aws

User Guide

Amazon Detective

Amazon Detective: User Guide

Table of Contents

How Amazon Detective is used for investigation

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of security findings or suspicious activity. If you are new to Detective, see What is Detective? and Detective terms and concepts in the *Detective Administration Guide*.

Topics

Detective investigations

You can use the Amazon Detective investigations feature to investigate IAM users and IAM roles using indicators of compromise, which can help you determine if a resource is involved in a security incident. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident. With Detective investigations you can maximize efficiency, focus on the security threats, and strengthen incidence response capabilities.

Detective investigations uses machine learning models and threat intelligence to automatically analyze resources in your AWS environment to identify potential security incidents. It lets you proactively, effectively, and efficiently use automation built on top of Detective's behavioral graph to improve security operations. Using Detective investigations you can investigate attack tactics, impossible travel, flagged IP addresses, and finding groups. It performs initial security investigation steps and generates a report highlighting the risks identified by Detective, to help you understand security events and respond to potential incidents.

For more details, see *Detective investigations*

Investigation phases and starting points

Amazon Detective provides tools to support the overall investigation process. An investigation in Detective can start from a finding, a finding group, or an entity.

Investigation phases

Any investigation process involves the following phases:

Triage

The investigation process starts when you are notified about a suspected instance of malicious or high-risk activity. For example, you are assigned to look into findings or alerts uncovered by services such as Amazon GuardDuty and Amazon Inspector.

In the triage phase, you determine whether you believe the activity is a true positive (genuine malicious activity) or false positive (not malicious or high-risk activity). Detective profiles support the triage process by providing insight into the activity for the involved entity.

For true positive instances, you continue to the next phase.

Scoping

During the scoping phase, analysts determine the extent of the malicious or high-risk activity and the underlying cause.

Scoping answers the following types of questions:

- What systems and users were compromised?
- Where did the attack originate?
- How long has the attack been going on?
- Is there other related activity to uncover? For example, if an attacker is extracting data from your system, how did they obtain it?

Detective visualizations can help you to identify other entities that were involved or affected.

Response

The final step is to respond to the attack in order to stop the attack, minimize the damage, and prevent a similar attack from happening again.

Starting points for a Detective investigation

Every investigation in Detective has an essential starting point. For example, you might be assigned an Amazon GuardDuty or AWS Security Hub finding to investigate. Or you might have a concern about unusual activity for a specific IP address.

Typical starting points for an investigation include findings detected by GuardDuty and entities extracted from Detective source data.

Findings detected by GuardDuty

GuardDuty uses your log data to uncover suspected instances of malicious or high-risk activity. Detective provides resources that help you investigate these findings.

For each finding, Detective provides the associated finding details. Detective also shows the entities, such as IP addresses and AWS accounts, that are connected to the finding.

You can then explore the activity for the involved entities to determine whether the detected activity from the finding is a genuine cause for concern.

For more information, see *Viewing a finding overview*.

AWS security findings aggregated by Security Hub

AWS Security Hub aggregates security findings from various findings providers in a single place, and provides you with a comprehensive view of your security state in AWS. Security Hub eliminates the complexity of addressing large volumes of findings from multiple providers. It reduces the effort required to manage and improve the security of all of your AWS accounts, resources, and workloads. Detective provides resources that help you investigate these findings.

For each finding, Detective provides the associated finding details. Detective also shows the entities, such as IP addresses and AWS accounts, that are connected to the finding.

For more information, see *Viewing a finding overview*.

Entities extracted from Detective source data

From the ingested Detective source data, Detective extracts entities such as IP addresses and AWS users. You can use one of these as an investigation starting point.

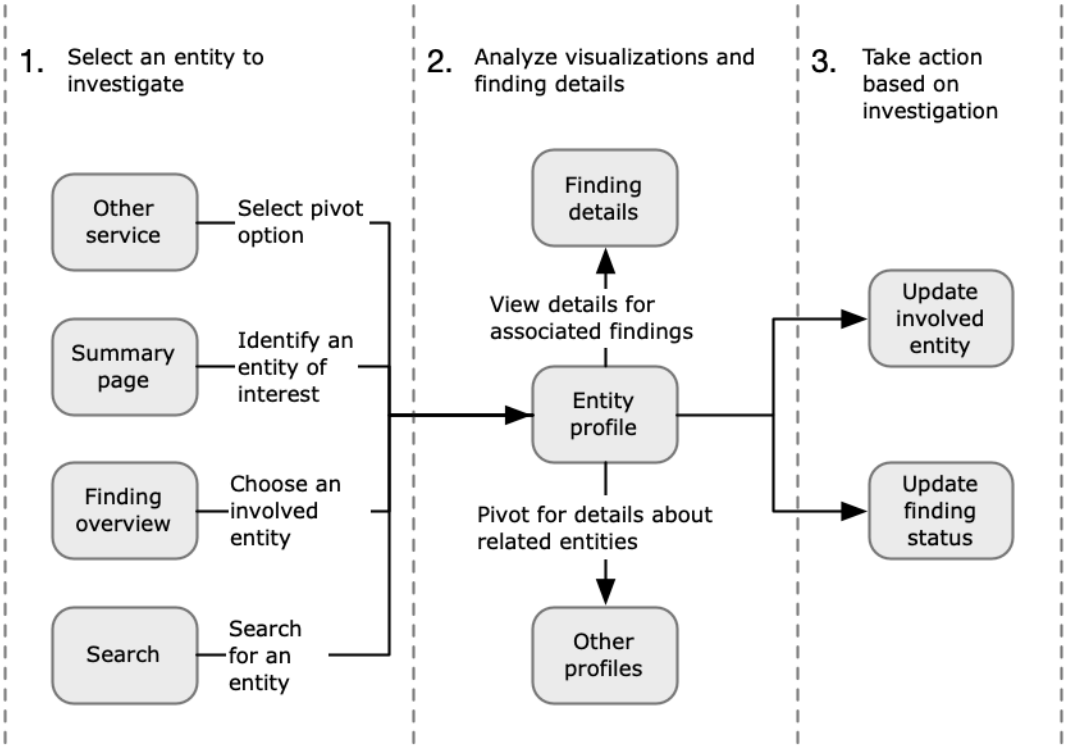
Detective provides general details about the entity, such as the IP address or user name. It also provides details on activity history. For example, Detective can report what other IP addresses an entity has connected to, been connected to, or used.

For more information, see *Analyzing entity details*.

Amazon Detective investigation flow

You can use Amazon Detective to investigate an entity such as an EC2 instance or an AWS user. You can also investigate security findings.

At a high level, the following image shows the process for a Detective investigation.



Step 1: Select the entity to investigate

When looking at a finding in GuardDuty, analysts can choose to investigate an associated entity in Detective. See the section called “Pivoting from another console”.

You can also use the Detective **Summary** page to identify an entity to investigate. See *Using the Summary page*.

From a Detective finding overview, you can choose an involved entity to investigate. See *Viewing a finding overview*.

You can use the Detective search function to find and select an entity to investigate. See *Searching for a finding or entity*.

Selecting the entity takes you to the entity profile in Detective.

Step 2: Analyze visualizations on profiles

Each entity profile contains a set of visualizations that are generated from the behavior graph. The behavior graph is created from the log files and other data that are fed into Detective.

The visualizations show activity that is related to an entity. You use these visualizations to answer questions to determine whether the entity activity is unusual. See *Analyzing entity details*.

To help guide the investigation, you can use the Detective guidance provided for each visualization. The guidance outlines the displayed information, suggests questions for you to ask, and proposes next steps based on the answers. See the section called "Using profile panel guidance".

Each profile contains a list of associated findings. You can view the details for a finding, and view the finding overview. See *Viewing findings for an entity*.

From an entity profile, you can pivot to other entity and finding profiles, to investigate further into activity for related assets.

Step 3: Take action

Based on the results of your investigation, take the appropriate action.

For a finding that is a false positive, you can archive the finding. From Detective, you can archive GuardDuty findings. See *Archiving a GuardDuty finding*.

Otherwise, you take the appropriate action to address the vulnerability and mitigate damage. For example, you might need to update the configuration of a resource.

Data in a behavior graph

In Amazon Detective, you conduct investigations using data from a Detective behavior graph.

A behavior graph is a linked set of data generated from the Detective source data that is ingested from one or more Amazon Web Services (AWS) accounts.

The behavior graph uses the source data to do the following:

- Generate an overall picture of your systems, users, and the interactions among them over time
- Perform more detailed analysis of specific activity to help you answer questions that arise as you conduct investigations
- Correlate collections of findings, entities, and evidence that may be related to the same event or security issue.

Note that all extraction, modeling, and analytics of behavior graph data occurs within the context of each individual behavior graph.

For information about how an administrator account manages the member accounts in a behavior graph, see Managing accounts in the *Detective Administration Guide*.

Contents

How Amazon Detective uses source data to populate a behavior graph

To provide the raw data for investigations, Detective brings together data from across your AWS environment and beyond, including the following:

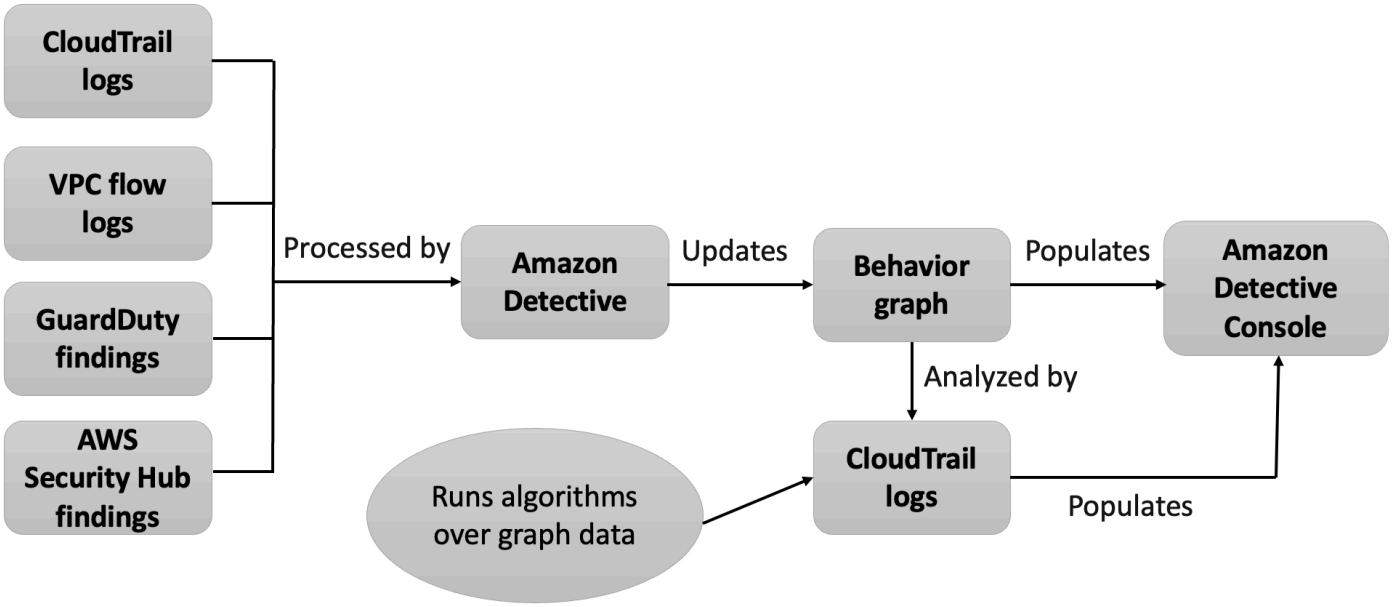
- Log data, including Amazon Virtual Private Cloud (Amazon VPC) and AWS CloudTrail
- Findings from Amazon GuardDuty

- Findings from AWS Security Hub

To learn more about the source data used in a behavior graph, see Source data used in a behavior graph in the *Detective Administration Guide*.

How Detective processes source data

As new data comes in, Detective uses a combination of extraction and analytics to populate the behavior graph.



Detective extraction

Extraction is based on configured mapping rules. A mapping rule basically says, "Whenever you see this piece of data, use it in this specific way to update behavior graph data."

For example, an incoming Detective source data record might include an IP address. If it does, Detective uses the information in that record to create a new IP address entity or update an existing IP address entity.

Detective analytics

Analytics are more complex algorithms that analyze the data to provide insight into activity that is associated with entities.

For example, one type of Detective analytic analyzes how often activity occurs by running algorithms. For entities that make API calls, the algorithm looks for API calls that the entity doesn't normally use. The algorithm also looks for a large spike in the number of API calls.

Analytic insights support investigations by providing answers to key analyst questions and are frequently used to populate finding and entity profile panels.

Training period for new behavior graphs

One avenue of investigation for a finding is to compare the activity during the finding scope time to activity that occurred before the finding was detected. Activity that has not been seen before might be more likely to be suspicious.

Some Amazon Detective profile panels highlight activity that was not observed during the time period before the finding. Several profile panels also display a baseline value to show the average activity during the 45 days before the scope time.

As more data is extracted into your behavior graph, Detective develops a more accurate picture of what activity is normal in your organization and what activity is unusual.

However, to create this picture, Detective needs access to at least two weeks of data. The maturity of the Detective analysis also increases with the number of accounts in the behavior graph.

The first two weeks after you activate Detective are considered a training period. During this period, profile panels that compare scope time activity to earlier activity display a message that Detective is in a training period.

During the free trial, Detective recommends that you add as many member accounts as you can to the behavior graph. This provides Detective with a larger pool of data, which allows it to generate a more accurate picture of the normal activity for your organization.

Overview of the behavior graph data structure

The behavior graph data structure defines the structure of the extracted and analyzed data. It also defines how the source data is mapped to the behavior graph.

Types of elements in the behavior graph data structure

The behavior graph data structure is made up of the following information elements.

Entity

An entity represents an item extracted from the Detective source data.

Each entity has a type, which identifies the type of object it represents. Examples of entity types include IP addresses, Amazon EC2 instances, and AWS users.

For each entity, the source data is also used to populate entity properties. Property values might be extracted directly from source records or aggregated across multiple records.

Some properties consist of a single scalar or aggregated value. For example, for an EC2 instance, Detective tracks the type of instance and the total number of bytes processed.

Time series properties track activity over time. For example, for an EC2 instance, Detective tracks over time the unique ports that it used.

Relationships

A relationship represents activity occurring between individual entities. Relationships are also extracted from the Detective source data.

Similar to an entity, a relationship has a type, which identifies the types of entities involved and the direction of the connection. An example of a relationship type is IP addresses connecting to EC2 instances.

For each individual relationship, such as a specific IP address connecting to a specific instance, Detective tracks the occurrences over time.

Types of entities in the behavior graph data structure

The behavior graph data structure consists of entity and relationship types that do the following:

- Track the servers, IP addresses, and user agents being used
- Track the AWS users, roles, and accounts being used
- Track the network connections and authorizations that occur in your AWS environment

The behavior graph data structure contains the following entity types.

AWS account

AWS accounts that are present in the Detective source data.

For each account, Detective answers several questions:

- What API calls has the account used?
- What user agents has the account used?
- What autonomous system organizations (ASOs) has the account used?
- In what geographic locations has the account been active?

AWS role

AWS roles that are present in the Detective source data.

For each role, Detective answers several questions:

- What API calls has the role used?
- What user agents has the role used?
- What ASOs has the role used?
- In what geographic locations has the role been active?
- What resources have assumed this role?
- What roles has this role assumed?
- What role sessions have involved this role?

AWS user

AWS users that are present in the Detective source data.

For each user, Detective answers several questions:

- What API calls has the user used?
- What user agents has the user used?
- In what geographic locations has the user been active?
- What roles has this user assumed?
- What role sessions have involved this user?

Federated user

Instances of a federated user. Examples of federated users include the following:

- An identity that logs in using Security Assertion Markup Language (SAML)
- An identity that logs in using web identity federation

For each federated user, Detective answers these questions:

- What identity provider did the federated user authenticate with?
- What was the audience of the federated user? The audience identifies the application that requested the web identity token of the federated user.
- In what geographic locations has the federated user been active?
- What user agents has the federated user used?
- What ASOs has the federated user used?
- What roles has this federated user assumed?
- What role sessions have involved this federated user?

EC2 instance

EC2 instances that are present in the Detective source data.

For EC2 instances, Detective answers several questions:

- What IP addresses have communicated with the instance?
- What ports have been used to communicate with the instance?
- What volume of data has been sent to and from the instance?
- What VPC contains the instance?
- What API calls has the EC2 instance used?
- What user agents has the EC2 instance used?
- What ASOs has the EC2 instance used?
- In what geographic locations has the EC2 instance been active?
- What roles has the EC2 instance assumed?

Role session

Instances of a resource that is assuming a role. Each role session is identified by the role identifier and a session name.

For each role, Detective answers several questions:

- What resources were involved in this role session? In other words, what role was assumed, and what resource assumed the role?

  Note that for cross-account role assumption, Detective cannot identify the resource that assumed the role.

- What API calls has the role session used?
- What user agents has the role session used?
- What ASOs has the role session used?
- In what geographic locations has the role session been active?
- What user or role started this role session?
- What role sessions started from this role session?

Finding

Findings uncovered by Amazon GuardDuty that are fed into the Detective source data.

For each finding, Detective tracks the finding type, origin, and the time window for the finding activity.

It also stores information specific to the finding, such as roles or IP addresses that are involved in the detected activity.

IP address

IP addresses that are present in the Detective source data.

For each IP address, Detective answers several questions:

- What API calls has the address used?
- What ports has the address used?
- What users and user agents have used the IP address?
- In what geographic locations has the IP address been active?
- What EC2 instances has this IP address been assigned to and communicated with?

S3 bucket

S3 buckets that are in the Detective source data.

For each S3 bucket, Detective answers these questions:

- What principals interacted with the S3 bucket?
- What API calls were made to the S3 bucket?
- From what geographic locations did principals make API calls to the S3 bucket?
- What user agents were used to interact with the S3 bucket?

- What ASOs were used to interact with the S3 bucket?

You can delete an S3 bucket and then create a new bucket with the same name. Because Detective uses the S3 bucket name to identify the S3 bucket, it treats these as a single S3 bucket entity. On the entity profile, **Creation time** is the first creation time. **Deletion time** is the most recent deletion time.

To view all of the creation and deletion events, set the scope time to start with the creation time and end with the deletion time. See *Managing the scope time*. On the **Overall API call volume** profile panel, display the activity details for the scope time. Filter the API methods to show `Create` and `Delete` methods. See the section called "Overall API call volume".

User agent

User agents that are present in the Detective source data.

For each user agent, Detective answers questions such as the following:

- What API calls has the user agent used?
- What users and roles have used the user agent?
- What IP addresses have used the user agent?

EKS Cluster

EKS clusters that are present in the Detective source data.

> **Note**
>
> To see complete details for this entity type the optional EKS audit logs data source must be enabled. For more info see Optional data sources

For each EKS cluster, Detective answers questions such as the following:

- What Kubernetes API calls have been run in this cluster?
- What Kubernetes users and service accounts (subjects) are active in this cluster?
- What containers have been launched in this cluster?
- What images are used to launch containers in this cluster?

Kubernetes Pod

Kubernetes pods that are present in the Detective source data.

> **Note**
>
> To see complete details for this entity type the optional EKS audit logs data source must be enabled. For more info see Optional data sources

For each pod, Detective answers questions such as the following:

- What container images in this pod are common in my accounts?
- What activity has been directed at this pod?
- What containers run in this pod?
- Are registries from containers in this pod common in my accounts?
- What other containers are running in the other pods of the workload?
- Are there any anomalous containers in this pod that are not in the other pods of the workload?

Container Image

Container images that are present in the Detective source data.

> **Note**
>
> To see complete details for this entity type the optional EKS audit logs data source must be enabled. For more info see Optional data sources

For each container image, Detective answers questions such as the following:

- What other images in my environment share the same repository or registry with this image?
- How many copies of this image are running in my environment?

Kubernetes Subject

Kubernetes subjects that are present in the Detective source data. A Kubernetes subject is a user or service account.

> **Note**
>
> To see complete details for this entity type the optional EKS audit logs data source must be enabled. For more info see Optional data sources

For each subject, Detective answers questions such as the following:

- What IAM principals have authenticated as this subject?
- What findings are associated with this subject?
- What IP addresses is the subject using?

Navigating directly to an entity profile or finding overview

To navigate directly to an entity profile or finding overview in Amazon Detective, you can use one of these options.

- From Amazon GuardDuty or AWS Security Hub, you can pivot from a GuardDuty finding to the corresponding Detective finding profile.
- You can assemble a Detective URL that identifies a finding or entity and sets the scope time to use.

Contents

Pivoting to an entity profile or finding overview from Amazon GuardDuty or AWS Security Hub

From the Amazon GuardDuty console, you can navigate to the entity profile for an entity that is related to a finding.

From the GuardDuty and AWS Security Hub consoles, you can also navigate to a finding overview. This also provides links to the entity profiles for the involved entities.

These links can help to streamline the investigation process. You can quickly use Detective to see the associated entity activity and determine next steps. You can then archive a finding if it is a false positive or explore further to determine the scope of the problem.

How to pivot to the Amazon Detective console

The investigation links are available for all GuardDuty findings. GuardDuty also allows you to choose whether to navigate to an entity profile or to the finding overview.

To pivot to Detective from the GuardDuty console

1. Open the GuardDuty console at https://console.aws.amazon.com/guardduty/.
2. If necessary, choose **Findings** in the left navigation pane.
3. On the GuardDuty **Findings** page, choose the finding.

   The finding details pane displays to the right of the finding list.
4. On the finding details pane, choose **Investigate in Detective**.

   GuardDuty displays a list of available items to investigate in Detective.

   The list contains both the related entities, such as IP addresses or EC2 instances, and the finding.
5. Choose an entity or the finding.

   The Detective console opens in a new tab. The console opens to the entity or finding profile.

   If you have not enabled Detective, then the console opens to a landing page that provides an overview of Detective. From there, you can choose to enable Detective.

To pivot to Detective from the Security Hub console

1. Open the AWS Security Hub console at https://console.aws.amazon.com/securityhub/.
2. If necessary, choose **Findings** in the left navigation pane.
3. On the Security Hub **Findings** page, choose a GuardDuty finding.
4. In the details pane, choose **Investigate in Detective** and then choose **Investigate finding**.

   When you choose **Investigate finding**, the Detective console opens in a new tab. The console opens to the finding overview.

   The Detective console always opens to the Region where the finding originated, even if you pivot from your aggregation Region. For more information about finding aggregation, see Aggregating findings across Regions in the *AWS Security Hub User Guide*.

   If you have not enabled Detective, the console opens to the Detective landing page. From there, you can enable Detective.

Troubleshooting the pivot

To use the pivot, one of the following must be true:

- Your account must be an administrator account for both Detective and the service you are pivoting from.
- You have assumed a cross-account role that grants you administrator account access to the behavior graph.

For more information about the recommendation to align administrator accounts, see Recommended alignment with Amazon GuardDuty and AWS Security Hub in *Detective Administration Guide*.

If the pivot does not work, check the following.

- **Does the finding belong to an enabled member account in your behavior graph?** If the associated account was not invited to the behavior graph as a member account, then the behavior graph does not contain data for that account.

  If an invited member account did not accept the invitation, then the behavior graph does not contain data for that account.
- **Is the finding archived?** Detective does not receive archived findings from GuardDuty.
- **Did the finding occur before Detective began to ingest data into your behavior graph?** If the finding is not present in the data that Detective ingests, then the behavior graph does not contain data for it.
- **Is the finding from the correct Region?** Each behavior graph is specific to a Region. A behavior graph does not contain data from other Regions.

Navigating to an entity profile or finding overview using a URL

To navigate to an entity profile or finding overview in Amazon Detective, you can use a URL that provides a direct link to it. The URL identifies the finding or entity. It can also specify the scope time to use on the profile. Detective maintains up to a year of historical event data.

Format of a profile URL

> **Note**
>
> If you are using the old URL format, Detective will automatically redirect to the new URL. The old format of the URL was: https://console.aws.amazon.com/detective/home?region=*Region*#*type*/*namespace*/*instanceID*?*parameters*

The new format of the profile URL is as follows:

- For entities - https://console.aws.amazon.com/detective/home?region=*Region*#*entities*/*namespace*/*instanceID*?*parameters*
- For findings - https://console.aws.amazon.com/detective/home?region=*Region*#*findings*/*instanceID*?*parameters*

The URL requires the following values.

Region

The Region that you want to use.

type

The type of item for the profile that you are navigating to.

- `entities` - Indicates that you are navigating to an entity profile
- `findings` - Indicates that you are navigating to a finding overview

namespace

For entities, the namespace is the name of the entity type.

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`

- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`
- `KubernetesSubject`
- `ContainerPod`
- `ContainerCluster`
- `ContainerImage`

instanceID

The instance identifier of the finding or entity.

- For a GuardDuty finding, the GuardDuty finding identifier.
- For an AWS account, the account ID.
- For AWS roles and users, the principal ID of the role or of the user.
- For federated users, the principal ID of the federated user. The principal ID is either *<identityProvider>*:*<username>* or *<identityProvider>*:*<audience>*:*<username>*.
- For IP addresses, the IP address.
- For user agents, the user agent name.
- For EC2 instances, the instance ID.
- For role sessions, the session identifier. The session identifier uses the format *<rolePrincipalID>*:*<sessionName>*.
- For S3 buckets, the bucket name.
- For FindingGroups, a UUID. for example, `ca6104bc-a315-4b15-bf88-1c1e60998f83`
- For EKS resources, use the following formats:
  - EKS cluster: *<clusterName>~<accountId>~EKS*
  - Kubernetes Pod: *<podUid>~<clusterName><accountId>~EKS*
  - Kubernetes Subject: *<subjectName>~<clusterName>~<accountId>*
  - Container image: *<registry>/<repository>:<tag>@<digest>*

The finding or entity must be associated with an enabled account in your behavior graph.

The URL can also include the following optional parameters, which are used to set the scope time. For more information about scope time and how it is used on profiles, see *Managing the scope time*.

`scopeStart`

Start time for the scope time to use on the profile. Start time must be within the last 365 days.

The value is the epoch timestamp.

If you provide a start time but no end time, then the scope time ends at the current time.

`scopeEnd`

End time for the scope time to use on the profile.

The value is the epoch timestamp.

If you provide an end time, but no start time, then the scope time includes all time before the end time.

If you don't specify the scope time, then the default scope time is used.

- For findings, the default scope time uses the first and last times that the finding activity was observed.
- For entities, the default scope time is the previous 24 hours.

Here is an example of a Detective URL:

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

This example URL provides the following instructions.

- Display the entity profile for the IP address 192.168.1.
- Use a scope time that starts Monday, March 18, 2019 12:00:00 AM GMT and that ends Monday, March 18, 2019 12:00:00 PM GMT.

Troubleshooting a URL

If the URL does not display the expected profile, first check that the URL uses the correct format and that you have provided the correct values.

- Did you start with the correct URL (`findings` or `entities`)?
- Did you specify the correct namespace?
- Did you provide the correct identifier?

If the values are correct, then you can also check the following.

- **Does the finding or entity belong to an enabled member account in your behavior graph?** If the associated account was not invited to the behavior graph as a member account, then the behavior graph does not contain data for that account.

  If an invited member account did not accept the invitation, then the behavior graph does not contain data for that account.
- **For a finding, is the finding archived?** Detective does not receive archived findings from Amazon GuardDuty.
- **Did the finding or entity occur before Detective began to ingest data into your behavior graph?** If the finding or entity is not present in the data that Detective ingests, then the behavior graph does not contain data for it.
- **Is the finding or entity from the correct Region?** Each behavior graph is specific to a Region. A behavior graph does not contain data from other Regions.

Adding Detective URLs for findings to Splunk

The Splunk Trumpet project allows you send data from AWS services to Splunk.

You can configure the Trumpet project to generate Detective URLs for Amazon GuardDuty findings. You can then use these URLs to pivot directly from Splunk to the corresponding Detective finding profiles.

The Trumpet project is available from GitHub at https://github.com/splunk/splunk-aws-project-trumpet.

On the configuration page for the Trumpet project, from **AWS CloudWatch Events**, choose **Detective GuardDuty URLs**.

Searching for a finding or entity

With the Amazon Detective search function, you can search for a finding or entity. From the search results, you can navigate to an entity profile or a finding overview. If your search returns more than 10,000 results, only the top 10,000 results are displayed. Changing the sorting order changes the returned results.

You can export your search results to a comma-separated values (.csv) file. This file contains the data returned in the search page. For more information, see *Exporting data from Detective*.

Completing the search

To complete the search, choose the type of entity to search for. Then provide the exact identifier or identifier with wildcard characters `*` or `?`. To search for a range of IP addresses, you can also use CIDR or dot notations. See the following example search strings.

For IP addresses:

- `1.0.*.*`
- `1.0.133.*`
- `1.0.0.0/16`
- `0.239.48.198/31`

For all other types of entities:

- `Admin`
- `ad*`
- `ad*n`
- `ad*n*`
- `adm?n`
- `a?m*`
- `*min`

For each entity type, the following identifiers are supported:

- For Findings, the finding identifier or finding Amazon Resource Name (ARN).
- For AWS accounts, the account ID.
- For AWS roles and AWS users, either the principal ID, the name, or the ARN.
- For Container clusters, the cluster name or ARN.
- For Container images, the repository or the full digest of the container image.
- For container Pods or Tasks, the pod name or the UID of the pod.
- For EC2 instances, the instance identifier or the ARN.
- For Finding group, the finding group identifier.
- For IP addresses, the address in CIDR or dot notation.
- For Kubernetes subjects (service accounts or users), the name.
- For a role session, you can use any of the following values to search:
  - Role session identifier.

    The role session identifier uses the format *<rolePrincipalID>*:*<sessionName>*.

    Here is an example: `AROA12345678910111213:MySession`.
  - Role session ARN
  - Session name
  - Principal ID of the role that was assumed
  - Name of the role that was assumed
- For S3 buckets, the bucket name or bucket ARN.
- For federated users, the principal ID or the user name. The principal ID is either *<identityProvider>*:*<username>* or *<identityProvider>*:*<audience>*:*<username>*.
- For user agents, the user agent name.

To search for a finding or entity

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Search**.
3. From the **Choose type** menu, choose the type of item you're looking for.

   Note that when you choose **User**, you can search for either an AWS user or a federated user.

Examples from your data contains a sample set of identifiers of the selected type that are in your behavior graph data. To display the profile for one of the examples, choose its identifier.

4. Enter the exact identifier or an identifier with wildcard characters to search for.

   The search is case insensitive.

5. Choose **Search** or press **Enter**.

Using the search results

When you complete the search, Detective displays a list of up to 10,000 matching results. For searches that use a unique identifier, there is only one matching result.

From the results, to navigate to the entity profile or finding overview, choose the identifier.

For findings, roles, users, and EC2 instances, the search results include the associated account. To navigate to the profile for the account, choose the account identifier.

Troubleshooting the search

If Detective does not find the finding or entity, first check that you entered the correct identifier. If the identifier is correct, you can also check the following.

- **Does the finding or entity belong to an enabled member account in your behavior graph?** If the associated account was not invited to the behavior graph as a member account, then the behavior graph does not contain data for that account.

  If an invited member account did not accept the invitation, then the behavior graph does not contain data for that account.
- **For a finding, is the finding archived?** Detective does not receive archived findings from Amazon GuardDuty.
- **Did the finding or entity occur before Detective began to ingest data into your behavior graph?** If the finding or entity is not present in the data that Detective ingests, then the behavior graph does not contain data for it.
- **Is the finding or entity from the correct Region?** Each behavior graph is specific to an AWS Region. A behavior graph does not contain data from other Regions.

Exporting data from Detective

You can export data from the Amazon Detective **Summary** page and search results page. The data is exported in comma-separated values (CSV) format. The file name of the exported data follows the pattern `detective-page-panel-yyyy-mm-dd.csv` format. You can enrich your security investigations by manipulating the data using other AWS services, third-party applications, or spreadsheet programs that support CSV import.

> **Note**
>
> If an export is currently in progress, wait until the export is complete before you try to export additional data.

You can export a comma-separated values (.csv) file that contains data from the following panels and pages in Detective:

- **Summary** page
  - **Roles and users with the most API call volume** panel
  - **EC2 instances with the most traffic volume** panel
  - **EKS clusters with the most Kubernetes pods created** panel
- **Search** page – If your search returns more than 10,000 results, only the top 10,000 results are exported. Changing the sorting order changes the returned results.

Using the Summary page to identify an entity of interest

Use the Summary page in Amazon Detective to identify entities to investigate the origin of activity during the previous 24 hours. The Amazon Detective Summary page helps you to identify entities that are associated with specific types of unusual activity. It is one of several possible starting points for an investigation.

To display the **Summary** page, in the Detective navigation pane, choose **Summary**. The **Summary** page is also displayed by default when you first open the Detective console.

From the **Summary** page, you can identify entities that meet the following criteria:

- Investigations that show potential security events identified by Detective
- Entities involved in activity that occurred in newly observed geolocations
- Entities that made the largest number of API calls
- EC2 instances that had the largest volume of traffic
- Container clusters that had the largest number of containers

From each **Summary** page panel, you can pivot to the profile for a selected entity.

As you review the **Summary** page, you can adjust the **Scope time** to view the activity for any 24-hour time frame in the previous 365 days. When you change the **Start date and time**, the **End date and time** is automatically updated to 24 hours after your chosen start time.

With Detective, you can access up to a year of historical event data. This data is available through a set of visualizations that show changes in the type and volume of activity over a selected time window. Detective links these changes to GuardDuty findings.

For more information about source data in Detective, see Source data used in a behavior graph in the *Detective Administration Guide*.

Investigations

Investigations shows you the potential security events identified by Detective. On the Investigations panel, you can view Critical investigations and the corresponding AWS roles and users that were impacted by security events over a set period of time. Investigations groups together indicators of compromise to help determine if a AWS resource is involved in unusual activity that could indicate malicious behavior and its impact.

Select **View all investigations** to review findings, triage finding groups, and resource details to accelerate your security investigation. Investigations are displayed depending on the selected Scope time. You can adjust the scope time to view investigations in a 24-hour time frame in the previous 365 days. You can pivot directly to **Critical investigations** to see a detailed investigation report.

If you identify a AWS role or user that seems to have suspicious activity, you can pivot directly from the **Investigations** panel to the role or user to continue your investigation. Pivot to a role or user and click **Run investigation** to generate an investigations report. Once you run an investigation on a role or user, the role or user is moved to the **Investigated** tab.

Newly observed geolocations

Newly observed geolocations highlights geographic locations that were the origin of activity during the previous 24 hours, but that were not seen during the baseline time period before that.

The panel includes up to 100 geolocations. The locations are marked on the map and listed in the table below the map.

For each geolocation, the table displays the number of failed and successful API calls made from that geolocation during the previous 24 hours.

You can expand each geolocation to display the list of users and roles that made API calls from that geolocation. For each principal, the table lists the type and the associated AWS account.

If you identify a user or role that seems suspicious, then you can pivot directly from the panel to the user or role profile to continue your investigation. To pivot to a profile, choose the user or role identifier.

Detective determines the location of requests using MaxMind GeoIP databases. MaxMind reports very high accuracy of their data at the country level, although accuracy varies according to factors such as country and type of IP. For more information about MaxMind, see MaxMind IP Geolocation. If you think any of the GeoIP data is incorrect, you can submit a correction request to Maxmind at MaxMind Correct GeoIP2 Data.

Active finding groups in the last 7 days

Active finding groups in the last 7 days shows you correlated groupings of Detective findings, entities, and evidence in your environment that occurred over a set period of time. These groupings

correlate unusual activity that could indicate malicious behavior. The summary page shows up to five groups sorted by the groups containing the most critical findings that have been active in the last week.

You can select values in the **Tactic**, **Account**, **Resource**, and **Findings** content to see more details.

Findings groups are generated on a daily basis. If you identify a finding group of interest, you can select the title to move to a detailed view of a group profile to continue your investigation.

Roles and users with the most API call volume

Roles and users with the most API call volume identifies the users and roles that have made the largest number of API calls during the previous 24 hours.

The panel can include up to 100 users and roles. For each user or role, you can see the type (user or role) and the associated account. You can also see the number of API calls issued by that user or role during the previous 24 hours.

By default, service-linked roles are displayed. Service-linked roles can produce large volumes of AWS CloudTrail activity, which displaces the principals that you want to investigate further. You can choose to turn off **Show service-linked roles**, to filter out service-linked roles from the summary page view.

You can export a comma-separated values (.csv) file that contains the data in this panel. For more information, see *Exporting data from Detective*.

There is also a timeline of the API call volume for the previous 7 days. The timeline can help you to determine whether the volume of API calls is unusual for that principal.

If you identify a user or role for which the API call volume seems suspicious, then you can pivot directly from the panel to the user or role profile to continue your investigation. You can also view the profile of the account associated with the user or role. To view a profile, choose the user, role, or account identifier.

EC2 instances with the most traffic volume

EC2 instances with the most traffic volume identifies the EC2 instances that have had the largest total volume of traffic during the previous 24 hours.

The panel can include up to 100 EC2 instances. For each EC2 instance, you can see the associated account and the number of inbound bytes, outbound bytes, and total bytes from the previous 24 hours.

You can export a comma-separated values (.csv) file that contains the data in this panel. For more information, see *Exporting data from Detective*.

You can also see a timeline showing the inbound and outbound traffic over the previous 7 days. The timeline can help determine whether the volume of traffic is unusual for that EC2 instance.

If you identify an EC2 instance that has suspicious traffic volume, then you can go directly from the panel to the EC2 instance profile to continue your investigation. You can also view the profile of the account that owns the EC2 instance. To view a profile, choose the EC2 instance or account identifier.

Container clusters with the most Kubernetes pods

Container clusters with the most Kubernetes pods created identifies the clusters that have had the most containers running during the previous 24 hours.

This panel includes up to 100 clusters organized by which clusters had the most findings associated with them. For each cluster you can see the associated account, the current number of containers in that cluster, and the number of findings associated with that cluster over the last 24 hours. You can export a comma-separated values (.csv) file that contains the data in this panel. For more information, see *Exporting data from Detective*.

If you identify a cluster with recent findings you can pivot directly from the panel to the cluster profile to continue your investigation. You can also pivot to the profile of the account that owns the cluster. To pivot to a profile, choose the cluster name or account identifier.

Approximate value notification

On **Roles and users with the most API call volume** and **EC2 instances with the most traffic volume**, if a value is followed by an asterisk (*), it means that the value is an approximation. The true value is either equal to or greater than the displayed value.

This occurs because of the method that Detective uses to calculate the volume for each time interval. On the **Summary** page, the time interval is an hour.

For each hour, Detective calculates the total volume for the 1,000 users, roles, or EC2 instances with the largest volume. It excludes the data for the remaining users, roles, or EC2 instances.

If a resource was sometimes in the top 1,000 and sometimes not, then the calculated volume for that resource might not include all of the data. The data for the time intervals where it was not in the top 1,000 is excluded.

Note that this only applies to the **Summary** page. The profile for the user, role, or EC2 instance provides precise details.

Managing the scope time

Customize the scope time used to limit the data displayed on entity profiles.

The charts, timelines, and other data displayed on entity profiles are all based on the current scope time. Scope time is the summary of activity for an entity over time. This appears at the top right of each profile in the Amazon Detective console. The data displayed on those charts, timelines, and other visualizations is based on the scope time. For some profile panels, additional time is added before and after the scope time to provide context. In Detective, all timestamps are displayed in UTC by default. You can select your local time zone by changing the **Timestamp preferences**. To update the **Timestamp preference**, see the section called "Setting the timestamp format".

Detective analytics uses the scope time when checking for unusual activity. The analytics process gets the activity during the scope time, then compares it to the activity during the 45 days before the scope time. It also uses that 45-day timeframe to generate baselines of activity.

On a finding overview, the scope time reflects the first and last time the finding was observed. For more information about finding overview, see *Viewing a finding overview*.

As you work through an investigation, you can adjust the scope time. For example, if the original analysis was based on activity from a single day, you might want to expand that to a week or a month. The expanded period could help you get a better sense of whether the activity fits a normal pattern or is unusual.

You can also set the scope time to match an associated finding for the current entity.

When you change the scope time, Detective repeats its analysis and updates the displayed data based on the new scope time.

The scope time cannot be shorter than one hour and not longer than one year. The start and end time must be on an hour.

Setting specific start and end dates and times

You can set the scope time start and end dates from the Detective console.

To set specific start and end times for the new scope time

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.

2. On an entity profile, choose the scope time.
3. On the **Edit scope time** panel, under **Start**, choose the new start date and time for the scope time. For the new start time, you choose the hour only.
4. Under **End**, choose the new end date and time for the scope time. For the new end time, you choose the hour only. The end time must be at least an hour later than the start time.
5. When you're finished editing, to save the changes and update the displayed data, choose **Update scope time**.

Edit the length of time for the scope time

When you set a scope time length, Detective sets the scope time to that amount of time from the current time.

To edit the length of time for the scope time

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. On an entity profile, choose the scope time.
3. On the **Edit scope time** panel, next to **Historical**, choose the length of time for the scope time.

   Specifying a time range updates the **Start** and **End** settings.
4. When you're finished editing, to save the changes and update the displayed data, choose **Update scope time**.

Setting the scope time to a finding time window

Each finding has an associated time window, which reflects the first and last times the finding was observed. When you view a finding overview, the scope time changes to the finding time window.

From an entity profile, you can align the scope time to the time window for an associated finding. This allows you to investigate the activity that occurred during that time.

To align the scope time to a finding time window, on the **Associated findings** panel, choose the finding that you want to use.

Detective populates the finding details and sets the scope time to the finding time window.

Setting the scope time on the summary page

As you review the **Summary** page, you can adjust the Scope time to view the activity for any 24-hour time frame in the previous 365 days.

To set the scope time on the Summary page

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Summary**.
3. On the **Scope time** panel, next to **Summary**, you can change the **Start date and time**. Start time must be within the last 365 days.

   When you change the **Start date and time**, the **End date and time** is automatically updated to 24 hours after your chosen start time.

   > **Note**
   >
   > With Detective, you can access up to a year of historical event data. For more information on source data in Detective, see Source data used in a behavior graph in the *Detective Administration Guide*.

4. When you're finished editing, to save the changes and update the displayed data, choose **Update scope time**.

Viewing a finding overview

A finding is an instance of potentially malicious activity or other risk that was detected. Amazon GuardDuty and AWS security findings are loaded into Amazon Detective so that you can use Detective to investigate the activity associated with the involved entities. GuardDuty findings are part of the Detective core package and are ingested by default. All other AWS security findings that are aggregated by Security Hub are ingested as an optional data source. See Source data used in a behavior graph for more details.

A Detective finding overview provides detailed information about the finding. It also displays a summary of the involved entities, with links to the associated entity profiles.

If a finding is correlated to a larger activity, Detective notifies you to **Go to finding group**. We recommend using finding groups to continue your investigation, as finding groups enable you to examine multiple activities that relate to a potential security event. See *Analyzing finding groups*.

Scope time used for the finding overview

The scope time for a finding overview is set to the finding time window. The finding time window reflects the first and last time that the finding activity was observed.

Finding details

The panel at the right contains the details for the finding. These are the details provided by the finding provider.

From the finding details, you can also archive the finding. See *Archiving a GuardDuty finding*.

Related entities

The finding overview contains a list of entities that are involved in the finding. For each entity, the list provides overview information about the entity. This information reflects the information on the entity details profile panel on the corresponding entity profile.

You can filter the list based on entity type. You can also filter the list based on text in the entity identifier.

To pivot to the profile for an entity, choose **See profile**. When you pivot to the entity profile, the following occurs:

- The scope time is set to the finding time window.
- On the **Associated findings** panel for the entity, the finding is selected. The finding details remain displayed at the right of the entity profile.

Troubleshooting 'Page not found'

When you navigate to an entity or a finding in Detective, you may see a **Page not found** error message.

To resolve this, do one of the following:

- Make sure that the entity or finding belongs to one of your member accounts. For information on how to review member accounts, see Viewing the list of accounts in the Detective Administration Guide.
- Make sure your administrator account is aligned with GuardDuty and/or Security Hub to pivot to Detective from these services. For the recommendations, see Recommended alignment with GuardDuty and Security Hub in the Detective Administration Guide.
- Verify that the finding occurred after the member account accepted your invitation.
- Verify the Detective behavior graph is ingesting data from an optional data source package. For more information about source data used in Detective behavior graphs, see Source data used in a behavior graph in the Detective Administration Guide.

- To allow Detective to ingest data from Security Hub and add that data to your behavior graph, you must enable Detective for AWS security findings as a data source package. For more information, see AWS security findings in the Detective Administration Guide.

- If you are navigating to an entity profile or finding overview in Detective, make sure that the URL is in the right format. For details on the formation of a profile URL, see Navigating to an entity profile or finding overview using URL.

Analyzing entity details

An entity is a single object extracted from the source data. Examples include a specific IP address, Amazon EC2 instance, or AWS account. For a list of entity types, see the section called "Types of entities in the behavior graph data structure".

An Amazon Detective entity profile is a single page that provides detailed information about the entity and its activity. You might use an entity profile to get supporting details for an investigation into a finding or as part of a general hunt for suspicious activity.

How to display an entity profile

An entity profile appears when you perform one of the following actions:

- From the Amazon GuardDuty console, choose the option to investigate an entity that is related to a selected finding.

  See the section called "Pivoting from another console".
- Go to the Detective URL for the entity profile.

  See the section called "Navigating using a URL".
- Use the Detective search in the Detective console to look up an entity.

  See *Searching for a finding or entity*.
- Choose a link to the entity profile from another entity profile or from a finding overview.

Scope time for an entity profile

When you navigate directly to an entity profile without providing the scope time, the scope time is set to the previous 24 hours.

When you navigate to an entity profile from another entity profile, the currently selected scope time remains in place.

When you navigate to an entity profile from a finding overview, the scope time is set to the finding time window.

For information on setting the scope time, see *Managing the scope time*.

Entity identifier and type

At the top of the profile are the entity identifier and the entity type. Each entity type has a corresponding icon, to provide a visual indicator of the type of profile.

Involved findings

Each profile contains a list of findings that the entity was involved in during the scope time.

You can see the details for each finding, change the scope time to reflect the finding time window, and go to the finding overview to look for other involved resources.

See *Viewing findings for an entity*.

Finding groups involving this entity

Each profile contains a list of finding groups that an entity is included in.

A finding group is made up of findings, entities, and evidence that Detective collects into a group to provide more context on possible security issues.

For more information on finding groups, see *Analyzing finding groups*.

Profile panels containing entity details and analytics results

Each entity profile contains a set of one or more tabs. Each tab contains one or more profile panels. Each profile panel contains text and visualizations that are generated from the behavior graph data. The specific tabs and profile panels are tailored to the entity type.

For most entities, the panel at the top of the first tab provides high-level summary information about the entity.

Other profile panels highlight different types of activity. For an entity that is involved with a finding, the information on the entity profile panels can provide additional supporting evidence to help complete an investigation. Each profile panel provides access to guidance on how to use the information. For more information, see the section called “Using profile panel guidance”.

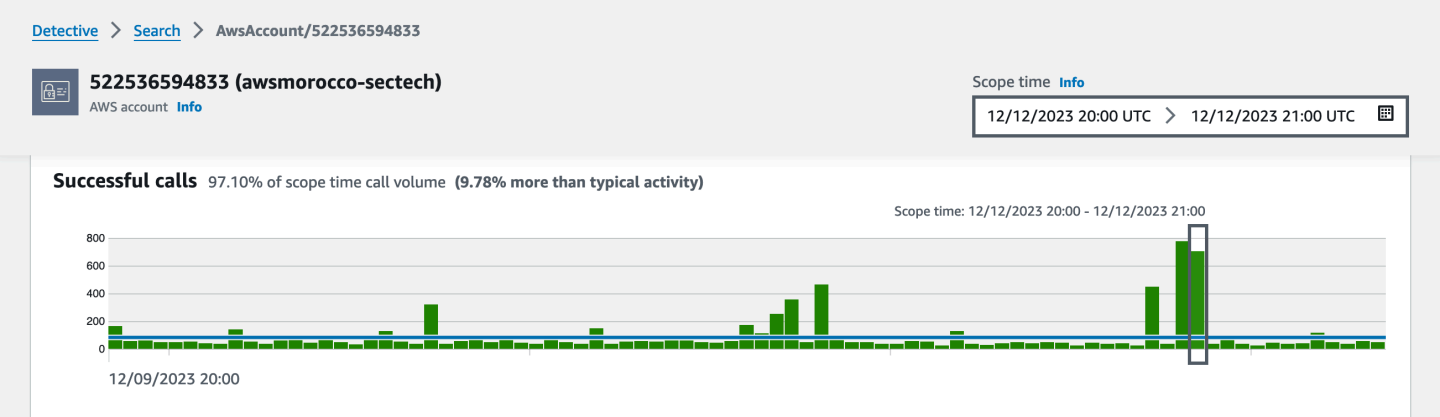
For more details about profile panels, the types of data they contain, and available options for interacting with them, see *Viewing and interacting with profile panels*.

Navigating in a profile

An entity profile contains a set of one or more tabs. Each tab contains one or more profile panels. Each profile panel contains text and visualizations that are generated from the behavior graph data.

As you scroll down through a profile tab, the following information remains visible at the top of the profile:

- Entity type
- Entity identifier
- Scope time



Viewing details for associated findings

Each entity profile contains an associated findings panel that lists the findings that involved the entity during the current scope time. One indication that an entity has been compromised is its involvement in multiple findings. The types of findings can also provide insight into the type of activity to be concerned about.

The associated findings panel is displayed immediately below the entity details profile panel.

For each finding, the table includes the following information:

- The finding title, which is also a link to the finding overview.
- The AWS account associated with the finding, which is also a link to the account profile
- The finding type
- The earliest time that the finding was observed
- The most recent time that the finding was observed
- The finding severity

To display the finding details for a finding, choose the radio button for the finding. Detective populates the finding details panel at the right of the page. Detective also changes the scope time to be the finding time window. This allows you to focus on activity that occurred during that time.

If you navigated to the entity profile from a finding overview, then that finding is selected automatically and the details for the finding are displayed.

From the finding details, to navigate back to the finding overview, choose **See all related entities**.

You can also archive the finding. See *Archiving a GuardDuty finding*.

Analyzing finding groups

Amazon Detective finding groups let you examine multiple activities as they relate to a potential security event. You can analyze the root cause for high severity GuardDuty findings using finding groups. If a threat actor is attempting to compromise your AWS environment, they typically perform a sequence of actions that lead to multiple security findings and unusual behaviors. These actions are often spread across time and entities. When security findings are investigated in isolation, it can lead to a misinterpretation of their significance, and difficulty in finding the root cause. Amazon Detective addresses this problem by applying a graph analysis technique that infers relationships between findings and entities, and groups them together. We recommend treating finding groups as the starting point for investigating the involved entities and findings.

Detective analyzes data from findings and groups them with other findings that are likely to be related based on resources they share. For example, findings related to actions taken by the same IAM role sessions or originating from the same IP address are very likely to be part of the same underlying activity. It's valuable to investigate findings and evidence as a group, even if the associations made by Detective aren't related.

In addition to findings, each group includes entities involved in the findings. The entities can include resources outside of AWS such as IP Addresses or user agents.

> **Note**
>
> After an initial GuardDuty finding occurs that is related to another finding, the finding group with all related findings and all involved entities is created within 48 hours.

Understanding the finding groups page

The finding groups page lists all the finding groups collected by Amazon Detective from your behavior graph. take note of the following attributes of finding groups:

Severity of a group

Each finding group is assigned a severity based on the AWS Security Finding Format (ASFF) severity of the associated findings. ASFF finding severity values are **Critical**, **High**, **Medium**, **Low**, or **Informational** from most to least severe. The severity of a grouping is equal to the highest severity finding among the findings in that grouping.

Groups that consist of **Critical** or **High** severity findings that impact a large number of entities should be prioritized for investigations, as they are more likely to represent high-impact security issues.

Group title

In the **Title** column, each group has a unique ID and a non-unique title. These are based on the ASFF type namespace for the group and the number of findings within that namespace in the cluster. For example, if a grouping has the title: Group with: **TTP (2), Effect (1), and Unusual behavior (2)** it includes five total findings consisting of two findings in the **TTP** namespace, one finding in the **Effect** namespace, and two findings in the **Unusual Behavior** namespace. For a complete list of namespaces, see Types taxonomy for ASFF.

Tactics in a group

The **Tactics** column in a group details which tactics category the activity falls into. The tactics, techniques, and procedures categories in the following list align to the MITRE ATT&CK matrix.

You can select a tactic on the chain to see a description of the tactic and which findings within the group are within that category. Following the chain is a list of the tactics detected within the group. These categories and the activities they typically represent are as follows:

- **Initial Access** – An adversary is trying to get into someone else's network.
- **Execution** – An adversary is trying to get into someone else's network.
- **Persistence** – An adversary is trying to maintain their foothold.
- **Privilege Escalation** – An adversary is trying to gain higher-level permissions.
- **Defense Evasion** – An adversary is trying to avoid being detected.
- **Credential Access** – An adversary is trying to steal account names and passwords.
- **Discovery** – An adversary is trying to understand and learn about an environment.
- **Lateral Movement** – An adversary is trying to move through an environment.
- **Collection** – An adversary is trying to gather data of interest to their goal.
- **Command and Control** – An adversary is trying to get into someone else's network.
- **Exfiltration** – An adversary is trying to steal data.
- **Impact** – An adversary is trying to manipulate, interrupt, or destroy your systems and data.
- **Other** – Indicates activity from a finding that does not align with tactics listed in the matrix.

Entities within a group

The **Entities** column contains details on the specific entities detected within this grouping. Select this value for a breakdown of entities based on the categories: **Identity**, **Network**, **Storage**, and **Compute**. Examples of entities in each category are:

- **Identity** – IAM principals and AWS accounts, such as user and role
- **Network** – IP address or other networking and VPC entities
- **Storage** – Amazon S3 buckets or DDBs
- **Compute** Amazon EC2 instances or Kubernetes containers

Accounts within a group

The **Accounts** column tells you what AWS accounts own entities involved with the findings in the group. The AWS Accounts are listed by name and AWS ID so you can prioritize investigations of activity involving critical accounts.

Findings within a group

The **Findings** column has a lists the entities within a group by severity. The findings include Amazon GuardDuty findings, Amazon Inspector findings, AWS security findings, and evidence from Detective. You can select the graph to see an exact count of findings by severity.

GuardDuty findings are part of the Detective core package and are ingested by default. All other AWS security findings that are aggregated by Security Hub are ingested as an optional data source. See Source data used in a behavior graph for more details.

Informational findings in finding groups

Amazon Detective identifies additional information related to a finding group based on data in your behavior graph collected within the last 45 days. Detective presents this information as a finding with the **Informational** severity. Evidence provides supporting information that highlights an unusual activity or unknown behavior that is potentially suspicious when viewed within a finding group. This might include newly observed geolocations or API calls observed within the scope time of a finding. Evidence findings are only viewable in Detective and are not sent to AWS Security Hub.

Detective determines the location of requests using MaxMind GeoIP databases. MaxMind reports very high accuracy of their data at the country level, although accuracy varies according to factors

such as country and type of IP. For more information about MaxMind, see MaxMind IP Geolocation. If you think any of the GeoIP data is incorrect, you can submit a correction request to Maxmind at MaxMind Correct GeoIP2 Data.

You can observe evidence for different principal types (such as IAM user or IAM role). For some evidence types, you can observe evidence for **all accounts**. This means evidences affect your entire behavior graph. If an evidence finding is observed for all accounts, you will also see at least one additional informational evidence finding of the same type for an individual IAM role. For example, if you see a **New geolocation observed for all accounts** finding, you will see another for **New geolocation observed for a principal**.

Types of evidence in finding groups

- New geolocation observed
- New Autonomous System Organization (ASO) observed
- New user agent observed
- New API call issued
- New geolocation observed for all accounts
- New IAM principal observed for all accounts

Finding group profiles

When you select a group title, a finding group profile opens with additional details about that group. The details panel in the finding groups profile page supports the display of up to 1000 entities and findings for finding groups parent and children.

The group profile page displays the set **Scope time** of the group. This is the date and time from the earliest finding or evidence included in the group to the most recently updated finding or evidence in a group. You can also see the **Finding group severity**, which is equal to the highest severity category among findings in the group. Other details within this profile panel include:

- The **Involved tactics** chain shows you which tactics, are attributed to the findings in the group. Tactics are based on the MITRE ATT&CK Matrix for Enterprise. The tactics are shown as a chain of colored dots that represents the typical progression of an attack from the earliest to latest stages. This means the leftmost circles on the chain typically represent less severe activities where an adversary is trying to gain or maintain access your environment. Conversely, activities toward the right are the most severe and can include data tampering or destruction.

- The relationships that this group has with other groups. Occasionally, one or more previously unconnected groups of findings could be merged into a new group based on a newly discovered link, for example, a finding that involves entities from the existing groups. In this case, Amazon Detective deactivates the parent groups and creates a child group. You can trace the lineage for any group back to its parent groups. Groups can have the following relationships:
  - **Child finding group** – A finding group created when a finding involved in two other finding groups is involved in a new finding. The parent groups of the finding are listed for any child group.
  - **Parent finding group** – A finding group is a parent when a child group has been created from it. If a finding group is a parent, the related children are listed with it. A parent group's status becomes **Inactive** when it's merged into an **Active** child group.

There are two information tabs that open profile panels. Using the **Involved entities** and **Involved findings** tabs, you can view further details about the group.

Use **Run investigation** to generate an investigation report. The generated report details anomalous behavior that indicates compromise. For more details about Detective investigations, see *Detective investigations*.

Profile panels within groups

Involved entities

Focuses on the entities in the finding group, including what findings within the group each entity is linked to. The tags attached to each entity are also displayed so you can quickly identify important entities based on tagging. Select an entity to view its entity profile.

Involved findings

Has details about each finding, including finding severity, each entity involved, and when that finding was first and last seen. Select a finding type in the list to open a finding details panel with additional information about that finding. As part of the **Involved findings** panel, you may see **Informational** findings based on Detective evidence from your behavior graph.

Finding group visualization

Amazon Detective provides an interactive visualization of finding groups. This visualization is designed to help you investigate issues faster and more thoroughly with less effort. The finding

group **Visualization** panel displays the findings and entities involved in a finding group. You can use this interactive visualization to analyze, understand, and triage the impact of the finding group. This panel helps visualize the information presented in the **Involved entities** and **Involved findings** table. From the visual presentation, you can select findings or entities for further analysis.

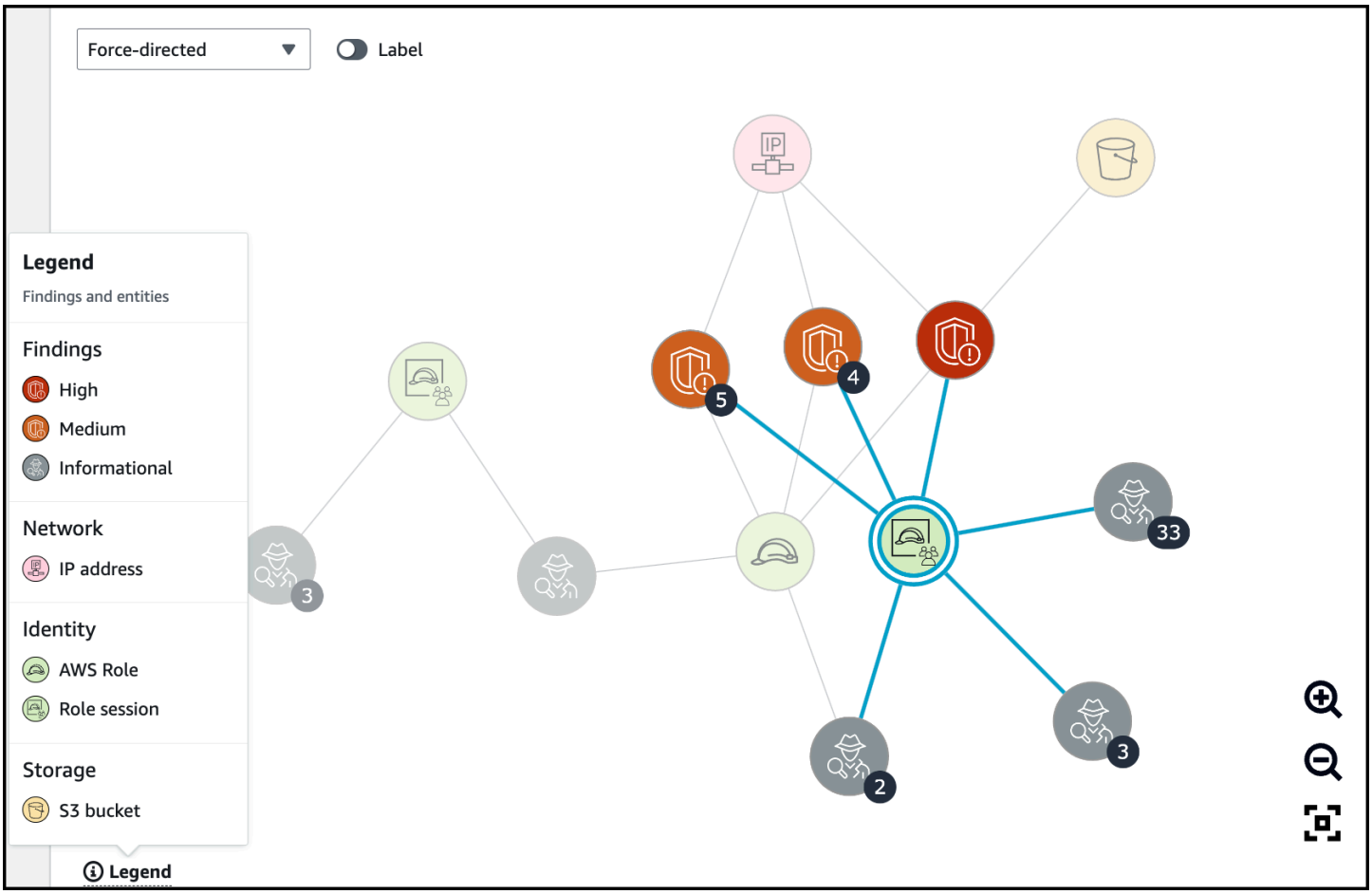
Detective finding groups with aggregated findings are a cluster of findings that are connected to the same type of resource. With aggregated findings, you can quickly assess the makeup of a finding group and interpret security issues faster. In the finding groups details panel, similar findings are combined and you can expand the findings to view relatively similar findings together. For example, an evidence node, which has informational findings and medium findings of the same type are aggregated. Currently, you can view the title, source, type, and severity of finding groups with aggregated findings.

From this interactive panel, you can:

- Use **Run investigation** to generate an investigation report. The generated report details anomalous behavior that indicates compromise. For more details about Detective investigations, see *Detective investigations*.
- View more details on finding groups with aggregated findings to analyze the involved evidence, entities, and findings.
- View the labels for the entities and findings to identify the affected entities with potential security issues. You can toggle off the **Label**.
- Rearrange the entities and findings to better understand their interconnectedness. Isolate entities and findings from a group by moving the selected item in the finding group.
- Select the evidences, entities, and findings to view more details about them. To select multiple items, choose **`command/control`** and either choose the items, or drag and drop them using your pointer.
- Adjust the layout to fit all entities and findings into the finding group window. View what entity types are prevalent in a finding group.

> **Note**
>
> The finding group **Visualization** panel supports the display of finding groups with up to 100 entities and findings.

You can choose **Select layout** to view the findings and entities in a **Circle**, **Force-directed**, or **Grid** layout. The **Force-directed** layout positions the entities and findings so that links are a consistent length between items and the links are distributed evenly. This helps to reduce overlapping. The layout that you select defines the placement of findings in the **Visualization** panel.



The dynamic **Legend** changes based on the entities and findings in your current graph. It helps you identify what each visual element represents.

Finding group summary powered by generative AI

By default, Amazon Detective automatically provides summaries of an individual finding group. The summaries are powered by generative artificial intelligence (generative AI) models hosted on Amazon Bedrock.

By using finding groups, you can examine multiple security findings, as they relate to a potential security event, and identify potential threat actors. Finding group summaries for finding groups builds upon these capabilities. Finding group summaries consume the data for a finding group,

rapidly analyze relationships between the findings and affected resources, and then summarize potential threats in natural language. You can leverage these summaries to identify larger security threats, improve investigation efficiency, and shorten the response timelines.

> **Note**
>
> Finding group summaries powered by generative AI may and not always provide completely accurate information. See AWS Responsible AI Policy for more information.

Reviewing finding group summary

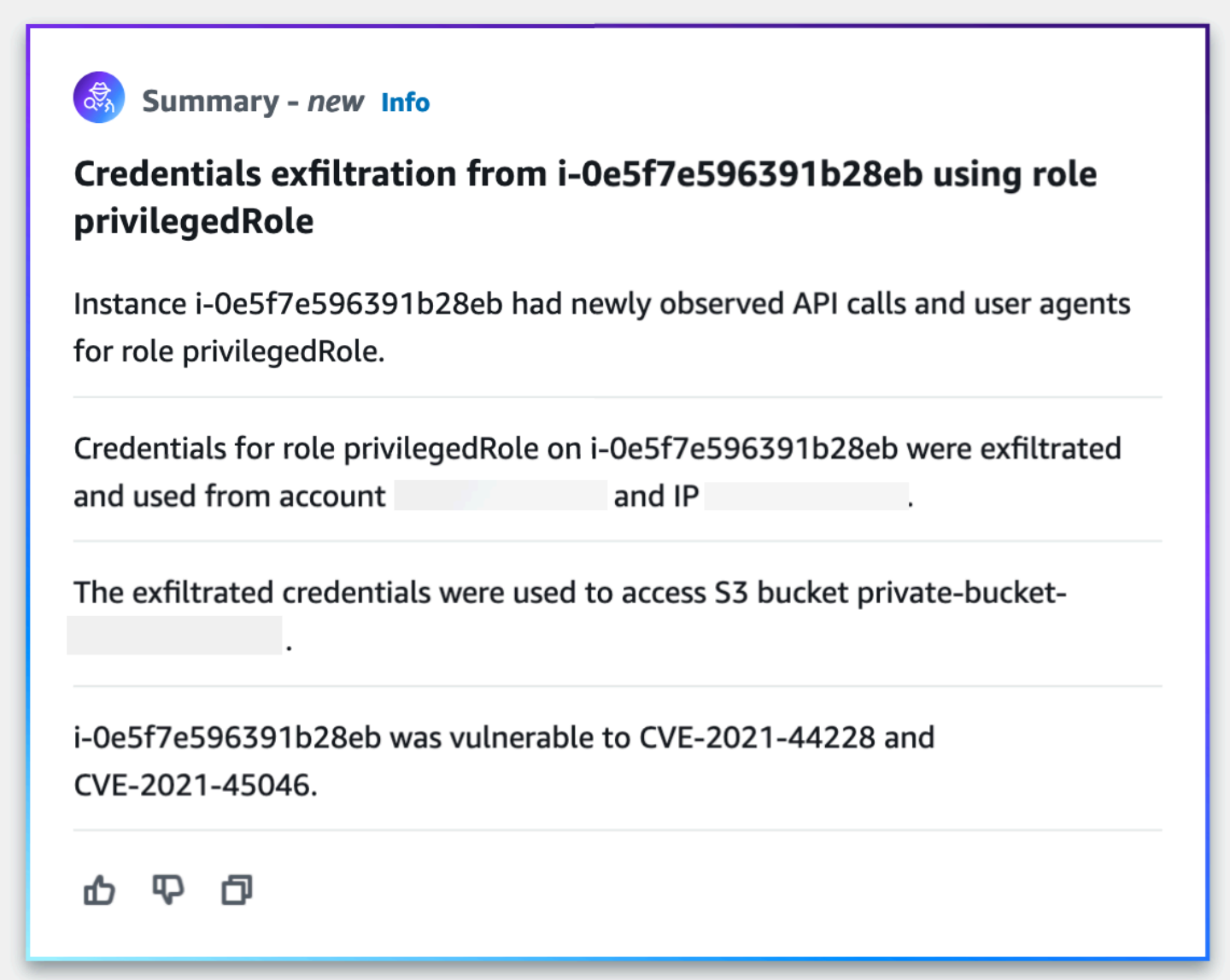
The finding group summary for a finding group gives you a clear, detailed explanation of a security event. In natural language, the explanation includes a succinct title, a summary of the resources involved, and curated information about those resources.

To review a finding group summary

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Finding groups**.
3. In the **Finding groups** table, choose the finding group that you want to display a summary of. A details page appears.

On the details page, you can use the **Summary** pane to review a generated, descriptive summary of the top findings in the finding group. You can also review an analysis of the top threat events in the finding group, which you can then investigate further. To add the generated summary to your notes or a ticketing system, choose the copy icon in the pane. This copies the summary to your clipboard. You can also share your feedback about the finding group summary output in the summary, which can provide a better experience in the future. To share your feedback, choose the thumbs up or thumbs down icon, depending on the nature of your feedback.

> **Note**
>
> If you provide feedback about the finding group summary, your feedback is not used for model tuning. We use it only to help facilitate that the prompts in Detective are crafted effectively.



Disabling finding group summary

By default, finding group summary is enabled for finding groups. You can disable finding group summary at any time. If you disable, you can enable them again later.

To disable finding group summary

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Preferences**.
3. Under **Finding group summary**, choose **Edit**.
4. Turn off **Enabled**.

5. Choose **Save**.

Enabling finding group summary

If you previously disabled finding group summary for finding groups, you can enable them again at any time.

To enable finding group summary

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Preferences**.
3. Under **Finding group summary**, choose **Edit**.
4. Turn on **Enabled**.
5. Choose **Save**.

Supported Regions

Finding group summary is available in the following AWS Regions.

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Tokyo)
- Europe (Frankfurt)

Integration with Amazon Security Lake

Amazon Security Lake is a fully managed security data lake service. You can use Security Lake to automatically centralize security data from AWS environments, SaaS providers, on-premises sources, cloud sources, and third-party sources into a purpose-built data lake that's stored in your AWS account. Security Lake helps you analyze security data, so you can get a more complete understanding of your security posture across your entire organization. With Security Lake, you can also improve the protection of your workloads, applications, and data.

Amazon Detective integrates with Amazon Security Lake, which means that you can query and retrieve the raw log data stored by Security Lake.

Using this integration, you can collect logs and events from the following sources which Security Lake natively supports.

- AWS CloudTrail management events version 1.0
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs version 1.0

For details on how Security Lake automatically converts logs and events that come from natively-supported AWS services to the OCSF schema, see the Amazon Security Lake User Guide.

After you integrate Detective with Security Lake, Detective begins pulling raw logs from Security Lake related to AWS CloudTrail management events and Amazon VPC Flow Logs. For more details, see Querying raw logs.

To integrate Detective with Security Lake, complete the following steps:

1. Before you begin

   Use an Organizations management account to designate a delegated Security Lake administrator for your organization. Make sure that Security Lake is enabled and verify that Security Lake is collecting logs and events from AWS CloudTrail management events and Amazon Virtual Private Cloud (Amazon VPC) Flow Logs.

   In alignment with the Security Reference Architecture, Detective recommends using a Log Archive account and defer from using a Security Tooling account for the Security Lake deployment.
2. Create a Security Lake subscriber

To consume logs and events from Amazon Security Lake, you must be a Security Lake subscriber. Follow these steps to grant query access to a Detective account administrator.

3. Add the required AWS Identity and Access Management (IAM) permissions to your IAM identity.
   - Add these permissions to create Detective integration with Security Lake:
     - Attach these AWS Identity and Access Management (IAM) permissions to your IAM identity. For details, see the Add the required IAM permissions to your account section.
     - Add this IAM policy to the IAM principal that you plan to use to pass the AWS CloudFormation service role. For more details, see the Add permissions to your IAM principal section.
   - If you have already integrated Detective with Security Lake, to use the integration attach these (IAM) permissions to your IAM identity. For details, see the Add the required IAM permissions to your account section.
4. Accept the Resource Share ARN invitation and enable the integration

Use the AWS CloudFormation template to set up the parameters required to create and manage query access for Security Lake subscribers. For the detailed steps to create a stack, see Create a stack using the AWS CloudFormation template. After you finish creating the stack, enable the integration.

For a demonstration of how to integrate Amazon Detective with Amazon Security Lake using the Detective console, watch the following video: Amazon Detective integration with Amazon Security Lake- How to Setup-->

Before you begin

Security Lake integrates with AWS Organizations to manage log collection across multiple accounts in an organization. To use Security Lake for an organization, your AWS Organizations management account must first designate a delegated Security Lake administrator for your organization. The delegated Security Lake administrator must then enable Security Lake, and enable log and event collection for member accounts in the organization.

Before you integrate Security Lake, with Detective, make sure that Security Lake is enabled for the Security Lake administrator account. For the detailed steps on how to enable Security Lake, see Getting Started in the Amazon Security Lake User Guide.

Also, verify that Security Lake is collecting logs and events from AWS CloudTrail management events and Amazon Virtual Private Cloud (Amazon VPC) Flow Logs. For more details about log collection in Security Lake, see Collecting data from AWS services in the Amazon Security Lake User Guide.

Step 1: Create a Security Lake subscriber

To consume logs and events from Amazon Security Lake, you must be a Security Lake subscriber. A Subscriber can query and access the data that Security Lake collects. A subscriber with query access can query AWS Lake Formation tables directly in an Amazon Simple Storage Service (Amazon S3) bucket by using services such as Amazon Athena. To become a subscriber, the Security Lake administrator has to provide you with subscriber access that lets you query the data lake. For information about how the administrator does this, see Creating a subscriber with query access in the Amazon Security Lake User Guide.

Follow these steps to grant query access to a Detective account administrator.

To create a Detective subscriber in Security Lake

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Integrations**.
3. In the Security Lake subscriber pane, note the **Account ID** and **External ID** values.

   Ask the Security Lake administrator to use these IDs to:

   - To create a Detective subscriber for you in Security Lake.
   - To configure the subscriber to have query access.
   - To make sure that the Security Lake query subscriber is created with Lake Formation permissions, select **Lake Formation** as the **Data Access Method** in the Security Lake console.

   When the Security Lake administrator creates a subscriber for you, Security Lake generates an Amazon Resource Share ARN for you. Ask the administrator to send this ARN to you.
4. Enter the **Resource Share ARN** that is provided by the Security Lake administrator in the **Security Lake subscriber** pane.
5. After you receive the Resource Share ARN from the Security Lake Administrator, enter the ARN in the **Resource Share ARN** box in the **Security Lake subscriber** pane.

Step 2: Add the required IAM permissions to your account

To enable Detective integration with Security Lake, you must attach the following AWS Identity and Access Management (IAM) permissions policy to your IAM identity.

Attach the following inline policies to the role. Replace `athena-results-bucket` with your Amazon S3 bucket name if you want to use your own Amazon S3 bucket to store the Athena query results. If you want Detective to automatically generate an Amazon S3 bucket to store the Athena query result, remove the entire `S3ObjectPermissions` from the IAM policy.

If you do not have the required permissions to attach this policy to your IAM identity, contact your AWS administrator. If you have the required permissions but an issue occurs, see Troubleshooting general IAM issues in the IAM User Guide.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
```

```
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "lakeformation:GetDataAccess"
      ],
      "Resource": "*"
    },
    {
       "Effect": "Allow",
        "Action": [
          "ssm:GetParametersByPath"
        ],
        "Resource": [
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/ResourceShareArn",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/S3Bucket",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/TableNames",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/DatabaseName",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/StackId"
        ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "iam:ListRoles"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "securitylake.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Step 3: Accept the Resource Share ARN invitation and enable the integration

To access raw data logs from Security Lake, you must accept a Resource Share invitation from the Security Lake account that was created by the Security Lake administrator. You also need AWS Lake Formation permissions to set up cross-account table sharing. In addition, you must create an Amazon Simple Storage Service (Amazon S3) bucket that can receive raw query logs.

In this next step, you'll use an AWS CloudFormation template to create a stack for: accepting the Resource Share ARN invitation, create required AWS Glue crawler resources, and grant AWS Lake Formation administrator permissions.

To create an AWS CloudFormation stack

1. Create a new CloudFormation stack using the CloudFormation template. For more details, see Creating a stack using the AWS CloudFormation template.
2. After you finish creating the stack, choose **Enable integration**.

Creating a stack using the AWS CloudFormation template

Detective provides an AWS CloudFormation template, which you can use to set up the parameters required to create and manage query access for Security Lake subscribers.

Step 1: Create an AWS CloudFormation service role

You must create an AWS CloudFormation service role to create a stack using the AWS CloudFormation template. If you do not have the required permissions to create a service role, contact the administrator of the Detective administrator account. For more information about the AWS CloudFormation service role, see AWS CloudFormation service role.

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the IAM console, choose **Roles**, and then choose **Create role**.
3. For **Select trusted entity**, choose **AWS service**.
4. Choose **AWS CloudFormation**. Then, choose **Next**.
5. Enter a name for the role. For example, `CFN-DetectiveSecurityLakeIntegration`.
6. Attach the following inline policies to the role. Replace `<Account ID>` with your AWS Account ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudFormationPermission",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:aws:transform/*"
            ]
        },
        {
            "Sid": "IamPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
```

```
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:PassRole",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::<ACCOUNT ID>:role/*",
                "arn:aws:iam::<ACCOUNT ID>:policy/*"
            ]
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "LambdaPermissions",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:TagResource",
                "lambda:InvokeFunction"
            ],
            "Resource": [
```

```
                "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
            ]
        },
        {
            "Sid": "CloudwatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        },
        {
            "Sid": "KmsPermission",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
        }
    ]
}
```

Step 2: Add permissions to your IAM principal.

You'll need the following permissions to create a stack using the CloudFormation service role that you created in the preceding step. Add the following IAM policy to the IAM principal that you plan to use to pass the CloudFormation service role. You will assume this IAM principal to create the stack. If you do not have the required permissions to add the IAM policy, contact the administrator of the Detective administrator account.

> **Note**
>
> In the following policy, `CFN-DetectiveSecurityLakeIntegration` used in this policy refers to the role that you created in the previous `Creating an AWS CloudFormation` service role step. Change it to the role name that you entered in the preceding step if it's different.

```
 {
    "Version": "2012-10-17",
    "Statement": [
        {
             "Sid": "PassRole",
             "Effect": "Allow",
             "Action":
             [
                "iam:GetRole",
                "iam:PassRole"
             ],
             "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
        },
        {
            "Sid": "RestrictCloudFormationAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:UpdateStack"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
            "Condition": {
                "StringEquals": {
                    "cloudformation:RoleArn": [
                        "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
                    ]
                }
            }
        },
        {
            "Sid": "CloudformationDescribeStack",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:GetStackPolicy"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
        },
        {
```

```
            "Sid": "CloudformationListStacks",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        }
    ]
}
```

Step 3: Specify custom values in the AWS CloudFormation console

1. Go to the AWS CloudFormation console from Detective.
2. (Optional) Enter a **Stack name**. The stack name is auto-filled. You can change the stack name to a name that does not conflict with existing stack names.
3. Enter the following **Parameters**.

   - **AthenaResultsBucket** – If you don't enter values, this template generates an Amazon S3 bucket. If you want to use your own bucket, enter a bucket name to store the Athena query results. If you use your own bucket, make sure that the bucket is in the same Region as the Resource Share ARN. If you use your own bucket, make sure the `LakeFormationPrincipals` you choose have permissions to write objects to and read objects from the bucket. For more details about bucket permissions, see Query results and recent queries in the Amazon Athena User Guide.
   - **DTRegion** – This field is pre-filled. Do not change the values in this field.
   - **LakeFormationPrincipals** – Enter the ARN of the IAM principals (for example, IAM role ARN) that you want to grant access to use the Security Lake integration, separated by commas. These could be your security analysts and security engineers that use Detective.

     You can only use the IAM principals that you previously attached the IAM permissions to in step [`Step 2: Add the required IAM permissions to your account`].

- **ResourceShareARN** – This field is pre-filled. Do not change the values in this field.

4. **Permissions**

   IAM role – Select the role that you created in the `Creating an AWS CloudFormation Service Role` step. Optionally, you can keep it blank if your current IAM role has all the required permissions in the `Creating an AWS CloudFormation Service Role` step.

5. Review and check all the **I Acknowledge** boxes and then click the **Create stack** button. For more details, review the following IAM resources that will be created.

```
* ResourceShareAcceptorCustomResourceFunction
    - ResourceShareAcceptorLambdaRole
    - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
    - SsmParametersLambdaRole
    - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
    - GlueDatabaseLambdaRole
    - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
    - GlueTablesLambdaRole
    - GlueTablesLogsAccessPolicy
```

Step 4: Add Amazon S3 bucket policy to IAM principals in `LakeFormationPrincipals`

(Optional) If you let this template generate an `AthenaResultsBucket` for you, you must attach the following policy to the IAM principals in `LakeFormationPrincipals`.

```
{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

Replace `athena-results-bucket` with the `AthenaResultsBucket` name. The `AthenaResultsBucket` can be found on the AWS CloudFormation console:

1. Open the AWS CloudFormation console at https://console.aws.amazon.com/cloudformation.
2. Click on your Stack.
3. Click the **Resources** tab.
4. Search for the logical ID `AthenaResultsBucket` and copy its physical ID.

Deleting a CloudFormation stack

If you do not delete the existing stack, new stack creation in the same Region will fail. You can delete a CloudFormation stack by using the CloudFormation console or use the AWS CLI.

To delete the AWS CloudFormation stack (Console)

1. Open the AWS CloudFormation console at https://console.aws.amazon.com/cloudformation.
2. On the **Stacks** page in the CloudFormation console, select the stack that you want to delete. The stack must be currently running.
3. In the stack details pane, choose **Delete**.
4. Select **Delete stack** when prompted.

> **Note**
>
> The stack deletion operation can't be stopped once the stack deletion has begun. The stack proceeds to the `DELETE_IN_PROGRESS` state.

After the stack deletion is complete, the stack will be in the `DELETE_COMPLETE` state.

Troubleshooting stack deletion errors

If you are seeing a permission error with the message `Failed to delete stack` after clicking the `Delete` button, your IAM role doesn't have CloudFormation permission to delete a stack. Contact your account administrator to delete the stack.

To delete the CloudFormation stack (AWS CLI)

Enter the following command in the AWS CLI interface:

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
      arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

`CFN-DetectiveSecurityLakeIntegration` is the service role that you created in the `Creating an AWS CloudFormation Service Role` step.

Changing the integration configuration

If you want to change any of the parameters that you used to integrate Detective with Security Lake, you can edit them, and then enable the integration again. You can edit the AWS CloudFormation template to re-enable this integration for the following scenarios:

- To update the Security Lake subscription, you can either create a new subscriber, or the Security Lake administrator can update the data source for the existing subscription.
- To specify a different Amazon S3 bucket to store the raw query logs.
- To specify different Lake Formation principals.

When you re-enable Detective integration with Security Lake, you can edit the **Resource Share ARN**, and view the **IAM permissions**. To edit the IAM permissions, you can go to the IAM console from Detective. You can also edit the values you previously entered in the AWS CloudFormation template. You must delete the existing CloudFormation stack and re-create it to re-enable the integration.

To re-enable Detective integration with Security Lake

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Integrations**.
3. You can edit the integration using either of these steps:
   - In the **Security Lake** pane, choose **Edit**.
   - In the **Security Lake** pane, choose **View**. In the view page, choose **Edit**.
4. Enter a new **Resource Share ARN**, to access the data sources in a Region.
5. View the current IAM permissions, and go to the IAM console, if you want to edit the IAM permissions.
6. Edit the values in the CloudFormation template.

1. Delete the existing stack first, before creating a new stack. If you do not delete the existing stack and you try to create a new stack in the same Region, your request fails. For more details, see Deleting a CloudFormation stack.

1. Create a new CloudFormation stack. For more details, see Creating a stack using the AWS CloudFormation template.

7. Choose **Enable integration**.

Disabling the integration

If you disable Detective integration with Security Lake, you can no longer query log and event data from Security Lake.

To disable Detective integration with Security Lake

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Integrations**.
3. Delete the existing stack. For more details, see Deleting a CloudFormation stack.
4. In the **Disable Security Lake integration** pane, choose **Disable**.

Supported AWS Regions

You can integrate Detective with Security Lake in the following AWS Regions.

Region Name	Region	Endpoint	Protocol;
US East (Ohio)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
US West (N. California)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS

Region Name	Region	Endpoint	Protocol;
US West (Oregon)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Querying raw logs in Detective

After you integrate Detective with Security Lake, Detective begins pulling raw logs from Security Lake related to AWS CloudTrail management events and Amazon Virtual Private Cloud (Amazon VPC) Flow Logs.

> **Note**
>
> There are no additional charges to query raw logs in Detective. Usage charges for other AWS Services, including Amazon Athena, still apply at published rates.

AWS CloudTrail management events are available for the following profiles:

- AWS account
- AWS user
- AWS role
- AWS role Session
- Amazon EC2 instance
- Amazon S3 bucket
- IP address

Amazon VPC FLow Logs are available for the following profiles:

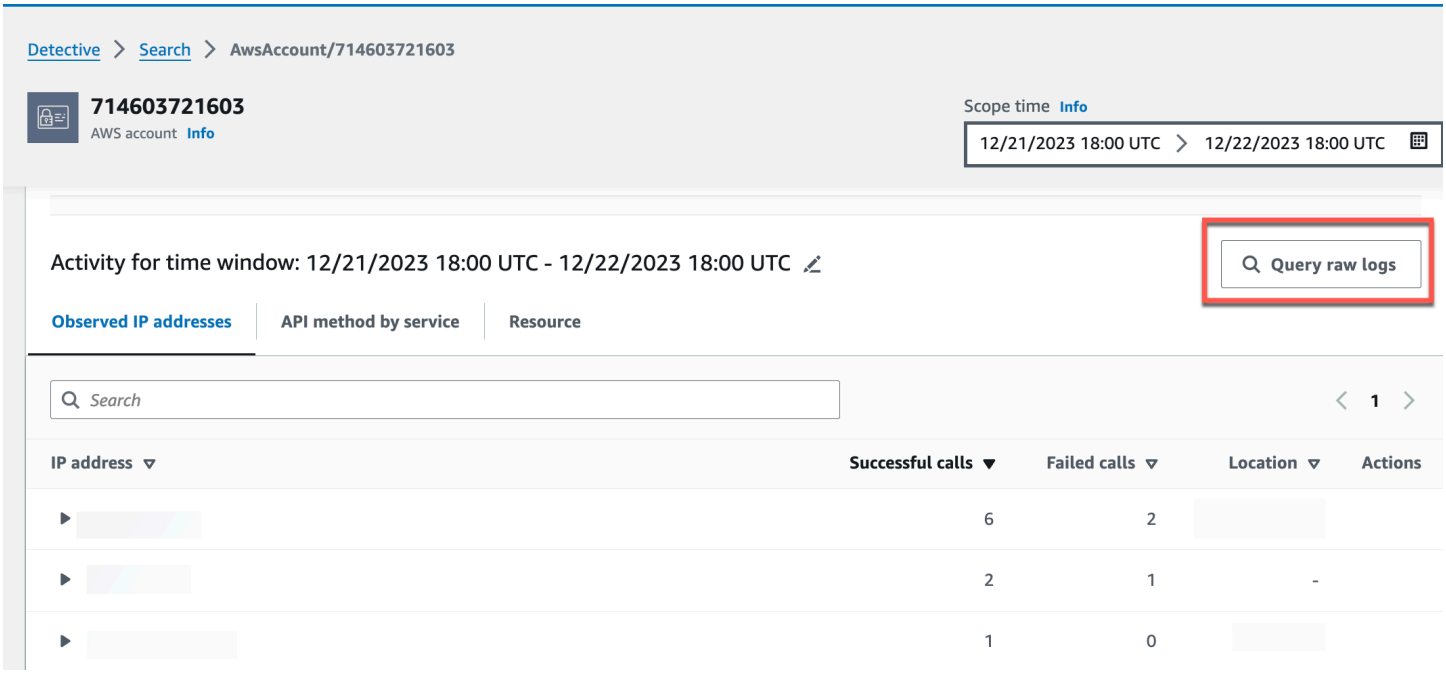
- Amazon EC2 instance
- Kubernetes pod

For a demonstration of how to integrate Amazon Detective with Amazon Security Lake using the Detective console, watch the following video: Amazon Detective integration with Amazon Security Lake- How to Use-->

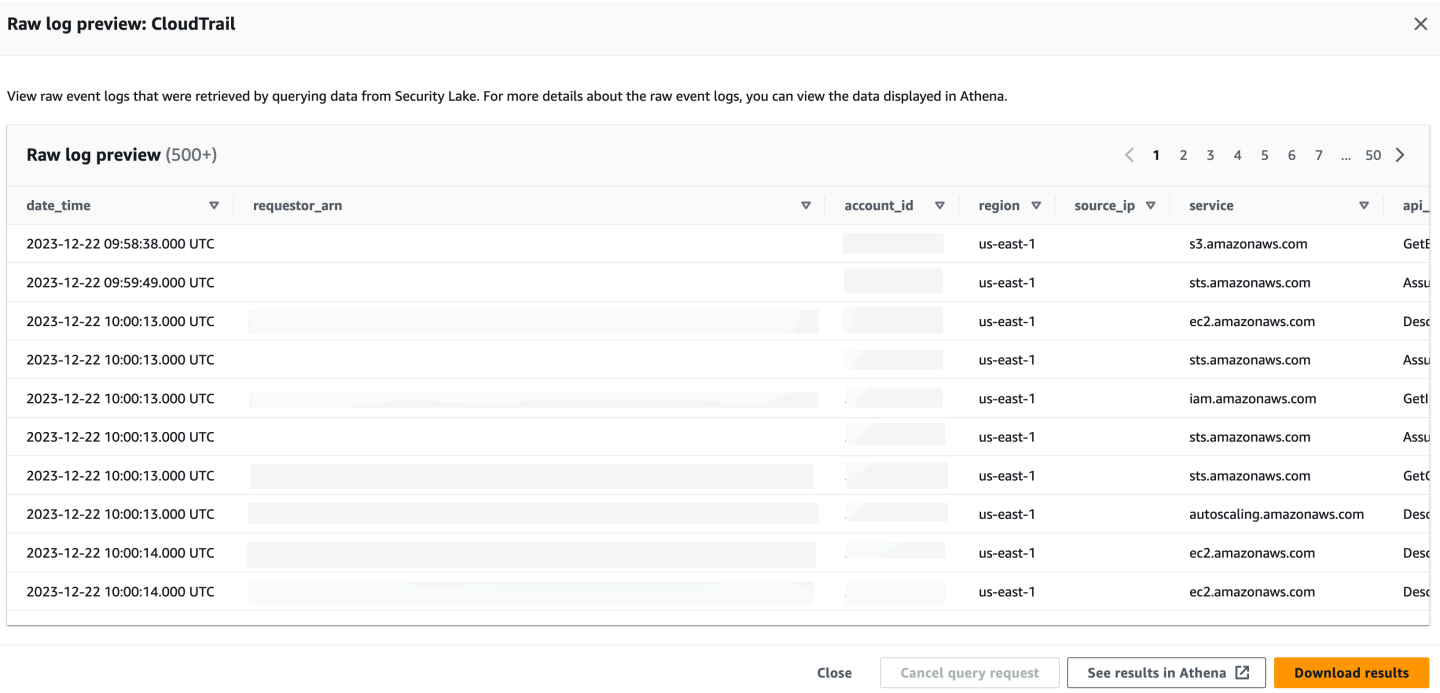
To query raw logs for an AWS account

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Search** and search for an `AWS account`.

3. In the **Overall API call volume** section, choose **display details for scope time**.
4. From here, you can start to **Query raw logs**.



In the **Raw log preview** table, you can view the logs and events retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Amazon Athena.



From the Query raw logs table, you can **Cancel query request**, **See results in Amazon Athena**, and **Download results** as a comma-separated values (.csv) file.

If you see logs in Detective, but the query returned no results, it could happen because of the following reasons.

- Raw logs may become available in Detective before showing up in Security Lake log tables. Try again later.
- Logs may be missing from Security Lake. If you waited for an extended period of time, it indicates that logs are missing from Security Lake. Contact your Security Lake administrator to resolve the issue.

Examples

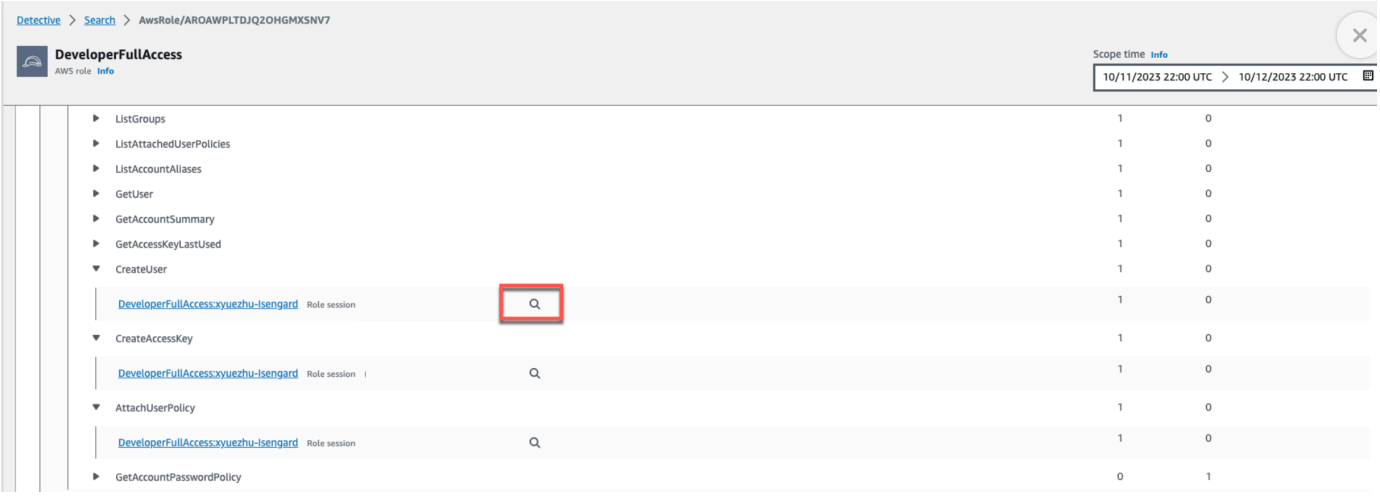
- Query raw logs for an AWS role
- Query raw logs for an Amazon EC2 instance

Query raw logs for an AWS role

If you want to understand the activity of an AWS role in a new geolocation, you can do so within the Detective console.

To query raw logs for an AWS role

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. From the Detective **Summary** page **Newly observed geolocations** section, note down the AWS role.
3. In the navigation pane, choose **Search** and search for the `AWS role`.
4. For the AWS role, expand the resource to display the specific API calls that were issued from that IP address by that resource.
5. Choose the magnifier icon next to the API call that you want to investigate to open the **Raw log preview** table.

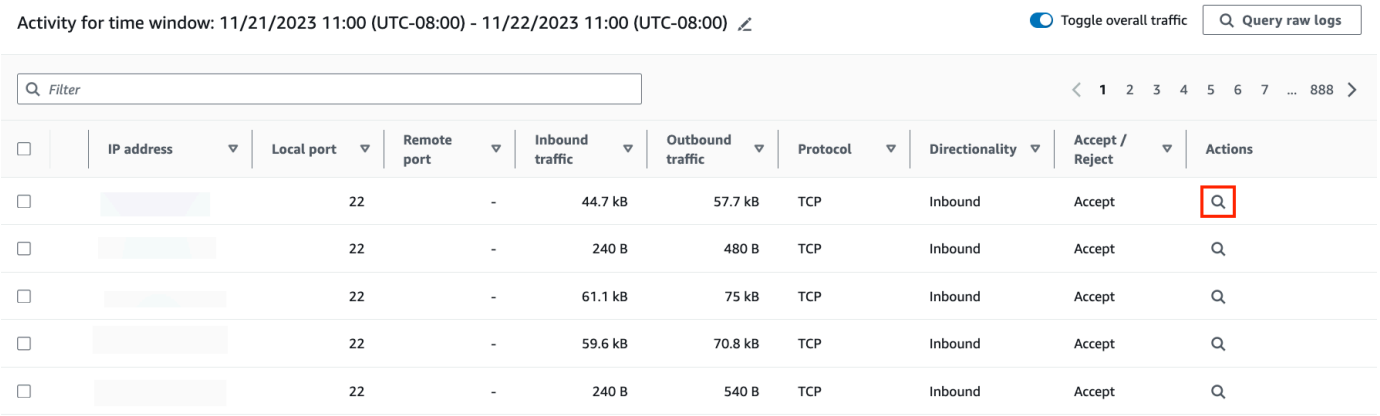


In the **Raw log preview** table, you can view the logs and events retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Amazon Athena.

From the Query raw logs table, you can **Cancel query request**, **See results in Amazon Athena**, and **Download results** as a comma-separated values (.csv) file.

Query raw logs for an Amazon EC2 instance

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Search** and search for an `Amazon EC2 instance`.
3. In the **Overall VPC Flow volume** section, choose the magnifier icon next to the API call that you want to investigate to open the **Raw log preview** table.
4. From here, you can start to **Query raw logs**.



In the **Raw log preview** table, you can view the logs and events retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Amazon Athena.

From the Query raw logs table, you can **Cancel query request**, **See results in Amazon Athena**, and **Download results** as a comma-separated values (.csv) file.

Investigating IAM resources using Detective investigations

You can use the Amazon Detective investigations feature to investigate IAM users and IAM roles using indicators of compromise, which can help you determine if a resource is involved in a security incident. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident. You can maximize efficiency, focus on the security threats, and strengthen incidence response capabilities.

Detective investigations uses machine learning models and threat intelligence to automatically analyze resources in your AWS environment to identify potential security incidents. It lets you proactively, effectively, and efficiently use automation built on top of Detective's behavioral graph to improve security operations. Using Detective investigations you can investigate attack tactics, impossible travel, flagged IP addresses, and finding groups. It performs initial security investigation steps and generates a report highlighting the risks identified by Detective, to help you understand security events and respond to potential incidents.

A severity identified by Detective represents the disposition as analyzed by the investigation of a single resource at a given scope time. A severity reported by an investigation doesn't imply or otherwise indicate the criticality or importance that an affected resource might have for your organization.

Detective investigations can generate up to 500 investigations per month in each AWS Region. If you want to increase the quota, contact AWS support.

Running a Detective investigation

Use **Run investigation** to analyze resources such as IAM users and IAM roles and to generate an investigation report. The generated report details anomalous behavior that indicates potential compromise.

Console

Follow these steps to run a Detective investigation from the **Investigations page** using the Amazon Detective console.

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Investigations**.
3. In the **Investigations** page, choose **Run investigation** in the top right corner.
4. In the **Select resource** section, you have three ways to run an investigation. You can choose to run the investigation for a resource recommended by Detective. You can run the investigation for a specific resource. You can also investigate a resource from the Detective Search page.

    1. `Choose a recommended resource` – Detective recommends resources based on its activity in findings and finding groups. To run the investigation for a resource recommended by Detective, in the **Recommended resources** table, select a resource to investigate.

        The Recommended resources table provides the following details:

        - **Resource ARN** – The Amazon Resource Name (ARN) of the AWS resource.
        - **Reason to investigate** – Displays the key reason(s) to investigate the resource. The reasons for which Detective recommends to investigate a resource are as follows:
            - If a resource was involved in a High Severity finding in the last 24 hours.
            - If a resource was involved in a finding group observed in the last 7 days. Detective finding groups let you examine multiple activities as they relate to a potential security event. For more details, see *Analyzing finding groups*.
            - If a resource was involved in a finding in the last 7 days.
        - **Latest finding** – Latest findings are prioritized on top of the list.
        - **Resource type** – Identifies the type of resource. For example, an AWS user or AWS role.
    2. `Specify an AWS role or user with an ARN` – You can select an AWS role or AWS user and run an investigation for the specific resource.

        Follow these steps to investigate a specific resource type.

        a. From the **Select resource type** drop-down list, choose AWS role or AWS user.

        b. Enter the **Resource ARN** of the IAM resource. For more details about Resource ARNs, see Amazon Resource Names (ARNs) in the IAM User Guide.
    3. `Find a resource to investigate from the Search page` – You can search all of your IAM resources from the Detective **Search** page. For more details about search in Detective, see *Searching for a finding or entity*.

Follow these steps to investigate a resource from the Search page.

a. In the navigation pane, choose **Search**.

b. In the Search page, search for an IAM resource.

c. Navigate to the profile page of the resource and run investigation from there.

5. In the **Investigation scope time** section, choose the **Scope time** for the investigation to assess the selected resource's activity. You can select a **Start date** and **Start time**; and **End date** and **End time** in UTC format. The selected scope time window can be between at a minimum of 3 hours and a maximum of 30 days.
6. Choose **Run investigation**.

API

To run an investigation programmatically, use the StartInvestigation operation of the Detective API. If you're using the AWS Command Line Interface (AWS CLI) run the start-investigation command.

In your request, use these parameters to run an investigation in Detective:

- `GraphArn` – Specify the Amazon Resource Name (ARN) of the behavior graph.
- `EntityArn` – Specify the unique Amazon Resource Name (ARN) of the IAM user and IAM role.
- `ScopeStartTime` – Optionally, specify the data and time from which the investigation should begin. The value is an UTC ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.
- `ScopeEndTime` – Optionally, specify the data and time when the investigation should end. The value is an UTC ISO8601 formatted string. For example, `2021-08-18T16:35:56.284Z`.

This example is formatted for Linux, macOS, or Unix, and it uses the backslash (\) line-continuation character to improve readability.

```
aws detective start-investigation \
--graph-arn arn:aws:detective:us-
east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0
 --entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-
time 2023-09-27T20:00:00.00Z
--scope-end-time 2023-09-28T22:00:00.00Z
```

You can also run an investigation from the following pages in Detective:

- An IAM user or IAM role profile page in Detective.
- Graph visualization pane of a finding group.
- Actions column of an involved resource.
- IAM user or IAM role on a finding page.

After Detective runs the investigation for a resource, an investigation report is generated. To access the report, go to **Investigations** from the navigation pane.

Reviewing investigations reports

Investigations reports lets you review the generated **Reports** for investigations that you have run previously in Detective.

To review investigations reports

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Investigations**.

Take note of the following attributes from an investigations report.

- **ID** – The generated identifier of the investigations report. You can choose this **ID** to read a summary of the investigation report, which has the details of the investigation.
- **Status** – Each investigation is associated with a **Status** based on the completion status of the investigation. Status values can be **In progress**, **Succeeded**, or **Failed**.
- **Severity** – Each investigation is assigned a **Severity**. Detective automatically assigns a severity to the finding.

  A severity represents the disposition as analyzed by the investigation of a single resource at a given scope time. A severity reported by an investigation doesn't imply or otherwise indicate the criticality or importance that an affected resource might have for your organization.

  Investigation severity values can be **Critical**, **High**, **Medium**, **Low**, or **Informational** from most to least severe.

Investigations that are assigned a Critical or High severity value should be prioritized for further inspection, as they are more likely to represent high-impact security issues identified by Detective.

- **Entity** – The **Entity** column contains details on the specific entities detected in the investigation. Some entities are AWS accounts, such as user and role.
- **Status** – The **Creation** date column contains details on the date and time the investigation report was first created.

Understanding an investigations report

An investigations report lists a summary of the uncommon behavior or malicious activity that indicates compromise. It also lists the recommendations that Detective suggests to mitigate the security risk.

To view an investigations report for a specific investigation ID.

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Investigations**.
3. In the **Reports** table, select an investigation **ID**.

Detective generates the report for the selected **Scope** time and **User**. The report contains an **Indicators of Compromise** section that includes details regarding one or more of the indicators of compromise listed below. As you review each indicator of compromise, optionally choose an item to drill down and review its details.

- **Tactics. Techniques, and Procedures** – Identifies tactics, techniques, and procedures (TTPs) used in a potential security event. The MITRE ATT&CK framework is used to understand the TTPs. Tactics are based on the MITRE ATT&CK matrix for Enterprise.
- **Threat Intelligence Flagged IP Addresses** – Suspicious IP addresses are flagged and identified as critical or severe threats based on Detective threat intelligence.
- **Impossible Travel** – Detects and identifies unusual and impossible user activity for an account. For example, this indicator lists a drastic change between source to destination location of a user within a short time span.

- **Related Finding Group** – Shows multiple activities as they relate to a potential security event. Detective uses graph analysis techniques that infers relationships between findings and entities, and groups them together as a finding group.
- **Related Findings** – Related activities associated with a potential security event. Lists all distinct categories of evidence that are connected to the resource or the finding group.
- **New Geolocations** – Identifies new geolocations used either at the resource or account level. For example, this indicator lists an observed geolocation that is an infrequent or unused location based on previous user activity.
- **New User Agents** – Identifies new user agents used either at the resource or account level.
- **New ASOs** – Identifies new Autonomous System Organizations (ASOs) used either at the resource or account level. For example, this indicator lists a new organization assigned as an ASO.

Investigations report summary

Investigations summary highlights anomalous indicators that require attention, for the selected scope time. Using the summary, you can more quickly identify the root cause of potential security issues, identify patterns, and understand the resources impacted by security events.

In the detailed investigations report summary, you can view the following details.

Investigations overview

In the **Overview** panel, you can see a visualization of IPs with high severity activity, which can give more context on the pathway of an attacker.

Detective highlights **Unusual activity** in the investigation, for example impossible travel from a source to a faraway destination by the IAM user.

Detective maps the investigations to tactics, techniques, and procedures (TTPs) used in a potential security event. The MITRE ATT&CK framework is used to understand the TTPs. Tactics are based on the MITRE ATT&CK matrix for Enterprise.

Investigations indicators

You can use the information in the **Indicators** pane, to determine if an AWS resource is involved in unusual activity that could indicate malicious behavior and its impact. An indicator of compromise (IOC) is an artifact observed in or on a network, system, or environment that can (with a high level of confidence) identify malicious activity or a security incident.

Downloading an investigation report

You can download a Detective investigation report in JSON format, to analyze it further or store it to your preferred storage solution such as an Amazon S3 bucket.

To download an investigations report from the Reports table.

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Investigations**.
3. Select an investigation, from the **Reports** table, and choose **Download**.

To download an investigations report from the summary page.

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Investigations**.
3. Select an investigation, from the **Reports** table.
4. In the investigations summary page, choose **Download**.

Archiving an investigation report

When you complete your investigation in Amazon Detective, you can **Archive** the investigation report. An archived investigation indicates you have completed reviewing the investigation.

You can archive or unarchive an investigation only if you are a Detective Administrator. Detective will store your archived investigations for 90 days.

To archive an investigations report from the Reports table.

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Investigations**.
3. Select an investigation, from the **Reports** table, and choose **Archive**.

To archive an investigations report from the summary page.

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Investigations**.
3. Select an investigation, from the **Reports** table.
4. In the investigations summary page, choose **Archive**.

Viewing and interacting with profile panels

Each entity profile on the Amazon Detective console consists of a set of profile panels. A profile panel is a visualization that provides general details or highlights specific activity associated with an entity. Profile panels use different types of visualizations to present different types of information. They can also provide links to additional details or to other profiles.

Each profile panel is intended to help analysts find answers to specific questions about entities and their associated activity. The answers to those questions help lead to a conclusion about whether the activity represents a genuine threat.

Contents

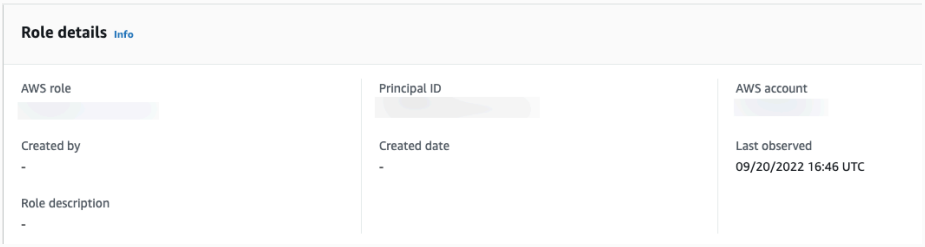
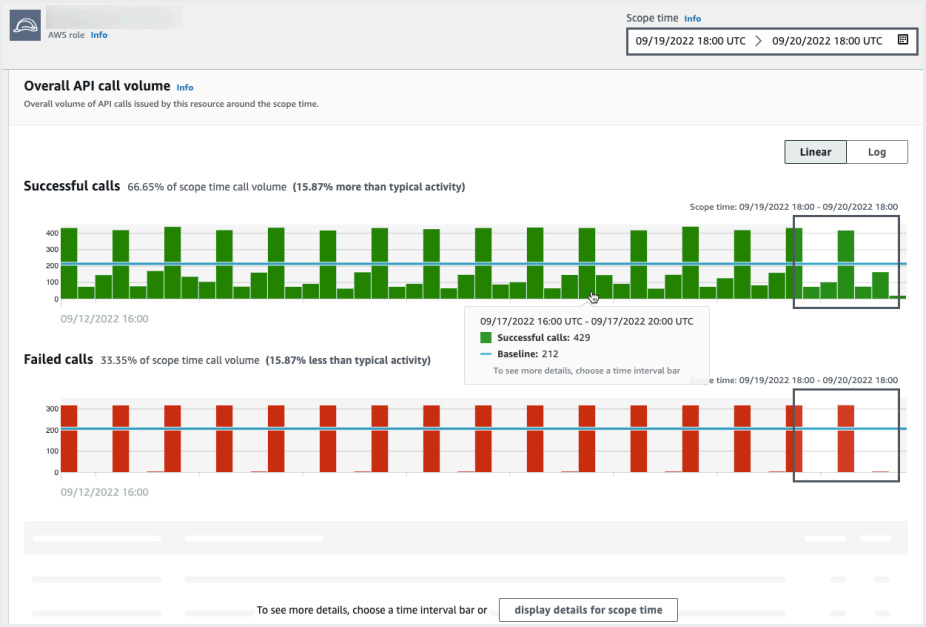
Profile panel content

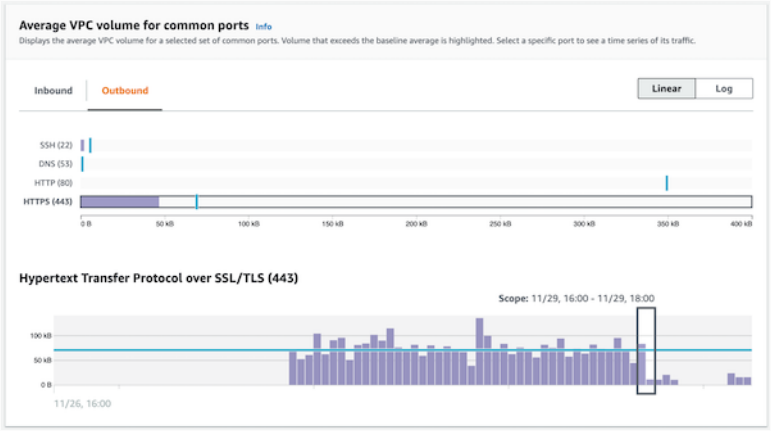
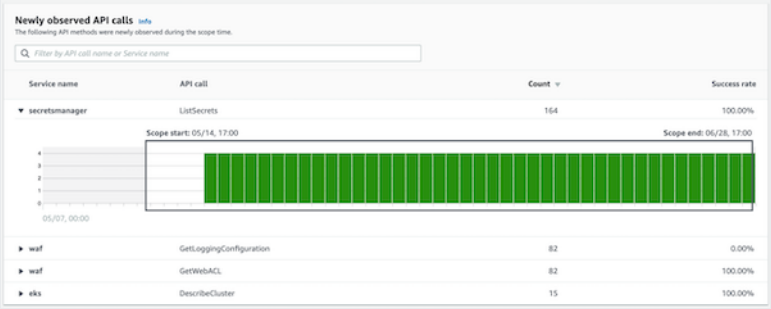
Profile panels use different types of visualizations to present different types of information.

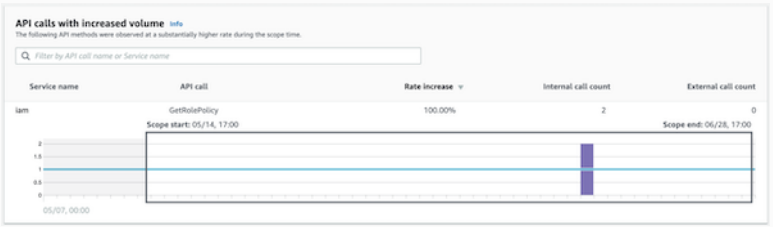
Types of information on a profile panel

Profile panels typically provide the following types of data.

Panel data type	Description
High-level information about a finding or entity	The simplest type of panel provides some basic information about an entity. Examples of information included on an information panel include the identifier, name, type, and creation date.

Panel data type	Description
	 Most entity profiles contain an information panel for that entity.
General summary of activity over time	Displays a summary of activity for an entity over time. This type of panel provides an overall view of how an entity is behaving during the scope time.  Here are some examples of summary data provided on Detective profile panels: • Failed and successful API calls • Inbound and outbound VPC volume

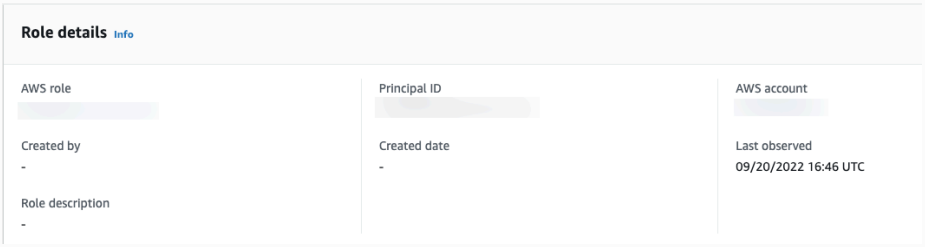
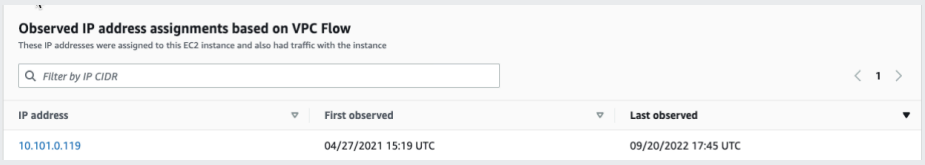
Panel data type	Description
Summary of activity grouped by values	Displays a summary of activity for an entity, grouped by specific values. You can see this type of profile panel on the profile for an EC2 instance. The profile panel shows the average volume of VPC flow log data to and from an EC2 instance for common ports that are associated with specific types of services. 
Activity that only started during the scope time	During an investigation, it is valuable to see what activity only began to occur during a specific time frame. For example, are there API calls, geographic locations, or user agents that were not seen before?  If the behavior graph is still in training mode, the profile panel displays a notification message. The message is removed when the behavior graph has accumulated at least two weeks of data. For more information about training mode, see the section called “Training period for new behavior graphs”.

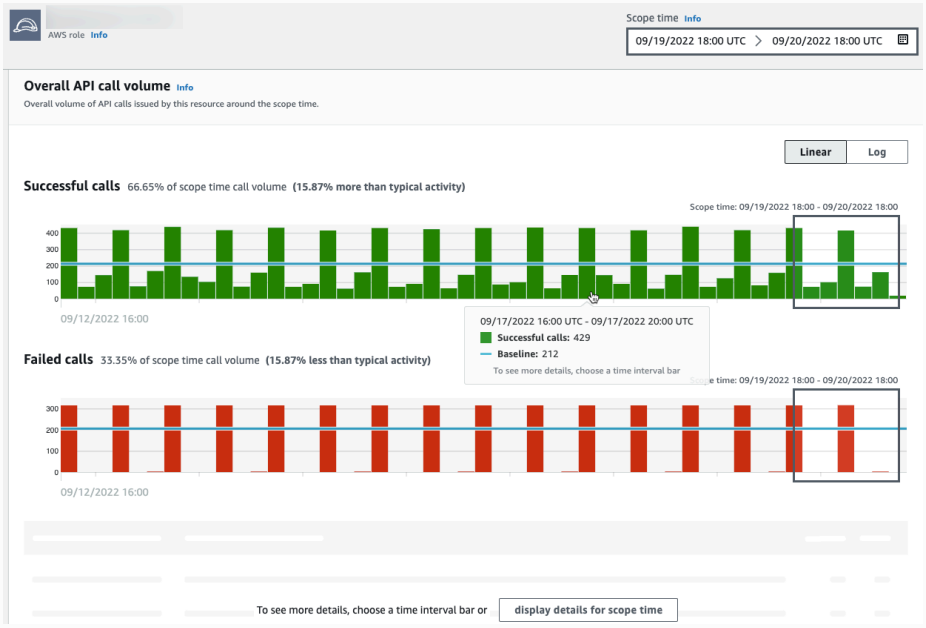
Panel data type	Description
Activity that changed significantly during the scope time	Similar to the new activity panels, profile panels can also display activity that changed significantly during the scope time. For example, a user might regularly issue a certain API call a few times a week. If the same user suddenly issues the same call multiple times in a single day, that might be evidence of malicious activity.  If the behavior graph is still in training mode, the profile panel displays a notification message. The message is removed when the behavior graph has accumulated at least two weeks of data. For more information about training mode, see the section called “Training period for new behavior graphs”.

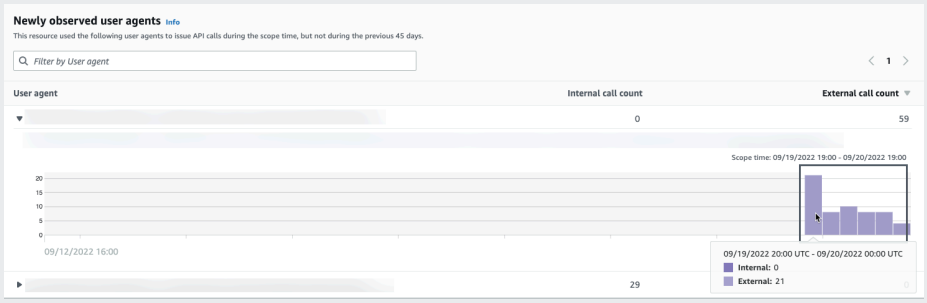
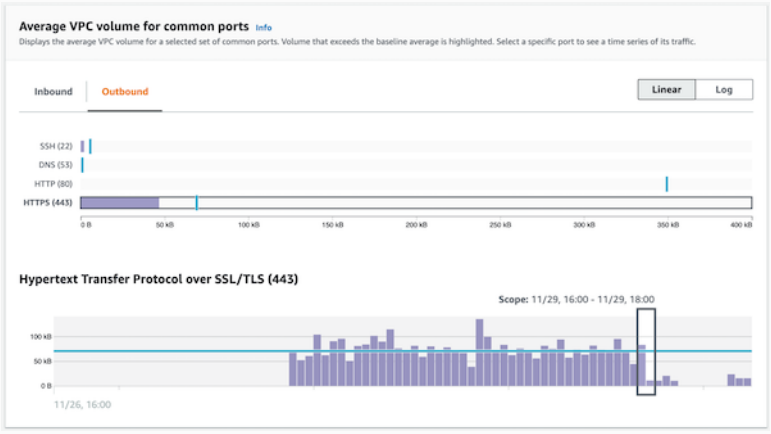
Types of profile panel visualizations

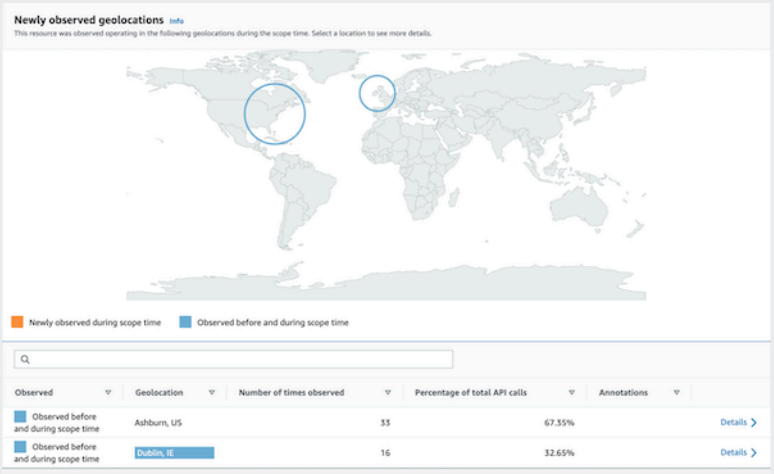
Profile panel content can take one of the following forms.

Visualization type	Description
Key-value pairs	The simplest type of visualization is a set of key-value pairs. A finding or entity information panel is the most common example of a key-value pair panel.

Visualization type	Description
	 Key-value pairs can also be used to add additional information to other types of panels. From a key-value pair panel, if a value is an identifier of an entity, then you can pivot to its profile.
Table	A table is a simple multiple-column list of items.  You can sort, filter, and page through the table. You can change the number of entries to display on each page. See the section called “Preferences for profile panels”. If a value in the table is an identifier of an entity, then you can pivot to its profile.

Visualization type	Description
Timeline	A timeline visualization shows an aggregated value for defined intervals over time.  The timeline highlights the current scope time, and includes additional peripheral time before and after the scope time. The peripheral time provides context for the activity in the scope time. Hover over a time interval to display a summary of the data for that time interval.

Visualization type	Description
Expandable table	An expandable table combines tables and timelines.  The visualization starts as a table. You can sort, filter, and page through the table. You can change the number of entries to display on each page. See the section called “Preferences for profile panels”. You can then expand each row to show a timeline visualization specific to that row.
Bar chart	A bar chart shows values based on groupings. Depending on the chart, you might be able to choose a bar to display a timeline of related activity. 

Visualization type	Description
Geolocation chart	A geolocation chart displays a map that is marked to highlight data based on geographic location. It may be followed by a table containing details about individual geolocations.  Note that when processing incoming geographic data, Detective rounds the latitude and longitude values to a single decimal point.

Other notes on profile panel content

When viewing the content of a profile panel, be aware of the following items:

Approximate count data warning

This warning indicates that items with extremely low counts do not appear due to the volume of applicable data.

To ensure a completely accurate count, reduce the amount of data. The simplest way to do that is to reduce the length of the scope time. See *Managing the scope time*.

Rounding for geographic locations

Detective rounds all latitude and longitude values to a single decimal point.

Changes to how Detective represents API calls

Beginning on July 14, 2021, Detective tracks the service that made each API call. Whenever Detective displays an API method, it also displays the associated service. On profile panels that

display information about API calls, the calls are always grouped by the service. For data that Detective ingested before that date, the service name is listed as **Unknown service**.

Also beginning on July 14, 2021, for accounts and roles, the activity details for the **Overall API call volume** profile panel no longer show the AKID of the resource that issued the call. For accounts, Detective displays the identifier of the principal (user or role) that issued the call. For roles, Detective displays the identifier of the role session. For data that Detective ingested before July 14, 2021, the identifier is listed as **Unknown resource**.

For profile panels that display a list of API calls, the associated timeline highlights the period of time during which this transition occurred. The highlight starts on July 14, 2021, and ends when the update was fully propagated in Detective.

Setting the preferences for a profile panel

In the Detective console, you can set the **Table length** and the **Timestamp** display on the **Preferences** page.

Setting the table length

For profile panels that contain tables or expandable tables, you can configure the number of rows to display on each page.

Set your preference for the number of entries on each page.

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, under **Settings**, choose **Preferences**.
3. On the **Preferences** page, under **Table length**, click **Edit**.
4. Choose the number of table rows you want to display on each page.
5. Choose **Save**.

Setting the timestamp format

For profile panels, you can configure the timestamp format preference that will be applied to all timestamps for each IAM user or IAM role in Detective.

> **Note**
>
> The timestamp format preference is not applied across the entire AWS account.

Set the preference for timestamp.

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, under **Settings**, choose **Preferences**.
3. On the **Preferences** page, under **Timestamp preferences**, view and change the preferred display for all timestamps.
4. By default, the timestamp format is set to UTC. Click **Edit** to choose your local timezone.

   Example:

   Example

   UTC - 09/20/22 16:39 UTC

   Local - 09/20/2022 9:39 (UTC-07:00)
5. Choose **Save**.

Pivoting from a profile panel to another console

For EC2 instances, IAM users, and IAM roles, you can navigate directly from the details profile panel to the corresponding console. The information available from the console can provide additional input for your investigation.

On the **EC2 instance details** profile panel, the EC2 instance identifier is linked to the Amazon EC2 console.

On the **User details** profile panel, the user name is linked to the IAM console.

On the **Role details** profile panel, the role name is linked to the IAM console.

Pivoting from a profile panel to another entity profile

When a profile panel contains an identifier of a different entity, it is usually a link to that entity profile. The exceptions are the links to the Amazon EC2 and IAM consoles on the EC2 instance, IAM users, and IAM roles profiles. See the section called “Pivoting to another console”.

For example, from a list of IP addresses, you might be able to display the profile for a specific IP address. That way you can see if there is any other information available to help you to complete your investigation.

Exploring activity details on a profile panel

During an investigation, you might want to investigate further into the pattern of activity for an entity.

On the following profile panels, you can display a summary of the activity details:

- **Overall API call volume**, except for the profile panel on the user agent profile
- **Newly observed geolocations**
- **Overall VPC flow volume**
- **VPC flow volume to and from the finding IP address**, for findings that are associated with a single IP address
- **Container details**
- **VPC flow volume** for clusters
- **Overall Kubernetes API activity**

The activity details can answer these types of questions:

- Which IP addresses were used?
- Where were those IP addresses located?
- Which API calls did each IP address make, and from which services did they make those calls?
- Which principals or access key identifiers (AKIDs) were used to make the calls?
- What resources were used to make those calls?
- How many calls were made? How many succeeded and failed?
- What volume of VPC flow log data was sent to or from each IP address?

- What containers were active for a given cluster, image, or pod?

Topics

Activity details for Overall API call volume

The activity details for **Overall API call volume** show the API calls that were issued during a selected time range.

To display the activity details for a single time interval, choose the time interval on the chart.

To display the activity details for the current scope time, choose **Display details for scope time**.

Note that Detective began to store and display the service name for API calls as of July 14, 2021. That date is highlighted on the profile panel timeline. For activity that occurs before that date, the service name is **Unknown service**.

Content of the activity details (users, roles, accounts, role sessions, EC2 instances, S3 buckets)

For IAM users, IAM roles, accounts, role sessions, EC2 instances, and S3 buckets, the activity details contain the following information:

- Each tab provides information about the set of API calls that were issued during the selected time range.

  For S3 buckets, the information reflects API calls that were made to the S3 bucket.

  The API calls are grouped by the services that called them. For S3 buckets, the service is always Amazon S3. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.
- For each entry, the activity details show the number of successful and failed calls. The **Observed IP addresses** tab also shows the location of each IP address.

- Each entry shows information about who made the calls. For accounts, the activity details identify the users or roles. For roles, the activity details identify the role sessions. For users and role sessions, the activity details identify the access key identifiers (AKIDs).

  Note that as of July 14, 2021, for account profiles, the activity details show users or roles instead of AKIDs. For role profiles, the activity details show role sessions instead of AKIDs. For activity that occurs before July 14, 2021, the caller is listed as **Unknown resource**.

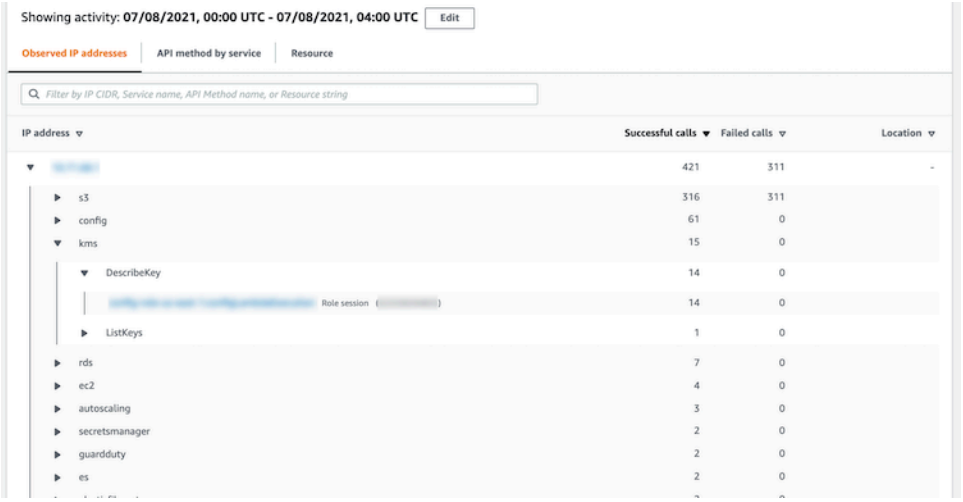
The activity details contain the following tabs:

Observed IP addresses

Initially displays the list of IP addresses used to issue API calls.

You can expand each IP address to display the list of API calls that were issued from that IP address. The API calls are grouped by the services that called them. For S3 buckets, the service is always Amazon S3. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.

You can then expand each API call to display the list of callers from that IP address. Depending on the profile, the caller might be a user, role, role session, or AKID.

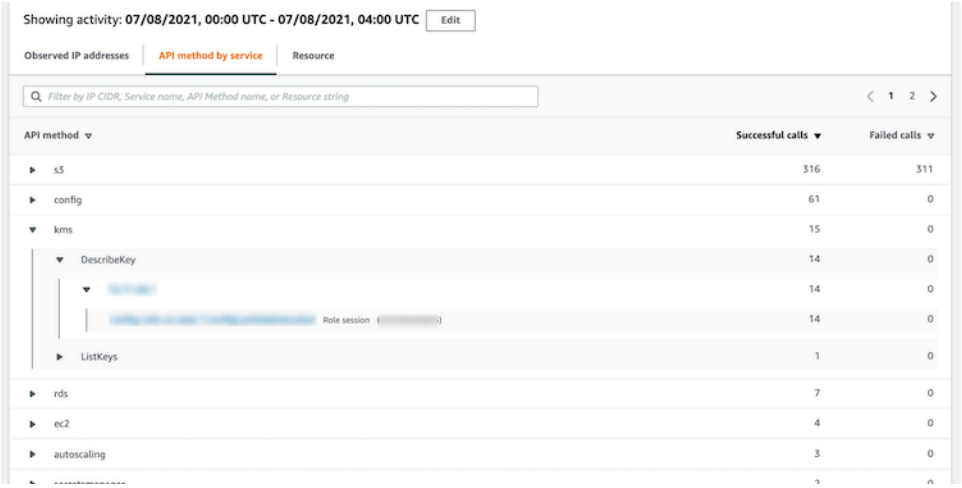


API method by service

Initially displays the list of API calls that were issued. The API calls are grouped by the services that issued the calls. For S3 buckets, the service is always Amazon S3. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.

You can expand each API method to display the list of IP addresses from which the calls were issued.

You can then expand each IP address to display the list of AKIDs that issued that API call from that IP address.

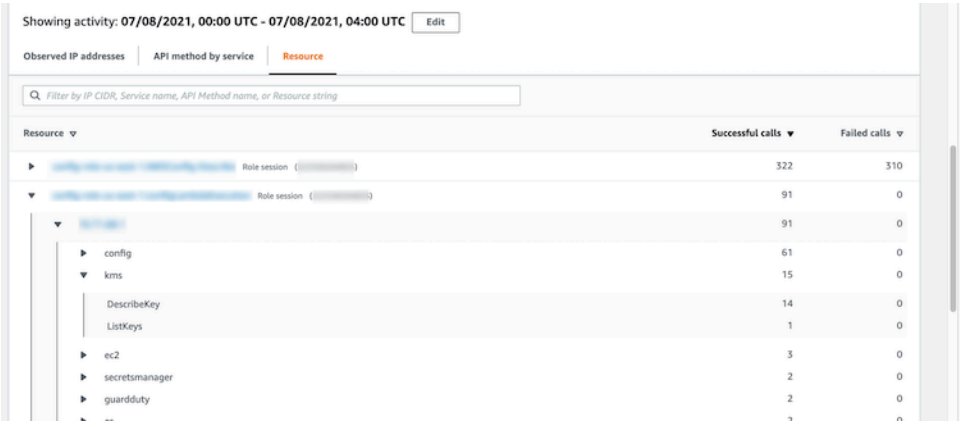


Resource or Access Key ID

Initially displays the list of users, roles, role sessions, or AKIDs that were used to issue API calls.

You can expand each caller to display the list of IP addresses from which the caller issued API calls.

You can then expand each IP address to display the list of API calls that were issued from that IP address by that caller. The API calls are grouped by the services that issued the calls. For S3 buckets, the service is always Amazon S3. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.



Content of the activity details (IP addresses)

For IP addresses, the activity details contain the following information:

- Each tab provides information about the set of API calls that were issued during the selected time range. The API calls are grouped by the services that issued the calls. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.
- For each entry, the activity details show the number of successful and failed calls.

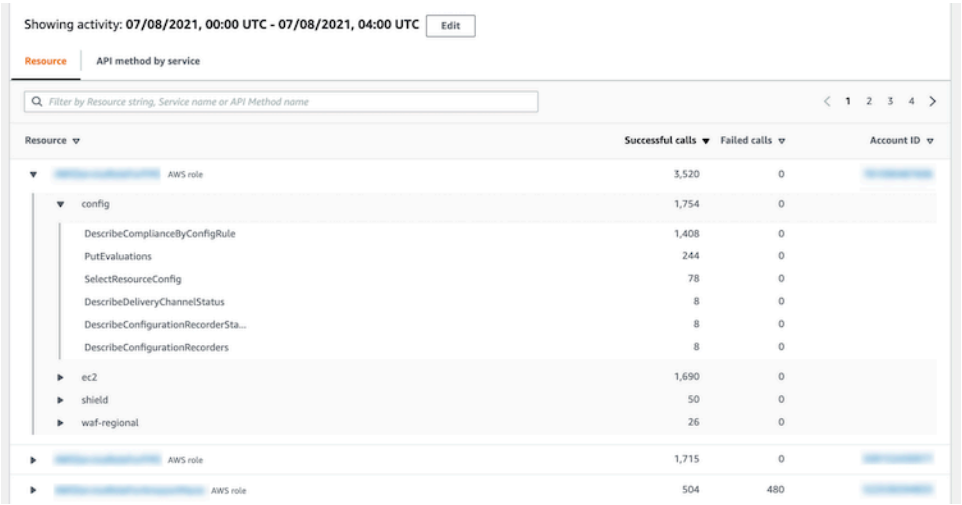
The activity details contain the following tabs:

Resource

Initially displays the list of resources that issued API calls from the IP address.

For each resource, the list includes the resource name, the type, and the AWS account.

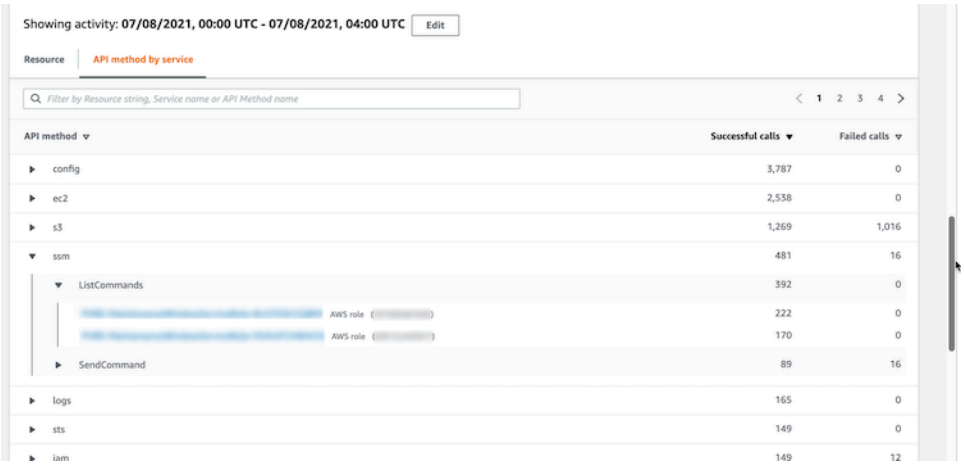
You can expand each resource to display the list of API calls that the resource issued from the IP address. The API calls are grouped by the services that issued the calls. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.



API method by service

Initially displays the list of API calls that were issued. The API calls are grouped by the services that issued the calls. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.

You can expand each API call to display the list of resources that issued the API call from the IP address during the selected time period.



Sorting the activity details

You can sort the activity details by any of the list columns.

When you sort using the first column, only the top-level list is sorted. The lower-level lists are always sorted by the count of successful API calls.

Filtering the activity details

You can use the filtering options to focus on specific subsets or aspects of the activity represented in the activity details.

On all of the tabs, you can filter the list by any of the values in the first column.

To add a filter

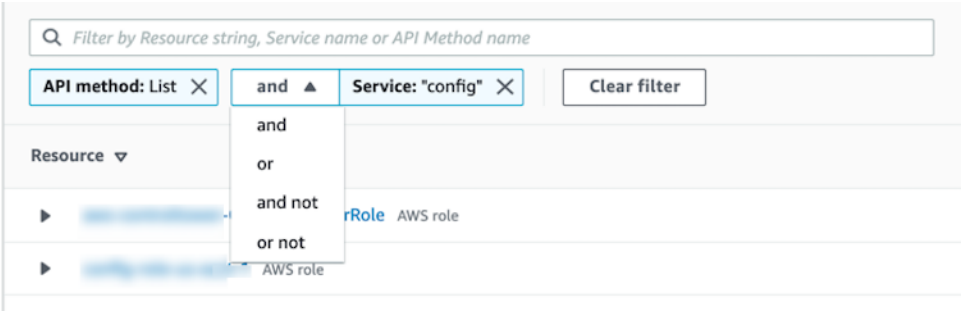
1. Choose the filter box.
2. From **Properties**, choose the property to use for the filtering.
3. Provide the value to use for the filtering. The filter supports partial values. For example, when you filter by API method, if you filter by **`Instance`**, the results include any API operation that has `Instance` in its name. So both `ListInstanceAssociations` and `UpdateInstanceInformation` would match.

   For service names, API methods, and IP addresses, you can either specify a value or choose a built-in filter.

   For **Common API substrings**, choose the substring that represents the type of operation, such as `List`, `Create`, or `Delete`. Each API method name starts with the operation type.

For **CIDR patterns**, you can choose to include only public IP addresses, private IP addresses, or IP addresses that match a specific CIDR pattern.

4. If you have multiple filters, choose a Boolean option to set how those filters are connected.



5. To remove a filter, choose the **x** icon in the top-right corner.
6. To clear all of the filters, choose **Clear filter**.

Selecting the time range for the activity details

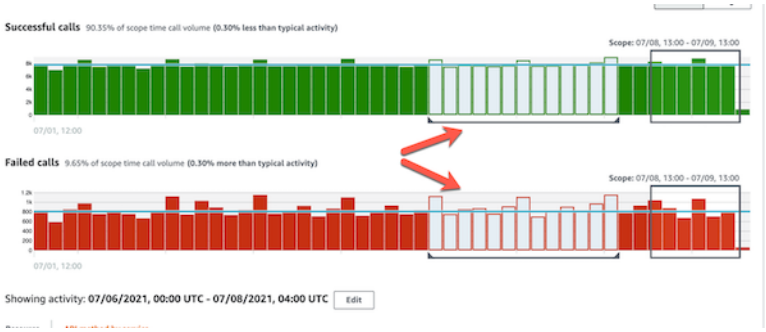
When you first display the activity details, the time range is either the scope time or a selected time interval. You can change the time range for the activity details.

To change the time range for the activity details

1. Choose **Edit**.
2. On **Edit time window**, choose the start and end time to use.

   To set the time window to the default scope time for the profile, choose **Set to default scope time**.
3. Choose **Update time window**.

The time range for the activity details is highlighted on the profile panel charts.



Querying raw logs

Amazon Detective integrates with Amazon Security Lake, which means that you can query and retrieve the raw log data stored by Security Lake. For more details about this integration, see *Integration with Amazon Security Lake*.

Using this integration, you can collect and query logs and events from the following sources which Security Lake natively supports.

- AWS CloudTrail management events
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs

> **Note**
>
> There are no additional charges to query raw data logs in Detective. Usage charges for other AWS Services, including Amazon Athena, still apply at published rates.

To query raw logs

1. Choose **display details for scope time**.
2. From here, you can start to **Query raw logs**.
3. In the **Raw log preview** table, you can view the logs and events retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Amazon Athena.

   From the Query raw logs table, you can **Cancel query request**, **See results in Amazon Athena**, and **Download results** as a comma-separated values (.csv) file.

If you see logs in Detective, but the query returned no results, it could happen because of the following reasons.

- Raw logs may become available in Detective before showing up in Security Lake log tables. Try again later.
- Logs may be missing from Security Lake. If you waited for an extended period of time, it indicates that logs are missing from Security Lake. Contact your Security Lake administrator to resolve the issue.

Activity details for a geolocation

The activity details for **Newly observed geolocations** show the API calls that were issued from a geolocation during the scope time. The API calls include all calls issued from the geolocation. They are not limited to calls that used the finding or profile entity. For S3 buckets, the activity calls are API calls made to the S3 bucket.

Detective determines the location of requests using MaxMind GeoIP databases. MaxMind reports very high accuracy of their data at the country level, although accuracy varies according to factors such as country and type of IP. For more information about MaxMind, see MaxMind IP Geolocation. If you think any of the GeoIP data is incorrect, you can submit a correction request to Maxmind at MaxMind Correct GeoIP2 Data.

The API calls are grouped by the services that issued the calls. For S3 buckets, the service is always Amazon S3. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.

To display the activity details, do one of the following:

- On the map, choose a geolocation.
- In the list, choose **Details** for a geolocation.

The activity details replace the geolocation list. To return to the geolocation list, choose **Return to all results**.

Note that Detective began to store and display the service name for API calls as of July 14, 2021. For activity that occurs before that date, the service name is **Unknown service**.

Content of the activity details

Each tab provides information about all of the API calls that were issued from the geolocation during the scope time.

For each IP address, resource, and API method, the list shows the number of successful and failed API calls.

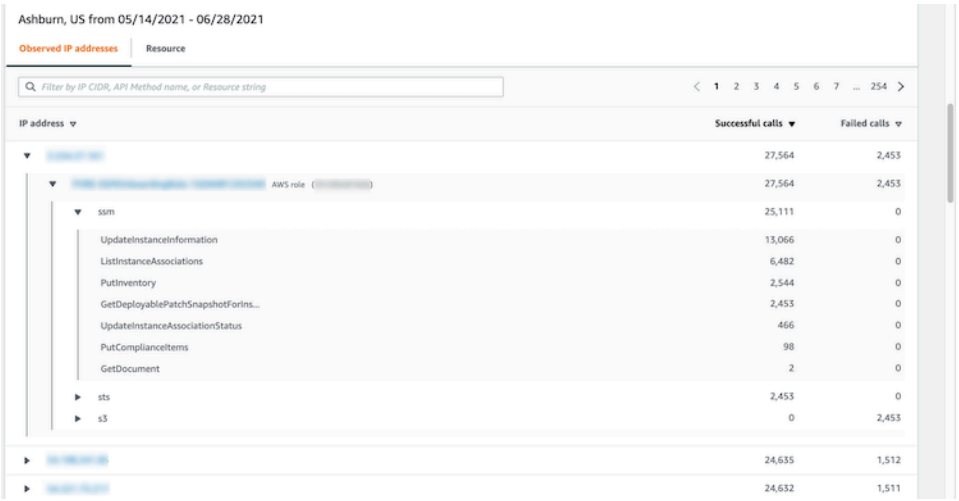
The activity details contain the following tabs:

Observed IP addresses

Initially displays the list of IP addresses that were used to issue API calls from the selected geolocation.

You can expand each IP address to display the resources that issued API calls from that IP address. The list displays the resource name. To see the principal ID, hover over the name.

You can then expand each resource to display the specific API calls that were issued from that IP address by that resource. The API calls are grouped by the services that issued the calls. For S3 buckets, the service is always Amazon S3. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.

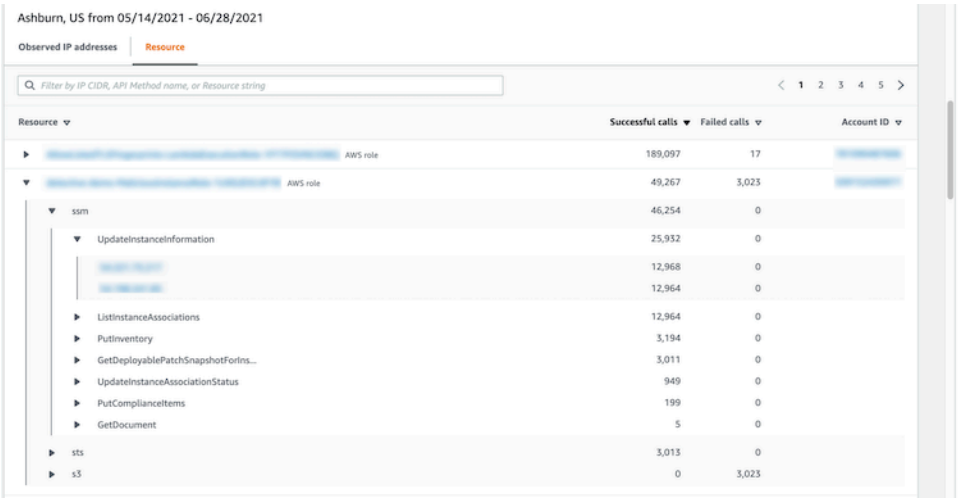


Resource

Initially displays the list of resources that issued API calls from the selected geolocation. The list displays the resource name. To see the principal ID, pause on the name. For each resource, the **Resource** tab also displays the associated AWS account.

You can expand each user or role to display the list of API calls that were issued by that resource. The API calls are grouped by the services that issued the calls. For S3 buckets, the service is always Amazon S3. If Detective cannot determine the service that issued a call, the call is listed under **Unknown service**.

You can then expand each API call to display the list of IP addresses from which the resource issued the API call.



Sorting the activity details

You can sort the activity details by any of the list columns.

When you sort using the first column, only the top-level list is sorted. The lower-level lists are always sorted by the count of successful API calls.

Filtering the activity details

You can use the filtering options to focus on specific subsets or aspects of the activity represented in the activity details.

On all of the tabs, you can filter the list by any of the values in the first column.

To add a filter

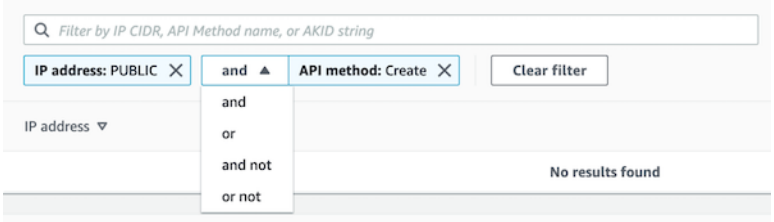
1. Choose the filter box.
2. From **Properties**, choose the property to use for the filtering.
3. Provide the value to use for the filtering. The filter supports partial values. For example, when you filter by API method, if you filter by **`Instance`**, the results include any API operation that has `Instance` in its name. So both `ListInstanceAssociations` and `UpdateInstanceInformation` would match.

   For service names, API methods, and IP addresses, you can either specify a value or choose a built-in filter.

For **Common API substrings**, choose the substring that represents the type of operation, such as `List`, `Create`, or `Delete`. Each API method name starts with the operation type.

For **CIDR patterns**, you can choose to include only public IP addresses, private IP addresses, or IP addresses that match a specific CIDR pattern.

4. If you have multiple filters, choose a Boolean option to set how those filters are connected.



5. To remove a filter, choose the **x** icon in the top-right corner.
6. To clear all of the filters, choose **Clear filter**.

Activity details for overall VPC flow volume

For an EC2 instance, the activity details for **Overall VPC flow volume** show the interactions between the EC2 instance and IP addresses during a selected time range.

For a Kubernetes pod, **Overall VPC flow volume** displays the overall volume of bytes into and out of the Kubernetes pod's assigned IP address for all destination IP addresses. The Kubernetes pod's IP address is not unique when `hostNetwork:true`. In this case, the panel shows traffic to other pods with the same configuration and the node hosting them.

For an IP address, the activity details for **Overall VPC flow volume** show the interactions between the IP address and EC2 instances during a selected time range.

To display the activity details for a single time interval, choose the time interval on the chart.

To display the activity details for the current scope time, choose **display details for scope time**.

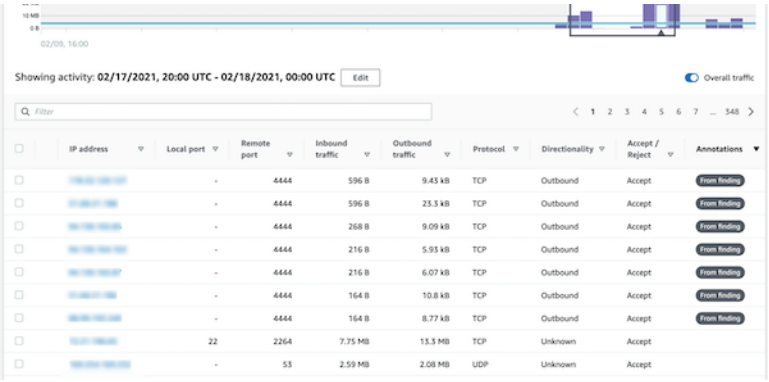
Content of the activity details

The content reflects the activity during the selected time range.

For an EC2 instance, the activity details contain an entry for each unique combination of IP address, local port, remote port, protocol, and direction.

For an IP address, the activity details contain an entry for each unique combination of EC2 instance, local port, remote port, protocol, and direction.

Each entry displays the volume of inbound traffic, the volume of outbound traffic, and whether the access request was accepted or rejected. On finding profiles, the **Annotations** column indicates when an IP address is related to the current finding.



Sorting the activity details

You can sort the activity details by any of the columns in the table.

By default, the activity details are sorted first by the annotations, then by the inbound traffic.

Filtering the activity details

To focus on specific activity, you can filter the activity details by the following values:

- IP address or EC2 instance
- Local or remote port
- Direction
- Protocol
- Whether the request was accepted or rejected

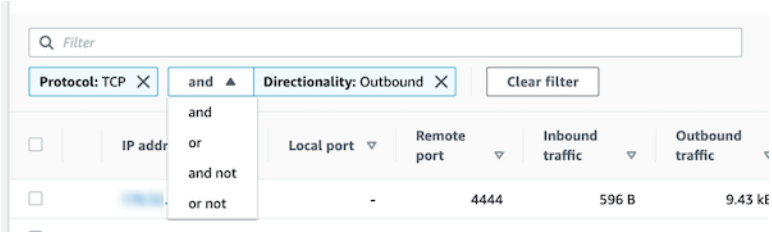
To add and remove filters

1. Choose the filter box.
2. From **Properties**, choose the property to use for the filtering.
3. Provide the value to use for the filtering. The filter supports partial values.

To filter by IP address, you can either specify a value or choose a built-in filter.

For **CIDR patterns**, you can choose to include only public IP addresses, private IP addresses, or IP addresses that match a specific CIDR pattern.

4. If you have multiple filters, choose a Boolean option to set how those filters are connected.



5. To remove a filter, choose the **x** icon in the top-right corner.
6. To clear all of the filters, choose **Clear filter**.

Selecting the time range for the activity details

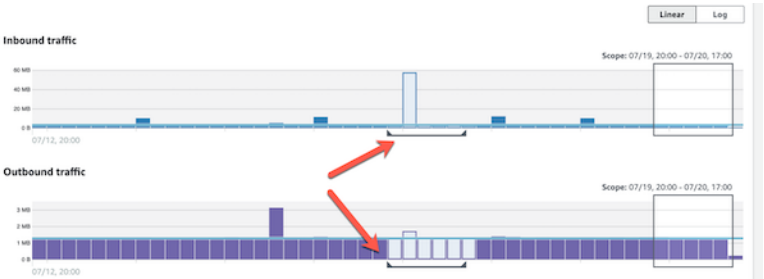
When you first display the activity details, the time range is either the scope time or a selected time interval. You can change the time range for the activity details.

To change the time range for the activity details

1. Choose **Edit**.
2. On **Edit time window**, choose the start and end time to use.

   To set the time window to the default scope time for the profile, choose **Set to default scope time**.
3. Choose **Update time window**.

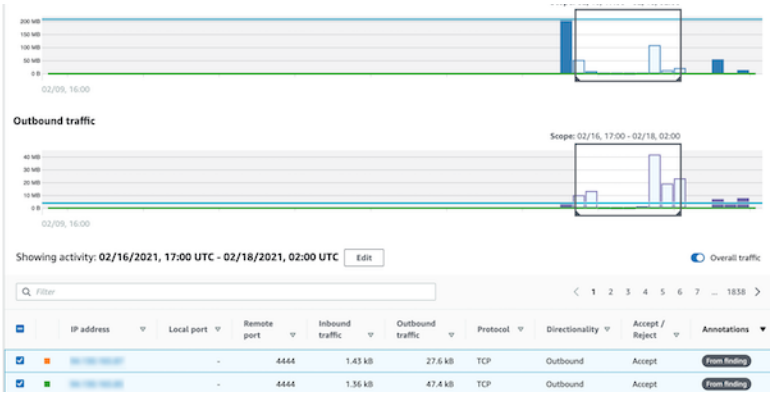
The time range for the activity details is highlighted on the profile panel charts.



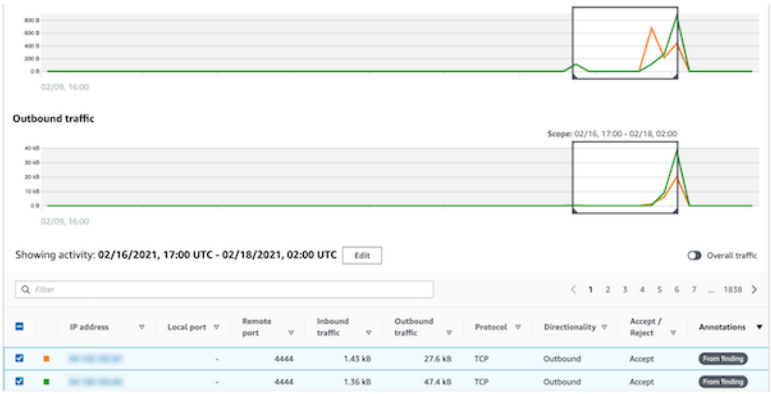
Displaying the volume of traffic for selected rows

When you identify rows that are of interest, you can display on the main charts the volume of traffic over time for those rows.

For each row to add to the charts, select the check box. For each selected row, the volume is displayed as a line on the inbound or outbound charts.



To focus on the traffic volume for the selected entries, you can hide the overall volume. To show or hide the overall traffic volume, toggle **Overall traffic**.



Displaying the VPC flow traffic for EKS clusters

Detective has visibility into your Amazon Virtual Private Cloud (Amazon VPC) flow logs, which represent the traffic that traverses your Amazon Elastic Kubernetes Service (Amazon EKS) clusters. For Kubernetes resources, the content of the VPC flow logs depends on the Container Network Interface (CNI) deployed in the EKS cluster.

An EKS cluster with a default configuration uses the Amazon VPC CNI plugin. For more details, see Managing VPC CNI in the Amazon EKS User Guide. The Amazon VPC CNI plugin sends internal traffic with the IP address of the pod and translates the source IP address to the IP address of the

node for external communication. Detective can capture and correlate internal traffic to the correct pod but it can't do the same for external traffic.

If you want Detective to have visibility into the external traffic of your pods, enable External Source Network Address Translation (SNAT). Enabling SNAT comes with limitations and drawbacks. For more details, see SNAT for pods in the Amazon EKS User Guide.

If you use a different CNI plugin, Detective has limited visibility to pods with `hostNetwork:true`. For these pods, the **VPC Flow** panel displays all traffic to the IP address of the pod. This includes the traffic to the host node and any pod on the node with the `hostNetwork:true` configuration.

Detective displays traffic in the **VPC flow** panel of an EKS pod for the following EKS cluster configurations:

- In a cluster with the Amazon VPC CNI plugin, any pod with the configuration `hostNetwork:false` sending traffic inside the VPC of the cluster.
- In a cluster with the Amazon VPC CNI plugin and the configuration `AWS_VPC_K8S_CNI_EXTERNALSNAT=true`, any pod with `hostNetwork:false` sending traffic outside the VPC of the cluster.
- Any pod with the configuration `hostNetwork:true`. Traffic from the node is mixed with traffic from other pods that have the configuration `hostNetwork:true`.

Detective does not display traffic in the **VPC flow** panel for:

- In a cluster with the Amazon VPC CNI plugin and the configuration `AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, any pod with the configuration `hostNetwork:false` sending traffic outside the VPC of the cluster.
- In a cluster without the Amazon VPC CNI plugin for Kubernetes, any pod with the configuration `hostNetwork:false`.
- Any pod sending traffic to another pod that is hosted in the same node.

Displaying the VPC flow traffic for shared Amazon VPCs

Detective has visibility into your Amazon Virtual Private Cloud (Amazon VPC) flow logs for shared VPCs:

- If a Detective member account has a shared Amazon VPC and there are other non-Detective accounts using the shared VPC, Detective monitors all traffic from that VPC, and provides visualization on all the traffic flow within the VPC.
- If you have an Amazon EC2 instance inside a shared Amazon VPC and the shared VPC owner is not a Detective member, Detective will not monitor any traffic from the VPC. If you want to view the traffic flow within the VPC, you must add the Amazon VPC owner as a member of your Detective graph.

Overall Kubernetes API activity involving EKS cluster

The activity details for **Overall Kubernetes API activity involving EKS cluster** show the number of successful and failed Kubernetes API calls that were issued during a selected time range.

To display the activity details for a single time interval, choose the time interval on the chart.

To display the activity details for the current scope time, choose **Display details for scope time**.

Content of the activity details (Cluster, pod, user, role, role session)

For a cluster, pod, user, role, or role session, the activity details contain the following information:

- Each tab provides information about the set of API calls that were issued during the selected time range.

  For clusters, the API calls occurred inside the cluster.

  For pods, the API calls targeted the pod.

  For users, roles, and role sessions, the API calls were issued by Kubernetes users that authenticated as that user, role, or role session.
- For each entry, the activity details show the number of successful, failed, unauthorized, and forbidden calls.
- The information includes the IP address, the type of Kubernetes call, the entity that was affected by the call, and the subject (service account or user) that made the call. From the activity details, you can pivot to the profiles for the IP address, subject, and the affected entity.

The activity details contain the following tabs:

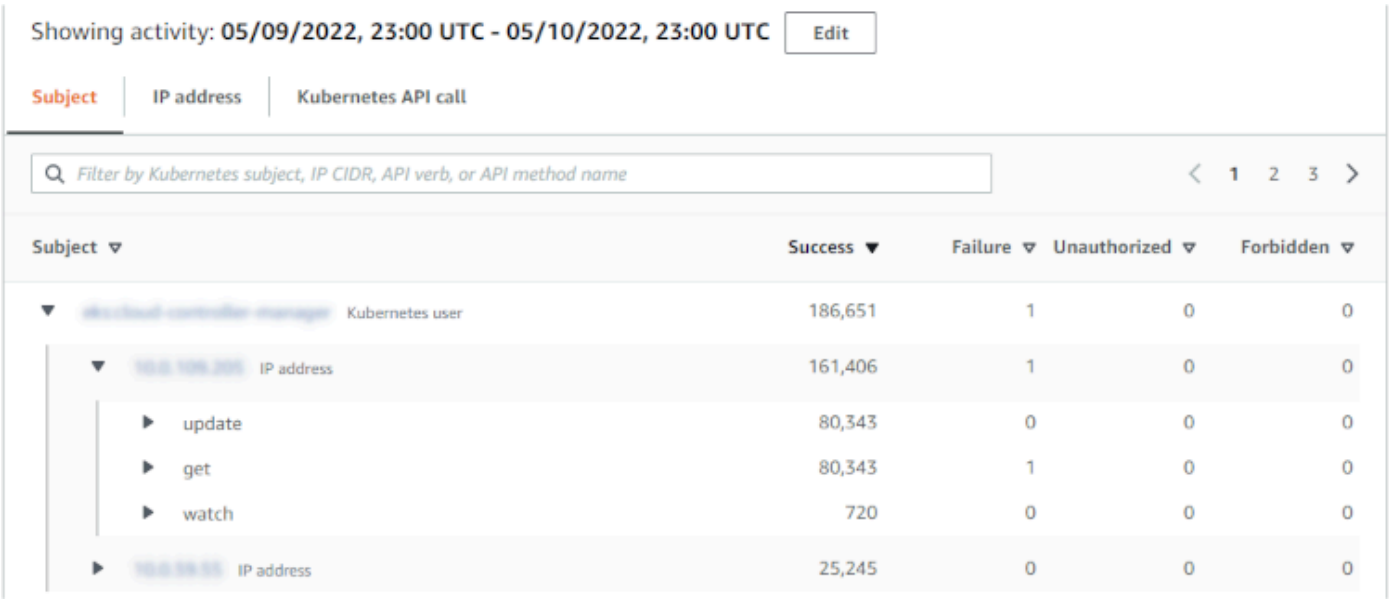
Subject

Initially displays the list of service accounts and users that were used to make API calls.

You can expand each service account and user to display the list of IP addresses from which the account or user made API calls.

You can then expand each IP address to show the Kubernetes API calls that were made by that account or user from that IP address.

Expand the Kubernetes API call to see the `requestURI` to identify the action that was done.



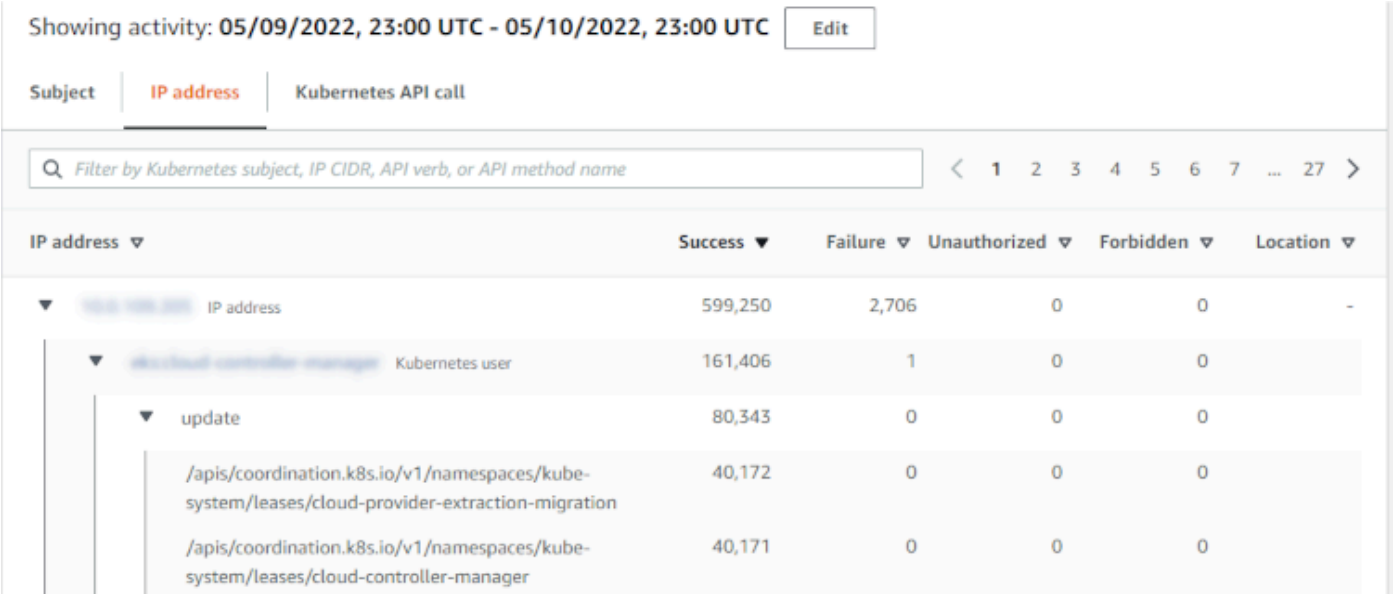
IP Address

Initially displays the list of IP addresses from which the API calls were made.

You can expand each call to display the list of Kubernetes subjects (service accounts and users) that made the call.

You can then expand each subject to a list of API call types made by the subject during the scope time.

Expand the API call type to see the requestURI to identify the action that was done.



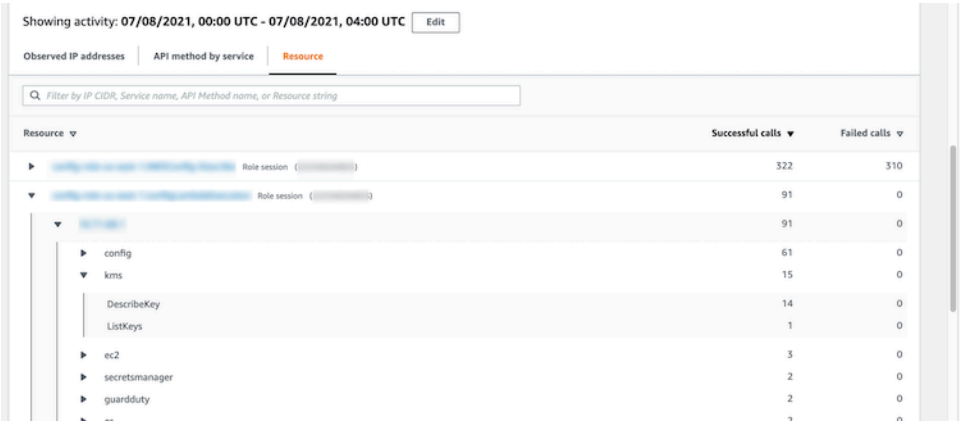
Kubernetes API call

Initially displays the list of Kubernetes API call verbs.

You can expand each API verb to display the requestURIs associated with that action.

You can then expand each requestURI to see Kubernetes subject (service accounts and users) that made the API call.

Expand the subject to see which IPs that subject used to make the API call.



Sorting the activity details

You can sort the activity details by any of the list columns.

When you sort using the first column, only the top-level list is sorted. The lower-level lists are always sorted by the count of successful API calls.

Filtering the activity details

You can use the filtering options to focus on specific subsets or aspects of the activity represented in the activity details.

On all of the tabs, you can filter the list by any of the values in the first column.

Selecting the time range for the activity details

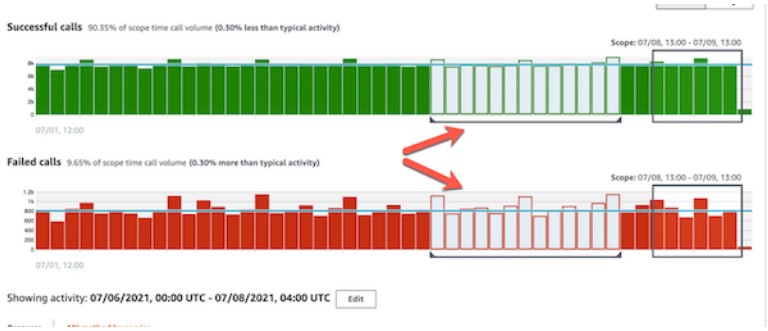
When you first display the activity details, the time range is either the scope time or a selected time interval. You can change the time range for the activity details.

To change the time range for the activity details

1. Choose **Edit**.
2. On **Edit time window**, choose the start and end time to use.

   To set the time window to the default scope time for the profile, choose **Set to default scope time**.
3. Choose **Update time window**.

The time range for the activity details is highlighted on the profile panel charts.



Using profile panel guidance during an investigation

Each profile panel is designed to provide answers to specific questions that arise as you conduct an investigation and analyze the activity for the related entities.

The guidance provided for each profile panel helps you find these answers.

Profile panel guidance starts with a single sentence on the panel itself. This guidance provides a brief explanation of the data presented on the panel.

To display more detailed guidance for a panel, choose **More info** from the panel heading. This extended guidance appears in the help pane.

The guidance can provide these types of information:

- An overview of the panel content
- How to use the panel to answer the relevant questions
- Suggested next steps based on the answers

Viewing details for high-volume entities

In the behavior graph, Amazon Detective tracks relationships between entities. For example, each behavior graph tracks when an AWS user creates an AWS role and when an EC2 instance connects to an IP address.

When an entity has too many relationships during a time period, Detective cannot store all of the relationships. When this occurs during the current scope time, Detective notifies you. Detective also provides a list of occurrences of high-volume entities.

What is a high-volume entity?

During a given time interval, an entity might be the origin or destination of an extremely large number of connections. For example, an EC2 instance may have connections from millions of IP addresses.

Detective maintains a limit on the number of connections that it can accommodate during each time interval. If an entity exceeds that limit, then Detective discards the connections for that time interval.

For example, assume that the limit is 100,000,000 connections per time interval. If an EC2 instance is connected to by more than 100,000,000 IP addresses during a time interval, then Detective discards the connections from that time interval.

However, you might be able to analyze that activity based on the entity at the other end of the relationship. To continue the example, while an EC2 instance might be connected to from millions of IP addresses, a single IP address connects to far fewer EC2 instances. Each IP address profile provides details about the EC2 instances that the IP address connected to.

Viewing the high-volume entity notification on a profile

Detective displays a notice at the top of a finding or entity profile if the scope time includes a time interval where the entity is high-volume. For finding profiles, the notice is for the involved entity.

The notice includes the list of relationships that have high-volume time intervals. Each list entry contains a description of the relationship and the start of the high-volume time interval.

A high-volume time interval might be an indicator of suspicious activity. To understand what other activity occurred at the same time, you can focus your investigation on a high-volume time

interval. The high-volume entity notice includes an option to set the scope time to that time interval.

To set the scope time to a high-volume time interval

1. In the high-volume entity notice, choose the time interval.
2. On the pop-up menu, choose **Apply scope time**.

Viewing the list of high-volume entities for the current scope time

The **High-volume entities** page contains a list of high-volume time intervals and entities during the current scope time.

To display the High-volume entities page

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **High-volume entities**.

Each entry in the list contains the following information:

- The start of the high-volume time interval
- The identifier and type of the entity
- The description of the relationship, such as "EC2 instance connected from IP address"

You can filter and sort the list by any of the columns. You can also navigate to the entity profile for an involved entity.

To navigate to the profile for an entity

1. In the **High-volume entities** list, choose the row to navigate from.
2. Choose **View profile with high-volume scope time**.

When you use this option to navigate to an entity profile, the scope time is set as follows:

- The scope time starts 30 days before the high-volume time interval.

- The scope time ends at the end of the high-volume time interval.

Archiving an Amazon GuardDuty finding

When you complete your investigation of an Amazon GuardDuty finding, you can archive the finding from Amazon Detective. This saves you the trouble of having to return to GuardDuty to make the update. Archiving a finding indicates that you have finished your investigation of it.

You can only archive a GuardDuty finding from within Detective if you are also the GuardDuty administrator account for the account associated with the finding. If you are not a GuardDuty administrator account and you attempt to archive a finding, GuardDuty displays an error.

To archive a GuardDuty finding

1. In the Detective console, in the finding details panel, choose **Archive finding**.
2. When prompted to confirm, choose **Archive**.

You can view archived GuardDuty findings in the GuardDuty console. To learn more, see Suppression Rules in the *Amazon GuardDuty User Guide*.

Document history for Detective User Guide

The following table describes the important changes to the documentation since the last release of Detective. For notification about updates to this documentation, you can subscribe to an RSS feed.

- **Latest documentation update:** April 05, 2024

Change	Description	Date
Added support for Amazon GuardDuty findings	Detective now provides support for the following GuardDuty Runtime Monitoring finding types. `Execution:Runtime/MaliciousFileExecuted` `Execution:Runtime/SuspiciousTool` `DefenseEvasion:Runtime/PtraceAntiDebugging` `Execution:Runtime/SuspiciousCommand` `DefenseEvasion:Runtime/SuspiciousCommand`	April 5, 2024
Added support for Amazon GuardDuty findings	Detective extends support for GuardDuty EC2 Runtime Monitoring finding types to ECS and EC2 resources.	January 30, 2024
Updated functionality	You can now run a Detective investigation from the Investigations page for a specific resource that you want to investigate. Detective recommends resources based	January 16, 2024

	on its activity in findings and finding groups. Detective investigations lets you investigate IAM users and IAM roles with indicators of compromise, which can help you determine if a resource is involved in a security incident.	
Updated functionality	You can now run a Detective investigation from the Investigations page on a recommended resource. Detective recommends resources based on its activity in findings and finding groups. Detective investigations lets you investigate IAM users and IAM roles with indicators of compromise, which can help you determine if a resource is involved in a security incident.	December 26, 2023
Regional availability	Added Europe (Stockholm), Europe (Paris), and Canada (Central) Regions to the list of AWS Regions where Detective integration with Security Lake is available.	December 8, 2023
New feature	Detective investigations lets you investigate IAM users and IAM roles with indicators of compromise, which can help you determine if a resource is involved in a security incident.	November 26, 2023

New feature	By default, Detective automatically generates finding group summaries for finding groups, powered by generative artificial intelligence (generative AI). Finding group summary, rapidly analyzes relations hips between findings and affected resources, and then summarizes potential threats in natural language.	November 26, 2023
New feature	Detective integration with Security Lake lets you can query and retrieve the raw log data stored by Security Lake. Using this integration, you can collect logs and events from CloudTrail managemen t events and Amazon Virtual Private Cloud (Amazon VPC) Flow Logs.	November 26, 2023
Viewing a finding overview	If a finding is correlated to a larger activity, Detective now notifies you to navigate to that finding group.	September 18, 2023
Enhanced finding groups visualization	Detective finding groups visualization now includes finding groups with aggregate d findings making it more efficient to analyze related evidences, entities, and findings.	August 8, 2023

Enhanced finding groups	Finding groups now include vulnerability findings from Amazon Inspector.	June 13, 2023
Added support for Amazon GuardDuty Lambda Protection	Detective now provides support for GuardDuty Lambda Protection.	May 26, 2023
Added AWS security findings as a new optional data source package.	Detective now provides AWS security findings as an optional data source package. This optional data source package allows Detective to ingest data from Security Hub and adds that data to your behavior graph.	May 16, 2023
Added support for Amazon GuardDuty EKS Runtime Monitoring finding types	Detective now provides support for GuardDuty EKS Runtime Monitoring finding types.	May 3, 2023
Added support for Amazon GuardDuty RDS Protection finding types	Detective now provides support for GuardDuty RDS Protection finding types.	April 20, 2023
Added support for additional Amazon GuardDuty finding types	Detective now provides profiles for the following additional GuardDuty finding types: `DefenseEvasion: EC2UnusualDNSResolver` `DefenseEvasion: EvasionEC2UnusualDoHActivity` `DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity`	April 12, 2023

Displaying the VPC flow traffic for EKS clusters	Added new section for Amazon Virtual Private Cloud (Amazon VPC) flow traffic with Amazon Elastic Kubernetes Service (Amazon EKS) clusters.	March 2, 2023
Finding group now includes a dynamic visual representation of Detective's behavior graph	Detective finding group now includes a dynamic visual representation of Detective's behavior graph to emphasize the relationship between entities and findings within the finding group.	February 28, 2023
Export data from Detective **Summary** page and search results page. The data is exported in comma-separated values (CSV) format.	Detective now provides the option to export data to your browser from the Detective console.	February 7, 2023
Added overall VPC flow volume for EKS Amazon EKS workloads	Detective now adds visual summaries and analytics about your Amazon Virtual Private Cloud (VPC) flow logs from your Amazon Elastic Kubernetes Service Amazon EKS workloads.	January 19, 2023
Added data retention	With Detective, you can access up to a year of historical event data.	December 20, 2022

Added the option to adjust scope time on the summary page.	Detective now provides the option to adjust the scope time so view the activity for any 24-hour time frame in the previous 365 days.	October 5, 2022
Searching for a finding or entity	Detective now provides case insensitive search.	October 3, 2022
Added the ability to set scope timestamp	Detective now provides a way to configure the scope timestamp format preferenc e. This preference will be applied to all timestamps in Detective.	October 3, 2022
Added new profiles associated with Amazon EKS audit logs	Detective now provides profiles to allow you to investigate activity associate d with the following container -related entities: Amazon EKS clusters, container images, Kubernetes pods, and Kubernetes subjects.	July 26, 2022
Replaced finding profiles with finding overviews	Finding profiles contained visualizations that analyzed activity for the involved resource. The new finding overview contains finding details ingested from GuardDuty, and a list of involved entities. From the finding overview, you can pivot to the profiles for related entities.	September 20, 2021

Removed the limit on supported GuardDuty finding types	Detective is no longer limited to a selected set of GuardDuty finding types. Detective automatically collects finding details for all finding types, and provides access to the entity profiles for the related entities.	September 20, 2021
Link to finding details from the associated findings profile panel	On an entity profile, when you choose a finding in the associated findings list, the finding details are displayed in the panel to the right. The scope time is set to the finding time window.	September 20, 2021
Added S3 buckets to the available entity types in Detective	Detective now provides profiles for S3 buckets. The S3 bucket profiles provide details about the principals that interacted with the S3 bucket and the API operation s that they performed on the S3 bucket.	September 20, 2021
New option to generate Detective URLs in Splunk	The Splunk Trumpet project allows you to send AWS content to Splunk. The project now allows you to add Detective URLs to navigate to profiles for GuardDuty findings.	September 8, 2021

Replaced AKIDs in the activity details for accounts and roles	On account profiles, the activity details for **Overall API call volume** now show users or roles instead of access key identifiers (AKIDs). On role profiles, the activity details for **Overall API call volume** now show role sessions instead of AKIDs. For activity that occurred before this change, the caller is listed as **Unknown resource**.	July 14, 2021
Added the calling service to information about API calls	On the Detective console, information about API calls now includes the service that issued the call. Added a **Service** column to the lists on the **Overall API call volume**, **Newly observed API calls**, and **API calls with increased volume**. On the activity details for **Overall API call volume** and **Newly observed geolocations**, API methods are grouped under the services that issued them. For activity that occurred before this change, the API methods are grouped under **Unknown service**.	July 14, 2021

New **Resource interaction** tab for users, roles, and role sessions	The **Resource interaction** tab for users, roles, and role sessions contains information about role assumption activity that involved those entities. For role sessions, this is a new tab. For users and roles, this is an existing tab with new content.	June 29, 2021
Added support for additional Amazon GuardDuty finding types	Detective now provides profiles for the following additional GuardDuty finding types: `CredentialAccess:IAMUser/AnomalousBehavior`, `DefenseEvasion:IAMUser/AnomalousBehavior`, `Discovery:IAMUser/AnomalousBehavior`, `Exfiltration:IAMUser/AnomalousBehavior`, `Impact:IAMUser/AnomalousBehavior`, `InitialAccess:IAMUser/AnomalousBehavior`, `Persistence:IAMUser/AnomalousBehavior`, `PrivilegeEscalation:IAMUser/AnomalousBehavior`	March 29, 2021

Added support for additional Amazon GuardDuty finding types	Detective now provides profiles for the following additional GuardDuty finding types: `Backdoor:EC2/C&CActivity.B` , `Impact:EC2/PortSweep` , `Impact:EC2/WinRMBruteForce` , and `PrivilegeEscalation:IAMUser/AdministrativePermissions`	March 4, 2021
Changed "master account" to "administrator account"	The term "master account" is changed to "administrator account." The term is also changed in the Detective console and API.	February 25, 2021
Added activity details for the profile panel VPC flow volume to and from the finding's IP address	The profile panel **VPC flow volume to and from the finding's IP address** now allows you to display activity details. The activity details are available only if the finding is associated with a single IP address. The activity details show the volume for each combination of ports, protocol, and direction.	February 25, 2021

New activity details for the Overall API call volume profile panel on IP address profiles	You can now display activity details for IP addresses from the **Overall API call volume** profile panel. The activity details show the number of successful and failed calls for each resource that issued the call from the IP address.	February 23, 2021
New Overall VPC flow volume profile panel on IP address profiles	The IP address profile now contains the **Overall VPC flow volume** profile panel. The profile panel shows the volume of VPC flow traffic to and from the IP address. You can display activity details to show the volume for each EC2 instance that the IP address communicated with.	January 21, 2021
Added the Detective Summary page	The Detective **Summary** page contains visualizations to guide analysts to entities of interest based on geolocati on, numbers of API calls, and Amazon EC2 traffic volume.	January 21, 2021

Updated the option to pivot from Amazon GuardDuty to Detective	In GuardDuty, the **Investigate in Detective** option is moved from the **Actions** menu to the finding details panel. It displays a list of related entities. If the finding type is supported, the list also includes the finding. You can then choose to navigate to either an entity profile or a finding profile.	January 15, 2021
Added option to set the activity details window to the default scope time	On the activity details for **Overall API call volume** and **Overall VPC flow volume**, you can set the time window for the activity details to the default scope time for the profile.	January 15, 2021
Added handling of high-volume time intervals for entities	Added a new notice to indicate when an entity has one or more high-volume time intervals. A new **High-volume entities** page displays all of the high-volume intervals for the current scope time.	December 18, 2020
Added time range selection for activity details on the Overall API call volume profile panel	On the **Overall API flow volume** panel, you can now display activity details for any selected time range. The panel initially displays an option to display the activity details for the scope time.	September 29, 2020

Added time interval selection for activity details on the Overall VPC flow volume profile panel	On the **Overall VPC flow** volume panel, you can display activity details for a single time interval from the chart. To display the details for time interval, choose the time interval.	September 25, 2020
New role session and federated user entities	Detective now allows you to explore and investigate federated authentication. You can see what resources have assumed each role, and when those authentications occurred.	September 17, 2020
Updates to scope time management	Removed the option to lock or unlock the scope time. It is always locked. On a finding profile, a warning is displayed if the scope time is different from the finding time window.	September 4, 2020
Profile header remains visible as you scroll through a profile	On profiles, the type, identifier, and scope time remain visible as you scroll through the profile panels on a tab. When the tabs are not visible, you can use the tab drop down list in the breadcrumbs to navigate to a different tab.	September 4, 2020

Search always displays search results	When you conduct a search, it now displays the results on the **Search** page. From the results, you can pivot to a finding or entity profile.	August 27, 2020
Added to the allowed criteria for searches	The allowed criteria for searches has expanded. You can search for AWS users and AWS roles by name. You can use the ARN to search for findings, AWS roles, AWS users, and EC2 instances.	August 27, 2020
Links to other consoles from profile panels	On the **EC2 instance details** profile panel, the EC2 instance identifier is linked to the Amazon EC2 console. On the **User details**, and **Role details** profile panels, the user name and role name are linked to the IAM console.	August 14, 2020
Activity details for VPC flow data	The **Overall VPC flow volume** profile panel now provides access to activity details. The activity details show the traffic flow between IP addresses and an EC2 instance during a selected time period.	July 23, 2020

Introducing Amazon Detective	Detective uses machine learning and purpose-built visualizations to help you analyze and investigate security issues across your Amazon Web Services (AWS) workloads.	December 2, 2019