

NetWitness[®] Platform

Amazon GuardDuty Event Source Log Configuration Guide

Amazon GuardDuty

Last Modified: Wednesday, July 10, 2024

Event Source Product Information:

Vendor: [Amazon](#)

Event Source: GuardDuty

Versions: all

RSA Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: cef

Note: The CEF parser parses this event source as `device.type=amazonguardduty`.

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

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

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

Miscellaneous

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

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

February, 2024

Contents

Configure the Amazon GuardDuty Event Source	6
Enable the GuardDuty Service	7
Set Up the Amazon GuardDuty Event Source in NetWitness Platform	10
Deploy Amazon GuardDuty Files from Live	10
Configure SELinux mode to Enforcing mode in the Log Decoder	10
Configure the Event Source	11
Amazon GuardDuty Collection Configuration Parameters	13
Getting Help with NetWitness Platform	14
Self-Help Resources	14
Contact NetWitness Support	14
Feedback on Product Documentation	15

To configure Amazon GuardDuty, you must complete these tasks:

- I. Configure the Amazon GuardDuty event source
- II. Set Up Amazon GuardDuty Event Source in RSA NetWitness

Configure the Amazon GuardDuty Event Source

Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. The service analyzes Amazon CloudTrail and AWS VPC Flow Log data to look for issues such as inbound port scans, possible backdoor access to your systems, unauthorized use of your account, and many other potential problems.

GuardDuty can be used to monitor a group of AWS accounts and have their findings routed to another AWS account—the master account—that is owned by a security team. Amazon GuardDuty starts to generate customized threat intelligence for you.

GuardDuty is a regional service. This means that when you enable GuardDuty in an AWS Region, all findings are generated and delivered in that region. Using the NetWitness Platform plugin framework, we can establish a connection with Amazon GuardDuty to provide visibility into the AWS Network.

Note: The GuardDuty plugin is meant for collecting the security alerts provided by AWS. The AWS GuardDuty alerts are sent in JSON format, as detailed in the AWS documentation here: <https://docs.aws.amazon.com/guardduty/latest/ug/get-findings.html>

Enable the GuardDuty Service

To use GuardDuty, you must first enable it.

To enable GuardDuty:

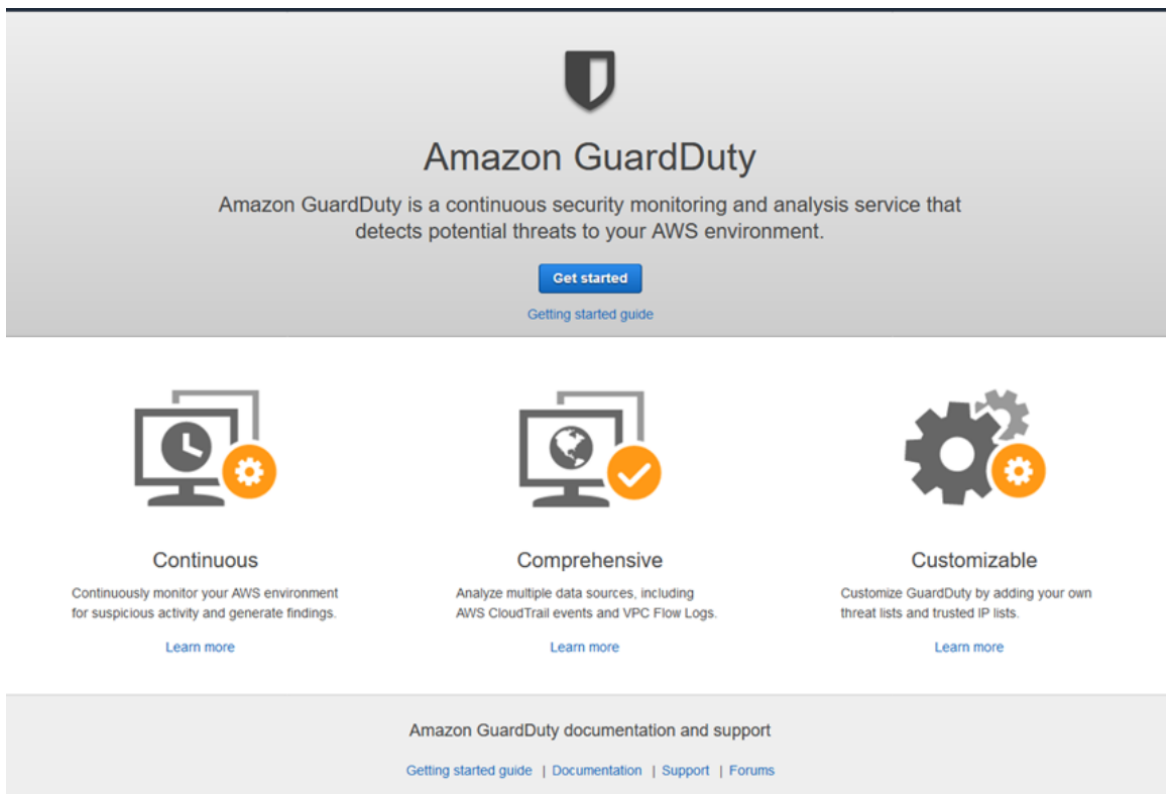
1. The IAM identity (user, role, group) that you use to enable GuardDuty must have the required permissions. To grant the permissions required to enable GuardDuty, attach the following policy to an IAM user, group, or role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["guardduty:*"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["iam:CreateServiceLinkedRole"],
      "Resource": "arn:aws:iam::123456789012:role/aws-service-
role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
      "Condition": {
        "StringLike": {"iam:AWSServiceName": "guardduty.amazonaws.com"}
      }
    },
    {
      "Effect": "Allow",
      "Action": ["iam:PutRolePolicy","iam>DeleteRolePolicy"],
      "Resource": "arn:aws:iam::1234567890123:role/aws-service-
role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
    }
  ]
}
```

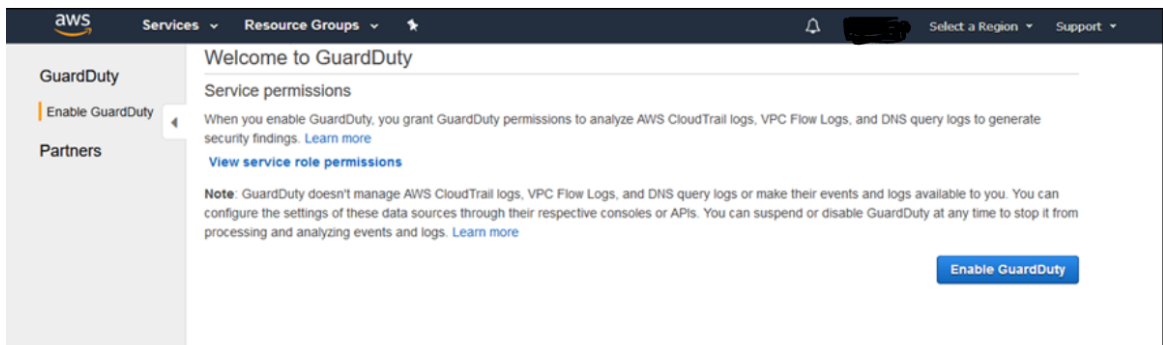
Note: Replace the sample account ID in the example above with your actual AWS account ID.

2. Use the credentials of the IAM identity from step 1 to sign in to the GuardDuty console.

- a. When you open the GuardDuty console for the first time, choose **Get Started**.



- b. Then choose **Enable GuardDuty**.



3. In the GuardDuty console, note the value for the **Detector ID** parameter, which you will need later.

The screenshot shows the Amazon GuardDuty console interface. On the left is a navigation sidebar with the following items: GuardDuty, Findings, Current, Archived, Settings, General (highlighted with an orange bar), Lists, Accounts, Usage, Details, and Partners. The main content area is titled 'Settings' and contains several sections:

- About GuardDuty**: Shows the Detector ID as a redacted black box with a 'Learn more' link.
- Permissions**: States that GuardDuty uses a service role and provides a 'View service role permissions' button and a 'Learn more' link.
- CloudWatch events**: States that GuardDuty supports CloudWatch events and provides a 'Learn more' link.
- Sample findings**: Explains that sample findings help visualize and analyze finding types. It includes a 'Generate sample findings' button and a 'Learn more' link.
- Suspend GuardDuty**: Contains two radio button options:
 - Suspend GuardDuty**: When you suspend GuardDuty, it stops monitoring your AWS environment and doesn't generate new findings. Your existing findings remain intact and aren't affected. You can choose to re-enable GuardDuty later. You will not be charged for using GuardDuty when the service is suspended. [Learn more](#)
 - Disable GuardDuty**: When you disable GuardDuty, you not only stop GuardDuty from monitoring your AWS environment and generating new findings, you also lose your existing findings and your GuardDuty configuration. You can't recover that data later. To save a copy of existing findings, export them before you disable GuardDuty. [Learn more](#)

At the bottom right of the settings area are two buttons: 'Cancel' and 'Save settings'.

Set Up the Amazon GuardDuty Event Source in NetWitness Platform

In NetWitness Platform , perform the following tasks:

- I. Deploy the **amazonguardduty** package and CEF parser from Live
- II. Configure SELinux mode to Enforcing mode in the Log Decoder
- III. Configure the event source.

Deploy Amazon GuardDuty Files from Live

Amazon GuardDuty uses the cef parser.

To deploy the cef parser from Live:

1. In the RSA NetWitness Platform menu, select **CONFIGURE**.
The **Live Content** tab is displayed.
2. Browse Live Content for the **Common Event Format (cef)** parser, using **Log Device** as the **Resource Type**.
3. Select the **cef** 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 Amazon GuardDuty package. Browse Live for Amazon GuardDuty content, typing "Amazon GuardDuty" into the Keywords text box, then click **Search**.
5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

Note: On a hybrid installation, you need to deploy the package on both the VLC and the LC.

6. Restart the **nwlogcollector** service.

For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic, or the *Live Services Management Guide*.

Configure SELinux mode to Enforcing mode in the Log Decoder

Run the script `update_selinux_policy.sh`, which is provided in the package, as a root user, after you deploy the package to the Log Decoder.

To enable the Enforcing mode for the SELinux, run the script on the Log Decoder:

```
sh
/etc/netwitness/ng/logcollection/content/collection/cmdscript/amazonpc/update_selinux_policy.sh
```

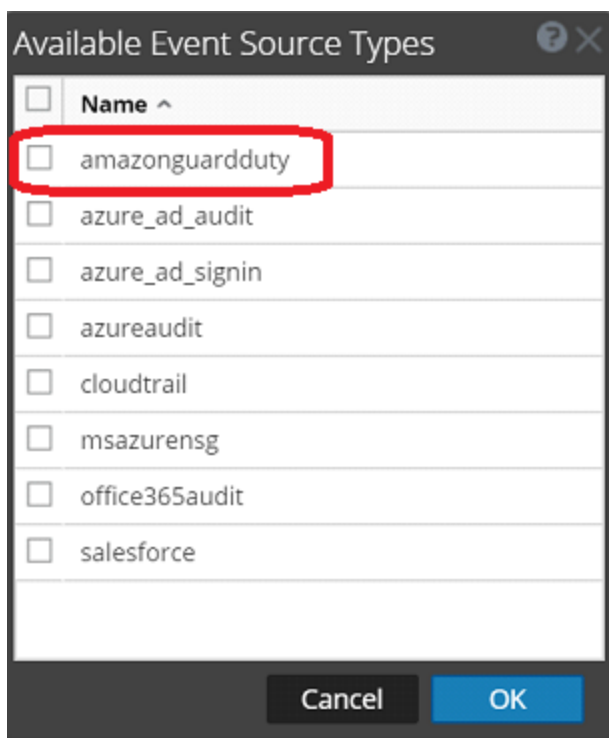
Note: You only need to run this script once, during the initial configuration. Also, you do not need to run the script in NetWitness version 11.2 and later.

Configure the Event Source

To configure the Amazon GuardDuty Event Source:

1. In the RSA NetWitness Platform 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 **amazonguardduty** 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 [Amazon GuardDuty 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 RSA NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.
The new event source is displayed in the Sources panel.

Amazon GuardDuty Collection Configuration

Parameters

The following table describes the configuration parameters for the Amazon GuardDuty integration with NetWitness Platform . Fields marked with an asterisk (*) are required.

Note: When run from behind an SSL proxy, if certificate verification needs to be disabled, uncheck the **SSL Enable** checkbox in the Advanced section.

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 Region Name *	Name of the region where GuardDuty is enabled.
AWS Access Key Id *	Access key for the AWS account.
AWS Secret Access Key *	Secret access key for the AWS account.
GuardDuty detector ID	Detector ID for the enabled GuardDuty account. This ID was shown in step 3 of Enable the GuardDuty Service section.
In Hours	Specifies whether Start From represents number of hours or days. <ul style="list-style-type: none"> • Selected (default): if selected, Start From represents number of hours. • Cleared: if not checked, indicates Start From represents number of days.
Start From *	Specifies the number of hours or days (see the In Hours parameter above) prior to the current time, from which log collection should start.
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	Input the IP address that needs to appear as the device.ip .

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

Getting Help with NetWitness Platform

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 the documentation for Logstash JDBC input plugin here: <https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- 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 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 feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.