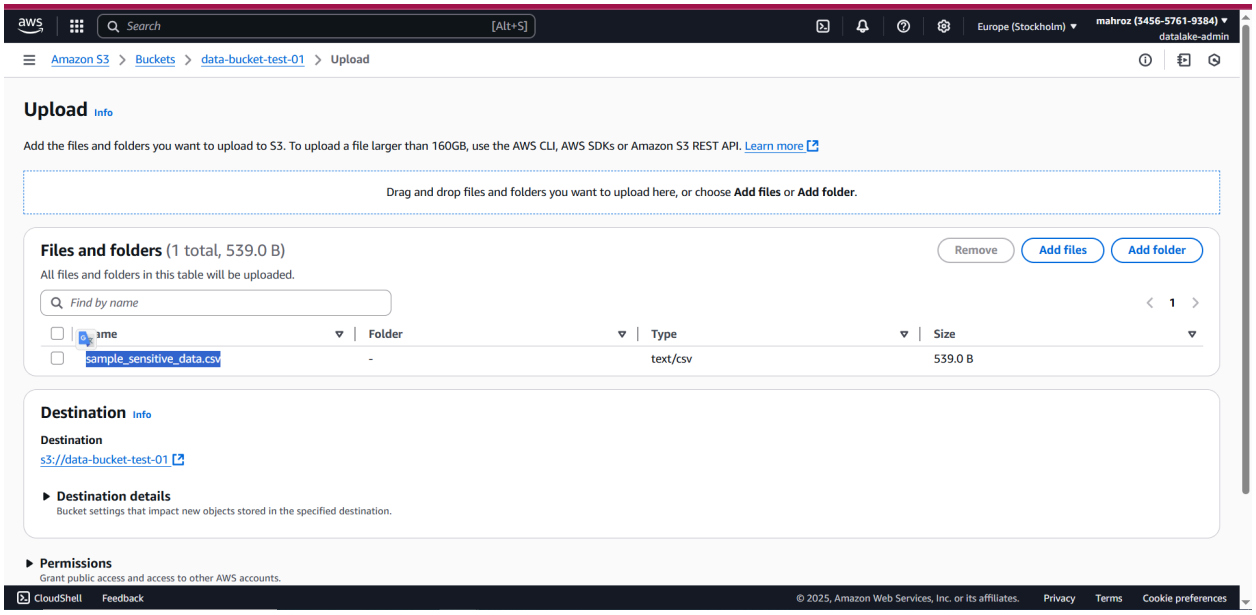
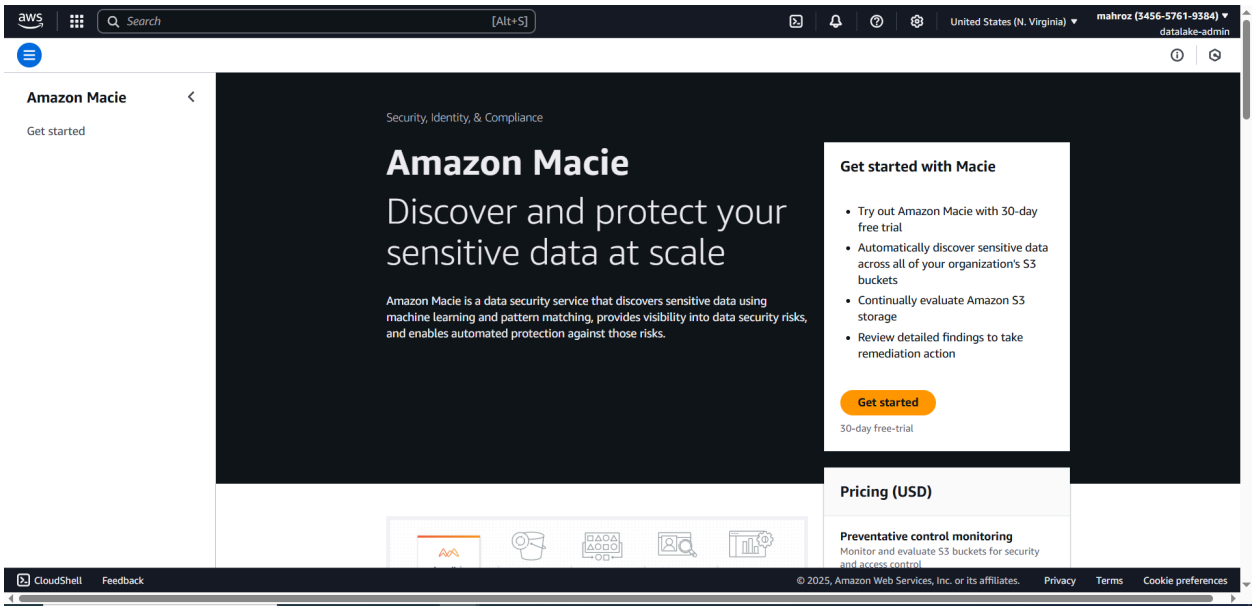
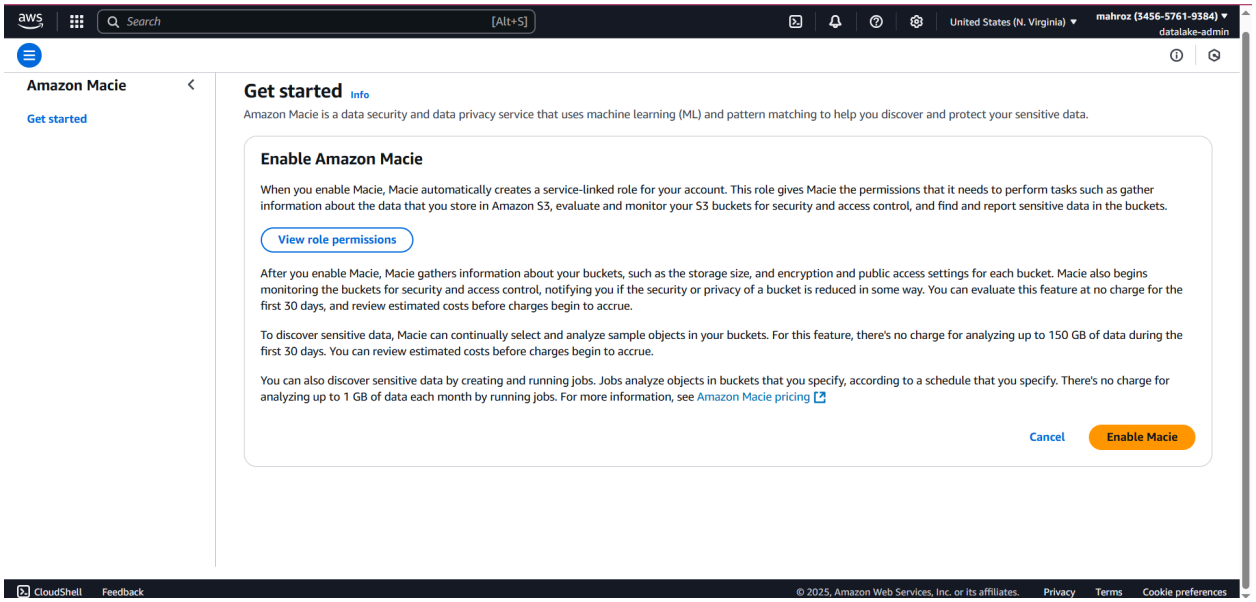
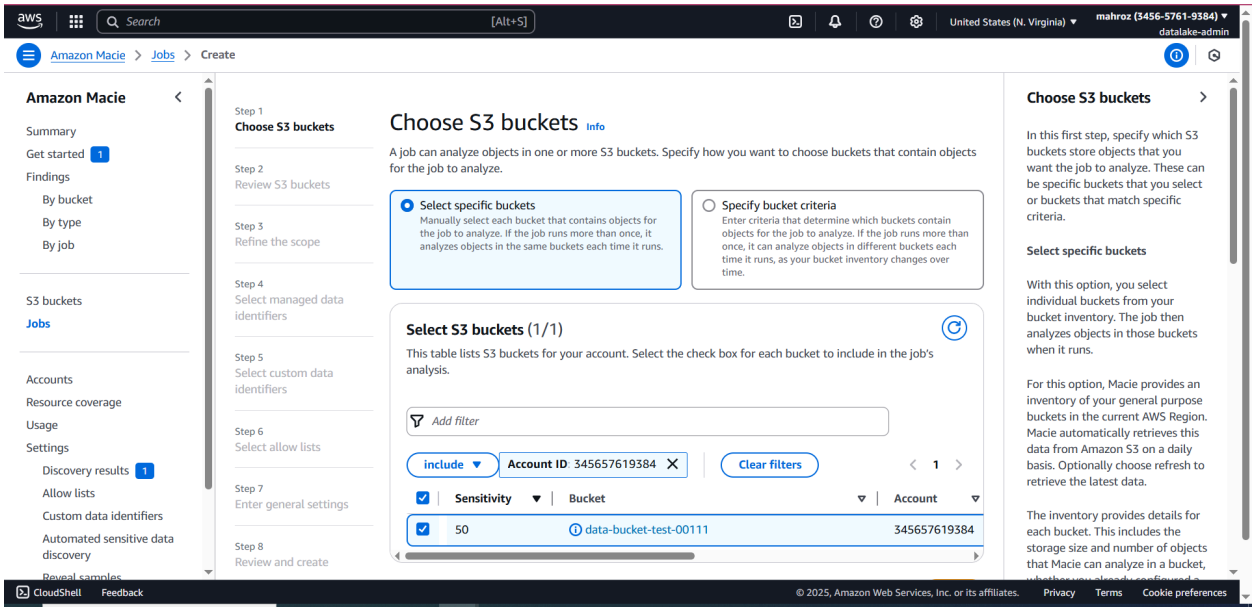
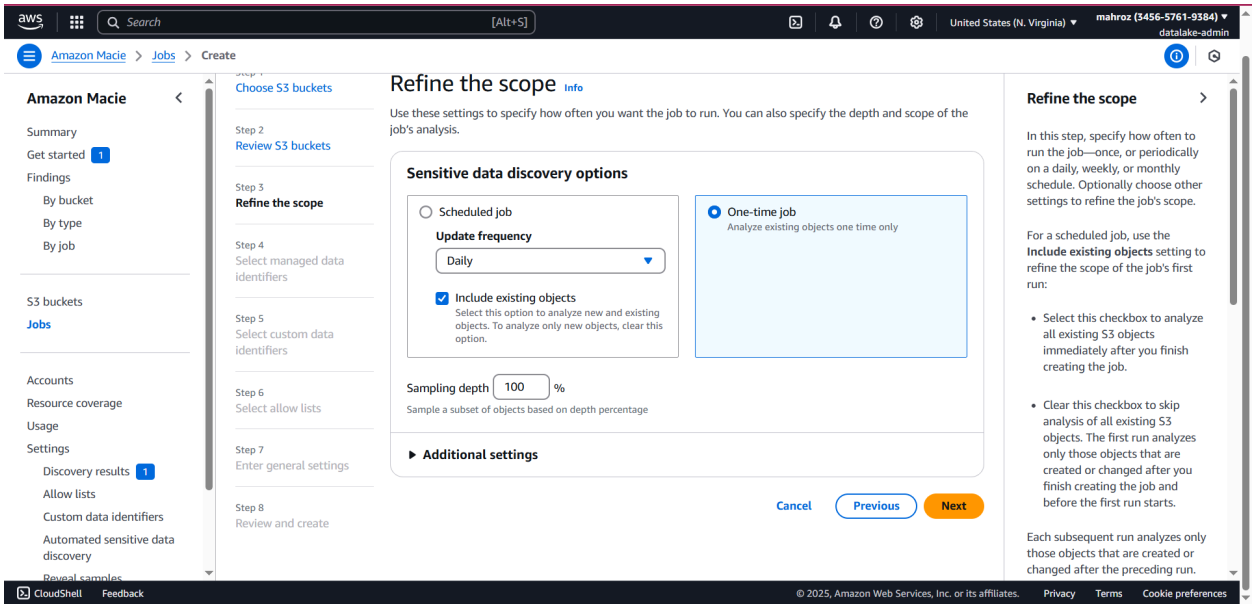
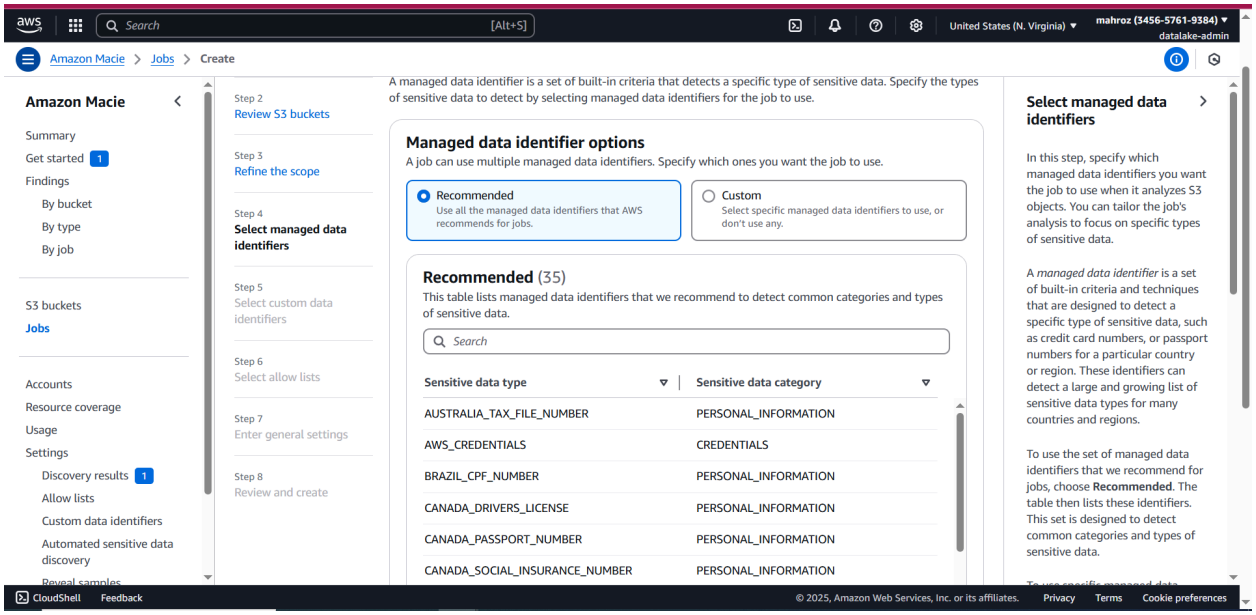

Search [Alt+S]
Europe (Stockholm)
mahroz (3456-5761-9384)
datalake-admin
Amazon S3 > Buckets > data-bucket-test-01 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 total, 539.0 B)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
Size
sample_sensitive_data.csv
-
text/csv
539.0 B
Destination Info
Destination
s3://data-bucket-test-01
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

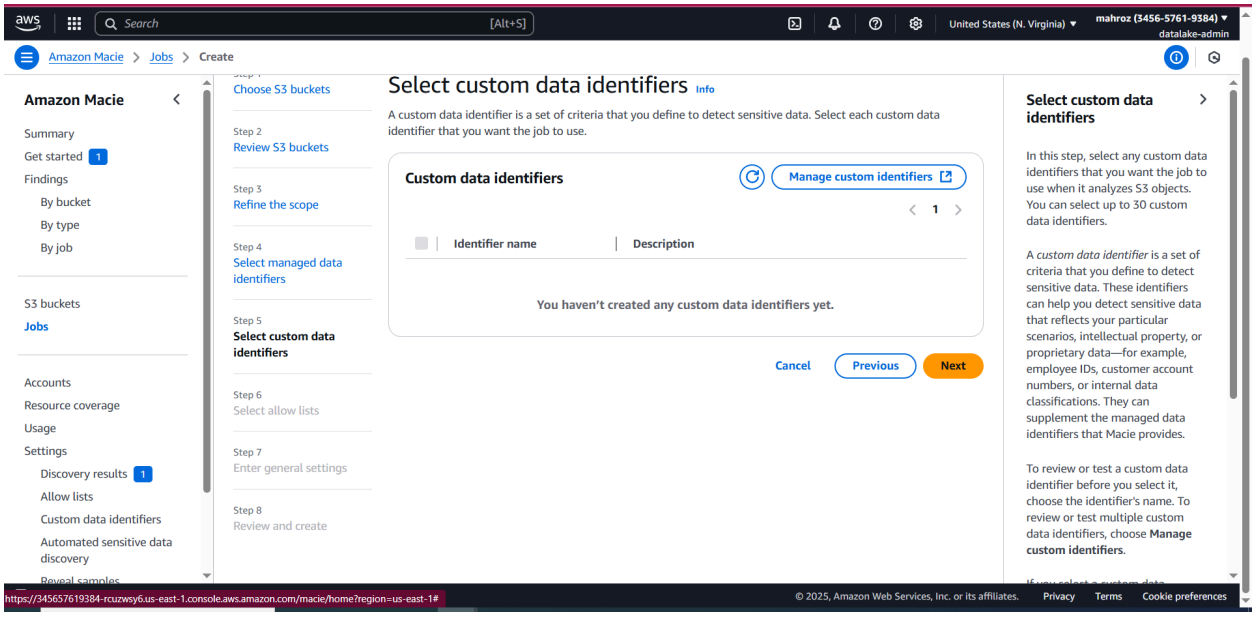

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie
Get started
Security, Identity, & Compliance
Amazon Macie
Discover and protect your sensitive data at scale
Amazon Macie is a data security service that discovers sensitive data using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks.
Get started with Macie
Try out Amazon Macie with 30-day free trial
Automatically discover sensitive data across all of your organization's S3 buckets
Continually evaluate Amazon S3 storage
Review detailed findings to take remediation action
Get started
30-day free-trial
Pricing (USD)
Preventative control monitoring
Monitor and evaluate S3 buckets for security and access control
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

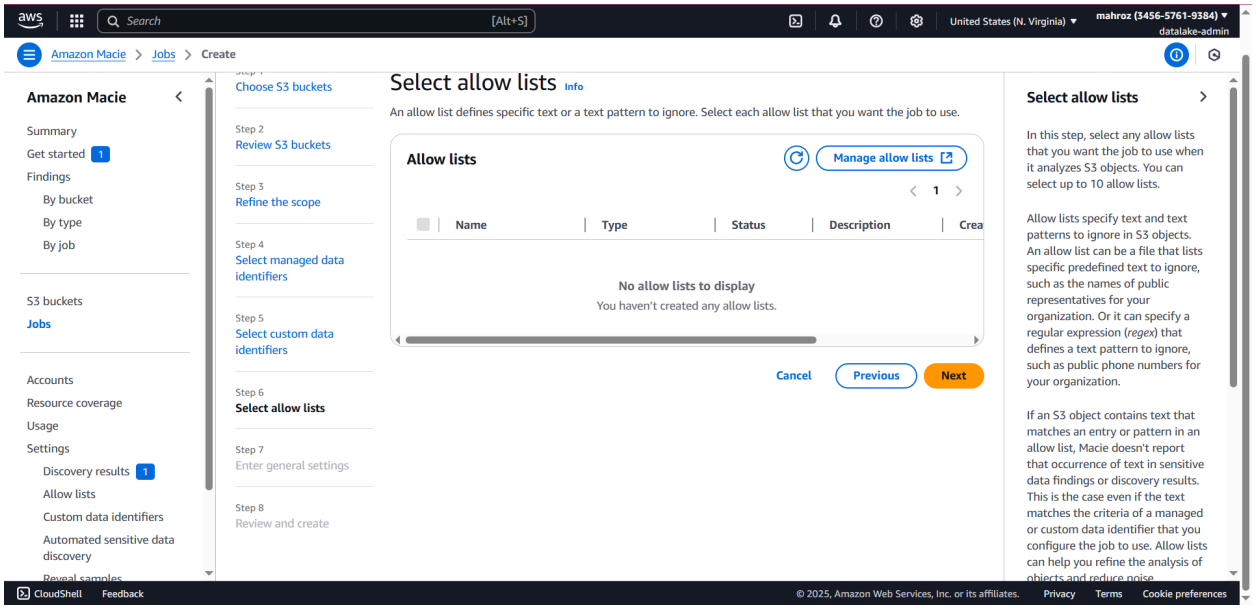

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie
Get started
Get started Info
Amazon Macie is a data security and data privacy service that uses machine learning (ML) and pattern matching to help you discover and protect your sensitive data.
Enable Amazon Macie
When you enable Macie, Macie automatically creates a service-linked role for your account. This role gives Macie the permissions that it needs to perform tasks such as gather information about the data that you store in Amazon S3, evaluate and monitor your S3 buckets for security and access control, and find and report sensitive data in the buckets.
View role permissions
After you enable Macie, Macie gathers information about your buckets, such as the storage size, and encryption and public access settings for each bucket. Macie also begins monitoring the buckets for security and access control, notifying you if the security or privacy of a bucket is reduced in some way. You can evaluate this feature at no charge for the first 30 days, and review estimated costs before charges begin to accrue.
To discover sensitive data, Macie can continually select and analyze sample objects in your buckets. For this feature, there's no charge for analyzing up to 150 GB of data during the first 30 days. You can review estimated costs before charges begin to accrue.
You can also discover sensitive data by creating and running jobs. Jobs analyze objects in buckets that you specify, according to a schedule that you specify. There's no charge for analyzing up to 1 GB of data each month by running jobs. For more information, see Amazon Macie pricing
Cancel
Enable Macie
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

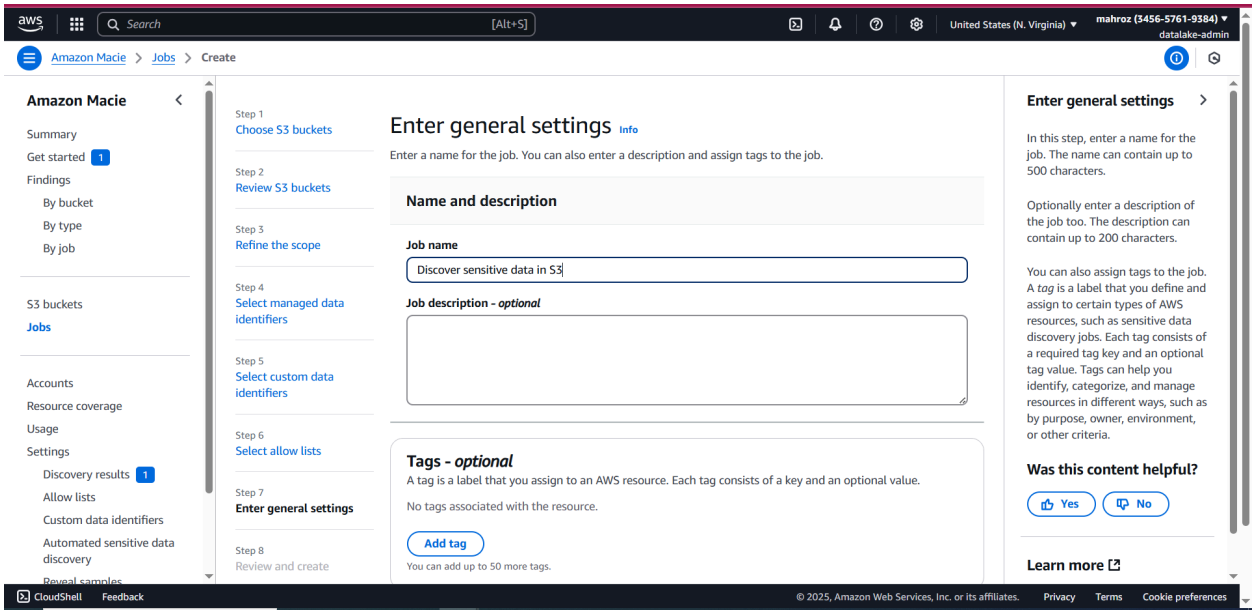

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs > Create
Amazon Macie
Summary
Get started 1
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Step 1 Choose S3 buckets
Step 2 Review S3 buckets
Step 3 Refine the scope
Step 4 Select managed data identifiers
Step 5 Select custom data identifiers
Step 6 Select allow lists
Step 7 Enter general settings
Step 8 Review and create
Choose S3 buckets Info
A job can analyze objects in one or more S3 buckets. Specify how you want to choose buckets that contain objects for the job to analyze.
Select specific buckets
Manually select each bucket that contains objects for the job to analyze. If the job runs more than once, it analyzes objects in the same buckets each time it runs.
Specify bucket criteria
Enter criteria that determine which buckets contain objects for the job to analyze. If the job runs more than once, it can analyze objects in different buckets each time it runs, as your bucket inventory changes over time.
Select S3 buckets (1/1)
This table lists S3 buckets for your account. Select the check box for each bucket to include in the job's analysis.
Add filter
include
Account ID: 345657619384
Clear filters
1
Sensitivity
Bucket
Account
50
data-bucket-test-00111
345657619384
Choose S3 buckets
In this first step, specify which S3 buckets store objects that you want the job to analyze. These can be specific buckets that you select or buckets that match specific criteria.
Select specific buckets
With this option, you select individual buckets from your bucket inventory. The job then analyzes objects in those buckets when it runs.
For this option, Macie provides an inventory of your general purpose buckets in the current AWS Region. Macie automatically retrieves this data from Amazon S3 on a daily basis. Optionally choose refresh to retrieve the latest data.
The inventory provides details for each bucket. This includes the storage size and number of objects that Macie can analyze in a bucket,
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

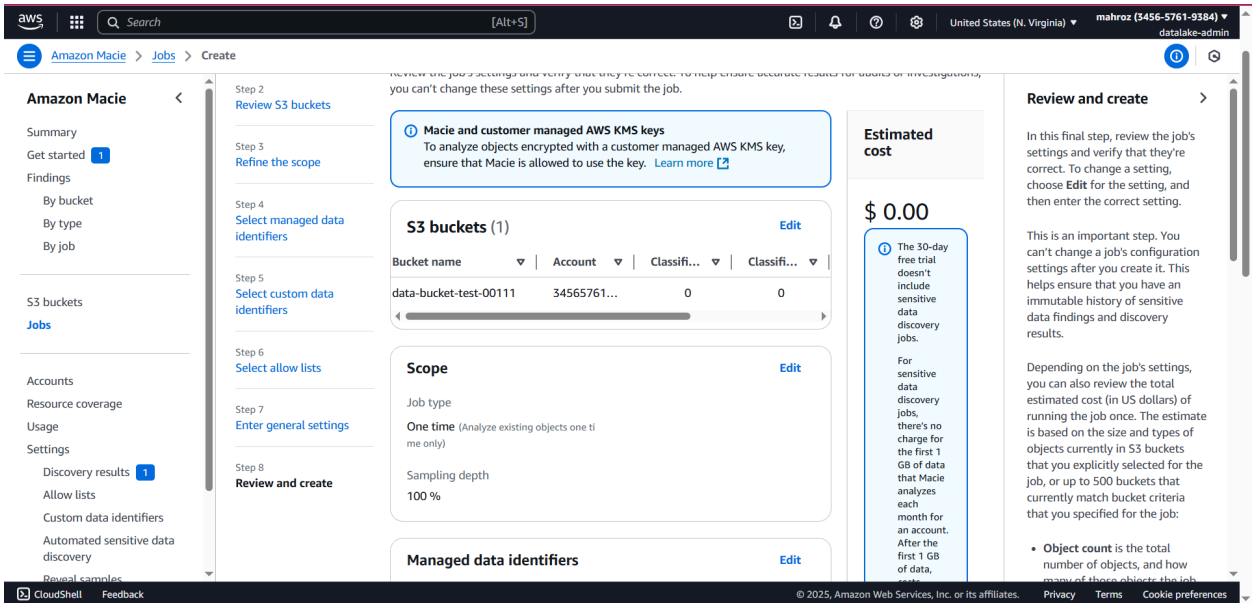

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs > Create
Amazon Macie
Summary
Get started 1
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Reveal samples
Step 1 Choose S3 buckets
Step 2 Review S3 buckets
Step 3 Refine the scope
Step 4 Select managed data identifiers
Step 5 Select custom data identifiers
Step 6 Select allow lists
Step 7 Enter general settings
Step 8 Review and create
Refine the scope Info
Use these settings to specify how often you want the job to run. You can also specify the depth and scope of the job's analysis.
Sensitive data discovery options
Scheduled job
Update frequency
Daily
Include existing objects
Select this option to analyze new and existing objects. To analyze only new objects, clear this option.
One-time job
Analyze existing objects one time only
Sampling depth 100 %
Sample a subset of objects based on depth percentage
Additional settings
Cancel Previous Next
Refine the scope
In this step, specify how often to run the job—once, or periodically on a daily, weekly, or monthly schedule. Optionally choose other settings to refine the job's scope.
For a scheduled job, use the Include existing objects setting to refine the scope of the job's first run:
Select this checkbox to analyze all existing S3 objects immediately after you finish creating the job.
Clear this checkbox to skip analysis of all existing S3 objects. The first run analyzes only those objects that are created or changed after you finish creating the job and before the first run starts.
Each subsequent run analyzes only those objects that are created or changed after the preceding run.
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

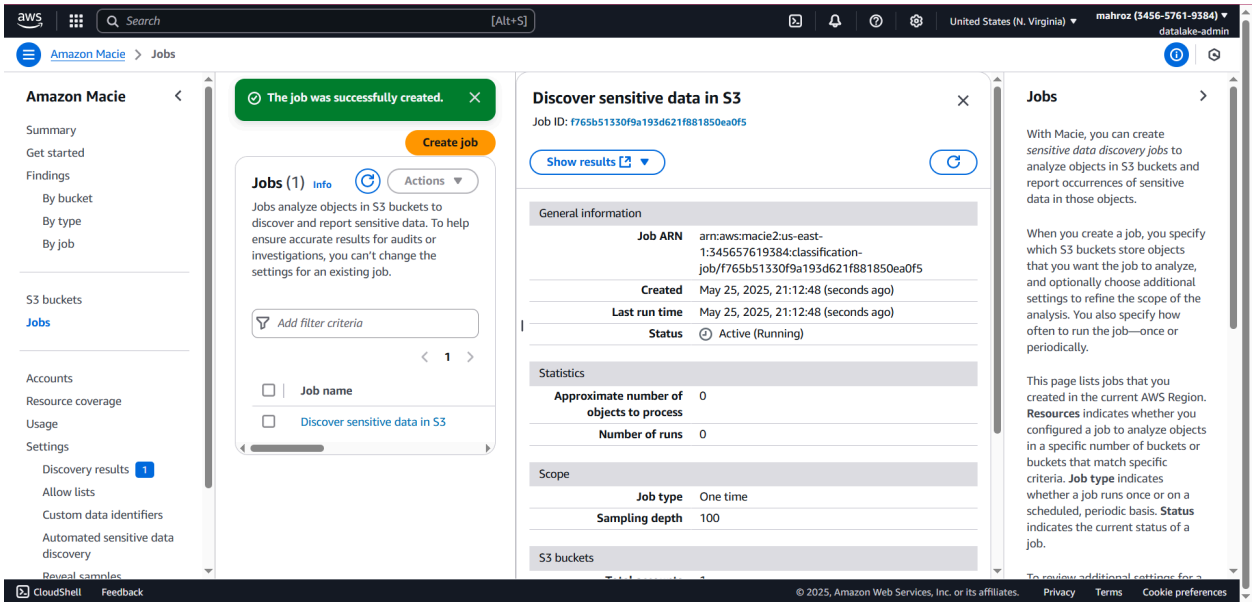

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs > Create
Amazon Macie
Summary
Get started 1
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Reveal samples
Step 2 Review S3 buckets
Step 3 Refine the scope
Step 4 Select managed data identifiers
Step 5 Select custom data identifiers
Step 6 Select allow lists
Step 7 Enter general settings
Step 8 Review and create
A managed data identifier is a set of built-in criteria that detects a specific type of sensitive data. Specify the types of sensitive data to detect by selecting managed data identifiers for the job to use.
Managed data identifier options
A job can use multiple managed data identifiers. Specify which ones you want the job to use.
Recommended
Use all the managed data identifiers that AWS recommends for jobs.
Custom
Select specific managed data identifiers to use, or don't use any.
Recommended (35)
This table lists managed data identifiers that we recommend to detect common categories and types of sensitive data.
Search
Sensitive data type
Sensitive data category
AUSTRALIA_TAX_FILE_NUMBER PERSONAL_INFORMATION
AWS_CREDENTIALS CREDENTIALS
BRAZIL_CPF_NUMBER PERSONAL_INFORMATION
CANADA_DRIVERS_LICENSE PERSONAL_INFORMATION
CANADA_PASSPORT_NUMBER PERSONAL_INFORMATION
CANADA_SOCIAL_INSURANCE_NUMBER PERSONAL_INFORMATION
Select managed data identifiers
In this step, specify which managed data identifiers you want the job to use when it analyzes S3 objects. You can tailor the job's analysis to focus on specific types of sensitive data.
A managed data identifier is a set of built-in criteria and techniques that are designed to detect a specific type of sensitive data, such as credit card numbers, or passport numbers for a particular country or region. These identifiers can detect a large and growing list of sensitive data types for many countries and regions.
To use the set of managed data identifiers that we recommend for jobs, choose Recommended. The table then lists these identifiers. This set is designed to detect common categories and types of sensitive data.
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

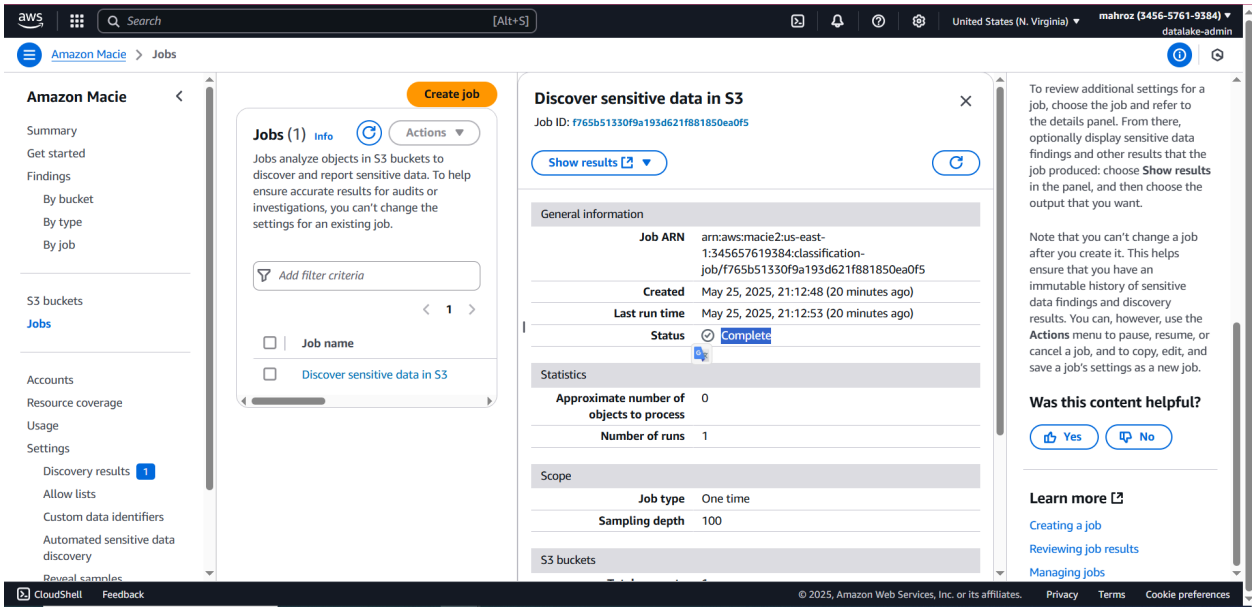

aws
Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs > Create
Amazon Macie
Summary
Get started 1
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Reveal samples
Choose S3 buckets
Step 2
Review S3 buckets
Step 3
Refine the scope
Step 4
Select managed data identifiers
Step 5
Select custom data identifiers
Step 6
Select allow lists
Step 7
Enter general settings
Step 8
Review and create
Select custom data identifiers Info
A custom data identifier is a set of criteria that you define to detect sensitive data. Select each custom data identifier that you want the job to use.
Custom data identifiers
Manage custom identifiers
1
Identifier name
Description
You haven't created any custom data identifiers yet.
Cancel
Previous
Next
Select custom data identifiers
In this step, select any custom data identifiers that you want the job to use when it analyzes S3 objects. You can select up to 30 custom data identifiers.
A custom data identifier is a set of criteria that you define to detect sensitive data. These identifiers can help you detect sensitive data that reflects your particular scenarios, intellectual property, or proprietary data—for example, employee IDs, customer account numbers, or internal data classifications. They can supplement the managed data identifiers that Macie provides.
To review or test a custom data identifier before you select it, choose the identifier's name. To review or test multiple custom data identifiers, choose Manage custom identifiers.
https://345657619384-rcuzwsy6.us-east-1.console.aws.amazon.com/macie/home?region=us-east-1#
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

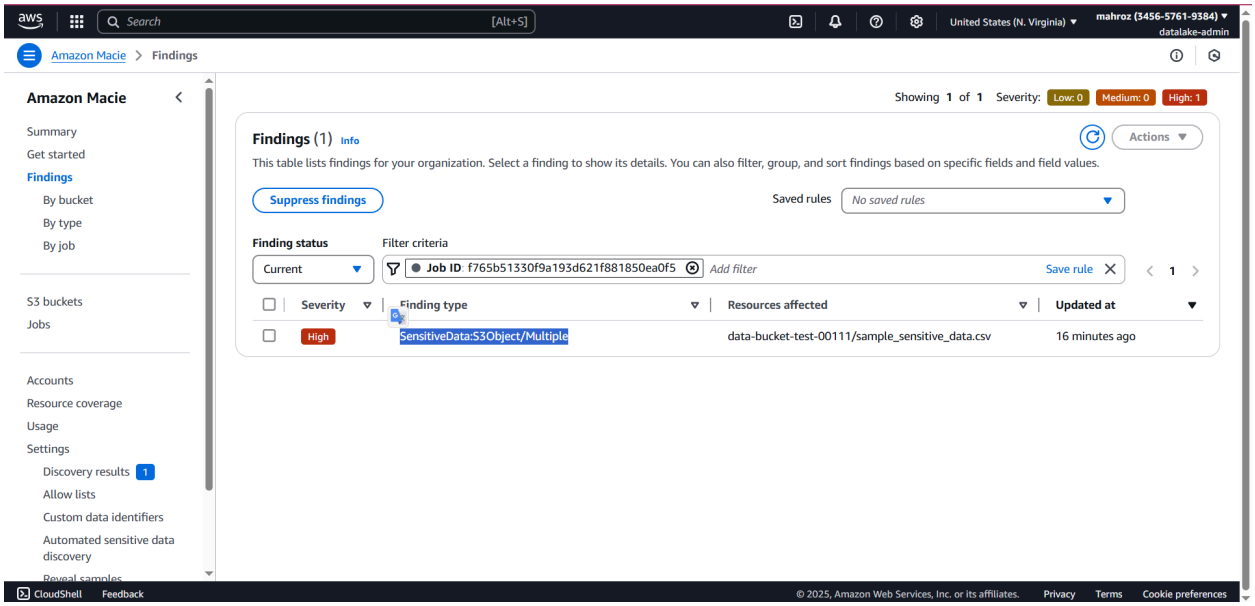

aws
Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs > Create
Amazon Macie
Summary
Get started 1
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Reveal samples
Choose S3 buckets
Step 2
Review S3 buckets
Step 3
Refine the scope
Step 4
Select managed data identifiers
Step 5
Select custom data identifiers
Step 6
Select allow lists
Step 7
Enter general settings
Step 8
Review and create
Select allow lists Info
An allow list defines specific text or a text pattern to ignore. Select each allow list that you want the job to use.
Allow lists
Manage allow lists
1
Name
Type
Status
Description
Crea
No allow lists to display
You haven't created any allow lists.
Cancel
Previous
Next
Select allow lists
In this step, select any allow lists that you want the job to use when it analyzes S3 objects. You can select up to 10 allow lists.
Allow lists specify text and text patterns to ignore in S3 objects. An allow list can be a file that lists specific predefined text to ignore, such as the names of public representatives for your organization. Or it can specify a regular expression (regex) that defines a text pattern to ignore, such as public phone numbers for your organization.
If an S3 object contains text that matches an entry or pattern in an allow list, Macie doesn't report that occurrence of text in sensitive data findings or discovery results. This is the case even if the text matches the criteria of a managed or custom data identifier that you configure the job to use. Allow lists can help you refine the analysis of objects and reduce noise.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

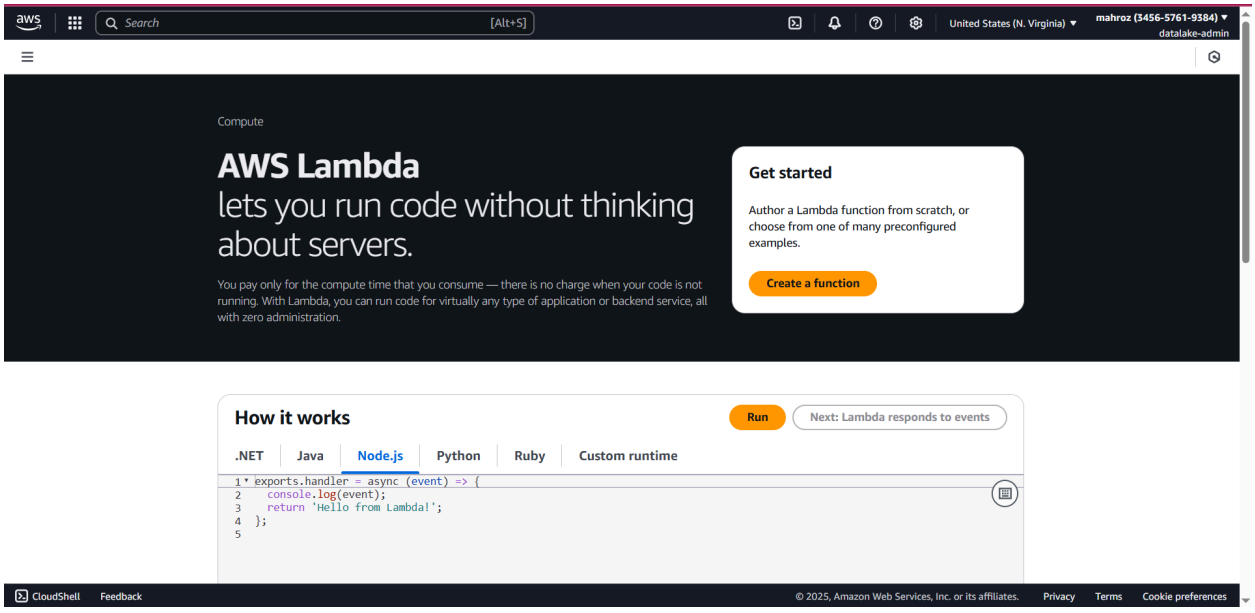

aws
Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs > Create
Amazon Macie
Summary
Get started 1
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Step 1 Choose S3 buckets
Step 2 Review S3 buckets
Step 3 Refine the scope
Step 4 Select managed data identifiers
Step 5 Select custom data identifiers
Step 6 Select allow lists
Step 7 Enter general settings
Step 8 Review and create
Enter general settings Info
Enter a name for the job. You can also enter a description and assign tags to the job.
Name and description
Job name
Discover sensitive data in S3
Job description - optional
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value.
No tags associated with the resource.
Add tag
You can add up to 50 more tags.
Enter general settings
In this step, enter a name for the job. The name can contain up to 500 characters.
Optionally enter a description of the job too. The description can contain up to 200 characters.
You can also assign tags to the job. A tag is a label that you define and assign to certain types of AWS resources, such as sensitive data discovery jobs. Each tag consists of a required tag key and an optional tag value. Tags can help you identify, categorize, and manage resources in different ways, such as by purpose, owner, environment, or other criteria.
Was this content helpful?
Yes
No
Learn more
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

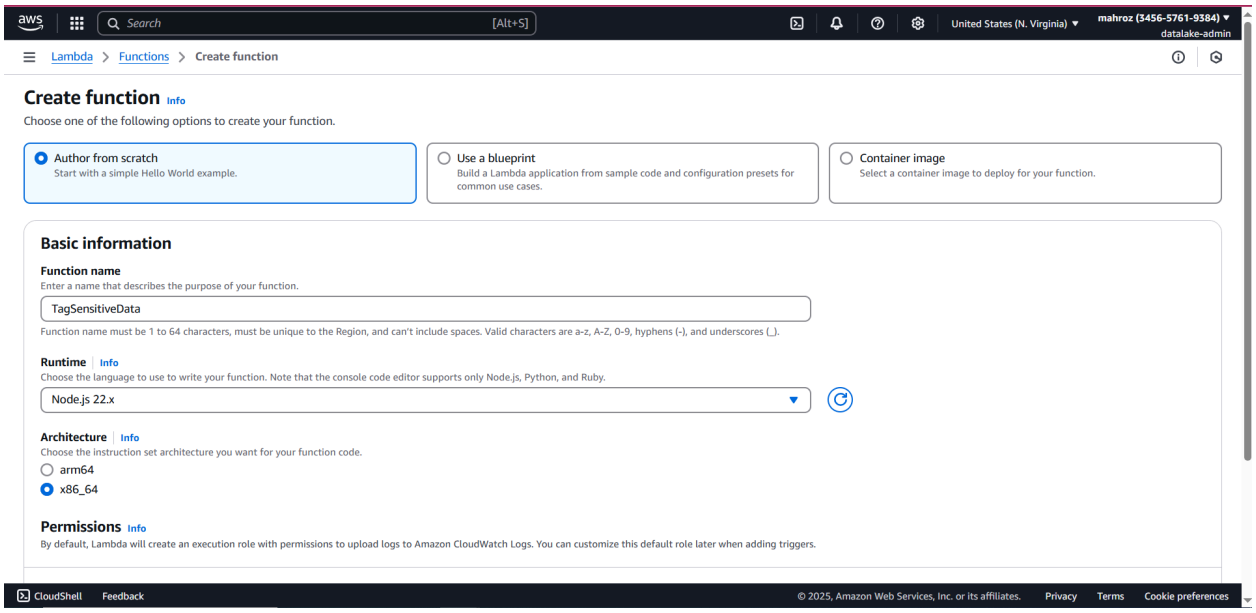

aws
Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs > Create
Amazon Macie
Summary
Get started 1
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Step 2 Review S3 buckets
Step 3 Refine the scope
Step 4 Select managed data identifiers
Step 5 Select custom data identifiers
Step 6 Select allow lists
Step 7 Enter general settings
Step 8 Review and create
you can't change these settings after you submit the job.
Macie and customer managed AWS KMS keys
To analyze objects encrypted with a customer managed AWS KMS key, ensure that Macie is allowed to use the key. Learn more
S3 buckets (1)
Edit
Bucket name
Account
Classifi...
Classifi...
data-bucket-test-00111
34565761...
0
0
Scope
Edit
Job type
One time (Analyze existing objects one time only)
Sampling depth
100 %
Managed data identifiers
Edit
Estimated cost
$ 0.00
The 30-day free trial doesn't include sensitive data discovery jobs.
For sensitive data discovery jobs, there's no charge for the first 1 GB of data that Macie analyzes each month for an account. After the first 1 GB of data,
Review and create
In this final step, review the job's settings and verify that they're correct. To change a setting, choose Edit for the setting, and then enter the correct setting.
This is an important step. You can't change a job's configuration settings after you create it. This helps ensure that you have an immutable history of sensitive data findings and discovery results.
Depending on the job's settings, you can also review the total estimated cost (in US dollars) of running the job once. The estimate is based on the size and types of objects currently in S3 buckets that you explicitly selected for the job, or up to 500 buckets that currently match bucket criteria that you specified for the job:
Object count is the total number of objects, and how
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

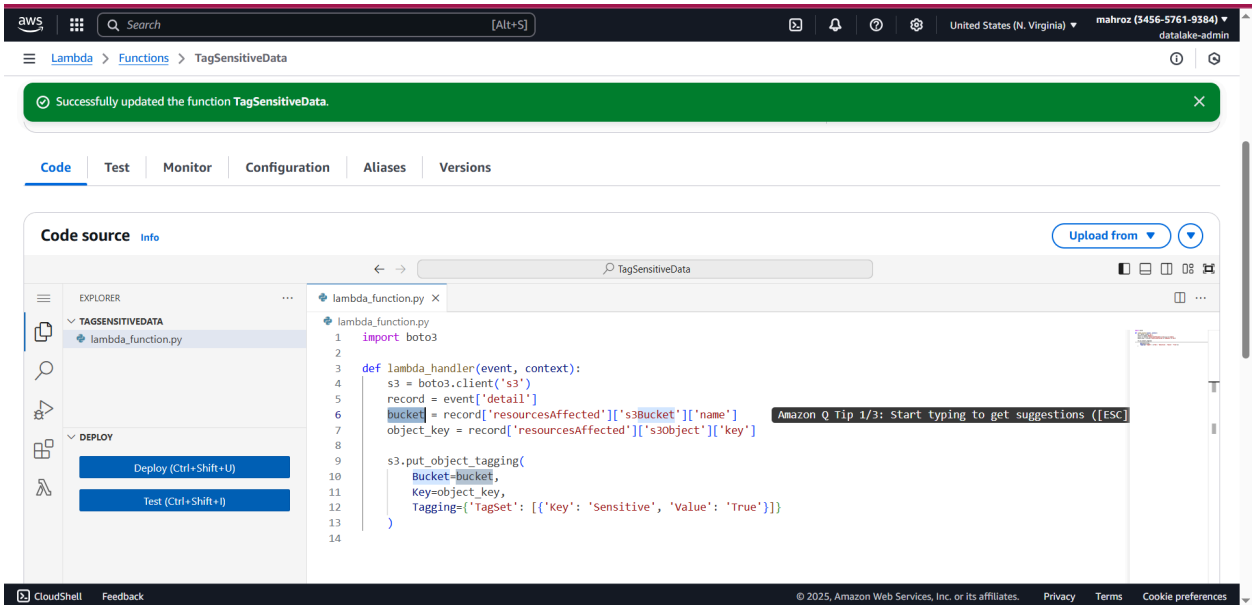

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs
Amazon Macie
Summary
Get started
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
The job was successfully created.
Create job
Jobs (1) Info
Actions
Jobs analyze objects in S3 buckets to discover and report sensitive data. To help ensure accurate results for audits or investigations, you can't change the settings for an existing job.
Add filter criteria
Job name
Discover sensitive data in S3
Discover sensitive data in S3
Job ID: f765b51330f9a193d621f881850ea0f5
Show results
General information
Job ARN arn:aws:macie2:us-east-1:345657619384:classification-job/f765b51330f9a193d621f881850ea0f5
Created May 25, 2025, 21:12:48 (seconds ago)
Last run time May 25, 2025, 21:12:48 (seconds ago)
Status Active (Running)
Statistics
Approximate number of objects to process 0
Number of runs 0
Scope
Job type One time
Sampling depth 100
S3 buckets
Jobs
With Macie, you can create sensitive data discovery jobs to analyze objects in S3 buckets and report occurrences of sensitive data in those objects.
When you create a job, you specify which S3 buckets store objects that you want the job to analyze, and optionally choose additional settings to refine the scope of the analysis. You also specify how often to run the job—once or periodically.
This page lists jobs that you created in the current AWS Region. Resources indicates whether you configured a job to analyze objects in a specific number of buckets or buckets that match specific criteria. Job type indicates whether a job runs once or on a scheduled, periodic basis. Status indicates the current status of a job.
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

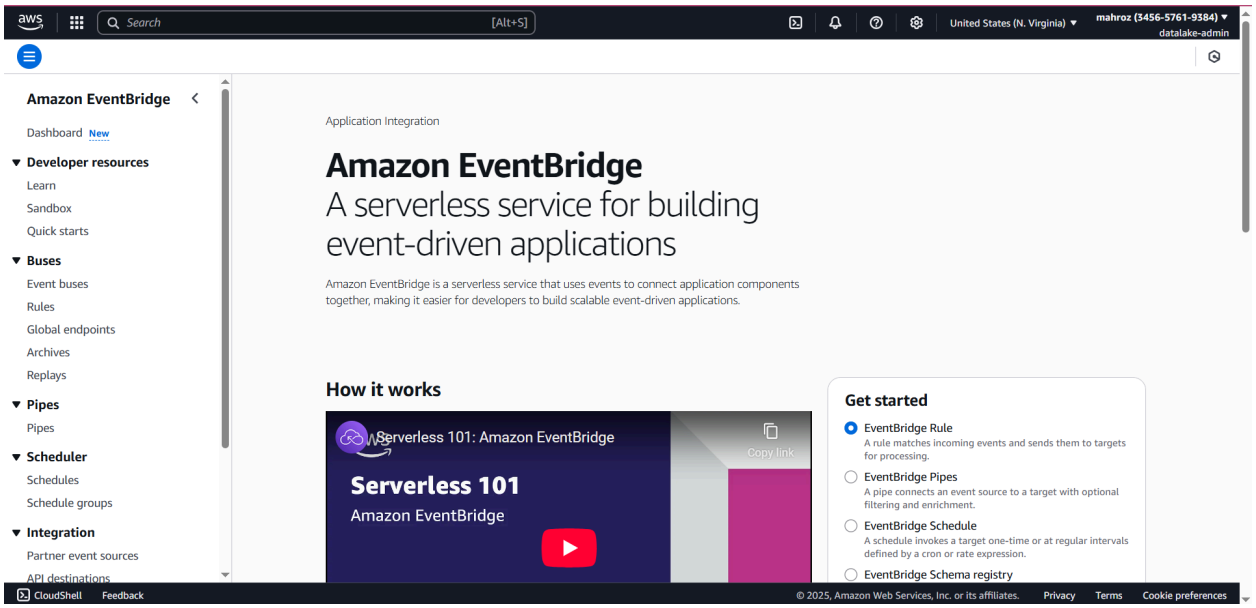

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie > Jobs
Amazon Macie
Summary
Get started
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Create job
Jobs (1) Info
Actions
Jobs analyze objects in S3 buckets to discover and report sensitive data. To help ensure accurate results for audits or investigations, you can't change the settings for an existing job.
Add filter criteria
Job name
Discover sensitive data in S3
Discover sensitive data in S3
Job ID: f765b51330f9a193d621f881850ea0f5
Show results
General information
Job ARN arn:aws:macie2:us-east-1:345657619384:classification-job/f765b51330f9a193d621f881850ea0f5
Created May 25, 2025, 21:12:48 (20 minutes ago)
Last run time May 25, 2025, 21:12:53 (20 minutes ago)
Status Complete
Statistics
Approximate number of objects to process 0
Number of runs 1
Scope
Job type One time
Sampling depth 100
S3 buckets
To review additional settings for a job, choose the job and refer to the details panel. From there, optionally display sensitive data findings and other results that the job produced: choose Show results in the panel, and then choose the output that you want.
Note that you can't change a job after you create it. This helps ensure that you have an immutable history of sensitive data findings and discovery results. You can, however, use the Actions menu to pause, resume, or cancel a job, and to copy, edit, and save a job's settings as a new job.
Was this content helpful?
Yes
No
Learn more
Creating a job
Reviewing job results
Managing jobs
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

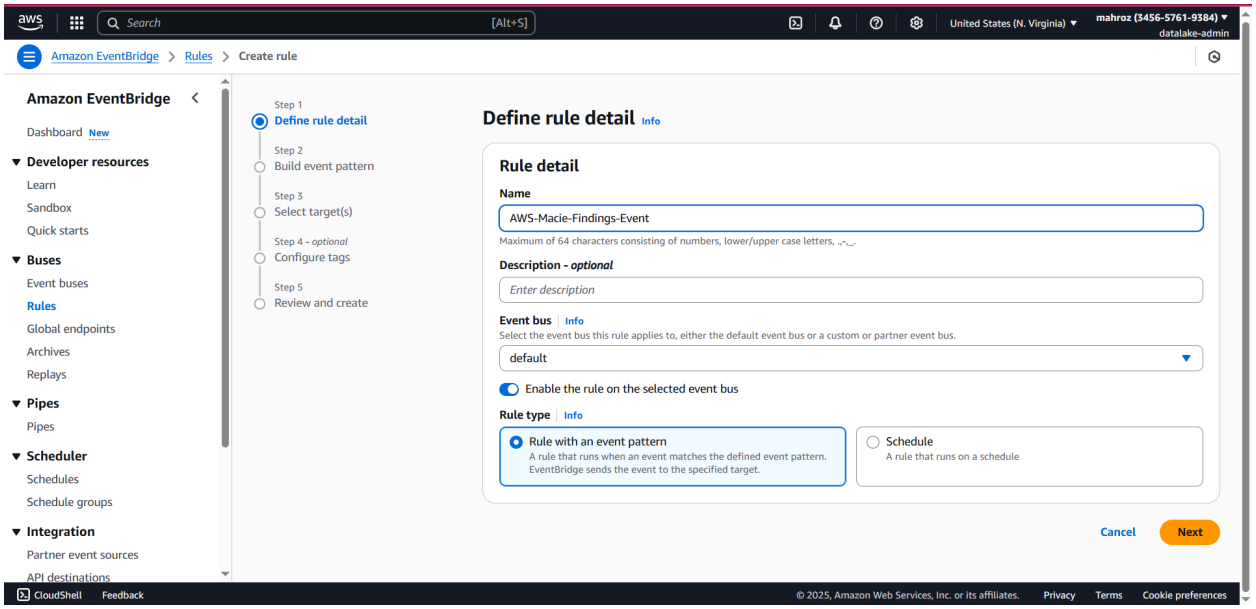

Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon Macie
Findings
Amazon Macie
Summary
Get started
Findings
By bucket
By type
By job
S3 buckets
Jobs
Accounts
Resource coverage
Usage
Settings
Discovery results 1
Allow lists
Custom data identifiers
Automated sensitive data discovery
Showing 1 of 1
Severity: Low: 0 Medium: 0 High: 1
Findings (1) Info
This table lists findings for your organization. Select a finding to show its details. You can also filter, group, and sort findings based on specific fields and field values.
Actions
Suppress findings
Saved rules
No saved rules
Finding status
Filter criteria
Current
Job ID: f765b51330f9a193d621f881850ea0f5
Add filter
Save rule
Severity
Finding type
Resources affected
Updated at
High
SensitiveData:S3Object/Multiple
data-bucket-test-00111/sample_sensitive_data.csv
16 minutes ago
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

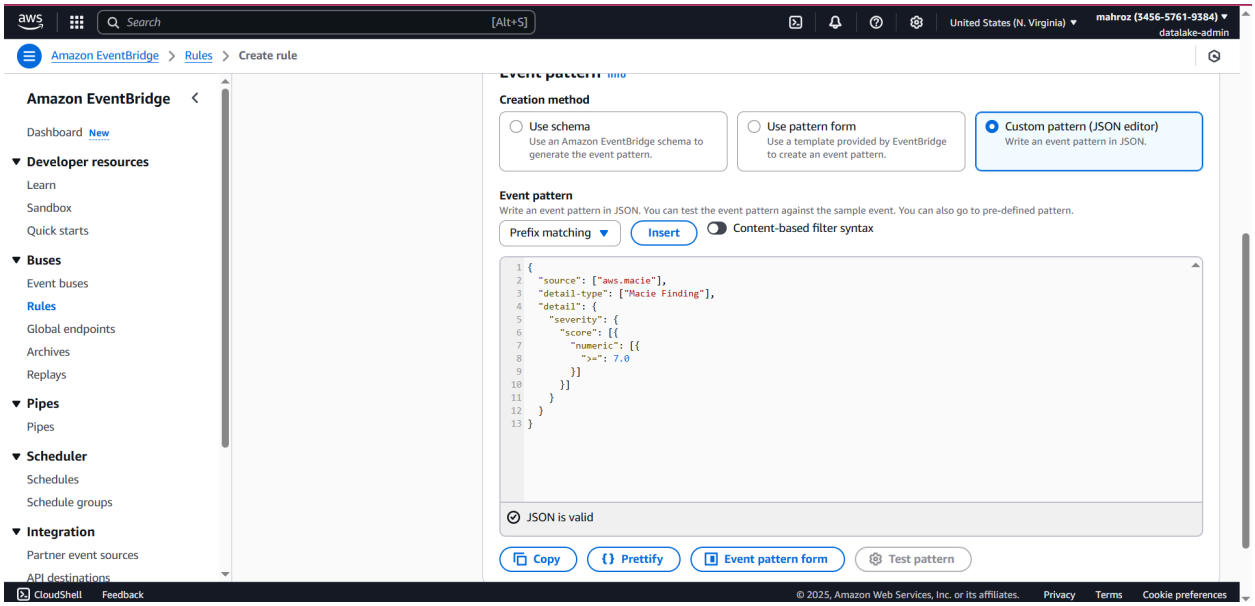

Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Compute
AWS Lambda
lets you run code without thinking about servers.
You pay only for the compute time that you consume — there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service, all with zero administration.
Get started
Author a Lambda function from scratch, or choose from one of many preconfigured examples.
Create a function
How it works
Run
Next: Lambda responds to events
.NET
Java
Node.js
Python
Ruby
Custom runtime
exports.handler = async (event) => {
console.log(event);
return 'Hello from Lambda!';
};
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

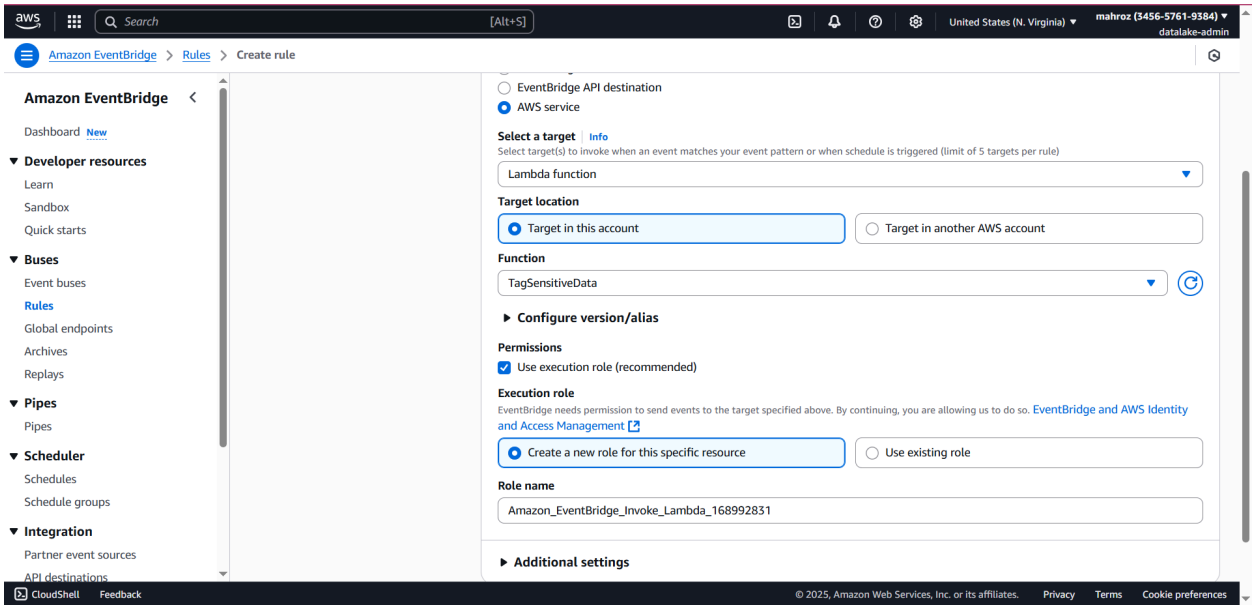

aws
Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Lambda > Functions > Create function
Create function Info
Choose one of the following options to create your function.
Author from scratch
Start with a simple Hello World example.
Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.
Container image
Select a container image to deploy for your function.
Basic information
Function name
Enter a name that describes the purpose of your function.
TagSensitiveData
Function name must be 1 to 64 characters, must be unique to the Region, and can't include spaces. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (_).
Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Node.js 22.x
Architecture Info
Choose the instruction set architecture you want for your function code.
arm64
x86_64
Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

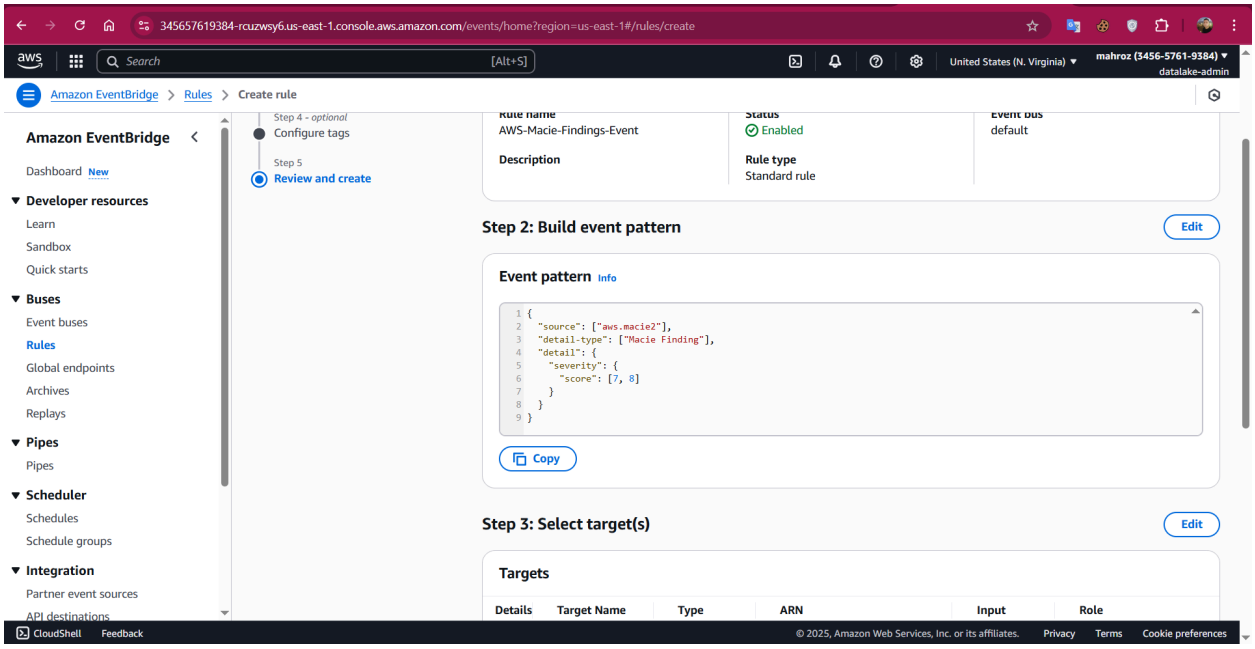

aws
Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Lambda > Functions > TagSensitiveData
Successfully updated the function TagSensitiveData.
Code
Test
Monitor
Configuration
Aliases
Versions
Code source Info
Upload from
TagSensitiveData
EXPLORER
TAGSENSITIVEDATA
lambda_function.py
DEPLOY
Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)
lambda_function.py
import boto3
def lambda_handler(event, context):
s3 = boto3.client('s3')
record = event['detail']
bucket = record['resourcesAffected']['s3Bucket']['name']
object_key = record['resourcesAffected']['s3Object']['key']
s3.put_object_tagging(
Bucket=bucket,
Key=object_key,
Tagging={'TagSet': [{'Key': 'Sensitive', 'Value': 'True'}]}
)
Amazon Q Tip 1/3: Start typing to get suggestions ([ESC]
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

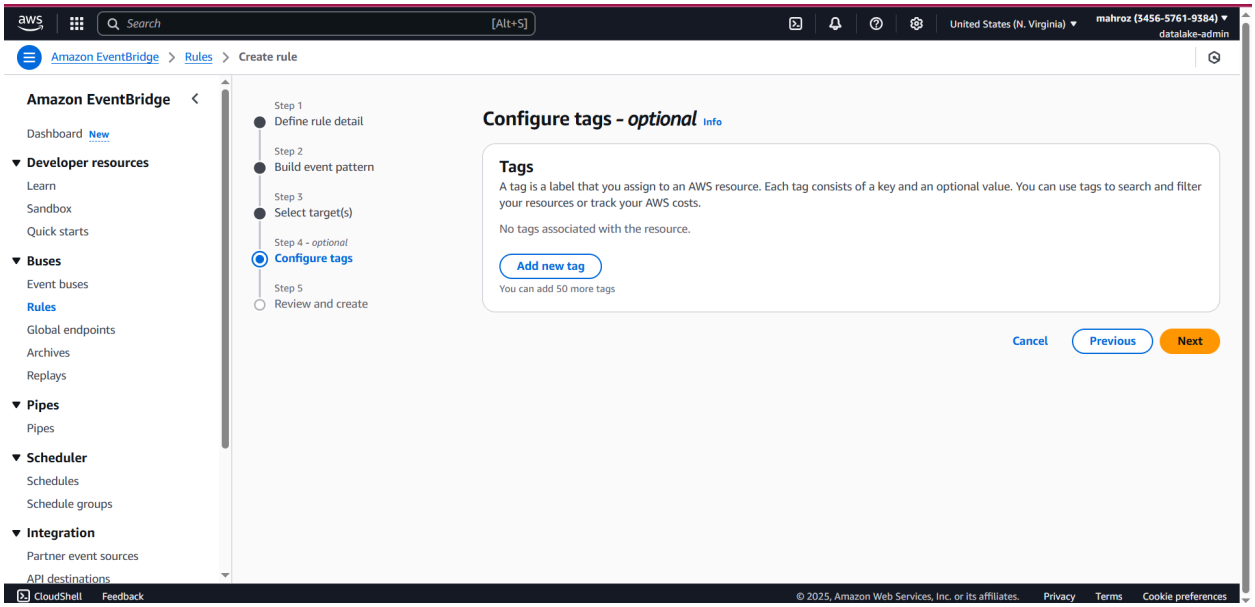

Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Application Integration
Amazon EventBridge
A serverless service for building event-driven applications
Amazon EventBridge is a serverless service that uses events to connect application components together, making it easier for developers to build scalable event-driven applications.
How it works
Serverless 101: Amazon EventBridge
Serverless 101
Amazon EventBridge
Copy link
Get started
EventBridge Rule
A rule matches incoming events and sends them to targets for processing.
EventBridge Pipes
A pipe connects an event source to a target with optional filtering and enrichment.
EventBridge Schedule
A schedule invokes a target one-time or at regular intervals defined by a cron or rate expression.
EventBridge Schema registry
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

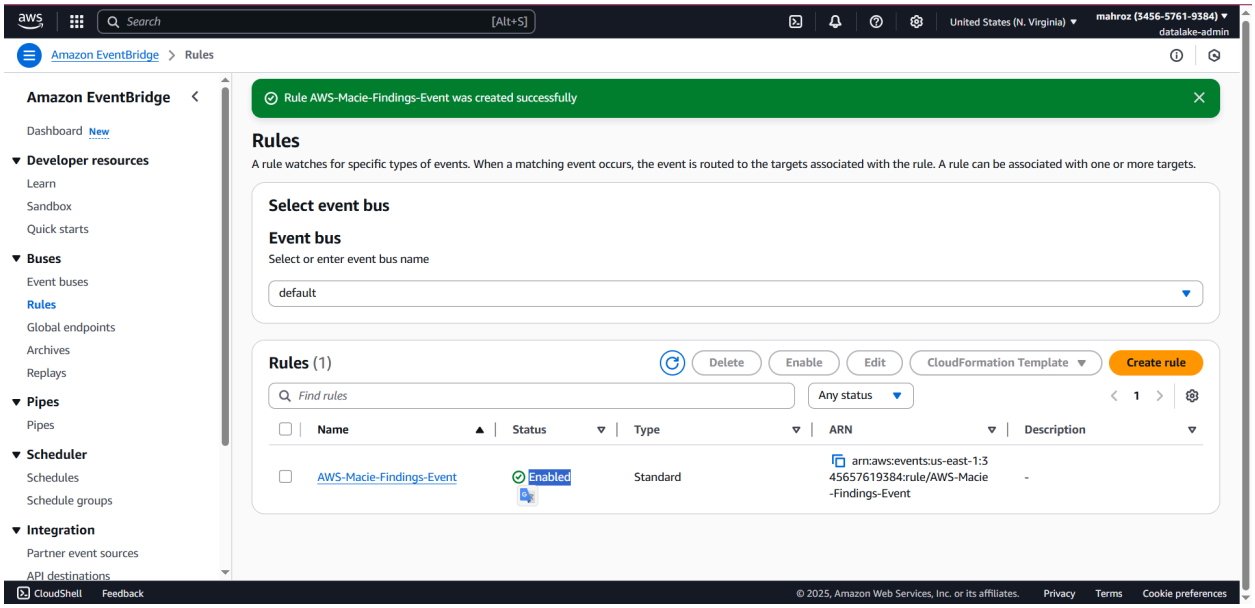

Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Step 1
Define rule detail
Step 2
Build event pattern
Step 3
Select target(s)
Step 4 - optional
Configure tags
Step 5
Review and create
Define rule detail Info
Rule detail
Name
AWS-Macie-Findings-Event
Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.
Description - optional
Enter description
Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default
Enable the rule on the selected event bus
Rule type Info
Rule with an event pattern
A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
Schedule
A rule that runs on a schedule
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Creation method
Use schema
Use an Amazon EventBridge schema to generate the event pattern.
Use pattern form
Use a template provided by EventBridge to create an event pattern.
Custom pattern (JSON editor)
Write an event pattern in JSON.
Event pattern
Write an event pattern in JSON. You can test the event pattern against the sample event. You can also go to pre-defined pattern.
Prefix matching
Insert
Content-based filter syntax
{
"source": ["aws.macie"],
"detail-type": ["Macie Finding"],
"detail": {
"severity": {
"score": [{
"numeric": [{
">=": 7.0
}]
}]
}
}
}
JSON is valid
Copy
Prettify
Event pattern form
Test pattern
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

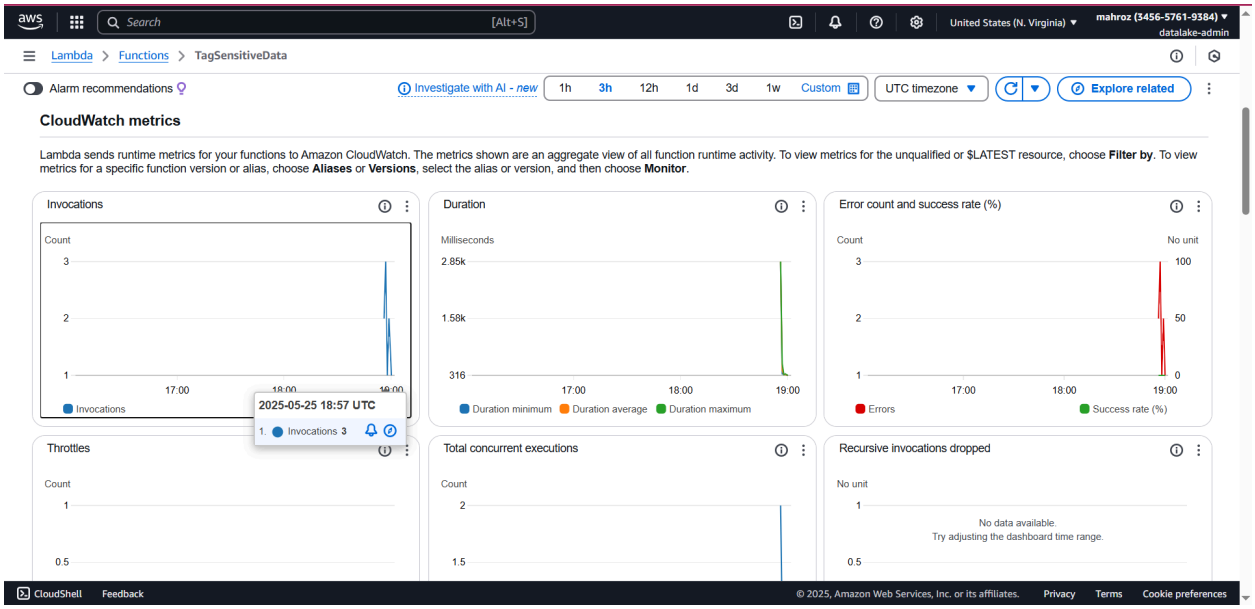

Search [Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
EventBridge API destination
AWS service
Select a target Info
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)
Lambda function
Target location
Target in this account
Target in another AWS account
Function
TagSensitiveData
Configure version/alias
Permissions
Use execution role (recommended)
Execution role
EventBridge needs permission to send events to the target specified above. By continuing, you are allowing us to do so. EventBridge and AWS Identity and Access Management
Create a new role for this specific resource
Use existing role
Role name
Amazon_EventBridge_Invoke_Lambda_168992831
Additional settings
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


345657619384-rcuzwsy6.us-east-1.console.aws.amazon.com/events/home?region=us-east-1#/rules/create
Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Step 4 - optional
Configure tags
Step 5
Review and create
Rule name
AWS-Macie-Findings-Event
Status
Enabled
Event bus
default
Description
Rule type
Standard rule
Step 2: Build event pattern
Edit
Event pattern Info
{
"source": ["aws.macie2"],
"detail-type": ["Macie Finding"],
"detail": {
"severity": {
"score": [7, 8]
}
}
}
Copy
Step 3: Select target(s)
Edit
Targets
Details
Target Name
Type
ARN
Input
Role
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)
mahroz (3456-5761-9384)
datalake-admin
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Step 1
Define rule detail
Step 2
Build event pattern
Step 3
Select target(s)
Step 4 - optional
Configure tags
Step 5
Review and create
Configure tags - optional Info
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
No tags associated with the resource.
Add new tag
You can add 50 more tags
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Event Bridge Successfully Trigger the Lambda Function



Lambda function successfully marked the data with TAG sensitive