aws

Administration Guide

Amazon Detective

Amazon Detective: Administration Guide

Table of Contents

What is Amazon Detective?

Amazon Detective helps you analyze, investigate, and quickly identify the root cause of security findings or suspicious activities. Detective automatically collects log data from your AWS resources. It then uses machine learning, statistical analysis, and graph theory to generate visualizations that help you to conduct faster and more efficient security investigations. The Detective prebuilt data aggregations, summaries, and context help you to quickly analyze and determine the nature and extent of possible security issues.

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 on source data in Detective, see *Source data used in a behavior graph*.

How does Detective work?

Detective automatically extracts time-based events such as login attempts, API calls, and network traffic from AWS CloudTrail and Amazon VPC flow logs. It also ingests findings detected by GuardDuty.

From those events, Detective uses machine learning and visualization to create a unified, interactive view of your resource behaviors and the interactions between them over time. You can explore this behavior graph to examine disparate actions such as failed logon attempts or suspicious API calls. You can also see how these actions affect resources such as AWS accounts and Amazon EC2 instances. You can adjust the behavior graph's scope and timeline for a variety of tasks:

- Rapidly investigate any activity that falls outside the norm.
- Identify patterns that may indicate a security issue.
- Understand all of the resources affected by a finding.

Detective tailored visualizations provide a baseline for and summarize the account information. These findings can help answer questions such as "Is this an unusual API call for this role?" Or "Is this spike in traffic from this instance expected?"

With Detective, you don't have to organize any data or develop, configure, or tune your own queries and algorithms. There are no upfront costs and you pay only for the events analyzed, with no additional software to deploy or other feeds to subscribe to.

Who uses Detective?

When an account enables Detective, it becomes the administrator account for a behavior graph. A behavior graph is a linked set of extracted and analyzed data from one or more AWS accounts. Administrator accounts invite member accounts to contribute their data to the administrator account's behavior graph.

Detective is also integrated with AWS Organizations. Your organization management account designates a Detective administrator account for the organization. The Detective administrator account enables organization accounts as member accounts in the organization behavior graph.

For information about how Detective uses source data from behavior graph accounts, see *Source data used in a behavior graph*.

For information on how administrator accounts manage behavior graphs, see *Managing accounts*. For information on how member accounts manage their behavior graph invitations and memberships, see the section called “For member accounts: Managing invitations and memberships”.

The administrator account uses the analytics and visualizations generated from the behavior graph to investigate AWS resources and GuardDuty findings. Using the Detective integrations with GuardDuty and AWS Security Hub, you can pivot from a GuardDuty finding in these services directly into the Detective console.

A Detective investigation focuses on the activity that is connected to the involved AWS resources. For an overview of the investigation process in Detective, see How Amazon Detective is used for investigation in *Detective User Guide*.

Amazon Detective terms and concepts

The following terms and concepts are important for understanding Amazon Detective and how it works.

Administrator account

The AWS account that owns a behavior graph and that uses the behavior graph for investigation.

The administrator account invites member accounts to contribute their data to the behavior graph. For more information, see the section called "Inviting member accounts to a behavior graph".

For the organization behavior graph, the administrator account is the Detective administrator account that the organization management account designates. For more information, see the section called "Designating the Detective administrator account". The Detective administrator account can enable any organization account as a member account in the organization behavior graph. For more information, see the section called "Managing organization member accounts".

Administrator accounts can also view data usage for the behavior graph, and remove member accounts from the behavior graph.

Autonomous System Organization (ASO)

The titled organization which is assigned an autonomous system. This autonomous system is a heterogenous network or a set of networks using similar routing logic and policies.

Behavior graph

A linked set of data generated from incoming source data that is associated with one or more AWS accounts.

Each behavior graph uses the same structure of findings, entities, and relationships.

Delegated administrator account (AWS Organizations)

In Organizations, the delegated administrator account for a service is able to manage the use of a service for the organization.

In Detective, the Detective administrator account is also the delegated administrator account, unless the Detective administrator account is the organization management account. The organization management account cannot be a delegated administrator account.

In Detective, self-delegation is allowed. An organization management account can delegate their own account to be the delegated administrator of Detective but this would be registered or remembered only in the scope of Detective and not organizations.

Detective administrator account

The account designated by the organization management account to be the administrator account for the organization behavior graph in a Region. For more information, see the section called “Designating the Detective administrator account”.

Detective recommends that the organization management account chooses an account other than their account.

If the account is not the organization management account, then the Detective administrator account is also the delegated administrator account for Detective in Organizations.

Detective source data

Processed, structured versions of information from the following types of feeds:

- Logs from AWS services, such as AWS CloudTrail logs and Amazon VPC Flow Logs
- GuardDuty findings

Detective uses the Detective source data to populate the behavior graph. Detective also stores copies of the Detective source data to support its analytics.

Entity

An item extracted from the ingested 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.

Entities can be AWS resources that you manage, or external IP addresses that have interacted with your resources.

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

Finding

A security issue detected by Amazon GuardDuty.

Finding group

A collection of related findings, entities, and evidence that may be related to the same event or security issue. Detective generates finding groups based on a built-in machine learning model.

Detective evidence

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

Finding overview

A single page that provides a summary of information about a finding.

A finding overview contains the list of involved entities for the findings. From the list, you can pivot to the profile for an entity.

A finding overview also contains a details panel that contains the finding attributes.

High-volume entity

An entity that has connections to or from a large number of other entities during a time interval. For example, an EC2 instance might have connections from millions of IP addresses. The number of connections exceeds the threshold that Detective can accommodate.

When the current scope time contains a high-volume time interval, Detective notifies the user.

For more information, see Viewing details for high-volume entities in the *Amazon Detective User Guide*.

Investigation

The process of triaging suspicious or interesting activity, determining its scope, getting to its underlying source or cause, and then determining how to proceed.

Member account

An AWS account that an administrator account invited to contribute data to a behavior graph. In the organization behavior graph, a member account can be an organization account that the Detective administrator account enabled as a member account.

Member accounts that are invited can respond to the behavior graph invitation and remove their account from the behavior graph. For more information, see the section called "For member accounts: Managing invitations and memberships".

Organization accounts cannot change their membership in the organization behavior graph.

All member accounts can also view usage information for their account across the behavior graphs that they contribute data to.

They have no other access to the behavior graph.

Organization behavior graph

The behavior graph that is owned by the Detective administrator account. The organization management account designates the Detective administrator account. For more information, see the section called "Designating the Detective administrator account".

In the organization behavior graph, the Detective administrator account controls whether an organization account is a member account. An organization account cannot remove itself from the organization behavior graph.

The Detective administrator account can also invite other accounts to the organization behavior graph.

Profile

A single page that provides a collection of data visualizations related to activity for an entity.

For findings, profiles help analysts to determine whether the finding is of genuine concern or a false positive.

Profiles provide information to support an investigation into a finding or for a general hunt for suspicious activity.

Profile panel

A single visualization on a profile. Each profile panel is intended to help answer a specific question or questions to assist an analyst in an investigation.

Profile panels can contain key-value pairs, tables, timelines, bar charts, or geolocation charts.

Relationship

Activity that occurs between individual entities. Relationships are also extracted from the incoming 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 an IP address connecting to an Amazon EC2 instance.

Scope time

The time window that is used to scope the data displayed on profiles.

The default scope time for a finding reflects the first and last times when the suspicious activity was observed.

The default scope time for an entity profile is the previous 24 hours.

Amazon Detective Regions and quotas

When using Amazon Detective, be aware of these quotas.

Detective Regions and endpoints

To see the list of AWS Regions where Detective is available, see Detective service endpoints.

Detective quotas

Detective has the following quotas, which cannot be configured.

Resource	Quota	Comments
Number of member accounts	1,200	The number of member accounts that an administrator account can add to a behavior graph.
Behavior graph data volume – volume warning	9 TB per day	If the behavior graph data volume is larger than 9 TB per day, then Detective displays a warning that the behavior graph is nearing the maximum allowed volume.
Behavior graph data volume – no new accounts	10 TB per day	If the behavior graph data volume is larger than 10 TB per day, then you cannot add new member accounts to the behavior graph.
Behavior graph data volume – stop data ingest into the behavior graph	15 TB per day	If the behavior graph data volume is larger than 15 TB per day, then Detective stops ingesting data into the behavior graph. The 15 TB per day reflects both normal data volume and spikes in the data volume.

Resource	Quota	Comments
		To re-enable the data ingest, you must contact AWS Support.

Internet Explorer 11 not supported

You cannot use Detective with Internet Explorer 11.

Setting up Amazon Detective

When you enable Amazon Detective, Detective creates a Region-specific behavior graph that has your account as its administrator account. This is initially the only account in the behavior graph. The administrator account can then invite other AWS accounts to contribute their data to the behavior graph. See *Managing accounts*.

Enabling Detective in a Region for the first time also begins a 30-day free trial for the behavior graph. If the account disables Detective and then enables it again, no free trial is available. See *About the free trial for behavior graphs*.

After the free trial, each account in the behavior graph is billed for the data they contribute to it. The administrator account can track the usage and see the total projected cost for a typical 30-day period for their entire behavior graph. For more information, see the section called "Administrator account usage and cost". Member accounts can track the usage and projected cost for the behavior graphs that they belong to. For more information, see the section called "Member account usage tracking".

Contents

Amazon Detective prerequisites and recommendations

Before you can enable Amazon Detective, you must have an AWS account.

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to an administrative user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

Create an administrative user

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

Create an administrative user

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to an administrative user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

Sign in as the administrative user

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

You also need to be aware of the following requirements and recommendations.

Supported AWS Command Line Interface version

To use the AWS CLI to perform Detective tasks, the minimum required version is 1.16.303.

Recommended alignment with GuardDuty and AWS Security Hub

If you are enrolled in GuardDuty and AWS Security Hub, we recommend that your account be an administrator account for those services. If the administrator accounts are the same for all three services, then the following integration points work seamlessly.

- In GuardDuty or Security Hub, when viewing details for a GuardDuty finding, you can pivot from the finding details to the Detective finding profile.
- In Detective, when investigating a GuardDuty finding, you can choose the option to archive that finding.

If you have different administrator accounts for GuardDuty and Security Hub, we recommend that you align the administrator accounts based on the service you use more frequently.

- If you use GuardDuty more frequently, then enable Detective using the GuardDuty administrator account.

  If you use AWS Organizations to manage accounts, designate the GuardDuty administrator account as the Detective administrator account for the organization.
- If you use Security Hub more frequently, then enable Detective using the Security Hub administrator account.

  If you use Organizations to manage accounts, designate the Security Hub administrator account as the Detective administrator account for the organization.

If you cannot use the same administrator accounts across all of the services, then after you enable Detective, you can optionally create a cross-account role. This role grants an administrator account access to other accounts.

For information about how IAM supports this type of role, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.

Granting the required Detective permissions

Before you can enable Detective, you must make sure that your IAM principal has the required Detective permissions. The principal can be an existing user or role that you are already using, or you can create a new user or role to use for Detective.

When you sign up for Amazon Web Services (AWS), your account is automatically signed up for all AWS services, including Amazon Detective. However, to enable and use Detective, you first have to set up permissions that allow you to access the Amazon Detective console and API operations. You or your administrator can do this by using AWS Identity and Access Management (IAM) to attach the `AmazonDetectiveFullAccess` managed policy to your IAM principal, which grants access to all Detective actions.

Recommended update to the GuardDuty CloudWatch notification frequency

In GuardDuty, detectors are configured with an Amazon CloudWatch notification frequency for reporting subsequent occurrences of a finding. This includes sending notifications to Detective.

By default, the frequency is six hours. This means that even if a finding recurs many times, the new occurrences are not reflected in Detective until up to six hours later.

To reduce the amount of time it takes for Detective to receive these updates, we recommend that the GuardDuty administrator account changes the setting on their detectors to 15 minutes. Note that changing the configuration has no effect on the cost of using GuardDuty.

For information about setting the notification frequency, see Monitoring GuardDuty Findings with Amazon CloudWatch Events in the *Amazon GuardDuty User Guide*.

Enabling Amazon Detective

When you enable Detective, you designate a Detective administrator account and invite other accounts to become member accounts. The administrator-member relationship is established when a prospective member account accepts the invitation. For more details, see Managing accounts.

In the organization behavior graph, the Detective administrator account manages the behavior graph membership for all organization accounts. For more information on how the Detective administrator account is managed, see Designating the Detective administrator account for an organization.

You can enable Detective from the Detective console, the Detective API, or the AWS Command Line Interface.

You can only enable Detective once in each Region. If you already are the administrator account for a behavior graph in the Region, then you cannot enable Detective again in that Region.

Enabling Detective (Console)

You can enable Amazon Detective from the AWS Management Console.

To enable Detective (console)

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. Choose **Get started**.
3. On the **Enable Amazon Detective** page, **Align administrator accounts (recommended)** explains the recommendation to align the administrator accounts between Detective and Amazon GuardDuty and AWS Security Hub. See the section called “Recommended alignment with GuardDuty and AWS Security Hub”.
4. The **Attach IAM policy** button takes you directly to the IAM console and opens up the recommended policy, You have the option to attach the recommended policy to the principal you use for Detective. If you do not have permissions to operate in the IAM console, within the **Required permissions** you can copy the policy Amazon Resource Name (ARN) to provide it to your IAM administrator. They can attach the policy on your behalf.

   Confirm that the required IAM policy is in place.
5. The **Add tags** section allows you to add tags to the behavior graph.

To add a tag, do the following:

a. Choose **Add new tag**.

b. For **Key**, enter the name of the tag.

c. For **Value**, enter the value of the tag.

To remove a tag, choose the **Remove** option for that tag.

6. Choose **Enable Amazon Detective**.
7. After you enable Detective, you can invite member accounts to your behavior graph.

   To navigate to the **Account management** page, choose **Add members now**. For information about inviting member accounts, see the section called “Inviting member accounts to a behavior graph”.

Enabling Detective (Detective API, AWS CLI)

You can enable Amazon Detective from the Detective API or the AWS Command Line Interface.

To enable Detective (Detective API, AWS CLI)

- **Detective API:** Use the `CreateGraph` operation.
- **AWS CLI:** At the command line, run the `create-graph` command.

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

The following command enables Detective and sets the value of the `Department` tag to `Security`.

```
aws detective create-graph --tags '{"Department": "Security"}'
```

Enabling Detective across Regions (Python script on GitHub)

Detective provides an open-source script in GitHub that does the following:

- Enables Detective for an administrator account in a specified list of Regions

- Adds a provided list of member accounts to each of the resulting behavior graphs
- Sends invitation emails to the member accounts
- Automatically accepts the invitations for the member accounts

For information about how to configure and use the GitHub scripts, see *Using the Amazon Detective Python scripts*.

Checking that data is being extracted

After you enable Detective, it begins to ingest and extract data from your AWS account into your behavior graph.

For the initial extraction, data usually becomes available in the behavior graph within 2 hours.

One way to check that Detective is extracting data is to look for example values on the Detective **Search** page.

To check for example values on the Search page

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, choose **Search**.
3. From the **Select type** menu, choose a type of item.

   Examples from your data contains a sample set of identifiers of the selected type that are in your behavior graph data.

   If you can see example values, then you know that data is being ingested and extracted into your behavior graph.

About the free trial for behavior graphs

Amazon Detective provides a 30-day free trial for each account in each Region. The free trial for an account starts the first time one of the following actions occurs.

- An account enables Detective manually and becomes the administrator account for a behavior graph.
- An account is designated as the Detective administrator account for an organization in AWS Organizations, and has Detective enabled for the first time.
- If the Detective administrator account already had Detective enabled before they were designated, then the account does not start a new 30-day free trial.
- An account accepts an invitation to be a member account in a behavior graph and is enabled as a member account.
- An organization account is enabled as a member account by the Detective administrator account.

The free trial lasts for 30 days from that point. The account is not billed for any data processed during that period. When the trial period ends, Detective begins to bill the account for the data it contributes to behavior graphs. For more information about how you can track your Detective activity, monitor usage and view the projected cost see Tracking actions and usage in Amazon Detective. For more information on pricing, see Detective pricing

The same 30-day period is used for all behavior graphs in the Region. For example, an account is enabled as a member account for a behavior graph. This starts the 30-day free trial. After 10 days, the account is enabled for a second behavior graph in the same Region. For the second behavior graph, the account receives 20 days of free data.

The free trial provides multiple benefits:

- Administrator accounts can explore Detective features and functionality to verify its value.
- Administrator and member accounts can monitor the amount of data and the estimated cost before Detective begins to bill them for it. See the section called “Administrator account usage and cost” and the section called “Member account usage tracking”.

Free trial for optional data sources

Detective also provides a free 30-day trial for optional data sources. This free trial is separate from the free trial provided for the core Detective data sources when Detective is first enabled.

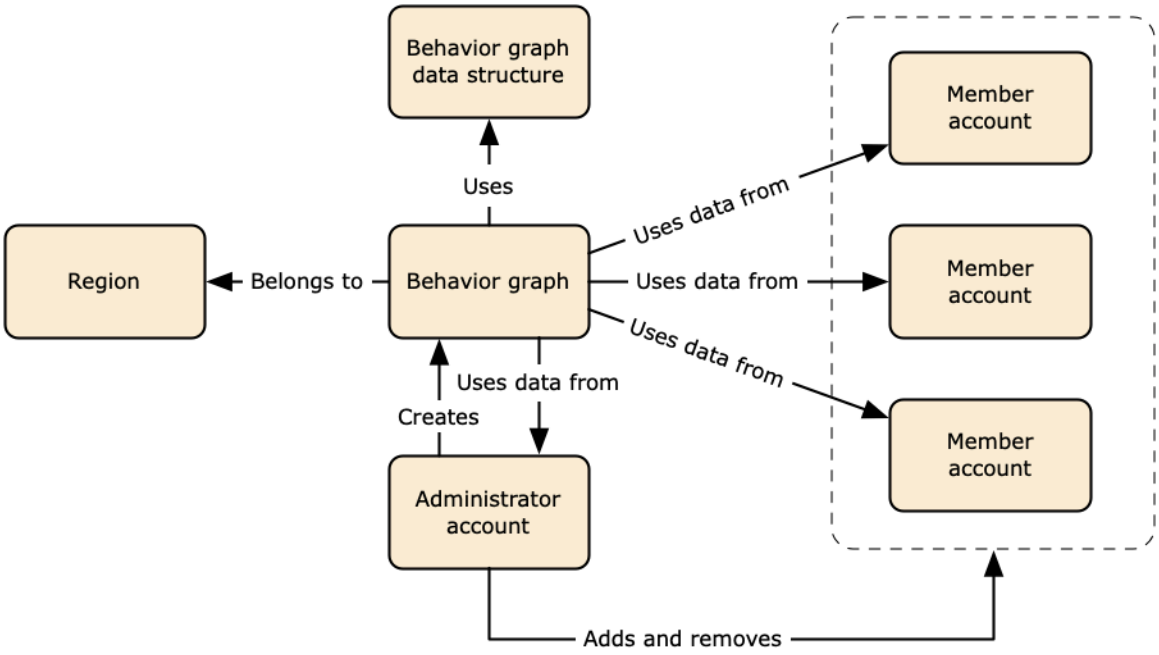
> **Note**
>
> If a customer disables an optional data source package within 7 days of enabling it, Detective does a one-time automatic reset of the free trial for that data source package if it is enabled again.

To enable or disable an optional data source see Types of optional data sources in Detective.

Source data used in a behavior graph

To populate a behavior graph, Amazon Detective uses source data from the behavior graph administrator account and member accounts.

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 details about the behavior graph data structure, see Overview of the behavior graph data structure in *Detective User Guide*.

Types of core data sources in Detective

Detective ingests data from these types of AWS logs:

- AWS CloudTrail logs
- Amazon Virtual Private Cloud (Amazon VPC) flow logs
- For accounts that are enrolled in GuardDuty, Detective also ingests GuardDuty findings.

Detective consumes CloudTrail and VPC flow log events using independent and duplicative streams of CloudTrail and VPC flow logs. These processes do not affect or use your existing CloudTrail and

VPC flow log configurations. They also do not affect the performance of or increase your costs for these services.

Types of optional data sources in Detective

Detective offers optional source packages in addition to the three data sources offered in the Detective core package (the core package includes AWS CloudTrail logs, VPC Flow logs, and GuardDuty findings). An optional data source package can be started or stopped for a behavior graph at any time.

Detective provides a 30-day free trial for all core and optional source packages per Region.

> **Note**
>
> Detective retains all data received from each data source package for up to 1 year.

Currently the following optional source packages are available:

- **EKS audit logs**

  This optional data source package allows Detective to ingest detailed information on EKS clusters in your environment and adds that data to your behavior graph. See Amazon EKS audit logs for Detective for details.

- **AWS security findings**

  This optional data source package allows Detective to ingest data from Security Hub and adds that data to your behavior graph. See **AWS security findings** for details.

Starting or stopping an optional data source:

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. From the navigation panel under **Settings**, choose **General**.
3. Under **Optional source packages**, select **Update**. Then select the data source you wish to enable or deselect a box for an already enabled data source and choose **Update** to change which data source packages are enabled.

> **Note**
>
> If you stop and then restart an optional data source you will see a gap in the data displayed on some entity profiles. This gap will be noted in the console display and represent the period of time when the data source was stopped. When a data source is restarted Detective does not retroactively ingest data.

Amazon EKS audit logs for Detective

Amazon EKS audit logs is an optional data source package that can be added to your Detective behavior graph. You can view the available optional source packages, and their status in your account, from the **Settings** page in the console or through the Detective API.

A 30 day free trial is provided for this data source. To learn more see Free trial for optional data sources.

Enabling Amazon EKS audit logs allows Detective to add in-depth information about resources created with Amazon EKS to your behavior graph. This data source enhances the information provided about the following entity types: EKS Cluster, Kubernetes Pod, Container Image and Kubernetes subject.

Additionally, If you have enabled EKS audit logs as a data source in Amazon GuardDuty you will be able to see details for Kubernetes findings from GuardDuty. For more info on enabling this data source in GuardDuty see Kubernetes protection in Amazon GuardDuty.

> **Note**
>
> This data source is enabled by default for new behavior graphs created after July 26, 2022. For behavior graphs created before July 26, 2022 it must be enabled manually.

Adding or removing Amazon EKS audit logs as an optional data source:

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. From the navigation panel under **Settings**, choose **General**.
3. Under **Source packages**, select **EKS audit logs** to enable this data source. If it is already enabled, select it again to stop ingesting **EKS audit logs** into your behavior graph.

AWS security findings

AWS security findings is an optional data source package that can be added to your Detective behavior graph.

You can view the available optional source packages, and their status in your account, from the Settings page in the console or through the Detective API.

A 30 day free trial is provided for this data source. To learn more see Free trial for optional data sources.

Enabling **AWS security findings** allows Detective to use the findings from Security Hub aggregated by Security Hub from upstream services in a standard findings format called the AWS Security Format (ASFF), which eliminates the need for time-consuming data conversion efforts. Then it correlates ingested findings across products to prioritize the most important ones.

Adding or removing AWS security findings as an optional data source:

> **Note**
>
> The AWS security findings data source is enabled by default for new behavior graphs created after May 16, 2023. For behavior graphs created before May 16, 2023 it must be enabled manually.

1. Open the Detective console at https://console.aws.amazon.com/detective/.
2. From the navigation panel under **Settings**, choose **General**.
3. Under **Source packages**, select AWS security findings to enable this data source. If it is already enabled, select it again to stop ingesting AWS Security Finding Format (ASFF) findings into your behavior graph.

Currently supported findings

Detective ingests all ASFF findings in Security Hub from services that are owned by Amazon or AWS.

- To see the list of supported service integrations, see Available AWS service integrations in the AWS Security Hub User Guide.

- For the list of supported resources, see Resources in the AWS Security Hub User Guide.
- AWS Service Findings with a Compliance status not set to `FAILED` and cross-Region aggregated findings are not ingested.

How Detective ingests and stores source data

When Detective is enabled, Detective begins ingesting source data from the behavior graph administrator account. As member accounts are added to the behavior graph, Detective also begins using the data from those member accounts.

Detective source data consists of structured and processed versions of the original feeds. To support Detective analytics, Detective stores copies of the Detective source data.

The Detective ingest process feeds data into Amazon Simple Storage Service (Amazon S3) buckets in the Detective source data store. As new source data arrives, other Detective components pick up the data and start the extraction and analytics processes. For more information, see How Detective uses source data to populate a behavior graph in *Detective User Guide*.

How Detective enforces the data volume quota for behavior graphs

Detective has strict quotas on the volume of data it allows in each behavior graph. The data volume is the amount of data per day that flows into the Detective behavior graph.

Detective enforces these quotas when an administrator account enables Detective, and when a member account accepts an invitation to contribute to a behavior graph.

- If the data volume for an administrator account exceeds 10 TB per day, then the administrator account cannot enable Detective.
- If the added data volume from a member account would cause the behavior graph to exceed 10 TB per day, the member account cannot be enabled.

The data volume for a behavior graph also can grow naturally over time. Detective checks the behavior graph data volume each day to make sure that it does not exceed the quota.

If the behavior graph data volume is approaching the quota, Detective displays a warning message on the console. To avoid exceeding the quota, you can remove member accounts.

If the behavior graph data volume exceeds 10 TB per day, then you cannot add a new member account to the behavior graph.

If the behavior graph data volume exceeds 15 TB per day, then Detective stops ingesting data into the behavior graph. The 15 TB per day quota reflects both normal data volume and spikes in the data volume. When this quota is reached, no new data is ingested into the behavior graph, but existing data is not removed. You can still use that historical data for investigation. The console displays a message to indicate that the data ingest is suspended for the behavior graph.

If the data ingest is suspended, you must work with AWS Support to get it re-enabled. If possible, before you contact AWS Support, try to remove member accounts to get the data volume below the quota. This makes it easier to re-enable the data ingest for the behavior graph.

Managing accounts

Each behavior graph contains data from one or more accounts. When an account enables Detective, it becomes the administrator account for the behavior graph, and it chooses the member accounts for the behavior graph. A behavior graph can have up to 1,200 member accounts.

If you are integrated with AWS Organizations, then the organization management account designates the Detective administrator account for the organization. That Detective administrator account then becomes the administrator account for the organization behavior graph. The Detective administrator account can enable any organization account as a member account in the organization behavior graph. Organization accounts cannot remove themselves from the organization behavior graph.

An administrator account also can invite accounts to join a behavior graph. When the account accepts the invitation, Detective enables the account as a member account. Member accounts that are added by invitation can remove themselves from the behavior graph.

When an account is enabled as a member account, Detective begins to ingest and extract the member account's data into that behavior graph.

Detective charges each account for the data that it contributes to each behavior graph. For information on tracking the volume of data for each account in a behavior graph, see the section called “Administrator account usage and cost”.

Contents

Account restrictions and recommendations in Detective

When managing accounts in Amazon Detective, be aware of the following restrictions and recommendations.

Maximum number of member accounts

Detective allows up to 1,200 member accounts in each behavior graph.

Accounts and Regions

If you use AWS Organizations to manage accounts, the organization management account designates a Detective administrator account for the organization. The Detective administrator account becomes the administrator account for the organization behavior graph.

The Detective administrator account must be the same in all Regions. The organization management account designates the Detective administrator account separately in each Region. The Detective administrator account also manages the organization behavior graphs and member accounts separately in each Region.

For member accounts created by invitation, the administrator-member association is created only in the Region that the invitation is sent from. The administrator account must enable Detective in each Region, and has a separate behavior graph in each Region. The administrator account then invites each account to associate as a member account in that Region.

An account can be a member account of multiple behavior graphs in the same Region. An account can only be the administrator account of one behavior graph per Region. An account can be an administrator account in different Regions.

Alignment of administrator accounts with Security Hub and GuardDuty

To ensure that the integrations with AWS Security Hub and Amazon GuardDuty work smoothly, we recommend that the same account is the administrator account in all of these services.

See the section called “Recommended alignment with GuardDuty and AWS Security Hub”.

Granting the required permissions for administrator accounts

To ensure that an administrator account has the required permissions to manage its behavior graph, attach the `AmazonDetectiveFullAccess` managed policy to the IAM principal.

Reflecting organization updates in Detective

Changes to an organization are not immediately reflected in Detective.

For most changes, such as new and removed organization accounts, it can take up to an hour for Detective to be notified.

A change to the designated Detective administrator account in Organizations takes less time to propagate.

Making the transition to use Organizations to manage behavior graph accounts

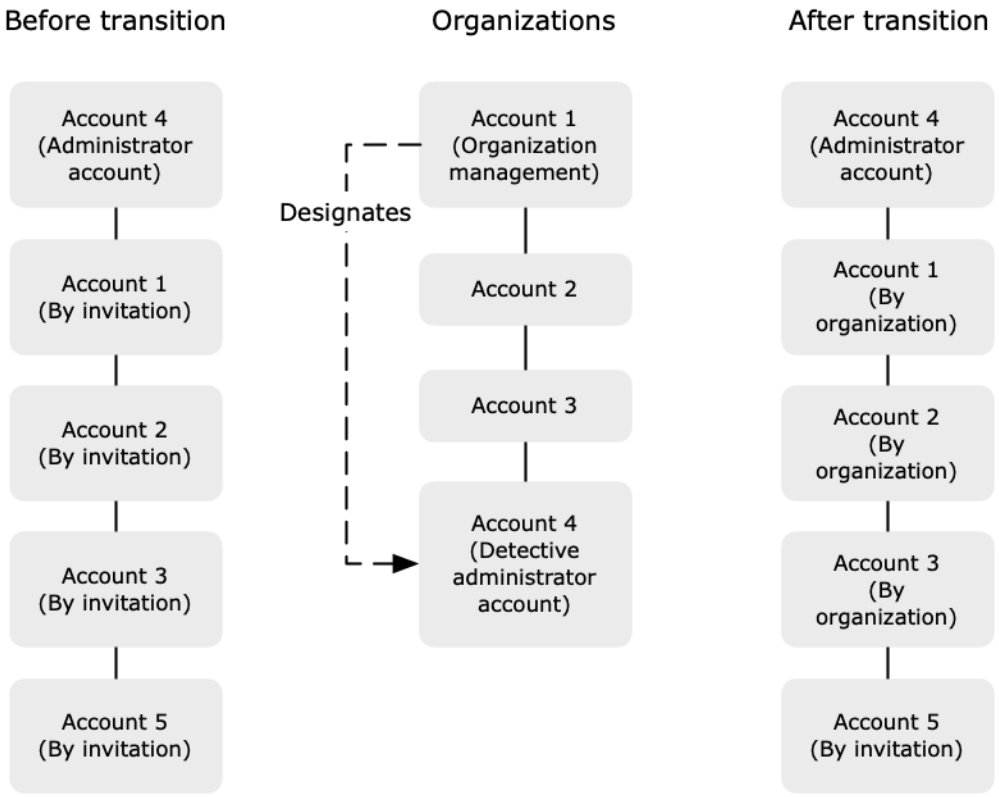
You might have an existing behavior graph with member accounts that accepted a manual invitation. If you are enrolled in AWS Organizations, use the following steps to use Organizations to enable and manage member accounts instead of using the manual invitation process:

1. Designate the Detective administrator account for your organization. This creates the organization behavior graph.

   If the Detective administrator account already has a behavior graph, then that behavior graph becomes the organization behavior graph.
2. Enable organization accounts as member accounts in the organization behavior graph.

   If the organization behavior graph has existing member accounts that are organization accounts, those accounts are enabled automatically.

The following diagram shows an overview of a behavior graph structure before the transition, the configuration in Organizations, and the behavior graph account structure after the transition.



Designate a Detective administrator account for your organization

Your organization management account designates the Detective administrator account from your organization. See the section called “Designating the Detective administrator account”.

To make the transition simpler, Detective recommends that you choose a current administrator account as the Detective administrator account for the organization.

If there is a delegated administrator account for Detective in Organizations, then you must use either that account or the organization management account as the Detective administrator account.

Otherwise, the first time you designate a Detective administrator account that is not the organization management account, Detective calls Organizations to make that account the delegated administrator account for Detective.

Enable organization accounts as member accounts

The Detective administrator account is the administrator account for the organization behavior graph. The Detective administrator account chooses the organization accounts to enable

as member accounts in the organization behavior graph. See the section called "Managing organization member accounts".

On the **Accounts** page, the Detective administrator account sees all of the accounts in the organization.

If the Detective administrator account was already the administrator account for a behavior graph, then that behavior graph becomes the organization behavior graph. Organization accounts that were already member accounts in that behavior graph are enabled as member accounts automatically. Other organization accounts have a status of **Not a member**.

Organization accounts have a type of **By organization**, even if they were previously member accounts by invitation.

Member accounts that do not belong to the organization have a type of **By invitation**.

The **Account management** page also provides an option, **Automatically enable new organization accounts**, to automatically enable new accounts as they are added to an organization. See the section called "Enabling new organization accounts automatically". The option is initially turned off.

When the Detective administrator account first displays the **Account management** page, it displays a message that contains an **Enable all organization accounts** button. When you choose **Enable all organization accounts**, Detective performs the following actions:

- Enables all of the current organization accounts as member accounts.
- Turns on the option to automatically enable new organization accounts.

There is also an **Enable all organization accounts** option on the member account list.

Available actions for accounts

Administrator and member accounts have access to the following Detective actions. In the table, the values have the following meanings:

- **Any** – The account can perform the action for all of the accounts under the same Detective administrator account.
- **Self** – The account can only perform the action on their own account.

- Dash (–) – The account cannot perform the action.

The following table reflects the default permissions for administrator and member accounts. You can use custom IAM policies to restrict access further to Detective features and functions.

Action	Administrator account (Organization)	Administrator account (Invitation)	Member (Organization)	Member (Invitation)
View accounts	Any	Any	Self (View administrator accounts)	Self (View administrator accounts)
Remove member account	Any Invited accounts are removed Organization accounts are disassociated	Any	–	Self
Add or remove optional data source packages	Any (Setting applies to all member accounts)	Any (Setting applies to all member accounts)	–	–
Disable Detective	Self	Self	–	–
View behavior graph data	Any	Any	–	–
Enable or disable optional data source packages	All	All	–	–

Designating the Detective administrator account for an organization

In the organization behavior graph, the Detective administrator account manages the behavior graph membership for all organization accounts.

How the Detective administrator account is managed

The organization management account designates the Detective administrator account for the organization in each AWS Region.

Setting the Detective administrator account as the delegated administrator account

The Detective administrator account also becomes the delegated administrator account for Detective in AWS Organizations. The exception is if the organization management account designates itself as the Detective administrator account. The organization management account cannot be a delegated administrator in Organizations.

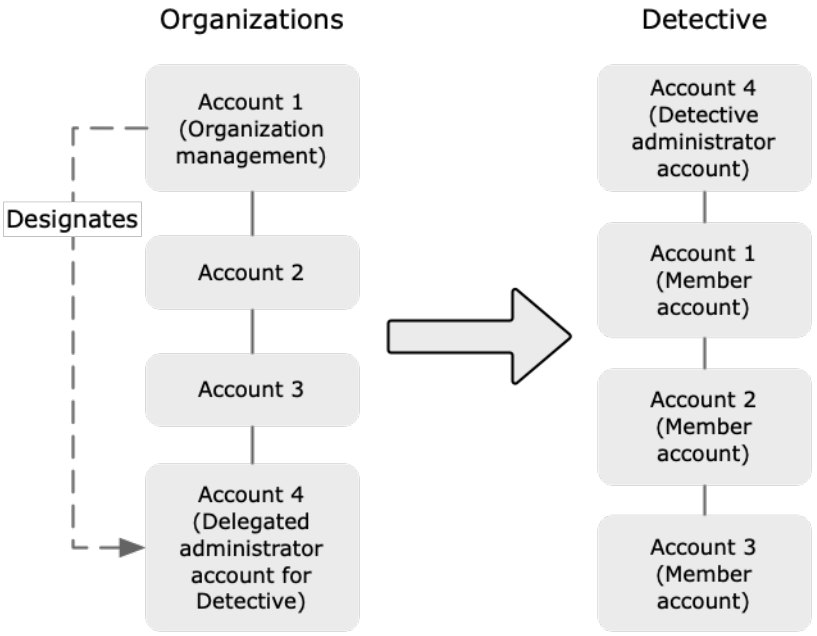
After the delegated administrator account is set in Organizations, the organization management account can only choose either the delegated administrator account or their own account as the Detective administrator account. We recommend that you choose the delegated administrator account in all Regions.

Creating and managing the organization behavior graph

When the organization management account chooses a Detective administrator account, Detective creates a new behavior graph for that account. That behavior graph is the organization behavior graph.

If the Detective administrator account is an administrator account for an existing behavior graph, then that behavior graph becomes the organization behavior graph.

The Detective administrator account chooses organization accounts to enable as member accounts in the organization behavior graph.



The Detective administrator account can also send invitations to accounts that do not belong to the organization. For more information, see the section called "Managing organization member accounts" and the section called "Managing invited accounts".

Removing the Detective administrator account

The organization management account can remove the current Detective administrator account in a Region. When you remove the Detective administrator account, Detective only removes it from the current Region. It does not change the delegated administrator account in Organizations.

When the organization management account removes the Detective administrator account in a Region, Detective deletes the organization behavior graph. Detective is disabled for the removed Detective administrator account.

To remove the current delegated administrator account for Detective, you use the Organizations API. When you remove the delegated administrator account for Detective in Organizations, Detective deletes all of the organization behavior graphs where the delegated administrator account is the Detective administrator account. Organization behavior graphs that have the organization management account as the Detective administrator account are not affected.

Required permissions to configure the Detective administrator account

To ensure that the organization management account is able to configure the Detective administrator account, you can attach the `AmazonDetectiveOrganizationsAccess` managed policy to your AWS Identity and Access Management (IAM) entities.

Designating a Detective administrator account (console)

The organization management account can use the Detective console to designate the Detective administrator account.

You do not need to enable Detective in order to manage the Detective administrator account. You can manage the Detective administrator account from the **Enable Detective** page.

To designate a Detective administrator account (Enable Detective page)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. Choose **Get started**.
3. In the **Required permissions for administrator accounts** panel, grant necessary the permissions to the account you choose so that they can operate as a Detective administrator with full access to all actions in Detective. To operate as an administrator, We recommend attaching the `AmazonDetectiveFullAccess` policy to the principal.
4. Choose **Attach policy from IAM** to view the recommended policy directly in the IAM console.
5. Depending on whether you have permissions in the IAM console, proceed as follows:

   - If you have permissions to operate in the IAM console, attach the recommended policy to the principal you use for Detective.
   - If you don't have permissions to operate in the IAM console, copy the Amazon Resource Name (ARN) of the policy and provide it to your IAM administrator. They can then attach the policy on your behalf.
6. Under **Delegated administrator**, choose the Detective administrator account.

   The available options depend on whether you have a delegated administrator account for Detective in Organizations.

   - If you do not have a delegated administrator account for Detective in Organizations, then enter the account identifier of the account to designate it as the Detective administrator account.

You might have an existing administrator account and behavior graph from the manual invitation process. If so, we recommend that you designate that account as the Detective administrator account.

If you have a delegated administrator account in Organizations for Amazon GuardDuty, AWS Security Hub, or Amazon Macie, then Detective prompts you to select one of those accounts. You can also enter a different account.

- If you do have a delegated administrator account for Detective in Organizations, then you are prompted to choose either that account or your account. We recommend that you choose the delegated administrator account in all Regions.

7. Choose **Delegate**.

If you have Detective enabled, or are a member account in an existing behavior graph, then you can designate the Detective administrator account from the **General** page.

To designate a Detective administrator account (General page)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, under **Settings**, choose **General**.
3. In the **Managed policies** panel, you can learn more about all the managed policies Detective supports. You can grant necessary permissions to an account depending on the actions you want users to perform in Detective. To operate as an administrator, We recommend attaching the `AmazonDetectiveFullAccess` policy to the principal.
4. Depending on whether you have permissions in the IAM console, proceed as follows:

   - If you have permissions to operate in the IAM console, attach the recommended policy to the principal you use for Detective.
   - If you don't have permissions to operate in the IAM console, copy the Amazon Resource Name (ARN) of the policy and provide it to your IAM administrator. They can then attach the policy on your behalf.

   The available options depend on whether you have a delegated administrator account for Detective in Organizations.

- If you do not have a delegated administrator account for Detective in Organizations, then enter the account identifier of the account to designate it as the Detective administrator account.

  You might have an existing administrator account and behavior graph from the manual invitation process. If so, then we recommend that you designate that account as the Detective administrator account.

  If you have a delegated administrator account in Organizations for Amazon GuardDuty, AWS Security Hub, or Amazon Macie, then Detective prompts you to select one of those accounts. You can also enter a different account.
- If you do have a delegated administrator account for Detective in Organizations, then you are prompted to choose either that account or your account. We recommend that you choose the delegated administrator account in all Regions.

5. Choose **Delegate**.

Designating a Detective administrator account (Detective API, AWS CLI)

To designate the Detective administrator account, you can use an API call or the AWS Command Line Interface. You must use the organization management account credentials.

If you already have a delegated administrator account for Detective in organizations, then you must choose either that account or your account we recommend that you choose the delegated administrator account.

To designate the Detective administrator account (Detective API, AWS CLI)

- **Detective API:** Use the `EnableOrganizationAdminAccount` operation. You must provide the AWS account identifier of the Detective administrator account. To obtain the account identifier, use the `ListOrganizationAdminAccounts` operation.
- **AWS CLI:** At the command line, run the `enable-organization-admin-account` command.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Example

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Removing a Detective administrator account (console)

From the Detective console, you can remove the Detective administrator account.

When you remove the Detective administrator account, Detective is disabled for the account, and the organization behavior graph is deleted. The Detective administrator account is only removed in the current Region.

> **Important**
>
> Removing a Detective administrator account does not affect the delegated administrator account in Organizations.

To remove the Detective administrator account (Enable Detective page)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. Choose **Get started**.
3. Under **Delegated Administrator**, choose **Disable Amazon Detective**.
4. On the confirmation dialog box, enter **`disable`**, then choose **Disable Amazon Detective**.

To remove a Detective administrator account (General page)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, under **Settings**, choose **General**.
3. Under **Delegated Administrator**, choose **Disable Amazon Detective**.
4. On the confirmation dialog box, enter **`disable`**, then choose **Disable Amazon Detective**.

Removing the Detective administrator account (Detective API, AWS CLI)

To remove the Detective administrator account, you can use an API call or the AWS CLI. You must use the organization management account credentials.

When you remove the Detective administrator account, Detective is disabled for the account, and the organization behavior graph is deleted.

> **Important**
>
> Removing a Detective administrator account does not affect the delegated administrator account in Organizations.

To remove the Detective administrator account (Detective API, AWS CLI)

- **Detective API:** Use the `DisableOrganizationAdminAccount` operation.

  When you use the Detective API to remove the Detective administrator account, it is only removed in the Region where the API call or command was issued.
- **AWS CLI:** At the command line, run the `disable-organization-admin-account` command.

```
aws detective disable-organization-admin-account
```

Removing the delegated administrator account (Organizations API, AWS CLI)

Removing the Detective administrator account does not automatically remove the delegated administrator account in Organizations. To remove the delegated administrator account for Detective, you can use the Organizations API.

When you remove the delegated administrator account, this deletes all organization behavior graphs where the delegated administrator account is the Detective administrator account. It also disables Detective for the account in those Regions.

To remove the delegated administrator account (Organizations API, AWS CLI)

- **Organizations API:** Use the `DeregisterDelegatedAdministrator` operation. You must provide the account identifier of the Detective administrator account, and the service principal for Detective, which is `detective.amazonaws.com`.
- **AWS CLI:** At the command line, run the `deregister-delegated-administrator` command.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

Example

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

Viewing the list of accounts

The administrator account can use the Detective console or API to view a list of accounts. The list can include:

- Accounts that the administrator account invited to join the behavior graph. These accounts have a type of **By invitation**.
- For the organization behavior graph, all of the accounts in the organization. These accounts have a type of **By organization**.

The results do not include invited member accounts that declined an invitation or that the administrator account removed from the behavior graph. It only includes accounts with the following statuses.

Verification in progress

For invited accounts, Detective is verifying the account email address before it sends the invitation.

For organization accounts, Detective is verifying that the account belongs to the organization. Detective also verifies that it was the Detective administrator account that enabled the account.

Verification failed

The verification failed. The invitation was not sent, or the organization account was not enabled as a member.

Invited

For invited accounts. The invitation was sent, but the member account has not yet responded.

Not a member

For organization accounts in the organization behavior graph. The organization account is not currently a member account. It does not contribute data to the organization behavior graph.

Enabled

For invited accounts, the member account accepted the invitation and contributes data to the behavior graph.

For organization accounts in the organization behavior graph, the Detective administrator account enabled the account as a member account. The account contributes data to the organization behavior graph.

Not enabled

For invited accounts, the member account accepted the invitation, but cannot be enabled.

For organization accounts in the organization behavior graph, the Detective administrator account tried to enable the account, but the account cannot be enabled.

For invited accounts, Detective checks the number of member accounts. The maximum number of member accounts for a behavior graph is 1,200. If the behavior graph already contains 1,200 member accounts, then new accounts cannot be enabled.

Detective checks whether your data volume is within the Detective quota. The volume of data flowing into a behavior graph must be less than the maximum allowed by Detective. If the current volume ingested is above the limit of 10 TB per day for Behavior graph data volume, then Detective will not allow you to add additional member accounts.

Listing accounts (Console)

You can use the AWS Management Console to see and filter your list of accounts.

To display the list of accounts (console)

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

   The member account list contains the following accounts:

   - Your account
   - Accounts that you invited to contribute data to the behavior graph
   - In the organization behavior graph, all of the organization accounts

For each account, the list displays the following information:

- The AWS account identifier.
- For organization accounts, the account name.
- The account type (**By invitation** or **By organization**).
- For invited accounts, the account root user email address.
- The account status.
- The daily data volume for the account. Detective cannot retrieve the data volume for accounts that are not enabled as member accounts.
- The date when the account status was last updated.

You can use the tabs at the top of the table to filter the list based on the member account status. Each tab shows the number of matching member accounts.

- Choose **All** to view all of the member accounts.
- Choose **Enabled** to view accounts that have a status of **Enabled**.
- Choose **Not enabled** to view accounts that have a status other than **Enabled**.

You also can add other filters to the member account list.

To add a filter to the list of accounts in the behavior graph (console)

1. Choose the filter box.
2. Choose the column that you want to use to filter the list.
3. For the specified column, choose the value to use for the filter.
4. To remove a filter, choose the **x** icon at the top right.
5. To update the list with the most recent status information, choose the refresh icon at the top right.

Listing your member accounts (Detective API, AWS CLI)

You can use an API call or the AWS Command Line Interface to view a list of member accounts in your behavior graph.

To get the ARN of your behavior graph to use in the request, use the `ListGraphs` operation.

To retrieve a list of member accounts (Detective API, AWS CLI)

- **Detective API:** Use the `ListMembers` operation. To identify the intended behavior graph, specify the behavior graph ARN.

  Note that for the organization behavior graph, `ListMembers` does not return organization accounts that you did not enable as member accounts or that you disassociated from the behavior graph.
- **AWS CLI:** At the command line, run the `list-members` command.

```
aws detective list-members --graph-arn <behavior graph ARN>
```

Example:

```
aws detective list-members --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

To retrieve details about specific member accounts in your behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `GetMembers` operation. Specify the behavior graph ARN and the list of account identifiers for the member accounts.
- **AWS CLI:** At the command line, run the `get-members` command.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
 graph ARN>
```

Example:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Managing organization accounts as member accounts

In the organization behavior graph, the Detective administrator account determines which organization accounts to enable as member accounts.

They can configure Detective to enable new organization accounts as member accounts automatically, or they can enable organization accounts manually.

The Detective administrator account also can disassociate organization accounts from the organization behavior graph.

Contents

Enabling new organization accounts as member accounts automatically

The Detective administrator account can configure Detective to automatically enable new organization accounts as member accounts in the organization behavior graph.

When new accounts are added to your organization, they are added to the list on the **Account management** page. For organization accounts, **Type** is **By organization**.

By default, new organization accounts are not enabled as member accounts. Their status is **Not a member**.

When you choose to enable organization accounts automatically, then Detective begins to enable new accounts as member accounts as they are added to the organization. Detective does not enable existing organization accounts that are not yet enabled.

Detective can enable organization accounts as member accounts only if the maximum number of member accounts for a behavior graph is 1,200. If your behavior graph already contains 1,200 member accounts, then new accounts cannot be enabled.

Detective checks whether your data volume is within the Detective quota. The volume of data flowing into a behavior graph must be less than the maximum allowed by Detective. If the current

volume ingested is above the limit of 10 TB per day, you cannot add more accounts and Detective will disable further ingestion of data.

Enabling new organization accounts automatically (console)

On the **Account management** page, the **Automatically enable new organization accounts** setting determines whether to automatically enable accounts as they are added to an organization.

To automatically enable new organization accounts as member accounts

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.
3. Toggle **Automatically enable new organization accounts** to the on position.

Enabling new organization accounts automatically (Detective API, AWS CLI)

To determine whether to automatically enable new organization accounts as member accounts, the administrator account can use the Detective API or the AWS Command Line Interface.

To view and manage the configuration, you must provide the behavior graph ARN. To obtain the ARN, use the `ListGraphs` operation.

To view the current configuration for automatically enabling organization accounts

- **Detective API:** Use the `DescribeOrganizationConfiguration` operation.

  In the response, if new organization accounts are enabled automatically, then `AutoEnable` is `true`.
- **AWS CLI:** At the command line, run the `describe-organization-configuration` command.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

Example

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

To automatically enable new organization accounts

- **Detective API:** Use the UpdateOrganizationConfiguration operation. To automatically enable new organization accounts, set `AutoEnable` to `true`.
- **AWS CLI:** At the command line, run the update-organization-configuration command.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --
auto-enable | --no-auto-enable
```

Example

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

Enabling organization accounts as member accounts

If you do not automatically enable new organization accounts, then you can enable those accounts manually. You must also manually enable accounts that you disassociated.

Determining whether an account can be enabled

You cannot enable an organization account as a member account if the organization behavior graph already has the maximum 1,200 enabled accounts. In this case, the organization account status remains **Not a member**. The account does not contribute data to the behavior graph.

As soon as the member account can be enabled, Detective automatically changes the member account status to **Enabled**. For example, the member account status changes to **Enabled** if the administrator account removes other member accounts to make space for an account.

Enabling organization accounts as member accounts (console)

From the **Account management** page, you can enable organization accounts as member accounts.

To enable organization accounts as member accounts

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.
3. To view the list of accounts that are not currently enabled, choose **Not enabled**.

4. You can either select specific organization accounts, or enable all organization accounts.

   To enable selected organization accounts:

   a. Select each organization account that you want to enable.

   b. Choose **Enable accounts**.

   To enable all organization accounts, choose **Enable all organization accounts**.

Enabling organization accounts as member accounts (Detective API, AWS CLI)

You can use the Detective API or the AWS Command Line Interface to enable organization accounts as member accounts in the organization behavior graph. To get the ARN of your behavior graph to use in the request, use the `ListGraphs` operation.

To enable organization accounts as member accounts (Detective API, AWS CLI)

- **Detective API:** Use the `CreateMembers` operation. You must provide the graph ARN.

  For each account, specify the account identifier. Organization accounts in the organization behavior graph do not receive an invitation. You do not need to provide an email address or other invitation information.
- **AWS CLI:** At the command line, run the `create-members` command.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

Example

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012
 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Disassociating organization accounts as member accounts

To stop ingesting data from an organization account in the organization behavior graph, you can disassociate the account. Existing data for that account remains in the behavior graph.

When you disassociate an organization account, the status changes to **Not a member**. Detective stops ingesting data from that account, but the account remains in the list.

Disassociating organization accounts (console)

From the **Account management** page, you can disassociate organization accounts as member accounts.

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.
3. To display the list of enabled accounts, choose **Enabled**.
4. Select the check box for each account to disassociate.
5. Choose **Actions**. Then choose **Disable accounts**.

   The account status for the disassociated accounts changes to **Not a member**.

Disassociating organization accounts (Detective API, AWS CLI)

You can use the Detective API or the AWS Command Line Interface to disassociate organization accounts as member accounts in your behavior graph.

To get the ARN of your behavior graph to use in the request, use the `ListGraphs` operation.

To disassociate organization accounts from the organization behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `DeleteMembers` operation. Specify the graph ARN and the list of account identifiers for the member accounts to disassociate.
- **AWS CLI:** At the command line, run the `delete-members` command.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Example

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Managing invited member accounts

An administrator account can invite accounts to be member accounts in the behavior graph. When a member account accepts the invitation and is enabled, Amazon Detective begins to ingest and extract the member account's data into that behavior graph.

For behavior graphs other than the organization behavior graph, all of the member accounts are invited accounts.

The Detective administrator account can also invite accounts that are not organization accounts to the organization behavior graph.

The administrator account can remove invited member accounts from the behavior graph.

Contents

Inviting member accounts to a behavior graph

The administrator account can invite accounts to contribute to a behavior graph. A behavior graph can contain up to 1,200 member accounts.

At a high level, the process for inviting accounts to contribute to a behavior graph is as follows.

1. For each member account to add, the administrator account provides the AWS account identifier and the root user email address.
2. Detective validates that the email address is the root user email address for the account. If the account information is valid, Detective sends the invitation to the member account.

   Detective does not perform this validation or sends email invitations to member accounts in these Regions:

   - AWS GovCloud (US-East) Region
   - AWS GovCloud (US-West) Region

   For other Regions, you can `DisableEmailNotification` using the CreateMembers operation of the Detective API. If `DisableEmailNotification` is set to true, then Detective will not

send invitations to the member accounts. This is a useful setting for accounts that are managed centrally.

3. The member account accepts or declines the invitation.

   Even if the administrator account does not send invitation emails, the member account still must respond to the invitation.

4. After the member account accepts the invitation, Detective begins to ingest data from the member account into the behavior graph.

5. As soon as the member account is eligible to be enabled, Detective automatically changes the member account status to **Enabled**.

   For example, the member account status changes to **Enabled** if the administrator account removes other member accounts to make space for an account.

   If more than one account is **Not enabled**, then Detective enables the accounts in the order in which they were invited. The process to check whether to enable any **Not enabled** accounts runs every hour.

   The administrator account also can enable accounts manually, instead of waiting for the automatic process. For example, the administrator account might want to select the accounts to enable. See the section called “Enabling a member account that is Not enabled”.

   Note that Detective began to automatically enable accounts that are **Not enabled** on May 12, 2021. Accounts that were **Not enabled** before then are not enabled automatically. The administrator account must enable them manually.

Inviting individual accounts to a behavior graph (Console)

You can manually specify the member accounts to invite to contribute their data to a behavior graph.

To manually select the member accounts to invite (console)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.
3. Choose **Actions**. Then choose **Invite accounts**.
4. Under **Add accounts**, choose **Add individual accounts**.

5. To add a member account to the invitation list, perform the following steps.

   a. Choose **Add account**.

   b. For **AWS Account ID**, enter the AWS account ID.

   c. For **Email address**, enter the root user email address for the account.

6. To remove an account from the list, choose **Remove** for that account.
7. Under **Personalize invitation email**, add customized content to include in the invitation email.

   For example, you can use this area to provide contact information. Or use it to remind the member account that they need to attach the required IAM policy to their user or role before they can accept the invitation.

8. **Member account IAM policy** contains the text of the required IAM policy for member accounts. The email invitation includes this policy text. To copy the policy text, choose **Copy**.
9. Choose **Invite**.

Inviting a list of member accounts to a behavior graph (Console)

From the Detective console, you can provide a `.csv` file containing a list of member accounts to invite to your behavior graph.

The first line in the file is the header row. Each account is then listed on a separate line. Each member account entry contains the AWS account ID and the account's root user email address.

Example:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

When Detective processes the file, it ignores accounts that were already invited, unless the account status is **Verification failed**. That status indicates that the email address provided for the account did not match the account's root user email address. In that case, Detective deletes the original invitation and tries again to verify the email address and send the invitation.

This option also provides a template that you can use to create the list of accounts.

To invite member accounts from a .csv list (console)

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

2. In the Detective navigation pane, choose **Account management**.
3. Choose **Actions**. Then choose **Invite accounts**.
4. Under **Add accounts**, choose **Add from .csv**.
5. To download a template file to work from, choose **Download .csv template**.
6. To select the file containing the list of accounts, choose **Choose .csv file**.
7. Under **Review member accounts**, verify the list of member accounts that Detective found in the file.
8. Under **Personalize invitation email**, add customized content to include in the invitation email.

   For example, you can provide contact information, or remind the member account about the required IAM policy.
9. **Member account IAM policy** contains the text of the required IAM policy for member accounts. The email invitation includes this policy text. To copy the policy text, choose **Copy**.
10. Choose **Invite**.

Inviting member accounts to a behavior graph (Detective API, AWS CLI)

You can use the Detective API or the AWS Command Line Interface to invite member accounts to contribute their data to a behavior graph. To get the ARN of your behavior graph to use in the request, use the `ListGraphs` operation.

To invite member accounts to a behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `CreateMembers` operation. You must provide the graph ARN. For each account, specify the account identifier and the root user email address.

  To not send invitation emails to the member accounts, set `DisableEmailNotification` to true. By default, `DisableEmailNotification` is false .

  If you do send invitation emails, you can optionally provide custom text to add to the invitation email.
- **AWS CLI:** At the command line, run the `create-members` command.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --message "<Custom message
 text>"
```

Example

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
 Santos. I need to add your account to the data we use for security investigation in
 Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

To indicate to not send invitation emails to the member accounts, include `--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

Example

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
notification
```

Adding a list of member accounts across Regions (Python script on GitHub)

Detective provides an open-source script in GitHub that allows you to do the following:

- Add a specified list of member accounts to an administrator account's behavior graphs across a specified list of Regions.
- If the administrator account does not have a behavior graph in a Region, then the script also enables Detective and creates the behavior graph in that Region.
- Send invitation emails to the member accounts.
- Automatically accept the invitations for the member accounts.

For information on how to configure and use the GitHub scripts, see *Using the Amazon Detective Python scripts*.

Enabling a member account that is Not enabled

After a member account accepts an invitation, Amazon Detective checks the number of member accounts. The maximum number of member accounts for a behavior graph is 1,200. If your behavior graph already contains 1,200 member accounts, then new accounts cannot be enabled. If Detective cannot enable the member account, then it sets the member account status to **Not enabled**.

Member accounts that are **Not enabled** do not contribute data to the behavior graph.

Detective automatically enables accounts as the behavior graph can accommodate them.

You can also try to enable member accounts manually that are **Not enabled** member accounts. For example, you might remove existing member accounts to reduce the data volume. Instead of waiting for the automatic process to enable accounts, you can try to enable **Not enabled** member accounts.

Enabling a member account that is Not enabled (Console)

The member account list includes an option to enable selected member accounts that are **Not enabled.**

To enable a member account that is Not enabled

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.
3. Under **My member accounts**, select the check box for each member account to enable.

   You can only enable member accounts that have a status of **Not enabled**.
4. Choose **Enable accounts**.

Detective determines whether the member account can be enabled. If the member account can be enabled, the status changes to **Enabled**.

Enabling a member account that is Not enabled (Detective API, AWS CLI)

You can use an API call or the AWS Command Line Interface to enable a single member account that is **Not enabled**. To get the ARN of your behavior graph to use in the request, use the `ListGraphs` operation.

To enable a member account that is Not enabled

- **Detective API:** Use the `StartMonitoringMember` API operation. You must provide the behavior graph ARN. To identify the member account, use the AWS account identifier.
- **AWS CLI:** At the command line, run the `start-monitoring-member` command:

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

For example:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Removing invited member accounts from a behavior graph

The administrator account can remove member accounts from a behavior graph at any time.

Detective automatically removes member accounts that are terminated in AWS, except in the AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions.

When an invited member account is removed from a behavior graph, the following occurs.

- The member account is removed from **My member accounts**.
- Amazon Detective stops ingesting data from the removed account.

Detective does not remove any existing data from the behavior graph, which aggregates data across member accounts.

Removing invited member accounts from a behavior graph (console)

You can use the AWS Management Console to remove invited member accounts from your behavior graph.

To remove member accounts (console)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.

3. In the account list, select the check box for each member account to remove.

   You cannot remove your own account from the list.

4. Choose **Actions**. Then choose **Disable accounts**.

Removing invited member accounts from a behavior graph (Detective API, AWS CLI)

You can use the Detective API or the AWS Command Line Interface to remove invited member accounts from your behavior graph. To get the ARN of your behavior graph to use in the request, use the `ListGraphs` operation.

To remove invited member accounts from your behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `DeleteMembers` operation. Specify the graph ARN and the list of account identifiers for the member accounts to remove.
- **AWS CLI:** At the command line, run the `delete-members` command.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Example:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Removing a list of invited member accounts across Regions (Python script on GitHub)

Detective provides an open-source script in GitHub. You can use this script to remove a specified list of member accounts from an administrator account's behavior graphs across a specified list of Regions.

For information on how to configure and use the GitHub scripts, see *Using the Amazon Detective Python scripts*.

For member accounts: Managing behavior graph invitations and memberships

Amazon Detective charges each member account for the ingested data for each behavior graph that it contributes to.

The **Account management** page allows member accounts to see the administrator accounts for the behavior graphs they are a member of.

Member accounts that are invited to a behavior graph can view and respond to their invitations. They can also remove their account from the behavior graph.

For the organization behavior graph, organization accounts do not control whether their account is a member account. The Detective administrator account chooses the organization accounts to enable or disable as member accounts.

Contents

Required IAM policy for a member account

Before a member account can view and manage invitations, the required IAM policy must be attached to their principal. The principal can be an existing user or role, or you can create a new user or role to use for Detective.

Ideally, the administrator account has their IAM administrator attach the required policy.

The member account IAM policy grants access to member account actions in Amazon Detective. The email invitation to contribute to a behavior graph includes the text of that IAM policy.

To use this policy, replace *<behavior graph ARN>* with the graph ARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

Note that organization accounts in the organization behavior graph do not receive invitations and cannot disassociate their account from the organization behavior graph. If they do not belong to other behavior graphs, then they only require the `ListInvitations` permission. `ListInvitations` allows them to see the administrator account for the behavior graph. The permissions to manage invitations and disassociate memberships only apply to memberships by invitation.

Viewing your list of behavior graph invitations

From the Amazon Detective console, Detective API, or AWS Command Line Interface, a member account can see their behavior graph invitations.

Viewing behavior graph invitations (console)

You can view behavior graph invitations from the AWS Management Console.

To view behavior graph invitations (console)

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.

2. In the Detective navigation pane, choose **Account management**.

On the **Account management** page, **My administrator accounts** contains your open and accepted behavior graph invitations in the current Region. For an organization account, **My administrator accounts** also contains the organization behavior graph.

If your account is currently in the free trial period, the page also displays the number of days remaining in your free trial.

The list does not contain invitations that you declined, memberships that you resigned, or memberships that the administrator account removed.

Each invitation shows the administrator account number, the date that the invitation was accepted, and the current status of the invitation.

- For invitations that you have not responded to, the status is **Invited**.
- For invitations that you accepted, the status is either **Enabled** or **Not enabled**.

  If the status is **Enabled**, then your account contributes data to the behavior graph.

  If the status is **Not enabled**, then your account does not contribute data to the behavior graph.

  If your account would not cause the behavior graph to exceed the Detective quota, Detective updates your account status to **Enabled**. Otherwise, the status remains **Not enabled**.

  When the behavior graph is able to accommodate the data volume for your account, Detective automatically updates it to **Enabled**. For example, the administrator account might remove other member accounts so that your account can be enabled. The administrator account can also enable your account manually.

Viewing behavior graph invitations (Detective API, AWS CLI)

You can list behavior graph invitations from the Detective API or the AWS Command Line Interface.

To retrieve a list of open and accepted invitations to behavior graphs (Detective API, AWS CLI)

- **Detective API:** Use the `ListInvitations` operation.
- **AWS CLI:** At the command line, run the `list-invitations` command.

```
aws detective list-invitations
```

Responding to a behavior graph invitation

After you accept an invitation, Detective checks the number of member accounts. The maximum number of member accounts for a behavior graph is 1,200. If your behavior graph already contains 1,200 member accounts, then new accounts cannot be enabled.

After you accept the invitation, Detective is enabled in your account. Detective checks whether your data volume is within the Detective quota. The volume of data flowing into a behavior graph must be less than the maximum allowed by Detective. If the current volume ingested is above the limit of 10 TB per day, you cannot add more accounts and Detective will disable further ingestion of data. The Detective console displays a notification to indicate that data volume is too large and the status remains **Not enabled**.

If you decline the invitation, then it is removed from your list of invitations, and Detective does not use your account data in the behavior graph.

Responding to a behavior graph invitation (console)

You can use the AWS Management Console to respond to the email invitation, which includes a link to the Detective console. You can only respond to an invitation that has a status of **Invited**.

To respond to a behavior graph invitation (console)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.
3. Under **My administrator accounts**, to accept the invitation and begin contributing data to the behavior graph, choose **Accept invitation**.

   To decline the invitation and remove it from the list, choose **Decline**.

Responding to a behavior graph invitation (Detective API, AWS CLI)

You can respond to behavior graph invitations from the Detective API or the AWS Command Line Interface.

To accept a behavior graph invitation (Detective API, AWS CLI)

- **Detective API:** Use the `AcceptInvitation` operation. You must specify the graph ARN.
- **AWS CLI:** At the command line, run the `accept-invitation` command.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Example:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

To decline a behavior graph invitation (Detective API, AWS CLI)

- **Detective API:** Use the `RejectInvitation` operation. You must specify the graph ARN.
- **AWS CLI:** At the command line, run the `reject-invitation` command.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Example:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Removing your account from a behavior graph

After you accept an invitation, you can remove your account from a behavior graph at any time. When you remove your account from a behavior graph, Amazon Detective stops ingesting data from your account into the behavior graph. Existing data remains in the behavior graph.

Only invited accounts can remove their account from a behavior graph. Organization accounts cannot remove their account from the organization behavior graph.

Removing your account from a behavior graph (Console)

You can use the AWS Management Console to remove your account from a behavior graph.

To remove your account from a behavior graph (console)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, choose **Account management**.
3. Under **My administrator accounts**, for the behavior graph you want to resign from, choose **Resign**.

Removing your account from a behavior graph (Detective API, AWS CLI)

You can use the Detective API or the AWS Command Line Interface to remove your account from a behavior graph.

To remove your account from a behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `DisassociateMembership` operation. You must specify the graph ARN.
- **AWS CLI:** At the command line, run the `disassociate-membership` command.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Example:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Effect of account actions on behavior graphs

These actions have the following effects on Amazon Detective data and access.

Detective disabled

When an administrator account disables Detective, the following occurs:

- The behavior graph is removed.
- Detective stops ingesting data from the administrator account and the member accounts for that behavior graph.

Member account removed from the behavior graph

When a member account is removed from a behavior graph, Detective stops ingesting data from that account.

Existing data in the behavior graph is not affected.

For invited accounts, the account is removed from the **My member accounts** list.

For organization accounts in the organization behavior graph, the account status changes to **Not a member**.

Member account leaves the organization

When a member account leaves an organization, the following occurs:

- The account is removed from the **My member accounts** list for the organization behavior graph.
- Detective stops ingesting data from that account.

Existing data in the behavior graph is not affected.

AWS account suspended

When an administrator account is suspended in AWS, the account loses permission to view the behavior graph in Detective. Detective stops ingesting data into the behavior graph.

When a member account is suspended in AWS, Detective stops ingesting data for that account.

After 90 days, the account is either terminated or reactivated. When an administrator account is reactivated, its Detective permissions are restored. Detective resumes the ingest of data from the account. When a member account is reactivated, Detective resumes the ingest of data from the account.

AWS account closed

When an AWS account is closed, Detective responds to the closure as follows.

- For an administrator account, Detective deletes the behavior graph.
- For a member account, Detective removes the account from the behavior graph.

AWS retains the policy data for the account for 90 days from the effective date of the administrator account closure. At the end of the 90 day period, AWS permanently deletes all policy data for the account.

- To retain findings for more than 90 days, you can archive the policies. You can also use a custom action with an EventBridge rule to store the findings in an S3 bucket.
- As long as AWS retains the policy data, when you reopen the closed account, AWS reassigns the account as the service administrator and recovers the service policy data for the account.
- For more information, see Closing an account.

Important

For customers in the AWS GovCloud (US) Regions:

- Before closing your account, back up and then delete account resources. You will no longer have access to them after you close the account.

Tracking actions and usage in Amazon Detective

To help you to track your Detective activity, the **Usage** page shows the amount of data ingested and the projected cost.

- For administrator accounts, the **Usage** page shows the data volume and projected cost across the entire behavior graph.
- For member accounts, the **Usage** page shows the data volume and projected cost for their account across the behavior graphs that they contribute to.

Detective also supports AWS CloudTrail logging.

Contents

Monitoring usage and cost for a behavior graph (administrator account)

Amazon Detective bills each account for the data used in each behavior graph that the account belongs to. Detective charges a tiered flat rate per GB for all data regardless of the source.

For administrator accounts, the **Usage** page of the Detective console allows you to view the volume of data ingested **By data source** or **By account** over the previous 30 days. Administrator accounts also see a projected cost for a typical 30-day period for their account and for the entire behavior graph.

To view Detective usage information

1. Sign in to the AWS Management Console. Then open the Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, under **Settings**, choose **Usage**.
3. Choose a tab to select between viewing usage **By data source** or **By account**.

Volume of data ingested for each account

Ingested volume by member account lists the active accounts in the behavior graph. It does not list member accounts that were removed.

For each account, the ingested volume list provides the following information.

- The AWS account identifier and root user email address.
- The date when the account began to contribute data to the behavior graph.

  For the administrator account, this is the date when the account enabled Detective.

  For member accounts, this is the date when an account was enabled as a member account after accepting the invitation.
- The volume of ingested data from the account over the previous 30 days. The total includes all source types.
- Whether the account is currently in the free trial period. For accounts that are currently in their free trial period, the list displays the number of days remaining.

  If none of the accounts are in the free trial period, then the free trial status column is not displayed.

Projected costs for the behavior graph

This account's projected cost shows a projected cost for 30 days of data for the administrator account. The projected cost is based on the daily average volume for the administrator account.

> **Important**
>
> This amount is a projected cost only. It projects the total cost for the administrator account data for a typical 30-day time period. It is based on the usage from the previous 30 days. See the section called “How Detective calculates projected cost”.

Projected cost for the behavior graph

All accounts' projected cost shows a total projected cost for 30 days of data for the entire behavior graph. The projected cost is based on the daily average volume for each account.

Important

This amount is a projected cost only. It projects the total cost for the behavior graph data for a typical 30-day time period. It is based on the usage from the previous 30 days. The projected cost does not include member accounts that were removed from the behavior graph. See the section called "How Detective calculates projected cost".

Volume of data ingested by source packages

Select **By source package** to view the volume of data ingested listed by the different source packages enabled in your behavior graph.

All accounts can view this data for their own accounts. An administrator account can see additional panels that list the usage by source package for each member. It does not list member accounts that were removed.

Detective core

Detective core panels show the volume of data ingested from Detective core sources (CloudTrail logs, VPC Flow logs, and GuardDuty findings) for the last 30 days.

EKS audit logs

EKS audit logs panels show the volume of data ingested from EKS audit logs sources for the last 30 days. Panels for this source package are only available if EKS audit logs is enabled for your behavior graph.

Monitoring usage and cost across behavior graphs (member account)

Amazon Detective bills each account for the data used in each behavior graph that the account belongs to. Detective charges a tiered flat rate per GB for all data regardless of the source.

For member accounts, the **Usage** page shows the volume of data and projected 30-day cost for that account only.

To view Detective usage information

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

Ingested volume for each behavior graph

This account's ingested volume lists the behavior graphs that the member account contributes to. It does not include memberships that you resigned, or memberships that the administrator account removed.

For each behavior graph, the list includes the following information.

- The account number of the administrator account
- The volume of ingested data from the member account over the previous 30 days. The total includes all source types.
- The date when the member account was enabled for the behavior graph.

Projected cost across behavior graphs

This account's projected cost shows a projected cost for 30 days of data for the member account across all of the behavior graphs that it contributes to. The projected cost is based on the daily average volume for the member account.

> **Important**
>
> This amount is a projected cost only. It projects the total cost for the administrator account data for a typical 30-day time period. It is based on the usage from the previous 30 days. See the section called “How Detective calculates projected cost”.

How Amazon Detective calculates projected cost

To calculate the projected cost values that it displays on the **Usage** page, Detective does the following.

1. To get the projected cost for an individual account in a behavior graph, Detective does the following.
   a. Calculates the average volume per day. It adds the data volume across all of the active days and then divides by the number of days that the account has been active.

      If the account was enabled more than 30 days ago, then the number of days is 30. If the account was enabled fewer than 30 days ago, then it is the number of days since the acceptance date.

      For example, if the account was enabled 12 days ago, then Detective adds the volume ingested for those 12 days and then divides it by 12.
   b. Multiplies the account's daily average by 30. This is the projected 30-day usage for the account.
   c. Uses its pricing model to calculate the projected 30-day cost for the projected 30-day usage.
2. To get the total projected cost for a behavior graph, Detective does the following:
   a. Combines the projected 30-day usage from all of the accounts in the behavior graph.
   b. Uses its pricing model to calculate the projected 30-day cost for the total projected 30-day usage.
3. To get the total projected cost for a member account across behavior graphs, Detective does the following:
   a. Combines the projected 30-day usage across all of the behavior graphs.
   b. Uses its pricing model to calculated the projected 30-day cost for the total projected 30-day usage.
4. If you are using a shared Amazon VPC, Detective calculates the projected cost based on monitoring activity. We recommend that you review the projected cost for your investigations specific to your environment.
   a. If a Detective member account has a shared Amazon VPC and there are other non-Detective accounts using the shared VPC, Detective will monitor all traffic from that VPC. The usage and cost will increase and Detective will provide visualization on all the traffic flow within the VPC.
   b. If you have an EC2 instance inside a shared Amazon VPC and the shared owner is not a Detective member, Detective will not monitor any traffic from the VPC, and the usage and cost will decrease. 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.

Logging Amazon Detective API calls with AWS CloudTrail

Detective is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Detective. CloudTrail captures all API calls for Detective as events. The calls captured include calls from the Detective console and code calls to the Detective API operations.

- If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Detective.
- If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**.

Using the information collected by CloudTrail, you can determine the following:

- The request that was made to Detective
- The IP address from which the request was made
- Who made the request
- When it was made
- Additional details about the request

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Detective information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Detective, that activity is recorded in a CloudTrail event, along with other AWS service events, in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Detective, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket.

By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. You also can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs.

For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

CloudTrail logs all Detective operations, which are documented in the Detective API Reference.

For example, calls to the `CreateMembers`, `AcceptInvitation`, and `DeleteMembers` operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials
- Whether the request was made with temporary security credentials for a role or a federated user
- Whether the request was made by another AWS service

For more information, see the CloudTrail userIdentity Element.

Understanding Detective log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries.

An event represents a single request from any source. Events include information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so the entries don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `AcceptInvitation` action.

```
{
```

```
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn
\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId
\":\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":
{\"attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z
\"},\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS
\",\"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":
\"111122223333\",\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z
\",\"eventSource\":\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation
\",\"awsRegion\":\"us-east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent
\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/
AWS_Lambda_java8\",\"errorCode\":\"ValidationException\",\"requestParameters\":
{\"masterAccount\":\"111111111111\"},\"responseElements\":{\"message\":\"Invalid
 request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f\",\"eventID\":
\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":\"AwsApiCall
\",\"recipientAccountId\":\"111122223333\"}",
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
        },
```

Managing tags for a behavior graph

You can assign tags to your behavior graph. You can then use the tag values in IAM policies to manage access to behavior graph functions in Detective. See the section called "Authorization based on Detective behavior graph tags".

You also can use tags as a tool for cost reporting. For example, to track costs associated with security, you could assign the same tag to your Detective behavior graph, AWS Security Hub hub resource, and Amazon GuardDuty detectors. In AWS Cost Explorer, you could then search for that tag to see a consolidated view of the costs across those resources.

Viewing the tags for a behavior graph (Console)

You manage the tags for your behavior graph from the **General** page.

To view the list of tags assigned to the behavior graph

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the navigation pane, under **Settings**, choose **General**.

Listing the tags for a behavior graph (Detective API, AWS CLI)

You can use the Detective API or the AWS Command Line Interface to get the list of tags for your behavior graph.

To get the list of tags for a behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `ListTagsForResource` operation. You must provide the ARN of your behavior graph.
- **AWS CLI:** At the command line, run the `list-tags-for-resource` command.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Example

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Adding tags to a behavior graph (Console)

From the tag list on the **General** page, you can add tag values to the behavior graph.

To add a tag to your behavior graph

1. Choose **Add new tag**.
2. For **Key**, enter the name of the tag.
3. For **Value**, enter the value of the tag.

Adding tags to a behavior graph (Detective API, AWS CLI)

You can use the Detective API or the AWS CLI to add tag values to your behavior graph.

To add tags to a behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `TagResource` operation. You provide the behavior graph ARN and the tag values to add.
- **AWS CLI**: At the command line, run the `tag-resource` command.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

Example

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

Removing tags from a behavior graph (Console)

To remove a tag from the list on the **General** page, choose the **Remove** option for that tag.

Removing tags from a behavior graph (Detective API, AWS CLI)

You can use the Detective API or the AWS CLI to remove tag values from your behavior graph.

To remove tags from a behavior graph (Detective API, AWS CLI)

- **Detective API:** Use the `UntagResource` operation. You provide the behavior graph ARN, and the names of the tags to remove.
- **AWS CLI**: At the command line, run the `untag-resource` command.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

Example

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Security in Amazon Detective

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely.

  Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs.

  To learn about the compliance programs that apply to Amazon Detective, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Detective. The following topics show you how to configure Detective to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Detective resources.

Contents

- Security best practices for Amazon Detective

Data protection in Amazon Detective

The AWS shared responsibility model applies to data protection in Amazon Detective. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Detective or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Detective encrypts all data that it processes and stores at rest and in transit.

Contents

Key management for Amazon Detective

Because Detective does not store any personally identifiable customer data, it uses AWS managed keys.

This type of KMS key can be used across multiple accounts. See the description of AWS owned keys in the AWS Key Management Service Developer Guide.

This type of KMS key rotates automatically every one year (approximately 365 days). See the description of key rotation in the AWS Key Management Service Developer Guide.

Identity and access management for Amazon Detective

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Detective resources. IAM is an AWS service that you can use with no additional charge.

Contents

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Detective.

Service user – If you use the Detective service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Detective features to do your

work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Detective, see Troubleshooting Amazon Detective identity and access.

Service administrator – If you're in charge of Detective resources at your company, you probably have full access to Detective. It's your job to determine which Detective features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Detective, see How Amazon Detective works with IAM.

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Detective. To view example Detective identity-based policies that you can use in IAM, see Amazon Detective identity-based policy examples.

Authenticating With Identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Signing AWS API requests in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the

AWS IAM Identity Center User Guide and Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

IAM Users and Groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the *IAM User Guide*.

IAM Roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.
  - **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.
  - **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked

roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see When to create an IAM role (instead of a user) in the *IAM User Guide*.

Managing Access Using Policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-Based Policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can

perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the *IAM User Guide*.

Resource-Based Policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access Control Lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

Other Policy Types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the

intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

Multiple Policy Types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How Amazon Detective works with IAM

By default, users and roles don't have permission to create or modify Amazon Detective resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. A Detective administrator must have AWS Identity and Access Management (IAM) policies that grant IAM users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the principal that require those permissions.

Detective uses IAM identity-based policies to grant permissions for the following types of users and actions:

- **Administrator accounts** – The administrator account is the owner of a behavior graph, which uses data from their account. Administrator accounts can invite member accounts to contribute

their data to the behavior graph. They also use the behavior graph for triage and investigation of findings and resources associated with those accounts.

You can set up policies to allow users other than the administrator account to perform different types of tasks. For example, a user from an administrator account might only have permissions to manage member accounts. Another user might only have permissions to use the behavior graph for investigation.

- **Member accounts** – A member account is an account that is invited to contribute data to a behavior graph. A member account responds to an invitation. After accepting an invitation, a member account can remove their account from the behavior graph.

To get a high-level view of how Detective and other AWS services work with IAM, see Creating policies on the JSON tab in the *IAM User Guide*.

Detective identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources, as well as the conditions under which actions are allowed or denied. Detective supports specific actions, resources, and condition keys.

To learn about all of the elements that you use in a JSON policy, see IAM JSON Policy Elements Reference in the *IAM User Guide*.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Policy statements must include either an `Action` element or a `NotAction` element. The `Action` element lists the actions allowed by the policy. The `NotAction` element lists the actions that are not allowed.

The actions defined for Detective reflect tasks that you can perform using Detective. Policy actions in Detective have the following prefix: `detective:`.

For example, to grant permission to use the `CreateMembers` API operation to invite member accounts to a behavior graph, you include the `detective:CreateMembers` action in their policy.

To specify multiple actions in a single statement, separate them with commas. For example, for a member account, the policy includes the set of actions related to managing an invitation:

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

You can also use wildcards (*) to specify multiple actions. For example, to manage the data used in their behavior graph, administrator accounts in Detective must be able to perform the following tasks:

- View their list of member accounts (`ListMembers`).
- Get information about selected member accounts (`GetMembers`).
- Invite member accounts to their behavior graph (`CreateMembers`).
- Remove members from their behavior graph (`DeleteMembers`).

Instead of listing these actions separately, you can grant access to all actions that end with the word `Members`. The policy for that could include the following action:

```
"Action": "detective:*Members"
```

To see a list of Detective actions, see Actions defined by Amazon Detective in the *Service Authorization Reference*.

Resources

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

For Detective, the only resource type is the behavior graph. The behavior graph resource in Detective has the following ARN:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

For example, a behavior graph has the following values:

- The Region for the behavior graph is `us-east-1`.
- The account ID for the administrator account ID is `111122223333`.
- The graph ID of the behavior graph is `027c7c4610ea4aacaf0b883093cab899`.

To identify this behavior graph in a `Resource` statement, you would use the following ARN:

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

To specify multiple resources in a `Resource` statement, use commas to separate them.

```
"Resource": [
      "resource1",
      "resource2"
]
```

For example, the same AWS account may be invited to be a member account in more than one behavior graph. In the policy for that member account, the `Resource` statement would list the behavior graphs they were invited to.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

Some Detective actions, such as creating a behavior graph, listing behavior graphs, and listing behavior graph invitations, are not performed on a specific behavior graph. For those actions, the `Resource` statement must use the wildcard (*).

```
"Resource": "*"
```

For administrator account actions, Detective always verifies that the user making the request belongs to the administrator account for the affected behavior graph. For member account actions, Detective always verifies that the user making the request belongs to the member account. Even if an IAM policy grants access to a behavior graph, if the user does not belong to the correct account, the user cannot perform the action.

For all actions that are performed on a specific behavior graph, the IAM policy should include the graph ARN. The graph ARN can be added later. For example, when an account first enables Detective, the initial IAM policy provides access to all Detective actions, using the wildcard for the graph ARN. This allows the user to immediately start to manage member accounts for and conduct investigations in their behavior graph. After the behavior graph is created, you can update the policy to add the graph ARN.

Condition keys

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

Detective does not define its own set of condition keys. It does support using global condition keys. To see all AWS global condition keys, see AWS Global Condition Context Keys in the *IAM User Guide*.

To learn which actions and resources allow you to use a condition key, see Actions defined by Amazon Detective.

Examples

To view examples of Detective identity-based policies, see Amazon Detective identity-based policy examples.

Detective resource-based policies (Not supported)

Detective does not support resource-based policies.

Authorization based on Detective behavior graph tags

Each behavior graph can be assigned tag values. You can use those tag values in condition statements to manage access to the behavior graph.

The condition statement for a tag value uses the following format.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

For example, use the following code to allow or deny an action when the value of the `Department` tag is `Finance`.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

For examples of policies that use resource tag values, see the section called “Administrator account: Restricting access based on tag values”.

Detective IAM Roles

An IAM role is an entity within your AWS account that has specific permissions.

Using temporary credentials with Detective

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Detective supports using temporary credentials.

Service-linked roles

Service-linked roles allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

For details about creating or managing Detective service-linked roles, see the section called “Using service-linked roles”.

Service roles (Not supported)

This feature allows a service to assume a service role on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

Detective does not support service roles.

Amazon Detective identity-based policy examples

By default, IAM users and roles don't have permission to create or modify Detective resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API.

An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator then attaches those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating Policies on the JSON Tab in the *IAM User Guide*.

Topics

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Detective resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to

specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.

- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see IAM Access Analyzer policy validation in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Configuring MFA-protected API access in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the Detective console

To use the Amazon Detective console, the user or role must have access to the relevant actions, which match corresponding actions in the API.

To enable Detective and become an administrator account for a behavior graph, the user or role must be granted permission for the `CreateGraph` action.

To use the Detective console to perform any administrator account actions, the user or role must be granted permission for the `ListGraphs` action. This grants permission to retrieve the behavior graphs their account is an administrator account for. They also must be granted permission to perform specific administrator account actions.

The most basic administrator account actions are to view a list of member accounts in a behavior graph, and to use the behavior graph for investigation.

- To view the list of member accounts in a behavior graph, the principal must be granted permission for the `ListMembers` action.
- To conduct investigation in a behavior graph, the principal must be granted permission for the `SearchGraph` action.

To use the Detective console to perform any member account actions, the user or role must be granted permission for the `ListInvitations` action. This grants permission to view behavior graph invitations. They can then be granted permission for specific member account actions.

Allowing users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Administrator account: Managing the member accounts in a behavior graph

This example policy is intended for administrator account users who are only responsible for managing the member accounts used in the behavior graph. The policy also allows the user to view the usage information and deactivate Detective. The policy does not grant permission to use the behavior graph for investigation.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Administrator account: Using a behavior graph for investigation

This example policy is intended for administrator account users who use the behavior graph for investigation only. They cannot view or edit the list of member accounts in the behavior graph.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
```

```
 ]
}
```

Member account: Managing behavior graph invitations and memberships

This example policy is intended for users belonging to a member account. In the example, the member account belongs to two behavior graphs. The policy grants permission to respond to invitations and remove the member account from the behavior graph.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

Administrator account: Restricting access based on tag values

The following policy allows the user to use a behavior graph for investigation if the `SecurityDomain` tag of the behavior graph matches the `SecurityDomain` tag of the user.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
```

```
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
        "Resource":"*"
    } ]
}
```

The following policy prevents the users from using a behavior graph for investigation if the value of the `SecurityDomain` tag for the behavior graph is `Finance`.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

Troubleshooting Amazon Detective identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Detective and IAM. If you encounter access-denied issues or similar difficulties when working with AWS Identity and Access Management(IAM), consult the Troubleshooting IAM topics in the *IAM User Guide*.

I am not authorized to perform an action in Detective

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

The following example error occurs when the `mateojackson` IAM user tries to use the console to accept an invitation to become a member account for a behavior graph, but does not have `detective:AcceptInvitation` permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

In this case, Mateo asks his administrator to update his policies to allow him to access the `arn:aws:detective:us-east-1:444455556666:graph:567856785678` resource using the `detective:AcceptInvitation` action.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Detective.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Detective. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Detective resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Detective supports these features, see How Amazon Detective works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.

Using service-linked roles for Detective

Amazon Detective uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Detective. Service-linked roles are predefined by Detective and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Detective easier because you do not have to manually add the necessary permissions. Detective defines the permissions of its service-linked roles, and unless defined otherwise, only Detective can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Detective resources because you cannot inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Detective

Detective uses the service-linked role named **AWSServiceRoleForDetective** – Allows Detective to access AWS Organizations information on your behalf.

The AWSServiceRoleForDetective service-linked role trusts the following services to assume the role:

- `detective.amazonaws.com`

The AWSServiceRoleForDetective service-linked role uses the managed policy `AmazonDetectiveServiceLinkedRolePolicy`.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for Detective

You do not need to manually create a service-linked role. When you designate the Detective administrator account for an organization in the AWS Management Console, the AWS CLI, or the AWS API, Detective creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you designate the Detective administrator account for an organization, Detective creates the service-linked role for you again.

Editing a service-linked role for Detective

Detective does not allow you to edit the AWSServiceRoleForDetective service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Deleting a service-linked role for Detective

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

> **Note**
>
> If the Detective service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and then try the operation again.

To delete Detective resources used by the AWSServiceRoleForDetective

1. Remove the Detective administrator account. See the section called "Designating the Detective administrator account".
2. Repeat the process in each Region where you designated the Detective administrator account.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForDetective service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Detective service-linked roles

Detective supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Regions and Endpoints.

AWS managed policies for Amazon Detective

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the *IAM User Guide*.

AWS managed policy: AmazonDetectiveFullAccess

You can attach the `AmazonDetectiveFullAccess` policy to your IAM identities.

This policy grants administrative permissions that allow a principal full access to all Amazon Detective actions. You can attach this policy to a principal before they enable Detective for their account. It must also be attached to the role that is used to run the Detective Python scripts to create and manage a behavior graph.

Principals with these permissions can manage member accounts, add tags to their behavior graph, and use Detective for investigation. They can also archive GuardDuty findings. The policy provides permissions that the Detective console needs to display account names for accounts that are in AWS Organizations.

Permissions details

This policy includes the following permissions:

- `detective` – Allows principals full access to all Detective actions.
- `organizations` – Allows principals to retrieve from AWS Organizations information about the accounts in an organization. If an account belongs to an organization, these permissions allow the Detective console to display account names in addition to account numbers.
- `guardduty` – Allows principals to get and archive GuardDuty findings from within Detective.
- `securityhub` – Allows principals to get Security Hub findings from within Detective.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "detective:*",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
            "Resource": "*"
         }
    ]
}
```

AWS managed policy: AmazonDetectiveMemberAccess

You can attach the `AmazonDetectiveMemberAccess` policy to your IAM entities.

This policy provides member access to Amazon Detective and scoped access to the console.

With this policy, you can:

- View invitations to Detective graph membership and accept or reject those invitations.
- View how your activity in Detective contributes to the cost of using this service on the **Usage** page.
- Resign from your membership in a graph.

This policy grants read-only permissions that allow scoped access to the Detective console.

Permissions details

This policy includes the following permissions:

- `detective` – Allows member access to Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS managed policy: AmazonDetectiveInvestigatorAccess

You can attach the `AmazonDetectiveInvestigatorAccess` policy to your IAM entities.

This policy provides investigator access to the Detective service and scoped access to the Detective console UI dependencies. This policy grants permissions to enable Detective investigations in Detective for IAM users and IAM roles. You can investigate to identify indicators of compromise

such as findings using an investigation report, which provides analysis and insights about security indicators. The report is ranked by severity, which is determined using Detective's behavioral analysis and machine learning. You can use the report to prioritize remediation of resources.

Permissions details

This policy includes the following permissions:

- `detective` – Allows principals investigator access to Detective actions, to enable Detective investigations, and to enable finding groups summary.
- `guardduty` – Allows principals to get and archive GuardDuty findings from within Detective.
- `securityhub` – Allows principals to get Security Hub findings from within Detective.
- `organizations` – Allows principals to retrieve information about the accounts in an organization from AWS Organizations. If an account belongs to an organization, then these permissions allow the Detective console to display account names in addition to account numbers.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
```

```
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityHub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS managed policy: AmazonDetectiveOrganizationsAccess

You can attach the `AmazonDetectiveOrganizationsAccess` policy to your IAM entities.

This policy grants permission to enable and manage Amazon Detective within an organization. You can enable Detective across the organization and determine the delegated administrator account for Detective.

Permissions details

This policy includes the following permissions:

- `detective` – Allows principals access to Detective actions.
- `iam` – Specifies that a service linked role is created when Detective calls `EnableOrganizationAdminAccount`.
- `organizations` – Allows principals to retrieve information about the accounts in an organization from AWS Organizations. If an account belongs to an organization, then these permissions allow the Detective console to display account names in addition to account numbers. Enables the integration of an AWS service, allows register and deregister of the specified member account as a Delegated administrator, and allows principals to retrieve Delegated administrator accounts in other security services like Amazon Detective, Amazon GuardDuty, Amazon Macie, and AWS Security Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
```

```
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWS managed policy: AmazonDetectiveServiceLinkedRole

You can't attach the `AmazonDetectiveServiceLinkedRole` policy to your IAM entities. This policy is attached to a service-linked role that allows Detective to perform actions on your behalf. For more information, see the section called “Using service-linked roles”.

This policy grants administrative permissions that allow the service-linked role to retrieve account information for an organization.

Permissions details

This policy includes the following permissions:

- `organizations` – Retrieves account information for an organization.

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

Detective updates to AWS managed policies

View details about updates to AWS managed policies for Detective since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Document history page.

Change	Description	Date
AmazonDetectiveInvestigatorAccess – Updates to existing policies	Added Detective investigations and finding groups summary actions to the `AmazonDetectiveInvestigatorAccess` policy. These actions allow starting, retrieving, and updating Detective investigations; and obtaining a summary of finding groups from within Detective.	November 26, 2023
AmazonDetectiveFullAccess and AmazonDetectiveInvestigatorAccess – Updates to existing policies	Detective added Security Hub `GetFindings` actions to the `AmazonDetectiveFullAccess` and `AmazonDetectiveInvestigatorAccess` policies. These actions allow getting Security Hub findings from within Detective.	May 16, 2023
AmazonDetectiveOrganizationsAccess – New policy	Detective added `AmazonDetectiveOrganizationsAccess` policy.	March 02, 2023

Change	Description	Date
	This policy grants permission to enable and manage Detective within an organization	
AmazonDetectiveMemberAccess – New policy	Detective added the `AmazonDetectiveMemberAccess` policy. This policy provides member access to Detective and scoped access to the console UI dependencies.	January 17, 2023
AmazonDetectiveFullAccess – Updates to an existing policy	Detective added GuardDuty `GetFindings` actions to the `AmazonDetectiveFullAccess` policy. These actions allow getting GuardDuty findings from within Detective.	January 17, 2023
AmazonDetectiveInvestigatorAccess – New policy	Detective added the `AmazonDetectiveInvestigatorAccess` policy. This policy allows the principal to conduct investigations in Detective.	January 17, 2023
AmazonDetectiveServiceLinkedRole – New policy	Detective added a new policy for its service-linked role. The policy allows the service-linked role to retrieve information about the accounts in an organization.	December 16, 2021
Detective started to track changes	Detective started to track changes for its AWS managed policies.	May 10, 2021

Logging and monitoring in Amazon Detective

Amazon Detective is integrated AWS CloudTrail. CloudTrail captures all API calls for Detective as events.

For details on using CloudTrail logging for Detective, see the section called "Logging Detective API calls with CloudTrail".

Compliance validation for Amazon Detective

Amazon Detective is in Scope of the AWS assurance program. For more information, see Health Information Trust Alliance Common Security Framework (HITRUST) CSF.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Evaluating resources with rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon Detective

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones

without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

In addition to the AWS global infrastructure, Detective makes use of the resiliency built into Amazon DynamoDB and Amazon Simple Storage Service (Amazon S3).

The Detective architecture is also resilient to the failure of a single Availability Zone. This resilience is built into Detective, and does not require any configuration.

Infrastructure security in Amazon Detective

As a managed service, Amazon Detective; is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Detective; through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Security best practices for Amazon Detective

Detective provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

For Detective, the security best practices are associated with managing the accounts in a behavior graph.

Best practices for administrator accounts

When inviting member accounts to your behavior graph, only invite accounts that you oversee.

Limit access to the behavior graph. When a user has access to a behavior graph, they can see all of the findings for the member accounts. Such findings might expose sensitive security information.

Best practices for member accounts

When you receive an invitation to a behavior graph, make sure to validate the source of the invitation.

Check the AWS account identifier of the administrator account that sent the invitation. Verify that you know who the account belongs to, and that the inviting account has a legitimate reason to monitor your security data.

Disabling Amazon Detective

The administrator account for a behavior graph can disable Amazon Detective from the Detective console, the Detective API, or AWS Command Line Interface. When you disable Detective, the behavior graph and its associated Detective data are deleted.

Once a behavior graph is deleted, it cannot be restored.

Contents

Disabling Detective (Console)

You can disable Amazon Detective from the AWS Management Console.

To disable Detective (console)

1. Open the Amazon Detective console at https://console.aws.amazon.com/detective/.
2. In the Detective navigation pane, under **Settings**, choose **General**.
3. On the **General** page, under **Disable Detective**, choose **Disable Detective**.
4. When prompted to confirm, type **`disable`**.
5. Choose **Disable Detective**.

Disabling Detective (Detective API, AWS CLI)

You can disable Amazon Detective from the Detective API or the AWS Command Line Interface. To get the ARN of your behavior graph to use in the request, use the `ListGraphs` operation.

To disable Detective (Detective API, AWS CLI)

- **Detective API:** Use the `DeleteGraph` operation. You must provide the graph ARN.
- **AWS CLI:** At the command line, run the `delete-graph` command.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Example:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Disabling Detective across Regions (Python script on GitHub)

Detective provides an open-source script in GitHub that allows you to disable Detective for an administrator account across a specified list of Regions.

For information on how to configure and use the GitHub scripts, see *Using the Amazon Detective Python scripts*.

Using the Amazon Detective Python scripts

Amazon Detective provides a set of open-source Python scripts in the GitHub repository amazon-detective-multiaccount-scripts. The scripts require Python 3.

You can use these to perform the following tasks:

- Enable Detective for an administrator account across Regions.

  When you enable Detective, you can assign tag values to the behavior graph.
- Add member accounts to an administrator account's behavior graphs across Regions.
- Optionally send invitation emails to the member accounts. You can also configure the request to not send invitation emails.
- Remove member accounts from an administrator account's behavior graphs across Regions.
- Disable Detective for an administrator account across Regions. When an administrator account disables Detective, the administrator account's behavior graph in each Region is disabled.

Overview of the `enableDetective.py` script

The `enableDetective.py` script does the following:

1. Enables Detective in for an administrator account in each specified Region, if the administrator account does not already have Detective enabled in that Region.

   When you use the script to enable Detective, you can assign tag values to the behavior graph.
2. Optionally sends invitations from the administrator account to the specified member accounts for each behavior graph.

   The invitation email messages use the default message content and cannot be customized.

   You can also configure the request to not send invitation emails.
3. Automatically accepts the invitations for the member accounts.

   Because the script automatically accepts the invitations, member accounts can ignore these messages.

We recommend reaching out directly to the member accounts to notify them that the invitations are accepted automatically.

Overview of the `disableDetective.py` script

The `disableDetective.py` script deletes the specified member accounts from the administrator account's behavior graphs across the specified Regions.

It also provides an option to disable Detective for the administrator account across the specified Regions.

Required permissions for the scripts

The scripts require a preexisting AWS role in the administrator account and in all of the member accounts that you add or remove.

> **Note**
>
> The role name must be the same in all of the accounts.

IAM policy recommended best practices are to use least scoped roles. To execute the script's workflow of creating a graph, creating members, and adding members to the graph the required permissions are:

- detective:CreateGraph
- detective:CreateMembers
- detective:DeleteGraph
- detective:DeleteMembers
- detective:ListGraphs
- detective:ListMembers
- detective:AcceptInvitation

Role trust relationship

The role trust relationship must allow your instance or local credentials to assume the role.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

If you do not have a common role that includes the required permissions, you must create a role with at least those permissions in each member account. You must also create the role in the administrator account.

When you create the role, make sure that you do the following:

- Use the same role name in every account.
- Add the required permissions above (recommended) or select the AmazonDetectiveFullAccess managed policy.
- Add role trust relationship block as discussed above.

To automate this process, you can use the `EnableDetective.yaml` AWS CloudFormation template. Because the template creates only global resources, it can be run in any Region.

Setting up the run environment for the Python scripts

You can run the scripts from either an EC2 instance or from a local machine.

Launching and configuring an EC2 instance

One option for running the scripts is to run them from an EC2 instance.

To launch and configure an EC2 instance

1. Launch an EC2 instance in your administrator account. For details on how to launch an EC2 instance, see Getting Started with Amazon EC2 Linux Instances in the *Amazon EC2 User Guide for Linux Instances*.

2. Attach to the instance an IAM role that has permissions to allow the instance to call `AssumeRole` within the administrator account.

   If you used the `EnableDetective.yaml` AWS CloudFormation template, then an instance role with a profile named `EnableDetective` was created.

   Otherwise, for information on creating an instance role, see the blog post Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console.
3. Install the required software:

   - **APT:** `sudo apt-get -y install python3-pip python3 git`
   - **RPM:** `sudo yum -y install python3-pip python3 git`
   - **Boto (minimum version 1.15):** `sudo pip install boto3`
4. Clone the repository to the EC2 instance.

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

Configuring a local machine to run the scripts

You can also run the scripts from your local machine.

To configure a local machine to run the scripts

1. Make sure that you have set up on your local machine credentials for your administrator account that have permission to call `AssumeRole`.
2. Install the required software:

   - Python 3
   - Boto (minimum version 1.15)
   - GitHub scripts

Platform	Setup instructions
Windows	1. Install Python 3 (https://www.python.org/downloads/windows/). 2. Open a command prompt.

Platform	Setup instructions
	3. To install Boto, run: `pip install boto3` 4. Download the script source code from GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Mac	1. Install Python 3 (https://www.python.org/downloads/mac-osx/). 2. Open a command prompt. 3. To install Boto, run: `pip install boto3` 4. Download the script source code from GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Linux	1. To install Python 3, run one of the following: • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. To install Boto, run: `sudo pip install boto3` 3. Clone the script source code from https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Creating a `.csv` list of member accounts to add or remove

To identify the member accounts to add to or remove from the behavior graphs, you provide a `.csv` file that contains the list of accounts.

List each account on a separate line. Each member account entry contains the AWS account ID and the account's root user email address.

See the following example:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Running enableDetective.py

You can run the enableDetective.py script from an EC2 instance or your local machine.

To run enableDetective.py

1. Copy the .csv file to the amazon-detective-multiaccount-scripts directory on your EC2 instance or local machine.
2. Change to the amazon-detective-multiaccount-scripts directory.
3. Run the enableDetective.py script.

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
disable_email
```

When you run the script, replace the following values:

administratorAccountID

The AWS account ID for the administrator account.

roleName

The name of the AWS role to assume in the administrator account and each member account.

inputFileName

The name of the .csv file containing the list of member accounts to add to the administrator account's behavior graphs.

tagValueList

(Optional) A comma-separated list of tag values to assign to a new behavior graph.

For each tag value, the format is *key*=*value*. For example:

```
--tags Department=Finance,Geo=Americas
```

regionList

(Optional) A comma-separated list of Regions in which to add the member accounts to the administrator account's behavior graph. For example:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

The administrator account might not already have Detective enabled in a Region. In that case, the script enables Detective and creates a new behavior graph for the administrator account.

If you do not provide a list of Regions, then the script acts across all Regions that Detective supports.

`--disable_email`

(Optional) If included, Detective does not send invitation emails to the member accounts.

Running `disableDetective.py`

You can run the `disableDetective.py` script from an EC2 instance or your local machine.

To run `disableDetective.py`

1. Copy the `.csv` file to the `amazon-detective-multiaccount-scripts` directory.
2. To use the `.csv` file to delete the listed member accounts from the administrator account's behavior graphs across a specified list of Regions, run the `disableDetective.py` script as follows:

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList
```

3. To disable Detective for the administrator account across all Regions, run the `disableDetective.py` script with the `--delete-master` flag.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList --delete_master
```

When you run the script, replace the following values:

`administratorAccountID`

The AWS account ID for the administrator account.

roleName

The name of the AWS role to assume in the administrator account and each member account.

inputFileName

The name of the `.csv` file containing the list of member accounts to remove from the administrator account's behavior graphs.

You must provide a `.csv` file even if you are disabling Detective.

regionList

(Optional) A comma-separated list of Regions in which to do one of the following:

- Remove the member accounts from the administrator account's behavior graphs.
- If the `--delete-master` flag is included, disable Detective.

For example:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

If you do not provide a list of Regions, then the script acts across all Regions that Detective supports.

Document history for Detective Administration 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:** February 02, 2024

Change	Description	Date
Removed the Amazon GuardDuty membership requirement	You are no longer required to be a GuardDuty customer to enable Amazon Detective . The requirement to have GuardDuty enabled in your account for 48 hours before enabling Detective has been removed.	February 2, 2024
Changes in how Detective reads the flow traffic for shared VPCs	If you are using a shared Amazon VPC, you may see changes in the traffic monitored by Detective. We recommend that you review the changes in Activity details for overall VPC flow volume to understand the potential effects on your coverage, and review how Detective calculates projected cost to understand how that can impact your service costs.	December 20, 2023
Added managed policy information to the security chapter	Added Detective investiga tions and finding groups summary actions to the	November 26, 2023

	`AmazonDetectiveInvestigatorAccess` policy.	
Amazon Detective endpoints and quotas	Detective is now available in the Israel (Tel Aviv) Region.	August 25, 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 new console panels in the Detective console to help users select the appropriate AWS managed policy for their specific use case.	Detective offers managed policies to securely choose the permissions that you need.	April 3, 2023
Added managed policy information to the security chapter	Detective now supports GuardDuty get findings actions through the AmazonDetectiveFullAccess policy. The security chapter now provides details about the following new managed policies for Detective: AmazonDetectiveMemberAccess and AmazonDetectiveInvestigatorAccess.	January 17, 2023
Added data retention	With Detective, you can access up to a year of historical event data.	December 20, 2022

Added terms related to finding groups	Detective now supports finding groups that connect related findings together in a single display to help you investigate potential malicious activity in your environment. From a finding group profile, you can pivot to entity profiles and finding overviews related to that group.	August 3, 2022
Added a new optional data source	Detective now supports EKS audit logs as an optional data source package. An administrator account can enable this new data source for their existing behavior graph. Graphs created after this date will have this data source enabled by default. Administrators can disable this data source manually at any time.	July 26, 2022
New service-linked role and managed policy for Detective	Detective now has a service-linked role, `AWSServiceRoleForDetective`. The service-linked role is used to access Organizations data on your behalf. The role uses a new `AmazonDetectiveServiceLinkedRolePolicy` managed policy.	December 16, 2021

Added integration with AWS Organizations	Detective is now integrated with Organizations. The organization management account designates a Detective administrator account for the organization. The Detective administrator account can view all of the accounts in the organization, and enable those accounts as member accounts in the organization behavior graph.	December 16, 2021
Updated values for behavior graph data volume quotas	Increased the data volume quotas for behavior graphs. At 3.24 TB per day, Detective issues a warning. At 3.6 TB per day, no new accounts can be added. At 4.5 TB per day, Detective stops ingesting data into the behavior graph.	June 10, 2021
Added tag values to the Python script options	When you use the Detective Python script `enableDetective.py` to enable Detective, you can now assign tag values to the behavior graph.	May 19, 2021

Added automatic enabling of member accounts that pass the data volume check	When member accounts accept an invitation, their status is **Accepted (Not enabled)** until Detective verifies that their data will not cause the behavior graph data volume to exceed the quota. If the data volume is not a problem, Detective automatically changes the status to **Accepted (Enabled)** . Note that existing member accounts that are currently **Accepted (Not enabled)** cannot be enabled automatic ally.	May 12, 2021
Added managed policy information to the security chapter	A new section in the security chapter provides details about managed policies for Detective. Detective currently provides a single managed policy, `AmazonDetectiveFullAccess` .	May 10, 2021
Changed the data volume values in the member accounts list	On the account managemen t page, the member accounts list now displays the daily data volume for each member account. Previously the list displayed the volume as a percentage of the total allowed volume.	April 29, 2021

Revised options for managing member accounts	Replaced the **Manage accounts** menu with an **Actions** menu. Combined the options for adding individual accounts and adding accounts from a .csv file. Moved **Enable accounts** from **Manage accounts** to a separate option next to **Actions**.	April 5, 2021
Added behavior graph tags and authorization based on tags	When you enable Detective , you can add tags to the behavior graph. You can manage tags for a behavior graph from the **General** page. Detective also supports authorization based on tag values.	March 31, 2021
Added differences for AWS GovCloud (US) Regions	Detective is now available in the AWS GovCloud (US) Regions. In AWS GovCloud (US-East) and AWS GovCloud (US-West), Detective does not send invitation emails to member accounts. Detective also does not automatically remove member accounts that are shut down in AWS.	March 24, 2021

Added tabs to filter the member account list based on the member account status	The list of member accounts now displays tabs that you can use to filter the list based on the member account status. You can view all member accounts, those that have a status of **Accepted (Enabled)**, or those that have a status other than **Accepted (Enabled)**.	March 16, 2021
Added option to Python script to suppress invitation emails	The Detective `enableDetective.py` script now provides a `--disable_email` option. When you include that option, Detective does not send invitation emails to the member accounts.	February 26, 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 API option to not send invitation emails to member accounts	When using the Detective API to add member accounts, administrator accounts can choose to not send invitation emails to member accounts.	February 25, 2021
Member account quota increased to 1,200	Master accounts can now invite up to 1,200 member accounts to their behavior graph. Previously the quota was 1,000.	December 11, 2020

Added values for behavior graph data volume quotas	Updated the information about behavior graph data volume quotas to add the specific quota values.	December 11, 2020
Member accounts can now see their usage and projected cost	Member accounts can now view their own usage information. For member accounts, the **Usage** page shows the amount of data ingested into each behavior graph that they contribute to. Member accounts can also see their projected 30-day cost.	May 26, 2020
Free trial is now per account instead of per behavior graph	Each account Amazon Detective now receives a separate free trial within each Region. The free trial starts either when the account enables Detective, or the first time the account is enabled as a member account.	May 26, 2020
New open source Python scripts on GitHub	The new amazon-detective-multiaccount-scripts repository on GitHub provides open source Python scripts that you can use to manage behavior graphs across Regions. You can enable Detective, add member accounts, remove member accounts, and disable Detective.	January 21, 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