Amazon Macie Classic

User Guide

Amazon Macie Classic: User Guide

Table of Contents

This is the user guide for Amazon Macie Classic. For information about the new Amazon Macie, see the Amazon Macie User Guide. To access the Macie Classic console, open the Macie console at https://console.aws.amazon.com/macie/, and then choose **Macie Classic** in the navigation pane.

What Is Amazon Macie Classic?

A new Amazon Macie is now available with significant design improvements and additional features, at a lower price and in most AWS Regions. We encourage you to explore and use the new and improved features, and benefit from the reduced cost. To learn about features and pricing for the new Amazon Macie, see Amazon Macie. To learn how to move to the new Macie, see *Moving to the New Amazon Macie* (p. 3).

Features of Amazon Macie Classic

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

Macie Classic is supported in the following AWS Regions:

- US East (N. Virginia) (us-east-1)
- US West (Oregon) (us-west-2)

Data Discovery and Classification

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

- 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 Classic enables you to be proactive with security compliance and achieve preventive security as follows:

- 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

Accessing Macie Classic

The Macie Classic console is a browser-based interface for accessing and using Macie Classic. Sign in to your Amazon Web Services account and open the Macie Classic console using one of the following links:

- https://us-east-1.redirection.macie.aws.amazon.com/
- https://us-west-2.redirection.macie.aws.amazon.com/

Then, choose **Macie Classic** in the navigation pane.

Moving to the New Amazon Macie

A new Amazon Macie is now available with significant design improvements and additional features, at a lower price and in most AWS Regions. We encourage you to take advantage of these improvements and the reduced cost by moving to the new Macie. With the new Macie, you can use a native Amazon Web Services Console or a comprehensive API to perform tasks such as:

- Monitor and analyze an unlimited number of Amazon Simple Storage Service (Amazon S3) buckets.
- Conduct deeper discovery of sensitive data in S3 bucket objects. The new Macie can analyze more than the first 20 MB of data in an S3 object.
- Build and use custom data identifiers to discover sensitive data for particular scenarios.
- Tag Macie resources.
- Develop and deploy AWS CloudFormation templates for Macie resources.
- Centrally manage Macie for multiple accounts. The new Macie integrates with AWS Organizations, which means that you can manage as many as 5,000 Macie accounts for a single AWS organization. You can also continue to use native Macie features for managing multiple accounts, which enables you to manage as many as 1,000 member accounts with a single Macie administrator account.
- Discover and monitor sensitive data in most AWS Regions, instead of only two Regions.

To learn about all features and pricing for the new Macie, see Amazon Macie.

If you currently have an Amazon Macie Classic account, we'll continue to support your account. If you enable a new account, we'll configure the account to use the new Amazon Macie. To learn how to enable and manage an account for the new Macie, see the Amazon Macie User Guide.

This topic walks you through each step of the process to move from Amazon Macie Classic to the new Amazon Macie.

Topics

Overview

To help you move to the new Amazon Macie, we added an export feature to Macie Classic. With this feature, you can optionally create copies of (export) all the data classification results for your account in the current AWS Region. Macie Classic adds these copies to an S3 bucket, and it encrypts the data using an AWS Key Management Service (AWS KMS) key that you specify. If your account is a Macie Classic administrator account that has member accounts, the export includes classification results for all associated member accounts.

Note
The export doesn't include basic or predictive alerts for your account or any member accounts. It includes only data classification results. However, you can continue to review and analyze existing alert data in AWS Security Hub and existing event data in AWS CloudTrail.

When the export starts, your Macie Classic account and its member accounts switch to read-only mode. This means that you can't perform tasks such as adding S3 buckets to monitor and creating classification jobs. In addition, Macie Classic stops performing most activities for your account and its member accounts. This includes monitoring Amazon S3 resources and sending associated notifications to Amazon CloudWatch Events. Macie Classic remains in this mode for the duration of the export. Depending on how much data you have, the export might take up to two weeks to complete. You can check the status of the export at any time.

Important
To ensure continuous data discovery and monitoring for your account and its member accounts, don't start the export process until you enable and configure these accounts in the new Amazon Macie. To learn how, see the Amazon Macie User Guide. For continuous threat detection, we recommend that you also enable and configure Amazon GuardDuty for these accounts. To learn how, see Amazon S3 protection in Amazon GuardDuty in the *Amazon GuardDuty User Guide*. Note that you will incur costs for both new and existing accounts while the export is in progress. For each Macie Classic account, we will continue to charge you for CloudTrail event processing and extended data retention. We will also charge you for each new Macie account that you enable. To learn about Macie pricing, see Amazon Macie Pricing.

When the export finishes, Macie Classic stops monitoring and processing CloudTrail events for your account and its member accounts. This means that Macie Classic has stopped performing *all* activities for these accounts. However, the accounts are still enabled.

After the export is complete, you can continue to view your existing data classification results by using the Macie Classic console. (You can't view or access these results by using the new Macie.) You can also import the results into a log management or visualization tool from the S3 bucket that you exported them to.

After you complete the export process for a Macie Classic account and its member accounts, you can disable the accounts. If you use Macie Classic in multiple AWS Regions, repeat this process for each additional Region.

Before You Begin

Before you begin the export process and move to the new Amazon Macie, determine whether you have data classification results to export. You can do this by using the Amazon Macie Classic console.

To determine whether you have data classification results

1. Sign in to the AWS Management Console and open the Amazon Macie console at https://console.aws.amazon.com/macie/.
2. By using the AWS Region selector in the upper-right corner of the page, switch to the Region in which you use Macie Classic—**US East (N. Virginia)** or **US West (Oregon)**.
3. At the bottom of the navigation pane, choose **Macie Classic**.

   If you don't see this link, choose your user name in the upper-right corner of the page, and then sign in to the Amazon Web Services account and role with which you use Macie Classic in the current Region.
4. In the Amazon Macie Classic console, choose **Research** in the navigation pane.
5. Apply the following query filters:

- For the data index filter, choose **S3 objects**.
- For the number of results to display filter, choose any value.
- For the time range filter, choose **All Time**.

If the query returns any data classification results, you can export the results. Otherwise, you don't have any data classification results to export and you can proceed to step 2 (p. 7) to disable your Macie Classic account.

If you have data classification results to export, consider the following before you begin the export process, disable your Macie Classic account, and move to the new Macie.

Which accounts?

If your account is a Macie Classic administrator account that has member accounts, a first step is to determine which accounts you want to move to the new Macie. Only an administrator account can start the export process and subsequently disable a member account. In addition, when you start the export process, Macie Classic automatically switches the administrator account and all of its member accounts to read-only mode. Macie Classic then exports the data for the administrator account and all of its member accounts.

If you prefer to move to the new Macie in phases, consider adjusting the current administrator-member account associations for your organization. To exclude specific member accounts from a phase, disassociate those accounts from your administrator account. You can then optionally choose a new administrator account for those member accounts. After you do this, you can start the export process for the new administrator account and its member accounts during a separate phase.

Is continuous monitoring necessary?

When the export process starts, Macie Classic stops performing most activities for your account and its member accounts. This includes monitoring Amazon S3 resources and sending associated notifications to Amazon CloudWatch Events. Macie Classic remains in this mode for the duration of the export. Depending on how much data you have, the export can take up to two weeks to complete.

To ensure continuous data discovery and monitoring for your account and its member accounts, you should enable and configure the accounts in the new Amazon Macie before you start the export process. To learn how to do this, see the Amazon Macie User Guide. For continuous threat detection, we recommend that you also enable and configure Amazon GuardDuty for the accounts. To learn how to do this, see the Amazon GuardDuty User Guide.

Note, however, that you will incur costs for new and existing accounts. While the export is in progress for a Macie Classic account, we'll continue to charge the account for CloudTrail event processing and extended data retention. After the export is complete, we'll continue to charge the account for extended data retention until you disable the account. We'll also charge you for each new Macie account that you enable. To learn about Macie pricing, see Amazon Macie Pricing.

Which S3 bucket?

When you start the export process, you can specify where to export your classification results to. You have two options:

- **Use a new S3 bucket that you create** – If you prefer to export the results to a particular S3 bucket that you create, create the bucket, and ensure that the name of the bucket begins with `awsmacie-*`. (This allows Macie Classic to access the bucket by using the existing service-linked role (p. 18) for your Macie Classic account.) Also, define a bucket policy that allows Macie Classic to create objects in the bucket. For an example of the bucket policy to use, see S3 Bucket Policy for Exported Data Classification Results (p. 10) later in this topic.
- **Use a new S3 bucket that Macie Classic creates** – If you don't specify an S3 bucket, Macie Classic automatically creates a new bucket for you. (To do this, it uses the existing service-linked

role (p. 18) for your Macie Classic account.) To help you find the bucket, it includes `awsmacie-classification-export` in the bucket name. When it creates the bucket, Macie Classic also applies a bucket policy that allows it to write data to the bucket only if the bucket owner has full control of the bucket's objects. To see the policy, refer to S3 Bucket Policy for Exported Data Classification Results (p. 10) later in this topic.

Note that the new Amazon Macie also provides options for storing classification results in an S3 bucket. However, we don't recommend using the same bucket to store classification results for both versions of Macie. Macie Classic and the new Macie use different schemas for data classification results.

Which encryption key?

When you start the export process, you have to specify the AWS Key Management Service (AWS KMS) key that you want Macie Classic to use to encrypt the exported data. Therefore, it's a good idea to determine which key you want to use before you start the export, and to note the key's ARN. You'll need to enter the ARN when you start the export process. Also, verify that the key's policy allows Macie Classic to perform the `Encrypt` and `GenerateDataKey*` actions. For example:

```
{
    "Version":"2012-10-17",
    "Id":"key-policy-id",
    "Statement":[
        {
            "Sid":"Allow Macie Classic to use the key",
            "Effect":"Allow",
            "Principal":{
                "Service":"macie.amazonaws.com"
            },
            "Action":[
                "kms:Encrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource":"*"
        }
    ]
}
```

Step 1: Export Data Classification Results

The first step in moving to the new Amazon Macie is to optionally export the existing data classification results for your account. If your account is a Macie Classic administrator account, this includes classification results for all of its associated member accounts.

When you export data classification results, Macie Classic copies the results data to one or more objects in an S3 bucket. It encrypts the data using an AWS KMS key that you specify. The number of objects varies depending on how much data you have.

Each object contains JSON-formatted data for a batch of classification results. The data is grouped by calendar day and uses the Macie Classic schema for data classification results. This means that the data maps closely to the groups and fields in the Macie Classic **Dashboard**. For descriptions of these groups and fields, see Viewing Data and Activity that Amazon Macie Classic Monitors (p. 46). Each object is compressed and stored as a .gzip file.

In addition to these objects, Macie Classic creates an empty `JOB_START_TOKEN` object in the bucket. This object indicates that the export started. It also creates an empty `JOB_END_TOKEN` object. This object indicates that the export is complete. You can ignore these objects in any queries or subsequent analysis of the data.

To export data classification results

1. Sign in to the AWS Management Console and open the Amazon Macie console at https://console.aws.amazon.com/macie/.
2. By using the AWS Region selector in the upper-right corner of the page, switch to the Region in which you use Macie Classic—**US East (N. Virginia)** or **US West (Oregon)**.
3. At the bottom of the navigation pane, choose **Macie Classic**.

   If you don't see this link, choose your user name in the upper-right corner of the page, and then sign in to the Amazon Web Services account and role that you want to export data classification results for.
4. If your account is a Macie Classic administrator account that has member accounts, disassociate any member accounts that you don't want to include in the export process.
5. Remove all the S3 resources that you integrated with Macie Classic. To do this, choose **Integrations** in the navigation pane, and then clear all the current selections for data sources to monitor.
6. In the banner at the top of the console, choose **Export data**. If the banner is hidden, reload the page in your browser.
7. (Optional) For **Bucket**, enter the name of the S3 bucket that you want to store the exported data in. If you don't enter a bucket name, Macie Classic automatically creates a bucket for you, and it defines a bucket policy (p. 10) for the bucket.
8. For **KMS key ARN**, enter the Amazon Resource Name (ARN) of the AWS KMS key that you want to use to encrypt the exported data.
9. When you finish entering the export settings, choose **Export data** to start the export. Macie Classic then verifies that it can create or access the S3 bucket for the exported data. It also verifies that it can use the AWS KMS key that you specified. If it can do these things, it begins copying your classification results to the bucket.
10. To check the status of the export at any time, repeat steps 1 through 3 to return to the Macie Classic console. The banner at the top of the console displays the status of the export. When the export is complete, the banner displays **The export is complete**.

    If an issue occurs and Macie Classic can't complete the export, the banner displays **Export failed**. To display details about the issue, choose **Export failed**. Depending on the nature of the issue, try to export the data again or contact AWS Support for assistance.
11. When the export is complete, navigate to the S3 bucket that contains the exported data, and then verify the results. The number and nature of the results should match the data that appears in the Macie Classic **Dashboard**.

Repeat the preceding steps for each additional Macie Classic administrator account (and its member accounts) and AWS Region.

Step 2: Disable Your Macie Classic Account

After you export your data classification results or determine that you don't have any data classification results to export, you can disable your Macie Classic account.

Warning
When you disable a Macie Classic account, the following occurs:

- Macie Classic loses access to resources for the Macie Classic administrator account and all of its member accounts.
- You and all other users of the administrator account and its member accounts lose access to the Macie Classic console.

- Macie Classic deletes all the metadata that it collected while monitoring data for the administrator account and all of its member accounts. Within 90 days of disabling Macie Classic, all of this metadata is expired and removed from Macie Classic system backups.

Note that Macie Classic doesn't delete data that it generated and stored in other AWS services for you. This includes existing alert data in AWS Security Hub, event data in AWS CloudTrail, and logs and exported classification results in Amazon S3.

To disable your Macie Classic account

1. Sign in to the AWS Management Console and open the Amazon Macie console at https://console.aws.amazon.com/macie/.
2. By using the AWS Region selector in the upper-right corner of the page, switch to the Region in which you want to disable your Macie Classic account—**US East (N. Virginia)** or **US West (Oregon)**.
3. At the bottom of the navigation pane, choose **Macie Classic**.

   If you don't see this link, choose your user name in the upper-right corner of the page, and then sign in to the Amazon Web Services account and role that you want to disable Macie Classic for.
4. In the banner at the top of the console, choose **Disable Macie Classic**.
5. On the **general settings** page, review the information about the consequences of disabling your Macie Classic account. If you're sure that you want to disable your account and its member accounts, select the check boxes, and then choose **Disable Amazon Macie**.

Step 3: Delete Resources and Collected Metadata

When you disable a Macie Classic account, the service doesn't delete any data or resources that it created, used, or stored in other AWS services for the account. It deletes only the data that it collected and stored directly for the account.

As a best practice and to avoid unnecessary costs, we recommend that you assess the following resources and data after you disable your Macie Classic account:

- **AWS CloudTrail data events** – Macie Classic created a trail to enable Amazon S3 data events for the buckets that it monitored. The new Amazon Macie uses a different architecture and doesn't require you to enable Amazon S3 data events. If you don't need this logging anymore, you should delete the trail that Macie Classic created. This prevents further AWS CloudTrail billing charges for the trail. You can also archive or remove the log data that's stored in the S3 bucket.
- **Amazon CloudWatch Events** – Macie Classic doesn't delete CloudWatch Events that it generated for your account. Although the new Macie also publishes events to CloudWatch Events (Amazon EventBridge), the event data will be specific to your new Macie account. Therefore, you might decide to delete events for the Macie Classic account that you disabled.
- **Legacy IAM roles** – If you used Macie Classic before June 21, 2018 (when it began supporting service-linked roles), your Amazon Web Services account has two legacy AWS Identity and Access Management (IAM) roles that you don't need anymore. These roles are **AmazonMacieServiceRole** and **AmazonMacieSetupRole**. These roles allowed Macie Classic to call other AWS services on your behalf. The new Macie doesn't use these roles. You can, therefore, consider deleting them.

If you started using Macie Classic after June 21, 2018, the service created an **AWSServiceRoleForAmazonMacie** service-linked role on your behalf. This role allowed Macie Classic to discover and monitor sensitive data on your behalf. The new Amazon Macie uses the same service-linked role to perform similar tasks. For this reason, we recommend that you keep this role for use with your new Macie account.

Step 4: Enable Your New Amazon Macie Account

When you're ready to start using the new Amazon Macie, sign in to your Amazon Web Services account, navigate to the Amazon Macie console, and enable your new Macie account. To learn about features and pricing for the new Macie, see Amazon Macie.

To enable a new Macie account

1. Sign in to the AWS Management Console and open the Amazon Macie console at https://console.aws.amazon.com/macie/.
2. By using the AWS Region selector in the upper-right corner of the page, switch to the Region in which you want to enable the new Macie.
3. Choose **Get started**.
4. Choose **Enable Macie**.

Within minutes, the new Macie generates an inventory of the S3 buckets for your account, and begins monitoring the buckets for security and access control.

Next Steps

To ensure continued data classification with your new Macie account, immediate next steps are:

Configure a repository for your sensitive data discovery results

In the new Macie, you create and run sensitive data discovery jobs to analyze and report sensitive data in S3 buckets. When Macie runs a job, it reports any sensitive data that it discovers as a *sensitive data finding*, which is a detailed report of the sensitive data that Macie found. Macie also creates *sensitive data discovery results*, which are detailed analysis records for S3 objects that the job analyzes or attempts to analyze. This includes objects that don't contain sensitive data and, therefore, don't produce a finding.

When you configure a repository to store your discovery results, you ensure long-term access and storage of these results for your account. For more information, see Storing and retaining sensitive data discovery results in the *Amazon Macie User Guide*.

Create a sensitive data discovery job

After you configure a repository for your discovery results, create a job that runs periodically on a daily, weekly, or monthly basis.

To avoid unnecessary costs and duplicated classification data, you can configure the job to analyze only those objects that were created or modified after a certain point in time, such as when you started the export process in Macie Classic. You can do this in two ways during step 3 of the job creation process:

- **Skip objects that were created before the job** – With this configuration, the first run of the job analyzes only those objects that are created after you finish creating the job. Each subsequent run analyzes only those objects that are created after the preceding run. To use this configuration, clear the **Include existing objects** check box under **Scheduled job**.
- **Skip objects that were created or last modified before a certain time** – With this configuration, each run of the job skips any objects that were created or modified before a date and time that you specify. To use this configuration, use object criteria to refine the job's scope: Expand the **Additional settings** section, and then choose **Last modified** under **Object criteria**. Then, in the **To** boxes, enter the latest creation or modification date and time for the objects to skip, and choose **Exclude**.

For more information, see Creating a sensitive data discovery job in the *Amazon Macie User Guide*.

For additional next steps and information about configuring and managing your account, see the Amazon Macie User Guide. The guide also provides information about managing multiple accounts by using AWS Organizations or sending Macie membership invitations.

In addition to next steps for the new Macie, we recommend that you configure and use the Amazon S3 protection feature of Amazon GuardDuty for threat detection. This feature monitors object-level, Amazon S3 data events and analyzes them for malicious and suspicious activity. For more information, see Amazon S3 protection in Amazon GuardDuty in the *Amazon GuardDuty User Guide*.

Reference: S3 Bucket Policy for Exported Data Classification Results

As discussed earlier in this topic (p. 4), Macie Classic can automatically create an S3 bucket to store the data classification results that you export. If you choose this option, Macie Classic defines the following bucket policy for the bucket that it creates.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"MacieClassificationExportS3WriteBucketPolicy",
            "Effect":"Allow",
            "Principal":{
                "Service":"macie.amazonaws.com"
            },
            "Action":"s3:PutObject",
            "Resource":"arn:aws:s3:::{bucket_name}/*",
            "Condition":{
                "StringEquals":{
                    "s3:x-amz-acl":"bucket-owner-full-control"
                }
            }
        },
        {
            "Sid":"Deny non-HTTPS access",
            "Action":"s3:*",
            "Effect":"Deny",
            "Principal":"*",
            "Resource":[
                "arn:aws:s3:::{bucket_name}/*",
                "arn:aws:s3:::{bucket_name}"
            ],
            "Condition":{
                "Bool":{
                    "aws:SecureTransport":false
                }
            }
        },
        {
            "Sid":"Deny incorrect encryption header",
            "Action":"s3:PutObject",
            "Effect":"Deny",
            "Principal":"*",
            "Resource":"arn:aws:s3:::{bucket_name}/*",
            "Condition":{
                "StringNotEquals":{
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":"{kms_key_arn}"
                }
            }
        },
```

```
        {
            "Sid":"Deny unencrypted object uploads",
            "Action":"s3:PutObject",
            "Effect":"Deny",
            "Principal":"*",
            "Resource":"arn:aws:s3:::{bucket_name}/*",
            "Condition":{
                "StringNotEquals":{
                    "s3:x-amz-server-side-encryption":"aws:kms"
                }
            }
        }
    ]
}
```

Concepts and Terminology

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

Account

A standard Amazon Web Services (AWS) account that contains your AWS resources. When you sign up for AWS, your account is automatically signed up for all services in AWS. The account that you used to sign in to AWS when you enabled Macie Classic is designated as the *administrator account*.

If you integrated other accounts with Macie Classic, these accounts are called *member accounts*.

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

Alert

A notification about a potential security issue that Macie Classic discovers. Alerts appear on the Macie Classic console and provide a comprehensive narrative about all activity that occurred over the last 24 hours.

Macie Classic provides the following types of alerts:

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

For more information about alerts, including alert categories and details about the contents of Macie Classic alerts, see Amazon Macie Classic Alerts (p. 53).

Data source

The origin or location of a set of data. To classify and protect your data, Macie Classic 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 enables 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 Classic uses the ability in CloudTrail to capture object-level API activity on S3 objects (data events). For more information, see Working with CloudTrail Log Files.

Amazon S3

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

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. Amazon S3 stores data as objects in 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 that 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 Classic, a user is the AWS Identity and Access Management (IAM) identity that makes the request. Macie Classic 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 Amazon Web Services 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 operation.
- Federated user – The request was made with temporary security credentials that were obtained via a call to the AWS STS `GetFederationToken` API operation.
- AWS account – The request was made by another Amazon Web Services account.
- AWS service – The request was made by an account that belongs to an AWS service.

When specifying a user in the Macie Classic console, you must use a special Macie Classic format called `macieUniqueId`. Examples of specifying a user include searching for a user in the **Users** tab, constructing a query in the **Research** tab, and explicitly allowing a user in a basic alert with the index of **CloudTrail data**. The `macieUniqueId` is a combination of the IAM `UserIdentity` element and the `recipientAccountId`. For more information, see the preceding list of `UserIdentity` elements and the definition of `recipientAccountId` in the CloudTrail Record Contents. The following examples 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 Amazon Macie Classic–Monitored Data by User Activity (p. 60).

Setting Up Amazon Macie Classic

When you sign up for Amazon Web Services, your Amazon Web Services account is automatically signed up for all services in Amazon Web Services. The Amazon Web Services account that you used when you enabled Macie Classic is automatically designated as your Macie Classic administrator account. For more information, see Concepts and Terminology (p. 12).

When you enabled Macie Classic, Macie Classic created a service-linked role. To learn about the IAM policy for this role, see Service-Linked Roles for Amazon Macie Classic (p. 18).

After you enabled Macie Classic, it immediately began pulling and analyzing independent streams of data from AWS CloudTrail to generate alerts. Because Macie Classic consumes this data only to determine if there are potential security issues, Macie Classic doesn't manage CloudTrail for you or make its events and logs available to you. If you enabled CloudTrail independently of Macie Classic, you continue to have the option to configure its settings through the CloudTrail console or APIs. For more information, see the AWS CloudTrail User Guide.

You can disable Macie Classic at any time to stop it from processing and analyzing CloudTrail events. For more information, see Disabling Amazon Macie Classic and Deleting Collected Metadata (p. 98).

Integrate Amazon S3 with Macie Classic

To classify and protect your data, Macie Classic analyzes and processes information from CloudTrail and Amazon S3. Enabling CloudTrail in your account is required to use Macie Classic. Integrating S3 with Macie Classic is not required. However, we strongly recommend that you integrate with Amazon S3 as part of setting up Macie Classic. For more information about how Macie Classic classifies your data, see Classifying Data with Amazon Macie Classic (p. 25).

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

Prerequisites

- The IAM identity (user, role, group) that you use to integrate must have the required permissions. To grant the required permissions, attach the **AmazonMacieFullAccess** managed policy to this identity. For more information, see Predefined AWS Managed Policies for Macie Classic (p. 16).

To integrate with Amazon S3

1. Log in to Amazon Web Services (AWS) with the credentials of the account that is serving as your Macie Classic administrator account.
2. Open the Amazon Macie console and choose **Macie Classic** in the navigation pane.
3. Choose **Integrations** from the navigation pane.
4. Choose **S3 Resources** and choose **Select** next to the account (administrator or member).
5. On the **Integrate S3 resources with Macie Classic** page, choose **Add**. Select up to 250 Amazon S3 resources in the current AWS Region and then choose **Add**.
6. For **Classification of existing objects**, keep the default setting, **Full**. The one-time classification method is applied only once to all of the existing objects in the selected S3 buckets.

   Macie Classic displays the following information for each selected bucket:

   - **Total objects** – Total number of objects.

- **Processed estimate** – Total size of the data that Macie Classic will classify.
- **Cost estimate** – Cost estimate for classifying all of the objects.

Macie Classic also displays the following totals across all selected buckets:

- **Total size** – Total size of the data.
- **Total number of objects** – Total number of objects.
- **Processed estimate** – Total size of the data that Macie Classic will classify.
- **Total cost estimate** – Cost estimate for classifying all of the objects.

The cost estimate for each bucket is based on its processed estimate value. The total cost estimates are provided only for S3 buckets, not for prefixes. For more information, see Amazon Macie Classic Pricing.

The one-time classification cost estimates are only calculated per S3 bucket, not bucket prefixes. If you select a bucket prefix, the cost estimate for the entire S3 bucket is included in the total cost estimate. If you select multiple prefixes of the same S3 bucket, the cost estimate for the entire S3 bucket is included only once in the total cost estimate.

7. When you have finished your selections, choose **Review**.
8. When you have finished reviewing your selections, choose **Start classification**.

Controlling Access to Amazon Macie Classic

AWS uses security credentials to identify you and to grant you access to your AWS resources. You can use features of AWS Identity and Access Management (IAM) to allow other users, services, and applications to use your AWS resources fully or in a limited way. You can do this without sharing your security credentials.

By default, IAM users don't have permission to create, view, or modify AWS resources. To allow an IAM user to access resources such as a load balancer, and to perform tasks, you:

1. Create an IAM policy that grants the IAM user permission to use the specific resources and API actions they need.
2. Attach the policy to the IAM user or the group that the IAM user belongs to.

When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources.

For example, you can use IAM to create users and groups under your Amazon Web Services account. An IAM user can be a person, a system, or an application. Then you grant permissions to the users and groups to perform specific actions on the specified resources using an IAM policy.

For more information, see the IAM User Guide.

Granting Administrator Access to Macie Classic

Macie Classic administrator account users have access to the Macie Classic console, where they can configure Macie Classic and use it to monitor and protect the resources in both administrator and member accounts. For more information about Macie Classic administrator and member accounts, see Concepts and Terminology (p. 12) and Integrating Member Accounts and Amazon S3 with Amazon Macie Classic (p. 23).

For Macie Classic administrator account users to be able to use the Macie Classic console, they must be granted the required permissions. To ensure this, use the following policy document to create and attach an IAM policy to any user identity type that belongs to your Macie Classic administrator account. This policy grants administrator account users with the permissions that are required to use the Macie Classic 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"
            }
         }
      }
   ]
}
```

Granting Read-Only Access to Macie Classic

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "macie:List*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Predefined AWS Managed Policies for Macie Classic

The managed policies created by AWS grant the required permissions for common use cases. You can attach these policies to IAM users in your Amazon Web Services account, based on the access to Macie Classic that they require:

- **AmazonMacieFullAccess** – Grants full access to Macie Classic
- **AmazonMacieHandshakeRole** – Grants permission to create the service-linked role for Macie Classic

The following are legacy policies that have been replaced by a service-linked role. For more information, see Legacy Roles for Macie Classic (p. 20).

- **AmazonMacieServiceRole** – Grants Macie Classic read-only access to resource dependencies in your account in order to enable data analysis
- **AmazonMacieSetupRole** – Grants Macie Classic access to your Amazon Web Services account

Creating a Handshake Role

You can create a role that grants the permissions in the **AmazonMacieHandshakeRole** policy to Macie Classic from the administrator account as follows.

To create AWSMacieServiceCustomerHandshakeRole using the IAM console

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Roles**.
3. Choose **Create role** and do the following:
   a. For **Select type of trusted entity**, choose **AWS service**.
   b. For **Choose a use case**, select **EC2**.
   c. Choose **Next: Permissions**.
4. On the **Attach permissions policies** page, select the checkbox for the **AmazonMacieHandshakeRole** policy and choose **Next: Tags**.
5. (Optional) Add tags to your role and then choose **Next: Review**.
6. On the **Review** page, do the following:
   a. For **Role name**, enter **AWSMacieServiceCustomerHandshakeRole**.
   b. For **Role description**, enter the following: Allows the Macie Classic administrator account to create service-linked roles in the member accounts.
   c. Choose **Create role**.
7. Edit the trust policy as follows:
   a. Select **AWSMacieServiceCustomerHandshakeRole**, which you just created.
   b. On the **Trust relationships** tab, choose **Edit trust relationship**.
   c. Enter the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "macie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "administrator-account-id"
        }
      }
    }
  ]
}
```

   d. Choose **Update Trust Policy**.

To create AWSMacieServiceCustomerHandshakeRole using the AWS CLI

1. Create the following trust policy and save it in a text file named `macie-handshake-trust-policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "macie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "administrator-account-id"
        }
      }
    }
  ]
}
```

2. Create the role and specify the trust policy that you created in the previous step using the create-role command.

```
aws iam create-role --role-name AWSMacieServiceCustomerHandshakeRole --assume-role-policy-document file://macie-handshake-trust-policy.json
```

3. Attach the **AmazonMacieHandshakeRole** policy to the role using the attach-role-policy command.

```
aws iam attach-role-policy --role-name AWSMacieServiceCustomerHandshakeRole --policy-arn arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole
```

Service-Linked Roles for Amazon Macie Classic

Amazon Macie Classic uses an AWS Identity and Access Management (IAM) service-linked role. This service-linked role is a unique type of IAM role that's linked directly to Macie Classic. It's predefined by Macie Classic and includes all the permissions that Macie Classic needs to call other AWS services on your behalf. The defined permissions include the trust policy and the permissions policy, and that permissions policy can't be attached to any other IAM entity.

Macie Classic uses a service-linked role in all the AWS Regions where Macie Classic is available.

Service-Linked Role Permissions for Macie Classic

Macie Classic uses the service-linked role named **AWSServiceRoleForAmazonMacie**. The permissions policy for the role allows Macie Classic to discover, classify, and protect sensitive data in AWS on your behalf. The role trusts the `macie.amazonaws.com` service to assume the role.

The role is configured with the following AWS managed permissions policy, named **AmazonMacieServiceRolePolicy**.

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

```
            "Action":[
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:ListTags",
                "cloudtrail:LookupEvents",
                "iam:ListAccountAliases",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":[
                "cloudtrail:CreateTrail",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:PutEventSelectors"
            ],
            "Resource":"arn:aws:cloudtrail:*:*:trail/AWSMacieTrail-DO-NOT-EDIT"
        },
        {
            "Effect":"Allow",
            "Action":[
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteBucketPolicy",
                "s3:DeleteBucketWebsite",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObjectVersionTagging",
                "s3:PutBucketPolicy"
            ],
            "Resource":[
                "arn:aws:s3:::awsmacie-*",
                "arn:aws:s3:::awsmacietrail-*",
                "arn:aws:s3:::*-awsmacietrail-*"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "logs:CreateLogGroup"
            ],
```

```
            "Resource":[
                "arn:aws:logs:*:*:log-group:/aws/macie/*"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource":[
                "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
            ]
        }
    ]
}
```

For details about updates to the **AmazonMacieServiceRolePolicy** policy, see Updates to AWS Managed Policies for Macie and Macie Classic (p. 22).

Amazon Macie Classic and the new Amazon Macie use the same service-linked role and permissions policy. (This helps you move to and use the new Macie.) Macie Classic performs all the actions allowed by the policy except `CreateLogGroup`, `CreateLogStream`, `PutLogEvents`, and `DescribeLogStreams`. Only the new Macie performs those actions on resources, as defined by the policy.

In addition, Macie Classic doesn't perform actions on the following resources: `arn:aws:logs:*:*:log-group:/aws/macie/*` and `arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*`. Only the new Macie performs actions on those resources, as defined by the policy.

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

Creating a Service-Linked Role for Macie Classic

You don't need to manually create the **AWSServiceRoleForAmazonMacie** role. Macie Classic creates this role on your behalf as follows:

- **Macie Classic administrator account** — The **AWSServiceRoleForAmazonMacie** role was created for you when you enabled Macie Classic for the first time.
- **Member accounts** — The **AWSServiceRoleForAmazonMacie** role was created for you when the Macie Classic administrator account associated the member account with Macie Classic. The service-linked role that was created for the Macie Classic administrator account doesn't apply to Macie Classic member accounts.

Macie Classic can create the service-linked role on your behalf only if you have the required permissions. To grant the required permissions to an IAM entity, such as a user, group, or role, attach the **AmazonMacieFullAccess** policy. For more information, see Predefined AWS Managed Policies for Macie Classic (p. 16) and Service-linked role permissions in the *IAM User Guide*.

You can also create the **AWSServiceRoleForAmazonMacie** role manually. For more information, see Creating a service-linked role in the *IAM User Guide*.

Legacy Roles for Macie Classic

If you used Macie Classic before June 21, 2018, when it began supporting service-linked roles, the IAM roles that grant Macie Classic access to call other AWS services on your behalf already exist in

your account (Macie Classic administrator or member). These roles are **AmazonMacieServiceRole** and **AmazonMacieSetupRole**. They were created when you launched either the Macie Classic AWS CloudFormation template for an administrator account or the Macie Classic AWS CloudFormation template for a member account as part of setting up Macie Classic.

The service-linked role replaces these previously created IAM roles (in administrator and member accounts). The previously created roles were not deleted, but they're no longer used to grant Macie Classic permission to call other services on your behalf. You can use the IAM console to delete the previously created roles.

Editing a Service-Linked Role for Macie Classic

After you create a service-linked role, you can't change the name of 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 Classic

If you no longer need to use Amazon Macie Classic (or the new Amazon Macie), we recommend that you delete the **AWSServiceRoleForAmazonMacie** role.

For a Macie Classic administrator account, you can delete the service-linked role only after disabling Macie Classic. This ensures that you can't inadvertently remove permissions to access Macie Classic resources. For member accounts, the administrator account must first disassociate them from Macie Classic. For more information, see Disabling Amazon Macie Classic and Deleting Collected Metadata (p. 98).

When you disable Macie Classic, the **AWSServiceRoleForAmazonMacie** role is not deleted. If you move to the new Macie, the new Macie uses the existing **AWSServiceRoleForAmazonMacie** role.

You can use the IAM console, the IAM CLI, or the IAM API to delete the **AWSServiceRoleForAmazonMacie** role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

AWS Managed Policies for Amazon Macie and Amazon Macie Classic

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

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

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ViewOnlyAccess** AWS managed policy provides read-only access to many AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations

and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

Updates to AWS Managed Policies for Macie and Macie Classic

View details about updates to AWS managed policies for both Macie and Macie Classic since Macie began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Macie Classic Document History (p. 101) page.

Change	Description	Date
AmazonMacieServiceRolePolicy (p. 23) – Update to an existing policy	Macie added Amazon CloudWatch Logs actions to the *AmazonMacieServiceRolePolicy* policy. These actions allow the new Macie to publish log events to CloudWatch Logs for sensitive data discovery jobs.	April 13, 2021
Macie started tracking changes.	Macie started tracking changes for its AWS managed policies.	April 13, 2021

Integrating Member Accounts and Amazon S3 with Amazon Macie Classic

You can integrate member accounts with Amazon Macie Classic and integrate Amazon S3 with Macie Classic. For information about Macie Classic administrator and member accounts, see Concepts and Terminology (p. 12).

Contents

Integrating Member Accounts with Macie Classic

When you integrate member accounts with Macie Classic, you're enabling Macie Classic to monitor resources and activity in these member accounts.

Prerequisites

- Create a role that grants the member account the permissions required to create the **AWSServiceRoleForAmazonMacie** service-linked role. For more information, see Creating a Handshake Role (p. 17).

To integrate member accounts with Macie Classic

1. Log in to AWS with the credentials of the Amazon Web Services account that is serving as your Macie Classic administrator account.
2. Open the Macie Classic console and choose **Integrations** from the navigation pane.
3. Choose **Accounts** and choose the plus icon (**+**) next to **Member AWS accounts**.
4. When prompted, enter one or more account IDs, separated by commas. Choose **Add accounts**.
5. (Optional) Verify that Macie Classic created the **AWSServiceRoleForAmazonMacie** role in each member account that you integrated. For more information, see Creating a Service-Linked Role for Macie Classic (p. 20).

Specifying Data for Macie Classic to Monitor

You can specify the S3 buckets and prefixes that contain the data for Macie Classic to monitor.

Prerequisites

- The IAM identity (user, role, group) that you use to integrate must have the required permissions. To grant the required permissions, attach the **AmazonMacieFullAccess** managed policy to this identity. For more information, see Predefined AWS Managed Policies for Macie Classic (p. 16).

To update your integration with Amazon S3

1. Log in to AWS with the credentials of the account that is serving as your Macie Classic administrator account.
2. Open the Macie Classic console and choose **Integrations** from the navigation pane.
3. Choose **S3 Resources** and choose **Select** next to the account (administrator or member).
4. On the **Integrate S3 resources with Macie Classic** page, choose **Edit** to edit the buckets/prefixes that are already integrated or **Add** to integrate new buckets/prefixes.
5. For **Classification of existing objects**, keep the default setting, **Full**. The one-time classification method is applied only once to all of the existing objects in the selected S3 buckets.

   Macie Classic displays the following information for each selected bucket:

   - **Total objects** – Total number of objects.
   - **Processed estimate** – Total size of the data that Macie Classic will classify.
   - **Cost estimate** – Cost estimate for classifying all of the objects.

   Macie Classic also displays the following totals across all selected buckets:

   - **Total size** – Total size of the data.
   - **Total number of objects** – Total number of objects.
   - **Processed estimate** – Total size of the data that Macie Classic will classify.
   - **Total cost estimate** – Cost estimate for classifying all of the objects.

   The cost estimate for each bucket is based on its processed estimate value. The total cost estimates are provided only for S3 buckets, not for prefixes. For more information, see Amazon Macie Classic Pricing.

   The one-time classification cost estimates are only calculated per S3 bucket, not bucket prefixes. If you select a bucket prefix, the cost estimate for the entire S3 bucket is included in the total cost estimate. If you select multiple prefixes of the same S3 bucket, the cost estimate for the entire S3 bucket is included only once in the total cost estimate.
6. When you have finished your selections, choose **Review**.
7. When you have finished reviewing your selections, choose **Start classification**.

Encrypted Objects

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

- If your Amazon S3 objects are encrypted using Amazon S3–managed encryption keys (SSE-S3), Macie Classic 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 Classic 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 AWS KMS customer master key (CMK). If you don't add either of these roles as a user of the CMK, Macie Classic can't read and classify the objects. However, Macie Classic still stores metadata for the object, including which CMK was used to protect the object.
- If your Amazon S3 objects are encrypted using client-side encryption, Macie Classic can't read and classify the objects, but still stores metadata for the object.

Classifying Data with Amazon Macie Classic

Macie Classic can help you classify your sensitive and business-critical data stored in Amazon Simple Storage Service (Amazon S3); buckets. To classify your data, Macie Classic also uses the ability in AWS CloudTrail to capture object-level API activity on S3 objects (data events). However, Macie Classic monitors CloudTrail data events only if you specify at least one S3 bucket for Macie Classic to monitor.

After you specify the S3 bucket or buckets for Macie Classic to monitor, you enable Macie Classic to continuously monitor and discover new data as it enters your AWS infrastructure. For more information, see Specifying Data for Macie Classic to Monitor (p. 23).

Limits

- Macie Classic has a default limit on the amount of data that it can classify in an account. After this data limit is reached, Macie Classic stops classifying the data in this account. The default data classification limit is 3 TB. You can contact AWS Support and request an increase to the default limit.
- If you specify S3 buckets that include files of a format that isn't supported in Macie Classic, Macie Classic doesn't classify them.
- Macie Classic's content classification engine processes up to the first 20 MB of an S3 object.

Your Macie Classic usage charges include only the costs for the content that Macie Classic processes. For example, Macie Classic can't extract text from .wav files (images or movies); therefore, it doesn't process that content and you're not charged for it.

Contents

Supported Compression and Archive File Formats

Currently, Macie Classic 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

Content Type

Once Macie Classic begins monitoring your data, it uses several automatic content classification methods to identify and prioritize your sensitive and critical data and to accurately assign business value to your data. One of these methods is classifying by content type.

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

Macie Classic can assign only one content type to an object.

You can't modify existing or add new content types. You can enable or disable any existing content types, thus enabling or disabling Macie Classic to assign these them to your objects during the classification process.

To view, enable, or disable content types

1. In the Macie Classic 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** dropdown and choose **Save**.

The following list describes the complete list of content types that Macie Classic can assign to your objects.

Name	Description
application/cap	WireShark or Tcpdump Packet Capture
application/epub+zip	application/epub
application/illustrator	Adobe Illustrator
application/java	Binary (Java)
application/java-archive	application/java-archive
application/java-serialized-object	application/java-serialized-object

application/java-vm	application/java-vm
application/javascript	application/javascript
application/json	JSON
application/msaccess	application/msaccess
application/msexcel	Microsoft Excel
application/msonenote	application/msonenote
application/mspowerpoint	Microsoft PowerPoint
application/msword	Microsoft Word
application/octet-stream	application/octet-stream
application/octet-stream+fon	application/octet-stream+fon
application/ogg	application/ogg
application/onenote	application/onenote
application/pdf	Adobe PDF
application/pgp	application/pgp
application/pgp-encrypted	application/pgp-encrypted
application/pgp-keys	PGP keys
application/pgp-signature	PGP signature
application/postscript	Adobe Postscript
application/rar	RAR compressed archive
application/rdf+xml	application/rdf+xml
application/rss+xml	application/rss+xml
application/rtf	application/rtf
application/tar	TAR archive
application/unknown	application/unknown
application/vnd.3gpp.pic-bw-small	application/vnd.3gpp.pic-bw-small
application/vnd.android.package-archive	Android Package
application/vnd.audiograph	application/vnd.audiograph
application/vnd.balsamiq.bmpr	Balsamiq Mockup
application/vnd.cups-ppd	application/vnd.cups-ppd
application/vnd.curl.car	application/vnd.curl.car
application/vnd.dvb.ait	application/vnd.dvb.ait
application/vnd.google-apps.document	Google Apps Document
application/vnd.google-apps.drawing	application/vnd.google-apps.drawing

application/vnd.google-apps.form	Google Apps Form
application/vnd.google-apps.map	Google Apps Map
application/vnd.google-apps.presentation	Google Apps Presentation
application/vnd.google-apps.script	Google Apps script
application/vnd.google-apps.spreadsheet	Google Apps Spreadsheet
application/vnd.google-earth.kmz	Google Earth KMZ
application/vnd.jcp.javame.midlet-rms	application/vnd.jcp.javame.midlet-rms
application/vnd.jgraph.mxfile	application/vnd.jgraph.mxfile
application/vnd.jgraph.mxfile.realtime	application/vnd.jgraph.mxfile.realtime
application/vnd.jgraph.mxfile.rtlegacy	application/vnd.jgraph.mxfile.rtlegacy
application/vnd.kde.kontour	application/vnd.kde.kontour
application/vnd.lotus-1-2-3	application/vnd.lotus-1-2-3
application/vnd.lotus-organizer	application/vnd.lotus-organizer
application/vnd.mozilla.xul+xml	application/vnd.mozilla.xul+xml
application/vnd.ms-excel	Excel
application/vnd.ms-excel.addin.macroEnabled.12	application/vnd.ms-excel.addin.macroEnabled.12
application/vnd.ms-excel.sheet.binary.macroEnabled.12	Microsoft Excel - Macro enabled
application/vnd.ms-excel.sheet.macroEnabled.12	Microsoft Excel - Macro enabled
application/vnd.ms-excel.sheet.macroenabled.12	application/vnd.ms-excel.sheet.macroenabled.12
application/vnd.ms-excel.template.macroenabled.12	application/vnd.ms-excel.template.macroenabled.12
application/vnd.ms-fontobject	application/vnd.ms-fontobject
application/vnd.ms-htmlhelp	application/vnd.ms-htmlhelp
application/vnd.ms-officetheme	application/vnd.ms-officetheme
application/vnd.ms-package.relationships+xml	application/vnd.ms-package.relationships+xml
application/vnd.ms-pki.seccat	Microsoft Exchange Server Certificate Store
application/vnd.ms-powerpoint	Microsoft PowerPoint
application/vnd.ms-powerpoint.presentation.macroEnabled.12	application/vnd.ms-powerpoint.presentation.macroEnabled.12
application/vnd.ms-powerpoint.slideshow.macroEnabled.12	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
application/vnd.ms-powerpointtd	Microsoft PowerPoint

application/vnd.ms-project	application/vnd.ms-project
application/vnd.ms-publisher	application/vnd.ms-publisher
application/vnd.ms-word.document.macroEnabled.12	Microsoft Word - Macro enabled
application/vnd.ms-xpsdocument	application/vnd.ms-xpsdocument
application/vnd.oasis.opendocument.chart	application/vnd.oasis.opendocument.chart
application/vnd.oasis.opendocument.graphics	application/vnd.oasis.opendocument.graphics
application/vnd.oasis.opendocument.presentation	Presentation
application/vnd.oasis.opendocument.spreadsheet	Spreadsheet
application/vnd.oasis.opendocument.text	Open Document Text
application/vnd.openxmlformats-officedocument.presentationml.presentation	Microsoft PowerPoint
application/vnd.openxmlformats-officedocument.presentationml.slide	Microsoft Powerpoint
application/vnd.openxmlformats-officedocument.presentationml.slideshow	Microsoft Powerpoint
application/vnd.openxmlformats-officedocument.presentationml.template	application/vnd.openxmlformats-officedocument.presentationml.template
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Microsoft Excel
application/vnd.openxmlformats-officedocument.spreadsheetml.template	application/vnd.openxmlformats-officedocument.spreadsheetml.template
application/vnd.openxmlformats-officedocument.wordprocessingml.document	Microsoft Word
application/vnd.openxmlformats-officedocument.wordprocessingml.template	application/vnd.openxmlformats-officedocument.wordprocessingml.template
application/vnd.palm	application/vnd.palm
application/vnd.symbian.install	application/vnd.symbian.install
application/vnd.tcpdump.pcap	Wireshark or Tcpdump Packet Capture
application/vnd.visio	Microsoft Visio
application/vns.ms-outlook	Microsoft Outlook messages
application/x-7z-compressed	7zip compressed archive
application/x-adobeaamdetect	Adobe Application Manager
application/x-adobeexmandetect	application/x-adobeexmandetect
application/x-apple-diskimage	Apple disk image

application/x-bittorrent	application/x-bittorrent
application/x-bzip2	application/x-bzip2
application/x-cab	application/x-cab
application/x-cfs-compressed	application/x-cfs-compressed
application/x-coredump	application/x-coredump
application/x-couponprinterplugin	application/x-couponprinterplugin
application/x-dbm	application/x-dbm
application/x-dosexec	Executable
application/x-dvi	application/x-dvi
application/x-executable	Executable
application/x-fla	application/x-fla
application/x-font	application/x-font
application/x-font-otf	application/x-font-otf
application/x-font-ttf	application/x-font-ttf
application/x-font-type1	application/x-font-type1
application/x-font-woff	application/x-font-woff
application/x-freemind	application/x-freemind
application/x-gtar	GNU tar compressed archive
application/x-gzip	GNU Zip compressed archive
application/x-iso9660-image	application/x-iso9660-image
application/x-iwork-keynote-sffkey	application/x-iwork-keynote-sffkey
application/x-iwork-numbers-sffnumbers	application/x-iwork-numbers-sffnumbers
application/x-iwork-pages-sffpages	application/x-iwork-pages-sffpages
application/x-javascript	application/x-javascript
application/x-maker	application/x-maker
application/x-mobipocket-ebook	application/x-mobipocket-ebook
application/x-ms-shortcut	application/x-ms-shortcut
application/x-ms-wmz	application/x-ms-wmz
application/x-msdos-program	Microsoft Windows Application
application/x-msi	application/x-msi
application/x-msmetafile	application/x-msmetafile
application/x-mspublisher	application/x-mspublisher
application/x-nawk	application/x-nawk

application/x-ns-proxy-autoconfig	application/x-ns-proxy-autoconfig
application/x-object	application/x-object
application/x-perl	Perl Source Code
application/x-pkcs12	PKI Certificate
application/x-pkcs7-crl	PKI Files
application/x-python-code	Source Code (python)
application/x-rar-compressed	RAR compressed archive
application/x-redhat-package-manager	application/x-redhat-package-manager
application/x-sas	Statistical Analysis
application/x-sharedlib	application/x-sharedlib
application/x-shellscript	Shell Script
application/x-shockwave-flash	application/x-shockwave-flash
application/x-silverlight-app	application/x-silverlight-app
application/x-stuffit	Stuffit compressed archive
application/x-subrip	application/x-subrip
application/x-tar	TAR archive
application/x-tex-tfm	Apache Font
application/x-texinfo	application/x-texinfo
application/x-troff-man	application/x-troff-man
application/x-wais-source	application/x-wais-source
application/x-x509-ca-cert	application/x-x509-ca-cert
application/x-xcf	application/x-xcf
application/x-xfig	application/x-xfig
application/x-xpinstall	application/x-xpinstall
application/x-zip	Zip compressed archive
application/xhtml+xml	application/xhtml+xml
application/xmind	application/xmind
application/xml	XML Text
application/xv+xml	application/xv+xml
application/zip	Zip compressed archive
binary/octet-stream	binary/octet-stream
chemical/x-cache	chemical/x-cache
chemical/x-cerius	chemical/x-cerius

chemical/x-gamess-input	chemical/x-gamess-input
chemical/x-genbank	chemical/x-genbank
chemical/x-mdl-sdfile	chemical/x-mdl-sdfile
chemical/x-pdb	Protein Databank chemical/x-pdb
chemical/x-rosdal	chemical/x-rosdal
message/rfc822	message/rfc822
text/cache-manifest	text/cache-manifest
text/calendar	text/calendar
text/css	text/css
text/csv	Comma Separated Values
text/html	text/html
text/json	JavaScript Object Notation
text/plain	Plain Text
text/rtf	text/rtf
text/tab-separated-values	Tab separated values
text/texmacs	text/texmacs
text/vnd.graphviz	text/vnd.graphviz
text/x-asm	Source Code (Assembly)
text/x-bibtex	text/x-bibtex
text/x-c	Source Code (c)
text/x-c++hdr	Source Code (C++ headers)
text/x-c++src	Source Code (c++)
text/x-chdr	Source Code (C headers)
text/x-component	text/x-component
text/x-csh	Source Code (C shell)
text/x-csharp	Source Code (C#)
text/x-csrc	Source Code (C)
text/x-diff	text/x-diff
text/x-dsrc	text/x-dsrc
text/x-java	Source Code (Java)
text/x-java-source	Source Code (Java)
text/x-markdown	text/x-markdown
text/x-nfo	text/x-nfo

text/x-objcsrc	Source Code (Objective-C)
text/x-pascal	Source Code (Pascal)
text/x-perl	Source Code (Perl)
text/x-python	Source Code (Python)
text/x-sfv	text/x-sfv
text/x-sh	Source Code (x-sh)
text/x-sql	Source Code (SQL)
text/x-tex	text/x-tex
text/x-url	text/x-url
text/x-vcard	text/x-vcard
text/xml	XML Text

File Extension

Once Macie Classic begins monitoring your data, it uses several automatic content classification methods to identify and prioritize your sensitive and critical data and to accurately assign business value to your data. One of these methods is classifying by file extension.

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

Macie Classic can assign only one file extension to an object.

You can't modify existing or add new file extensions. You can enable or disable any existing file extensions, thus enabling or disabling Macie Classic to assign them to your objects during the classification process.

To view, enable, or disable file extensions

1. In the Macie Classic 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** dropdown and choose **Save**.

The following is the complete list of file extensions that Macie Classic can assign to your objects during classification.

Name	Description
7z	7-Zip compressed file
abc	SolidWorks CAD
accdb	Microsoft Access database

apk	Application installable on Android
bat	Batch file
bin	Compressed archive. Readable by Java. Extractable by 7-zip
bz2	Bzip2 compressed archive
bzip2	Bzip2 compressed archive
c	C source code
c#	C# source code
cab	Microsoft cabinet. Extractable via ZIP
cc	C++ source code
cer	PKI certificate
cpp	C++ source code
csv	Comma Separated Values
cxx	C++ source code
dbf	dBase database
dbx	Microsoft Outlook Express
deb	Debian Linux install package
dmg	Apple OS X Application Installer
doc	Microsoft Word
docx	Microsoft Word
dot	Microsoft Word
dotx	Microsoft Word
dwg	AutoDesk CAD
dxf	AutoCAD
eml	MIME email
emlx	Apple Mail email message
exe	Microsoft Windows PE Executable
gpg	PGP certificate
gz	GNU Zip compressed archive
gzip	GNU Zip compressed archive
html	Hyper Text Markup Language
iwa	Apple iWork document archive file
jar	Java source code archive
java	Java source code

json	Java Script Object Notation Values (JSON)
key	Apple Keynote Presentation
keynote	Apple Keynote Presentation
lua	Lua source code
mdb	Microsoft Access database
msg	Microsoft Outlook Message
msi	Microsoft Windows Application Installer
odp	OpenOffice.org OpenDocument presentation file
oos	OpenOffice.org spreadsheet file
p12	PKI certificate
pages	Apple Pages
pdf	Adobe PDF
perl	Perl source code
pgp	PGP certificate
pl	Perl source code
pot	Microsoft PowerPoint
pps	Microsoft PowerPoint
ppt	Microsoft PowerPoint
pptx	Microsoft PowerPoint
pst	Microsoft Outlook
py	Python source code
rar	RAR archive. Extractable by 7-zip
rtf	Rich Text Format
sdp	OpenOffice.org presentation file
sdw	OpenOffice.org text document file
sldasm	SolidWorks CAD
slddrw	SolidWorks CAD
sldprt	SolidWorks CAD
sql	Structured Query Language
sxi	OpenOffice.org presentation file
sxw	OpenOffice.org Writer document file
tar.gz	GNU Zip compressed archive
tsv	Tab Separated Values

txt	Text Document
vdx	Microsoft Visio
vsd	Microsoft Visio
vss	Microsoft Visio
vst	Microsoft Visio
vsx	Microsoft Visio
vtw	Microsoft Visio
vtx	Microsoft Visio
xls	Microsoft Excel
xlsx	Microsoft Excel
xlw	Microsoft Excel
xml	Extensible Markup Language (XML)
xps	Open XML document specification
zip	ZIP compressed archive

Theme

Once Macie Classic begins monitoring your data, it uses several automatic content classification methods to identify and prioritize your sensitive and critical data and to accurately assign business value to your data. One of these methods is classifying by theme.

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

Macie Classic can assign one or more themes to an object.

You can't modify existing or add new themes. You can enable or disable any existing themes, thus enabling or disabling Macie Classic to assign them to your objects during the classification process.

To view, enable, or disable themes

1. In the Macie Classic 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** dropdown and then choose **Save**.

The following is the complete list of themes that Macie Classic can assign to your objects during classification.

Theme title	Minimum keyword combinations
American Express Credit Card Keywords	1

Attorney Client Privileged	2
Audit Keywords	3
Banking Keywords	1
Big Data Frameworks	2
Cisco Analysis Keywords	1
Confidential Markings	2
Corporate Growth Keywords	3
Corporate Project Plan	3
Corporate Proposals	3
Credit Card Keywords	1
Encrypted Data Keywords	1
Financial Keywords	1
Hacker Keywords	2
Limit Distribution Markings	3
Mastercard Credit Card Keywords	1
Metasploit Framework Keywords	1
NMAP OS Fingerprinting	1
Network Scanner Keywords	1
Network Service Fingerprinting Keywords	1
Network Traffic Analysis Keywords	1
OS Backdoor Keywords	1
Offline Attacks Keywords	1
Online Attacks Keywords	1
Oracle DB Analysis Keywords	1
Password Keywords	2
Project Tracking Keywords	2
Proprietary Markings	2
Real-Time Processing Frameworks	2
Restricted Markings	2
SSL Forensic Analysis Keywords	1
Secret Markings	3
Sensitive Markings	3
Social Security Keywords	2

Stock Keywords	3
Taxpayer EIN Keywords	2
Tunneling Attacks Keywords	1
Unclassified Markings	2
VISA Credit Card Keywords	1
Vulnerability Assessment Keywords	2
Web Exploitation Tool Keywords	1
Web Vulnerability Scanner Keywords	1
pof OS Fingerprinting	2

Regex

Once Macie Classic begins monitoring your data, it uses several automatic content classification methods to identify and prioritize your sensitive and critical data and to accurately assign business value to your data. One of these methods is classifying by regex.

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

Macie Classic can assign one or more regexes to an object.

You can't modify existing or add new regexes. You can enable or disable any existing regexes, thus enabling or disabling Macie Classic to assign them to your objects during the classification process.

To view, enable, or disable regexes

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

   To enable or disable a regex, on its details page, use the **Enabled/Disabled** dropdown and choose **Save**.

The following is the complete list of regexes that Macie Classic can assign to your objects during classification.

Name	Classification
Arista network configuration	Regex
BBVA Compass Routing Number - California	Regex
Bank of America Routing Numbers - California	Regex
Box Links	Regex
CVE Number	Regex
California Drivers License	Regex

Chase Routing Numbers - California	Regex
Cisco Router Config	Regex
Citibank Routing Numbers - California	Regex
DSA Private Key	Regex
Dropbox Links	Regex
EC Private Key	Regex
Encrypted DSA Private Key	Regex
Encrypted EC Private Key	Regex
Encrypted Private Key	Regex
Encrypted PuTTY SSH DSA Key	Regex
Encrypted PuTTY SSH RSA Key	Regex
Encrypted RSA Private Key	Regex
Google Application Identifier	Regex
HIPAA PHI National Drug Code	Regex
Huawei config file	Regex
Individual Taxpayer Identification Numbers (ITIN)	Regex
John the Ripper	Regex
KeePass 1.x CSV Passwords	Regex
KeePass 1.x XML Passwords	Regex
Large number of US Phone Numbers	Regex
Large number of US Zip Codes	Regex
Lightweight Directory Access Protocol	Regex
Metasploit Module	Regex
MySQL database dump	Regex
MySQLite database dump	Regex
Network Proxy Auto-Config	Regex
Nmap Scan Report	Regex
PGP Header	Regex
PGP Private Key Block	Regex
PKCS7 Encrypted Data	Regex
Password etc passwd	Regex
Password etc shadow	Regex
PlainText Private Key	Regex

PuTTY SSH DSA Key	Regex
PuTTY SSH RSA Key	Regex
Public Key Cryptography System (PKCS)	Regex
Public encrypted key	Regex
RSA Private Key	Regex
SSL Certificate	Regex
SWIFT Codes	Regex
Samba Password config file	Regex
Simple Network Management Protocol Object Identifier	Regex
Slack 2FA Backup Codes	Regex
UK Drivers License Numbers	Regex
UK Passport Number	Regex
USBank Routing Numbers - California	Regex
United Bank Routing Number - California	Regex
Wells Fargo Routing Numbers - California	Regex
aws_access_key	Regex
aws_credentials_context	Regex
aws_secret_key	Regex
facebook_secret	Regex
github_key	Regex
google_two_factor_backup	Regex
heroku_key	Regex
microsoft_office_365_oauth_context	Regex
pgSQL Connection Information	Regex
slack_api_key	Regex
slack_api_token	Regex
ssh_dss_public	Regex
ssh_rsa_public	Regex

Personally Identifiable Information

Object classification by personally identifiable information (PII) is based on recognizing any personally identifiable artifacts based on industry standards such as NIST-80-122 and FIPS 199. Macie Classic can 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 Classic 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 Classic uses to classify your S3 objects is the Support Vector Machine (SVM) classifier. It classifies content inside your S3 objects (text, token n-grams, and character n-grams) that Macie Classic monitors and their metadata features (document length, extension, encoding, headers) to accurately classify documents based on content. This classifier, managed by Macie Classic, 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. The classifier can also 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 "source code."

> **Note**
> This data classification method isn't surfaced in the **Settings** page. Macie Classic manages the following list of artifacts. You can't edit, enable, or disable them.

The SVM classifier in Macie Classic 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
  - Amazon 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 previously described, an object that Macie Classic monitors is assigned various risk levels based on each content type, file extension, theme, regex, 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 Classic 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 Classic

Macie Classic can help you monitor how your sensitive and business-critical data stored in the Amazon Web Services Cloud is being used. Macie Classic 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.

After you enable Macie Classic, it uses the following automated methods to protect your data.

Topics

AWS CloudTrail Events

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

You can't modify existing or add new CloudTrail events to the list that Macie Classic manages. You can enable or disable the supported CloudTrail events, thus instructing Macie Classic to either include or exclude them in its data security process.

To view, enable, or disable supported CloudTrail events

1. In the Macie Classic 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** dropdown and then choose **Save**.

AWS CloudTrail Errors

Macie Classic analyzes and processes errors that can occur when a subset of data that CloudTrail logs and management events (API calls) take place in your infrastructure. Macie Classic designates a risk level between 1 and 10 for each of the supported CloudTrail errors, with 10 being the highest risk and 1 being the lowest.

You can't modify existing or add new CloudTrail errors to the list that Macie Classic manages. You can enable or disable the supported CloudTrail errors, thus instructing Macie Classic to either include or exclude them in its data security process.

To view, enable, or disable supported CloudTrail errors

1. In the Macie Classic 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** dropdown and then choose **Save**.

Viewing Data and Activity that Amazon Macie Classic Monitors

The Macie Classic **Dashboard** draws a comprehensive picture of all of your data and activity that Macie Classic monitors. 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 Classic console's **Research** tab. There you can construct and run queries in the query parser and conduct in-depth investigative research of your data and activity that Macie Classic monitors.

Dashboard Metrics

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

- **High-risk S3 objects** – While classifying data (p. 25), Macie Classic assigns a risk value to each monitored data object. This is Macie Classic'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 Classic-monitored data objects with a risk levels of 8 through 10.
- **Total event occurrences** – As part of securing data (p. 44), Macie Classic analyzes and processes events (API calls) logged by AWS CloudTrail that occur within your infrastructure. This metric provides the total count of all of the event occurrences monitored by Macie Classic that took place within your infrastructure since you enabled Macie Classic.
- **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 Classic analyzed and processed since it was enabled.

Dashboard Views

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

To use Macie Classic dashboard views

1. Choose the corresponding icon to select any of the following views to display various subsets of your data and activity monitored by Macie Classic:
   - S3 objects for a selected time range (p. 47)
   - S3 objects (p. 47)
   - S3 objects by PII (p. 48)
   - S3 public objects by buckets (p. 49)
   - S3 objects by ACL (p. 49)
   - CloudTrail events and associated users (p. 50)

- CloudTrail errors and associated users (p. 50)
- Activity location (p. 51)
- AWS CloudTrail events (p. 52)
- Activity ISPs (p. 52)
- AWS CloudTrail user identity types (p. 52)

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 view only 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 equal to or greater than the value selected on the **Minimum risk** slider
- The object was last modified during one of the following time ranges:
  - The past 6 months
  - Between the date when Macie Classic was enabled and a date six months before today

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

You can follow this sample procedure.

1. In the Macie Classic **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're redirected to the **Research** tab with the following query, which automatically appears 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 S3 objects monitored by Macie Classic 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 also appear. You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

S3 Objects

This view provides the complete list of your S3 objects monitored by Macie Classic, grouped by the assigned themes. For each theme, a percentage that this theme represents of the total number of your S3 objects monitored by Macie Classic 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, choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that appears in the query parser in the **Research** tab.

You can follow this sample procedure.

1. In the Macie Classic **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're redirected to the **Research** tab with the following query, which automatically appears in the query parser:

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

   This query matches your selection to view the S3 objects monitored by Macie Classic with the assigned theme of **json/aws_cloudtrail_logs**. The results of this query also appear. You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

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 PII priority assigned by Macie Classic. 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 Classic (p. 25).

To navigate from this view to the **Research** tab, 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 appears in the query parser in the **Research** tab.

You can follow this sample procedure.

1. In the Macie Classic **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're redirected to the **Research** tab with the following query, which automatically appears in the query parser:

   ```
   pii_impact:"low"
   ```

   The results of this query also appear. You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

S3 Public Objects by Buckets

This is a complete list of your public S3 objects grouped by the buckets that they're stored in. For each bucket, a percentage that this bucket's objects represent of the total number of your S3 objects managed by Macie Classic 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, choose the looking glass icon next to any of the displayed buckets. Your selection is automatically translated into a query that appears 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 (ACLs) 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, 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 Classic **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're redirected to the **Research** tab with the following query, which automatically appears in the query parser.

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

   The results of this query also appear. You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

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, select (double-click) any square that represents a particular event that you want to investigate further. The number in parentheses next to the event name represents the number of user sessions (5-minute aggregates of CloudTrail data) that this event is present in. In the **Research** tab, your selection is automatically translated into a query that appears in the query parser.

- **AWS CloudTrail 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, select (double-click) any square that represents a particular error that you want to investigate further. The number in parentheses next to the user name represents the number of user sessions (5-minute aggregates of CloudTrail data) that this user is associated with. In the **Research** tab, your selection is automatically translated into a query that appears in the query parser.

You can follow this sample procedure.

1. In the Macie Classic **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 that the **PutRestApi** event is present in. Double-click the square next to **PutRestApi**.

   As a result, you're redirected to the **Research** tab with the following query, which automatically appears in the query parser.

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

   The results of this query also appear. You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

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, select (double-click) any square that represents a particular error that you want to investigate further. The number in parentheses next to the error name represents the number of user sessions (5-minute aggregates of CloudTrail data) that this error is present in. In the **Research** tab, your selection is automatically translated into a query that appears in the query parser.

- **AWS CloudTrail 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, select (double-click) any square that represents a particular error that you want to investigate further. The number in parentheses next to the user name represents the number of user sessions (5-minute aggregates of CloudTrail data) that this user is associated in. In the **Research** tab, your selection is automatically translated into a query that appears in the query parser.

You can follow this sample procedure.

1. In the Macie Classic **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 that the **Client.InvalidPermission.NotFound** error is present in. Double-click the square next to **Client.InvalidPermission.NotFound**.

   As a result, you're redirected to the **Research** tab with the following query, which automatically appears in the query parser.

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

   The results of this query also appear. You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

Activity Location

This view includes a map that shows the locations of activity that Macie Classic is monitoring for a selected time period. To view details, 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 tool tip window for a location pin. In the **Research** tab, your selection is automatically translated into a query that appears in the query parser. For example, you can autogenerate 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 modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

AWS CloudTrail Events

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

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

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

You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

Activity ISPs

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

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

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

You can modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

AWS CloudTrail User Identity Types

This view provides the complete list of your CloudTrail data and management events monitored by Macie Classic, grouped by the user identity type (for more information, see the definition for *user* in Concepts and Terminology (p. 12)). For each user identity type, the total count of the user sessions (5-minute integrations of CloudTrail data) that this user identity type is present in 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, choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that appears in the query parser in the **Research** tab. For example, you can autogenerate 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 modify the query result controls available on the **Research** tab, run the query again, and conduct in-depth investigative research of the generated results. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

Amazon Macie Classic Alerts

An *alert* is a notification about a potential security issue discovered by Amazon Macie Classic.

Topics

Basic and Predictive Macie Classic Alerts

Macie Classic generates two types of alerts:

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

    Note
    You can identify managed basic alerts by the value of `Default` in the **Created by** field in the **Basic alerts** list in the **Settings** tab.
  - Custom basic alerts that you can create and modify to your exact specifications. For more information, see Adding New and Editing Existing Custom Basic Alerts (p. 56).
- **Predictive alerts** – Automatic alerts based on activity in your AWS infrastructure that deviates from the established normal activity baseline. More specifically, Macie Classic continuously monitors activity in your AWS infrastructure and builds a model of the normal behavior. Then it looks for deviations from that normal baseline, and when it detects such activity, it generates automatic predictive alerts. For example, a user uploading or downloading a large number of S3 objects in a day might trigger an alert if that user typically downloads one or two S3 objects in a week.

Alert Categories in Macie Classic

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

Severity Levels for Alerts in Macie Classic

Each Macie Classic 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 indicate a security issue that can result in compromised information confidentiality, integrity, and availability in your infrastructure. The **Informational** level highlights a security configuration detail of your infrastructure that Macie Classic monitors. The following are recommended ways to respond to each level:

- **Critical** – Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability in 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 in 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 in 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 in 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 note this information or use it to improve the security of your systems and resources.

Locating and Analyzing Macie Classic 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 Classic 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 Classic (p. 54).
   - A timestamp that indicates when the alert was generated or last updated.
   - The alert category. For more information, see Alert Categories in Macie Classic (p. 53).
   - One of the following:
     - If the alert's index is **CloudTrail data**, a user that engaged in the activity that prompted Macie Classic to generate the alert. For more information, see the definition of *user* in the context of Macie Classic in Concepts and Terminology (p. 12).
     - 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 Classic to generate the alert.

       Important
       In Macie Classic, 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 Classic 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 Classic to generate the alert.
   - The number of comments that were left on the alert.
   - The total number of results, which can consist of a list of user sessions, or a list of S3 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. 56).
   - The number of views on the alert.
   - The AWS Region where 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, S3 buckets, or 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, S3 buckets, or S3 objects, depending on the index that is specified in the definition for this alert. For more information, see Adding New and Editing Existing Custom Basic Alerts (p. 56).
     - 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 and view all its fields. For more information, see the *Researching AWS Data*, *Researching S3 Bucket Properties Data*, or *Researching S3 Objects Data* sections in Researching Through Data Monitored by Amazon Macie Classic (p. 65).

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 prepopulated 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 Classic 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 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 S3 bucket policy or S3 ACL that grants read rights to everyone."
     - Description for the alert – For example, "An S3 bucket policy or S3 ACL on an S3 bucket contains a clause that effectively grants read access to any user. We recommend 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 Classic (p. 53).
     - Alert query – A query that describes the activity that you want Macie Classic to generate an alert about. For example, `s3_world_readability:"true"`. This query looks for an S3 bucket policy or S3 ACL policy on an S3 bucket that grants read access to any user. For more information about constructing queries, see Constructing Queries in Macie Classic (p. 65).

       Note
       You can use the looking glass icon next to an existing alert to navigate to the **Research** tab. This alert's query automatically appears in the **Query Parser**, and the results of this query appear in the **Research** tab.
     - Query index – The repository of data against which Macie Classic 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 a list of CloudTrail user sessions (5-minute aggregates of raw CloudTrail data), S3 buckets, or 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 Classic (p. 54)
     - Users or buckets, depending on the selected alert index, that are explicitly allowed to perform the activity that the alert defines. If you explicitly allow a user or a bucket, Macie Classic doesn't generate an alert for this user or bucket when they're involved in the activity that the alert defines.

       Important
       In Macie Classic, 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 Classic 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 Classic to generate the alert.

When you explicitly allow a user in a basic alert with the index of CloudTrail data, you must use a special Macie Classic format called `macieUniqueId`. Examples include `123456789012:root`, `123456789012:user/Bob`, and `123456789012:assumed-role/Accounting-Role/Mary`, depending on the identity type of the user. For more information, see the definition of *user* in Analyzing Amazon Macie Classic–Monitored Data by User Activity (p. 60).

- 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 edit the existing basic alerts.

1. In the Macie Classic console, navigate to the **Alerts** page and locate the alert that you want to 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 isn't available for predictive alerts. You can't edit predictive alerts, which Macie Classic automatically generates based on activity in your AWS infrastructure that deviates from the established normal activity baseline. For more information, see Basic and Predictive Macie Classic Alerts (p. 53).

Group Archiving Alerts

You can use the following procedure to group archive alerts.

1. In the Macie Classic 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.

Explicitly Allowing Users or Buckets for Basic Alerts

You can explicitly allow users (if the alert's index is **CloudTrail data**) and buckets (if the alert's index is **S3 bucket properties** or **S3 objects**) for alerts managed by Macie Classic and custom basic alerts. (You cannot do this for predictive alerts.)

Use the following procedure to explicitly allow a specific user or a specific bucket that engaged in or was involved in the activity that prompted Macie Classic to generate a specific alert.

Important
In Macie Classic, 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 Classic 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 Classic to generate the alert.

To explicitly allow users or S3 buckets for custom basic alerts using the Alerts tab

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

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

To explicitly allow users or S3 buckets for custom basic alerts using the Settings tab

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

   Note
   When you explicitly allow a user in a basic alert with the index of CloudTrail data, you must use a special Macie Classic format called `macieUniqueId`. Examples include `123456789012:root`, `123456789012:user/Bob`, and `123456789012:assumed-role/Accounting-Role/Mary`, depending on the identity type of the user. For more information, see the definition of the user concept in Analyzing Amazon Macie Classic–Monitored Data by User Activity (p. 60).

Explicitly allow users or S3 buckets for Macie Classic-managed basic alerts

1. In the Macie Classic console's **Alerts** tab, locate the basic alert that is managed by Macie Classic and you want to explicitly allow users or S3 buckets for.
2. Choose the down arrow in the alert summary pane and then choose **Allow user** (if the alert's index is **CloudTrail data**) or **Allow bucket** (if the alert's index is **S3 bucket properties** or **S3 objects**).
3. In the window that appears, select the **Clone and disable the default managed alert** check box and choose **Submit**.
4. Navigate to the Macie Classic console's **Settings** tab.

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

Note
When you explicitly allow a user in a basic alert with the index of CloudTrail data, you must use a special Macie Classic format called `macieUniqueId`. Examples include `123456789012:root`, `123456789012:user/Bob`, and `123456789012:assumed-role/Accounting-Role/Mary`, depending on the identity type of the user. For more information, see the definition of *user* in Analyzing Amazon Macie Classic–Monitored Data by User Activity (p. 60).

Analyzing Amazon Macie Classic–Monitored Data by User Activity

The **Users** tab can help you draw a comprehensive picture of all of the data and activity monitored by Macie Classic 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. It also describes 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 Classic console's **Research** tab. There you can construct and run queries in the query parser and conduct in-depth investigative research of the data and activity monitored by Macie Classic for the selected users.

Topics

Macie ClassicUniqueID

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

- **Root** – The request was made with your Amazon Web Services 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 operation.
- **Federated user** – The request was made with temporary security credentials that were obtained via a call to the AWS STS `GetFederationToken` API operation.
- **AWS account** – The request was made by another Amazon Web Services account.
- **AWS service** – The request was made by an account that belongs to an AWS service.

When specifying a user in the Macie Classic console, you must use a special Macie Classic format called `macieUniqueId`. Examples of specifying a user include searching for a user in the **Users** tab, constructing a query in the **Research** tab, and explicitly allowing a user in a basic alert with the index of **CloudTrail data**. 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 following examples 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`
`"recipientAccountId": "123456789012", "userIdentity": { "invokedBy": "codepipeline.amazonaws.com", "type": "AWSService" }`	`123456789012:codepipeline.amazonaws.com`
`"recipientAccoundId": "123456789012", "userIdentity": { "type": "AWSAccount" "accountId": "987654321098", "principalId": "AIDABCDEFGHI123456XYZ", }`	`123456789012:AIDABCDEFGHI123456XYZ`

User Categories in Macie Classic

Based on their activity (API calls), users in Macie Classic 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 Simple Storage Service (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 make 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 data and activity monitored by Macie Classic for the specified user.

1. In the Macie Classic 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 Classic format called **macieUniqueId**: for example, `123456789012:root`, `123456789012:user/Bob`, or `123456789012:assumed-role/Accounting-Role/Mary`, depending on the identity type of the user. For more information, see the definition of *user* in Concepts and Terminology (p. 12).
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 data and activity that Macie Classic monitors:

   - High-risk CloudTrail events (p. 62)
   - High-risk CloudTrail errors (p. 63)
   - Activity location (p. 63)
   - CloudTrail events (p. 63)
   - Activity ISPs (p. 63)
   - CloudTrail user identity types (p. 63)
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 view only 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. 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, select (double-click) any square that represents a particular event that you want to investigate further. The number in parentheses next to the event name represents the number of user sessions (5-minute aggregates of CloudTrail data) that this event is present in. In the **Research** tab, your selection is automatically translated into a query that appears

in the query parser. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

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, select (double-click) any square that represents a particular error that you would like to investigate further. The number in parentheses next to the error name represents the number of user sessions (5-minute aggregates of CloudTrail data) that this error is present in. In the **Research** tab, your selection is automatically translated into a query that appears in the query parser. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

Activity Location

This view includes a map that shows the locations of activity that Macie Classic is monitoring for a selected time period for the specified user. To view details, use the available time period dropdown (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 tool tip window for a location pin. In the **Research** tab, your selection is automatically translated into a query that appears in the query parser. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

CloudTrail Events

This view provides the complete list of CloudTrail data and management events monitored by Macie Classic for the specified user. For each event, the total count of the user sessions (5-minute integrations of CloudTrail data) that this event is present in, 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, choose the looking glass icon next to any of the displayed events. Your selection is automatically translated into a query that appears in the query parser in the **Research** tab. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

Activity ISPs

This view provides the complete list of CloudTrail data and management events monitored by Macie Classic, 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) that this ISP is present in, 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, choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that appears in the query parser in the **Research** tab. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

CloudTrail User Identity Types

This view provides the complete list of CloudTrail data and management events monitored by Macie Classic, grouped by the user identity type for the specified users. For more information, see the definition

for *user* in Concepts and Terminology (p. 12) . For each user identity type, the total count of the user sessions (5-minute integrations of CloudTrail data) that this user identity type is present in, 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, choose the looking glass icon next to any of the displayed themes. Your selection is automatically translated into a query that appears in the query parser in the **Research** tab. For more information, see Researching Through Data Monitored by Amazon Macie Classic (p. 65).

Researching Through Data Monitored by Amazon Macie Classic

You can use the **Research** tab in the Macie Classic console to construct and run queries in the query parser and conduct in-depth investigative research of your data and activity that Macie Classic monitors. You can navigate to the **Research** tab at any time and construct queries in the empty parser. For more information, see Constructing Queries in Macie Classic (p. 65). You can be redirected to the **Research** tab from various places throughout the Macie Classic console: for example, any of the **Dashboard** views (see Viewing Data and Activity that Amazon Macie Classic Monitors (p. 46)) or the **Basic alerts** list (see Amazon Macie Classic Alerts (p. 53)). When redirected to the **Research** tab from other places in the console, your data selection is translated into an automatically generated query that appears in the query parser.

Topics

Constructing Queries in Macie Classic

Macie Classic enables you to construct queries in the query parser in the **Research** tab. The query parser is a lexer that 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:

- To search for any console login that didn't originate from IP addresses owned by Amazon: `eventNameIsp.compound:/ConsoleLogin:~(Amazon.*)/`
- 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 Classic date, integer, and string field types.

Example Queries: Date Field Type

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 Classic-monitored	CloudTrail data

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

Example Queries: Integer Field Type

Example Query	Description	Data Repository
`dlp_risk>6 AND filesystem_metadata.server_side_encryption:""`	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

Example Queries: String Field Type

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 might 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 Classic **Research** tab, you can apply the following filters to your searches.

Data Index

The first **Research** tab filter (dropdown) with the preselected default value of **CloudTrail data**, enables you to specifying the index (or the data repository) that you want Macie Classic 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 Classic is monitoring
- **S3 objects** – A collection of metadata about the S3 objects that are stored in the buckets that Macie Classic is monitoring

Number of Results to Display

The next **Research** tab filter with the preselected default value of **Top 10** enables 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 preselected default value of **Past 30 days** enables you to define a time range that you want to display your search results for. This filter includes the following options:

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

- Custom time range

Saving a Query as an Alert

You can use the following procedure to save a query that appears in the query parser as a basic alert. For more information about basic alerts, see Amazon Macie Classic Alerts (p. 53).

1. In the Macie Classic 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 choose **Save**. For more information, see Adding New and Editing Existing Custom Basic Alerts (p. 56).

Favorite Queries

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

1. In the Macie Classic 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 choose **Save**.
4. To view the list of your favorite queries, in the Macie Classic 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 Classic-monitored CloudTrail data.

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

1. Select **CloudTrail data** in the first filter dropdown.
2. For this example, select **Top 10** in the second filter dropdown.
3. For this example, select **Past 90** days in the third filter dropdown.
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 dataset is very large and you specify a very wide time range, your data might not render properly, and this graph might not appear 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 produces a subset of the results generated by your original selections in the preceding steps. Double-click any of the graph's results and your selection is translated into a new query that automatically appears in the query parser, and the **Research** tab is refreshed with the results of this new query.
- **Search results summary** – A list of the most significant fields from your search. The first line includes the top (or bottom) three 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 produces a subset of the results generated by your original selections in the preceding steps. 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 automatically appears 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. 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 Classic extracts from CloudTrail. These fields also include Amazon S3 data events. For example, `accountId` in Macie Classic corresponds to `userIdentity.accountId` in CloudTrail, and `eventNameErrorCode.key` in Macie Classic corresponds to `eventName` in CloudTrail.
- The second table includes the fields that Macie Classic generates to provide further security intelligence and context based on the examined CloudTrail data. For example, `isp.key` describes the organization or the ISP that the API request against your AWS resources is coming from, and `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 That Macie Classic Extracts

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 Classic unique ID: a format that is unique to Macie Classic for specifying users. Macie Classic unique ID is a combination of the IAM `UserIdentity` element and the `recipientAccountId`.

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
`accountId`	`userIdentity.accountId`	String	The Amazon Web Services account ID.	Search for user sessions with accesses related to a particular account:

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
				• **accountId:"110912345678"**
`awsRegion.key`	`awsRegion`	String	The AWS Region that the request is made to.	Search for user sessions with any AWS API calls by Region: • **awsRegion.key:"us-west-2"** • **awsRegion.key:"us-east-1"**

`eventNameErrorCode.key`	`eventName` or `errorCode`	String	The event name that resulted in the returned (if any) error code.	• Search for user sessions with any AWS `ConsoleLogin` call:
				  • **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 that the request was made to.	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 Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
`objectsDeleted.key`	`resources[0].ARN`	String	A list of S3 objects ARNs, S3 bucket ARNs, or prefix ARNs that were part of a `DeleteObject` or `DeleteObjects` API call. **Note** When you delete an S3 bucket, both `DeleteBucket` and `DeleteObjects` APIs are called. 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.	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 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:

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
				• **objectsDeleted.key:/ arn:aws:s3:::my_sensitive_bucket.* AND accountId:"ANONYMOUS_PRINCIP**

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
`objectsRead.key`	`resources[0].ARN`	String	A list of S3 object 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 that returns the results of a search against `objectsRead.key` has a maximum limit of 250 records.	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 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:

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
				• **objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket.*/ AND accountId:"ANONYMOUS_PRINCIPA**

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
`objectsWritten.key`	`resources[0].ARN`	String	A list of S3 object ARNs that were part of a `PutObject`, `CopyObject`, or `CompleteMultipartUpload` API call. **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 that returns the results of a search against `objectsWritten.key` has a maximum limit of 250 records.	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 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 Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
				• **objectsWritten.key:/ arn:aws:s3:::my_sensitive_bucket.*/ AND accountId:"ANONYMOUS_PRINCIPA**
principalId	userIdentity.principalId	String	The IAM principal ID. **Note** When an assumed role makes a request, the session name is removed from the principal ID.	Search for user sessions with access requests from a particular principal ID: • **principalId:"AIDAIMABCKFJSKEOAH**
recipientAccountId	recipientAccountId	String	The account ID that received the CloudTrail event.	Search for all activity in a particular account: • **recipientAccountId:"110912345678** Search for anonymous access requests to a particular account: • **recipientAccountId:"110912345678 AND accountId: "ANONYMOUS_PRINCIPAL"**
resourceOwnerAccountIds.key	Resources[1].accountId	String	List of AWS resource owners. An example is a list of account IDs that own an S3 object or bucket.	Search for activity against resources owned by a particular account: • **resourceOwnerAccountIds.key: "110951234567"**
resources.key	Resources[0].arn	String	List of resources (S3 buckets only) associated with the CloudTrail events in 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_PRINCIPA**

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
`sessionName.key`	`userIdentity.principalId`	String	The identifier for the assumed role session. When an assumed role makes a request, the session name is removed from the principal ID and is assigned as a value to `sessionName.key`. When an identity other than an assumed role makes a request, `sessionName.key` is set to `None`.	Search for assumed role access requests from session name `examplesession-cli`: • **sessionName.key:"examplesession-cli"** Search for EC2 instance IDs in 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 an assumed role makes a request, the session name is removed from `sourceARN`.	Search for user sessions with access requests from a particular ARN: • **sourceARN:"arn:aws:iam::1234567 cluster-api"**

Macie Classic Field Name	CloudTrail Field Name	Macie Classic Field Type	Description	Example Search Query
`sourceIPAddress.key`	`sourceIPAddress`	String	The IP address that the request was made from. **Note** A user session that returns the results of a search against `sourceIPAddress.key` has a maximum limit of 60,000 records.	Search for user sessions with access requests from a particular source IP address: • **sourceIPAddress.key:"194.68.22.22** 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.RunInstance AND NOT (sourceIPAddress.key:"autoscaling.**
`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 made by Amazon 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 account: • **userIdentityType.key:"Root"**

Fields That Macie Classic Generates

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 Classic unique ID: a format that is unique to Macie Classic for specifying users. The Macie Classic unique ID is a combination of the IAM `UserIdentity` element and the `recipientAccountId`.

Macie Classic Field Name	Macie Classic 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:

Macie Classic Field Name	Macie Classic Field Type	Description	Example Search Query
			• **@timestamp:>"2017-02-06T23:01:08Z"** • **@timestamp:>"2017-02-06"** 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 43,200 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 that returns 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 that returns 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"**

Macie Classic Field Name	Macie Classic Field Type	Description	Example Search Query
`dcObjectsWritten`	Integer	A count of unique S3 objects written in a user session. **Note** A user session that returns 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]**
`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 made 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 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 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 compound	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 enables Macie Classic to associate an API event name with the error code, if any, that is returned. If there is no error code for the event, 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:"GetO** Search for user sessions with any errors associated with `PutObject` calls: • **eventNameErrorCode.compound:/PutObject:.*/**

Macie Classic Field Name	Macie Classic Field Type	Description	Example Search Query
`eventNameIsp.compound`	String	A compound aggregation that summarizes each CloudTrail event name along with the Internet Service Provider (ISP) that the request originated from. The format is `EventName:ISP` for the term value, which enables Macie Classic to associate an API operation name with the ISP that it originated from.	Search for user sessions with `ConsoleLogin` calls from non-AWS IPs using a regular expression: • **eventNameIsp.compound:/ConsoleLogin:~(Amazon.*)/**
`eventNameIsp.secondary`	String	The ISP that the AWS API call was made from.	Search for user sessions with AWS API calls coming from outside Amazon IP addresses: • **eventNameIsp.secondary:/~(Amazon.*)/**
`macieUniqueId`	String	A format that is unique to Macie Classic for specifying users. The Macie Classic unique ID is a combination of the IAM `UserIdentity` element and the `recipientAccountId`. For more information, see Macie ClassicUniqueID (p. 60).	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**

Macie Classic Field Name	Macie Classic Field Type	Description	Example Search Query
`ipLocation.key`	String	The IP geolocation (city and country) accessed by an identity that Macie Classic monitors.	Search for user sessions with any AWS API call events originating in Los Angeles: • **ipLocation.key:"LosAngeles:UnitedState** Search for user session any AWS API call events originating from outside the United States: • **ipLocation.key:/ ~(.*UnitedStates)/**
`isp.key`	String	The ISP that the AWS API call originated from.	Search for user sessions with AWS API calls coming from outside 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 appear when you use the **Research** tab to investigate your S3 bucket properties data that Macie Classic monitors.

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

1. Select **S3 bucket properties** in the first filter dropdown.
2. For this example, select **Top 10** in the second filter dropdown.
3. For this example, select **Past 90** days in the third filter dropdown.
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 dataset is very large and you specify a very wide time range, your data might not render properly, and this graph might not appear 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 produces a subset of the results generated by your original selections in the preceding steps. Double-click any of the graph's results, and your selection is translated into a new query that automatically appears in the query parser, and the **Research** tab is refreshed with the results of this new query.

- **Search results summary** – A list of the most significant fields from your search. The first line includes the top (or bottom) three 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 produces a subset of the results generated by your original selections in the preceding steps. 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 translated into a new query that automatically appears 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. Choose any bucket to expand it and view its details.

S3 Bucket Properties Data Fields and Example 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 Classic extracts from the Amazon S3 bucket API metadata. For example, `acl.Grants.Grantee.DisplayName` in Macie Classic corresponds to `Grants.Grantee.DisplayName` in the Amazon S3 `getbucket-acl` API response.
- The second table includes the fields that Macie Classic generates 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 Amazon S3 ACL and bucket (IAM) policy.

S3 Bucket Properties Data Fields That Macie Classic Extracts

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
`acl.Grants.Grantee.DisplayName`	`Grantee.DisplayName`	`getbucket-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`	`Grantee.ID`	`getbucket-acl`	String	The ID of the identity that was granted access to	Search for an S3 bucket's grantee

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
				the S3 bucket by the bucket owner.	with a particular canonical ID: • **acl.Grants.Grantee.ID:"75bee88**
`acl.Grants.Grantee.Type`	`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:Canoni** Search for all S3 buckets that are granted to `Groups`: • **acl.Grants.Grantee.Type:Group**
`acl.Grants.Grantee.URI`	`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: • **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"**

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
acl.Grants.Permission	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**
location.LocationConstraint	LocationConstraint	get-bucket-location	String	The AWS Region where the S3 bucket resides. **Note** By default, buckets in the us-east-1 Region have no region returned from the S3 API call. To facilitate searching, Macie Classic automatically populates them with the string "us-east-1".	Search for buckets hosted in the us-west-2 Region: • **location.LocationConstraint:"us west-2"** Search for buckets hosted in the us-east-1 Region: • **location.LocationConstraint:"us east-1"**

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
`logging.LoggingEnabled.TargetGrants.Grantee.DisplayName`	`LoggingEnabled.TargetGrants.Grantee.DisplayName`	`get-bucket-logging`	String	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 (`PutObject`, `PubBucketPolicy`, etc.): • **policy.Policy.Statement.Action: s3:Put.*/**
`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`	`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"**

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
policy.Policy.Statement.NotPrincipal.CanonicalUser	Policy.Statement.NotPrincipal.CanonicalUser	GetBucketPolicy, GetBucketPolicyStatus	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	GetBucketPolicy, GetBucketPolicyStatus	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	GetBucketPolicy, GetBucketPolicyStatus	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**
policy.Policy.Statement.Principal.AWS	Policy.Statement.Principal.AWS	GetBucketPolicy, GetBucketPolicyStatus	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, GetBucketPolicyStatus	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**

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
policy.Policy.Statement.NotPrincipal.Federated	Policy.Statement.NotPrincipal.Federated	get-bucket-policy	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.NotPrincipal.Service	Policy.Statement.NotPrincipal.Service	get-bucket-policy	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	get-bucket-policy	String	The S3 resource that the S3 bucket policy is applied to.	Search for S3 bucket policies containing wildcards: • **policy.Policy.Statement.Resour */**
policy.Policy.Statement.Sid	Policy.Statement.Sid	get-bucket-policy	String	The Sid of the S3 bucket policy.	Search for bucket policies with a particular Sid: • **policy.Policy.Statement.Sid:"1"**
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**

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
versioning.MFADelete	MFADelete	get-bucket-versioning	String	The MFADelete (enabled/disabled) state of the bucket version configuration.	Search for buckets where MFADelete 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"**
• lifecycle_configuration.Rules.Expiration.Date • lifecycle_configuration.Rules.Expiration.Days • lifecycle_configuration.Rules.AbortIncompleteMultipartUpload.DaysAfterInitiation • lifecycle_configuration.Rules.Filter.Prefix • lifecycle_configuration.Rules.Filter.And.Prefix • lifecycle_configuration.Rules.Filter.Tag.Key • lifecycle_configuration.Rules.Filter.And.Tags.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.And.Prefix • Rules.Filter.Tag.Key • Rules.Filter.And.Tags.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	• Date • Integer • Integer • String • 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 That Macie Classic Generates

Macie Classic Field Name	Macie Classic Field Type	Description	Example search query
`@timestamp`	Date	The timestamp when Macie Classic last analyzed the bucket.	Search for S3 buckets that Macie Classic analyzed in the last 24 hours: • **@timestamp:[now-1d TO now]**
`accountId`	String	The account ID of the S3 bucket owner.	Search for any S3 buckets that don't belong to a given 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 value indicating whether the S3 bucket is globally readable: `true`, `false`, or `unknown`. The `unknown` value indicates that Macie Classic can't determine whether the S3 bucket is globally readable.	Search for S3 buckets that are globally readable by either the Amazon S3 ACL or bucket (IAM) policy: • **s3_world_readability: "true"**
`s3_world_writability`	String	A value indicating if the S3 bucket is globally writable: `true`, `false`, or `unknown`. The `unknown` value indicates that Macie Classic can't determine whether the S3 bucket is globally writable.	Search for S3 buckets that is globally writable by either the Amazon 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 S3 objects that Macie Classic monitors.

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 dropdown.
3. For this sample procedure, select **Past 90** days in the third filter dropdown.
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 dataset is very large and you specify a very wide time range, your data might not render properly, and this graph might not appear 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 produces a subset of the results generated by your original selections in the preceding steps. Double-click any of the graph's results, and your selection is translated into a new query that automatically appears in the query parser, and the **Research** tab is refreshed with the results of this new query.
- **Search results summary** – A list of the most significant fields from your search. The first line includes the top (or bottom) three 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 produces a subset of the results generated by your original selections in the preceding steps. 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 translated into a new query that automatically appears 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. 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 Classic extracts from the Amazon S3 object API metadata. These are Macie Classic 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 Macie Classic generates 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, and `pii_types` describes any personal identifiable information contained in an S3 object.

S3 Object Data Fields That Macie Classic Extracts

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic 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 account ID for the Amazon Web Services account that owns the S3 object.	Search for S3 objects owned by a particular 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 Classic uses the S3 key field and parses out everything before the first '/', not including the bucket name.	`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**
`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**

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
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	DisplayName	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_encryption	ServerSideEncryption	get-object	String	The server side encryption used to encrypt an S3 object.	Search for objects that aren't encrypted with the AES256 standard: • **NOT filesystem.metadata.server_enc "AES256"**
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 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_ "arn:aws:kms:us-west-2: 110912345678:key/06f8b4fa-3 b60a56a9a1f2"**

Macie Classic Field Name	Amazon S3 API Field Name	Amazon S3 API Operation	Macie Classic Field Type	Description	Example Search Query
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"**
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 That Macie Classic Generates

Macie Classic Field Name	Macie Classic Field Type	Description	Example Search Query
`@timestamp`	Date	The timestamp when the S3 object was last modified.	Search for S3 objects classified by Macie Classic 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 Macie Classic console's **Settings** page.	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, an object monitored by Macie Classic is assigned risk levels based on each content type, file extension, theme, regex, 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 Classic console for their respective supported data classifiers.	Search for globally accessible (read or write) objects with the compound (final) risk level of 5 or higher: • **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.	Search for documents with the assigned file extension risk of greater than 6: • **filetype_risk: > 6**

Macie Classic Field Name	Macie Classic Field Type	Description	Example Search Query
		Note You can find risk levels in the **Settings** page of the Macie Classic console for their respective supported data classifiers.	
`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 Macie Classic console's **Settings** page.	Search for files with an extension of .pdf: • **filetypes: "Adobe PDF (.pdf)"**
`keyword_themes`	String	The themes assigned to an S3 object. You can find supported themes in the Macie Classic console's **Settings** page.	Search for S3 objects containing content related to Social Security: • **keyword_themes: "Social Security Keywords"**
`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 Macie Classic last analyzed an S3 object.	Search for S3 objects analyzed by Macie Classic in the last 24 hours: • **last_crawl_time: [now-1d/d TO now]**
`mimetype_risk`	Integer	The risk level based on an S3 object's content / MIME type.	Search for S3 objects containing MIME types associated with high-risk content: • **mimetype_risk: > 5**

Macie Classic Field Name	Macie Classic Field Type	Description	Example Search Query
`mimetypes`	String	The MIME type 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 PII severity impact of an S3 object, assigned by Macie Classic.	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 the regex, assigned by Macie Classic, of an S3 object.	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 themes, assigned by Macie Classic, of an S3 object.	Search for S3 objects with a theme-based risk level higher than 5: • **theme_risk: > 5**
`themes`	String	The combined themes of an S3 object.	Search for S3 objects containing RSA private keys: • **themes: "RSA Private Key"**

Disabling Amazon Macie Classic and Deleting Collected Metadata

Before you disable your Amazon Macie Classic account, you can optionally export your existing data classification results to an S3 bucket. If you're moving to the new Amazon Macie, we recommend that you do this before you disable Macie Classic and move to the new Amazon Macie. To learn how, see *Moving to the New Amazon Macie* (p. 3).

This topic explains how to disable Macie Classic without exporting your data classification results.

> **Important**
> Only a Macie Classic administrator account can disable Macie Classic. To disable Macie Classic for a member account, the administrator account must first disassociate the member account.

If you disable Macie Classic, it no longer has access to resources in the administrator account and all member accounts. In addition, you cannot re-enable Macie Classic. To start using Amazon Macie again after you disable your Macie Classic account, enable the new Amazon Macie for your account. For information about how to do this, see the Amazon Macie User Guide.

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

> **Important**
> Disabling Macie Classic doesn't prompt deletion of your data in your AWS services. After Macie Classic is disabled, only the metadata that was collected by Macie Classic while it monitored your accounts is deleted.

1. Sign in to the AWS Management Console and open the Amazon Macie console at https://console.aws.amazon.com/macie/.
2. By using the AWS Region selector in the upper-right corner of the page, switch to the Region in which you want to disable your Macie Classic account—**US East (N. Virginia)** or **US West (Oregon)**.
3. In the navigation pane, choose **Macie Classic**.

   If you don't see this link, choose your user name in the upper-right corner of the page, and then sign in to the Amazon Web Services account and role that you want to disable Macie Classic for.
4. In Macie Classic, navigate to the **general settings** page by choosing the down arrow next to your user name.
5. On the **general settings** page, review and select the following check boxes:

   - **I understand that if I disable Macie, the service will no longer have access to the resources in the administrator 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 administrator account and all member accounts. All metadata that Macie collected while monitoring the data in these accounts will be deleted.**
6. Choose **Disable Amazon Macie**.

Monitoring Amazon Macie Classic Alerts with Amazon CloudWatch Events

Amazon Macie Classic sends notifications based on CloudWatch Events when any change in Macie Classic alerts takes place. This includes newly generated alerts and updates to existing alerts. Notifications are sent for all Macie Classic alert types, including predictive alerts and basic alerts, both managed and custom. For more information about alert types, see Amazon Macie Classic Alerts (p. 53).

Macie Classic sends notifications based on CloudWatch Events for the alerts generated in both Macie Classic administrator and member accounts. However, only the Macie Classic administrator account has access to the generated events in CloudWatch Events. For more information about Macie Classic administrator and member accounts, see Concepts and Terminology (p. 12).

Event Format

The event for Macie Classic in CloudWatch Events has the following format. The fictional account ID `111122223333` represents the ID of the Macie Classic administrator 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}
```

```
  }
}
```

Configure CloudWatch Events

Complete the following procedure to configure your Macie Classic administrator account to receive events in CloudWatch Events from Macie Classic and pipe those events into an Amazon Simple Queue Service (Amazon SQS) queue.

Prerequisite

Create an Amazon SQS queue for the events from Macie Classic. For more information, see Tutorial: Creating an Amazon SQS Queue.

To configure CloudWatch events for your Macie Classic administrator account

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

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

4. In the **Targets** pane, choose **Add target**, select **SQS queue** in the target dropdown, and specify your queue for the events from Macie Classic.

Document History for Amazon Macie Classic

The following table describes important changes to the documentation for Amazon Macie Classic.

update-history-change	update-history-description	update-history-date
Policy updates (p. 101)	We added Amazon CloudWatch Logs actions to the AWS managed policy for the **AWSServiceRoleForAmazonMacie** service-linked role.	April 13, 2021
Updated content (p. 101)	We replaced the term *master account* with the term *administrator account*. An administrator account is used to centrally manage multiple accounts.	February 3, 2021
New content (p. 101)	Added content that explains how to move to the new version of Amazon Macie. Also, changed the name of this guide to *Amazon Macie Classic User Guide*.	May 13, 2020
New feature (p. 101)	Macie Classic can now use the service-linked role named **AWSServiceRoleForAmazonMacie**. This role allows Macie Classic to discover, classify, and protect sensitive data in AWS on your behalf.	June 28, 2018
New content (p. 101)	Added descriptions of data fields that can appear in the results of your data searches. For more information, see CloudTrail Data Fields, S3 Bucket Properties Data Fields, and S3 Objects Data Fields.	May 4, 2018
Initial release (p. 101)	Released this user guide for the first time.	August 14, 2017