NetWitness® Platform

Amazon Detective Event Source Log Configuration Guide

NETWITNESS
Platform

Amazon Detective

Last Modified: Monday, December 2, 2024

Event Source Product Information:

Vendor: AWS

Event Source: Amazon Detective

Versions: API v1.0

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 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 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/.

November 2024

Contents

Amazon Detective is an Amazon Web Services (AWS) threat hunting platform that offers a deep, cloud-native view of AWS resource data and history, optionally in the context of Amazon GuardDuty findings. Amazon Detective augments RSA NetWitness Platform by providing details about the size and scope of AWS specific security threats, and to help reconstruct security events that affect cloud assets and infrastructure.

This integration allows an analyst to pivot from RSA NetWitness investigation directly into Amazon Detective to view the related AWS resource as needed. Additionally, customers that have [[[Undefined variable SAVariables.ProductLogs]]] Logs, and are consuming AWS GuardDuty events, can pivot directly to related GuardDuty findings in Amazon Detective.

Note: AWS Detective Integration with [[[Undefined variable SAVariables.ProductSuiteName]]] is done based on events from the Amazon GuardDuty plugin. If you are adding support for other AWS services in AWS Detective, and need an integration with RSA Netwitness, please contact RSA customer support.

To integrate Amazon Detective with NetWitness, complete the following tasks:

I. Configure the AWS Detective Event Source

II. Integrate AWS Detective Resource URL in NetWitness Platform

III. Pivot to AWS Detective using RSA Netwitness Context Menu Actions

Configure the AWS Detective Event Source

You need an AWS account that has active AWS Detective service. Make sure that you are logged into the AWS account before you can begin pivoting from RSA Netwitness. Refer to https://aws.amazon.com/detective/ for more details on AWS Detective and its configuration.

Integrate AWS Detective Resource URL in NetWitness Platform

In [[[Undefined variable SAVariables.ProductSuiteName]]], perform the following tasks:

- Configure AWS GuardDuty Plugin
- Configure RSA Netwitness Context Menu Actions

Configure AWS GuardDuty Plugin

The configuration steps for configuring the AWS GuardDuty plugin in the NetWitness Platform are provided in the configuration guide on RSA Link: Amazon GuardDuty Event Source Configuration Guide. Please see that guide to configure the AWS GuardDuty plugin.

Configure RSA Netwitness Context Menu Actions

The following sections describe how to create context actions in [[[Undefined variable SAVariables.ProductSuiteName]]] and then perform an external lookup using meta keys.

Meta Keys

The following table lists the mappings between AWS Detective Concepts and the corresponding [[[Undefined variable SAVariables.ProductSuiteName]]] meta keys.

AWS Detective Concept (Namespace)	AWS Detective Type	NetWitnessMeta Key
GuardDuty	findings	operation.id
IpAddress	entities	ip.src,ip.dst,alias.ip
AwsAccount	entities	reference.id1
AwsRole	entities	user.id
AwsUser	entities	user.id
UserAgent	entities	user.agent
Ec2Instance	entities	agent.id

If the keys listed above are not indexed, you must index them in your [[[Undefined variable SAVariables.ProductSuiteName]]] Concentrator. Indexing is required for your Context Menu Actions to work. For details on how to index custom meta keys, see the Index Customization topic in the Core Database Tuning Guide.

Create AWS Detective Pivot URLs

We need to create Context Menu Actions for the meta keys listed above. The first step is to create AWS Detective Pivot URLs. After that, we need to input the pivot URL as a "Definition" in Context Menu Action configuration in [[[Undefined variable SAVariables.ProductName]]].

To create pivot URLs, use the information in the table above, and details provided in the Amazon document at https://docs.aws.amazon.com/detective/latest/userguide/profile-navigate-url.html.

Configure Content Menu Action in NetWitness

To pivot on the **instanceID** in AWS Detective, the pivoting URL is specified with a **{0}** suffix when you add it in the Context Menu Action Configuration dialog box. When you click and pivot on the indexed meta, **{0}** is replaced with the value for the specified Meta Key in the Context Menu Configuration.

For example, the Detective Pivoting URL shown in the example below (Example Context Menu Action Configuration Dialog Box) is converted as **https://console.aws.amazon.com/detective/home?region=us-east- 1#entities/AwsUser/*xyzpqr*** where ***xyzpqr*** is the value for the **user.id** meta.

Similarly, you need to define Pivot URLs for the other metas and create Context Menu Actions for each in [[[Undefined variable SAVariables.ProductSuiteName]]].

Both **AwsUser principal Id** and **AwsRole principal Id** are mapped to the same NetWitness meta, **user.id**. However, the AWS Detective pivot URL is different for these metas. Determine the correct context menu based on the value of the **user.role** meta.

Note: [[[Undefined variable SAVariables.ProductName]]] does not support parameters to be added to the AWS Detective pivoting URL. However, you can apply this property when you pivot to an AWS Detective page using the Scope time option. Refer to User ID Landing page in AWS Detective after pivoting from RSA Netwitness Events pagefor more details. Also, create separate Context Menu Actions for different AWS regions if you have GuardDuty logs from more than one AWS region.

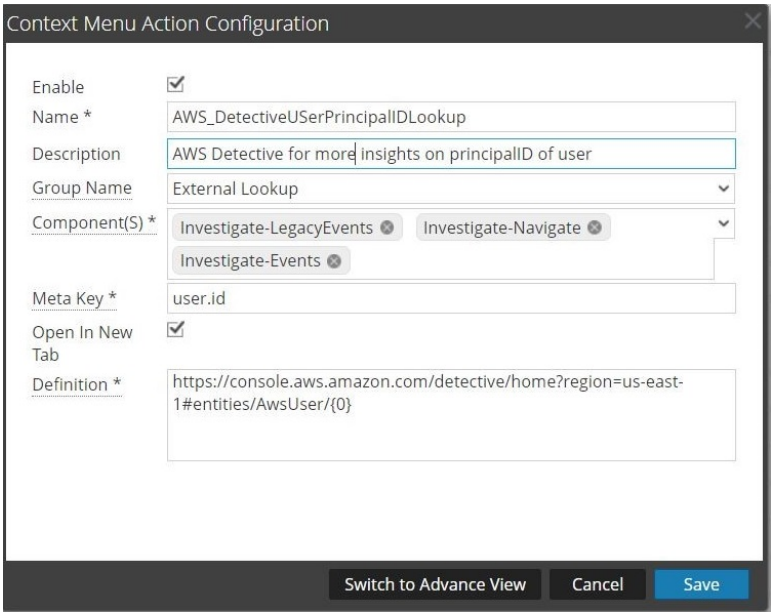
Example of adding a Context Menu Action

This example adds a Context Menu Action based on the **AwsUser principal ID** and **us-east-1** AWS region.

1. Log onto the [[[Undefined variable SAVariables.ProductSuiteName]]] UI.
2. Go to **ADMIN > System > Context Menu Actions**.

   The Context Menu Actions screen appears.

3. Click  to create a new context menu action.
4. Fill in details as shown in the following image.



Example Context Menu Action Configuration Dialog Box

5. Click **Save** to complete the process.

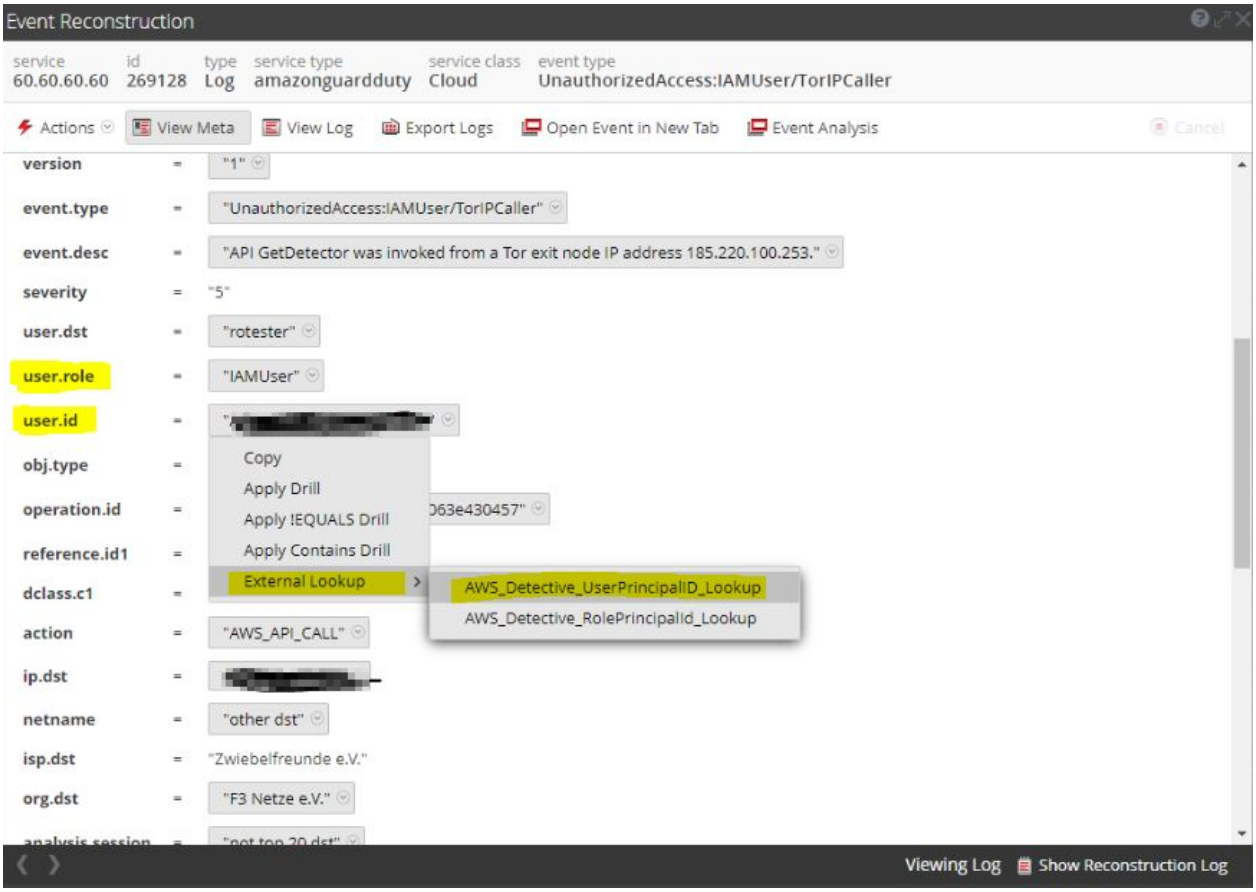
Note: You will need to repeat the procedure for other available Meta Keys to create Context Menu Actions for them.

For more details, see the Add Custom Context Menu Actions from the System Configuration Guide.

Pivot to AWS Detective using RSA Netwitness Context Menu Actions

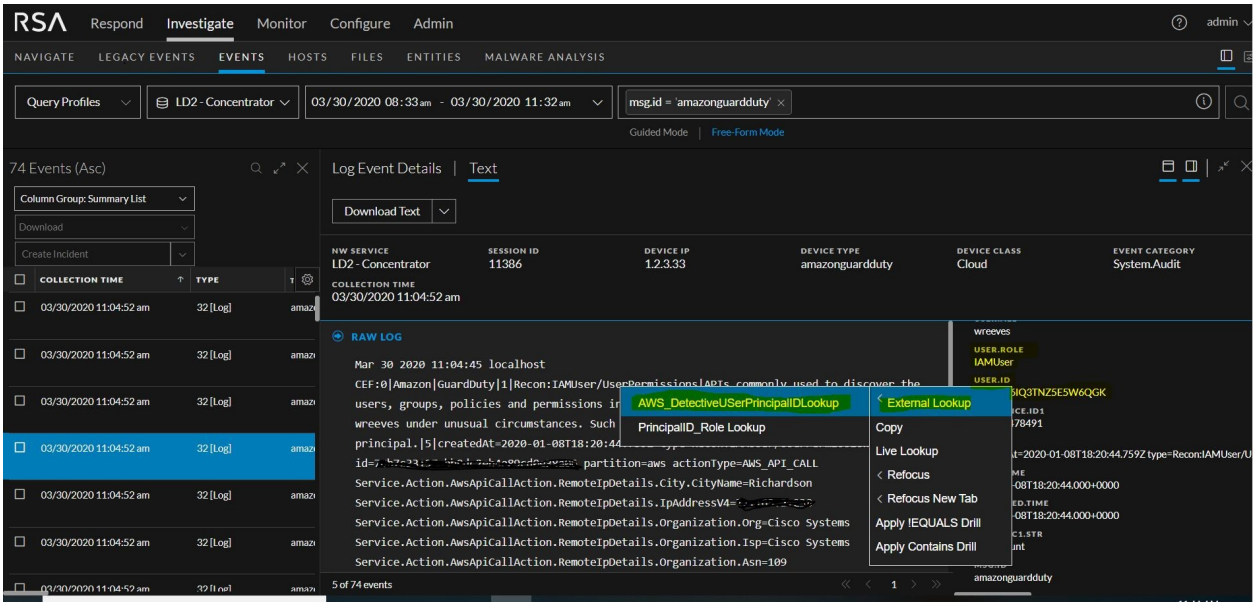
Go to event reconstruction for collected GuardDuty events in RSA Netwitness Concentrator. Pivot to AWS Detective using the RSA Context Menu Action as shown below in User Principal ID Pivoting in RSA Netwitness 11.3.1.

For more details, see the example procedure at the end of the Add Custom Context Menu Actions topic in the System Configuration Guide.



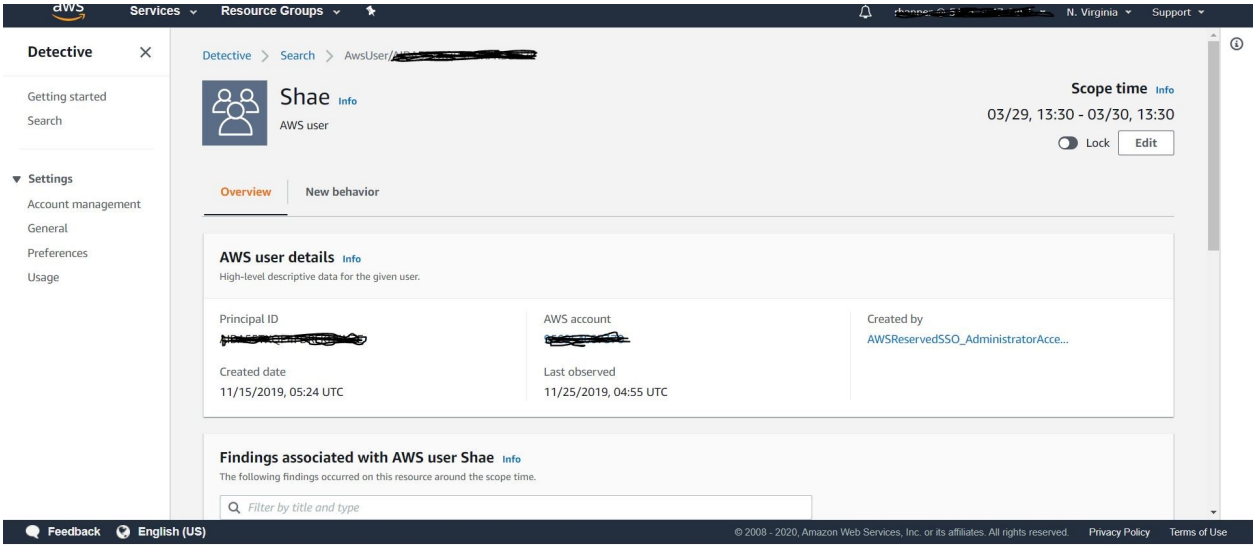
User Principal ID Pivoting in RSA Netwitness 11.3.1

The following image shows an example of pivoting on User Principal ID in RSA NetWitness 11.4.



User Principal ID Pivoting in RSA Netwitness 11.4 and later

The following image is taken from Amazon Detective, after pivoting on User Principal ID in RSA NetWitness.



User ID Landing page in AWS Detective after pivoting from RSA Netwitness Events page

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.