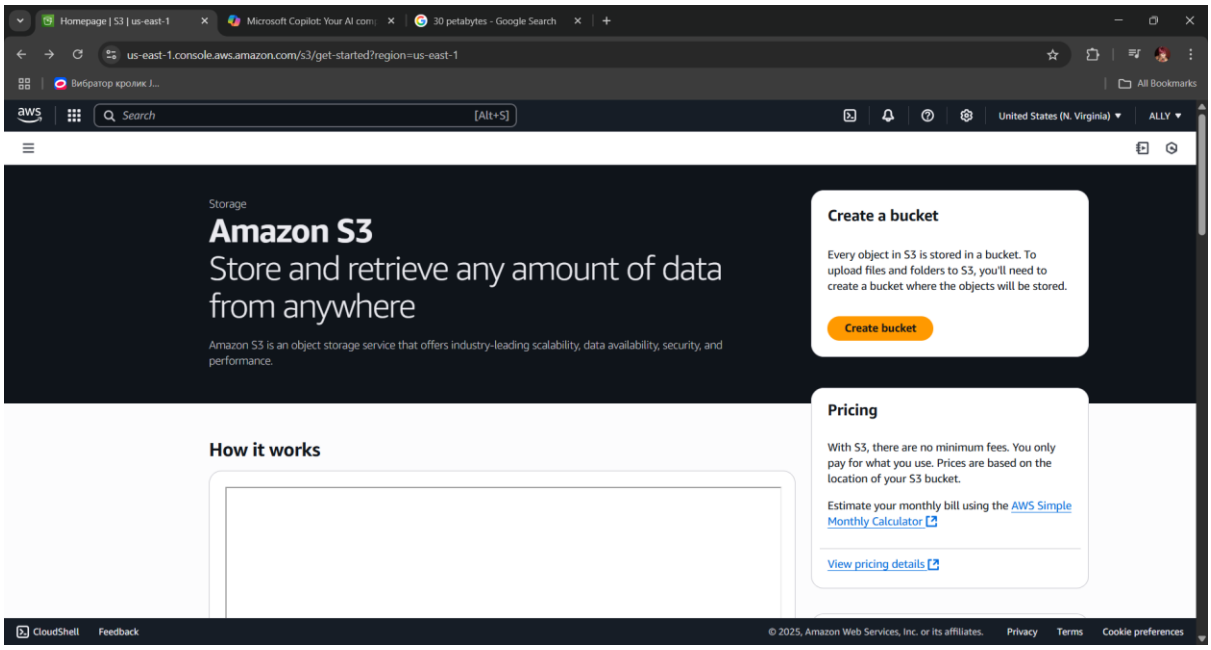
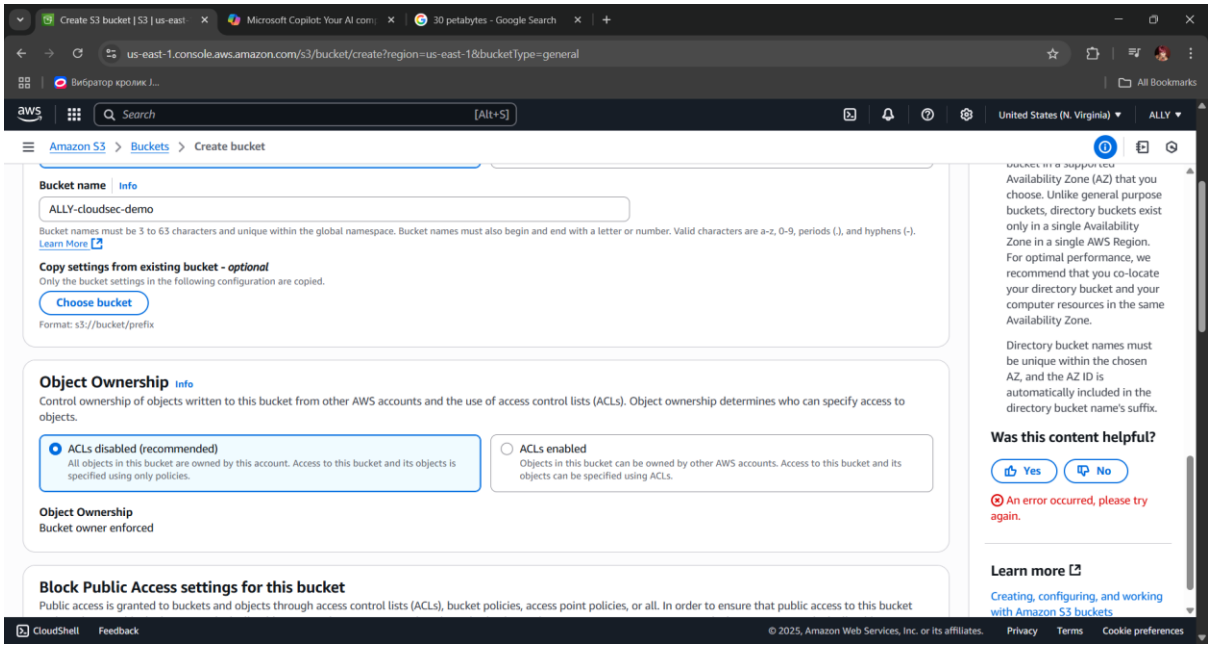
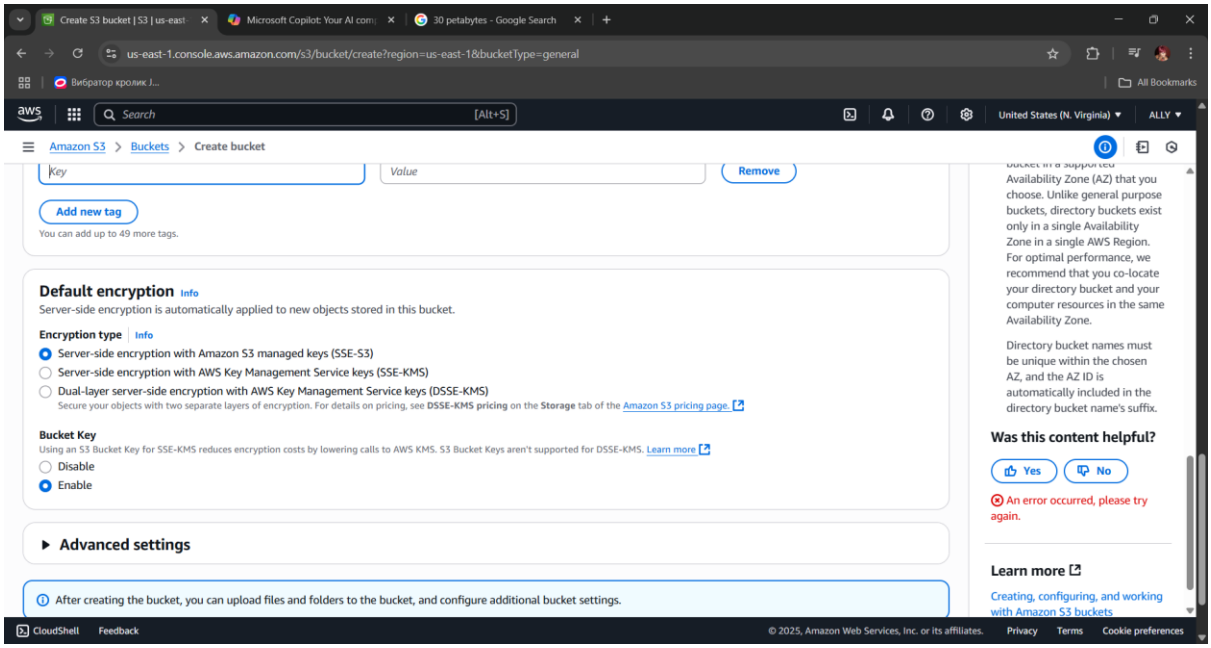
STEPS FOR THE FIRST PROJECT

Search for S3 in the search bar, after click on **CREATE BUCKET**

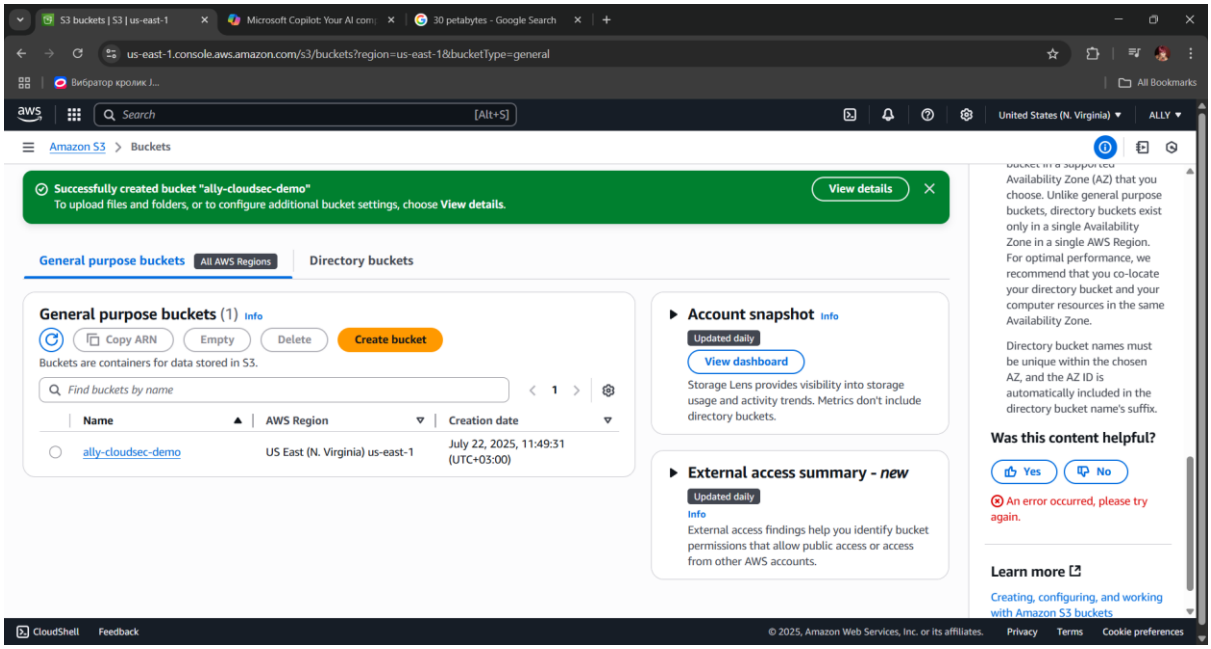


Named my bucket after which I keep all settings in default for now and went ahead to create bucket

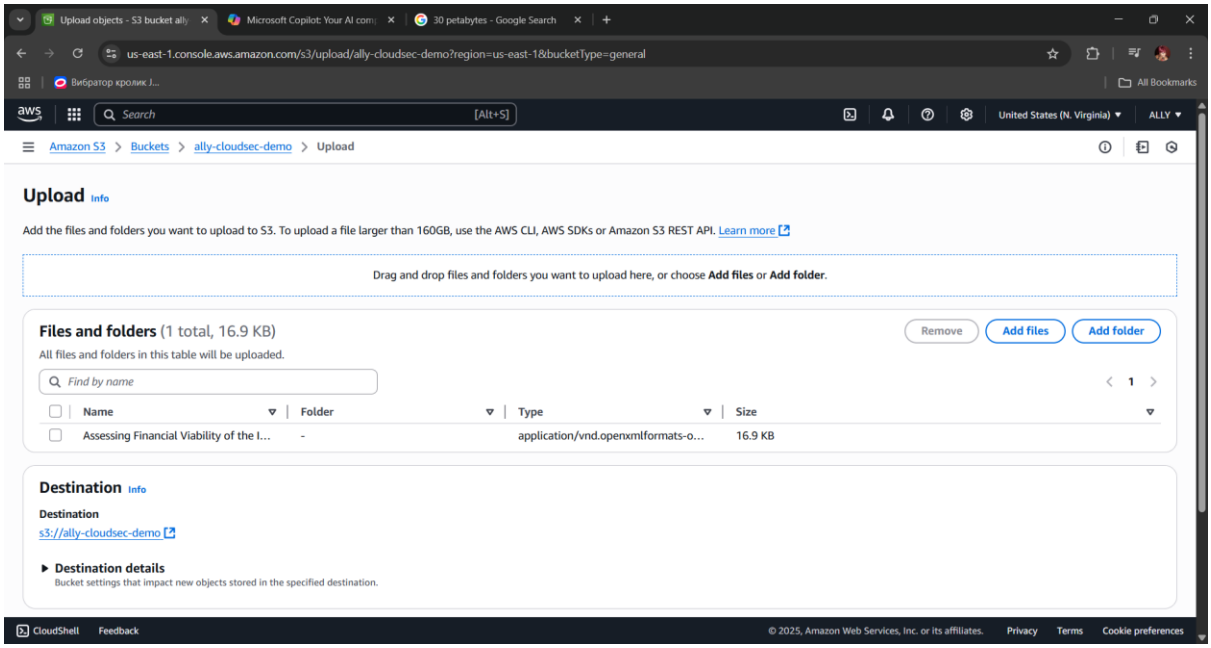


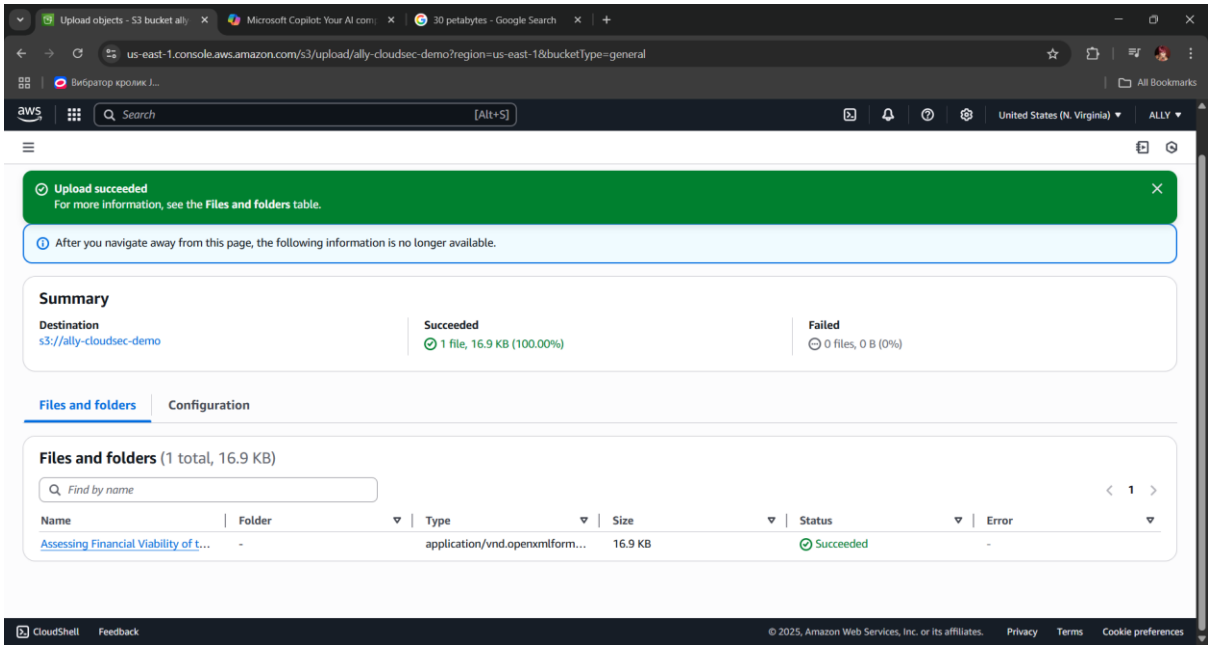


NOTE: Bucket name must not contain uppercase characters

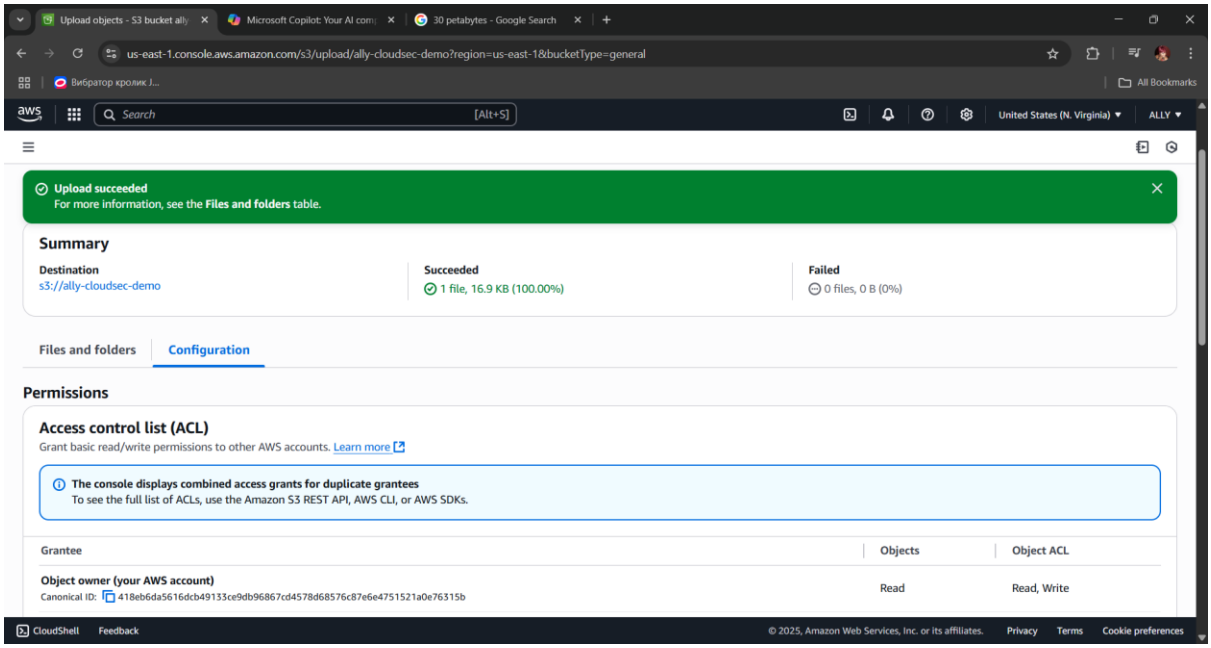


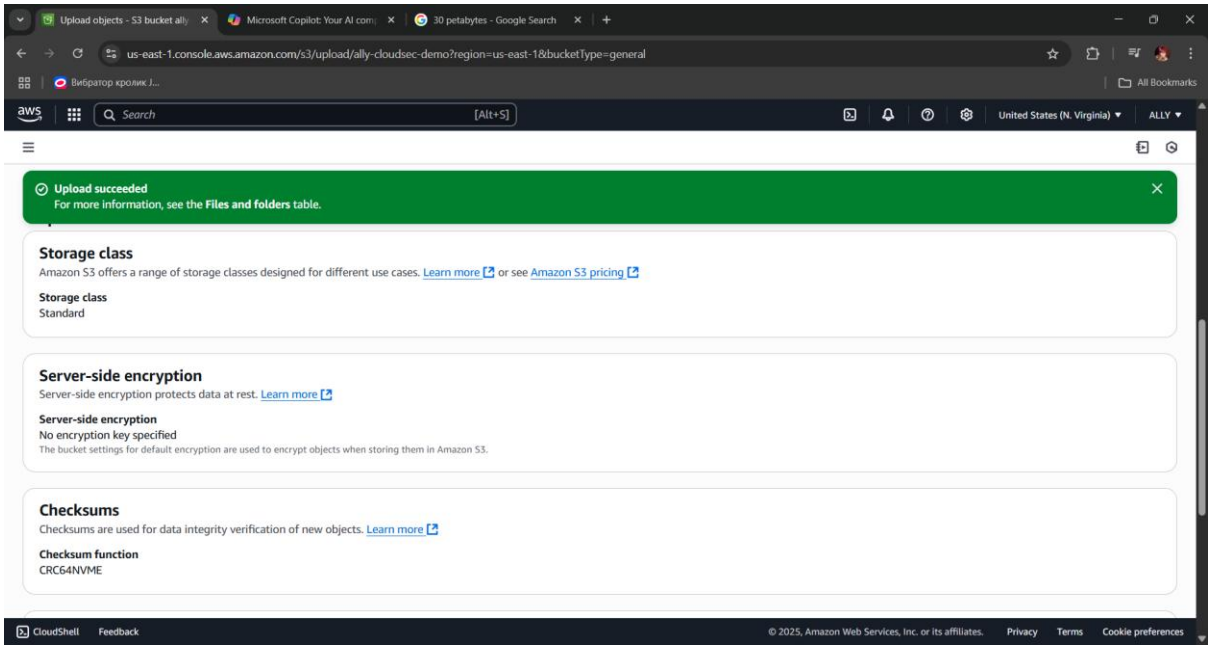
The above is the image after creating the bucket

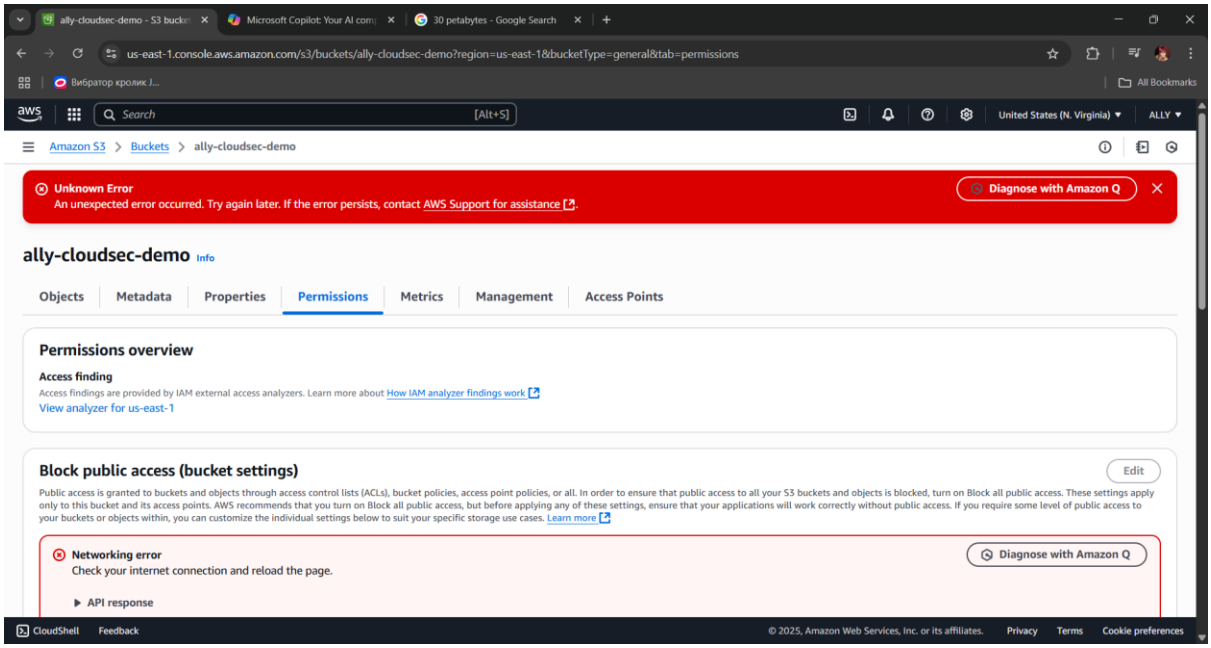




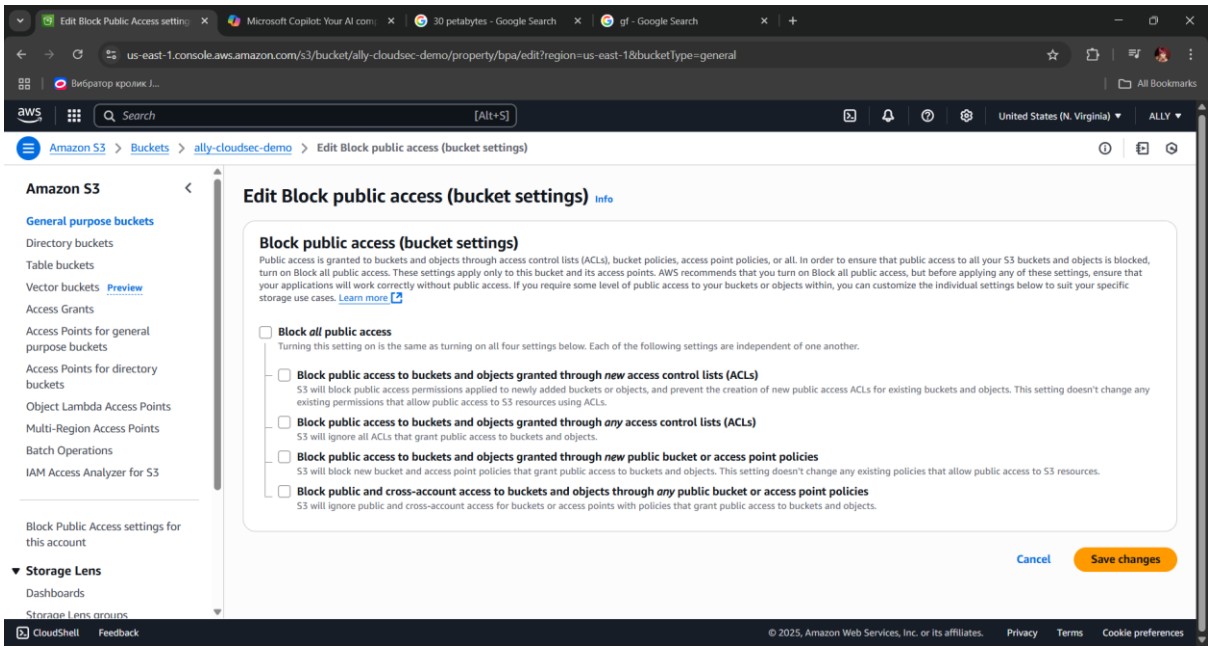
This is the point I uploaded the file into the bucket


Upload succeeded
For more information, see the Files and folders table.
Summary
Destination
s3://ally-cloudsec-demo
Succeeded
1 file, 16.9 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Permissions
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.
Grantee
Objects
Object ACL
Object owner (your AWS account)
Canonical ID: 418eb6da5616dcb49133ce9db96867cd4578d68576c87e6e4751521a0e76315b
Read
Read, Write

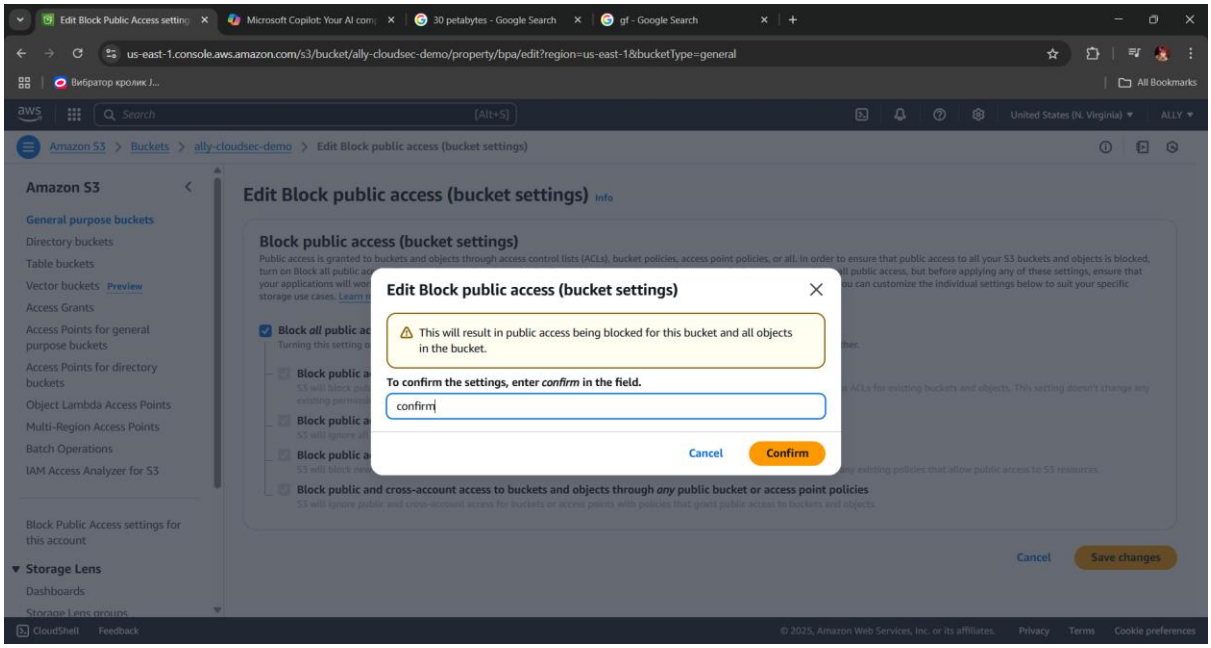

Upload succeeded
For more information, see the Files and folders table.
Storage class
Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing
Storage class
Standard
Server-side encryption
Server-side encryption protects data at rest. Learn more
Server-side encryption
No encryption key specified
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
Checksums
Checksums are used for data integrity verification of new objects. Learn more
Checksum function
CRC64NVME



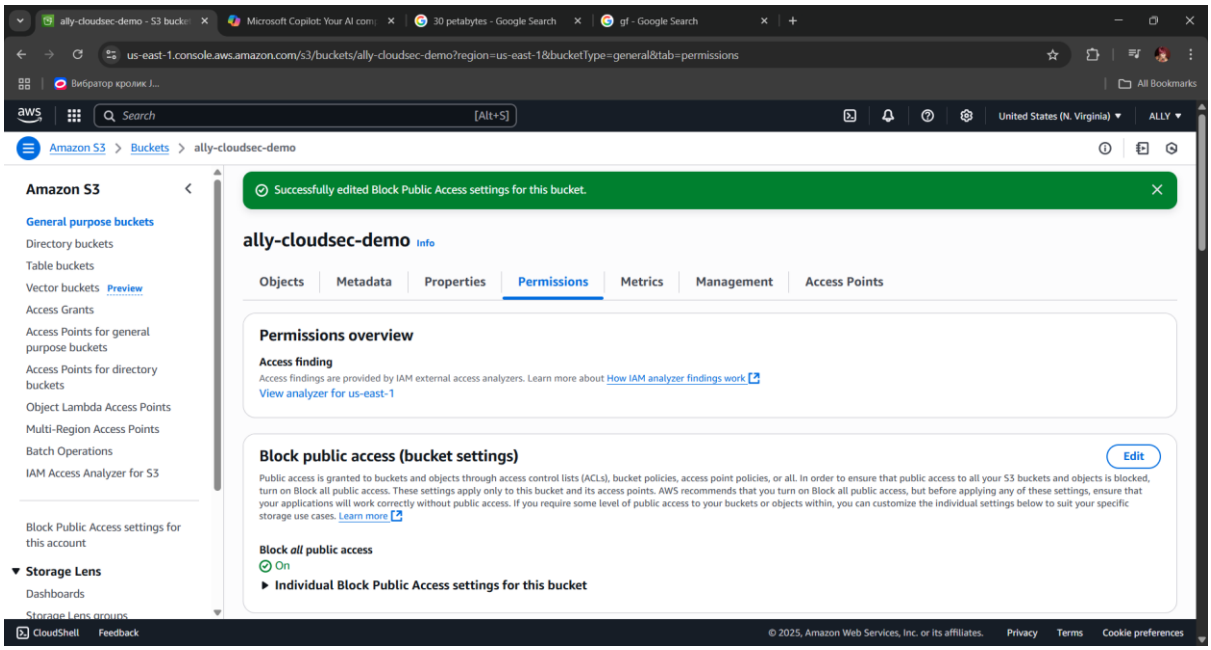
Encountered some errors when trying to load the permission access panel



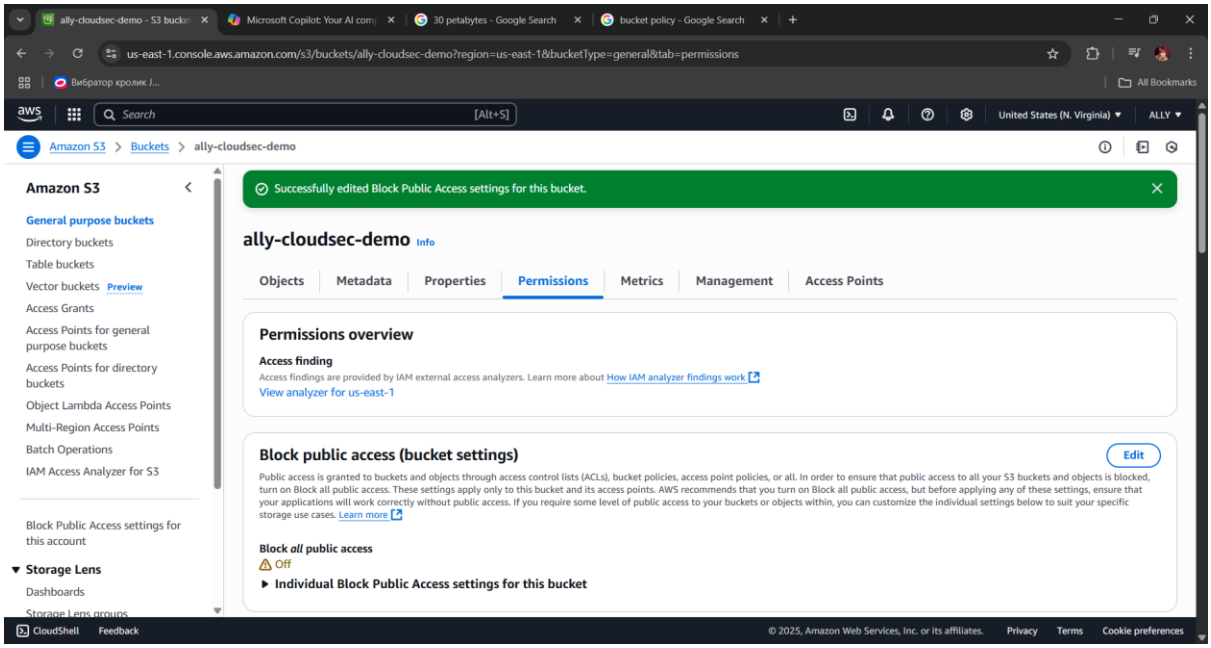
Making the bucket accessible to the public



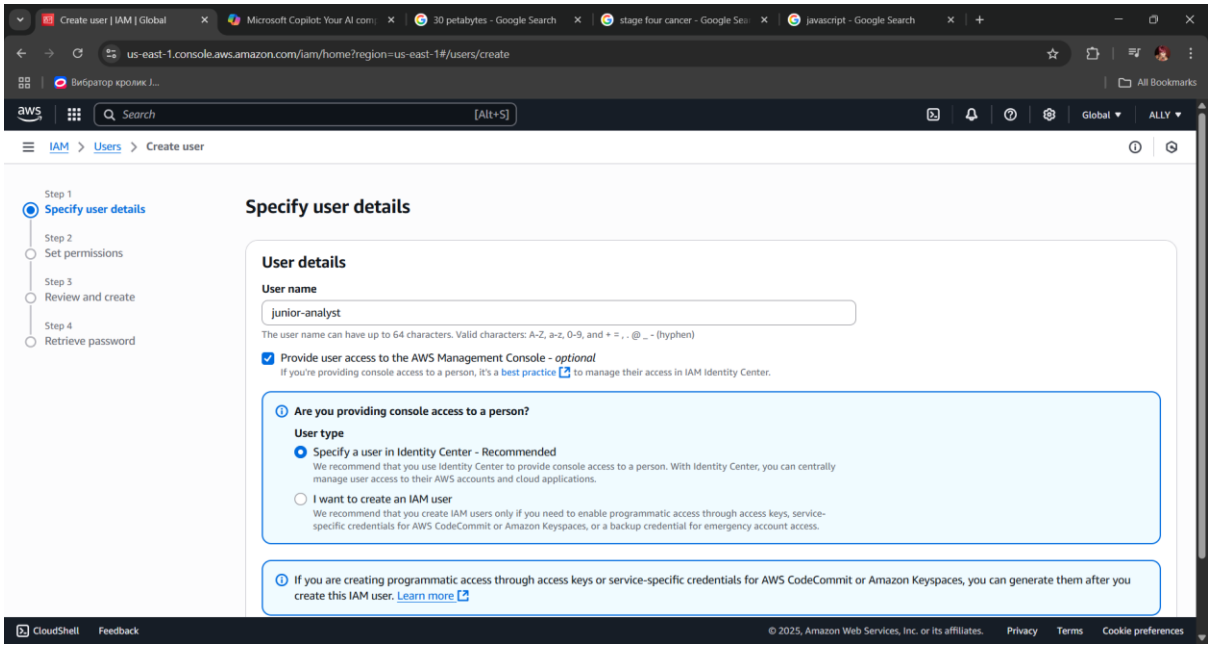
I have to confirm that I am making the bucket accessible to the public

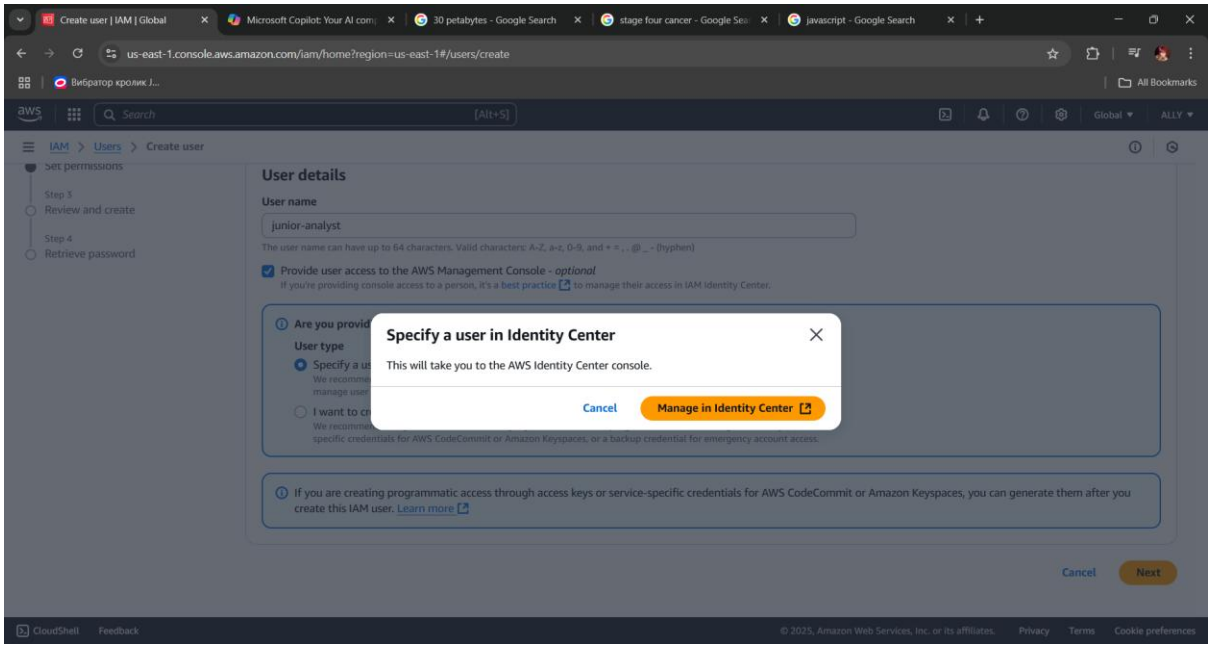


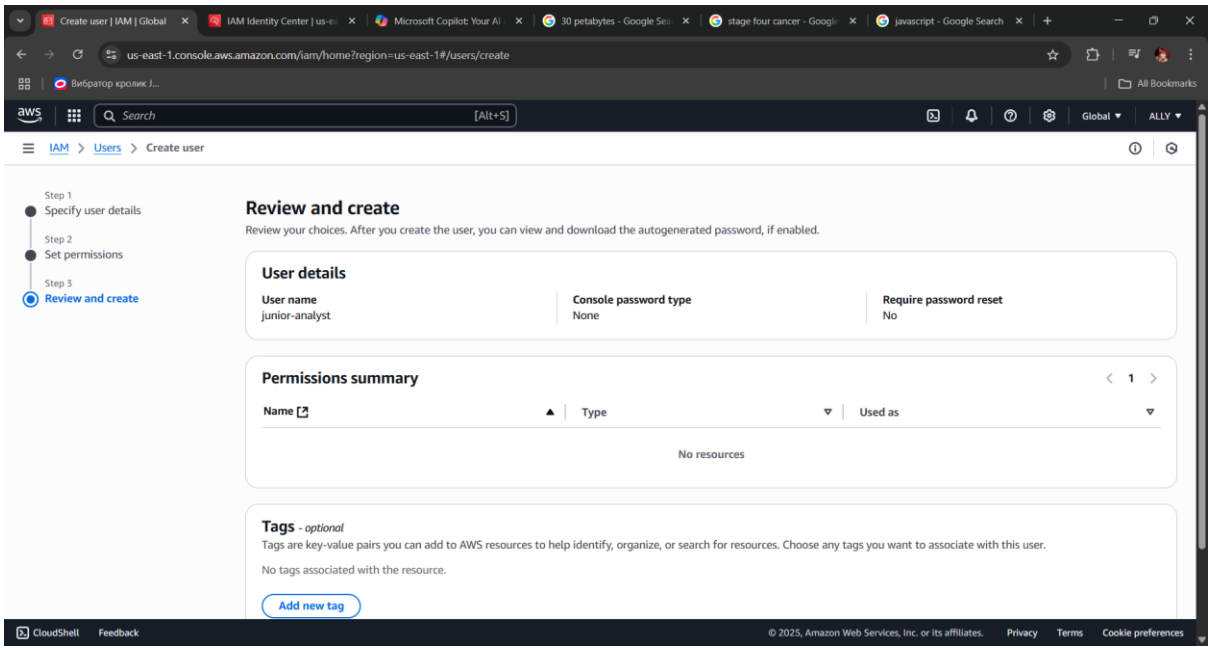
Successfully made it public

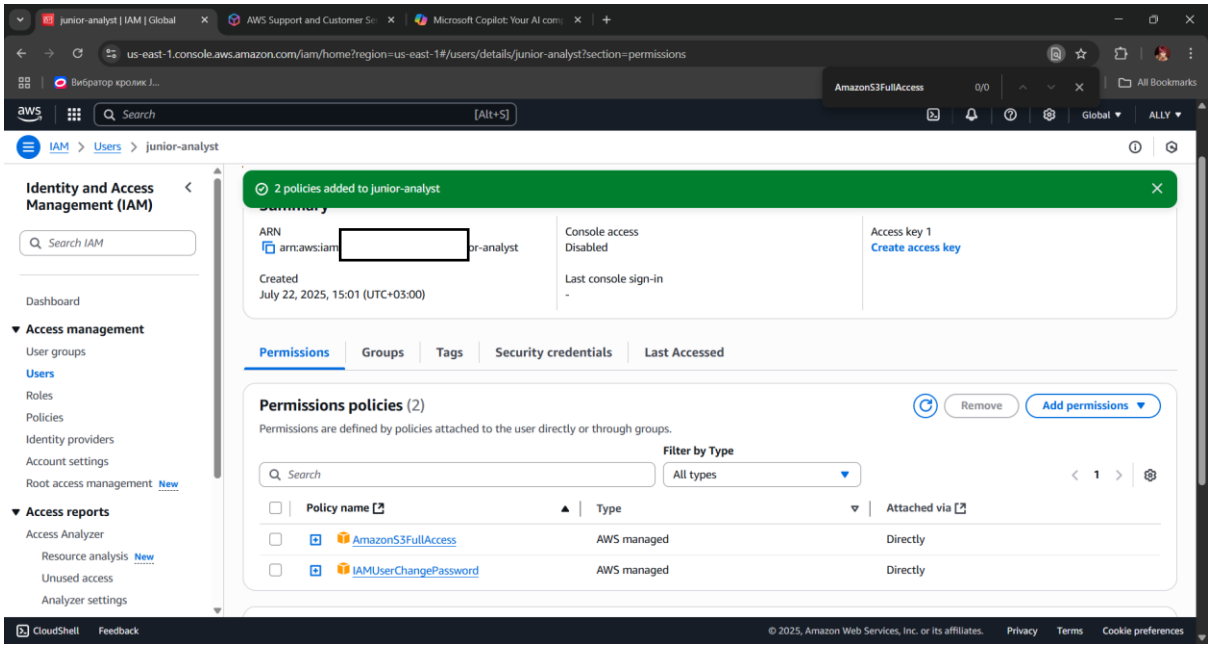


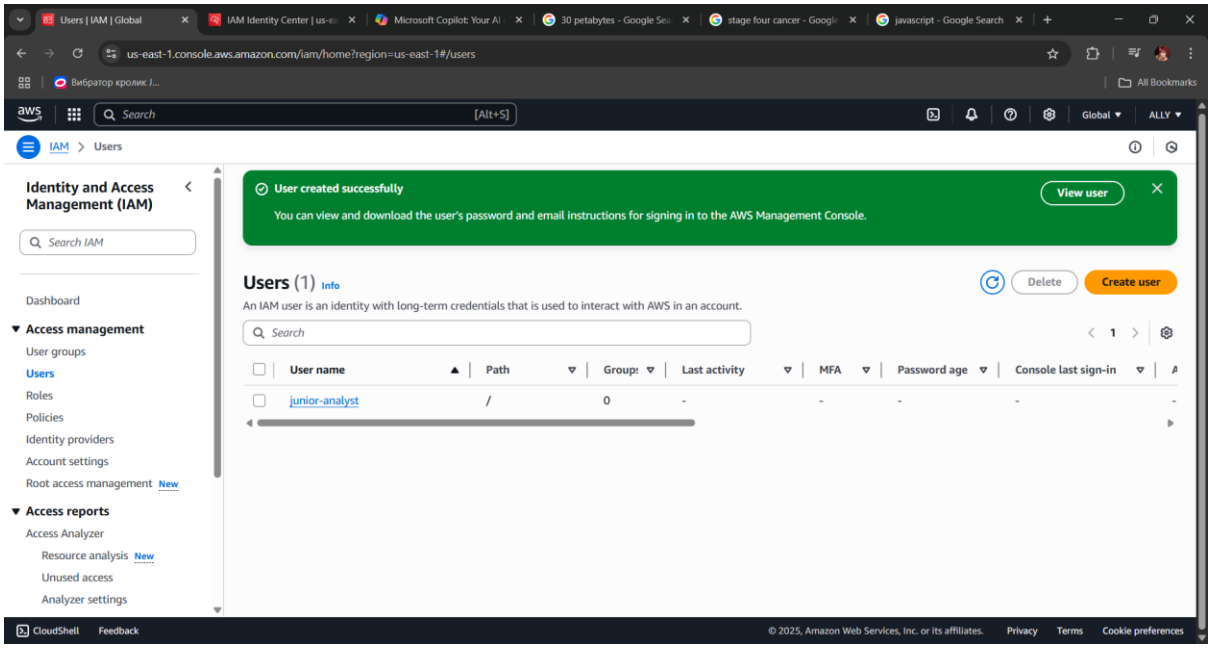
Below is creating user name called junior analyst




Create user | IAM | Global
Microsoft Copilot: Your AI com
30 petabytes - Google Search
stage four cancer - Google Sea
javascript - Google Search
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
All Bookmarks
IAM > Users > Create user
Set permissions
Step 3
Review and create
Step 4
Retrieve password
User details
User name
junior-analyst
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you provid
User type
Specify a us
I want to cr
Specify a user in Identity Center
This will take you to the AWS Identity Center console.
Cancel
Manage in Identity Center
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

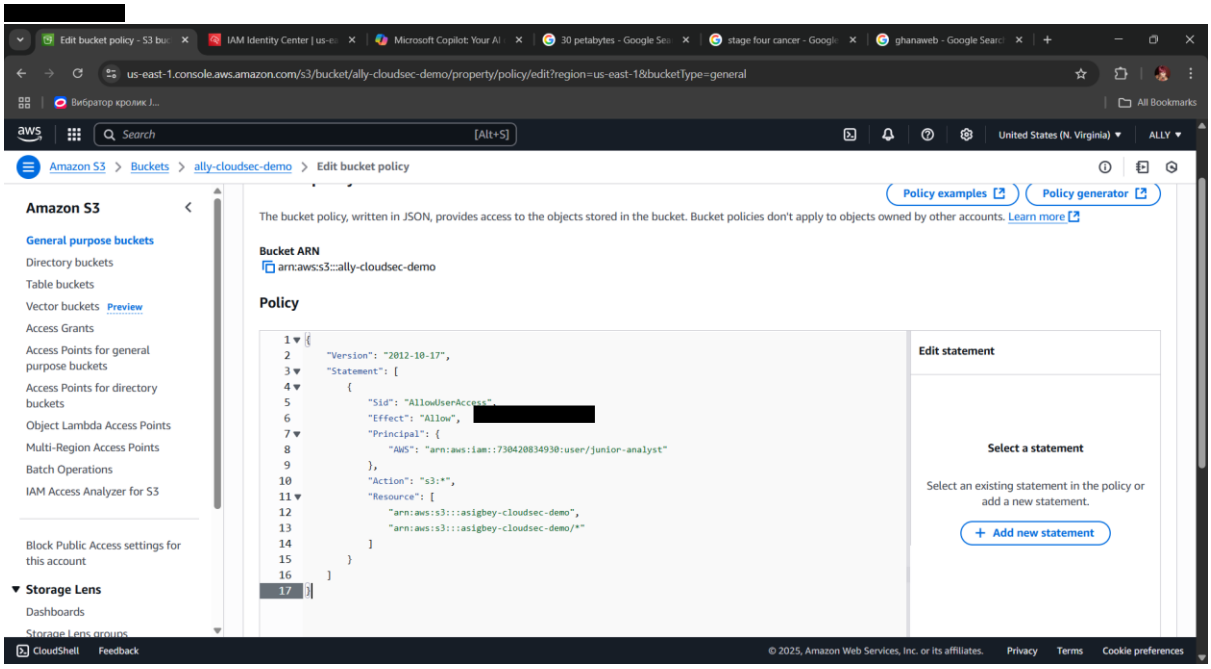

Create user | IAM | Global
IAM Identity Center | us-ea
Microsoft Copilot: Your AI
30 petabytes - Google Sea
stage four cancer - Google
javascript - Google Search
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
All Bookmarks
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
junior-analyst
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
No resources
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

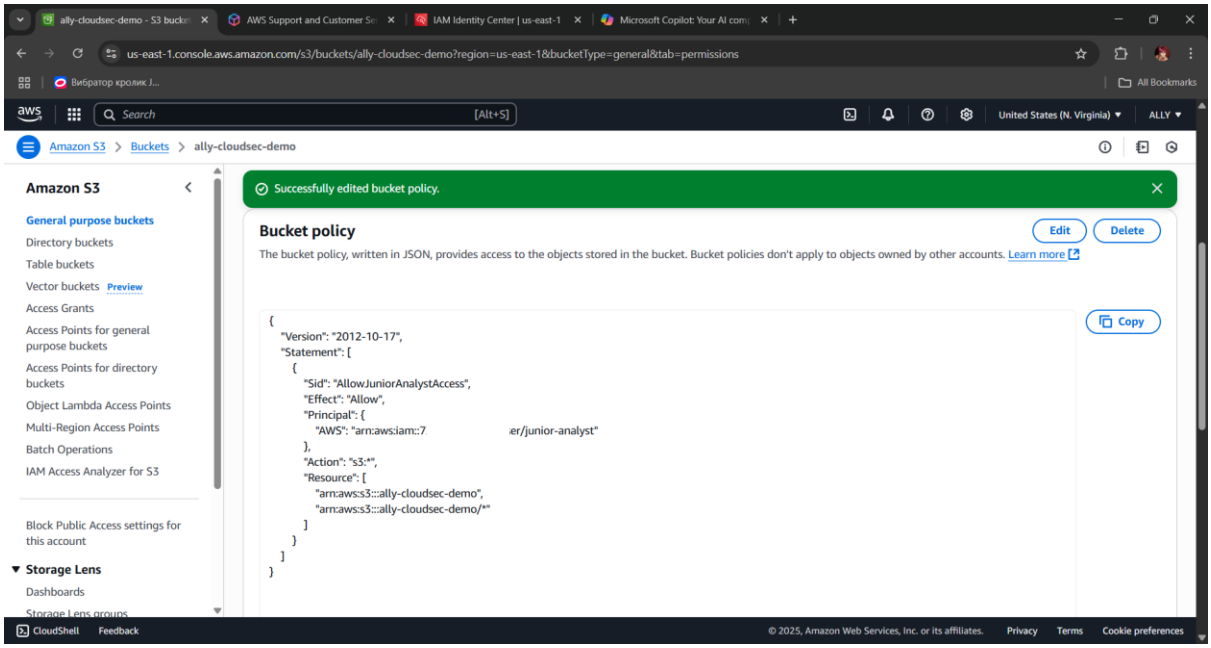

junior-analyst | IAM | Global
AWS Support and Customer Se
Microsoft Copilot: Your AI com
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/junior-analyst?section=permissions
AmazonS3FullAccess
0/0
All Bookmarks
Search
[Alt+S]
Global
ALLY
IAM > Users > junior-analyst
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
2 policies added to junior-analyst
ARN
arn:aws:iam
or-analyst
Console access
Disabled
Access key 1
Create access key
Created
July 22, 2025, 15:01 (UTC+03:00)
Last console sign-in
-
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
1
Policy name
Type
Attached via
AmazonS3FullAccess
AWS managed
Directly
IAMUserChangePassword
AWS managed
Directly
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

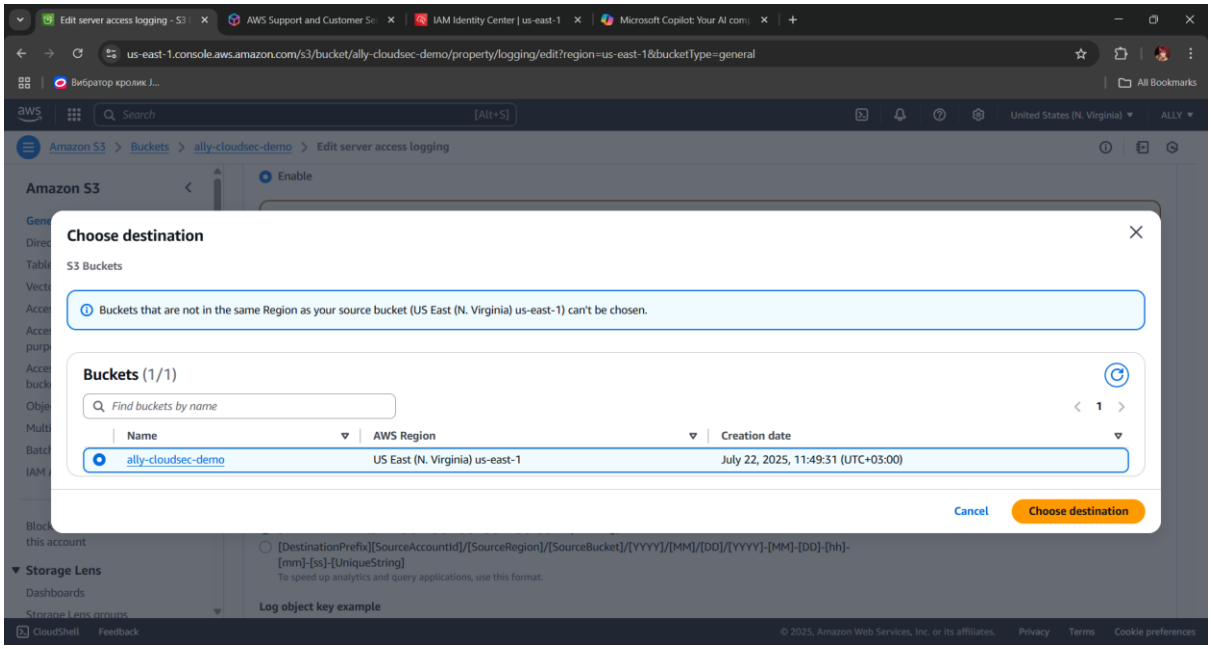


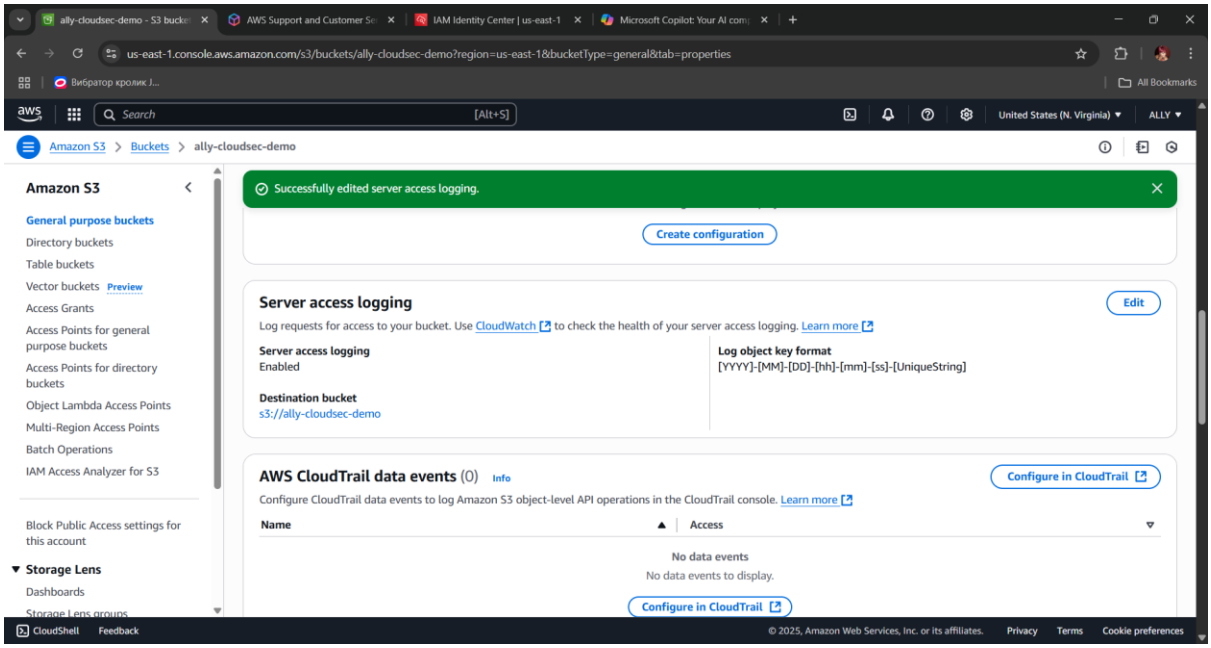
Policy of junior analyst

[redacted]




ally-cloudsec-demo - S3 bucket
AWS Support and Customer Se
IAM Identity Center | us-east-1
Microsoft Copilot: Your AI com
us-east-1.console.aws.amazon.com/s3/buckets/ally-cloudsec-demo?region=us-east-1&bucketType=general&tab=permissions
Вибратор кролик J...
All Bookmarks
Search
[Alt+S]
United States (N. Virginia)
ALLY
Amazon S3 > Buckets > ally-cloudsec-demo
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Vector buckets Preview
Access Grants
Access Points for general purpose buckets
Access Points for directory buckets
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
Successfully edited bucket policy.
Bucket policy
Edit
Delete
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Copy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AllowJuniorAnalystAccess",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::7 er/junior-analyst"
},
"Action": "s3:*",
"Resource": [
"arn:aws:s3:::ally-cloudsec-demo",
"arn:aws:s3:::ally-cloudsec-demo/*"
]
}
]
}
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Edit server access logging - S3
AWS Support and Customer Se
IAM Identity Center | us-east-1
Microsoft Copilot: Your AI com
us-east-1.console.aws.amazon.com/s3/bucket/ally-cloudsec-demo/property/logging/edit?region=us-east-1&bucketType=general
Вибратор кролик J...
All Bookmarks
Search
[Alt+S]
United States (N. Virginia)
ALLY
Amazon S3 > Buckets > ally-cloudsec-demo > Edit server access logging
Amazon S3
Enable
Choose destination
S3 Buckets
Buckets that are not in the same Region as your source bucket (US East (N. Virginia) us-east-1) can't be chosen.
Buckets (1/1)
Find buckets by name
1
Name
AWS Region
Creation date
ally-cloudsec-demo
US East (N. Virginia) us-east-1
July 22, 2025, 11:49:31 (UTC+03:00)
Cancel
Choose destination
[DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
To speed up analytics and query applications, use this format.
Log object key example
Storage Lens
Dashboards
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Initially I did not setup MFA for the root user account, I set it up and had to continue to the second project of the week which is Root Account Monitoring with CloudTrail + SNS with the below assignment;

Objective:

Simulate sensitive activity from the AWS root account and detect it using logging and alerts.

Tools Needed:

- **CloudTrail**
- **SNS(SimpleNotificationService)**
- **IAM**
- **AWSConsole**

Steps:

1.

2.

3.

4.

5.

6.

7.

Outcome:

Loginusing the root account (not recommended in production).

Perform a sensitive action (e.g., disable MFA, view billing dashboard).

Enable CloudTrail in your AWSaccount (if it's not already enabled).

Create a CloudTrail trail that logs activity to an S3bucket.

Set up anSNStopic andsubscribe your email or phone number.

Create a CloudWatch Event Rule to detect RootAccountUsage and trigger the SNS alert.

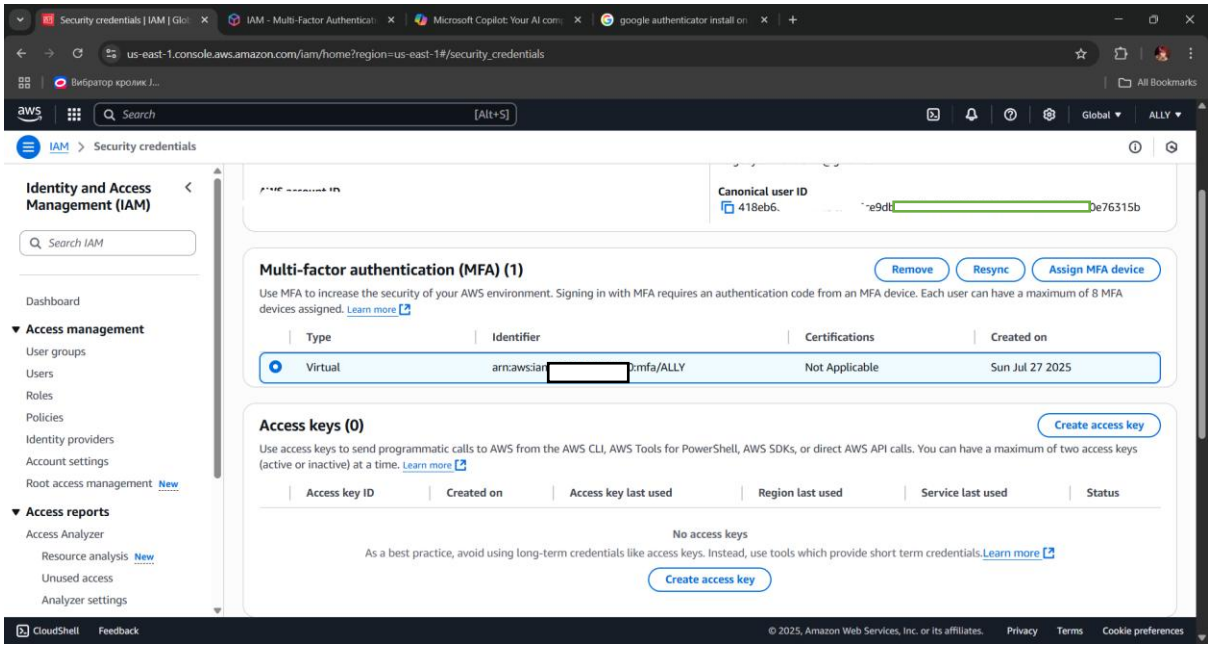
Test the setup by logging in again as root and checking that you receive a notification.

You'll learn how to detect and respond to root account usage, one of the most sensitive and high-risk actions in any AWS environment.

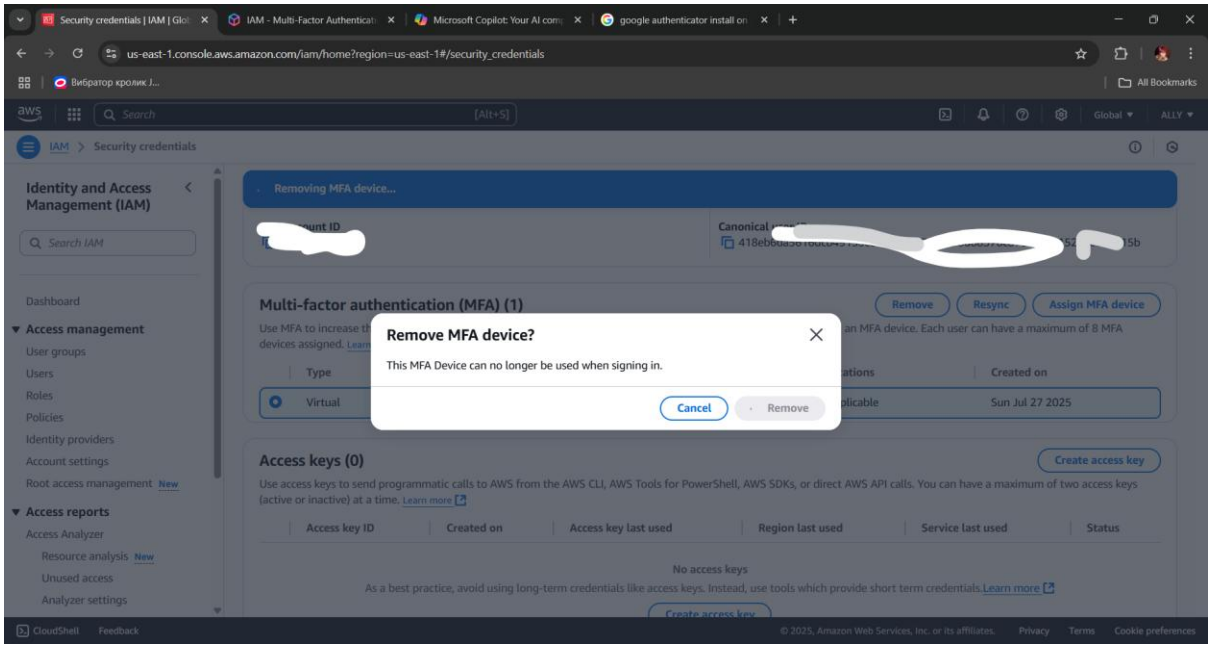
Whattodocument:

- **Screenshotsofall thesteps you took**
- **ScreenshotoftheCloudTrail log entry for root account activity**
- **YourSNStopicandsubscriptionconfiguration**
- **Screenshotofthealert received via email or SMS**
- **Ashortwrite-up:**

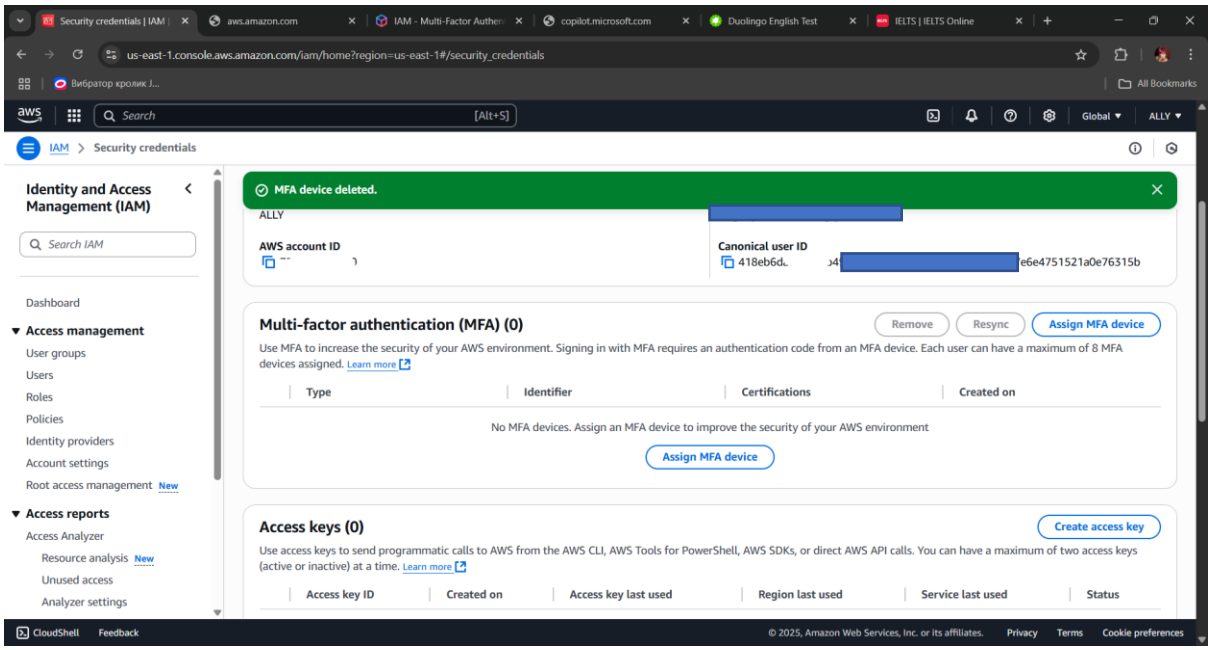
"What I didandwhat Ilearned



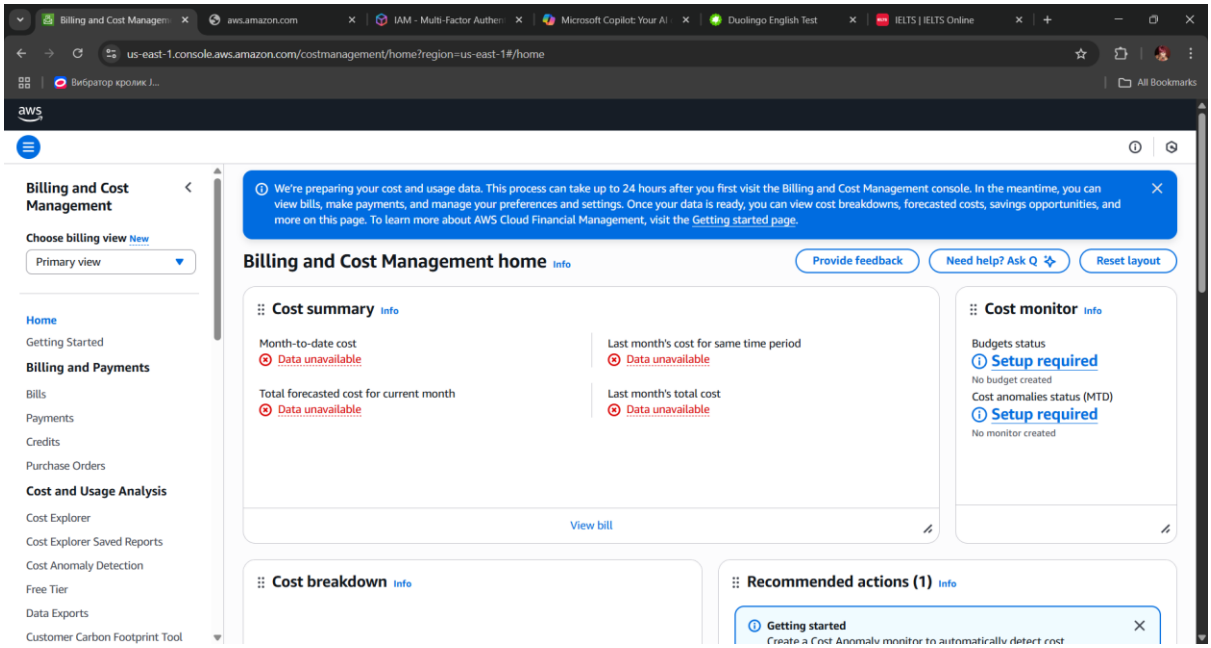
The above is the process of disabling/removing the MFA



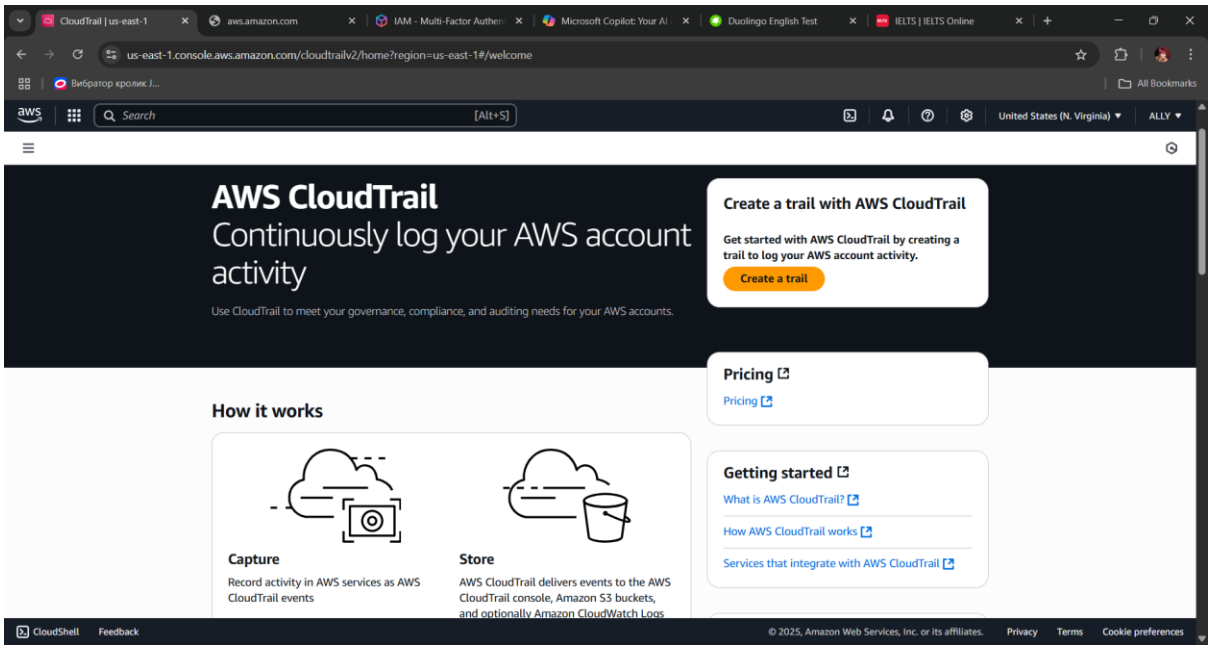
Successfully remove mfa below

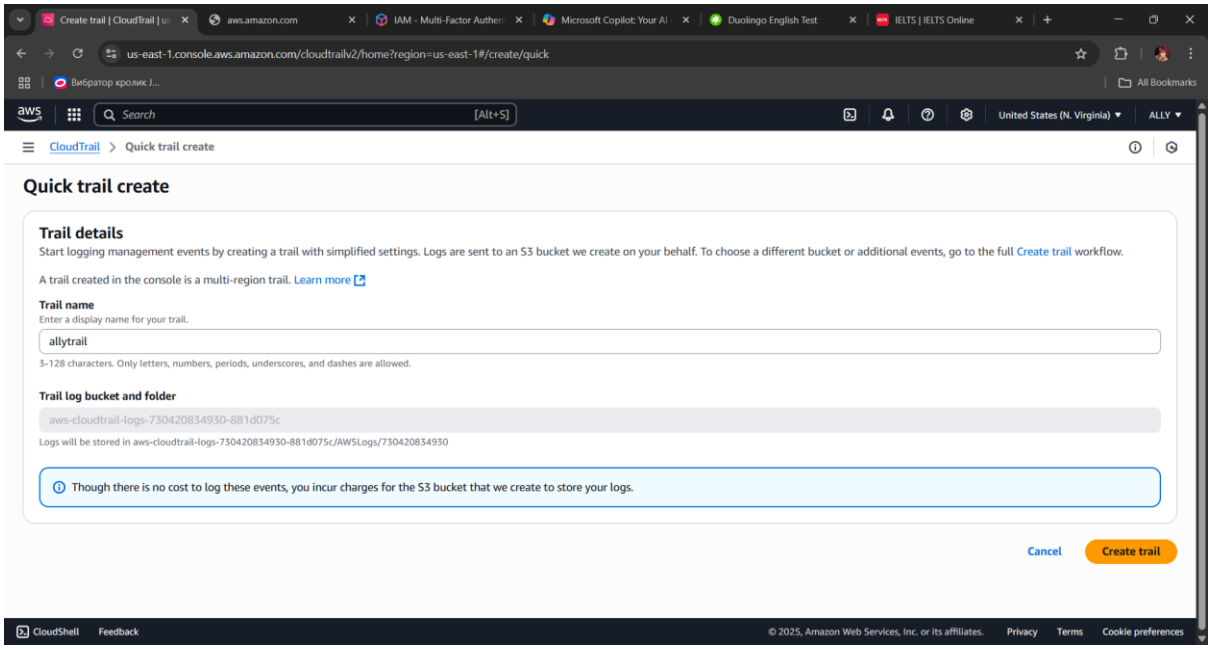


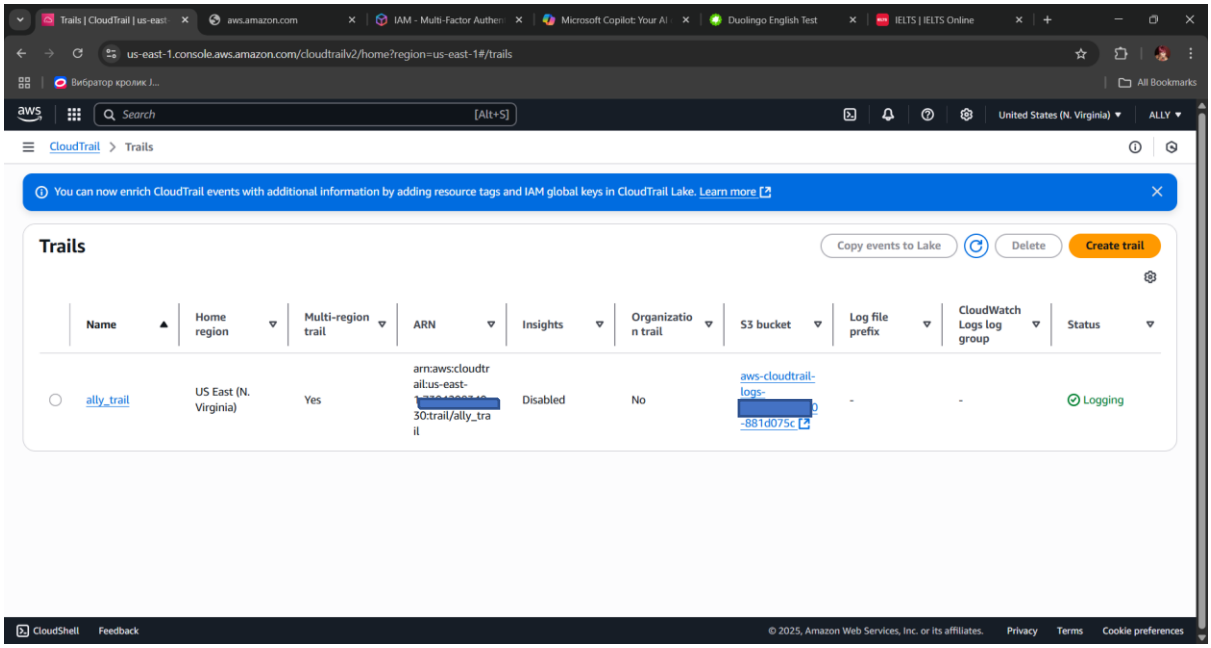
BILLING dashboard below

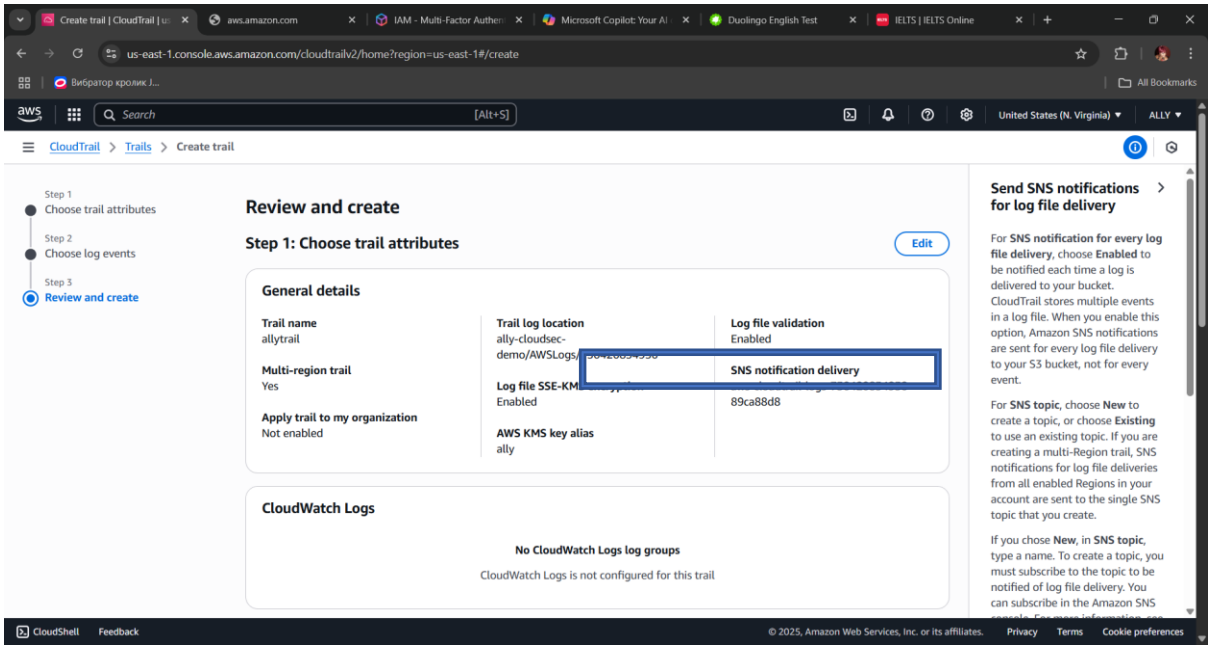

Billing and Cost Management
aws.amazon.com
IAM - Multi-Factor Authen
Microsoft Copilot: Your AI
Duolingo English Test
IELTS | IELTS Online
us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/home
All Bookmarks
aws
Billing and Cost Management
Choose billing view New
Primary view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Data Exports
Customer Carbon Footprint Tool
We're preparing your cost and usage data. This process can take up to 24 hours after you first visit the Billing and Cost Management console. In the meantime, you can view bills, make payments, and manage your preferences and settings. Once your data is ready, you can view cost breakdowns, forecasted costs, savings opportunities, and more on this page. To learn more about AWS Cloud Financial Management, visit the Getting started page.
Billing and Cost Management home Info
Provide feedback
Need help? Ask Q
Reset layout
Cost summary Info
Month-to-date cost
Data unavailable
Last month's cost for same time period
Data unavailable
Total forecasted cost for current month
Data unavailable
Last month's total cost
Data unavailable
View bill
Cost monitor Info
Budgets status
Setup required
No budget created
Cost anomalies status (MTD)
Setup required
No monitor created
Cost breakdown Info
Recommended actions (1) Info
Getting started
Create a Cost Anomaly monitor to automatically detect cost

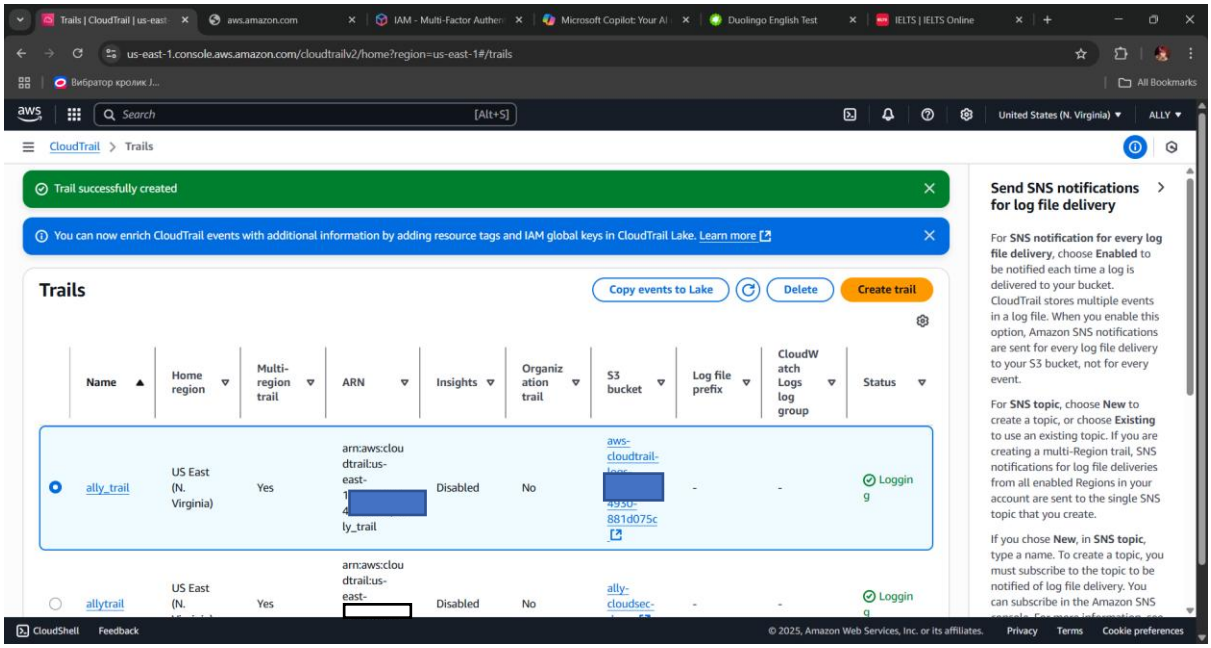
Enabling Cloudtrail in the account since I do not have it enabled.

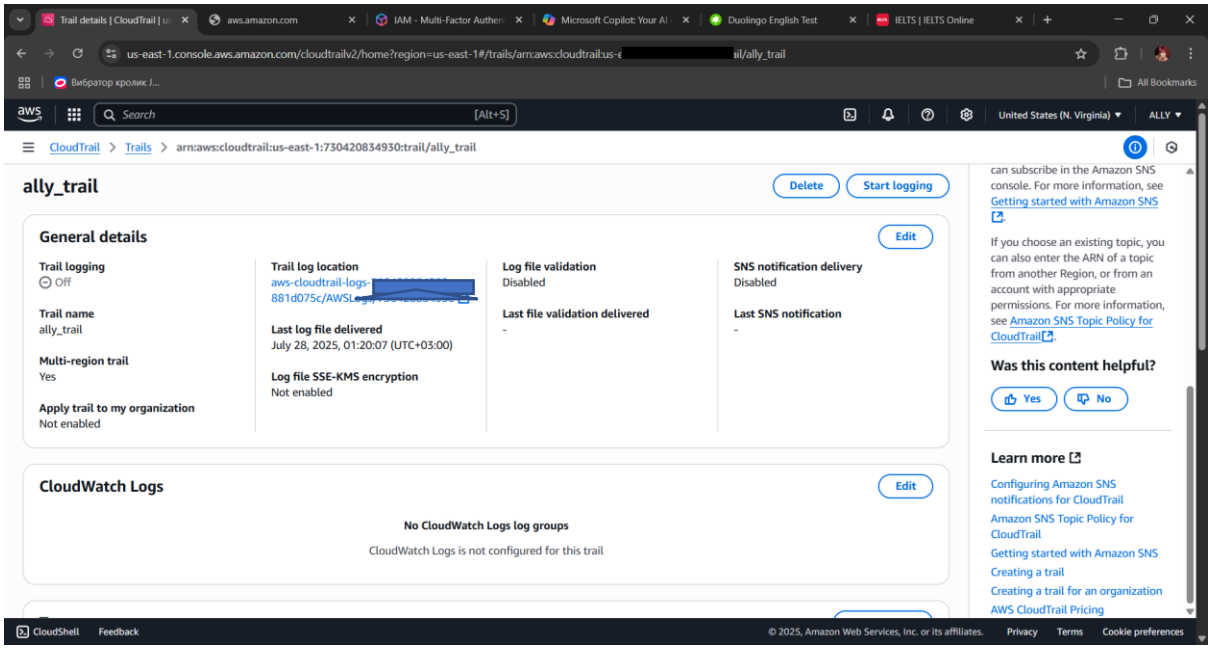


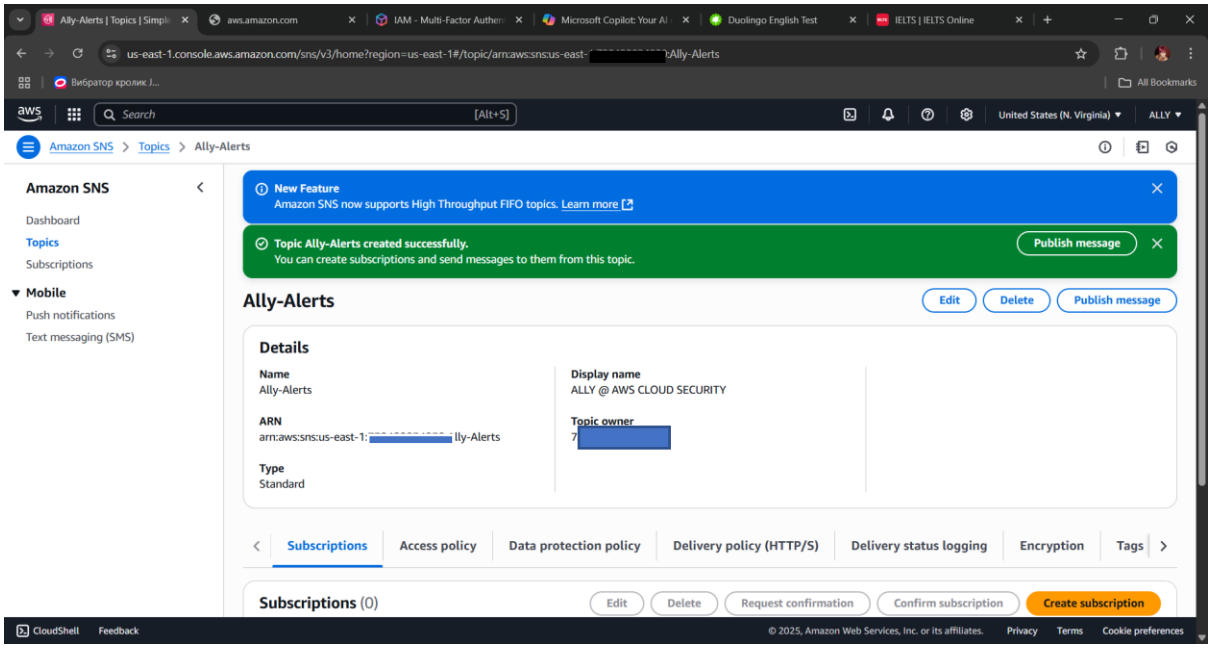


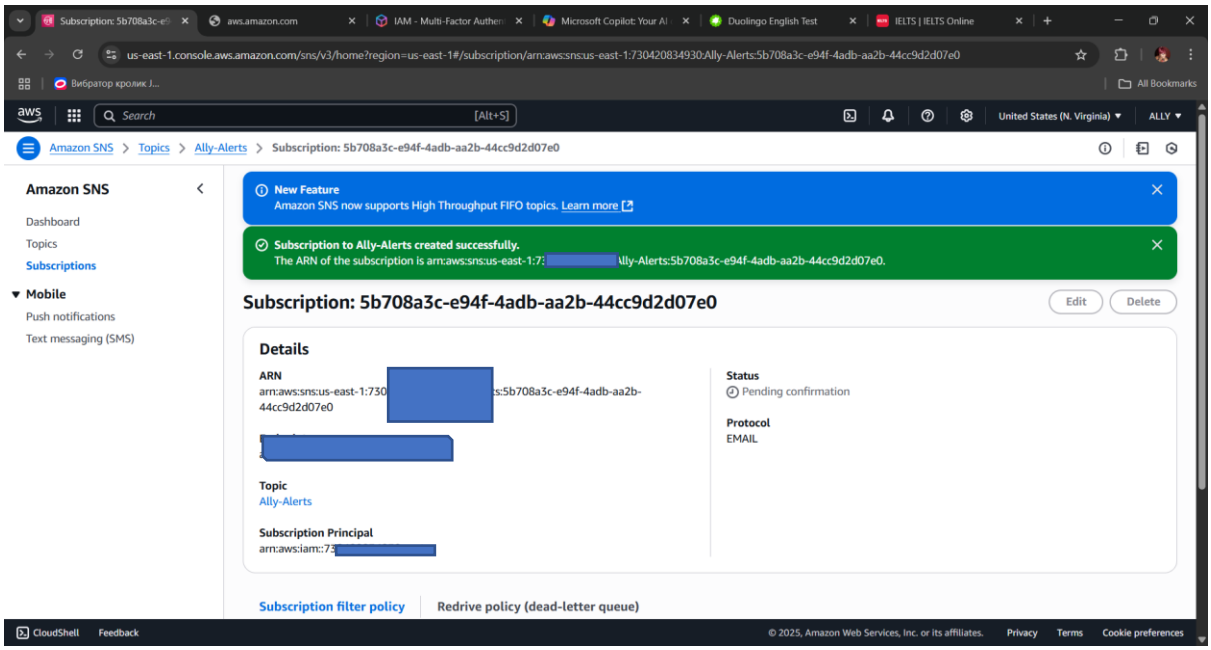

Trails | CloudTrail | us-east
aws.amazon.com
IAM - Multi-Factor Authen
Microsoft Copilot: Your AI
Duolingo English Test
IELTS | IELTS Online
us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/trails
Search
[Alt+S]
United States (N. Virginia)
ALLY
CloudTrail > Trails
You can now enrich 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
ally_trail
US East (N. Virginia)
Yes
arn:aws:cloudtrail:us-east-
30:trail/ally_trail
Disabled
No
aws-cloudtrail-logs-
-881d075c
-
-
Logging
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create trail | CloudTrail
aws.amazon.com
IAM - Multi-Factor Authen
Microsoft Copilot: Your AI
Duolingo English Test
IELTS | IELTS Online
us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/create
Search
[Alt+S]
United States (N. Virginia)
ALLY
CloudTrail > Trails > Create trail
Step 1
Choose trail attributes
Step 2
Choose log events
Step 3
Review and create
Review and create
Step 1: Choose trail attributes
Edit
General details
Trail name
allytrail
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
ally-cloudsec-demo/AWSLogs/
Log file SSE-KMS
Enabled
AWS KMS key alias
ally
Log file validation
Enabled
SNS notification delivery
89ca88d8
CloudWatch Logs
No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail
Send SNS notifications for log file delivery
For SNS notification for every log file delivery, choose Enabled to be notified each time a log is delivered to your bucket. CloudTrail stores multiple events in a log file. When you enable this option, Amazon SNS notifications are sent for every log file delivery to your S3 bucket, not for every event.
For SNS topic, choose New to create a topic, or choose Existing to use an existing topic. If you are creating a multi-Region trail, SNS notifications for log file deliveries from all enabled Regions in your account are sent to the single SNS topic that you create.
If you chose New, in SNS topic, type a name. To create a topic, you must subscribe to the topic to be notified of log file delivery. You can subscribe in the Amazon SNS
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

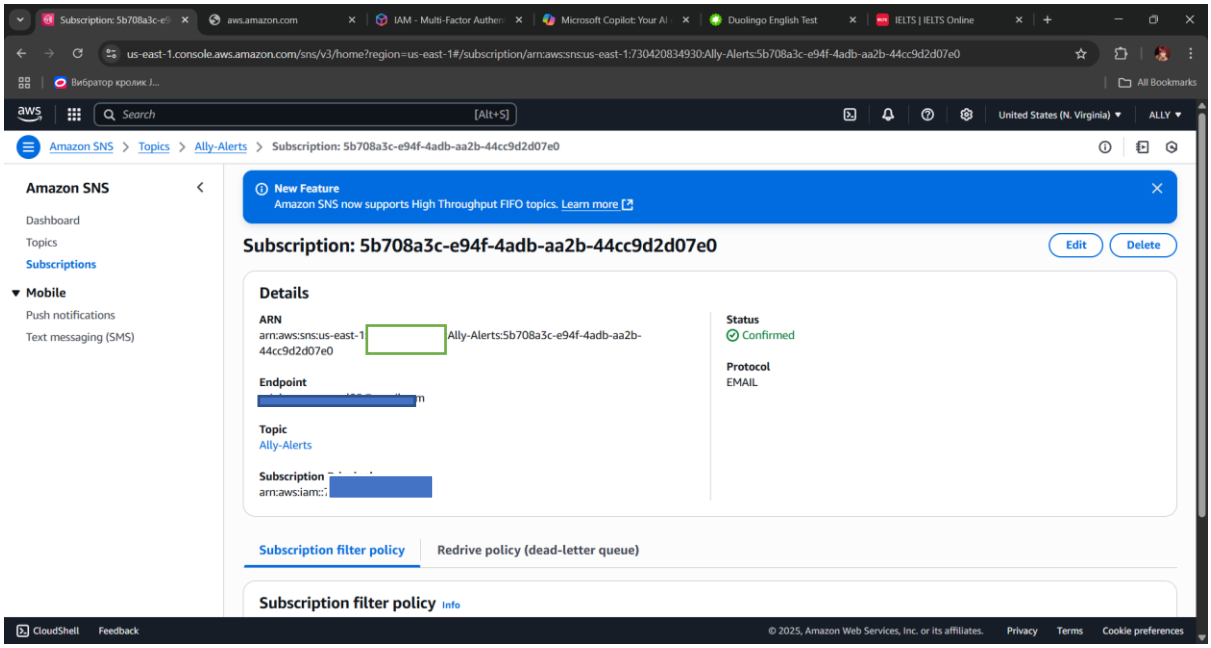

Trails | CloudTrail | us-east
us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/trails
CloudTrail > Trails
Trail successfully created
You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more
Trails
Copy 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
ally_trail
US East (N. Virginia)
Yes
Disabled
No
Logging
allytrail
Send SNS notifications for log file delivery
For SNS notification for every log file delivery, choose Enabled to be notified each time a log is delivered to your bucket. CloudTrail stores multiple events in a log file. When you enable this option, Amazon SNS notifications are sent for every log file delivery to your S3 bucket, not for every event.
For SNS topic, choose New to create a topic, or choose Existing to use an existing topic. If you are creating a multi-Region trail, SNS notifications for log file deliveries from all enabled Regions in your account are sent to the single SNS topic that you create.
If you chose New, in SNS topic, type a name. To create a topic, you must subscribe to the topic to be notified of log file delivery. You can subscribe in the Amazon SNS
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

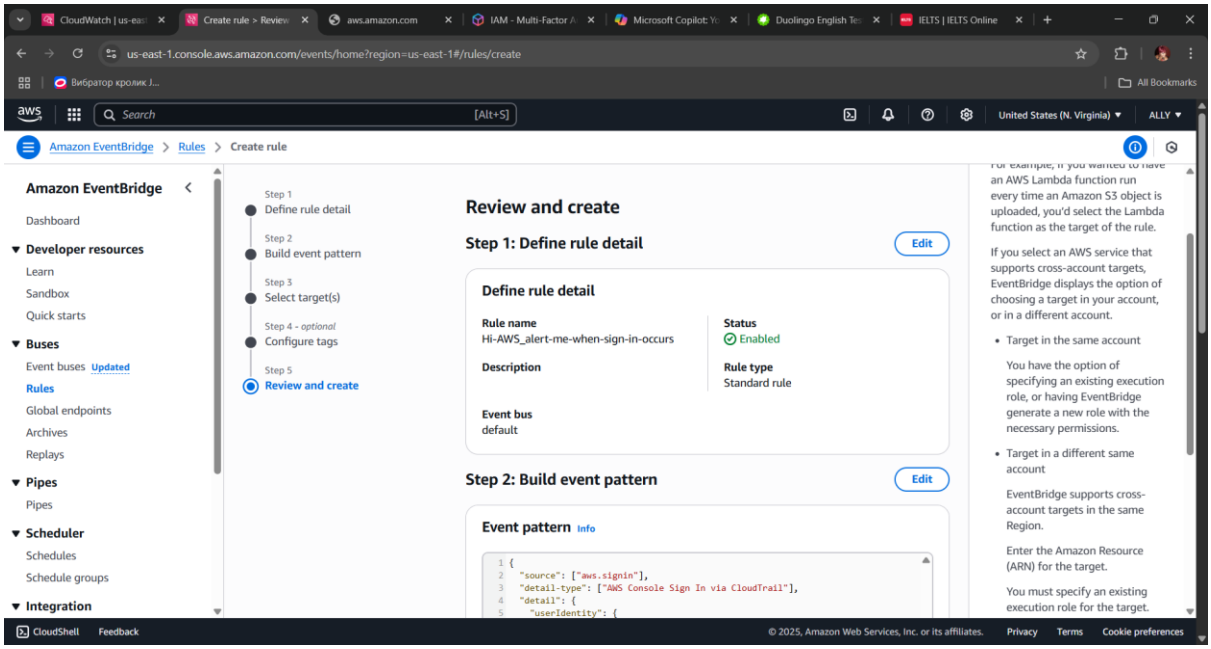

Trail details | CloudTrail
CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:730420834930:trail/ally_trail
ally_trail
Delete
Start logging
General details
Edit
Trail logging
Off
Trail name
ally_trail
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
Last log file delivered
July 28, 2025, 01:20:07 (UTC+03:00)
Log file SSE-KMS encryption
Not enabled
Log file validation
Disabled
Last file validation delivered
SNS notification delivery
Disabled
Last SNS notification
CloudWatch Logs
No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail
can subscribe in the Amazon SNS console. For more information, see Getting started with Amazon SNS.
If you choose an existing topic, you can also enter the ARN of a topic from another Region, or from an account with appropriate permissions. For more information, see Amazon SNS Topic Policy for CloudTrail.
Was this content helpful?
Yes
No
Learn more
Configuring Amazon SNS notifications for CloudTrail
Amazon SNS Topic Policy for CloudTrail
Getting started with Amazon SNS
Creating a trail
Creating a trail for an organization
AWS CloudTrail Pricing
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

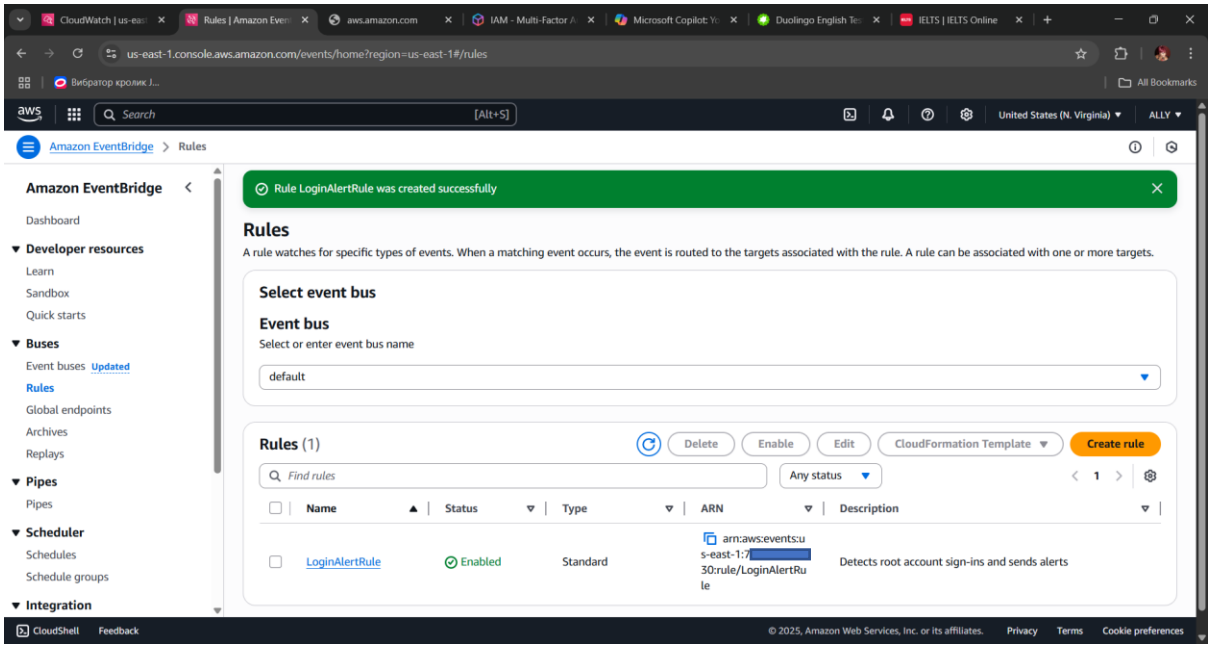

Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
Topic Ally-Alerts created successfully.
You can create subscriptions and send messages to them from this topic.
Publish message
Ally-Alerts
Edit
Delete
Publish message
Details
Name
Ally-Alerts
Display name
ALLY @ AWS CLOUD SECURITY
ARN
Topic owner
Type
Standard
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status logging
Encryption
Tags
Subscriptions (0)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription


Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
Subscription to Ally-Alerts created successfully.
Subscription: 5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0
Edit
Delete
Details
ARN
Status
Pending confirmation
Protocol
EMAIL
Topic
Ally-Alerts
Subscription Principal
Subscription filter policy
Redrive policy (dead-letter queue)

CONFIRMED


Amazon SNS > Topics > Ally-Alerts > Subscription: 5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0
Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
Subscription: 5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0
Edit
Delete
Details
ARN
arn:aws:sns:us-east-1 Ally-Alerts:5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0
Endpoint
Topic
Ally-Alerts
Subscription
Status
Confirmed
Protocol
EMAIL
Subscription filter policy
Redrive policy (dead-letter queue)
Subscription filter policy Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
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
Review and create
Step 1: Define rule detail
Edit
Define rule detail
Rule name
Hi-AWS_alert-me-when-sign-in-occurs
Status
Enabled
Description
Rule type
Standard rule
Event bus
default
Step 2: Build event pattern
Edit
Event pattern Info
{
"source": ["aws.signin"],
"detail-type": ["AWS Console Sign In via CloudTrail"],
"detail": {
"userIdentity": {
an AWS Lambda function run every time an Amazon S3 object is uploaded, you'd select the Lambda function as the target of the rule.
If you select an AWS service that supports cross-account targets, EventBridge displays the option of choosing a target in your account, or in a different account.
Target in the same account
You have the option of specifying an existing execution role, or having EventBridge generate a new role with the necessary permissions.
Target in a different same account
EventBridge supports cross-account targets in the same Region.
Enter the Amazon Resource (ARN) for the target.
You must specify an existing execution role for the target.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



I have done everything but after loging in and out, I do not receive an alert in my email.