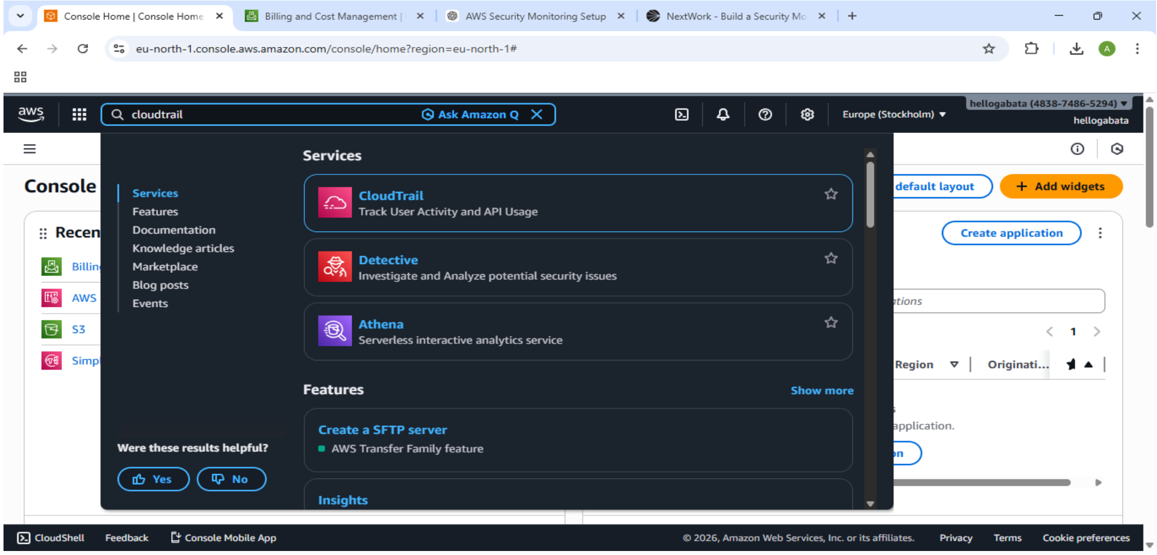
ABDULAKEEM AKINPELUMI MUHAMMED 2ND SEMESTER PROJECT REPORT

ALT/SOE/025/3504



Services

CloudTrail
Track User Activity and API Usage

Detective
Investigate and Analyze potential security issues

Athena
Serverless interactive analytics service

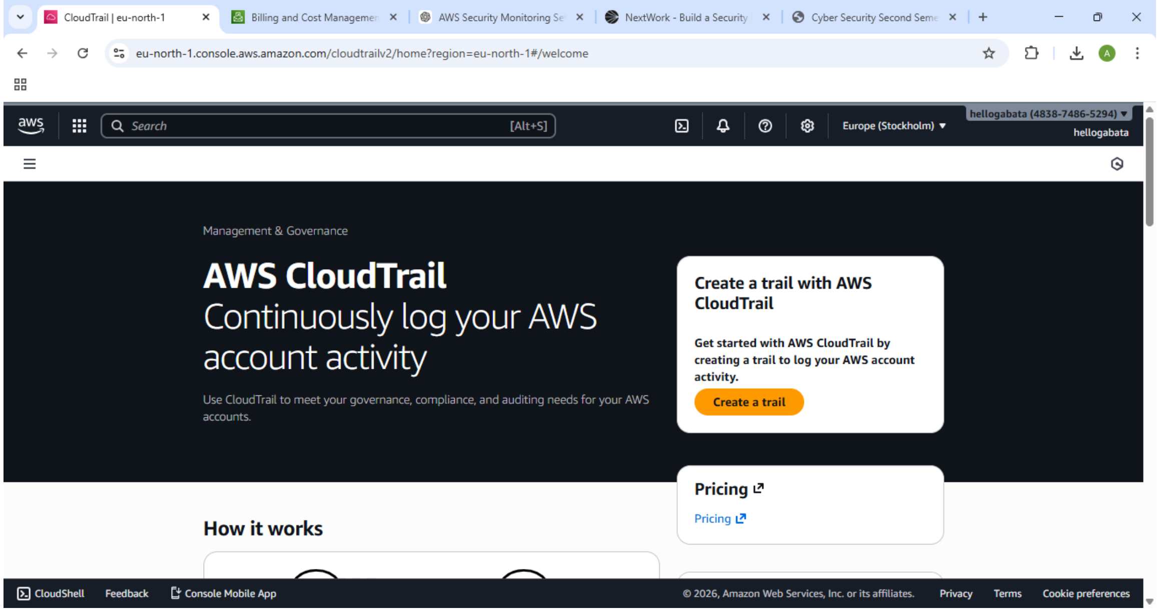
Features

Create a SFTP server
AWS Transfer Family feature

Insights

Task 1.1 — Create Multi-Region CloudTrail + CloudWatch Logs

Open AWS Console and search for **CloudTrail,** after that click on it and create a Trail.


CloudTrail | eu-north-1
Billing and Cost Managemen
AWS Security Monitoring Se
NextWork - Build a Security
Cyber Security Second Seme
eu-north-1.console.aws.amazon.com/cloudtrailv2/home?region=eu-north-1#/welcome
Search
[Alt+S]
Europe (Stockholm)
hellogabata (4838-7486-5294)
hellogabata
Create a trail
Pricing
Pricing
How it works
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

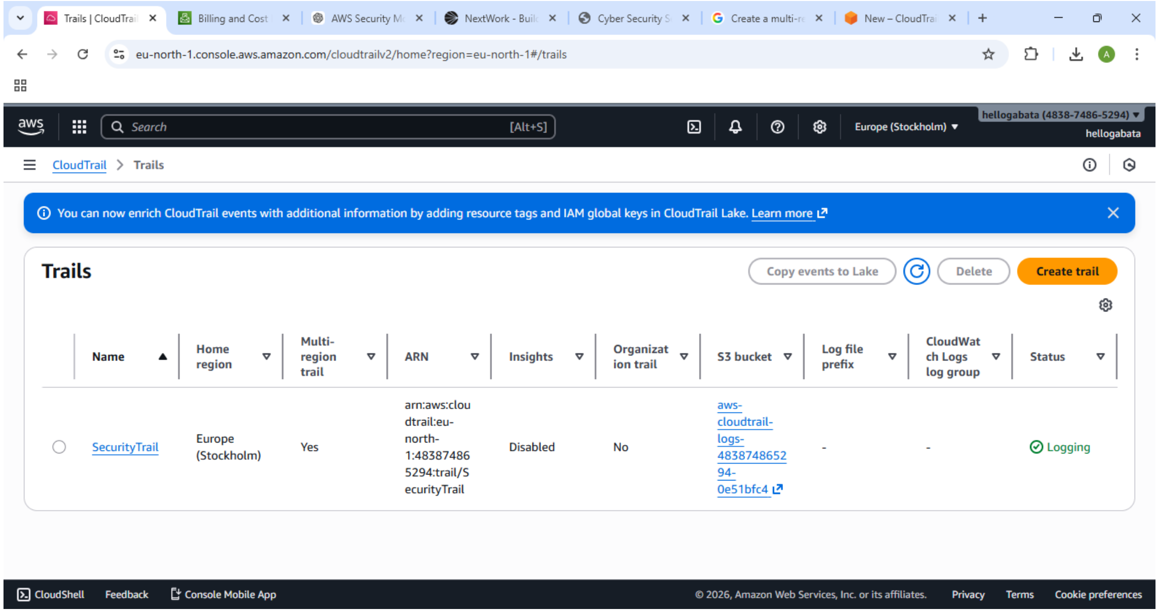
Management & Governance

AWS CloudTrail
Continuously log your AWS account activity

Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

Get started with AWS CloudTrail by creating a trail to log your AWS account activity.

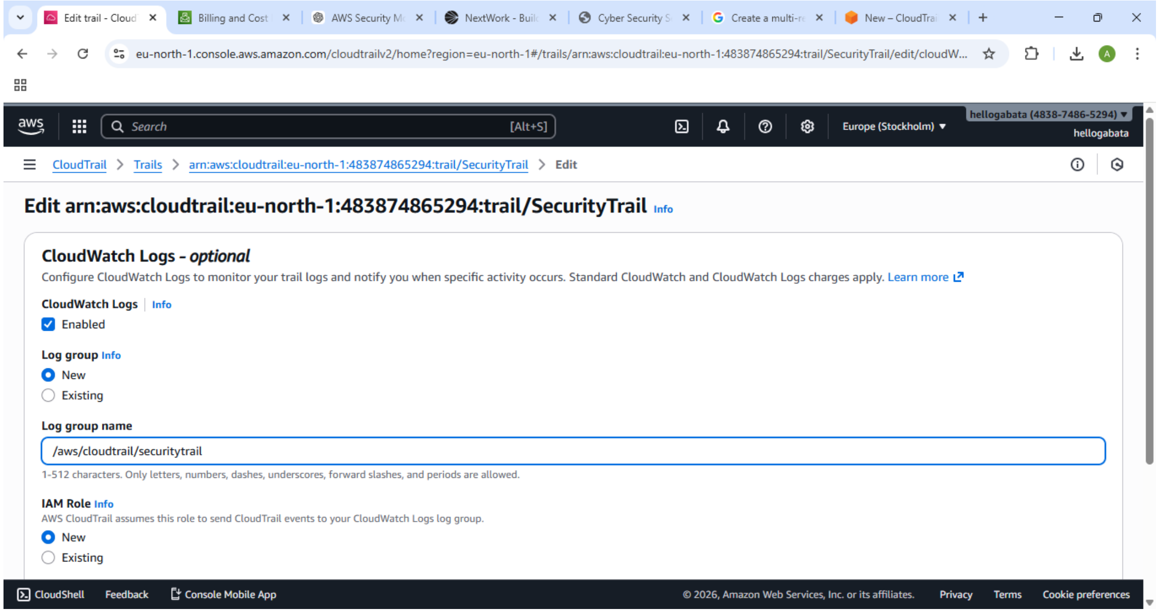


You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more

Trails

	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	SecurityTrail	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail	Disabled	No	aws-cloudtrail-logs-483874865294-0e51bfc4	-	-	✓ Logging

After creating the CloudTrail, you need to configure CloudWatch Logs Group. Click on the Trail you just created to configure the settings below


Edit trail - Cloud
Billing and Cost
AWS Security M
NextWork - Buil
Cyber Security S
Create a multi-r
New – CloudTrai
eu-north-1.console.aws.amazon.com/cloudtrailv2/home?region=eu-north-1#/trails/arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail/edit/cloudW...
Search
[Alt+S]
Europe (Stockholm) ▾
hellogabata (4838-7486-5294) ▾
hellogabata
CloudTrail > Trails > arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail > Edit
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail Info

CloudWatch Logs - *optional*

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. Learn more

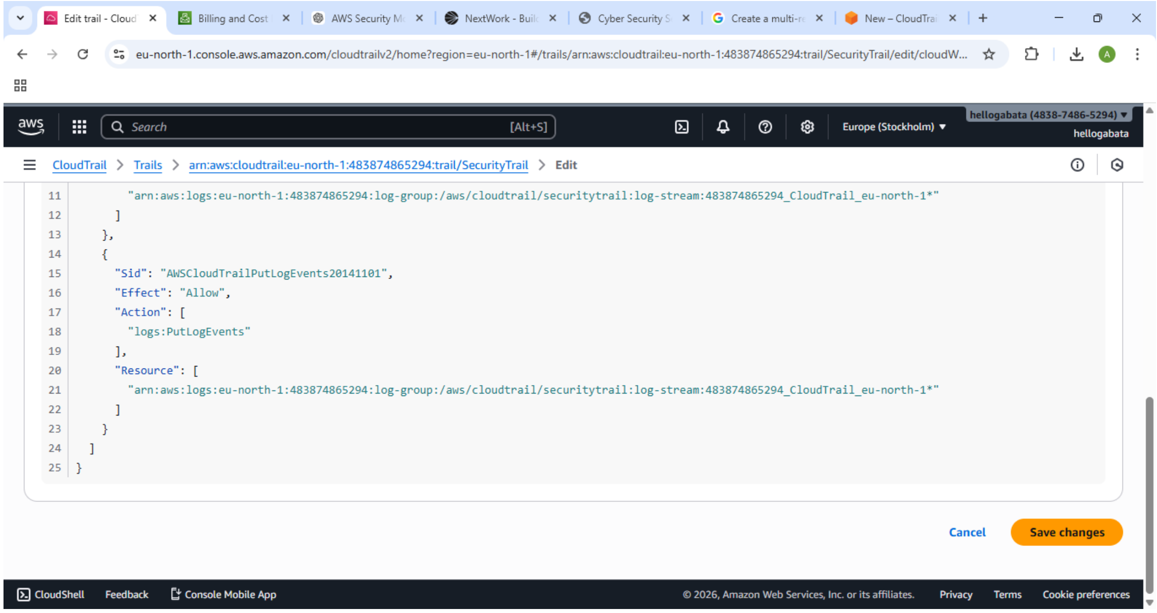
CloudWatch Logs | Info
☑ Enabled

Log group Info
● New
○ Existing

Log group name
/aws/cloudtrail/securitytrail
1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

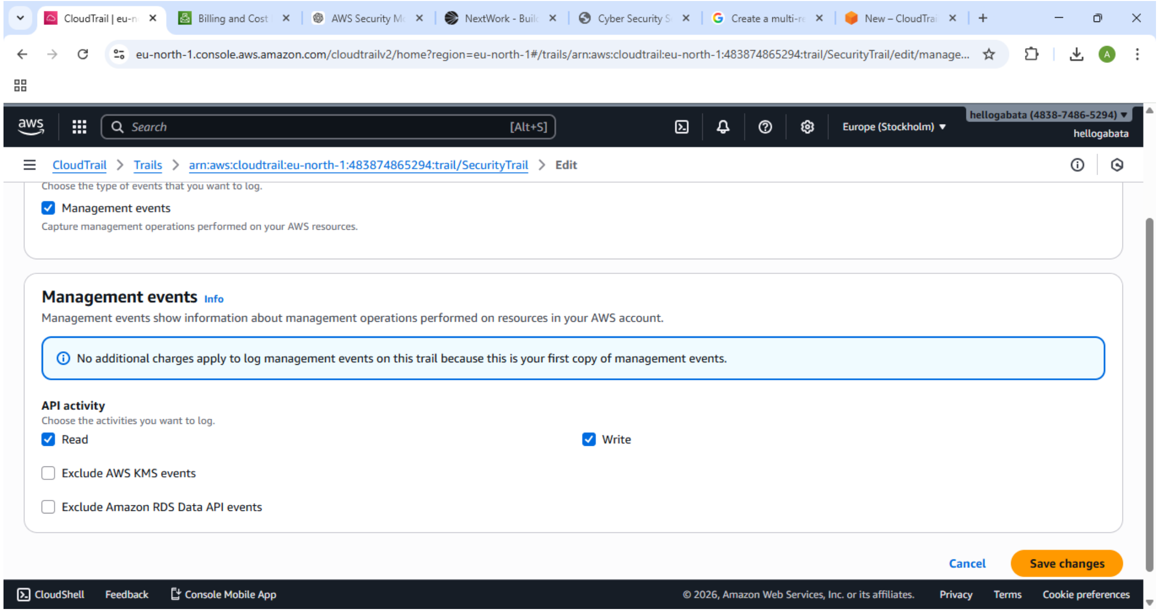
IAM Role Info
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.
● New
○ Existing

You will to enable **CloudWatch Logs integration** and create new Log Group: Here I set my own as /aws/cloudtrail/securitytrail and create an IAM role automatically by selecting **new.**


Edit trail - Cloud
Billing and Cost
AWS Security M
NextWork - Buil
Cyber Security S
Create a multi-r
New – CloudTra
eu-north-1.console.aws.amazon.com/cloudtrailv2/home?region=eu-north-1#/trails/arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail/edit/cloudW...
Search
[Alt+S]
Europe (Stockholm) ▾
hellogabata (4838-7486-5294) ▾
hellogabata
CloudTrail > Trails > arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail > Edit

```
          "arn:aws:logs:eu-north-1:483874865294:log-group:/aws/cloudtrail/securitytrail:log-stream:483874865294_CloudTrail_eu-north-1*"
        ]
      },
      {
        "Sid": "AWSCloudTrailPutLogEvents20141101",
        "Effect": "Allow",
        "Action": [
          "logs:PutLogEvents"
        ],
        "Resource": [
          "arn:aws:logs:eu-north-1:483874865294:log-group:/aws/cloudtrail/securitytrail:log-stream:483874865294_CloudTrail_eu-north-1*"
        ]
      }
    ]
  }
```

Cancel
Save changes
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudTrail | eu-n
Billing and Cost
AWS Security M
NextWork - Buil
Cyber Security S
Create a multi-r
New – CloudTra
eu-north-1.console.aws.amazon.com/cloudtrailv2/home?region=eu-north-1#/trails/arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail/edit/manage...
Search
[Alt+S]
Europe (Stockholm) ▾
hellogabata (4838-7486-5294) ▾
hellogabata
CloudTrail > Trails > arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail > Edit

Choose the type of events that you want to log.

☑ Management events

Capture management operations performed on your AWS resources.

Management events Info

Management events show information about management operations performed on resources in your AWS account.

ⓘ No additional charges apply to log management events on this trail because this is your first copy of management events.

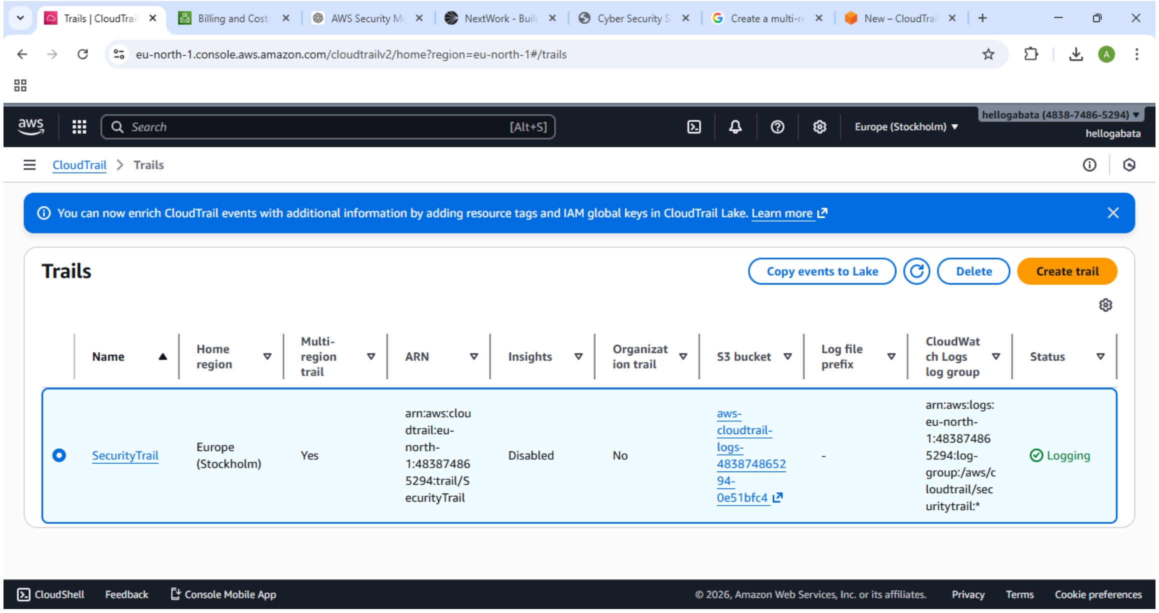
API activity

Choose the activities you want to log.

☑ Read ☑ Write

□ Exclude AWS KMS events

□ Exclude Amazon RDS Data API events



ⓘ You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more

Trails

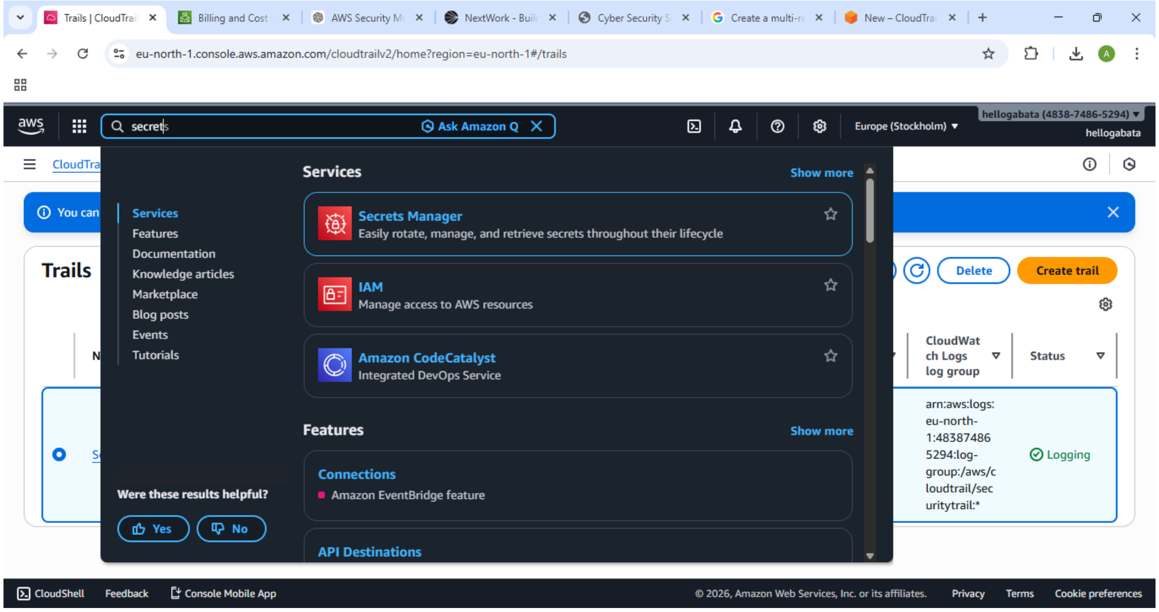
Copy events to Lake | Delete | Create trail

	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
●	SecurityTrail	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:483874865294:trail/SecurityTrail	Disabled	No	aws-cloudtrail-logs-483874865294-0e51bfc4	-	arn:aws:logs:eu-north-1:483874865294:log-group:/aws/cloudtrail/securitytrail:*	✓ Logging

Now you can see that we can configure the Multi region trail, we created a S3 bucket automatically, an IAM user was also created and we configure the Cloudwatch Log automatically. We can see that the Trail is now Logging.

Task 1.2 — Create the Honeytoken Secret

Open **Secrets Manage**



Services

Secrets Manager
Easily rotate, manage, and retrieve secrets throughout their lifecycle

IAM
Manage access to AWS resources

Amazon CodeCatalyst
Integrated DevOps Service

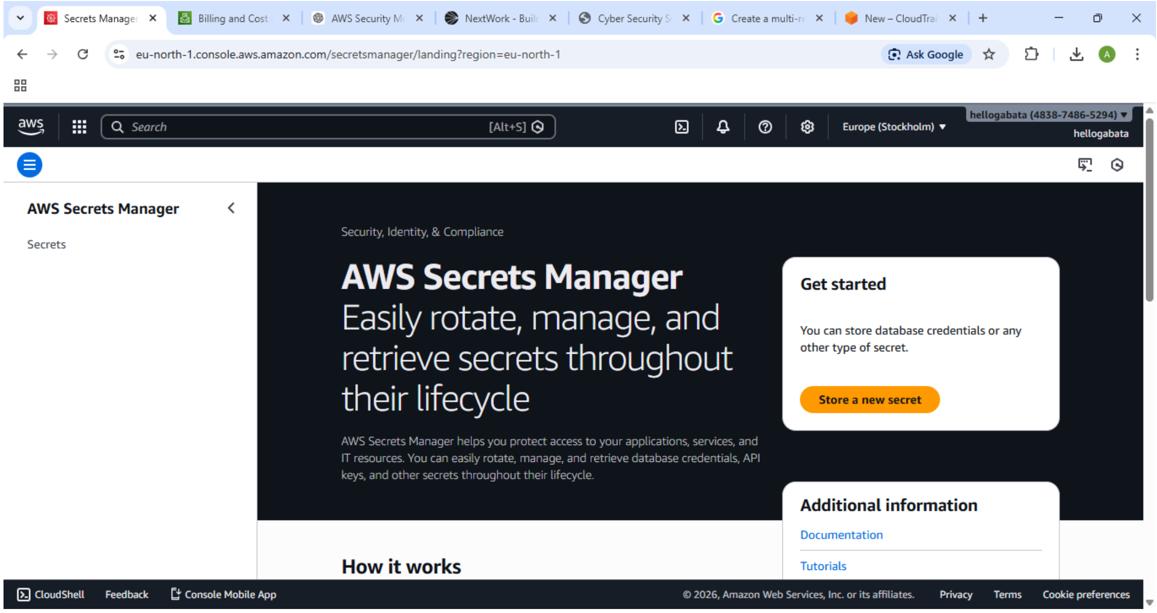
Features

Connections
Amazon EventBridge feature

API Destinations

arn:aws:logs:eu-north-1:483874865294:log-group:/aws/cloudtrail/securitytrail:* — Logging

© 2026, Amazon Web Services, Inc. or its affiliates.



Security, Identity, & Compliance

AWS Secrets Manager
Easily rotate, manage, and retrieve secrets throughout their lifecycle

AWS Secrets Manager helps you protect access to your applications, services, and IT resources. You can easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

Get started

You can store database credentials or any other type of secret.

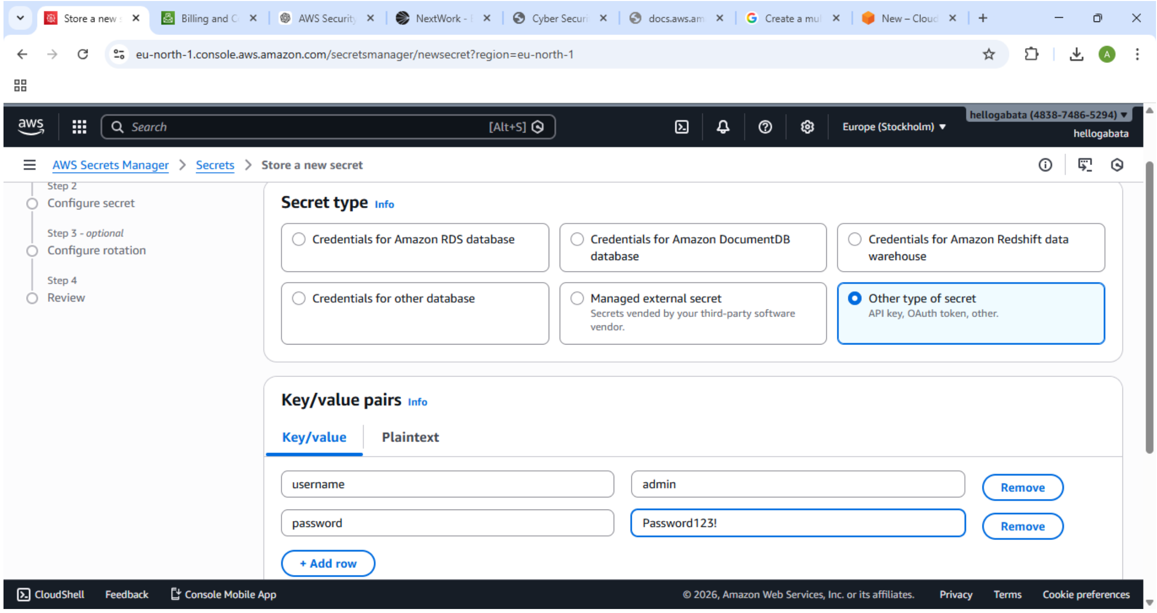
Additional information

Documentation

Tutorials

How it works

© 2026, Amazon Web Services, Inc. or its affiliates.



Secret type Info

○ Credentials for Amazon RDS database
○ Credentials for Amazon DocumentDB database
○ Credentials for Amazon Redshift data warehouse
○ Credentials for other database
○ Managed external secret
Secrets vended by your third-party software vendor.
● Other type of secret
API key, OAuth token, other.

Key/value pairs Info

Key/value | Plaintext

username	admin	Remove
password	Password123!	Remove

+ Add row

When selecting the Secret type: **Other type of secret**

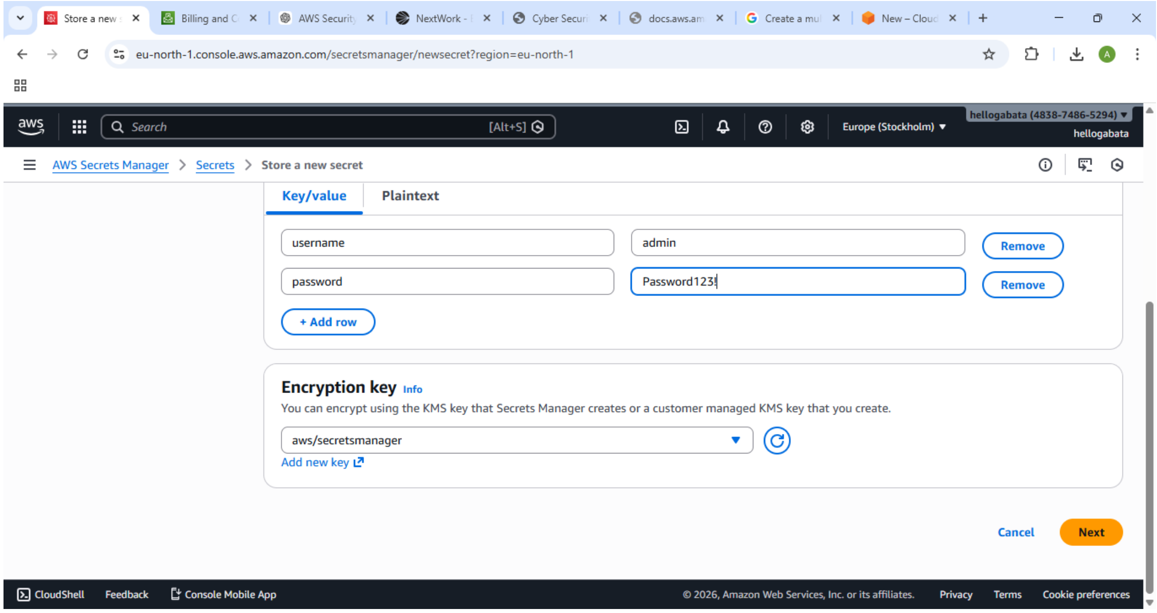
Here you’ll see that I configure it as follows

□ Key: username

□ Value: admin

□ Add another:

- Key: password
- Value: Password123!


eu-north-1.console.aws.amazon.com/secretsmanager/newsecret?region=eu-north-1
AWS Secrets Manager > Secrets > Store a new secret
Key/value
Plaintext
Remove
Remove
+ Add row
Cancel
Next
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

username	admin
password	Password123!

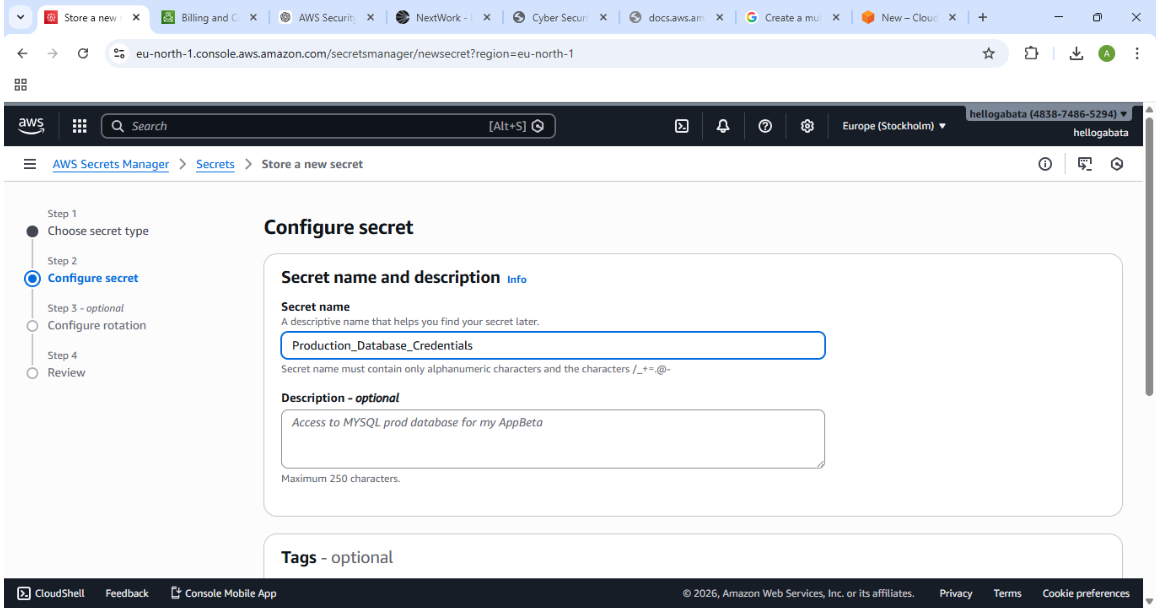
Encryption key Info

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager

Add new key

For your encryption key, choose **the aws/secretmanger.** This is enough for keeping your secrets.


eu-north-1.console.aws.amazon.com/secretsmanager/newsecret?region=eu-north-1
AWS Secrets Manager > Secrets > Store a new secret
Step 1
Choose secret type
Step 2
Configure secret
Step 3 - optional
Configure rotation
Step 4
Review
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Configure secret

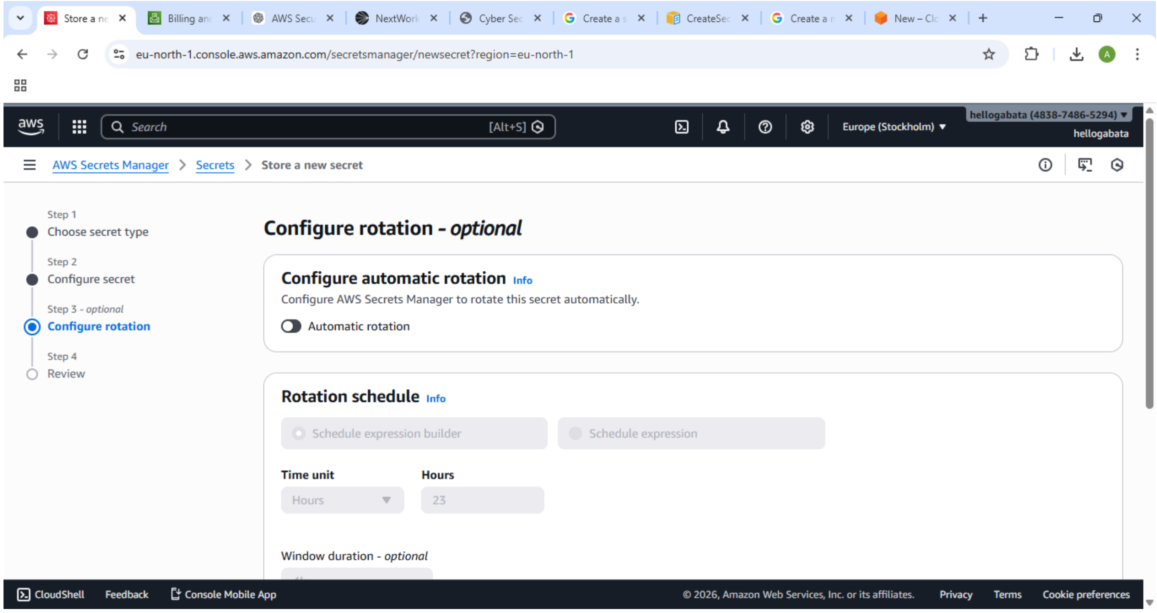
Secret name and description Info

Secret name
A descriptive name that helps you find your secret later.
Production_Database_Credentials
Secret name must contain only alphanumeric characters and the characters /_+=.@-

Description - *optional*
Access to MYSQL prod database for my AppBeta
Maximum 250 characters.

Tags - optional

The secret name is set as **Production_Database_Credentials**


eu-north-1.console.aws.amazon.com/secretsmanager/newsecret?region=eu-north-1
Search [Alt+S]
Europe (Stockholm)
hellogabata (4838-7486-5294)
hellogabata
AWS Secrets Manager > Secrets > Store a new secret
Step 1
Choose secret type
Step 2
Configure secret
Step 3 - optional
Configure rotation
Step 4
Review
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Configure rotation - *optional*

Configure automatic rotation Info

Configure AWS Secrets Manager to rotate this secret automatically.

Automatic rotation

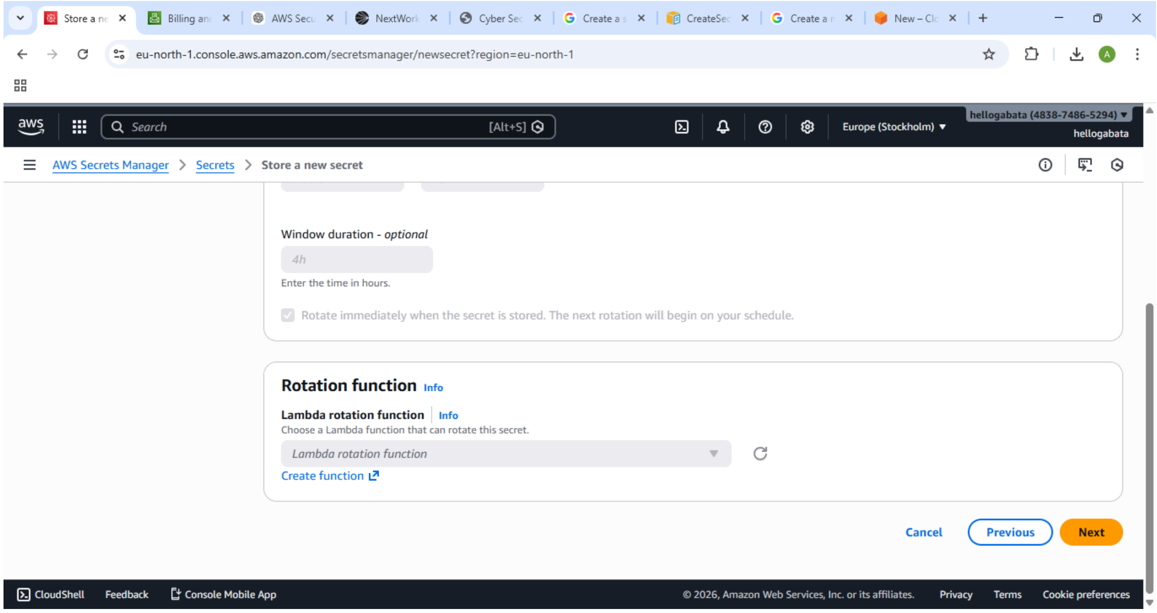
Rotation schedule Info

○ Schedule expression builder ○ Schedule expression

Time unit Hours

Hours 23

Window duration - *optional*


eu-north-1.console.aws.amazon.com/secretsmanager/newsecret?region=eu-north-1
Search [Alt+S]
Europe (Stockholm)
hellogabata (4838-7486-5294)
hellogabata
AWS Secrets Manager > Secrets > Store a new secret
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Window duration - *optional*

4h

Enter the time in hours.

☑ Rotate immediately when the secret is stored. The next rotation will begin on your schedule.

Rotation function Info

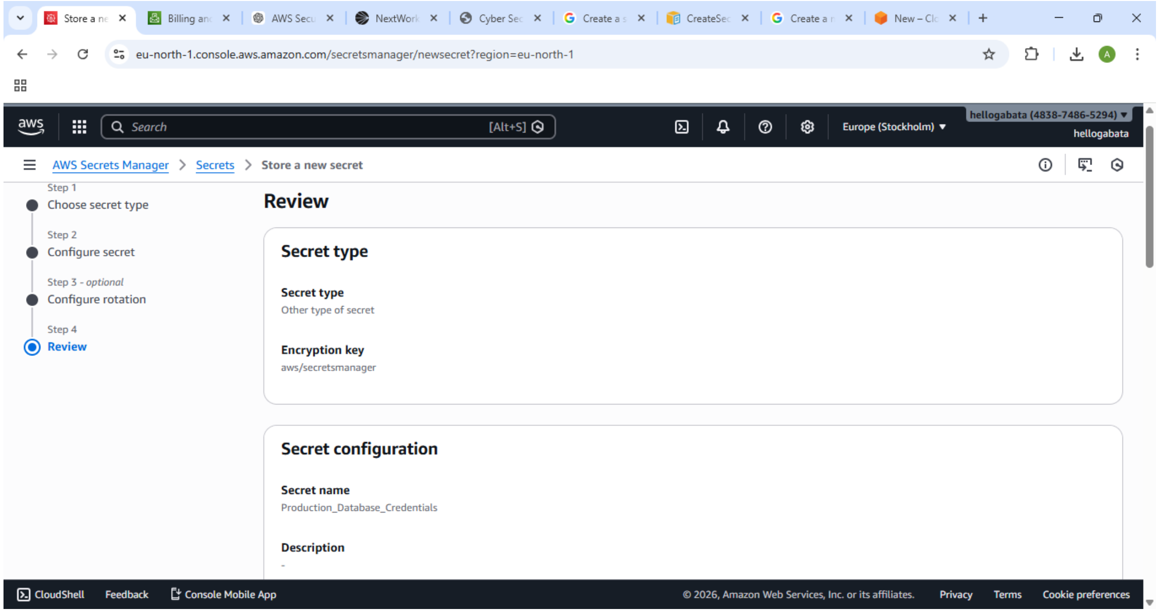
Lambda rotation function Info

Choose a Lambda function that can rotate this secret.

Lambda rotation function

Create function

Cancel Previous Next


eu-north-1.console.aws.amazon.com/secretsmanager/newsecret?region=eu-north-1
Search [Alt+S]
Europe (Stockholm) ▼
hellogabata (4838-7486-5294) ▼
hellogabata
AWS Secrets Manager > Secrets > Store a new secret
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
● Choose secret type

Step 2
● Configure secret

Step 3 - *optional*
● Configure rotation

Step 4
◉ Review

Review

Secret type

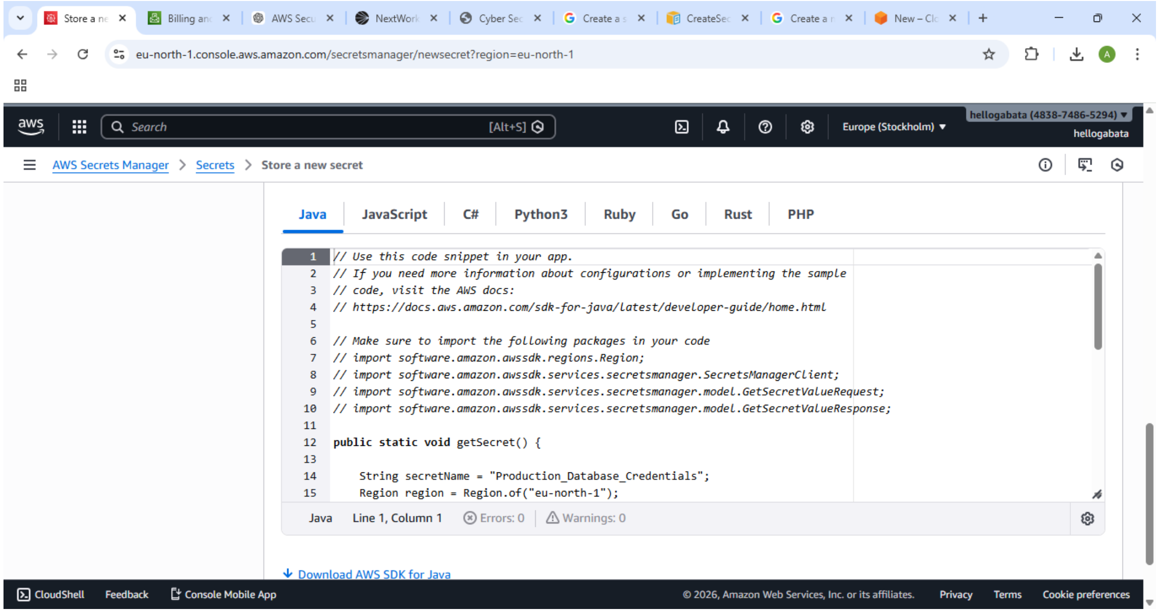
Secret type
Other type of secret

Encryption key
aws/secretsmanager

Secret configuration

Secret name
Production_Database_Credentials

Description
-


eu-north-1.console.aws.amazon.com/secretsmanager/newsecret?region=eu-north-1
Search [Alt+S]
Europe (Stockholm) ▼
hellogabata (4838-7486-5294) ▼
hellogabata
AWS Secrets Manager > Secrets > Store a new secret
Java
JavaScript
C#
Python3
Ruby
Go
Rust
PHP
Java
Line 1, Column 1
Errors: 0
Warnings: 0
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

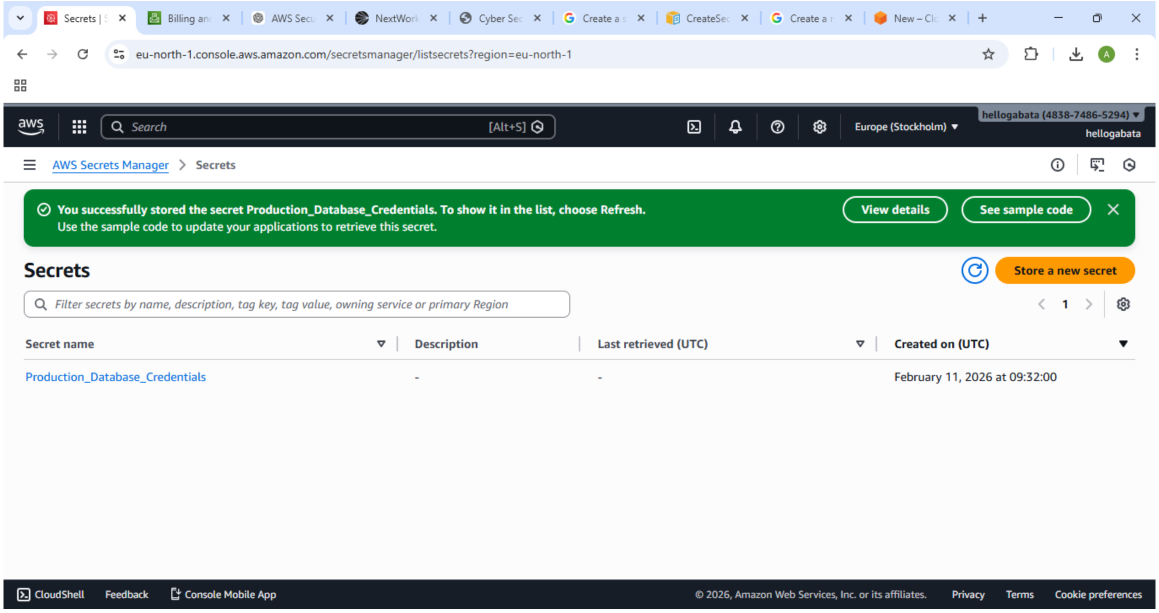
```
// Use this code snippet in your app.
// If you need more information about configurations or implementing the sample
// code, visit the AWS docs:
// https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/home.html

// Make sure to import the following packages in your code
// import software.amazon.awssdk.regions.Region;
// import software.amazon.awssdk.services.secretsmanager.SecretsManagerClient;
// import software.amazon.awssdk.services.secretsmanager.model.GetSecretValueRequest;
// import software.amazon.awssdk.services.secretsmanager.model.GetSecretValueResponse;

public static void getSecret() {

    String secretName = "Production_Database_Credentials";
    Region region = Region.of("eu-north-1");
```

↓ Download AWS SDK for Java


Secrets |
Billing an
AWS Secu
NextWork
Cyber Sec
Create a
CreateSec
Create a
New – Cl
eu-north-1.console.aws.amazon.com/secretsmanager/listsecrets?region=eu-north-1
aws
Search
[Alt+S]
Europe (Stockholm) ▾
hellogabata (4838-7486-5294) ▾
hellogabata
AWS Secrets Manager > Secrets
View details
See sample code
Store a new secret
Filter secrets by name, description, tag key, tag value, owning service or primary Region
1
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

You successfully stored the secret Production_Database_Credentials. To show it in the list, choose Refresh.
Use the sample code to update your applications to retrieve this secret.

Secrets

Secret name	Description	Last retrieved (UTC)	Created on (UTC)
Production_Database_Credentials	-	-	February 11, 2026 at 09:32:00

Our secret has been created.

The full report can be found here

https://muhakeem.hashnode.dev/build-a-security-monitoring-system-aws?showSharer=true

1. Executive Summary

This project implements a real-time security monitoring and automated response system using native AWS services. The primary goal of the system is to detect and respond immediately when sensitive information stored in AWS Secrets Manager is accessed.

Two detection mechanisms were implemented:

1. CloudWatch Metric Filter–based alerting.

2. Amazon EventBridge event-driven alerting.

When the sensitive secret named Production_Database_Credentials is accessed, the system generates alerts and automatically disables the offending IAM user by attaching a deny-all permissions boundary. This simulates a real-world insider threat or credential compromise scenario.

2. Lab Architecture

The system architecture consists of the following AWS services:

- AWS CloudTrail

- AWS Secrets Manager

- Amazon CloudWatch Logs & Alarms

- Amazon EventBridge

- Amazon SNS

- AWS Lambda

- AWS IAM

3. Evidence from Logs (CloudTrail)

Include JSON log snippet showing eventTime, userIdentity, and sourceIpAddress.

4. Technical Evidence

Screenshots required:

- Email notification

- IAM user permissions removed

- AccessDenied log

5. Security Analysis

Speed: EventBridge provided faster detection.

Context: EventBridge alerts provided more useful information.

Compliance: This satisfies NIST Continuous Monitoring (CA-7).

6. Conclusion

The project demonstrates practical cloud security monitoring and automated response.