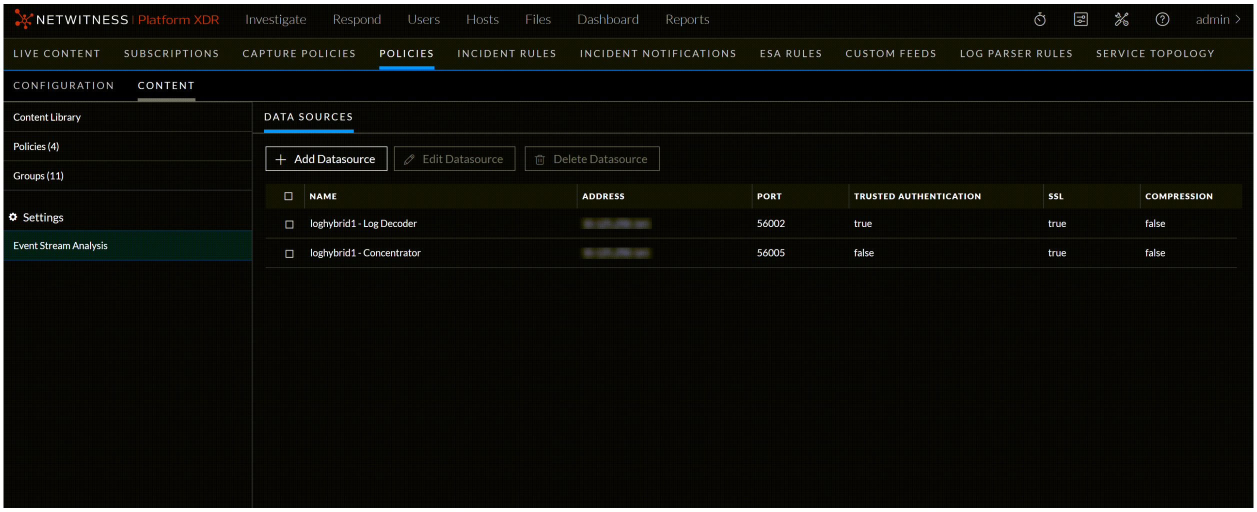
Cancel Clone

The table describes the information and options in the Clone Rule dialog for 12.1.1 version:

Field	Description
Rule Name	Name of the cloned rule. The name should be unique.
Rule Value	The rule value written to the alert meta. The rule value cannot be modified while cloning the rule.
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.
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.
Alert On	Conditions for which the alert should be turned on.
Clone	Clones the rule and closes the Cone Rule dialog.
Cancel	Cancels the operation.

Data Sources Tab

Below is an example of the **Content** > **Settings** > **Event Stream Analysis** > **Data Sources** tab:

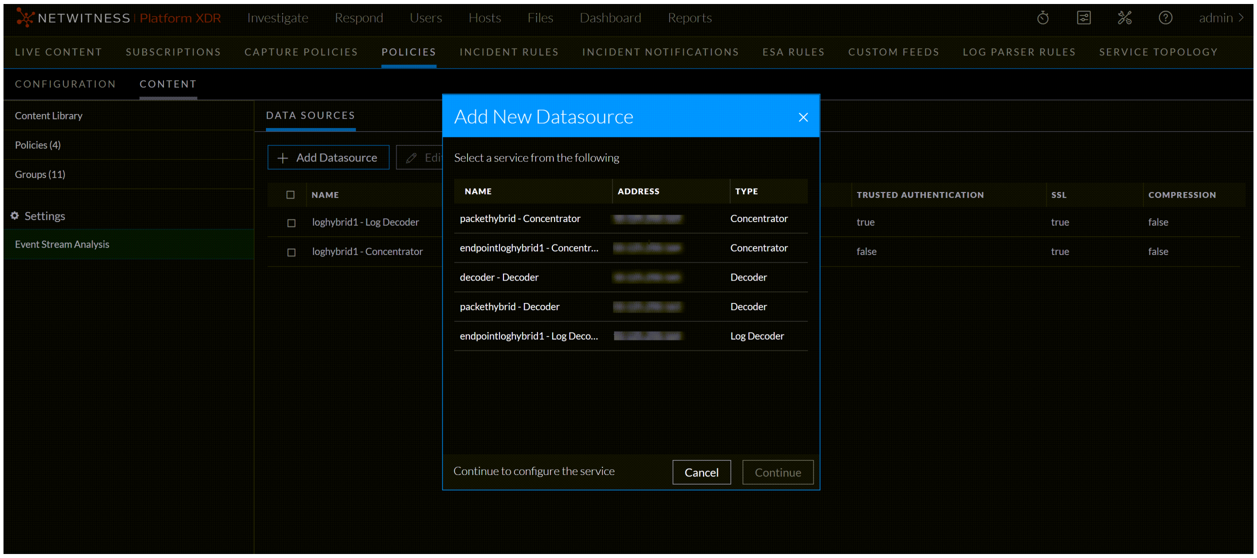


□	NAME	ADDRESS	PORT	TRUSTED AUTHENTICATION	SSL	COMPRESSION
□	loghybrid1 - Log Decoder	[redacted]	56002	true	true	false
□	loghybrid1 - Concentrator	[redacted]	56005	false	true	false

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:

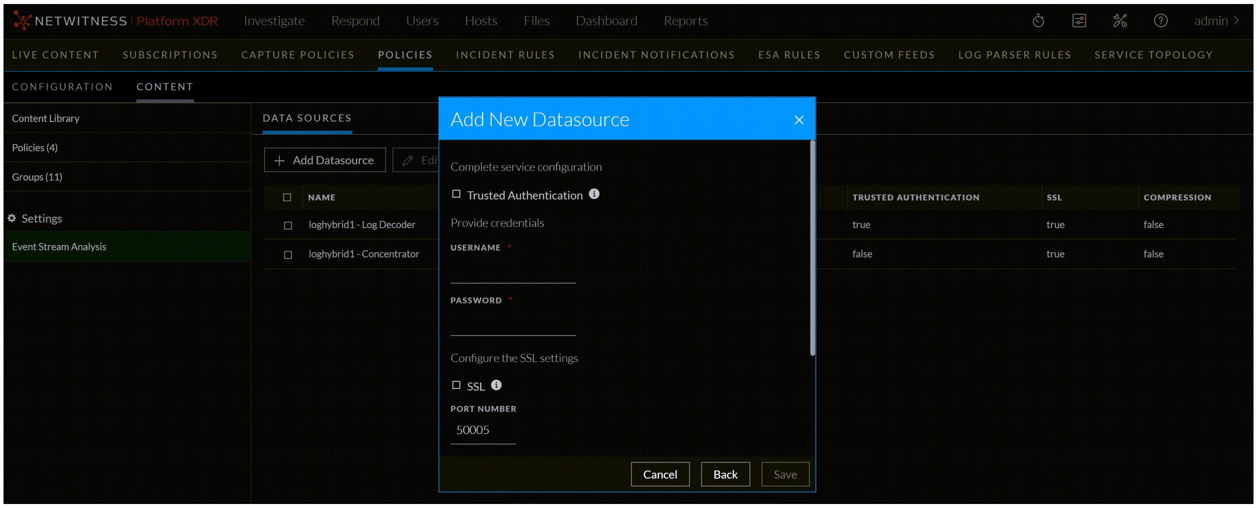


Add New Datasource

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



Add New Datasource

Complete service configuration

□ Trusted Authentication

Provide credentials

USERNAME *

PASSWORD *

Configure the SSL settings

□ SSL

PORT NUMBER

50005

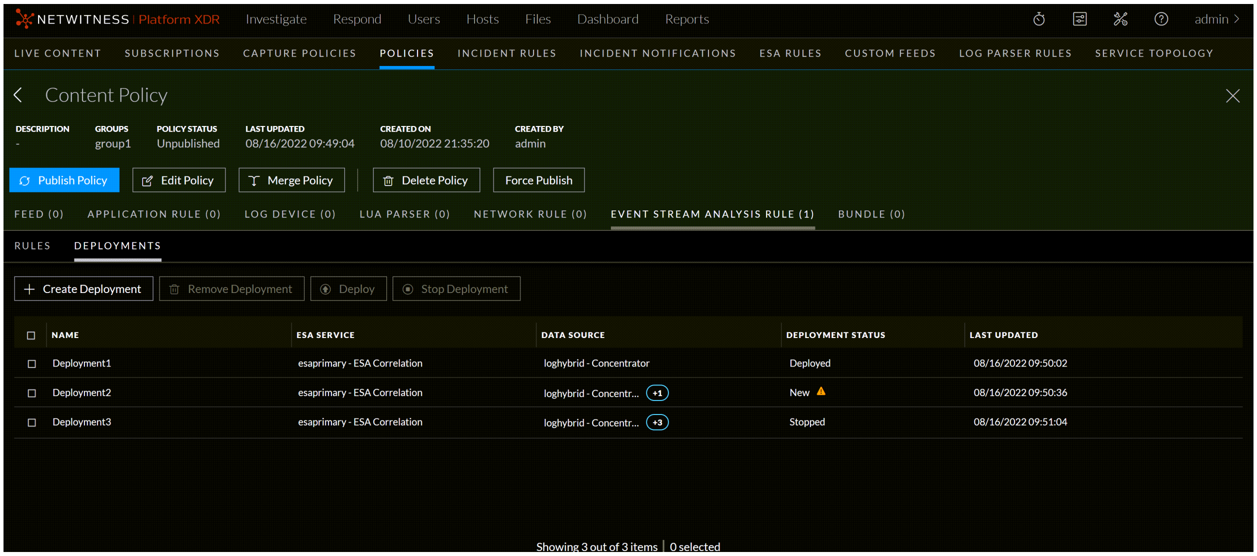
The table describes the information and options in the **Add New Datasource** dialog.

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:



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

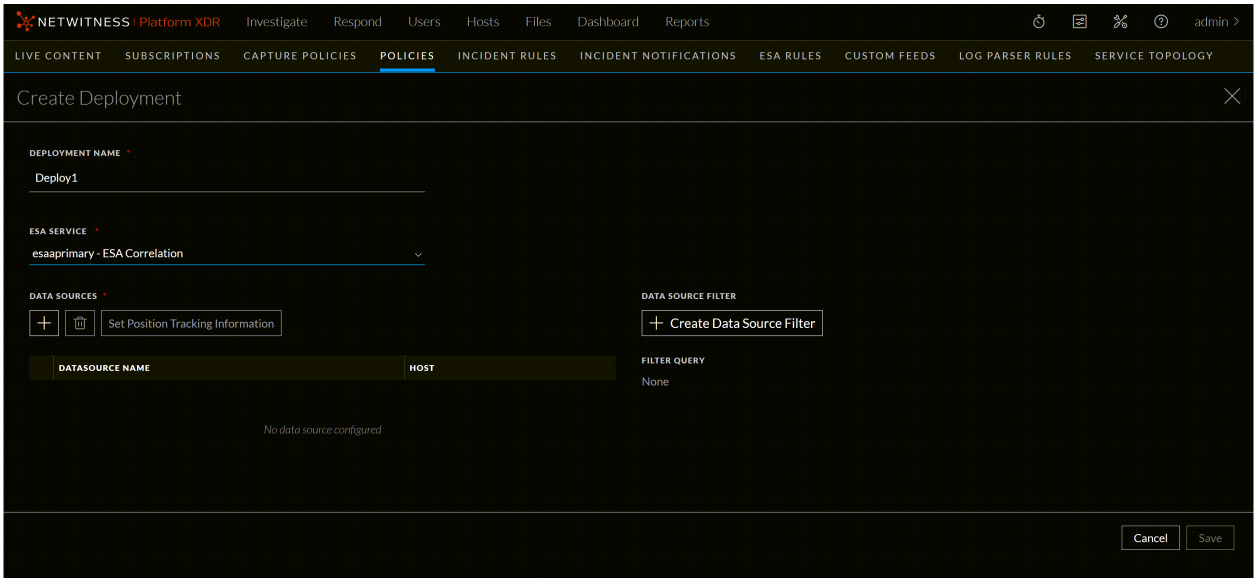
The following table describes the Deployments tab.

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 *

No data source configured

DATA SOURCE FILTER

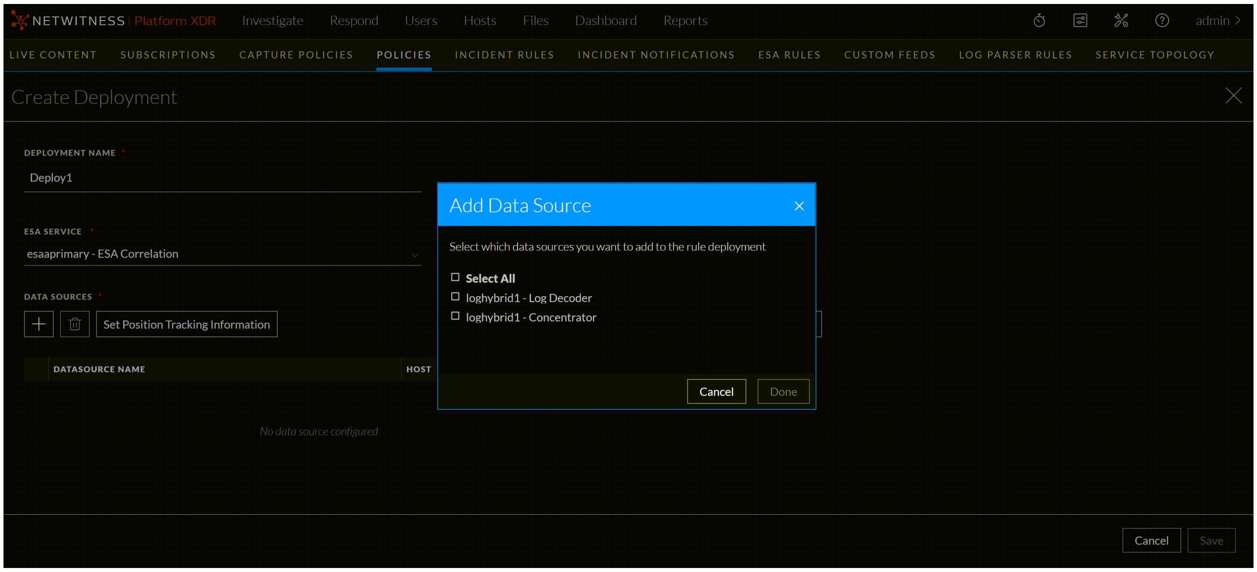
FILTER QUERY None

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 Appendix B: 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.



DEPLOYMENT NAME *: Deploy1

ESA SERVICE *: esaaprimary - ESA Correlation

No data source configured

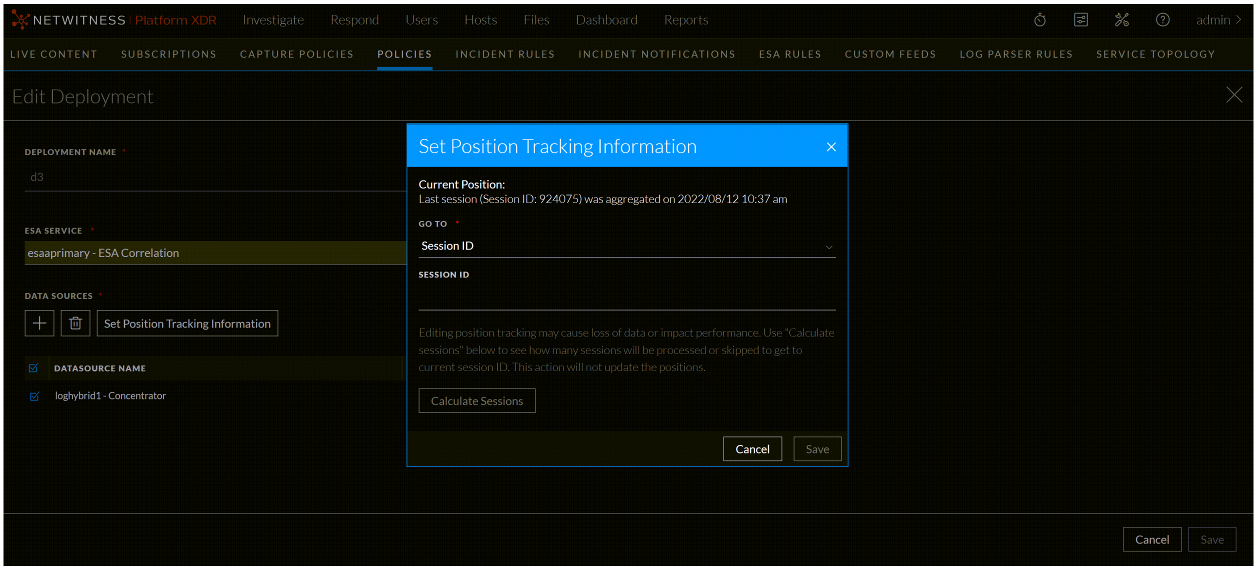
Select which data sources you want to add to the rule deployment

- ☐ **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.



DEPLOYMENT NAME *
d3

ESA SERVICE *
esaaprimary - ESA Correlation

DATA SOURCES *

☑	DATASOURCE NAME
☑	loghybrid1 - Concentrator

Current Position:
Last session (Session ID: 924075) was aggregated on 2022/08/12 10:37 am

GO TO *
Session ID

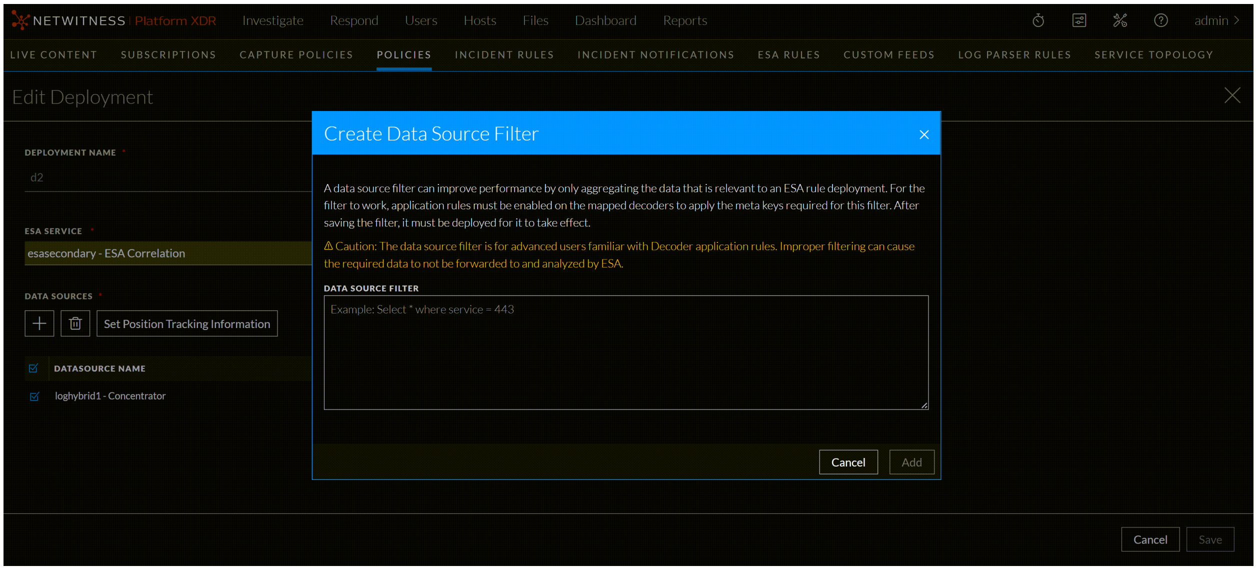
SESSION ID

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



DEPLOYMENT NAME * d2

ESA SERVICE * esasecondary - ESA Correlation

DATA SOURCES *

☑ 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.

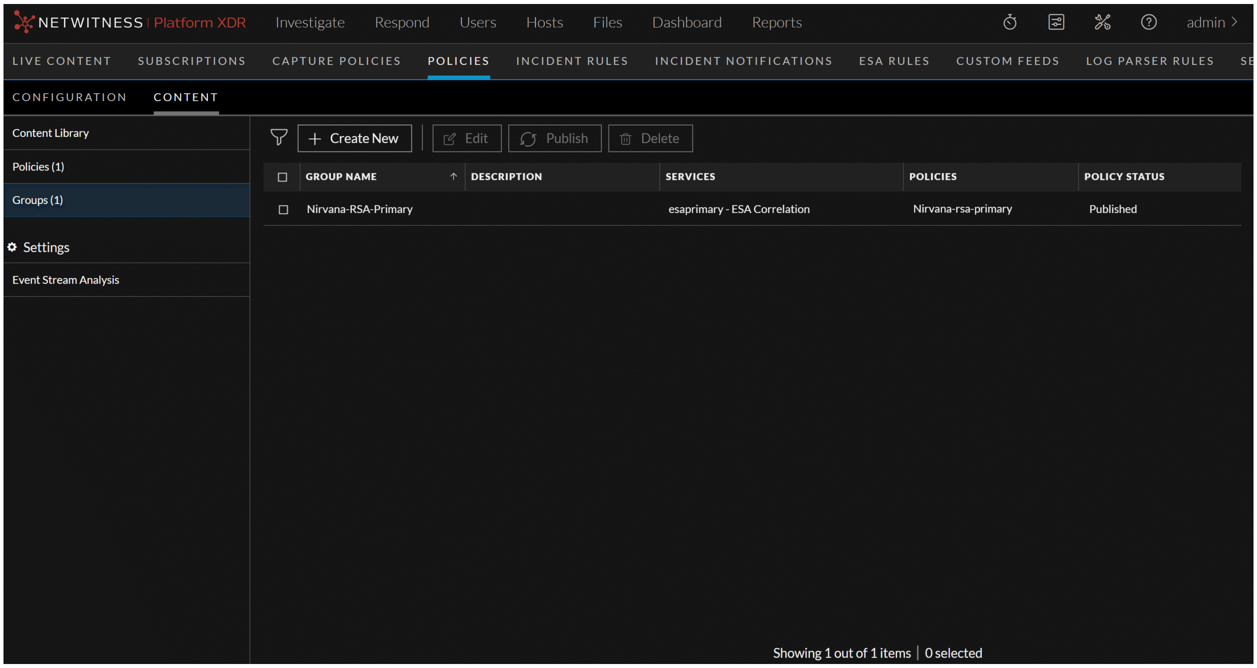
DATA SOURCE FILTER: Example: Select * where service = 443

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:



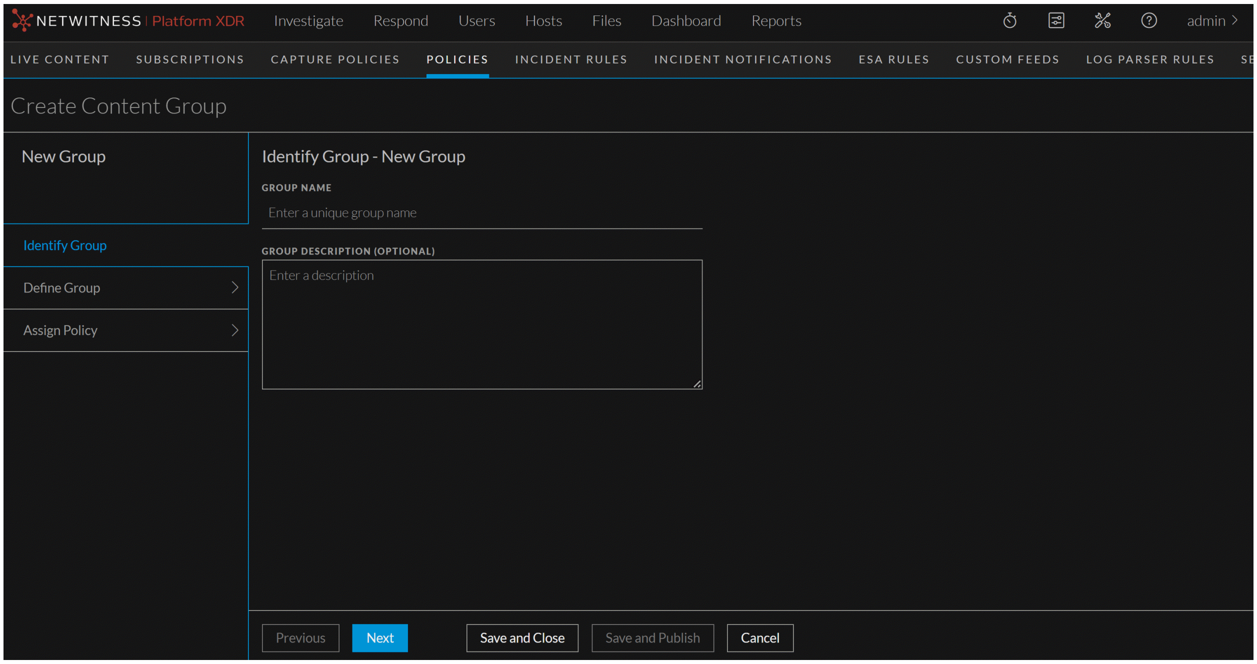
□	GROUP NAME	DESCRIPTION	SERVICES	POLICIES	POLICY STATUS
□	Nirvana-RSA-Primary		esaprimary - ESA Correlation	Nirvana-rsa-primary	Published

Showing 1 out of 1 items | 0 selected

The following table describes the Groups tab.

1	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.
2	Group List Pane • Group 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.
3	Groups Details Panel Displays the properties of the selected group.

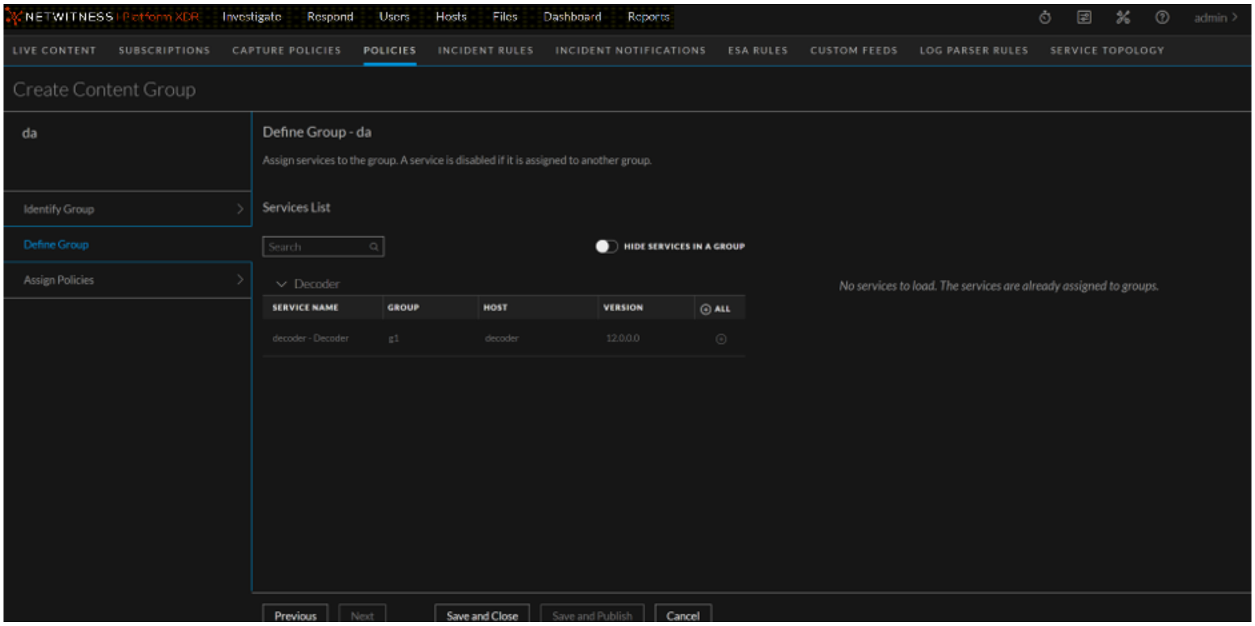
Below is an example of the Create group dialog:



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:



Define Group - da

Assign services to the group. A service is disabled if it is assigned to another group.

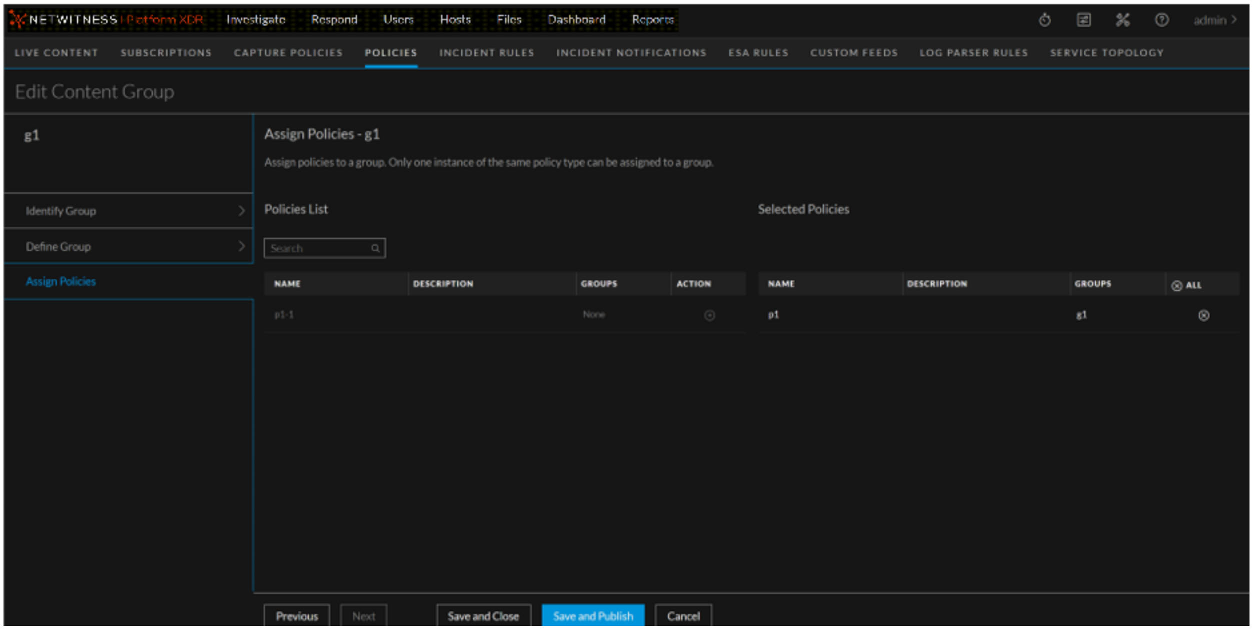
SERVICE NAME	GROUP	HOST	VERSION	ALL
decoder - Decoder	g1	decoder	12.0.0.0	⊕

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 ⊕ ALL 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:



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

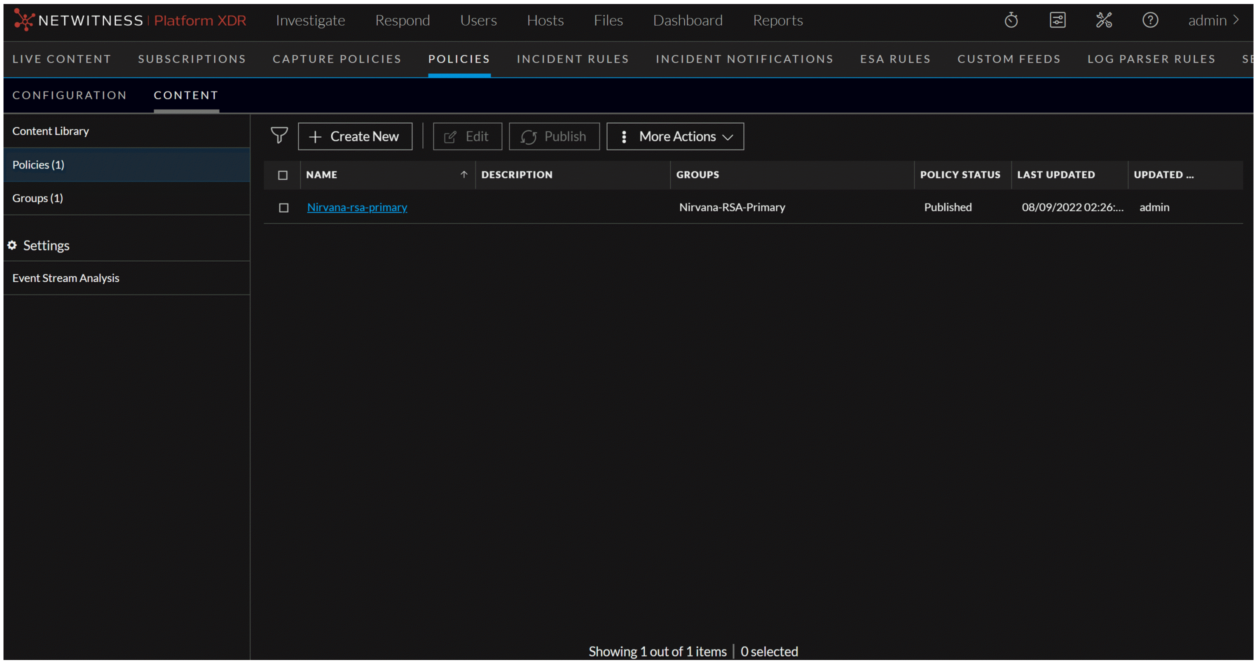
Policies List	Displays the list of policies associated with the group. The following describes policies list: • Name - Name of the policy. • Description - Description of the policy. • Groups - Groups associated with the policy. • Action - Click to add policies to the group.
Selected Policies	Displays 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

IMPORTANT: The customers should note that, while publishing the first policy to a service, all previous content except custom feeds, will be deleted. Ensure that all custom content are migrated to Content Library before publishing the first policy.

The **(CONFIGURE) > Policies** view contains two tabs: **Configuration** and **Content**.

Below is an example of the **Content > Policies** tab:



□	NAME	DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	UPDATED ...
□	Nirvana-rsa-primary		Nirvana-RSA-Primary	Published	08/09/2022 02:26:...	admin

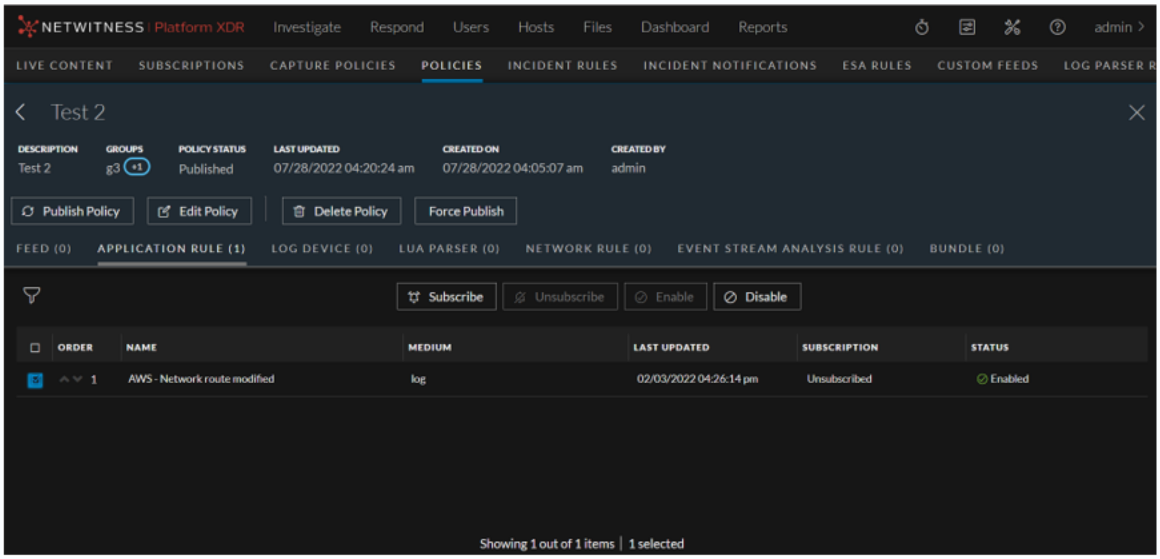
Showing 1 out of 1 items | 0 selected

1 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.
  - 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.

2	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.

3 Policy Details Panel:



Test 2

DESCRIPTION	GROUPS	POLICY STATUS	LAST UPDATED	CREATED ON	CREATED BY
Test 2	g3 +1	Published	07/28/2022 04:20:24 am	07/28/2022 04:05:07 am	admin

□	ORDER	NAME	MEDIUM	LAST UPDATED	SUBSCRIPTION	STATUS
☑	1	AWS - Network route modified	log	02/03/2022 04:26:14 pm	Unsubscribed	✓ Enabled

Showing 1 out of 1 items | 1 selected

Displays the Displays the properties of the selected policy.

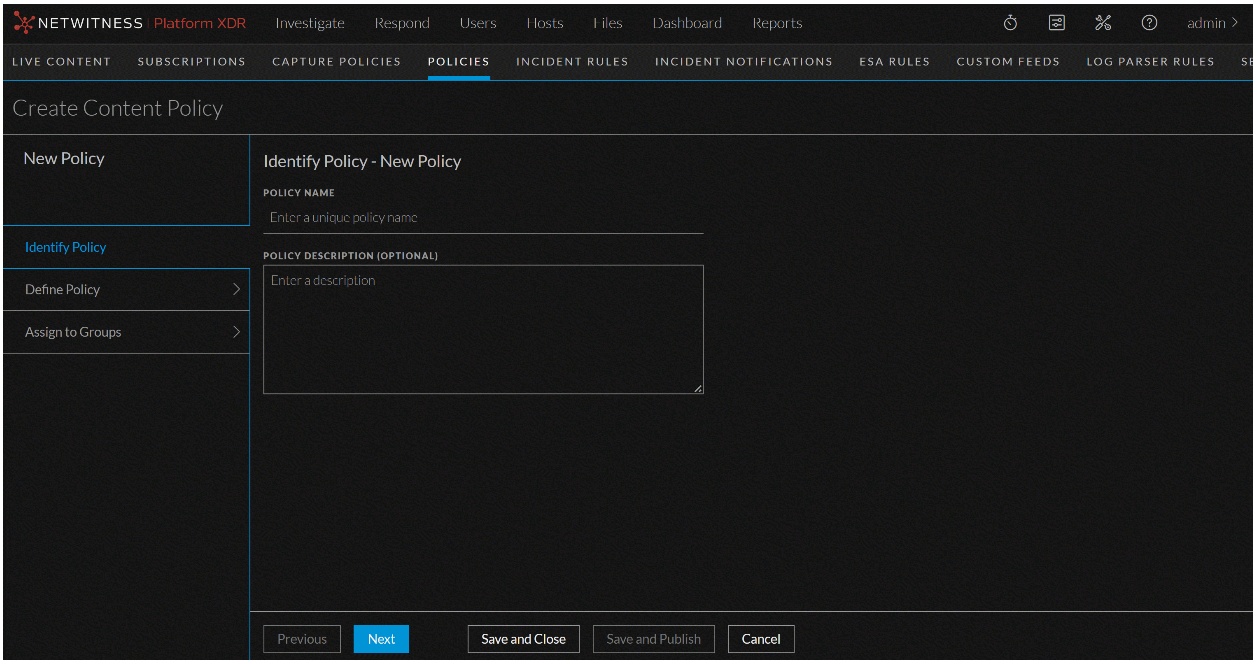
Toolbar:

- 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.
- Name - Name of the content.
- 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.
- 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.

Below is an example of the Create Content Policy dialog.



Create Content Policy

Identify Policy - New Policy

POLICY NAME

Enter a unique policy name

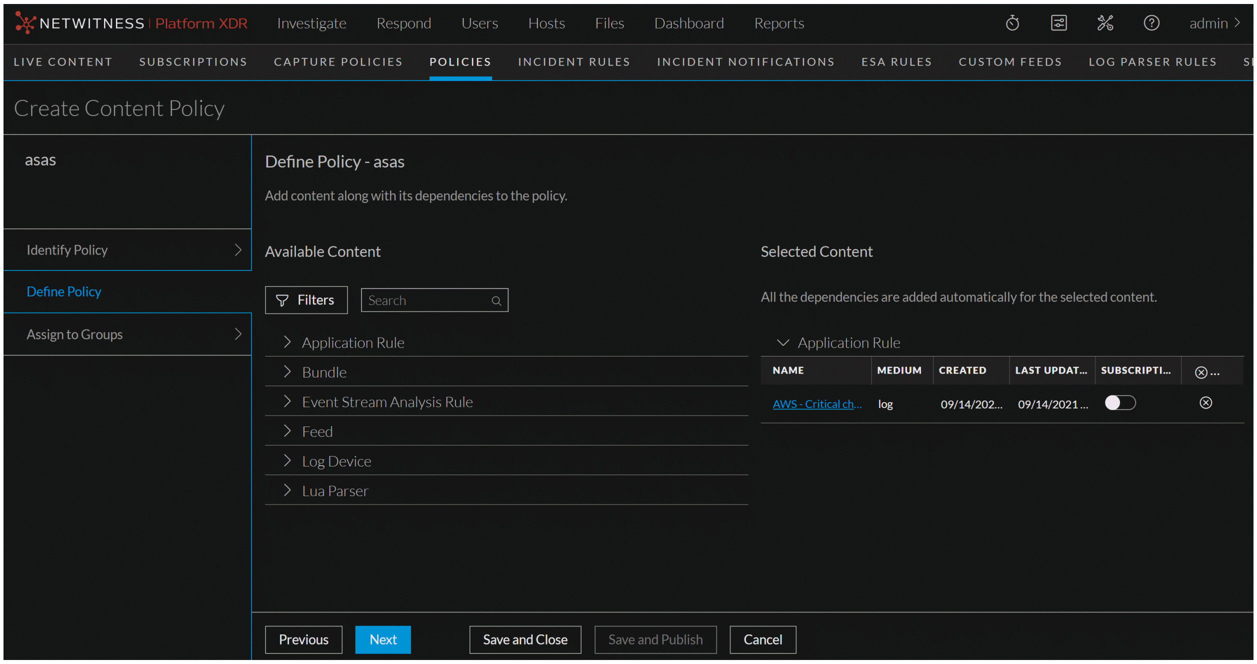
POLICY DESCRIPTION (OPTIONAL)

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:



Create Content Policy

Define Policy - asas

Add content along with its dependencies to the policy.

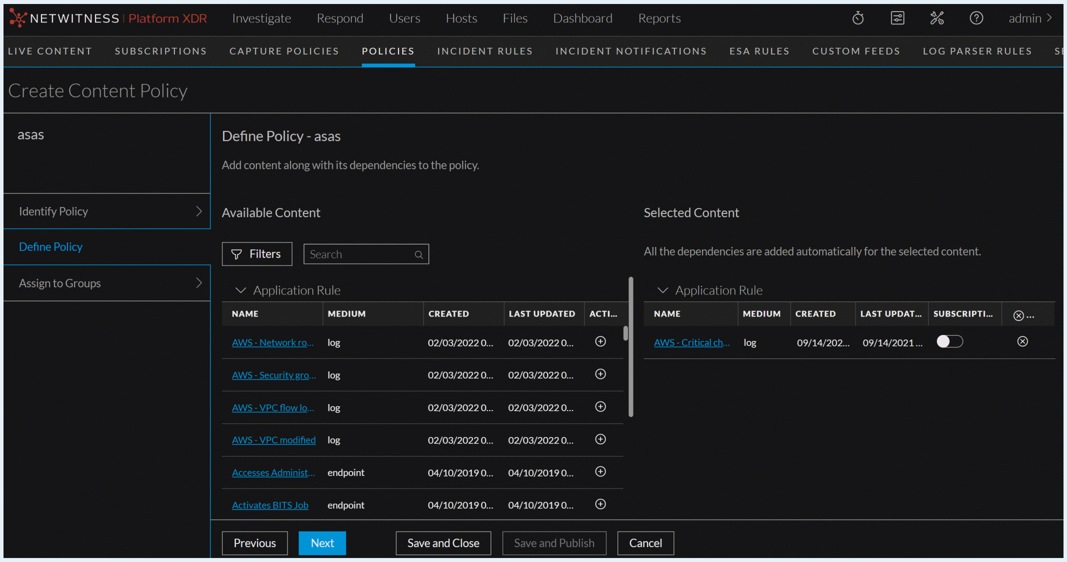
Available Content

Selected Content

All the dependencies are added automatically for the selected content.

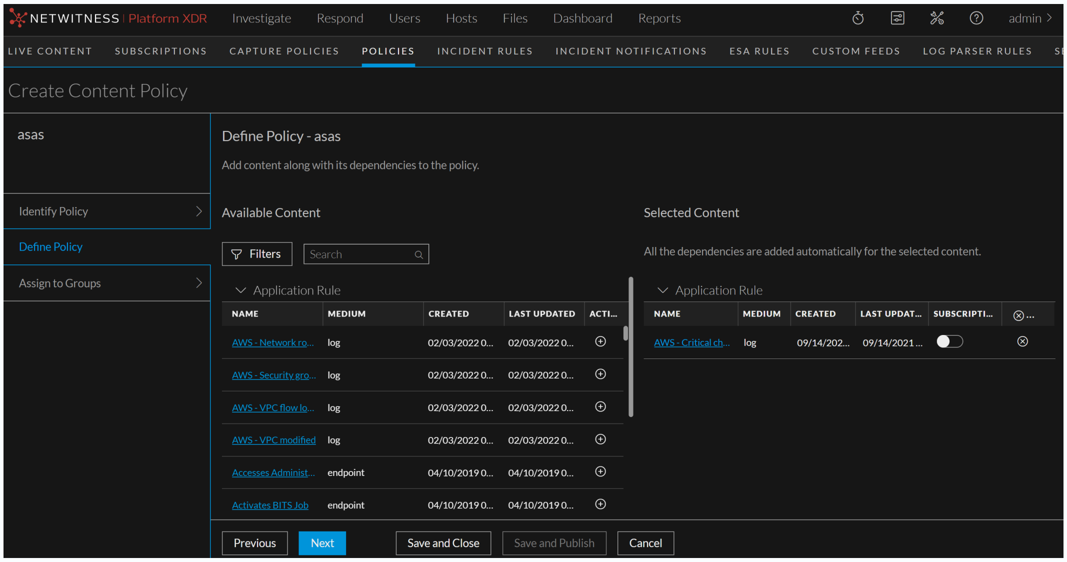
Application Rule

NAME	MEDIUM	CREATED	LAST UPDAT...	SUBSCRIPTI...
AWS - Critical ch...	log	09/14/202...	09/14/2021 ...	○

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Available Content</td><td>
<p>Displays the available content resources in your deployment. Click expand the resource type.</p>


<p>Define Policy - asas</p>
<p>Add content along with its dependencies to the policy.</p>
<p>Available Content</p>
<p>Application Rule</p>
<table>
<tr><th>NAME</th><th>MEDIUM</th><th>CREATED</th><th>LAST UPDATED</th><th>ACTI...</th></tr>
<tr><td>AWS - Network ro...</td><td>log</td><td>02/03/2022 0...</td><td>02/03/2022 0...</td><td>⊕</td></tr>
<tr><td>AWS - Security gro...</td><td>log</td><td>02/03/2022 0...</td><td>02/03/2022 0...</td><td>⊕</td></tr>
<tr><td>AWS - VPC flow lo...</td><td>log</td><td>02/03/2022 0...</td><td>02/03/2022 0...</td><td>⊕</td></tr>
<tr><td>AWS - VPC modified</td><td>log</td><td>02/03/2022 0...</td><td>02/03/2022 0...</td><td>⊕</td></tr>
<tr><td>Accesses Administ...</td><td>endpoint</td><td>04/10/2019 0...</td><td>04/10/2019 0...</td><td>⊕</td></tr>
<tr><td>Activates BITS Job</td><td>endpoint</td><td>04/10/2019 0...</td><td>04/10/2019 0...</td><td>⊕</td></tr>
</table>
<p>Selected Content</p>
<p>All the dependencies are added automatically for the selected content.</p>
<p>Application Rule</p>
<table>
<tr><th>NAME</th><th>MEDIUM</th><th>CREATED</th><th>LAST UPDAT...</th><th>SUBSCRIPTI...</th><th>⊗ ...</th></tr>
<tr><td>AWS - Critical ch...</td><td>log</td><td>09/14/202...</td><td>09/14/2021 ...</td><td>○</td><td>⊗</td></tr>
</table>
<p>The following describes resource type:</p>
<ul>
<li>Name - Name of the resource.</li>
<li>Medium - Meta data source medium. Available values for medium are as follows:
<ul>
<li><b>Endpoint</b>: applied to content that uses meta derived from endpoint agent and endpoint server data</li>
<li><b>Log</b>: applied to content that uses meta derived from log data</li>
<li><b>Packet</b>: applied to content that uses meta derived from network packets</li>
<li><b>Log and packet</b>: applied to content that correlates meta derived across log and packet data</li>
</ul></li>
<li>Created - Displays the time when the resource is created</li>
<li>Last Updated - Displays the time when the resource is updated last.</li>
<li>Action- Click + to add the resource and its dependencies to your deployment.</li>
</ul>
</td></tr>
</table>

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.



Create Content Policy

asas

Define Policy - asas

Add content along with its dependencies to the policy.

Available Content

Application Rule

NAME	MEDIUM	CREATED	LAST UPDATED	ACTI...
AWS - Network ro...	log	02/03/2022 0...	02/03/2022 0...	⊕
AWS - Security gro...	log	02/03/2022 0...	02/03/2022 0...	⊕
AWS - VPC flow lo...	log	02/03/2022 0...	02/03/2022 0...	⊕
AWS - VPC modified	log	02/03/2022 0...	02/03/2022 0...	⊕
Accesses Administ...	endpoint	04/10/2019 0...	04/10/2019 0...	⊕
Activates BITS Job	endpoint	04/10/2019 0...	04/10/2019 0...	⊕

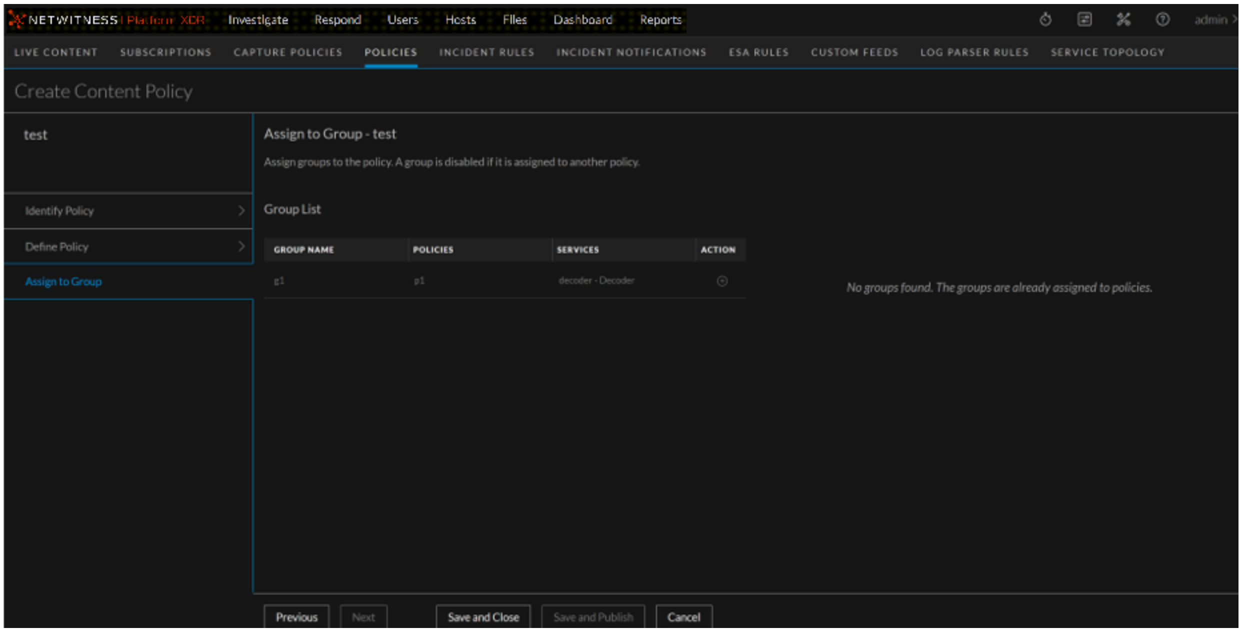
Selected Content

All the dependencies are added automatically for the selected content.

Application Rule

NAME	MEDIUM	CREATED	LAST UPDAT...	SUBSCRIPTI...	⊗ ...
AWS - Critical ch...	log	09/14/202...	09/14/2021 ...	○	⊗

Assign to Group:



Create Content Policy

test

Assign to Group - test

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

Group List

GROUP NAME	POLICIES	SERVICES	ACTION
g1	p1	decoder - Decoder	⊕

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
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.

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"

Appendix B: 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 XDR 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.

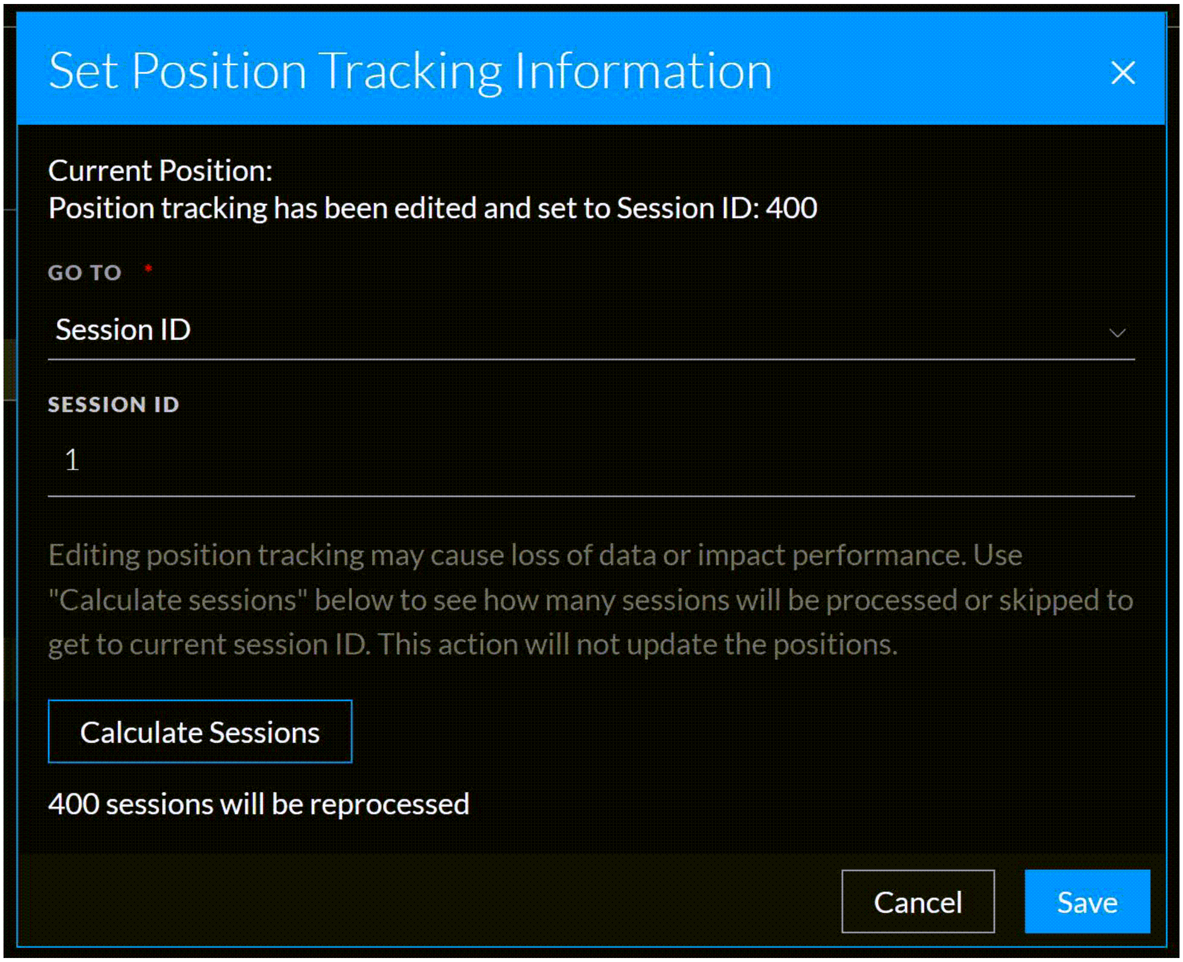
4. Click **Calculate Sessions**.

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

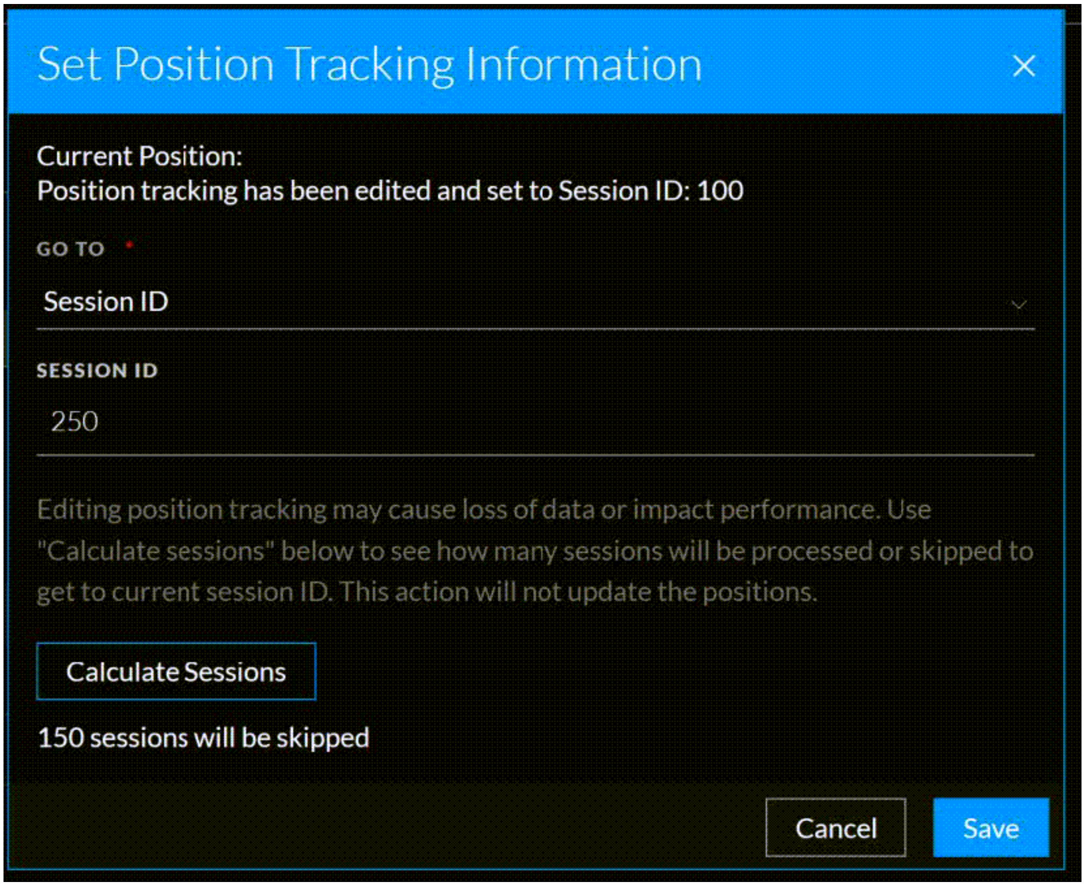
1

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.



Set Position Tracking Information

Current Position:
Position tracking has been edited and set to Session ID: 100

GO TO *

Session ID

SESSION ID

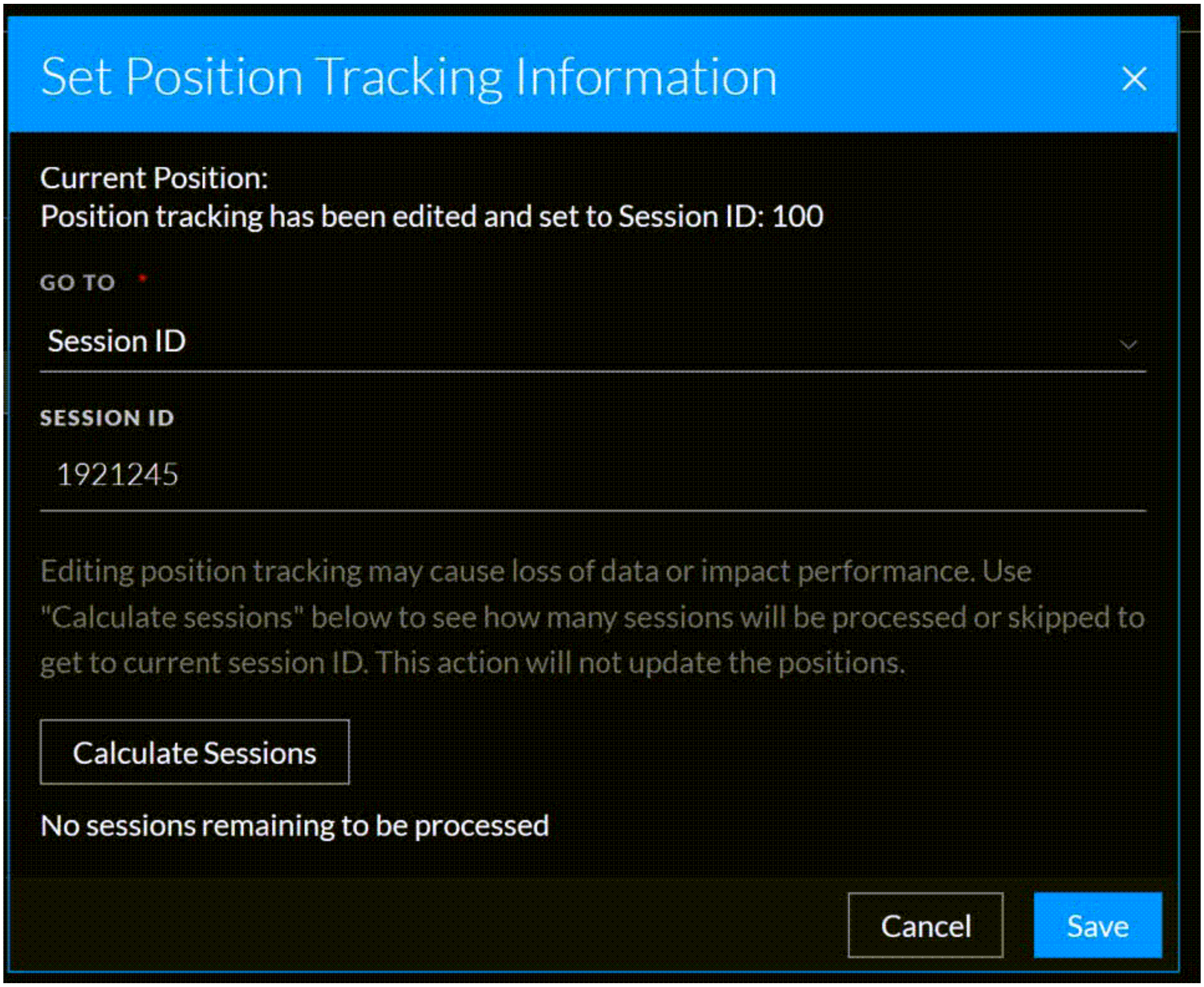
250

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.

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.