Amazon Detective

Administration Guide

Amazon Detective: Administration Guide

Table of Contents

What is Amazon Detective?

Amazon Detective makes it easy to 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. Detective maintains up to a year of historical event data. This data is easily available through a set of visualizations that show changes in the type and volume of activity over a selected time window. Detective links those changes to GuardDuty findings.

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.

For information about how Detective uses source data from behavior graph accounts, see *Source data used in a behavior graph* (p. 13).

For information on how administrator accounts manage behavior graphs, see *For administrator accounts: Managing member accounts* (p. 15). For information on how member accounts manage their behavior graph invitations and memberships, see *For member accounts: Managing invitations and memberships* (p. 24).

The administrator account uses the analytics and visualizations generated from the behavior graph to investigate AWS resources and GuardDuty findings. The Detective integrations with GuardDuty and AWS Security Hub allow you to 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. Administrator accounts can also view data usage for the behavior graph, and remove member accounts from the behavior graph.

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.

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 incoming 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.

High-volume entity

An entity that has connections to or from a very 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.

See Viewing details for high-volume entities in the *Amazon Detective User Guide*.

Investigation

The process of performing triage on suspicious or interesting activity, determining the 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.

Member accounts can respond to the behavior graph invitation and remove their account from the behavior graph.

They 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.

Profile

For a finding or an entity, a single page that provides a collection of data visualizations plus supporting guidance.

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

For entities, profiles provide supporting details for 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 simple 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 finding and entity profiles.

The default scope time for a finding profile 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 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	3.24 TB per day	If the behavior graph data volume is larger than 3.24 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	3.6 TB per day	If the behavior graph data volume is larger than 3.6 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	4.5 TB per day	If the behavior graph data volume is larger than 4.5 TB per day, then Detective stops ingesting data into the behavior graph. The 4.5 TB per day reflects both normal data volume and spikes in the data volume. 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 *For administrator accounts: Managing member accounts* (p. 15).

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* (p. 12).

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. See the section called "Administrator account usage and cost" (p. 29). Member accounts can track the usage and projected cost for the behavior graphs that they belong to. See the section called "Member account usage tracking" (p. 30).

Contents

Amazon Detective prerequisites and recommendations

Before you can enable Amazon Detective, you must have an AWS account. If you don't have an account, use this procedure to create one.

To sign up for AWS

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.

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

Contents

Supported AWS Command Line Interface version

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

Account must have Amazon GuardDuty enabled

When you try to enable Detective, Detective checks whether GuardDuty has been enabled for your account for at least 48 hours.

If you are not a GuardDuty customer, or have been a GuardDuty customer for less than 48 hours, you cannot enable Detective. You must either enable GuardDuty or wait for 48 hours. This allows GuardDuty to assess the data volume that your account produces.

Account data volume must be within the Detective quota

The volume of data flowing into a behavior graph must be less than the maximum allowed by Detective.

When you try to enable Detective, if the data volume for your account is too large, you cannot enable Detective. The Detective console displays a notification to indicate that data volume is too large.

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 Security Hub more frequently, then enable Detective using the Security Hub administrator account.

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 the Detective administrator account access to other accounts.

For information on 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*.

Required IAM policy for Detective

Before you can enable Detective, if you are not an administrator, then you must attach the following permissions policy to your IAM principal. 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.

This policy allows you to perform all administrator account actions in Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:Get*",
        "detective:CreateGraph",
        "detective:CreateMembers",
        "detective:DeleteGraph",
        "detective:DeleteMembers",
        "detective:ListGraphs",
        "detective:ListMembers",
        "detective:SearchGraph",
        "detective:StartMonitoringMember",
        "detective:ListTagsForResource",
        "detective:TagResource",
        "detective:UntagResource",
        "guardduty:ArchiveFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    }
  ]
}
```

You can also use the `AmazonDetectiveFullAccess` managed policy (p. 51), which grants access to all Detective actions.

Enabling the display of account names

By default, the Detective console displays AWS account IDs.

If your account belongs to an organization in AWS Organizations, then Detective can also display account names. Detective retrieves the account names from Organizations.

To have Detective display account names, your account must belong to the organization.

You also must have the following permissions:

- `organizations:ListAccounts`
- `organizations:DescribeOrganization`

These permissions are included in the `AmazonDetectiveFullAccess` managed policy (p. 51).

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 on setting the notification frequency, see Monitoring GuardDuty Findings with Amazon CloudWatch Events in the Amazon GuardDuty User Guide.

Enabling Amazon Detective

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.

Before you try to enable Detective, make sure that your account has been enrolled in Amazon GuardDuty for at least 48 hours. If you do not meet this requirement, you cannot enable Detective.

If you do meet the GuardDuty requirement, then when you make the request to enable Detective, Detective checks whether your data volume is within the Detective quota. If your data volume exceeds the quota, then you cannot enable Detective.

Contents

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" (p. 7).
4. **Attach IAM policy (required)** contains the IAM policy that is required to enable Detective and manage a behavior graph. The policy should already be attached to your principal.

   If it is not yet attached, choose **Copy IAM policy** to copy the policy so that you can attach it.

   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 on inviting member accounts, see the section called "Inviting member accounts to a behavior graph" (p. 17).

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 on how to configure and use the GitHub scripts, see *Using the Amazon Detective Python scripts* (p. 57).

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 24 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 Detective console.
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 the account performs one of the following actions.

- Enables Detective and becomes the Detective administrator account for a behavior graph
- Accepts an invitation to be a member account in a behavior graph and is enabled as a member 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.

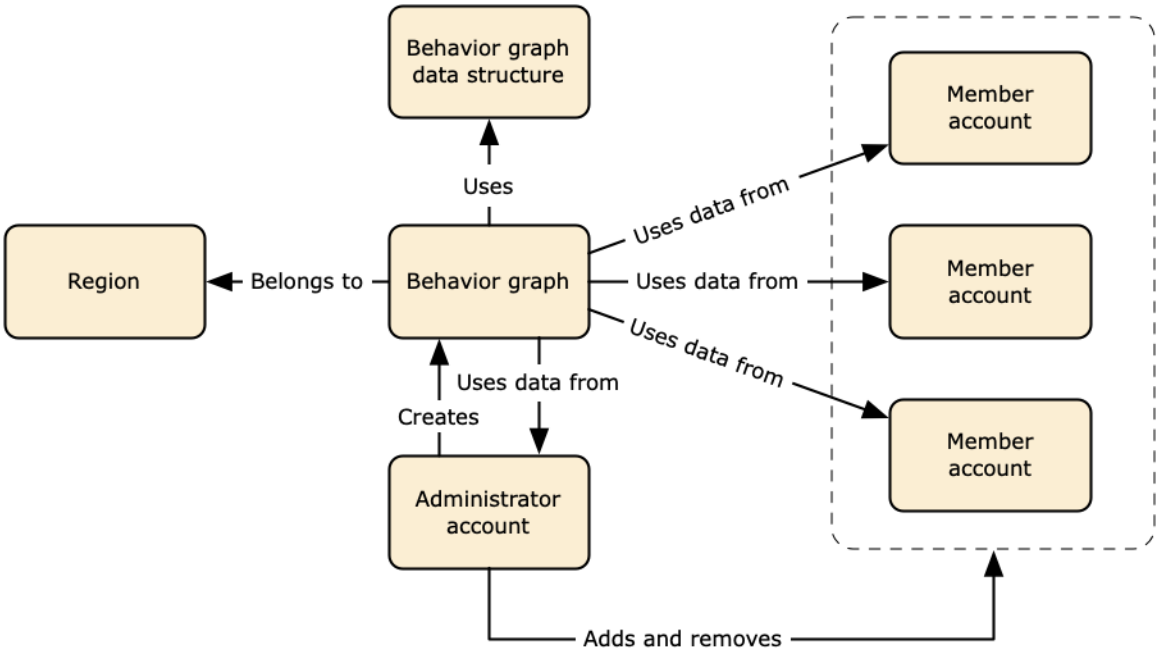
The same 30-day period is used for all behavior graphs in the Region. For example, an account is enabled as a member account for a behavior graph. This starts the 30-day free trial. After 10 days, the account is enabled for a second behavior graph in the same Region. For the second behavior graph, the 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” (p. 29) and the section called “Member account usage tracking” (p. 30).

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.



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

Contents

Types of Detective source data

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.

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 3.6 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 3.6 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 3.6 TB per day, then you cannot add a new member account to the behavior graph.

If the behavior graph data volume exceeds 4.5 TB per day, then Detective stops ingesting data into the behavior graph. The 4.5 TB per day 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.

For administrator accounts: Managing the accounts in your behavior graph

An administrator account can invite 1,200 other accounts to be member accounts in the behavior graph. See the section called “Inviting member accounts to a behavior graph” (p. 17). 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.

The administrator account can also remove member accounts from their behavior graph. See the section called “Removing member accounts from a behavior graph” (p. 22).

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.

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 the behavior graph, see the section called “Administrator account usage and cost” (p. 29).

Contents

Viewing the list of accounts in a behavior graph

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

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

Verification in progress

Detective is verifying the account email address before it sends the invitation.

Verification failed

The email address verification failed. The invitation was not sent.

Invited

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

Accepted (Enabled)

The member account accepted the invitation and is contributing data to the behavior graph.

Accepted (Not enabled)

The member account accepted the invitation, but cannot be enabled. This status occurs for one of the following reasons.

- The member account has not been an Amazon GuardDuty customer for at least 48 hours.
- The member account data would cause the behavior graph data volume to exceed the Detective quota.

Listing accounts in the Detective behavior graph (Console)

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

To display the list of accounts in the behavior graph (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**.

   My member accounts lists your account and the member accounts that you invited to contribute data to the behavior graph. For each account, the list displays the following information:

   - The AWS account identifier.
   - For member accounts only, the account root user email address.
   - The account status.
   - The daily data volume for the account. Detective cannot retrieve the data volume for member accounts that have not accepted the behavior graph invitation.
   - 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 **Accepted (Enabled)**.
- Choose **Not enabled** to view accounts that have a status other than **Accepted (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 the accounts in the Detective behavior graph (Detective API, AWS CLI)

You can use an API call or the AWS Command Line Interface to view a list of all invited and monitored 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 all of the invited and monitored member accounts (Detective API, AWS CLI)

- **Detective API:** Use the `ListMembers` operation. To identify the intended behavior graph, specify the behavior graph ARN.
- **AWS CLI:** At the command line, run the `list-members` command.

```
aws detective list-members --graph-arn <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
```

Inviting member accounts to a behavior graph

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

At a high level, the process for inviting members 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.

   Detective does not perform this validation in the AWS GovCloud (US-East) or AWS GovCloud (US-West) Regions.
3. If the account information is valid, Detective sends the invitation to the member account.

   Detective never sends email invitations to member accounts in the AWS GovCloud (US-East) or AWS GovCloud (US-West) Regions.

   For other Regions, the Detective API includes an option to not send invitations to the member accounts.

   This option is useful for accounts that are managed centrally.
4. The member account accepts or declines the invitation.

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

5. If the member account accepts the invitation, then Detective checks whether the member account has been an Amazon GuardDuty customer for at least 48 hours.

   If it has, then Detective checks whether the member account data would cause the data rate for the behavior graph to exceed the quota.

   This check can take between 24 to 48 hours.

   While Detective verifies the data rate, the member account status is **Accepted (Not enabled)**.
6. If the member account passes both of those checks, then the member account status is updated automatically to **Accepted (Enabled)**. Detective begins to ingest data from the member account into the behavior graph.

   If it fails either of those checks, then the member account status remains **Accepted (Not enabled)**. The member account does not contribute data to the behavior graph.
7. As soon as the member account is eligible to be enabled, Detective automatically changes the member account status to **Accepted (Enabled)**.

   For example, a member account enables GuardDuty, and Detective verifies that their data volume is not too large. Or the administrator account removes other member accounts to make space for an account.

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

   The administrator account can also 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 Accepted (Not enabled)” (p. 21).

   Note that Detective began to automatically enable accounts that are **Accepted (Not enabled)** on May 12, 2021. Accounts that were **Accepted (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 which member accounts to invite to contribute their data to a behavior graph.

To manually select the member accounts to invite (console)

1. Open the Detective console.
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 Detective console.
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.

- Sends 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* (p. 57).

Enabling a member account that is Accepted (Not enabled)

After a member account accepts an invitation, Amazon Detective checks whether it can enable the member account. If Detective cannot enable the member account, then it sets the member account status to **Accepted (Not enabled)**. This can happen for one of the following reasons.

- The member account has not been an Amazon GuardDuty customer for at least 48 hours.
- Detective is verifying the data volume for the member account.
- The member account data would cause the behavior graph data rate to exceed the quota.

Member accounts that are **Accepted (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 **Accepted (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 **Accepted (Not enabled)** member accounts.

Enabling a member account that is Accepted (Not enabled) (Console)

On the member account list, the **Manage** menu includes an option to enable selected member accounts that are **Accepted (Not enabled).**

To enable a member account that is Accepted (Not enabled)

1. Open the Detective console.
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 **Accepted (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 **Accepted (Enabled)**.

Enabling a member account that is Accepted (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 **Accepted (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 Accepted (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 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 a 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 member accounts from a behavior graph (Console)

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

To remove member accounts (console)

1. Open the Detective console.
2. In the Detective navigation pane, choose **Account management**.
3. Under **My member accounts**, select the check box for each member account to delete.

   You cannot delete your own account from the list.
4. Choose **Actions**. Then choose **Remove accounts**.
5. When prompted to confirm, enter **`remove`**.
6. Choose **Remove member accounts**.

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

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

To use remove 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 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* (p. 57).

For member accounts: Managing behavior graph invitations and memberships

A member account receives an invitation from the administrator account for a behavior graph. The invitation indicates that the administrator account wants to use the member account's data in the behavior graph. A member account can be invited to contribute to multiple behavior graphs. For more information, see the section called “Viewing behavior graph invitations” (p. 25).

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

Before Detective can ingest and extract the member account's data, the member account must accept the invitation. If the member account declines the invitation, then the behavior graph does not use the member account's data. See the section called “Responding to a behavior graph invitation” (p. 26).

A member account can remove their account from a behavior graph at any time. When they remove their account, Detective stops ingesting and extracting the account data into that behavior graph. See the section called “Removing your account from a behavior graph” (p. 27).

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:ListInvitations"],
    "Resource":"*"
   }
 ]
}
```

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.

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 **Accepted (Enabled)** or **Accepted (Not enabled)**.

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

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

  Your account status is set initially to **Accepted (Not enabled)** while Detective checks whether you have GuardDuty enabled, and if so, whether your account would cause the data volume for the behavior graph to exceed the Detective quota.

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

When the behavior graph is able to accommodate the data volume for your account, Detective automatically updates it to **Accepted (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

When you accept an invitation, your account status is set initially to **Accepted (Not enabled)** while Detective checks whether your account would cause the data volume for the behavior graph to exceed the Detective quota. For Detective to make this check, your account must have had Amazon GuardDuty enabled for at least 48 hours.

If your account would not cause the behavior graph to exceed the quota, Detective updates your account status to **Accepted (Enabled)**. Detective begins to ingest and extract data from logs and findings into the behavior graph as of that point in time. Your account is charged for the data.

If the addition of your account would cause the volume of data for the behavior graph to exceed the Detective quota, or if you do not have GuardDuty enabled, the status remains **Accepted (Not enabled)**. In this case, unless you remove your account, Detective automatically enables your account as soon as the behavior graph can accommodate it. The administrator account can also enable your account manually.

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 Detective console.
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.

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 Detective console.
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
```

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 shows the volume of data ingested into their behavior graph 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**.

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 cost for the administrator account

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" (p. 31).

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" (p. 31).

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" (p. 31).

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.

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" (p. 45).

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 you behavior graph from the **General** page.

To view the list of tags assigned to the behavior graph

1. Open the Detective console.
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

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. This content includes 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 user accounts with 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 recommend TLS 1.2 or later.
- 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 personal 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 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 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 three years (1095 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

- Troubleshooting Amazon Detective identity and access (p. 49)

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 (p. 49).

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 employees 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 (p. 41).

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 (p. 45).

Authenticating With Identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see Signing in to the AWS Management Console as an IAM user or root user in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 signing process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also 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 Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single 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 do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM Users and Groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing access keys for IAM users in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

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:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated users and roles in the *IAM User Guide*.
- **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.
  - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, resources, and condition keys for Amazon Detective in the *Service Authorization Reference*.
  - **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 IAM 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 IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. 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**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

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 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

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 also 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 different policies to allow different users from 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 AWS Services That Work with IAM 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 (p. 45).

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” (p. 48).

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 (Not supported)

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.

Detective does not support 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 are very powerful. They 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 using AWS managed policies** – To start using Detective quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the *IAM User Guide*.
- **Grant least privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the *IAM User Guide*.
- **Enable MFA for sensitive operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.
- **Use policy conditions for extra security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON policy elements: Condition 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:DeleteGraph","d
    "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.

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, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies 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 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 asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

> **Important**
> Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access Detective

To allow others to access Detective, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Detective.

To get started right away, see Creating your first IAM delegated user and group in the *IAM User Guide*.

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 (p. 41).
- 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*.

AWS managed policies for Amazon Detective

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ViewOnlyAccess** AWS managed policy provides read-only access to many AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions 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 Detective actions. This policy can be attached 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 archive GuardDuty findings. The policy also 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, then these permissions allow the Detective console to display account names in addition to account numbers.
- `guardduty` – Allows principals to archive GuardDuty 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:ListDetectors"
            ],
            "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 (p. 63).

Change	Description	Date
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” (p. 31).

Compliance validation for Amazon Detective

Detective is not in scope of any AWS compliance programs.

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 the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Detective through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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. For more information on access keys, see Managing access keys in the *IAM User Guide*.

If you prefer, 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 Detective console.
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* (p. 57).

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.

The role name must be the same in all of the accounts.

The `AmazonDetectiveFullAccess` managed policy (p. 51) contains the permissions that are required for the script to succeed.

The role trust relationship must allow your instance or local credentials to assume the role.

Role trust relationship

```
{
  "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.
- Select the `AmazonDetectiveFullAccess` managed policy.

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. 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`

Platform	Setup instructions
	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 provides a history of the updates to this guide.

Change	Description	Date
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 to the behavior graph. 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 automatically.	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

Change	Description	Date
Changed the data volume values in the member accounts list	On the account management page, the member accounts list now displays the daily data volume for each member account. Previously the list displayed the data volume as a percentage of the total allowed data 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 never sends invitation emails to member accounts. Detective also does not automatically remove member accounts that are terminated 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, member accounts that have a status of **Accepted (Enabled)**, or member accounts that have a status other than **Accepted (Enabled)**.	March 16, 2021

Change	Description	Date
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
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
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 values for behavior graph data volume quotas	Added the specific quota values for behavior graph data volume quotas.	December 11, 2020
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
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
Amazon Detective general availability release	Detective is now generally available.	March 31, 2020

Change	Description	Date
New open source Python scripts on GitHub (p. 57)	The new amazon-detective-multiaccount-scripts repository on GitHub provides open source Python scripts you can use to manage behavior graphs across Regions. You can enable Detective for a master account, add member accounts to behavior graphs, remove member accounts from behavior graphs, and disable Detective for a master account.	January 21, 2020
Introducing Amazon Detective (preview)	Detective uses machine learning and purpose-built visualizations to help you analyze and investigate security issues across your Amazon Web Services (AWS) workloads. Detective is currently in preview.	December 3, 2019