RSA NetWitness Platform

Event Source Log Configuration Guide

Amazon Detective

Last Modified: Thursday, April 2, 2020

Event Source Product Information:

Vendor: AWS
Event Source: Amazon Detective
Versions: API v1.0

RSA Product Information:

Supported On: NetWitness Platform 11.3.1 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

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 RSA NetWitness Platform Logs, and are consuming AWS GuardDuty events, can pivot directly to related GuardDuty findings in Amazon Detective.

> **Note:** AWS Detective Integration with RSA NetWitness Platform 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 RSA NetWitness Platform, 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 RSA NetWitness Platform and then perform an external lookup using meta keys.

Meta Keys

The following table lists the mappings between AWS Detective Concepts and the corresponding RSA NetWitness Platform 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 RSA NetWitness Platform 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 RSA NetWitness.

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 (Figure 1 . 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 RSA NetWitness Platform.

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.

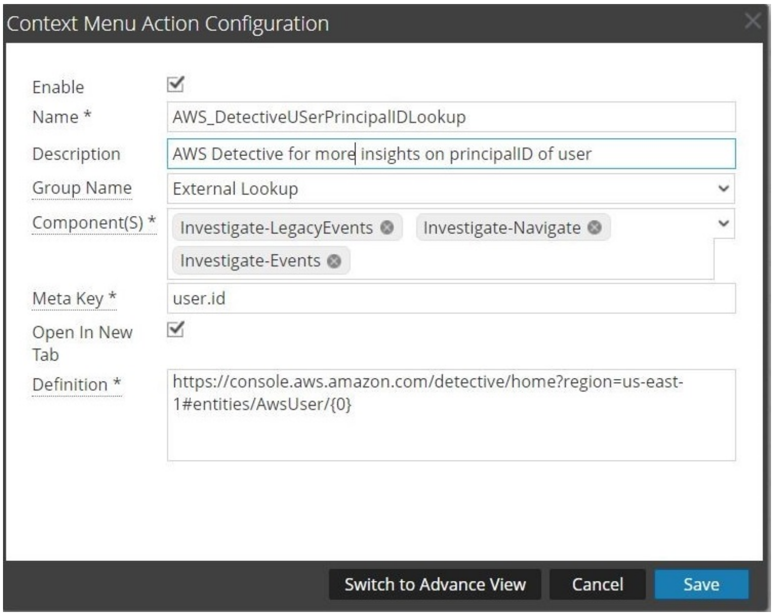
Note: RSA NetWitness does not support parameters to be added to the AWS Detective pivoting URL. However, you can apply this property when you pivot to an AWS Detective page using the Scope time option. Refer to Figure 4 . User ID Landing page in AWS Detective after pivoting from RSA Netwitness Events 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 RSA NetWitness Platform 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.



Context Menu Action Configuration

Enable ☑

Name * AWS_DetectiveUSerPrincipalIDLookup

Description AWS Detective for more insights on principalID of user

Group Name External Lookup

Component(S) * Investigate-LegacyEvents ⊗ Investigate-Navigate ⊗ Investigate-Events ⊗

Meta Key * user.id

Open In New Tab ☑

Definition * https://console.aws.amazon.com/detective/home?region=us-east-1#entities/AwsUser/{0}

Figure 1 Example Context Menu Action Configuration Dialog Box

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

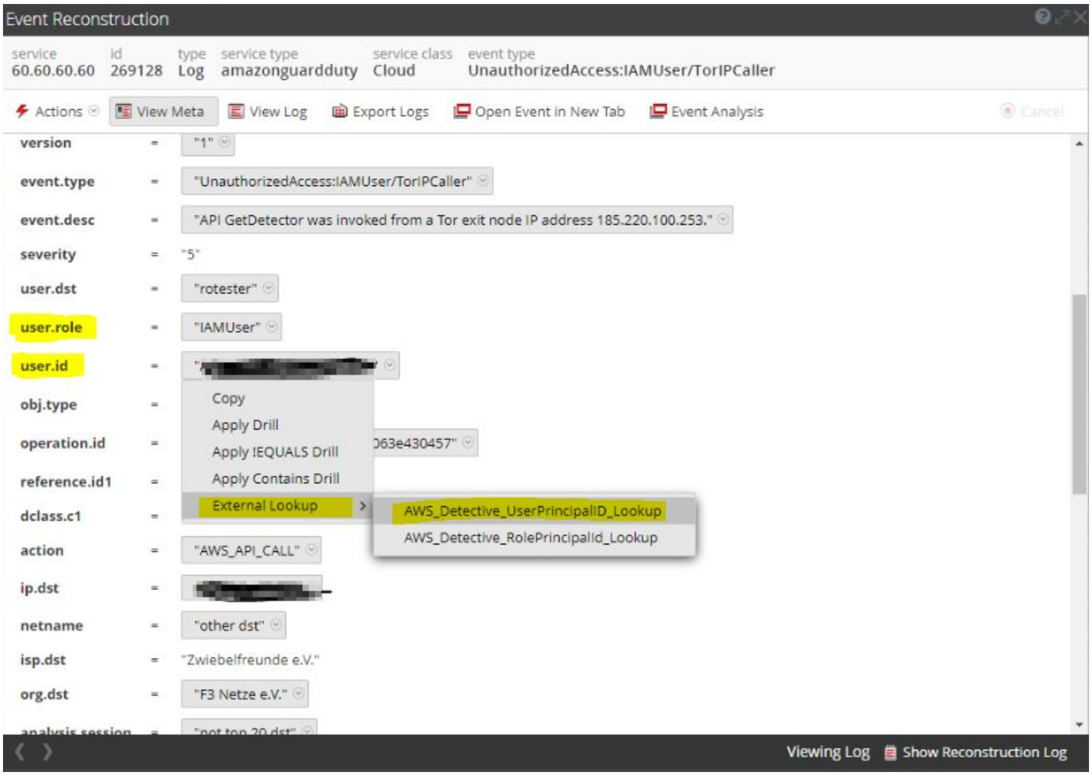
Note: You will need to repeat the procedure for other available Meta Keys to create Context Menu Actions for them.

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 Figure 2 . 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.

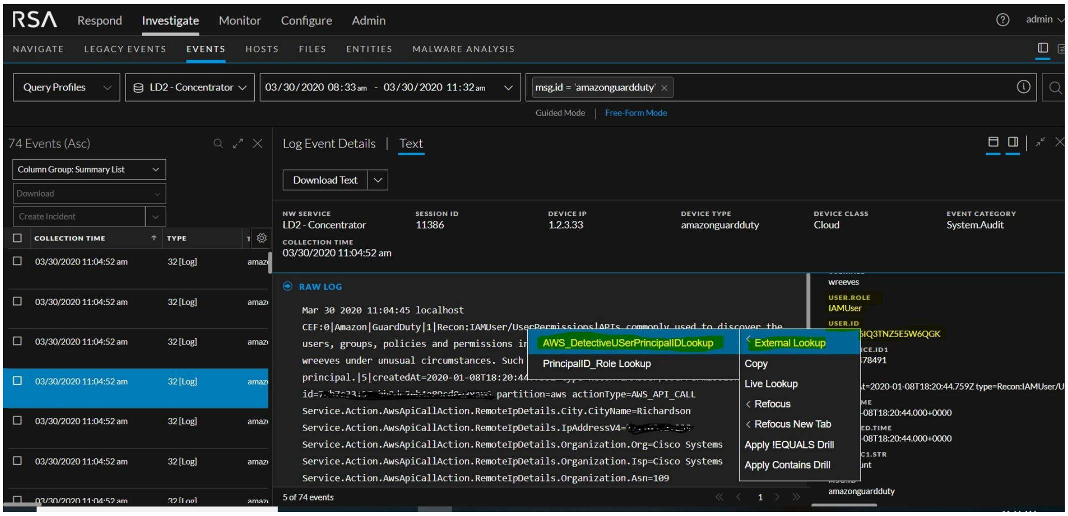


service	id	type	service type	service class	event type
60.60.60.60	269128	Log	amazonguardduty	Cloud	UnauthorizedAccess:IAMUser/TorIPCaller

version = "1"
event.type = "UnauthorizedAccess:IAMUser/TorIPCaller"
event.desc = "API GetDetector was invoked from a Tor exit node IP address 185.220.100.253."
severity = "5"
user.dst = "rotester"
user.role = "IAMUser"
user.id = "[redacted]
obj.type =
operation.id = 063e430457"
reference.id1 =
dclass.c1 =
action = "AWS_API_CALL"
ip.dst = [redacted]
netname = "other dst"
isp.dst = "Zwiebelfreunde e.V."
org.dst = "F3 Netze e.V."
analysis.session = "not top 20 dst"

Figure 2 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.



03/30/2020 08:33 am - 03/30/2020 11:32 am

msg.id = 'amazonguardduty'

74 Events (Asc)

COLLECTION TIME	TYPE	
03/30/2020 11:04:52 am	32 [Log]	amaz
03/30/2020 11:04:52 am	32 [Log]	amaz
03/30/2020 11:04:52 am	32 [Log]	amaz
03/30/2020 11:04:52 am	32 [Log]	amaz
03/30/2020 11:04:52 am	32 [Log]	amaz
03/30/2020 11:04:52 am	32 [Log]	amaz
03/30/2020 11:04:52 am	32 [Log]	amaz

NW SERVICE	SESSION ID	DEVICE IP	DEVICE TYPE	DEVICE CLASS	EVENT CATEGORY
LD2 - Concentrator	11386	1.2.3.33	amazonguardduty	Cloud	System.Audit

COLLECTION TIME
03/30/2020 11:04:52 am

RAW LOG

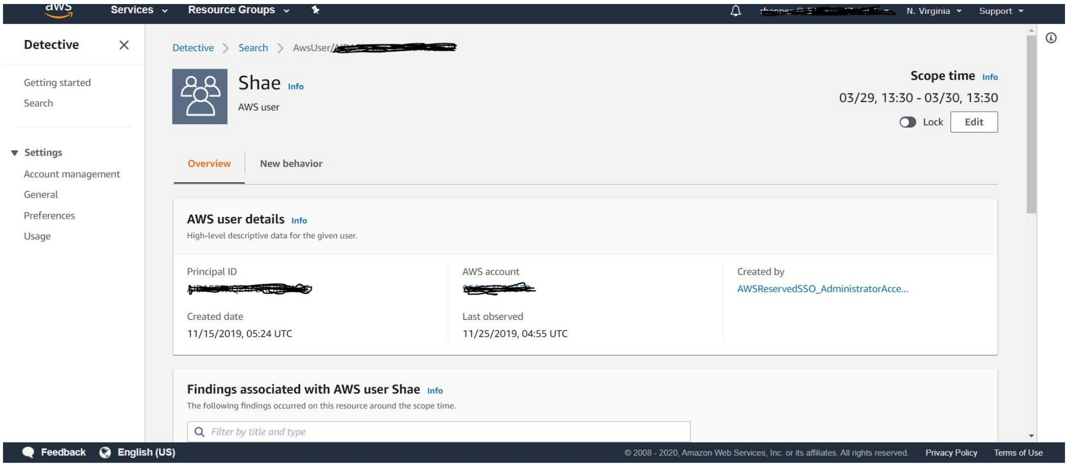
```
Mar 30 2020 11:04:45 localhost
CEF:0|Amazon|GuardDuty|1|Recon:IAMUser/UserPermissions|APIs commonly used to discover the
users, groups, policies and permissions ir
wreeves under unusual circumstances. Such
principal.|5|createdAt=2020-01-08T18:20:44
id=[redacted] partition=aws actionType=AWS_API_CALL
Service.Action.AwsApiCallAction.RemoteIpDetails.City.CityName=Richardson
Service.Action.AwsApiCallAction.RemoteIpDetails.IpAddressV4=[redacted]
Service.Action.AwsApiCallAction.RemoteIpDetails.Organization.Org=Cisco Systems
Service.Action.AwsApiCallAction.RemoteIpDetails.Organization.Isp=Cisco Systems
Service.Action.AwsApiCallAction.RemoteIpDetails.Organization.Asn=109
```

wreeves
USER.ROLE
IAMUser
USER.ID
6IQ3TNZ5E5W6QGK
ICE.ID1
178491
t=2020-01-08T18:20:44.759Z type=Recon:IAMUser/U
ME
-08T18:20:44.000+0000
ED.TIME
-08T18:20:44.000+0000
C1.STR
unt
amazonguardduty

5 of 74 events

Figure 3 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.



Detective > Search > AwsUser/[redacted]

Shae
AWS user

Scope time
03/29, 13:30 - 03/30, 13:30

AWS user details
High-level descriptive data for the given user.

Principal ID
[redacted]

AWS account
[redacted]

Created by
AWSReservedSSO_AdministratorAcce...

Created date
11/15/2019, 05:24 UTC

Last observed
11/25/2019, 04:55 UTC

Findings associated with AWS user Shae
The following findings occurred on this resource around the scope time.

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Figure 4 User ID Landing page in AWS Detective after pivoting from RSA Netwitness Events page

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.