Amazon Macie

User Guide

Amazon Macie: User Guide

Table of Contents

What Is Amazon Macie?

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.

Important
Currently, Macie is supported in the following regions:

- US East (Northern Virginia)
- US West (Oregon)

Features of Amazon Macie

Data Discovery and Classification

Amazon Macie enables you to identify business-critical data and analyze access patterns and user behavior:

- Continuously monitor new data in your AWS environment
- Use artificial intelligence to understand access patterns of historical data
- Automatically access user activity, applications, and service accounts
- Use natural language processing (NLP) methods to understand data
- Intelligently and accurately assign business value to data and prioritize business-critical data based on your unique organization
- Create your own security alerts and custom policy definitions

Data Security

Amazon Macie enables you to be proactive with security compliance and achieve preventive security:

- Identify and protect various data types, including PII, PHI, regulatory documents, API keys, and secret keys
- Verify compliance with automated logs that allow for instant auditing
- Identify changes to policies and access control lists
- Observe changes in user behavior and receive actionable alerts
- Receive notifications when data and account credentials leave protected zones
- Detect when large quantities of business-critical documents are shared internally and externally

Pricing for Macie

Pricing in Macie is based on the content sources classified or processed. For detailed information about Macie pricing, see Amazon Macie Pricing.

Accessing Macie

You can work with Macie in any of the following ways:

Macie Console

Sign in to the AWS Management Console and open the Macie console at https://us-east-1.redirection.macie.aws.amazon.com/.

The console is a browser-based interface to access and use Macie.

Concepts and Terminology

As you get started with Amazon Macie, you can benefit from learning about its key concepts.

Account

A standard AWS account that contains your AWS resources. When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Macie. The account that you use to sign in to AWS at the time when you first enable Macie is designated as the **master** account.

You can also integrate other accounts with Macie. These other accounts are called **member** accounts.

> **Note**
> No users from the member accounts are granted access to the Macie console. Only the master account users have access to the Macie console where they can configure Macie and monitor and protect the resources in both master and member accounts.

Alert

A notification about a potential security issue that is discovered by Macie. Alerts are displayed on the Macie console and provide a comprehensive narrative about all activity that occurred over the last 24 hours.

Macie provides the following types of alerts:

- *Basic alerts* - alerts that are generated by the security checks that Macie performs. There are two types of basic alerts in Macie:
  - Managed (Macie-curated) basic alerts which you cannot modify. You can only enable or disable the existing managed basic alerts.
  - Custom basic alerts which you can create and modify to your exact specifications.
- *Predictive alerts* - automatic alerts based on activity within your AWS infrastructure that deviates from the established normal activity baseline. More specifically, Macie continuously monitors IAM user and role activity within your AWS infrastructure and builds a model of the normal behavior. It then looks for deviations from that normal baseline and when such activity is detected, it generates automatic predictive alerts. For example a user uploading or downloading a large number of S3 objects in a single day might trigger an alert if that user typically downloads one or two S3 objects over the course of a week.

For more information about alerts, including alert categories and details about the contents of Macie alerts, see Amazon Macie Alerts (p. 28).

Data source

The origin or location of a set of data. To classify and protect your data, Macie analyzes and processes information from the following data sources:

AWS CloudTrail event logs, Including Amazon S3 Object-Level API Activity

AWS CloudTrail provides you with a history of AWS API calls for your account, including API calls made using the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. AWS CloudTrail also allows you to identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address that the calls were made from, and when the calls occurred. For more information, see What is AWS CloudTrail?

For data classification purposes, Macie utilizes CloudTrail's ability to capture object-level API activity on S3 objects (data events). For more information, see Logging Data and Management Events for Trails.

Amazon S3

In this release, Macie analyzes and processes data stored in the Amazon S3 buckets. You can select the S3 buckets that contain objects that you want Macie to classify and monitor.

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. Amazon S3 stores data as objects within buckets. An object consists of a file and optionally any metadata that describes that file. To store an object in Amazon S3, you upload the file you want to store to a bucket. Buckets are the containers for objects. For more information, see Getting Started with Amazon Simple Storage Service.

User

In the context of Macie a user is the AWS Identity and Access Management (IAM) identity that makes the request. Macie uses the CloudTrail `userIdentity` element to distinguish the following user types. For more information, see CloudTrail userIdentity Element.

- Root – The request was made with your AWS account credentials.
- IAM user – The request was made with the credentials of an IAM user.
- Assumed role – The request was made with temporary security credentials that were obtained with a role via a call to the AWS Security Token Service (AWS STS) AssumeRole API.
- Federated user – The request was made with temporary security credentials that were obtained via a call to the AWS STS GetFederationToken API.
- AWS account – The request was made by another AWS account.
- AWS service – The request was made by an AWS account that belongs to an AWS service.

When specifying a user in the Macie console, for example searching for a user in the **Users** tab or constructing a query in the **Research** tab, or whitelisting a user in a basic alert with the index of **Cloudtrail data**, you must use a special Macie format called **macieUniqueId**. The macieUniqueId is a combination of the IAM UserIdentity element and the recipientAccountId. For more information, see the list of UserIdentity elements above and the definition of recipientAccountId in the CloudTrail Record Contents. The examples below list various structures of macieUniqueId, depending on the user identity type:

- 123456789012:root
- 123456789012:user/Bob
- 123456789012:assumed-role/Accounting-Role/Mary

For more detailed examples, see Analyzing Macie-Monitored Data by User Activity (p. 35).

Setting Up Amazon Macie

When you sign up for AWS, your AWS account is automatically signed up for all services in AWS, including Amazon Macie. If you don't have an account, use the following procedure to create one.

To sign up for AWS

1. Open https://aws.amazon.com/, and then choose **Create an AWS Account**.

   Note
   This might be unavailable in your browser if you previously signed into the AWS Management Console. In that case, choose **Sign in to a different account**, and then choose **Create a new AWS account**.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Topics

Step 1 - Enable Macie

When you launch the Macie console for the first time, choose **Get Started** and complete the following procedure to enable Macie.

Important
The AWS account that you use to enable Macie is automatically designated as your master account. For more information, see Concepts and Terminology (p. 3).

To enable Amazon Macie

1. The IAM identity (user, role, group) that you use to enable Macie must have the required permissions. To grant the permissions required to enable Macie, attach the AmazonMacieFullAccess managed policy to this IAM user, group, or role. For more information, see AWS Managed (Predefined) Policies for Macie (p. 74).
2. Use the credentials of the IAM identity from Step 1 to sign in to the Macie console. When you open the Macie console for the first time, choose **Get Started**.
3. On the **Enable Amazon Macie** page, verify region preferences by reviewing the value in the drop-down menu under the **Region** section.

   Note
   The region to which you are currently signed in is automatically selected.
4. Choose **Enable Macie**.

   Note the following about enabling Macie:

   - Macie is assigned a service-linked role called AWSServiceRoleForAmazonMacie. This service-linked role includes the permissions and trust policy that Macie requires to discover, classify, and protect sensitive data in AWS on your behalf and to generate alerts about potential security issues. To view the details of AWSServiceRoleForAmazonMacie, on the **Enable Amazon Macie** page, choose

View service role permissions. For more information, see Using Service-Linked Roles for Amazon Macie (p. 7). For more information about service-linked roles, see Using Service-Linked Roles.

- After you enable Macie, it immediately begins pulling and analyzing independent streams of data from AWS CloudTrail in order to generate alerts. Because Macie only consumes this data for purposes of determining if there are potential security issues, Macie doesn't manage AWS CloudTrail for you or make its events and logs available to you. If you have enabled AWS CloudTrail independent of Macie, you will continue to have the option to configure its settings through the AWS CloudTrail console or APIs. For more information, see What is AWS CloudTrail?
- You can disable Macie at any time to stop it from processing and analyzing AWS CloudTrail events. For more information, see Disabling Amazon Macie and Deleting Collected Metadata (p. 75).

Step 2 - Integrate Amazon S3 with Macie

To classify and protect your data, Macie analyzes and processes information from AWS CloudTrail and Amazon S3. Enabling CloudTrail in your account is required in order to enable Macie. Integrating S3 with Macie (in other words, initially specifying one or more S3 buckets for Macie to monitor) is not required in order to enable Macie. However we strongly recommend that you integrate with S3 as part of setting up Macie and specify at least one S3 bucket that contains objects that you want Macie to classify and monitor. For more information and details about how Macie classifies your data, see Classifying Data with Amazon Macie (p. 14).

When you integrate with S3, Macie creates a trail and a bucket to store the logs about the S3 object-level API activity (data events) that it will now analyze along with other CloudTrail logs that it processes.

Important
Macie has a default limit on the amount of data that it can classify in an AWS account. Once this data limit is reached, Macie stops classifying the data in this AWS account. The default data classification limit is 3TB. You can contact customer support and request an increase to the default limit.

You can use the following procedure to integrate with S3 as part of setting up Macie:

1. Log in to AWS with the credentials of the AWS account that is serving as your Macie master account.
2. In the Macie console's **Integrations** tab, choose the **Services** tab.
3. In the **Services** tab, select the account id (master or member) in the **Select an account** drop-down. The **Amazon S3** tile is then displayed.
4. Choose the **Details** button in the **Amazon S3** tile.
5. On the **Selected S3 buckets and prefixes** page, choose the edit icon, and then select either the full buckets (recommended) or bucket/prefix combinations for Macie to monitor. You can select up to 250 S3 buckets and prefixes.

   Note
   You can only select S3 buckets in your current AWS region.

   Important
   When you specify an S3 bucket, by default, Macie only classifies objects that are added to the bucket after your bucket selection is complete. However you can instruct Macie to classify all existing objects in the specified S3 bucket by checking the **Classify all** checkbox. If you decide to **Classify all** S3 objects in a bucket, make sure to note the following values:

   - **Total size** - total size of the data within this bucket, which is the sum of the sizes of all the objects in the bucket. This value is displayed in the **Total size** column on the **Select S3 buckets for Macie to monitor** page.
   - **Total processed** - total size of the data from the bucket that Macie will actually classify. This value is displayed in the **Total processed** column on the **Select S3 buckets for Macie to monitor** page.

- **Total cost estimate** - the total content classification cost estimate for each S3 bucket. This value is displayed in the **Total cost estimate** column on the **Select S3 buckets for Macie to monitor** page.

These values are greyed out if **Classify all** checkbox is not checked. These values are calculated based on the snapshot of the contents of your S3 buckets taken within the last 48 hours.
The **Total cost estimate** for each bucket is based on the **Total processed** value for that bucket and the general Macie pricing of $5 per GB processed by the content classification engine. The total cost estimates are provided only for S3 buckets, not for prefixes. For more information, see Amazon Macie Pricing.
The **Total processed** value for each bucket is calculated as follows:

- If an object's size is less than 1KB, 1KB is added to the **Total processed** value. Otherwise, the object's actual size is added to the **Total processed** value.
- If the object's size is greater than 20MB, 20MB is added to the **Total processed** value. Otherwise, the object's actual size is added to the **Total processed** value.
- For object in Amazon Glacier vaults, 0 is added to the **Total processed** value.

Note that it is possible for the **Total processed** value of an S3 bucket to be higher than the **Total size** value.

6. When you've finished your selections, choose **Review and Save**. And when you've finished reviewing your selections, choose **Save**.

Using Service-Linked Roles for Amazon Macie

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

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

You can delete the Macie service-linked role only after first disabling Macie. This protects your Macie resources because you can't inadvertently remove permission to access them.

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

Service-Linked Role Permissions for Macie

Macie uses the service-linked role named `AWSServiceRoleForAmazonMacie`. It allows Amazon Macie to discover, classify, and protect sensitive data in AWS on your behalf.

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

- `macie.amazonaws.com`

The role permissions policy allows Macie to complete the following actions on the specified resources:

- Action: `iam:CreateServiceLinkedRole`
- Resources: `arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For the `AWSServiceRoleForAmazonMacie` service-linked role to be successfully created, the IAM identity that you use Macie with must have the required permissions. To grant the required permissions, attach the `AmazonMacieFullAccess` managed policy to this IAM user, group, or role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a Service-Linked Role for Macie

- **For the master Macie account**, the `AWSServiceRoleForAmazonMacie` service-linked role is automatically created when you enable Macie for the first time or enable Macie in a supported region where you previously didn't have it enabled. You can also create the `AWSServiceRoleForAmazonMacie` service-linked role manually for the master account using the IAM console, the IAM CLI, or the IAM API.
- **For member Macie accounts**, the `AWSServiceRoleForAmazonMacie` service-linked role is automatically created when the master account associates a member account with Macie. You can also create `AWSServiceRoleForAmazonMacie` for member accounts manually using the IAM console, the IAM CLI, or the IAM API.

  Important
  The service-linked role that is created for the master Macie account doesn't apply to the member Macie accounts.

For more information about creating the role manually, see Creating a Service-Linked Role in the *IAM User Guide*.

Important
If you were using the Macie service before June 21, 2018, when it began supporting service-linked roles, the IAM roles that grant Macie access to call other AWS services on your behalf already exist in your AWS account (Macie master or member). These roles are `AmazonMacieServiceRole` and `AmazonMacieSetupRole`. They were created when you launched either the Macie AWS CloudFormation template for a master account or the Macie AWS CloudFormation template for a member account as part of setting up Macie.
The newly created service-linked role replaces these previously created IAM roles (in master and member accounts).

Note
These previously created IAM roles aren't deleted. They remain intact, but they're no longer used to grant Macie access to call other AWS services on your behalf. You can use the IAM console to manage or delete these IAM roles.

Editing a Service-Linked Role for Macie

Macie doesn't allow you to edit the `AWSServiceRoleForAmazonMacie` service-linked role. After you create a service-linked role, you can't change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Deleting a Service-Linked Role for Macie

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that isn't actively monitored or maintained.

Important
For a master account, you must first disable Macie in order to delete the `AWSServiceRoleForAmazonMacie`.
For Macie member accounts, in order to delete the service-linked role used in a member account, the master Macie account must first disassociate this member account from Macie.
If the Macie service isn't disabled when you try to delete the service-linked role, the deletion fails. For more information, see Disabling Amazon Macie and Deleting Collected Metadata (p. 75).

When you disable Macie, the `AWSServiceRoleForAmazonMacie` is NOT automatically deleted. If you then enable Macie again, it'll start using the existing `AWSServiceRoleForAmazonMacie`.

To manually delete the service-linked role using IAM

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

Integrate Member Accounts and Amazon S3 with Amazon Macie

You can use the Macie console's **Integrations** tab to integrate member accounts with Macie and to integrate Amazon S3 with Macie for both your master account and member accounts. For more information about the master and member accounts, see Concepts and Terminology (p. 3).

Topics

Integrate Member Accounts with Macie

When you integrate member accounts with Macie you are enabling Macie to monitor resources and activity in these member accounts.

To integrate member accounts with Macie

1. Log in to AWS with the credentials of the AWS account that you want to integrate with Macie as a member account.
2. **Important**
   This is a required step if you're adding an AWS account as a Macie member account for the first time.
   You can skip this step if you're re-adding an AWS account as a Macie member account after disassociating it from Macie.

   Create the IAM role called `AmazonMacieHandshakeRole` that grants this account the required permissions to be successfully integrated with Macie. You can create this role by launching the AWS CloudFormation stack templates found at the URLs listed below. This role only needs to be created once for use in all regions. For more information about AWS CloudFormation and CloudFormation stacks, see What is AWS CloudFormation? and Working with Stacks.

   Important
   Make sure to specify the master AWS account ID when running the stack templates below.

   - US East (Virginia): Macie CloudFormation template for a member account
   - US West (Oregon): Macie CloudFormation template for a member account
3. Log in to AWS with the Macie master account, navigate to the Macie console, and then choose the **Integrations** tab.
4. To integrate a member account, choose the **+** icon next to **Member accounts**.
5. In the **Add member AWS account(s)** pop up window, enter one or more AWS account IDs. Separate multiple account numbers with commas. Choose **Add accounts**.

   Important
   Once Macie is enabled in this member account, Macie is assigned a service-linked role called `AWSServiceRoleForAmazonMacie`. This service-linked role includes the permissions and the trust policy that Macie requires to discover, classify, and protect sensitive data in AWS in this

account and to generate alerts about potential security issues. The following are the details of `AWSServiceRoleForAmazonMacie`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:ListTags",
                "cloudtrail:LookupEvents",
                "iam:ListAccountAliases",
                "s3:Get*",
                "s3:List*"
            ]
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:cloudtrail:*:*:trail/AWSMacieTrail-DO-NOT-EDIT",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:PutEventSelectors"
            ]
        },
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::awsmacie-*",
                "arn:aws:s3:::awsmacietrail-*",
                "arn:aws:s3:::*-awsmacietrail-*"
            ],
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteBucketPolicy",
                "s3:DeleteBucketWebsite",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObjectVersionTagging",
                "s3:DeleteReplicationConfiguration",
                "s3:PutBucketPolicy"
            ]
        }
    ]
}
```

For more information, see Using Service-Linked Roles for Amazon Macie (p. 7). For more information about service-linked roles, see Using Service-Linked Roles.

If you disable Macie, the service no longer has access to the resources in your member account. However, the `AmazonMacieHandshakeRole` IAM role that you created for this member account in Step 2 above and the `AWSServiceRoleForAmazonMacie` service-linked role that was automatically created for this member account when it was integrated with Macie remain intact after you disable Macie. These existing

roles are used again if you decide to re-enable Macie for this member account. To re-enable Macie for a member account, you must use the steps above to integrate this member account with Macie.

Specify Data for Macie to Monitor

In order for Macie to start monitoring and classifying your data, you must specify what data you want Macie to monitor and classify. You can use the **Integrations/Services** tab to specify the S3 buckets that contain the data that you want Macie to monitor.

Important
Currently, Macie can only monitor objects stored in Amazon S3 buckets.

Important
Macie has a default limit on the amount of data that it can classify in an AWS account. Once this data limit is reached, Macie stops classifying the data in this AWS account. The default data classification limit is 3TB. You can contact customer support and request an increase to the default limit.

You can integrate S3 with Macie (in other words, specifying one or more S3 buckets for Macie to monitor) during the initial Macie setup. For more information and instructions, see Setting Up Amazon Macie (p. 5). You can also use the the following procedure to integrate S3 with Macie at any time after you've enabled Macie.

1. Log in to AWS with the credentials of the AWS account that is serving as your Macie master account.
2. In the Macie console's **Integrations** tab, choose the **Services** tab.
3. In the **Services** tab, select the account id (master or member) in the **Select an account** drop-down. The **Amazon S3** tile is then displayed.
4. Choose the **Details** button in the **Amazon S3** tile.
5. On the **Selected S3 buckets and prefixes** page, choose the edit icon, and then select either the full buckets (recommended) or bucket/prefix combinations for Macie to monitor. You can select up to 250 S3 buckets and prefixes.

   Note
   You can only select S3 buckets in your current AWS region.

   Important
   When you specify an S3 bucket, by default, Macie only classifies objects that are added to the bucket after your bucket selection is complete. However you can instruct Macie to classify all existing objects in the specified S3 bucket by checking the **Classify all** checkbox. If you decide to **Classify all** S3 objects in a bucket, make sure to note the following values:

   - **Total size** - total size of the data within this bucket, which is the sum of the sizes of all the objects in the bucket. This value is displayed in the **Total size** column on the **Select S3 buckets for Macie to monitor** page.
   - **Total processed** - total size of the data from the bucket that Macie will actually classify. This value is displayed in the **Total processed** column on the **Select S3 buckets for Macie to monitor** page.
   - **Total cost estimate** - the total content classification cost estimate for each S3 bucket. This value is displayed in the **Total cost estimate** column on the **Select S3 buckets for Macie to monitor** page.

   These values are greyed out if **Classify all** checkbox is not checked. These values are calculated based on the snapshot of the contents of your S3 buckets taken within the last 48 hours.
   The **Total cost estimate** for each bucket is based on the **Total processed** value for that bucket and the general Macie pricing of $5 per GB processed by the content classification

engine. The total cost estimates are provided only for S3 buckets, not for prefixes. For more information, see Amazon Macie Pricing.
The **Total processed** value for each bucket is calculated as follows:

- If an object's size is less than 1KB, 1KB is added to the **Total processed** value. Otherwise, the object's actual size is added to the **Total processed** value.
- If the object's size is greater than 20MB, 20MB is added to the **Total processed** value. Otherwise, the object's actual size is added to the **Total processed** value.
- For object in Amazon Glacier vaults, 0 is added to the **Total processed** value.

Note that it is possible for the **Total processed** value of an S3 bucket to be higher than the **Total size** value.
Note that the one-time classification cost estimates are only calculated per S3 buckets and NOT per S3 bucket prefixes. If you select an S3 bucket prefix, the cost estimate for the entire S3 bucket is included in the total cost estimate summary for the selected resources. If you select multiple prefixes of the same S3 bucket, the cost estimate for this entire S3 bucket is included only once in the total cost estimate summary for the selected resources.

6. When you've finished your selections, choose **Review and Save**. And when you've finished reviewing your selections, choose **Save**.

Encrypted Objects

If objects stored in your Amazon S3 buckets are encrypted, Macie might not be able to read and classify those objects:

- If your Amazon S3 objects are encrypted using Amazon S3-managed encryption keys (SSE-S3), Macie can read and classify the objects using the roles created during the setup process.
- If your Amazon S3 objects are encrypted using AWS KMS-managed keys (SSE-KMS), Macie can read and classify the objects only if you add the `AWSMacieServiceCustomerServiceRole` IAM role or the `AWSServiceRoleForAmazonMacie` service-linked role as a key user for the KMS customer master key (CMK). If you don't add either of these roles as a key user for the KMS CMK, Macie cannot read and classify the objects. However, Macie still stores metadata on the object, including which KMS CMK was used to protect the object.
- If your Amazon S3 objects are encrypted using client-side encryption, Macie cannot read and classify the objects, but still stores metadata on the object.

Classifying Data with Amazon Macie

Macie can help you classify your sensitive and business-critical data stored in the cloud. Currently, Macie analyzes and processes data stored in AWS S3 buckets. To classify your data, Macie also uses CloudTrail's ability to capture object-level API activity on S3 objects (data events). However, Macie only monitors CloudTrail data events if you specify at least one S3 bucket for Macie to monitor.

Once you specify the S3 bucket(s) for Macie to monitor, you enable Macie to continuously monitor and discover new data as it enters your AWS infrastructure. For more information on how to specify S3 buckets for Macie to monitor, see Specify Data for Macie to Monitor (p. 12).

> **Note**
> Macie's content classification engine processes up to the first 20 MB of an S3 object.

If you specify S3 buckets that include files of a format that is not supported in Macie, then Macie does not classify them and your Macie usage charges do not include any costs for this content. Your Macie usage charges include only the costs for the content that Macie processes. For example, Macie cannot extract text from .wav files (images or movies), therefore it doesn't process that content and you're not charged for it.

Topics

Classify data with Macie

> **Important**
> Currently, Macie supports the following compression and archive file formats:

- BZIP
- GZIP
- LZO
- RAR
- SNAPPY
- AR
- CPIO
- Unix dump
- TAR
- zip
- XZ
- Pack200
- BZIP2
- 7z
- ARJ
- LZMA

- DEFLATE
- Brotli

Once Macie begins monitoring your data, it uses the following automatic content classification methods to identify and prioritize your sensitive and critical data and to accurately assign business value to your data.

Content Type

To classify your data objects by a content type, Macie uses an identifier that is embedded in the file header. Macie offers a set of managed (Macie-curated) content types, each with a designated risk level between 1 and 10.

Macie can assign only one content type to an object.

You cannot modify existing or add new content types. You can enable or disable the existing content types, thus instructing Macie to either include or exclude them in its data classification process.

To view, enable, or disable content types

1. In the Macie console, navigate to the **Settings** page.
2. In the **Classify data** section, choose **Content types**.
3. Choose any of the listed managed content types to view its details.

   To enable or disable a content type, on its details page, use the **Enabled/Disabled** drop-down menu, and then choose **Save**.

File Extension

Macie can also classify your objects by their file extensions. Macie offers a set of managed file extensions, each with a designated risk level between 1 and 10.

Macie can assign only one file extension to an object.

You cannot modify existing or add new file extensions. You can enable or disable the existing file extensions, thus instructing Macie to either include or exclude them in its data classification process.

To view, enable, or disable file extensions

1. In the Macie console, navigate to the **Settings** page.
2. In the **Classify data** section, choose **File extensions**.
3. Choose any of the listed managed file extensions to view its details.

   To enable or disable a file extension, on its details page, use the **Enabled/Disabled** drop-down menu, and then choose **Save**.

Theme

Object classification by theme is based on keywords that Macie searches for as it examines the contents of data objects. Macie offers a set of managed themes, each with a designated risk level between 1 and 10.

Macie can assign one or more themes to an object.

You cannot modify existing or add new themes. You can enable or disable the existing themes, thus instructing Macie to either include or exclude them in its data classification process.

To view, enable, or disable themes

1. In the Macie console, navigate to the **Settings** page.
2. In the **Classify data** section, choose **Themes**.
3. Choose any of the listed managed themes to view its details.

   To enable or disable a theme, on its details page, use the **Enabled/Disabled** drop-down menu, and then choose **Save**.

Regex

Object classification by regex is based on specific data or data patterns that Macie searches for as it examines the contents of data objects. Macie offers a set of managed regex, each with a designated risk level between 1 and 10.

Macie can assign one or more regex to an object.

You cannot modify existing or add new regex. You can enable or disable the existing regex, thus instructing Macie to either include or exclude them in its data classification process.

To view, enable, or disable regex

1. In the Macie console, navigate to the **Settings** page.
2. In the **Classify data** section, choose **Regex**.
3. Choose any of the listed managed regex to view its details.

   To enable or disable a regex, on its details page, use the **Enabled/Disabled** drop-down menu, and then choose **Save**.

Personally Identifiable Information (PII)

Object classification by PII is based on recognizing any personally identifiable artifacts based on industry standards such as NIST-80-122 and FIPS 199. Macie is able to recognize the following PII artifacts:

- Full names
- Mailing addresses
- Email addresses
- Credit card numbers
- IP addresses (IPv4 and IPv6)
- Drivers license IDs (USA)
- National identification numbers (USA)
- Birth dates

As part of PII object classification, Macie also assigns each matching object a PII impact of high, moderate, and low using the following criteria:

- High
  - >= 1 full name and credit card

  - >= 50 names or emails and any combination of other PII
- Moderate
  - >= 5 names or emails and any combination of other PII
- Low
  - 1-5 names or emails and any combination of PII
  - Any quantity of PII attributes above (without names or emails)

Support Vector Machine-Based Classifier

Another method that Macie uses to classify your S3 objects is a Support Vector Machine (SVM) classifier that classifies content inside your Macie-monitored S3 objects (text, token n-grams, and character n-grams) as well as their metadata features (document length, extension, encoding, headers) in order to achieve accurate classification of documents based on content. This Macie-managed classifier was trained against a large corpus of training data of various types and has been optimized to support accurate detection of various content types, including source code, application logs, regulatory documents, and database backups. Also, the classifier has the ability to generalize its detections. For example, if it detected a new kind of source code that doesn't match any of the types of source code that it is trained to recognize, it can generalize the detection as being just "source code".

> **Note**
> This data classification method is not surfaced in the Macie's Settings. The following list of artifacts is Macie-managed and cannot be edited, enabled, or disabled.

The SVM classifier in Macie is trained to detect the following content types:

- E-books
- Email
- Generic encryption keys
- Financial
  - SEC regulatory forms
- JSON
  - AWS CloudTrail logs
  - Jupyter notebooks
- Application logs
  - Apache format
  - AWS S3 server logs
  - Linux syslog
- Database
  - MongoDB backup
  - MySQLbackup
  - MySQL script
- Source code
  - F#
  - VimL
  - ActionScript
  - Assembly
  - Bash
  - Batchfile
  - C

  - Clojure
  - Cobol
  - CoffeeScript
  - CUDA
  - Erlang
  - Fortran
  - Go
  - Haskell
  - Java
  - JavaScript
  - LISP
  - Lua
  - Matlab
  - ObjectiveC
  - Perl
  - PHP
  - PowerShell
  - Processing
  - Python
  - R
  - Ruby
  - Scala
  - Swift
  - VHDL
- Web languages
  - CSS
  - HTML
  - XML

Object Risk Level

Through the automatic classification methods described above, a Macie-monitored object is assigned various risk levels based on each content type, file extension, theme, regex, PII, and SVM artifact that is assigned to it. The object's compound (final) risk level is then set to the highest value of its assigned risk levels.

Retention Duration for S3 Metadata

Macie stores metadata about your S3 objects for the default duration of 1 month. You can extend this duration up to 12 months.

Protecting Data with Amazon Macie

Topics

Macie can help you monitor how your sensitive and business-critical data stored in the cloud is being used. Macie applies artificial intelligence to understand historical data access patterns and automatically assesses activity of users, applications and service accounts. This can help you detect unauthorized access and avoid data leaks.

Once you enable Macie it uses the following automated methods to protect your data:

CloudTrail events

Macie analyzes and processes a subset of CloudTrail-logged data and management events (API calls) that can occur within your infrastructure. Macie designates a risk level between 1 and 10 for each of the supported CloudTrail events.

You cannot modify existing or add new CloudTrail events to the Macie-managed list. You can enable or disable the supported CloudTrail events, thus instructing Macie to either include or exclude them in its data security process.

To view, enable, or disable supported CloudTrail events

1. In the Macie console, navigate to the **Settings** page.
2. In the **Protect data** section, choose **AWS CloudTrail events**.
3. Choose any of the listed events to view its details.

   To enable or disable an event, on its details page, use the **Enabled/Disabled** drop-down menu, and then choose **Save**.

CloudTrail errors

Macie analyzes and processes errors that can occur when Macie-supported subset of CloudTrail-logged data and management events (API calls) take place within your infrastructure. Macie designates a risk level between 1 and 10 for each of the supported CloudTrail errors.

You cannot modify existing or add new CloudTrail errors to the Macie-managed list. You can enable or disable the supported CloudTrail errors, thus instructing Macie to either include or exclude them in its data security process.

To view, enable, or disable supported CloudTrail errors

1. In the Macie console, navigate to the **Settings** page.
2. In the **Protect data** section, choose **AWS CloudTrail errors**.
3. Choose any of the listed errors to view its details.

To enable or disable an error, on its details page, use the **Enabled/Disabled** drop-down menu, and then choose **Save**.

Using the Macie Dashboard

The Macie **Dashboard** draws a comprehensive picture of all of your Macie-monitored data and activity. This topic describes the metrics and views that you can use in the **Dashboard** to view your monitored data grouped by various interest points. Each metric and view provides you with one or more ways of navigating to the Macie console's **Research** tab, where you can construct and run queries in the query parser and conduct in-depth investigative research of your Macie-monitored data and activity.

Dashboard Metrics

The following **Dashboard** metrics allow you to view your monitored data grouped by several key interest points:

- **High-risk S3 objects** - While classifying data (p. 14), Macie assigns a risk value to each monitored data object. This is Macie's way of helping you identify and prioritize your sensitive data over other, less business-critical data. This metric allows you to see all of your Macie-monitored data objects with a risk levels of 8 through 10.
- **Total event occurrences** - As part of securing data (p. 19), Macie analyzes and processes CloudTrail-logged events (API calls) that occur within your infrastructure. This metric provides the total count of all Macie-monitored event occurrences that took place within your infrastructure since you enabled Macie.
- **Total user sessions** - A user session is a 5-minute aggregate of CloudTrail data. This metric provides the total count of all user sessions of CloudTrail data that Macie analyzed and processed since it was enabled.

Dashboard Views

Follow this procedure to use the predefined Macie **Dashboard** views and generate distinct subsets of your Macie-monitored data and activity:

To use Macie Dashboard views

1. Choose the corresponding icon to select any of the following views to display various subsets of your Macie-monitored data and activity:
   - S3 objects for a selected time range (p. 22)
   - S3 objects (p. 22)
   - S3 objects by PII (p. 23)
   - S3 public objects by buckets (p. 23)
   - S3 objects by ACL (p. 24)
   - CloudTrail events and associated users (p. 24)
   - CloudTrail errors and associated users (p. 25)
   - Activity location (p. 26)
   - AWS CloudTrail events (p. 26)
   - Activity ISPs (p. 27)
   - AWS CloudTrail user identity types (p. 27)
2. If present in the selected view, locate and move the **Minimum risk** slider to the desired value. The **Minimum risk** slider enables you to only view items with the assigned risk equal to and greater than the selected value.

S3 objects for selected time range

This view provides a visual representation of your monitored S3 objects that match the following search criteria:

- At least one of the object's assigned themes is of the top 20 most frequently assigned themes
- The object's assigned risk is either equal to or greater than the value selected on the **Minimum risk** slider
- S3 object was last modified during one of the following time ranges:
  - The past six months
  - Between the date when Macie was enabled and a date six months prior to today

To navigate from this view to the **Research** tab, you can select (double-click) any of the squares that represent the displayed time ranges or themes. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab.

You can follow this sample procedure:

1. In the Macie **Dashboard**, select the **S3 objects over selected time range** view.
2. Set the **Minimum risk** slider to 5.
3. In the generated graph, double-click the square next to **Range: 0 - 6 months ago**.

   As a result, you are redirected to the **Research** tab with the following query automatically displayed in the query parser:

   ```
   themes:* AND dlp_risk:[5 TO *] AND @timestamp:[now-6M/M TO now]
   ```

   This query matches your selection to view the Macie-monitored S3 objects that are assigned one or more of the top 20 most frequently assigned themes, that have an assigned risk of 5 or higher, and that were last modified at some point in the past 6 months. The results of this query are also displayed. You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

S3 objects

This view provides the complete list of your Macie-monitored S3 objects, grouped by the assigned themes. For each theme, a percentage that this theme represents of the total number of your Macie-monitored S3 objects is displayed, as well as the total count of the S3 objects that were assigned this theme.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab.

You can follow this sample procedure:

1. In the Macie **Dashboard**, select the **S3 objects** view.
2. From the generated list of S3 objects, choose the looking glass icon next to, for example, **json/aws_cloudtrail_logs**.

   As a result, you are redirected to the **Research** tab with the following query automatically displayed in the query parser:

   ```
   themes:"json/aws_cloudtrail_logs"
   ```

This query matches your selection to view the Macie-monitored S3 objects with the assigned theme of **json/aws_cloudtrail_logs**. The results of this query are also displayed. You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

S3 objects by PII

This view provides the following lists:

- **S3 objects by PII priority**

  This is a complete list of your S3 objects that contain PII artifacts, grouped by the Macie-assigned PII priority. For each PII priority level, a percentage that the number of objects with this level represents of the total number of the S3 objects with PII artifacts is displayed, as well as the total count of the S3 objects with this PII priority level.
- **S3 objects by PII types**

  This is a complete list of your S3 objects that contain PII artifacts, grouped by the PII artifact types. For each PII artifact type, a percentage that the number of objects with PII artifacts of this type represents of the total number of the S3 objects with PII artifacts is displayed, as well as the total count of the S3 objects with PII artifacts of this type.

For more information about PII-based object classification, see Classifying Data with Amazon Macie (p. 14).

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed PII impacts or PII types. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab.

You can follow this sample procedure:

1. In the Macie **Dashboard**, select the **S3 objects by PII** view.
2. For example, let's generate a list of S3 objects with low PII priority. In the **S3 objects by PII priority** list, choose the looking glass icon next to the low PII priority.

   As a result, you are redirected to the **Research** tab with the following query automatically displayed in the query parser:

   ```
   pii_impact:"low"
   ```

   The results of this query are also displayed. You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

S3 public objects by buckets

This is a complete list of your public S3 objects grouped by the buckets in which they are stored. For each bucket, a percentage that this bucket's objects represent of the total number of your Macie-monitored S3 objects is displayed, as well as the total count of the S3 objects that are stored in this bucket.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed buckets. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab.

S3 objects by ACL

This view provides the following lists:

- **S3 objects by ACL URIs**

  This is a complete list of URIs that appear in access control lists (ACL)s that are attached to your S3 objects. For each URI, a percentage that the number of objects with ACLs attached that contain this URI represents of the total number of the S3 objects with ACLs attached is displayed, as well as the total count of the S3 objects with ACLs attached that contain this URI.
- **S3 objects by ACL display names**

  This is a complete list of user display names that appear in ACLs that are attached to your S3 objects. For each display name, a percentage that the number of objects with ACLs attached that contain this display name represents of the total number of the S3 objects with ACLs attached is displayed, as well as the total count of the S3 objects with ACLs attached that contain this display name.
- **S3 objects by ACL permissions**

  This is a complete list of access permissions that appear in ACLs that are attached to your S3 objects. For each permissions level, a percentage that the number of objects with ACLs attached that contain this permission level represents of the total number of the S3 objects with ACLs attached is displayed, as well as the total count of the S3 objects with ACLs attached that contain this permission level.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed URIs, ACL display names, and ACL permissions. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab.

You can follow this sample procedure:

1. In the Macie **Dashboard**, select the **S3 objects by ACL** view.
2. For example, let's generate a list of S3 objects with attached ACLs that contain full control permissions. In the **S3 objects by ACL permissions** list, choose the looking glass icon next to the **FULL_CONTROL** permission.

   As a result, you are redirected to the **Research** tab with the following query automatically displayed in the query parser:

   ```
   object_acl.Grants.Permission:"FULL_CONTROL"
   ```

   The results of this query are also displayed. You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

CloudTrail events and associated users

This view provides the following lists:

- **AWS CloudTrail events**

  This is a visual representation of the top 20 (by assigned risk and based on the value selected on the **Minimum risk** slider) CloudTrail data and management events that occurred during the last 60 days. You can use the available **Daily** or **Weekly** radio buttons to modify the graph to view daily or weekly results.

  To navigate from this view to the **Research** tab, you can select (double-click) any square that represents a particular event that you would like to investigate further. The number in parenthesis

next to the event name represents the number of user sessions (5-minute aggregates of CloudTrail data) in which this event is present. In the **Research** tab, your selection is automatically translated into a query that is displayed in the query parser.

- AWS Cloud trail associated users

  This is a visual representation of the users associated with the top 20 (by assigned risk and based on the value selected on the **Minimum risk** slider) CloudTrail data and management events that occurred during the last 60 days. You can use the available **Daily** or **Weekly** radio buttons to modify the graph to view daily or weekly results.

  To navigate from this view to the **Research** tab, you can select (double-click) any square that represents a particular error that you would like to investigate further.The number in parenthesis next to the user name represents the number of user sessions (5-minute aggregates of CloudTrail data) with which this user is associated. In the **Research** tab, your selection is automatically translated into a query that is displayed in the query parser.

You can follow this sample procedure:

1. In the Macie **Dashboard**, select the **CloudTrail events and associated users** view.
2. Set the **Minimum risk** slider to 1.
3. For example, let's generate a list of user sessions in which **PutRestApi** event is present. Double-click on the square next to **PutRestApi**.

   As a result, you are redirected to the **Research** tab with the following query automatically displayed in the query parser:

   ```
   eventNameIsp.key.keyword:"PutRestApi" AND @timestamp:[now-60d TO now]
   ```

   The results of this query are also displayed. You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

CloudTrail errors and associated users

This view provides the following lists:

- **AWS CloudTrail errors**

  This is a visual representation of the top 20 (by assigned risk and based on the value selected on the **Minimum risk** slider) CloudTrail errors that occurred during the last 60 days. You can use the available **Daily** or **Weekly** radio buttons to modify the graph to view daily or weekly results.

  To navigate from this view to the **Research** tab, you can select (double-click) any square that represents a particular error that you would like to investigate further. The number in parenthesis next to the error name represents the number of user sessions (5-minute aggregates of CloudTrail data) in which this error is present. In the **Research** tab, your selection is automatically translated into a query that is displayed in the query parser.

- AWS Cloud trail associated users

  This is a visual representation of the users associated with the top 20 (by assigned risk and based on the value selected on the **Minimum risk** slider) CloudTrail errors that occurred during the last 60 days. You can use the available **Daily** or **Weekly** radio buttons to modify the graph to view daily or weekly results.

  To navigate from this view to the **Research** tab, you can select (double-click) any square that represents a particular error that you would like to investigate further. The number in parenthesis next

to the user name represents the number of user sessions (5-minute aggregates of CloudTrail data) with which this user is associated. In the **Research** tab, your selection is automatically translated into a query that is displayed in the query parser.

You can follow this sample procedure:

1. In the Macie **Dashboard**, select the **CloudTrail errors and associated users** view.
2. Set the **Minimum risk** slider to 1.
3. For example, let's generate a list of user sessions in which **Client.InvalidPermission.NotFound** error is present. Double-click on the square next to **Client.InvalidPermission.NotFound**.

   As a result, you are redirected to the **Research** tab with the following query automatically displayed in the query parser:

   ```
   eventNameErrorCode.secondary:"Client.InvalidPermission.NotFound" AND
   @timestamp:[now-60d TO now]
   ```

   The results of this query are also displayed. You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

Activity location

This view includes a map that shows the locations of activity that Macie is monitoring for a selected time period. To view details, you can use the available time period pull-down menu (past 15 days, past 30 days, past 90 days, or past year), and then choose any location pin.

To navigate from this view to the **Research** tab, choose the number of events that appears in a tooltip window for a location pin. In the **Research** tab, your selection is automatically translated into a query that is displayed in the query parser. For example, you can auto-generate the following query to display a list of user sessions that occurred in the past 15 days in Seattle:

```
geoLocation.key:"Seattle:UnitedStates:47.6145:-122.348" AND @timestamp:[now-15d
TO now]
```

You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

AWS CloudTrail events

AWS CloudTrail events

This view provides the complete list of your Macie-monitored CloudTrail data and management events. For each event, the total count of the user sessions (5-minute integrations of CloudTrail data) in which this event is present and the percentage that this total represents of the total number of user sessions is displayed.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed events. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab. For example, you can auto-generate the following query to view all user sessions in which the AssumeRole event is present:

```
eventNameIsp.key.keyword:"AssumeRole"
```

You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

Activity ISPs

Activity ISPs

This view provides the complete list of your Macie-monitored CloudTrail data and management events, grouped by the associated internet service providers (ISPs). For each ISP, the total count of the user sessions (5-minute integrations of CloudTrail data) in which this ISP is present and the percentage that this total represents of the total number of user sessions is displayed.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab. For example, you can auto-generate the following query to view all user sessions that are associated with Amazon:

```
eventNameIsp.secondary.keyword:"Amazon"
```

You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

AWS CloudTrail user identity types

This view provides the complete list of your Macie-monitored CloudTrail data and management events, grouped by the user identity type (for more information, see the definition for 'user' in Concepts and Terminology (p. 3). For each user identity type, the total count of the user sessions (5-minute integrations of CloudTrail data) in which this user identity type is present and the percentage that this total represents of the total number of user sessions is displayed.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab. For example, you can auto-generate the following query to view all user sessions that contain requests that were originated by the **AssumedRole** user identity type:

```
userIdentityType.key:"AssumedRole"
```

You can then modify the query result controls available on the **Research** tab and run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Macie-Monitored Data (p. 40).

Amazon Macie Alerts

An alert is a notification about a potential security issue discovered by Amazon Macie. This section describes the following information:

Topics

Basic and Predictive Macie Alerts

Macie generates two types of alerts:

- *Basic alerts* - alerts generated by the security checks that Macie performs. There are two types of basic alerts in Macie:
  - Managed (Macie-curated) basic alerts which you cannot modify. You can enable or disable the existing managed basic alerts.

    Note
    You can identify managed basic alerts by the value of `MacieDefault` in the **Created by** field in the **Basic alerts** list in the **Settings** tab.
  - Custom basic alerts which you can create and modify to your exact specifications. For more information, see Adding New and Editing Existing Custom Basic Alerts (p. 31).
- *Predictive alerts* - automatic alerts based on activity within your AWS infrastructure that deviates from the established 'normal' activity baseline. More specifically, Macie continuously monitors activity within your AWS infrastructure and builds a model of the 'normal' behavior. It then looks for deviations from that normal baseline and when such activity is detected, it generates automatic predictive alerts. For example a user uploading or downloading a large number of S3 objects in a single day might trigger an alert if that user typically downloads one or two S3 objects over the course of a week.

Alert Categories in Macie

Macie's basic alerts (managed and custom) can be of the following categories:

- **Configuration compliance** - related to compliance-controlled content, policy, configuration settings, control and data plane logging, and patch level.
- **Data compliance** - related to the discovery of compliance or security-controlled content, such as the existence of Personally Identifiable Information (PII), or access credentials.
- **File hosting** - related to you hosting possible malware, unsafe software, or attackers' command and control infrastructure through compromised hosts or storage services.

- **Service disruption** - configuration changes that can lead to you not being able to access resources in your own environment.
- **Ransomware** - potentially malicious software or activity designed to block your access to your own computer system until a sum of money is paid.
- **Suspicious access** - access to your resources from a risky anomalous IP address, user, or system, such as an attacker masquerading their connection through a compromised host.
- **Identity enumeration** - a series of API calls or accesses enumerating access levels to your systems that can possibly indicate the early stages of an attack or compromised credentials.
- **Privilege escalation** - successful or unsuccessful attempts to gain elevated access to resources that are normally protected from an application or user, or attempts to gain access to your system or network for an extended period of time.
- **Anonymous access** - attempted access to your resources from an IP address, user, or service with the intent to hide a user's true identity. Examples include the use of proxy servers, virtual private networks and other anonymity services such as Tor.
- **Open permissions** - identification of sensitive resources protected by potentially overly permissive (and thus risky) access control mechanisms.
- **Location anomaly** - an anomalous and risky location of the access attempt to your sensitive data.
- **Information loss** - an anomalous and risky access to your sensitive data.
- **Credentials loss** - possible compromise of your credentials.

To quickly view a list of your existing alerts of a particular category, choose that category from the **Categories** list on the Macie console's **Alerts** tab.

Severity Levels for Alerts in Macie

Each Macie alert has an assigned severity level. This reduces the need to prioritize one alert over another in your analyses. It can also help you determine your response when an alert highlights a potential problem. **Critical**, **High**, **Medium**, and **Low** levels all indicate a security issue that can result in compromised information confidentiality, integrity, and availability within your infrastructure. The **Informational** level simply highlights a security configuration detail of your Macie-monitored infrastructure. Following are recommended ways to respond to each:

- **Critical** – Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability within your infrastructure. We recommend that you treat this security issue as an emergency and implement an immediate remediation. The main difference between a Critical and High severity is that a Critical severity alert might be informing you of a security compromise of a large number of your resources or systems. A High severity alert is informing you of a security compromise of one or several of your resources or systems.
- **High** – Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability within your infrastructure. We recommend that you treat this security issue as an emergency and implement an immediate remediation.
- **Medium** – Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability within your infrastructure. We recommend that you fix this issue at the next possible opportunity, for example, during your next service update.
- **Low** - Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability within your infrastructure. We recommend that you fix this issue as part of one of your future service updates.
- **Informational** – Describes a particular security configuration detail of your infrastructure. Based on your business and organization goals, you can either simply make note of this information or use it to improve the security of your systems and resources.

Locating and Analyzing Macie Alerts

You can use the following procedure to locate and analyze existing alerts:

1. To view your generated alerts (including **Active** and **Archived** basic or predictive alerts), in the Macie console, navigate to the **Alerts** page.

   Each alert has a summary section that contains the following information:

   - Alert severity, which can be **Critical**, **High**, **Medium**, **Low**, or **Informational**. For more information, see Severity Levels for Alerts in Macie (p. 29).
   - A timestamp that indicates when the alert was generated or last updated.
   - The alert category - for more information, see Alert Categories in Macie (p. 28).
   - One of the following:
     - If the alert's index is **CloudTrail data**, a user that engaged in the activity that prompted Macie to generate the alert. For more information, see the definition of a 'user' concept in the context of Macie in Concepts and Terminology (p. 3)
     - If the alert's index is **S3 bucket properties** or **S3 objects**, a bucket name that was involved in or that contains the objects that were involved in the activity that prompted Macie to generate the alert.

       Important
       In Macie, each alert is based on one of the following:

       - For the alerts with the index of **CloudTrail data**, only one user - the IAM identity whose activity prompted Macie to generate the alert.
       - For the alerts with the index of **S3 bucket properties** or **S3 objects**, only one S3 bucket that was involved in or that contains objects that were involved in the activity that prompted Macie to generate the alert.
   - A number of comments that were left on the alert.
   - A total number of results, which can consist of a list of user sessions, or a list of 3 buckets, or a list of S3 objects that match the query that is included in the definition of the alert. For more information, see Adding New and Editing Existing Custom Basic Alerts (p. 31).
   - A number of views on the alert.
   - The AWS region in which the activity captured in this alert took place.
2. To analyze any alert further, choose the alert to expand its details pane. The following information is included in the alert details:

   - The alert summary that includes the description and the total number of results - a number of user sessions, or a number of S3 buckets, or a number of S3 objects that match the query that is included in the definition of the alert.
   - A list of the alert results. This is a list of user sessions, or a list of S3 buckets, or a list of S3 objects, depending the index that is specified in the definition for this alert. For more information, see Adding New and Editing Existing Custom Basic Alerts (p. 31).
     - If you specified **CloudTrail data** as the index, the alert details contain a list of user sessions that match the query specified in the alert definition for a particular user.
     - If you specified **S3 buckets** as the index, the alert details contain a list of S3 buckets that match the query specified in the alert definition for a particular user.
     - If you specified **S3 objects** as the index, the alert details contain a list of S3 objects that match the query specified in the alert definition for a particular user.

   You can choose each result to examine it further and view all its fields. For more information, see Researching AWS Data, Researching S3 Bucket Properties Data, or Researching S3 Objects Data sections in Researching Through Macie-Monitored Data (p. 40)

You can also use the **Research** looking glass icon to navigate to the **Research** tab and view the results of a particular alert there. The **Query Parser** in the **Research** tab is then pre-populated with the query that can be used to generate these results.

Adding New and Editing Existing Custom Basic Alerts

You can use the following procedure to add new and edit existing custom basic alerts:

1. In the Macie console, navigate to the **Settings** page and choose the icon for **Basic alerts**.
2. On the **Basic alerts** page, either choose the edit icon for the alert that you want to modify. Or, to add a new basic alert, choose **Add new**.
3. Do one of the following:

   - If you're editing the existing alert, make your changes, including enabling or disabling the alert, and then choose **Save**.
   - If you're adding a new alert, on the **Basic alert definition** page, specify the following:
     - Alert title - for example, "An S3 bucket has an IAM policy that grants 'read' rights to everyone."
     - Description for the alert - for example, "An IAM policy on an S3 bucket contains a clause that effectively grants 'read' access to any user. It is recommended that you audit this S3 bucket and its data and confirm that this is intentional.
     - Alert category - for more information, see Alert Categories in Macie (p. 28).
     - Alert query - a query that describes the activity that you want Macie to generate an alert about. For example, `s3_world_readability:"true"`. This query looks for an IAM policy on an S3 bucket that grants 'read' access to any user. For more information about constructing queries, see Constructing Queries in Macie (p. 40).

       Note
       You can use the looking glass icon next to an existing alert to navigate to the **Research** tab. This alert's query is then automatically displayed in the **Query Parser** and the results of this query are displayed in the **Research** tab.
   - Query index - this is the repository of data against which Macie will run the query specified in this alert. You can select either CloudTrail data, S3 buckets, or S3 objects. Depending on your selection, the alert will contain either a list of cloud trail user sessions (5-minute aggregates of raw CloudTrail data), a list of S3 buckets, or a list of S3 objects that match the activity that your alert defines.
   - A minimum number of activity matches that must occur before an alert is generated.
   - Alert severity - for more information, see Severity Levels for Alerts in Macie (p. 29)
   - Whitelisted users or whitelisted buckets, depending on the selected alert index. If you whitelist a user or a bucket, Macie will not generate an alert for this user or bucket when they are involved in the activity that the alert defines.

     Important
     In Macie, each alert is based on one of the following:
     - For the alerts with the index of **CloudTrail data**, only one user - the IAM identity whose activity prompted Macie to generate the alert.
     - For the alerts with the index of **S3 bucket properties** or **S3 objects**, only one S3 bucket that was involved in or that contains objects that were involved in the activity that prompted Macie to generate the alert.

     When whitelisting a user in a basic alert with the index of CloudTrail data, you must use a special Macie format called **macieUniqueId**. For example, 123456789012:root or

123456789012:user/Bob, or 123456789012:assumed-role/Accounting-Role/Mary, depending on the identity type of the user you want to whitelist. For more information, see the definition of the 'user' concept in Analyzing Macie-Monitored Data by User Activity (p. 35).

- Specify whether this alert is enabled or disabled.

Working with Existing Alerts

You can use the following procedure to archive or unarchive alerts or to choose edit the existing basic alerts.

1. In the Macie console, navigate to the **Alerts** page and locate the alert that you want to either archive, unarchive (if it's an archived alert), or edit.
2. Choose the down arrow in the alert summary pane and then choose either of the following:

   - **Archive**

     Note
     Or **Unarchive**, if this is an archived alert.

   - **Edit basic alert**

     Important
     This option is not available for predictive alerts. You cannot edit predictive alerts, which are automatically generated by Macie based on activity within your AWS infrastructure that deviates from the established 'normal' activity baseline. For more information, see Basic and Predictive Macie Alerts (p. 28).

Group Archiving Alerts

You can use the following procedure to group archive alerts:

1. In the Macie console's **Alerts** page, choose **Group Archive**.
2. In the **Group archive** window, use the available settings to archive or unarchive multiple alerts at the same time.

Whitelisting Users or Buckets for Basic Alerts

Macie allows you to whitelist users (if the alert's index is **CloudTrail data**) and buckets (if the alert's index is **S3 bucket properties** or **S3 objects**) for both Macie-managed and custom basic alerts.

Note
Macie does not allow you to whitelist users or buckets for predictive alerts.

You can use the following procedure to whitelist a specific user or a specific bucket that engaged in or was involved in the activity that prompted Macie to generate a specific alert.

Important
In Macie, each alert is based on one the following:

- For the alerts with the index of **CloudTrail data**, only one user - the IAM identity whose activity prompted Macie to generate the alert.
- For the alerts with the index of **S3 bucket properties** or **S3 objects**, only one S3 bucket that was involved in or that contains objects that were involved in the activity that prompted Macie to generate the alert.

Whitelist users or S3 buckets for custom basic alerts using the Alerts tab

1. In the Macie console's **Alerts** tab, locate the custom basic alert for which you want to whitelist a user or (S3 bucket) listed in the alert's summary.
2. Choose the down arrow in the alert summary pane and then choose **Whitelist user** (if this alert's index is **CloudTrail data**) or **Whitelist bucket** (if the alert's index is **S3 bucket properties** or **S3 objects**).
3. In the **Whitelist user** (or **Whitelist bucket**) window, verify the user or bucket that you want to whitelist (automatically pre-selected and matching the user or bucket listed in the alert's summary), and then choose **Submit**.

You can use the following procedure to whitelist multiple users or buckets at the same time for custom basic alerts.

Whitelist users or S3 buckets for custom basic alerts using the Settings tab

1. In the Macie console's **Settings** tab, choose **Basic alerts**, and then locate the custom basic alert for which you want to whitelist users or S3 buckets.
2. Choose the edit icon next to the alert.
3. Specify users or S3 buckets that you want to whitelist in either **Whitelisted users** (if this alert's index is **CloudTrail data**) or **Whitelisted buckets** (if the alert's index is **S3 bucket properties** or **S3 objects**) fields and then choose **Save**.

   Note
   When whitelisting a user in a basic alert with the index of CloudTrail data, you must use a special Macie format called **macieUniqueId**. For example, 123456789012:root or 123456789012:user/Bob, or 123456789012:assumed-role/Accounting-Role/Mary, depending on the identity type of the user you want to whitelist. For more information, see the definition of the 'user' concept in Analyzing Macie-Monitored Data by User Activity (p. 35).

Whitelist users or S3 buckets for Macie-managed basic alerts

1. In the Macie console's **Alerts** tab, locate the Macie-managed basic alert for which you want to whitelist users or S3 buckets.
2. Choose the down arrow in the alert summary pane and then choose **Whitelist user** (if this alert's index is **CloudTrail data**) or **Whitelist bucket** (if the alert's index is **S3 bucket properties** or **S3 objects**).
3. In the **Whitelist user** or **Whitelist bucket** window, check the **Clone and disable the default managed alert** checkbox and then choose **Submit**.
4. Navigate to the Macie console's **Settings** tab.

   Note that the original managed alert that you worked with in the previous step is now disabled. Note also that this alert has been cloned into a new custom basic alert. For example, if your original managed basic alert was called "An S3 bucket has an IAM policy that grants 'read' rights to everyone", this alert is now disabled and a new (cloned) custom basic alert called "An S3 bucket has an IAM policy that grants 'read' rights to everyone (modified)" is created.
5. Choose the edit icon next to the cloned custom basic alert.
6. Specify users or S3 buckets that you want to whitelist in either **Whitelisted users** (if this alert's index is **CloudTrail data**) or **Whitelisted buckets** (if the alert's index is **S3 bucket properties** or **S3 objects**) fields and then choose **Save**.

   Note
   When whitelisting a user in a basic alert with the index of CloudTrail data, you must use a special Macie format called **macieUniqueId**. For example, 123456789012:root

or 123456789012:user/Bob, or 123456789012:assumed-role/Accounting-Role/Mary, depending on the identity type of the user you want to whitelist. For more information, see the definition of the 'user' concept in Analyzing Macie-Monitored Data by User Activity (p. 35).

Analyzing Macie-Monitored Data by User Activity

The **Users** tab can help you draw a comprehensive picture of all of the Macie-monitored data and activity for a particular selected user. This topic describes how to search for the users whose activity you want to investigate further in the **Users** tab and the views that you can use in this tab to see the selected users' monitored data grouped by various interest points. Each view provides you with one or more ways of navigating to the Macie console's **Research** tab, where you can construct and run queries in the Query Parser and conduct in-depth investigative research of the Macie-monitored data and activity for the selected users.

Topics

MacieUniqueID

In the context of Macie a user is the AWS Identity and Access Management (IAM) identity that makes a particular request. Macie uses the CloudTrail `userIdentity` element to distinguish the following user types. For more information, see CloudTrail userIdentity Element.

- Root – The request was made with your AWS account credentials.
- IAM user – The request was made with the credentials of an IAM user.
- Assumed role – The request was made with temporary security credentials that were obtained with a role via a call to the AWS Security Token Service (AWS STS) AssumeRole API.
- Federated user – The request was made with temporary security credentials that were obtained via a call to the AWS STS GetFederationToken API.
- AWS account – The request was made by another AWS account.
- AWS service – The request was made by an AWS account that belongs to an AWS service.

When specifying a user in the Macie console, for example searching for a user in the **Users** tab or constructing a query in the **Research** tab, or whitelisting a user in a basic alert with the index of **Cloudtrail data**, you must use a special Macie format called **macieUniqueId**. The macieUniqueId is a combination of the IAM UserIdentity element and the recipientAccountId. For more information, see CloudTrail userIdentity Element and the definition of recipientAccountId in CloudTrail Record Contents.

The examples below list various structures of macieUniqueId, depending on the user identity type:

userIdentity	MacieUniqueId

`"userIdentity": {`
`"type": "AssumedRole"`
`"arn":`
`"arn:aws:sts::123456789012:assumed-role/Accounting-Role/Mary"`
`}`
	123456789012:assumed-role/accounting-role

userIdentity	MacieUniqueId
`"userIdentity": { "type": "IAMUser", "arn": "arn:aws:iam::123456789012:user/Bob", "userName": "Bob" }`	123456789012:user:bob
`"userIdentity": { "type": "FederatedUser" "arn": "arn:aws:sts::123456789012:federated-user/Alice", "principalId": "123456789012:Alice", }`	123456789012:federated-user:alice
`"recipientAccountId": "123456789012", "userIdentity": { "type": "AWSAccount" "accountId": "ANONYMOUS_PRINCIPAL", }`	123456789012:ANONYMOUS_PRINCIPAL
`"macieUniqueId": "123456789012:root:root", "userIdentity": { "type": "Root" "sourceARN": "arn:aws:iam::123456789012:root", }`	123456789012:root:root
`"userIdentity": { "invokedBy": "codepipeline.amazonaws.com", "type": "AWSService" } "recipientAccountId": "123456789012",`	123456789012:codepipeline.amazonaws.com
`"recipientAccoundId": "123456789012", "userIdentity": { "type": "AWSAccount" "accountId": "987654321098", "principalId": "AIDABCDEFGHI123456XYZ", }`	123456789012:AIDABCDEFGHI123456XYZ

User Categories in Macie

Based on their activity (API calls), users in Macie are grouped into the following categories:

- **Platinum**: these IAM users or roles have a history of making high risk API calls indicative of an administrator or root user, such as creating users, authorizing security group ingress, or updating policies. These accounts should be monitored closely for signs of account compromise.
- **Gold**: these IAM users or roles have a history of making infrastructure-related API calls indicative of a power user, such as running instances or writing data to Amazon S3. These accounts should be monitored closely for signs of account compromise.
- **Silver**: these IAM users or roles have a history of issuing high quantities of medium-risk API calls, such as Describe* and List* operations, or read-only access requests to Amazon S3.
- **Bronze**: these IAM users or roles typically execute lower quantities of Describe* and List* API calls in the AWS environment.

Investigating Users

Follow this procedure to generate a comprehensive picture of all of the Macie-monitored data and activity for the specified user:

1. In the Macie console's Users tab, specify a user name in the Search field and press Enter.

   Note
   When specifying a user, you must use a special Macie format called **macieUniqueId**. For example, 123456789012:root or 123456789012:user/Bob, or 123456789012:assumed-role/Accounting-Role/Mary, depending on the identity type of the user you want to whitelist. For more information, see the definition of the 'user' concept in Concepts and Terminology (p. 3).
2. When the user data is generated, choose the corresponding icon to select any of the following views to display various subsets of this user's Macie-monitored data and activity:

   - High-risk CloudTrail events (p. 37)
   - High-risk CloudTrail errors (p. 38)
   - Activity location (p. 38)
   - CloudTrail events (p. 38)
   - Activity ISPs (p. 38)
   - CloudTrail user identity types (p. 38)
3. If present in the selected view, locate and move the **Minimum risk** slider to the desired value. The **Minimum risk** slider enables you to only view items with the assigned risk equal to and greater than the selected value.

High-risk CloudTrail Events

This view provides a visual representation of the top 20 (by assigned risk and based on the value selected on the **Minimum risk** slider) CloudTrail data and management events that occurred during the last 60 days for the selected user. You can use the available **Daily** or **Weekly** radio buttons to modify the graph to view daily or weekly results.

To navigate from this view to the **Research** tab, you can select (double-click) any square that represents a particular event that you would like to investigate further. The number in parenthesis next to the event name represents the number of user sessions (5-minute aggregates of CloudTrail data) in which

this event is present. In the **Research** tab, your selection is automatically translated into a query that is displayed in the Query Parser. For more information, see Researching Through Macie-Monitored Data (p. 40)

High-risk CloudTrail Errors

This view provides a visual representation of the top 20 (by assigned risk and based on the value selected on the **Minimum risk** slider) CloudTrail errors that occurred during the last 60 days for the selected user. You can use the available **Daily** or **Weekly** radio buttons to modify the graph to view daily or weekly results.

To navigate from this view to the **Research** tab, you can select (double-click) any square that represents a particular error that you would like to investigate further. The number in parenthesis next to the error name represents the number of user sessions (5-minute aggregates of CloudTrail data) in which this error is present. In the **Research** tab, your selection is automatically translated into a query that is displayed in the query parser. For more information, see Researching Through Macie-Monitored Data (p. 40).

Activity Location

This view includes a map that shows the locations of activity that Macie is monitoring for a selected time period for the specified user. To view details, you can use the available time period pull-down menu (past 15 days, past 30 days, past 90 days, or past year), and then choose any location pin.

To navigate from this view to the **Research** tab, choose the number of events that appears in a tooltip window for a location pin. In the **Research** tab, your selection is automatically translated into a query that is displayed in the query parser. For more information, see Researching Through Macie-Monitored Data (p. 40).

CloudTrail Events

This view provides the complete list of Macie-monitored CloudTrail data and management events for the specified user. For each event, the total count of the user sessions (5-minute integrations of CloudTrail data) in which this event is present and the percentage that this total represents of the total number of user sessions is displayed.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed events. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab. For more information, see Researching Through Macie-Monitored Data (p. 40).

Activity ISPs

This view provides the complete list of Macie-monitored CloudTrail data and management events, grouped by the associated internet service providers (ISPs) for the specified user. For each ISP, the total count of the user sessions (5-minute integrations of CloudTrail data) in which this ISP is present and the percentage that this total represents of the total number of user sessions is displayed.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab. For more information, see Researching Through Macie-Monitored Data (p. 40).

CloudTrail User Identity Types

This view provides the complete list of Macie-monitored CloudTrail data and management events, grouped by the user identity type (for more information, see the definition for 'user' in Concepts and

Terminology (p. 3)) for the specified user. For each user identity type, the total count of the user sessions (5-minute integrations of CloudTrail data) in which this user identity type is present and the percentage that this total represents of the total number of user sessions is displayed.

To navigate from this view to the **Research** tab, you can choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that is displayed in the query parser in the **Research** tab. For more information, see Researching Through Macie-Monitored Data (p. 40).

Researching Through Macie-Monitored Data

You can use the **Research** tab in the Macie console to construct and run queries in the Query Parser and conduct in-depth investigative research of your Macie-monitored data and activity. You can navigate to the **Research** tab at any time and construct queries from scratch in the empty parser. For more information, see Constructing Queries in Macie (p. 40). Or you can be redirected to the **Research** tab from various places throughout the Macie console, for example, any of the **Dashboard** views (see Using the Macie Dashboard (p. 21)) or the **Basic alerts** list (see Amazon Macie Alerts (p. 28)). When redirected to the **Research** tab from other places in the console, your data selection is translated into an automatically generated query that is displayed in the query parser.

Topics

Constructing Queries in Macie

Macie allows you to construct queries in the Query Parser in the **Research** tab. This Query Parser is a lexer which interprets a string into a Lucene Query using JavaCC. For more information about query syntax, see Apache Lucene - Query Parser Syntax.

The following are example queries for common searches:

- You can use the following query to search for any console login not that did not originate from IP addresses owned by Amazon: `eventNameIsp.compound:/ConsoleLogin:~(Amazon.*)/`
- You can use the following query to search for PII artifacts inside a public S3 bucket: `filesystem_metadata.bucket:"my-public-bucket" AND (pii_impact:"moderate" OR pii_impact:"high")`

The following tables contains example queries for the Macie date, integer, and string field types:

Date field type example queries:

Example query	Description	Data repository
`objectsRead.key:* AND @timestamp:[2017-08-01 TO 2017-12-31]`	Search for S3 objects read in the fourth quarter of 2017.	CloudTrail data
`sourceIPAddress.ip_intel.type:"Tor" AND @timestamp:[now-1M TO now]`	Search for anonymous accesses to your Macie-monitored data	CloudTrail data

Example query	Description	Data repository
	from Tor exit notes over the last month.	
`macieUniqueId:"085924634393\:assumed-role\:malicious_user" AND @timestamp: [2018-01-18 TO *]`	Search for AWS activities of an assumed role named "malicious_user" in the AWS account ID 085924634393, starting from January 18, 2018.	CloudTrail data

Integer field type example queries:

Example query	Description	Data repository
`dlp_risk>6 AND filesystem_metadata.server_side_encrypted:"false"`	Search for S3 objects with a dlp_risk score greater than 6 and without a server-side encryption.	S3 objects
`filesystem_metadata.size: [10240 TO 1024000] AND pii_types:*`	Search for S3 objects between the sizes of 10 MB to 1 GB that contain potential PII data.	S3 objects

String field type example queries:

Example query	Description	Data repository
`dlp_risk>5 AND key: /.*contract.*|.*agreement.*|.*terms.*/ AND @timestamp:[now-1M/M TO now]`	Search for S3 object keys (names) that contain the keywords "contract","agreement", or "terms", with a dlp-risk score higher than 5, and that were last modified less than a month ago. **Note** Some regex queries may result in long search times. We recommend conducting searches for limited time frames.	S3 objects
`mimetypes:"Adobe PDF \(application/pdf\)" AND key: /~(.*\.pdf|.*\.PDF)/`	Search for S3 objects containing pdf data but in files with file extensions other than PDF/pdf. **Note** This query also returns archived objects (zip,7z, etc.) containing PDF documents.	S3 objects

Example query	Description	Data repository
`acl.Grants.Grantee.DisplayName: admin`	Search for S3 buckets with ACL grantee display names set to "admin".	S3 bucket properties
`acl.Grants.Grantee.DisplayName: admi?`	Search for S3 buckets with ACL grantee display names set to "admi(?)" (wildcard), including "admin".	S3 bucket properties
`bucket: *test*`	Search for S3 buckets with keywords "test".	S3 bucket properties

Research Filters

In the Macie **Research** tab, you can apply the following filters to your searches:

Data index

The first **Research** tab filter (pull-down list), with the pre-selected default value of **Cloudtrail data**, allows you to specifying the index (or the data repository) that you want Macie to search through. This filter includes the following options:

- **CloudTrail data** - a collection of 5-minute aggregates of raw Cloudtrail data
- **S3 bucket properties** - a collection of metadata about the S3 buckets that Macie is monitoring
- **S3 objects** - a collection of metadata about the S3 objects that are stored in the buckets that Macie is monitoring

Number of Results to Display

The next **Research** tab filter with the pre-selected default value of **Top 10**, allows you to control the number of results to display when you do your initial search and the number of additional results to display if more results are available. This filter includes the following options:

- Top 10
- Top 50
- Top 100
- Top 500

Time Range

The third **Research** tab filter with the pre-selected default value of **Past 30 days**, allows you to define a time range for which you want to display your search results. This filter includes the following options:

- Past 7 days
- Past 30 days
- Past 90 days
- Past 365 days

- All
- Custom time range

Save a Query as an Alert

You can use the following procedure to save a query that is displayed in the query parser as a basic alert. For more information about basic alerts, see Amazon Macie Alerts (p. 28).

1. In the Macie console's **Research** tab, either autogenerate or construct a query in the query parser.
2. Choose the **Save query as alert** icon.
3. Fill out the Basic alert definition form and then choose **Save**. For more information, see Adding New and Editing Existing Custom Basic Alerts (p. 31).

Favorite Queries

You can mark queries that you frequently run as favorite and quickly view a list of your favorite queries.

1. In the Macie console's **Research** tab, either autogenerate or construct a query in the query parser.
2. Choose the **Mark query as favorite** icon.
3. Fill out the **Favorite query definition** form by specifying the name and the description for the favorite query, and then choose **Save**.
4. To view the list of your favorite queries, in the Macie console's **Research** tab, choose the **Favorite queries** icon.

Researching AWS CloudTrail Data

Topics

Analyzing CloudTrail Search Results

The following section describes the elements of the search results that get displayed when you use the **Research** tab to investigate your Macie-monitored CloudTrail data.

Complete the following steps in the **Research** tab:

1. Select **CloudTrail data** in the first filter pull-down list.
2. For this sample procedure, select **Top 10** in the second filter pull-down list.
3. For this sample procedure, select **Past 90** days in the third filter pull-down list.
4. Choose the button with the looking glass icon to start the search.

Your search produces the following elements:

- The **total number of results** that matched your CloudTrail data search for the selected time range.
- The **graphical representation** of CloudTrail data search results for the selected time range.

Note
If your data set is very large and you specify a very wide time range, you data might not render properly and this graph might not be displayed as one of the resulting elements of your search.

Important
You can use the graph to further narrow your search and generate and run a query that will produce a subset of the results generated by your original selections in the steps above. Double-click any of the graph's results and your selection is translated into a new query that's automatically displayed in the **Query Parser**, and the **Research** tab is refreshed with the results of this new query.

- **Search results summary** - this is a list of the most significant fields from your search. The first line includes the top (or bottom) 3 values for each field. The second line includes the top (or bottom) 10 values for each field.

  Important
  You can use the fields in the search results summary to further narrow your search and generate and run a query that will produce a subset of the results generated by your original selections in the steps above. Choose the first or the second line of results for any field, and in the expanded results breakdown, choose the looking glass icon next to any of the results. Your choices are then translated into a new query that's automatically displayed in the **Query Parser**, and the **Research** tab is refreshed with the results of this new query.
- A list of **user sessions** (5-minute aggregates of CloudTrail data) that match your search criteria. You can choose any user session to expand it and view its details.

CloudTrail Data Fields and Sample Queries

The following tables include the fields that can appear in the results of your CloudTrail data searches.

- The first table includes the fields that Macie extracts from CloudTrail. These fields also include Amazon S3 data events. For example, accountId in Macie corresponds to userIdentity.accountId in Cloudtrail, or eventNameErrorCode.key in Macie corresponds to eventName in CloudTrail.
- The second table includes the fields that are generated by Macie to provide further security intelligence and context based on the examined CloudTrail data. For example, isp.key describes the organization or the ISP from where the API request against your AWS resources is coming, or sourceIPAddress.ip_intel.type describes the IP address history, for example, whether it's a Tor exit node that is being used to initiate API requests against your AWS resources.

CloudTrail Data Fields Extracted by Macie

Note
For this data repository (CloudTrail), your search always returns a list of user sessions - 5-minute aggregates of raw Cloudtrail data. A user session is determined by the Macie unique ID - a format that is unique to Macie for specifying users. Macie unique ID is a combination of the IAM UserIdentity element and the recipientAccountId.

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
accountId	userIdentity.accountId	string	The AWS account ID.	Search for user sessions with accesses related to a particular account: • **accountId:"110912345678"**

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
awsRegion.key	awsRegion	string	The AWS region to which the request is made.	Search for user sessions with any AWS API calls by region: • **awsRegion.key:"us-west-2"** • **awsRegion.key:"us-east-1"**
eventNameErrorCode.key	eventName	string	The event name that resulted in the returned (if any) error code.	• Search for user sessions with any AWS ConsoleLogin: • **eventNameErrorCode.key:Consol** • Search for user sessions with any AWS Delete call: • **eventNameErrorCode.key:Delete**
eventNameErrorCode.secondary	errorCode	string	The error code returned after an unsuccessful API request.	Search for user sessions with any "AccessDenied" error across all CloudTrail API events: • **eventNameErrorCode.secondary:"A**
eventSource.key	eventSource	string	The service to which the request was made.	Search for user sessions with any API calls of a particular AWS service: • **eventSource.key:"s3.amazonaws.co** • **eventSource.key:"lambda.amazona**
eventType.key	eventType	string	The type of the event that generated the event record (for example, AwsApiCall, AwsServiceEvent, or AwsConsoleSignIn).	Search for user sessions with any AWS API calls of a particular eventType: • **eventType.key:"AwsApiCall"**

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
objectsDeleted.key	Resources[0].ARN	string	A list of S3 objects', S3 buckets', or prefixes ARNs that were part of a DeleteObject or a DeleteObjects API calls. **Note** When you delete an S3 bucket, both DeleteBucket and DeleteObjects APIs are called, and the aggregate record with the DeleteObjects call lists the deleted bucket or prefix, not all the individual objects that were deleted. **Note** Objects that are part of a failed DeleteObject or DeleteObjects API call are also added to the aggregate record of objectsDeleted.key. **Note** A user session returning the results of a search against objectsDeleted.key has a maximum limit of 250 records.	Example search queries: • Search for all objects deleted from a particular bucket or prefix: • **objectsDeleted.key:/ arn:aws:s3:::my_sensitive_bucket** • Search for all Delete requests of a particular object that were made anonymously or by any user or role. • **objectsDeleted.key: "arn:aws:s3:::my-bucket-name/ sshKeys"** • Search for user sessions that contain both a DeleteObject:AccessDenied, and any attempt to delete a particular sensitive object, bucket, or prefix. • **objectsDeleted.key:/ arn:aws:s3:::my_sensitive_bucket AND eventNameErrorCode.compound** • Search for user sessions that contain both an attempt (or attempts) to delete S3 objects from outside of AWS and any attempt to delete a particular sensitive object, bucket, or prefix: • **objectsDeleted.key:/ arn:aws:s3:::my_sensitive_bucket AND eventNameIsp.compound:/ DeleteObject:~(Amazon.*)/** • Search for anonymous delete requests of a known sensitive object: • **objectsDeleted.key:/ arn:aws:s3:::my_sensitive_bucket**

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
				AND accountId:"ANONYMOUS_PRINC

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
objectsRead.key	Resources[0].ARN	string	A list of S3 objects' ARNs that were part of a GetObject API call. **Note** Objects that are part of a failed GetObject API call are also added to the aggregate record of objectsRead.key. **Note** A user session returning the results of a search against objectsRead.key has a maximum limit of 250 records.	Example search queries: • Search for user sessions with all objects read from a particular bucket or prefix: • **objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket** • Search for all access attempts of a particular object made either anonymously or by any user or role. • **objectsRead.key:"arn:aws:s3:::my bucket-name/ sshKeys"** • Search for user sessions that contain both a GetObject:AccessDenied, and any attempt to read a particular sensitive object, bucket, or prefix. • **objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket AND eventNameErrorCode.compound** • Search for user sessions that contain both an attempt (or attempts) to read S3 objects from outside of AWS and any attempt to read a particular sensitive object, bucket, or prefix: • **objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket AND eventNameIsp.compound:/ GetObject:~(Amazon.*)/** • Search for anonymous read accesses to a known sensitive object or bucket: • **objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket**

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
				AND accountId:"ANONYMOUS_PRINC

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
objectsWritten.key	resources[0].ARN	string	A list of S3 objects' ARNs that were part of a PutObject, CopyObject, or CompleteMultipartUpload API calls. **Note** Objects that are part of a failed PutObject API call are also added to the aggregate record of objectsWritten.key. **Note** A user session returning the results of a search against objectsWritten.key has a maximum limit of 250 records.	Example search queries: • Search for user sessions with all objects written to a particular bucket: • **objectsWritten.key:/ arn:aws:s3:::my_bucket_name.*/** • Search for user sessions with all write requests of a particular object made either anonymously or by any user or role: • **objectsWritten.key: "arn:aws:s3:::my-bucket-name/ sshKeys"** • Search for user sessions that contain both a PutObject:AccessDenied, and any attempt to read a particular sensitive object, bucket, or prefix. • **objectsWritten.key:/ arn:aws:s3:::my_sensitive_bucket AND eventNameErrorCode.compound** • Search for user sessions that contain both an attempt (or attempts) to write S3 objects from outside of AWS and any attempt to write a particular sensitive object, bucket, or prefix: • **objectsWritten.key:/ arn:aws:s3:::my_sensitive_bucket AND eventNameIsp.compound:/ PutObject:~(Amazon.*)/** • Search for anonymous write requests to a sensitive object or bucket:

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
				• **objectsWritten.key:/ arn:aws:s3:::my_sensitive_bucket AND accountId:"ANONYMOUS_PRINC**
principalId	userIdentity.principalId	string	The IAM principal ID. **Note** When a request is made by an assumed role, the session name is removed from the principal ID.	Search for user sessions wtih access requests from a particular principal ID: • **principalId:"AIDAIMABCKFJSKEOAI**
recipientAccountId	recipientAccountId	string	The AWS account ID that received the CloudTrail event.	• Search for all activity in a particular AWS account: • **recipientAccountId:"110912345** • Search for anonymous access requests to a particular AWS account: • **recipientAccountId:"110912345 AND accountId: "ANONYMOUS_PRINCIPAL"**
resourceOwnerAccountIds.key	Resources[0].accountId	string	List of AWS resource owners. For example, a list of AWS account IDs that own an S3 object or bucket.	Search for activity against resources owned by a particular AWS account: • **resourceOwnerAccountIds.key: "110951234567"**
resources.key	Resources[0].accountId	string	List of resources (S3 buckets only) associated with the CloudTrail events within the user session.	• Search for access requests to a particular S3 bucket: • **resources.key: "arn:aws:s3:::my-bucket-name"** • Search for anonymous access requests to a known sensitive bucket: • **resources.key: "arn:aws:s3:::my-super-sensitive-bucket" AND accountId:"ANONYMOUS_PRINC**

Macie field name	CloudTrail field name	Macie field type	Description	Example search query

sessionName.key	userIdentity.principalId	string	The identifier for the assumed role session. When a request is made by an assumed role, the session name is removed from the principal ID and is assigned as a value to sessionName.key. When a request is made by an identity other than assumed role, sessionName.key is set to 'None'.	• Search for assumed role access requests from session name 'examplesession-cli':
				  • **sessionName.key:"examplesessio cli"**
				• Search for EC2 instance IDs within session names:
				  • **(sessionName.key:/ i-[0-9a-f]{8}/ OR sessionName.key:/ i-[0-9a-f]{17}/)**
				• Search for assumed role access requests to a role from a sessionName other than 'examplesession-cli' using regex negation:
				  • **macieUniqueId: "123456789123:assumed-role:co-admin" AND sessionName.key:/ ~(examplesession-cli)/**

sourceARN	userIdentity.arn	string	The ARN used to make the request. **Note** When a request is made by an assumed role, the session name is removed from the sourceARN.	Search for user sessions with access requests from a particular ARN: • **sourceARN:"arn:aws:iam::1234567 cluster-api"**

Macie field name	CloudTrail field name	Macie field type	Description	Example search query
sourceIPAddress.key	sourceIPAddress	string	The IP address from which the request was made. **Note** A user session returning the results of a search against sourceIPAddress.key has a maximum limit of 60000 records.	• Search for user sessions with access requests from a particular source IP address: • **sourceIPAddress.key:"194.68.22.** • Search through user sessions with source IP addresses using wildcards: • **sourceIPAddress.key:194.68.*.*** • Search for user sessions with more than 10 RunInstances events and without any events requested by the autoscaling group: • **eventNameErrorCode.RunInstan AND NOT (sourceIPAddress.key:"autoscalin**
userAgent.key	userAgent	string	A list of client user agent strings used to make the AWS API call.	Search for user sessions with API calls executed by AWS S3: • **userAgent.key:"s3.amazonaws.com**
userIdentityType.key	userIdentity.type	string	A list of identity types in AWS.	Search for user sessions with access requests by the root identity in an AWS account: • **userIdentityType.key:"Root"**

Fields Generated by Macie

Note
For this data repository (CloudTrail), your search always returns a list of user sessions - 5-minute aggregates of raw Cloudtrail data. A user session is determined by the Macie unique ID - a format that is unique to Macie for specifying users. Macie unique ID is a combination of the IAM UserIdentity element and the recipientAccountId.

Macie field name	Macie field type	Description	Example search query
@timestamp	date	The start time of a user session.	• Search for user sessions with access requests after a specific time: • **@timestamp:>"2017-02-06T23:01:08** • **@timestamp:>"2017-02-06"**

Macie field name	Macie field type	Description	Example search query
			• Search for user sessions with access requests between two time intervals: • **@timestamp: [2017-02-01 TO 2017-02-27]**
countLongLifeAccessToken	integer	A count of GetSessionToken API calls with a lifespan longer than the default 43200 seconds.	Search for user sessions with a user or role creating a temporary access token with a longer than the default lifespan: • **countLongLifeAccessToken:>0**
dcObjectsDeleted	integer	A count of unique S3 objects deleted in a user session. **Note** A user session returning the results of a search against dcObjectsDeleted has a maximum limit of 250 entries.	Search for user sessions with more than 25 distinct objects deleted by an AWS user or a role: • **dcObjectsDeleted:>25** • **dcObjectsDeleted:[25 TO 100]**

dcObjectsRead	integer	A count of unique S3 objects read in a user session.
		Note
		A user session returning the results of a search against dcObjectsRead has a maximum limit of 250 entries.
			• Search for user sessions with more than 25 distinct objects read by an AWS user or a role:
			  • **dcObjectsRead:>25**
			  • **dcObjectsRead:[25 TO 100]**
			• Search for more than 25 distinct objects read by an anonymous principal during a user session:
			  • **dcObjectsRead:>25 AND accountId:"ANONYMOUS_PRINCIPAL"**

dcObjectsWritten	integer	A count of unique S3 objects written in a user session. **Note** A user session returning the results of a search against dcObjectsWritten has a maximum limit of 250 entries.	Search for user sessions with more than 25 distinct objects written by an AWS user or a role: • **dcObjectsWritten:>25** • **dcObjectsWritten:[25 TO 100]**

Macie field name	Macie field type	Description	Example search query
distinctEventName	integer	A count of unique event names that take place in a user session.	Search for user sessions with more than 25 unique API calls being executed by a user or a role: • **distinctEventName:>25** • **distinctEventName:[25 TO 100]**
distinctSourceIPAddress	integer	A count of unique source IP addresses involved in activity that takes place in a user session. The maximum value of this count is 60,000.	Search for user sessions with more than 25 distinct source IP addresses observed for a user or a role: • **distinctSourceIPAddress:>25** • **distinctSourceIPAddress:[25 TO 100]**
distinctUserAgent	integer	A count of unique client user agents involved in activity that takes place in a user session. The maximum value of this count is 60,000.	Search for user sessions with more than 25 user agents observed for a user or a role: • **distinctUserAgent:>25** • **distinctUserAgent:[25 TO 100]**
eventNameErrorCode.compound	string	A compound aggregation that summarizes each CloudTrail event name along with any error codes that are associated with the API Call. The format is EventName:ErrorCode for the term value, which allows Macie to associate an API event name with the error code, if any, that is returned. If there is no error code for the event, then the value is set only to the API name with no colon, for example: "PutObject".	• Search for user sessions with "AccessDenied" error while attempting a GetObject call: • **eventNameErrorCode.compound:"Get** • Search for user sessions with any errors associated with PutObject calls: • **eventNameErrorCode.compound:/PutObject:.*/**
eventNameIsp.compound	string	A compound aggregation that summarizes each CloudTrail event name along with the Internet Service Provider (ISP) from which the request originated. The format is EventName:ISP for the term value, which allows Macie to associate an API operation name with the ISP from which it originated.	Search for user sessions with ConsoleLogins from non-AWS IPs using a regular expression: • **eventNameIsp.compound:/ConsoleLogin:~(Amazon.*)/**

Macie field name	Macie field type	Description	Example search query
eventNameIsp.secondary	string	The ISP from which the AWS API call was made.	Search for user sessions with AWS API calls coming from outside of Amazon IP addresses: • **eventNameIsp.secondary:/~(Amazon.*)/**
macieUniqueId	string	A format that is unique to Macie for specifying users. Macie unique ID is a combination of the IAM UserIdentity element and the recipientAccountId. For more information, see MacieUniqueID (p. 35).	Search for user sessions with accesses from a particular role, user, or root account: • **macieUniqueId:"123456789123:assume role:co-admin"** • **macieUniqueId:"123456789123:root:roo** • **macieUniqueId:"123456789123:user:exa**
sourceIPAddress.ip_intel.type	string	The IP intelligence category associated with a source IP address.	• Search for user sessions with all accesses from a Tor network: • **sourceIPAddress.ip_intel.type:"TOR"** • Search for user sessions with all accesses from threat intelligence input feeds: • **sourceIPAddress.ip_intel.type:***
windowStartTimeInMillis	integer	The epoch timestamp for the start of a user session.	Search for user sessions whose first event time is greater than a given epoch time: • **windowStartTimeInMillis:>1424476529**
windowEndTimeInMillis	integer	The epoch timestamp for the end of a user session.	Search for user sessions whose last event time is less than a given epoch time: • **windowEndTimeInMillis:<1424476987**
ipLocation.key	string	IP geolocation (city and country) accessed by a Macie-monitored identity.	• Search for user sessions with any AWS API call events originating in Los Angeles: • **ipLocation.key:"LosAngeles:UnitedSta** • Search for user session any AWS API call events originating from outside of the United States: • **ipLocation.key:/~(.*UnitedStates)/**

Macie field name	Macie field type	Description	Example search query
isp.key	string	The ISP from which the AWS API call originated.	Search for user sessions with AWS API calls coming from outside of Amazon IP addresses: • **isp.key:/~(Amazon.*)/**

Researching S3 Bucket Properties Data

Topics

Analyzing S3 Buckets Properties Search Results

The following section describes the elements of the search results that get displayed when you use the **Research** tab to investigate your Macie-monitored S3 bucket properties data.

Complete the following steps in the **Research** tab:

1. Select **S3 bucket properties** in the first filter pull-down list.
2. For this sample procedure, select **Top 10** in the second filter pull-down list.
3. For this sample procedure, select **Past 90** days in the third filter pull-down list.
4. Choose the button with the looking glass icon to start the search.

Your search results contain the following elements:

- The **total number of results** that matched your S3 bucket properties data search for the selected time range.
- The **graphical representation** of the S3 bucket properties data search results for the selected time range.

  Note
  If your data set is very large and you specify a very wide time range, you data might not render properly and this graph might not be displayed as one of the resulting elements of your search.

  Important
  You can use the graph to further narrow your search and generate and run a query that will produce a subset of the results generated by your original selections in the steps above. Double-click any of the graph's results and your selection is translated into a new query that's automatically displayed in the **Query Parser**, and the **Research** tab is refreshed with the results of this new query.
- **Search results summary** - this is a list of the most significant fields from your search. The first line includes the top (or bottom) 3 values for each field. The second line includes the top (or bottom) 10 values for each field.

  Important
  You can use the fields in the search results summary to further narrow your search and generate and run a query that will produce a subset of the results generated by your original selections in the steps above. Choose the first or the second line of results for any field, and

in the expanded results breakdown, choose the looking glass icon next to any of the results. Your choices are then translated into a new query that's automatically displayed in the **Query Parser**, and the **Research** tab is refreshed with the results of this new query.

- A list of S3 buckets that match your search criteria. You can choose any bucket to expand it and view its details.

S3 Bucket Properties Data Fields and Sample Queries

The following tables include the fields that can appear in the results of your S3 buckets metadata searches.

- The first table includes the fields that Macie extracts from the Amazon S3 bucket API metadata. For example, **acl.Grants.Grantee.DisplayName** in Macie corresponds to **Grants.Grantee.DisplayName** in the S3 Get Bucket acl API response.
- The second table includes the fields that are generated by Macie to provide further security intelligence and context based on the examined S3 buckets metadata. For example, **s3_world_readability** describes a true/false/unknown state condition of whether an S3 bucket is readable by everyone as part of evaluating its S3 ACL and bucket (IAM) policy.

S3 Bucket Properties Data Fields Extracted by Macie

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
acl.Grants.Grantee.DisplayName	Grants.Grantee.DisplayName	Get-bucket-acl	string	The display name of the S3 bucket ACL grantee.	Search for S3 buckets accessible by John Doe: • **acl.Grants.Grantee.DisplayNam**
acl.Grants.Grantee.ID	Grants.Grantee.ID	Get-bucket-acl	string	The ID of the identity that was granted access to the S3 bucket by the bucket owner.	Search for an S3 bucket's grantee with a particular canonical ID: • **acl.Grants.Grantee.ID:"75bee88**
acl.Grants.Grantee.Type	Grants.Grantee.Type	Get-bucket-acl	string	The user type of the S3 bucket ACL grantee.	• Search for all S3 buckets that are granted to Users: • **acl.Grants.Grantee.Type:Canc** • Search for all S3 buckets that are granted to Groups: • **acl.Grants.Grantee.Type:Grou**
acl.Grants.Grantee.URI	Grants.Grantee.URI	Get-bucket-acl	string	The URI identifier of the S3 bucket ACL grantee.	• Search for all S3 buckets except those that belong to the LogDelivery group:

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
					• **acl.Grants.Grantee.URI:"http: acs.amazonaws.com/ groups/s3/ LogDelivery"** • Search for all S3 buckets that have global share permissions: • **acl.Grants.Grantee.URI:"http: acs.amazonaws.com/ groups/global/ AllUsers"** • Search for all S3 buckets that allow access to (any) AWS authenticated users: • **acl.Grants.Grantee.URI:"http: acs.amazonaws.com/ groups/global/ AuthenticatedUsers"**
acl.Grants.Permissions	Grants.Permission	get-bucket-acl	string	The permission level assigned to the ACL grantee.	Search for S3 buckets that grant full (read/write) access to anyone: • **acl.Grants.Grantee.URI:"http:// acs.amazonaws.com/ groups/global/ AllUsers" AND acl.Grants.Permission:"FULL_C**
acl.Owner.DisplayName	Owner.DisplayName	get-bucket-acl	string	The display name of the S3 bucket owner.	Search for S3 buckets owned by John Doe: • **acl.Owner.DisplayName: "JohnDoe"**
acl.Owner.ID	Owner.ID	get-bucket-acl	string	The ID of the S3 bucket owner.	Search for a particular S3 bucket owner ID: • **acl.Owner.ID:"73bee78dfe7b89**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
location.LocationConstraint	LocationConstraint	get-bucket-location	string	The AWS region where the S3 bucket resides. **Note** By default, buckets in us-east-1 region have no region returned from the S3 API call. In order to facilitate searching, Macie automatically populates these with the string "us-east-1".	• Search for buckets hosted in the us-west-2 region: • **location.LocationConstraint:" west-2"** • Search for buckets hosted in the us-east-1 region: • **location.LocationConstraint:" east-1"**
logging.LoggingEnabled.TargetBucket	LoggingEnabled.TargetBucket	get-bucket-logging	string	Specifies the bucket whose logging status is being returned.	Search for all buckets with S3 object level logging enabled: • **logging.LoggingEnabled.Target**
logging.LoggingEnabled.TargetPrefix	LoggingEnabled.TargetPrefix	get-bucket-logging	string	The configured prefix or folder containing Object Level Logging data for a particular S3 bucket.	Search for buckets configured with a prefix substring of "Production": • **logging.LoggingEnabled.Target "Production"**
policy.Policy.Id	Policy.Id	get-bucket-policy	string	The ID for an S3 bucket policy.	Search for bucket policies with a particular ID: • **policy.Policy.Id:"aaaa-bbbb-cccc-dddd"**
policy.Policy.Statement.Action	Policy.Statement.Action	get-bucket-policy	string	The list of actions (API requests) associated with an S3 bucket policy.	Search for bucket policies with "put" substring actions (for example, PutObject,PubBucketPolicy, etc.): • **policy.Policy.Statement.Action: s3:Put.*/**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
policy.Policy.Statement.Effect	Policy.Statement.Effect	get-bucket-policy	string	The list of policy effects associated with an S3 bucket policy.	Search for bucket policies with explicit "allow" grants: • **policy.Policy.Statement.Effect: "Allow"**
policy.Policy.Statement.NotPrincipal.AWS	Policy.Statement.NotPrincipal.AWS	get-bucket-policy	string	The principal exception to which the policy rule is applied.	Search for bucket policies with a particular account specified in the NotPrincipal section: • **policy.Policy.Statement.NotPri account-ID:role/ role-name"**
policy.Policy.Statement.NotPrincipal.CanonicalUser	Policy.Statement.NotPrincipal.CanonicalUser	get-bucket-policy	string	The CanonicalUser stated in the NotPrincipal expression of the policy.	Search for bucket policies with a particular CanonicalUser specified in the NotPrincipal section: • **policy.Policy.Statement.NotPri**
policy.Policy.Statement.NotPrincipal.Federated	Policy.Statement.NotPrincipal.Federated	get-bucket-policy	string	The Federated identity stated in the NotPrincipal expression of the policy.	Search for bucket policies with a particular Federated user specified in the NotPrincipal section: • **policy.Policy.Statement.NotPri account-ID:saml-provider/ provider-name"**
policy.Policy.Statement.NotPrincipal.Service	Policy.Statement.NotPrincipal.Service	get-bucket-policy	string	The Service stated in the NotPrincipal expression of the policy.	Search for bucket policies with a particular Service specified in the NotPrincipal section: • **policy.Policy.Statement.NotPri**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
policy.Policy.Statement.Principal.AWS	Policy.Statement.Principal.AWS	GetBucketPolicy	string	The principal specified in the AWS expression.	Search for bucket policies with explicit allow grants to any AWS resource: • **policy.Policy.Statement.Effect: Allow AND policy.Policy.Statement.Princip \"*\"**
policy.Policy.Statement.Principal.CanonicalUser	Policy.Statement.Principal.CanonicalUser	GetBucketPolicy	string	The CanonicalUser stated in the principal expression of the policy.	Search for bucket policies with a particular CanonicalUser specified in the Principal section: • **policy.Policy.Statement.Princip**
policy.Policy.Statement.Principal.Federated	Policy.Statement.Principal.Federated	GetBucketPolicy	string	The Federated identity stated in the principal expression of the policy.	Search for bucket policies with a particular Federated user specified in the NotPrincipal section: • **policy.Policy.Statement.NotPri account-ID:saml-provider/ provider-name"**
policy.Policy.Statement.Principal.Service	Policy.Statement.Principal.Service	GetBucketPolicy	string	The Service stated in the principal expression of the policy.	Search for bucket policies with a particular Service user specified in the NotPrincipal section: • **policy.Policy.Statement.NotPri**
policy.Policy.Statement.Resource	Policy.Statement.Resource	GetBucketPolicy	string	The S3 resource to which the S3 bucket policy is applied.	Search for S3 bucket policies containing wildcards: • **policy.Policy.Statement.Resour */**
policy.Policy.Statement.Sid	Policy.Statement.Sid	GetBucketPolicy	string	The Sid of the S3 bucket policy.	Search for bucket policies with a particular Sid: • **policy.Policy.Statement.Sid:"1"**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
policy.Policy.Version	Policy.Version	get-bucket-policy	string	The version number for the S3 bucket policy.	Search for bucket policies with a particular version: • **policy.Policy.Statement.Version**
tagging.TagSet.Key	TagSet.Key	get-bucket-tagging	string	The key of the S3 bucket tag.	Search for bucket policies with a particular tag key: • **tagging.TagSet.Key:"User"**
tagging.TagSet.Value	TagSet.Value	get-bucket-tagging	string	The value of the S3 bucket tag.	Search for bucket policies with a particular tag value: • **tagging.TagSet.Value:"johndoe"**
versioning.MFADelete	MFADelete	get-bucket-versioning	string	The MFA delete (enabled/disabled) state of the bucket version configuration.	Search for buckets where MFA delete is enabled in the bucket versioning configuration: • **versioning.MFADelete:"enabled**
website.ErrorDocument.Key	ErrorDocument.Key	get-bucket-website	string	The error document configured as part of S3 static website hosting.	Search for S3 buckets configured for static website hosting and with an error page redirection to 404.html: • **website.ErrorDocument.Key: "404.html"**
website.IndexDocument.Suffix	IndexDocument.Suffix	get-bucket-website	string	The suffix of a webpage that Amazon S3 returns when a request is made to the root of a website or any subfolder.	Search for the index document configured as part of S3 static website hosting and with an index page redirection to index.html: • **website.IndexDocument.Key: "index.html"**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
• lifecycle_configuration.Rules.Expiration.Date • lifecycle_configuration.Rules.Expiration.Days • lifecycle_configuration.Rules.AbortIncompleteMultipartUpload.DaysAfterInitiation • lifecycle_configuration.Rules.Filter.Prefix • lifecycle_configuration.Rules.Filter.Tag.Key • lifecycle_configuration.Rules.Filter.Tag.Value • lifecycle_configuration.Rules.ID • lifecycle_configuration.Rules.NoncurrentVersionExpiration.NoncurrentDays • lifecycle_configuration.Rules.NoncurrentVersionTransitions.NoncurrentDays • lifecycle_configuration.Rules.NoncurrentVersionTransitions.StorageClass • lifecycle_configuration.Rules.Prefix • lifecycle_configuration.Rules.Status • lifecycle_configuration.Rules.Transitions.Date • lifecycle_configuration.Rules.Transitions.Days • lifecycle_configuration.Rules.Transitions.StorageClass	Rules.Expiration.Date Rules.Expiration.Days Rules.AbortIncompleteMultipartUpload.DaysAfterInitiation Rules.Filter.Prefix Rules.Filter.Tag.Key Rules.Filter.Tag.Value Rules.ID Rules.NoncurrentVersionExpiration.NoncurrentDays Rules.NoncurrentVersionTransitions.NoncurrentDays Rules.NoncurrentVersionTransitions.StorageClass Rules.Prefix Rules.Status Rules.Transitions.Date Rules.Transitions.Days Rules.Transitions.StorageClass	GetBucketLifecycleConfiguration: Lifecycle configuration	• date • integer • integer • string • string • string • string • integer • integer • string • string • string • date • integer • string	For more information, see GET Bucket lifecycle.	Search for the S3 buckets with a lifecycle configuration rule whose expiration is less than 3 days: • **lifecycle_configuration.Rules.Ex**

S3 Bucket Properties Data Fields Generated by Macie

Macie field name	Macie field type	Description	Example search query
@timestamp	date	The timestamp when the bucket was last analyzed by Macie.	Search for S3 buckets analyzed by Macie in the last 24 hours: • **@timestamp:[now-1d TO now]**
accountId	string	The AWS Account ID of the S3 bucket owner.	Search for any S3 buckets that do not belong to a given AWS account: • **NOT accountId: 110912345678**
bucket	string	The name of an S3 bucket.	Search for a particular S3 bucket by name: • **bucket: "MyBucket"**
s3_world_readability	string	A "true" or "false" or "unknown" value indicating whether the S3 bucket is globally readable. The "unknown" value indicates that Macie is unable to determine whether the S3 bucket is globally readable.	Search for S3 buckets that are globally readable either by the S3 ACL or bucket (IAM) policy: • **s3_world_readability: "true"**

Macie field name	Macie field type	Description	Example search query
s3_world_writability	string	A "true" or "false" or "unknown" value indicating if the S3 bucket is globally writable. The "unknown" value indicates that Macie is unable to determine whether the S3 bucket is globally writable.	Search for S3 buckets that is globally writable either by the S3 ACL or the bucket (IAM) policy: • **s3_world_writability: "true"**

Researching S3 Objects Data

Topics

Analyzing S3 Objects Search Results

The following section describes the elements of the search results that get displayed when you use the **Research** tab to investigate your Macie-monitored S3 objects.

Complete the following steps in the **Research** tab:

1. Select **S3 objects** in the first filter pull-down list.
2. For this sample procedure, select **Top 10** in the second filter pull-down list.
3. For this sample procedure, select **Past 90** days in the third filter pull-down list.
4. Choose the button with the looking glass icon to start the search.

Your search results include the following elements:

- The **total number of results** that matched your S3 objects search for the selected time range.
- The **graphical representation** of the S3 objects search results for the selected time range.

  Note
  If your data set is very large and you specify a very wide time range, you data might not render properly and this graph might not be displayed as one of the resulting elements of your search.

  Important
  You can use the graph to further narrow your search and generate and run a query that will produce a subset of the results generated by your original selections in the steps above. Double-click any of the graph's results and your selection is translated into a new query that's automatically displayed in the **Query Parser**, and the **Research** tab is refreshed with the results of this new query.
- **Search results summary** - this is a list of the most significant fields from your search. The first line includes the top (or bottom) 3 values for each field. The second line includes the top (or bottom) 10 values for each field.

  Important
  You can use the fields in the search results summary to further narrow your search and generate and run a query that will produce a subset of the results generated by your original selections in the steps above. Choose the first or the second line of results for any field, and

in the expanded results breakdown, choose the looking glass icon next to any of the results. Your choices are then translated into a new query that's automatically displayed in the **Query Parser**, and the **Research** tab is refreshed with the results of this new query.

- A list of S3 objects that match your search criteria. You can choose any S3 object to expand it and view its details.

S3 Objects Data Fields and Sample Queries

The following tables include the fields that can appear in the results of your S3 object searches.

- The first table includes the fields that Macie extracts from the Amazon S3 object API metadata. These are Macie fields that are also found in S3 API metadata. For example, filesystem_metadata.ETag describes the entity tag of an S3 object based on the checksum or hash of its content.
- The second table includes the fields that are generated by Macie to provide further security intelligence and context based on the examined S3 objects content and metadata. For example, dlp_risk represents a weighted score describing the risk profile of an S3 object metadata and its content, or pii_types describes any personal identifiable information contained in an S3 object.

S3 Object Data Fields Extracted by Macie

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
key	key	get-bucket (listObjects)	string	The S3 object key path.	Search for document names with the keyword 'myobject' • **key: /.*myobject.*/**
accountId	None	None	string	The AWS account ID that owns the S3 object.	Search for S3 objects owned by a particular AWS account ID: • **accountId:"110912345678"**
filesystem_metadata.bucket	None	None	string	The S3 bucket name that holds the S3 object.	Search for S3 objects in a particular S3 bucket: • **filesystem_metadata.bucket:"M**
filesystem_metadata.first_prefix	None **Note** Macie uses the S3 key field and	get-bucket (listObjects)	string	The name of the first folder that contains the S3 object.	Search for S3 objects contained in first folder names where folder name is AWSLogs: • **filesystem_metadata.first_prefi**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
	parses out everything before the first '/', not including the bucket name.				
filesystem_metadata.ETag	ETag	get-bucket (listBuckets)	string	The entity tag as defined in RFC 2616.	Search for a particular eTag: • **filesystem_metadata.ETag:""8b**
filesystem_metadata.bucket_owner.id	ID	get-bucket-acl	string	The unique ID of the S3 bucket owner.	Search for S3 objects belonging to a particular owner ID: • **filesystem_metadata.bucket_ow "447fba12b05da301df359096f**
filesystem_metadata.bucket_owner.name	Owner	get-bucket-acl	string	The name of the S3 bucket owner.	Search for S3 objects owned by John Doe: • **filesystem_metadata.bucket_ow "JohnDoe"**
filesystem_metadata.last_modified	LastModified	get-bucket (list-buckets)	date	The timestamp when the S3 object was last modified.	Search for S3 objects that were modified in the last 24 hours: • **filesystem_metadata.last_modi [now-1d TO now]**
filesystem_metadata.server_side_encryption	ServerSideEncryption	get-object	string	The server side encryption used to encrypt an S3 object.	Search for objects that are not encrypted with the AES256 standard: • **NOT filesystem.metadata.server_enc "AES256"**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
filesystem_metadata.size	Size	get-bucket (list-buckets)	integer	The size of the S3 object's content in bytes.	Search for S3 objects that are larger than 1 MB: • **filesystem.metadata.size: > 1024000**
filesystem_metadata.sse_kms_key_id	SSEKMSKeyId	get-object	string	The unique identifier (ARN) of the master key used for server side encryption of the S3 objects.	Search for all S3 objects encrypted with a given key ID: • **filesystem_metadata.sse_kms_k "arn:aws:kms:us-west-2: 110912345678:key/06f8b4fa-3 b60a56a9a1f2"**
object_acl.Grants.Grantee.DisplayName	Grants.Grantee.DisplayName	get-object-acl	string	The ACL grantee name.	Search for S3 object ACL permissions granted to John Doe: • **object_acl.Grants.Grantee.Displ "JohnDoe"**
object_acl.Grants.Grantee.ID	Grants.Grantee.ID	get-object-acl	string	The ACL grantee unique ID.	Search for S3 object ACL permissions with a particular Grantee ID: • **object_acl.Grants.Grantee.ID:"7**
object_acl.Grants.Grantee.Type	Grants.Grantee.Type	get-object-acl	string	The ACL grantee type, such as "CanonicalUser" or "Group".	Search for all S3 object ACLs that are granted to users or groups: • **object_acl.Grants.Grantee.Type** • **object_acl.Grants.Grantee.Type**
object_acl.Grants.Grantee.URI	Grants.Grantee.URI	get-object-acl	string	The ACL grantee URI.	Search for S3 object ACLs with the AllUsers grant: • **object_acl.Grants.Grantee.URI: "http:// acs.amazonaws.com/ groups/global/ AllUsers"**

Macie field name	Amazon S3 API field name	Amazon S3 API operation	Macie field type	Description	Example search query
object_acl.Grants.Permission	Grants.Permission	get-object-acl	string	The ACL grantee permission.	Search for S3 object ACLs that grant full control: • **object_acl.Grants.Permission: "FULL_CONTROL"**
object_acl.Owner.DisplayName	Owner.DisplayName	get-object-acl	string	The ACL owner name.	Search for S3 objects owned by John Doe: • **object_acl.Owner.DisplayName "JohnDoe"**
object_acl.Owner.ID	Owner.ID	get-object-acl	string	The ACL owner ID.	Search for S3 objects belonging to a particular owner ID: • **object_acl.Owner.ID: "447fba12b05da301df359096f**

S3 Object Data Fields Generated by Macie

Macie field name	Macie field type	Description	Example search query
@timestamp	date	The timestamp when the S3 object was last modified.	Search for S3 objects classified by Macie in the last 24 hours: • **@timestamp:[now-1d TO now]**
content_type	string	The content and encoding type of the S3 object. **Note** You can locate this value in the **Name** field for a particular content type in the **Content types** section of the **Settings** page in the Macie console.	Search for java source code containing hard-coded AWS credentials: • **content_type:"text/x-java-source" AND regex_themes: "aws_access_key"** • **content_type:"text/x-java-source" AND regex_themes: "aws_access_key"**
dlp_risk	integer	Through the automatic classification methods, a Macie-monitored object is assigned various risk levels based on each content type, file extension, theme, regex,	Search for globally accessible (Read or Write) objects with the compound (final) risk level of 5 or higher:

Macie field name	Macie field type	Description	Example search query
		PII, and SVM artifact that is assigned to it. The object's compound (final) risk level (dlp_risk) is set to the highest value of its assigned risk levels. **Note** You can find risk levels in the **Settings** page of the Macie console for their respective supported data classifiers.	• **object_acl.Grants.Grantee.URI: "http://acs.amazonaws.com/groups/global/AllUsers" AND dlp_risk>5**
encoding	string	The encoding scheme identified when analyzing the S3 object content.	Search for Unicode text documents: • **encoding: "utf-8"**
filetype_risk	integer	The risk level assigned to an S3 object based on its file extension. **Note** You can find risk levels in the **Settings** page of the Macie console for their respective supported data classifiers.	Search for documents with the assigned file extension risk of greater than 6: • **filetype_risk: > 6**
filetypes	string	The type of the file based on the extension. **Note** You can locate this value in the **Name** and **Description** fields for a particular file type in the **File extensions** section of the **Settings** page in the Macie console.	Search for files with an extension of (.pdf): • **filetypes: "Adobe PDF (.pdf)"**
keyword_themes	string	The themes assigned to S3 object. You can find supported themes in the **Settings** page of the Macie console.	Search for S3 objects containing content related to Social Security • **keyword_themes: "Social Security Keywords"**

Macie field name	Macie field type	Description	Example search query
language_code	string	The language code found when analyzing the S3 object's content.	Search for S3 objects containing German keywords: • **language_code: "de"**
last_crawl_time	date	The timestamp of when an S3 object was last analyzed by Macie.	Search for S3 objects analyzed by Macie in the last 24 hours: • **last_crawl_time: [now-1d/d TO now]**
mimetype_risk	integer	The risk level based on an S3 objects content / mime type.	Search for S3 objects containing mimetypes associated with high risk content: • **mimetype_risk: > 5**
mimetypes	string	The mimetype of an S3 object.	Search for Plaintext documents containing AWS secret keys: • **mimetypes: "Plain Text (text/plain)" AND themes: aws_secret_key**
pii_impact	string	The Macie-assigned PII severity impact of an S3 object.	Search for S3 objects containing highly valuable personal identifiable information: • **pii_impact: "high"**
pii_types	string	The specific type of PII found in an S3 object.	Search for S3 objects containing emails: • **pii_types: "email"**
regex_risk	integer	The risk level based on an S3 object's Macie-assigned regex.	Search for S3 objects with a regex-based risk level greater than 5: • **regex_risk: > 5**
regex_themes	string	The regex themes of an S3 object.	Search for S3 objects containing RSA private keys • **regex_themes: "RSA Private Key"**
theme_risk	string	The risk level based on the Macie-assigned themes of an S3 object.	Search for S3 objects with a theme-based risk level higher than 5: • **theme_risk: > 5**

Macie field name	Macie field type	Description	Example search query
themes	string	The combined themes of an S3 object.	Search for S3 objects containing RSA private keys: • **themes: "RSA Private Key"**

Access Control in Amazon Macie

The master account users have access to the Macie console where they can configure Macie and use it to monitor and protect the resources in both master and member accounts. (For more information about master and member accounts, see Concepts and Terminology (p. 3) and Integrate Member Accounts and Amazon S3 with Amazon Macie (p. 10)).

Grant Macie Administrator Access

In order for the master account users to be able to use the Macie console, they must be granted the required permissions. To ensure this, you can use the following policy document to create and attach an IAM policy to any user identity type that belongs to your master Macie account. This policy grants master account users permissions to use the Macie console in its full capacity:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "macie:*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"iam:CreateServiceLinkedRole",
         "Resource":"*",
         "Condition":{
            "StringLike":{
               "iam:AWSServiceName":"macie.amazonaws.com"
            }
         }
      }
   ]
}
```

Grant Macie Read-Only Access

In order for a user to view any data in the Macie console, they must be granted the required permissions. To grant read-only access, you can create a custom policy using the following policy document and attach it to a IAM user, group, or role. This policy grants users permissions to only view information in the Macie console:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "macie:Get*",
                "macie:List*",
```

```
                "macie:Describe*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Note
Currently, there is no AWS managed policy that can be used to grant read-only access to Macie.

AWS Managed (Predefined) Policies for Macie

AWS addresses many common use cases by providing standalone IAM policies that are created and administered by AWS. Managed policies grant necessary permissions for common use cases so you can avoid having to investigate what permissions are needed.

The following AWS managed policies, which you can attach to users in your account, are specific to Macie:

- **AmazonMacieFullAccess** - Provides full access to Macie.
- **AmazonMacieSetupRole** - Provides Macie with access to your AWS account.
- **AmazonMacieServiceRole** - Grants Macie read-only access to resource dependencies in your account in order to enable data analysis.

Disabling Amazon Macie and Deleting Collected Metadata

You can use the Macie general settings page in the Macie console to disable Macie.

> **Important**
> Only the master Macie account can disable Macie. In order for Macie to be disabled in a member account, the master account must disassociate this member account from Macie.

If you disable Macie, it will no longer have access to the resources in the master account and all member accounts. You must add member accounts again if you decide to re-enable Macie.

If you disable Macie, it stops processing the resources in the master account and all member accounts. Once Macie is disabled, the metadata that Macie collected while monitoring the data in your master and member accounts is deleted. Within 90 days from disabling Macie, all of this metadata is expired from the Macie system backups.

> **Important**
> Disabling Macie does not prompt the deletion of your other data within your AWS accounts. Only the metadata that was collected by Macie while it monitored your accounts is deleted once Macie is disabled.

1. Navigate to the **Macie general settings** page by choosing the down arrow next to your signed in name.
2. In the **Macie general settings** page, check the following checkboxes:
   - **I understand that if I disable Macie, the service will no longer have access to the resources in the master account and all member accounts. You must add member accounts again if you decide to re-enable Macie.**
   - **I understand that if I disable Macie, the service will stop processing the resources in the master account and all member accounts. All metadata that Macie collected while monitoring the data in these accounts will be deleted.**
3. Choose **Disable Amazon Macie**.

Monitoring Amazon Macie Alerts with Amazon CloudWatch Events

Amazon Macie sends notifications based on Amazon CloudWatch Events when any change in the Macie alerts takes place. This includes newly generated alerts and updates to existing alerts. Notifications are sent for all Macie alert types, including predictive alerts and basic alerts, both managed and custom. For more information about alert types, see Amazon Macie Alerts (p. 28).

Macie sends notifications based on Amazon CloudWatch Events for the alerts generated in both master and member Macie accounts. However, only the master Macie account has access to the generated CloudWatch events. For more information about master and member accounts, see Concepts and Terminology (p. 3).

The CloudWatch event for Macie has the following format:

Note
In the sample format below, the fictional account ID of "111122223333" represents the ID of the master Macie account.

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Macie Alert",
  "source": "aws.macie",
  "account": "111122223333",
  "time": "2017-04-24T22:28:49Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id/alert/alert_id",
    "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id"
  ],
  "detail": {
    "notification-type": "ALERT_CREATED",
    "name": "Scanning bucket policies",
    "tags": [
      "Custom_Alert",
      "Insider"
    ],
    "url": "https://lb00.us-east-1.macie.aws.amazon.com/111122223333/posts/alert_id",
    "alert-arn": "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id/alert/alert_id",
    "risk-score": 8,
    "trigger": {
      "rule-arn": "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id",
      "alert-type": "basic",
      "created-at": "2017-01-02 19:54:00.644000",
      "description": "Alerting on failed enumeration of large number of bucket policies",
      "risk": 8
    },
    "created-at": "2017-04-18T00:21:12.059000",
    "actor": "555566667777:assumed-role:superawesome:aroaidpldc7nsesfnheji",
    "summary": {ALERT_DETAILS_JSON}
  }
}
```

You can complete the following procedure to configure your master Macie account to receive CloudWatch events from Macie and to pipe those events into an Amazon Simple Queue Service (SQS) queue. Before completing this procedure, make sure to create the SQS queue for the events from Macie. For more information, see Tutorial: Creating an Amazon SQS Queue.

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Events**, and then choose **Create rule**.
3. Choose **Edit** and type in the following event pattern for the Macie events:

```
{
   "source": [
   "aws.macie"
  ]
}
```

4. In the **Targets** pane, choose **Add target**, select **SQS queue** in the target drop-down menu, and then specify your queue for the events from Macie.

You should now be able to see Macie alerts in your specified queue in the SQS console.

Document History for Amazon Macie

Change	Description	Date
Add support for service-linked roles for Macie.	Macie can now use the service-linked role named `AWSServiceRoleForAmazonMacie`. It allows Macie to discover, classify, and protect sensitive data in AWS on your behalf. For more information, see Using Service-Linked Roles for Amazon Macie.	June 28, 2018
Added comprehensive tables of fields that can appear in the results of your CloudTrail, S3 bucket properties, and S3 objects data searches. The tables also include search query examples using described fields.	For more information, see Researching AWS CloudTrail Data, Researching S3 Bucket Properties Data, and Researching S3 Objects Data.	May 4, 2018

The following table describes important changes in each release of the *Macie* User Guide.

Earlier updates

Change	Description	Date
Initial publication	Initial publication of the Amazon Macie User Guide.	August 14, 2017