NetWitness® Platform XDR

AWS Security Hub Event Source Log Configuration Guide

NETWITNESS
Platform XDR

AWS Security Hub

Event Source Product Information:

Vendor: AWS Security Hub

Event Source: awssecurityhub

Versions: API v1.0

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.5 and later

Event Source Log Parser: awssecurityhub

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

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

Note on Encryption Technologies

Distribution

November, 2022

Contents

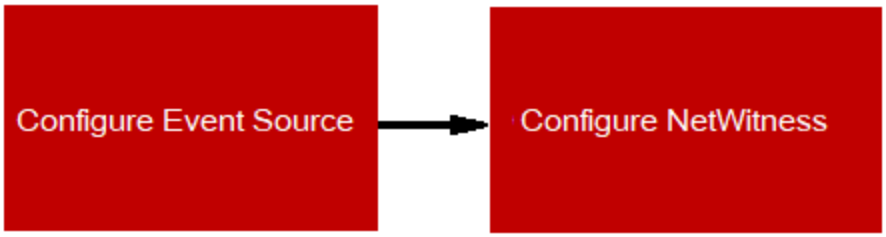
Introduction to AWS Security Hub

AWS Security Hub collects security findings from AWS accounts, services, and integrated third-party products and helps you analyze security trends in your environment to identify the highest priority security issues.

NetWitness Platform XDR captures these findings from Security Hub via the `aws_securityhub` Plugin.

For more information about integrated services for the Security Hub API, see https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-partner-providers.html.

To configure the Amazon Security Hub with NetWitness Platform XDR, complete the following tasks.



- Configure AWS Security Hub
- Set up AWS Security Hub in NetWitness Platform XDR

Configure AWS Security Hub

To set up the AWS Security Hub, see the following Amazon procedures:

- To Enable Security Hub and to attach the required IAM policy:

  Setting up AWS Security Hub.

- Reference information for AWS Security Hub supported regions:
  AWS Security Hub Supported Regions.

Set up AWS Security Hub in NetWitness Platform XDR

In NetWitness Platform XDR, perform the following tasks:

I. Deploy AWS Security Hub Files from Live

II. Configure the AWS Security Hub Event Source in NetWitness Platform XDR.

Deploy AWS Security Hub Files from Live

AWS Security Hub plugin requires resources available in Live in order to collect logs.

To deploy the required content from Live:

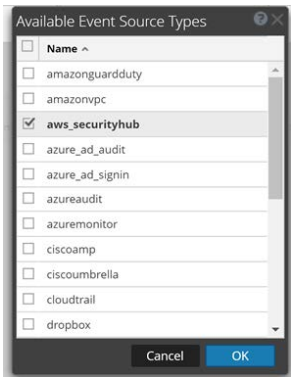
1. In the NetWitness Platform XDR menu, select (Configure).
   The **Live Content** tab is displayed.
2. Browse Live Content for the **awssecurityhub** parser, using **Log Device** as the **Resource Type**.
3. Select the **awssecurityhub** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.
4. You also need to deploy the AWS Security Hub package. Browse Live for AWS Security Hub content, typing "**aws_securityhub**" into the Keywords text box, then click **Search**.
5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors, using the Deployment Wizard.

For more details, see the Add or Update Supported Event Source Log Parsers.

Configure the AWS Security Hub Event Source in NetWitness Platform XDR

To configure the AWS Security Hub Event Source:

1. In the NetWitness Platform XDR menu, select (Admin) > **Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.
   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.
   The Available Event Source Types dialog is displayed.

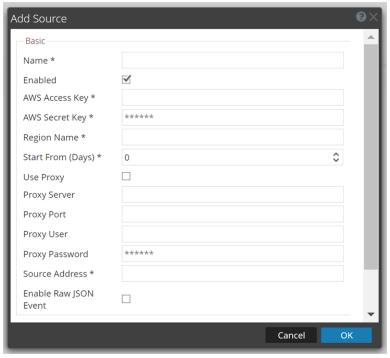


5. Select **aws_securityhub** from the list, and click **OK**.

   The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.



7. Define parameter values, as described in AWS Security Hub Collection Configuration Parameters.
8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform XDR displays an error message.

9. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

10. Repeat steps 4–9 to add another AWS Security Hub plugin instance.

AWS Security Hub Collection Configuration Parameters

The following table describes the configuration parameters for the AWS Security Hub integration with NetWitness Platform XDR. Fields marked with an asterisk (*) are required.

Note: Items that are followed by an asterisk (*) required.

Basic Parameters

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the box to enable the event source configuration to start collection. The box is selected by default.
AWS Access Key*	The access key needed to access the Security Hub.
AWS Secret Key *	The secret key needed to access the Security Hub.
AWS Region Name *	Name of the region where Security Hub is enabled.
Start From (Days) *	Choose the date from which to start collecting. This parameter defaults to the current date: collects information from the last 15 minutes before it is configured.
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address *	IP address that is to be provided to the AWS Security Hub plugin instance: logs from this event source will be collected with this device IP. **Note:** This is an arbitrary IP address chosen by the user. This value has no bearing on the collection of logs: its value is captured by the device.ip meta key, and can help you to query or group events collected by a particular instance of the plugin.

Name	Description
Enable Raw JSON Event	Enable if you want the plugin to collect logs in JSON format.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Note: Please avoid using special characters in the **Proxy User** and **Proxy Password** sections.

Advanced Parameters

Parameter	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify **180**, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.

Parameter	Description
SSL Enabled	The check box is selected by default. Uncheck this box to disable SSL certificate verification.

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.